Complexity Classification of Counting Problems on Boolean Variables

By

Shuai Shao

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

(Computer Sciences)

at the

UNIVERSITY OF WISCONSIN – MADISON

2020

Date of final oral examination: September 30, 2020

The dissertation is approved by the following members of the Final Oral Committee:

Jin-Yi Cai (advisor), Computer Sciences

Eric Bach, Computer Sciences

Shuchi Chawla, Computer Sciences

Alberto Del Pia, Industrial and Systems Engineering

Christos Tzamos, Computer Sciences

致母亲、父亲，

“谁言寸草心，报得三春晖。”

Acknowledgements

First and foremost, I am extremely grateful to my advisor, Jin-Yi Cai for his invaluable advice, continuous support, and patience during my Ph.D. studies. His guidance and wisdom helped me in all the time of my research and daily life. During a truly frustrating period, I lost all my confidence, my energy, and my passion. It is you who have always been so supportive and patient. Without your support and encouragement, this thesis would not have been possible. Nothing could express my appreciation here.

I would like to express my sincere gratitude to Zhiguo Fu, from whom I learned a lot. He generously and scrupulously shared his expertise with me when I started working on the topic of this thesis. I am very grateful to Yuxin Sun for many fantastic discussions that attracted me to a new research area. My sincere thanks also go to Mingji Xia. Although not (yet) one of my coauthors, some of the work in this thesis would not have been possible without his inspiration. To all of them, I am looking forward to more collaboration opportunities in the future.

I am deeply indebted to Eric Bach, Shuchi Chawla, Alberto Del Pia, and Christos Tzamos for the burden they took to serve on my committee, and for the excellent classes they taught me. Special thanks go to Shuchi and Christos for the algorithm reading group they have been organizing, which broadened my horizons.

I am fortunate to have a group of friends who gave me the feeling of a warm family here. I thank my fellow students Artem Govorov, Tianyu Liu, and Yifeng Teng in the theory group, and Yanfang Le, Qisi Wang, Yijing Zeng, and Xiaomin Zhang in the CS department for countless conversations about both our research and Ph.D. lives. In particular, I thank Qisi and Tianyu for teaching me coding and helping me debug when I struggled with CS breadth courses in my first year here. I thank my friends Ming Gao, Jiatong Li, Dongyue Liang, Boyuan Liu, Linquan Ma, Siyu Wang, and Qijun Zhang for all the enjoyable moments that distract me from research. I also thank my friend Yiming Huang back in China who is always available when I need a travel buddy.

Last but not least, Mom and Dad, thank you for everything that you have done and will continue to do for me. This is for you.

Abstract

This dissertation furthers a systematic study of the complexity classification of counting problems. A central goal of this study is to prove complexity classification theorems which state that every problem in some large class is either polynomial-time computable (tractable) or #P-hard. Such classification results are important as they tend to give a unified explanation for the tractability of certain counting problems and a reasonable basis for the conjecture that the remaining problems are inherently intractable. In this dissertation, we focus on the framework of Holant problems on Boolean variables, as well as other frameworks that are expressible as Holant problems, such as counting constraint satisfaction problems and counting Eulerian orientation problems.

First, we prove a complexity dichotomy for Holant problems on the Boolean domain with arbitrary sets of real-valued constraint functions. It is proved that for every set $\mathcal{F}$ of real-valued constraint functions, Holant($\mathcal{F}$) is either tractable or #P-hard. The classification has an explicit criterion. This is a culmination of much research on this decade-long study, and it uses many previous results and techniques. On the other hand, to achieve the present result, many new tools were developed, and a novel connection with quantum information theory was built. In particular, two functions exhibiting intriguing and extraordinary closure properties are related to Bell states in quantum information theory. Dealing with these functions plays an important role in the proof.

Then, we consider the complexity of Holant problems with respect to planar graphs, where physicists had discovered some remarkable algorithms, such as the FKT algorithm for counting planar perfecting matchings in polynomial time. For a basic case of Holant problems, called six-vertex models, we discover a new tractable class over planar graphs beyond the reach of the FKT algorithm. After carving out this new planar tractable class which had not been discovered for six-vertex models in the past six decades, we prove that everything else is #P-hard, even for the planar case. This leads to a complete complexity classification for planar six-vertex models. This result is the first substantive advance towards a planar Holant classification with asymmetric constraints.

We hope this work can help us better understand a fundamental question in theoretical computer science: *What does it mean for a computational counting problem to be easy or to be hard?*

Index of Notations

Signatures

$=_2$	Binary Equality signature $(1,0,0,1)$	p.7
$=_n$	Equality signature of arity n	p.16
$\neq_2$	Binary Disequality signature $(0,1,1,0)$	p.7
$\neq_{2n}$	Disequality signature or arity $2n$	p.16
$=_2^-$	Binary signature $(1,0,0,-1)$	p.27
$\neq_2^-$	Binary signature $(0,1,-1,0)$	p.27
Δ_0	Unary signature $(1,0)$	p.35
Δ_1	Unary signature $(0,1)$	p.35

Signature Sets

$\mathcal{EQ}_k$	$\{=_k, =_{2k}, \ldots, =_{nk}, \ldots\}$, $(\mathcal{EQ} = \mathcal{EQ}_1)$	p.16
$\mathcal{DEQ}$	$\{\neq_2, \neq_4, \ldots, \neq_{2n}, \ldots\}$	p.16
$\mathcal{B}$	$\{=_2, =_2^-, \neq_2, \neq_2^-\}$	p.27
$\widehat{\mathcal{B}}$	$Z^{-1}\mathcal{B} = \{\neq_2, =_2, (-\mathfrak{i})\cdot =_2^-, \mathfrak{i}\cdot \neq_2^-\}$	p.27
$\mathcal{O}$	Binary orthogonal signatures (Definition 3.16) and binary zero signature	p.33
$\widehat{\mathcal{O}}$	$Z^{-1}\mathcal{O}$, binary signatures with ars and parity	p.33
$\mathcal{E}$	Binary EO signatures satisfying ars, $(\mathcal{E}_{\not\equiv 0} = \{f \in \mathcal{E} \mid f \not\equiv 0\})$	p.43
$\mathcal{D}$	$\{\neq_2\}$	p.53
$\mathscr{P}$	Product-type signatures (Definition 2.5)	p.8
$\mathscr{A}$	Affine signatures (Definition 2.7)	p.8
$\mathscr{L}$	Local affine signatures (Definition 2.13)	p.10
$\mathscr{T}$	Tensor products of unary and binary signatures (Definition 2.5)	p.8
$\mathscr{T}_1$	Tensor products of unary signatures	p.104
$\mathscr{M}$	Matchgate signatures	p.239
$\widehat{\mathscr{M}}$	$H\mathscr{M}$	p.240

Matrices

H	$\frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$	p.10
H_4	$\left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{smallmatrix}\right]$	p.153
I_2	$\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $(I_4 = I_2^{\otimes 2})$	p.10
N_2	$\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, $(N_4 = N_2^{\otimes 2})$	p.10
T_{α^s}	$\left[\begin{smallmatrix} 1 & 0 \\ 0 & \alpha^s \end{smallmatrix}\right]$ where $\alpha = e^{\frac{\mathfrak{i}\pi}{4}} = \frac{1+\mathfrak{i}}{\sqrt{2}}$ and s is an integer	p.10
Z^{-1}	$\frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & -\mathfrak{i} \\ 1 & \mathfrak{i} \end{smallmatrix}\right]$	p.19
$\mathbf{O}_2$	$\{\left[\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right], \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$	p.18
$\widehat{\mathbf{O}_2}$	$\{\widehat{Q} = Z^{-1}QZ \mid Q \in \mathbf{O}_2\}$=$\{\left[\begin{smallmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & \alpha \\ \bar{\alpha} & 0 \end{smallmatrix}\right] \mid \alpha \in \mathbb{C}, \lvert\alpha\rvert = 1\}$	p.18

Gadget Constructions

∂_{ij} or ∂_{ij}^{+}	Merging gadget using $=_2$ on variables x_i and x_j	p.28
$\widehat{\partial}_{ij}$, $\widehat{\partial}_{ij}^{+}$, or $\partial_{ij}^{\widehat{+}}$	Merging gadget using $\neq_2$ on variables x_i and x_j	p.28
∂_{ij}^{-}	Merging gadget using $=_2^{-}$ on variables x_i and x_j	p.28
$\partial_{ij}^{\widehat{-}}$	Merging gadget using $\neq_2^{-}$ on variables x_i and x_j	p.28
∂_{ij}^{b}	Merging gadget using $b \in \mathcal{B}$ on variables x_i and x_j	p.143
$\mathfrak{m}_{ij}$	Mating gadget using $=_2$ with dangling variables x_i and x_j	p.33
$\widehat{\mathfrak{m}}_{ij}$	Mating gadget using $\neq_2$ with dangling variables x_i and x_j	p.33
$\{f\}_{=_2}^{\mathcal{B}}$	Extending gadget with binary signatures in $\mathcal{B}$ using $=_2$	p.30
$\{\widehat{f}\}_{\neq_2}^{\widehat{\mathcal{B}}}$	Extending gadget with binary signatures in $\widehat{\mathcal{B}}$ using $\neq_2$	p.30
f_i^0	Pinning gadget using Δ_0 on variable x_i	p.35
f_i^1	Pinning gadget using Δ_1 on variable x_i	p.35

Properties

Δ-property	Triangle property	p.46
$f \in \int_{\mathcal{B}} \mathscr{A}$	$\partial_{ij}^{b} f \in \mathscr{A}$ for all $\{i, j\}$ and every $b \in \mathcal{B}$	p.145

$f \in \widehat{\int} \mathcal{E}^{\otimes}$	$\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ for all $\{i, j\}$	p.46
$f \in \int_1 \mathscr{T}_1$	$f_i^0 \in \mathscr{T}_1$ for all i	p.104
$f \in \int_{12} \mathscr{T}$	$f_i^0 \in \mathscr{T}$ and $\partial_{jk} f \in \mathscr{T}$ for all i and all $\{j, k\}$	p.104
ARS	Arrow reversal symmetry (Definition 2.35)	p.19
1st-Orth	First order orthogonality (Definition 3.13)	p.32
2nd-Orth	Second order orthogonality (Definition 3.20)	p.34

Binary String Related

$\vec{0}^n$, $\vec{1}^n$	n-bit all-0, all-1 strings (we may omit the superscript n)	p.16
$\mathrm{wt}(\alpha)$	Hamming weight of $\alpha \in \mathbb{Z}_2^n$	p.10
α_i	The i-th bit of $\alpha \in \mathbb{Z}_2^n$	p.10
$\mathscr{S}(f)$	Support of signature f	p.8
$\mathscr{H}_{2n}$	$\{\alpha \in \mathbb{Z}_2^{2n} \mid \mathrm{wt}(\alpha) = n\}$	p.10
$\mathscr{E}_n$	$\{\alpha \in \mathbb{Z}_2^n \mid \mathrm{wt}(\alpha) \text{ is even}\}$	p.33
$\mathscr{O}_n$	$\{\alpha \in \mathbb{Z}_2^n \mid \mathrm{wt}(\alpha) \text{ is odd}\}$	p.33

Other Common Symbols

$\mathbb{Z}_2$	$\{0, 1\}$	
$\mathbb{R}$	Real numbers	
$\mathbb{C}$	Complex numbers	
$\mathfrak{i}$	$\sqrt{-1}$	p.8
$[n]$	$\{1, 2, \ldots, n\}$	
$\leqslant_T$ & $\equiv_T$	polynomial-time Turing reductions and equivalences	p.10
iff	if and only if	

Contents

Acknowledgements **ii**

Abstract **iii**

Index of Notations **iv**

1 Introduction **1**

2 Frameworks of Counting Problems **6**

2.1 Counting Constraint Satisfaction Problems (#CSP) 6

2.1.1 Definition and Examples 6

2.1.2 Existing Dichotomies for #CSP 7

2.2 Counting Eulerian Orientation Problems (#EO Problems) 10

2.2.1 Definition and Examples 10

2.2.2 #EO Problems Encompass #CSP 11

2.3 Holant Problems 15

2.3.1 Definition and Examples 15

2.3.2 Holographic Transformation 17

2.4 Sample Problems 20

3 Polynomial-Time Reductions **23**

3.1 Signature Factorization 23

3.2 Gadget Construction 26

3.2.1 Merging Gadget 28

3.2.2 Extending Gadget 30

3.2.3 Mating Gadget 31

3.2.4 Pinning Gadget 35

3.3 Polynomial Interpolation 36

4 Dichotomy for #EO Problems with Arrow Reversal Symmetry 38

4.1 Factorization and Gadget Construction of EO Signatures 38

4.2 Reduction from Six-Vertex Models to #EO problems 40

4.3 Interplay of Unique Prime Factorization and Merging Gadgets 45

4.4 Reduction from #CSP to #EO Problems 59

4.5 Putting Things Together 65

5 Dichotomy for Real Holant Problems with an Odd-ary Signature 66

5.1 Realization of Pinning or Equality Signatures 66

5.2 #P-Hardness of Holant($\neq_2|=_k, \widehat{\mathcal{F}}$) 68

5.3 #P-Hardness of Holant($\Delta_0, \mathcal{F}$) 95

5.4 Putting Things Together 110

6 Building Blocks of Even Arity: Binary and 4-ary Signatures 112

6.1 First and Second Order Orthogonality 112

6.2 The Induction Proof: Base Cases $2n \leqslant 4$ 119

7 First Major Obstacle: 6-ary Signatures with the Bell Property 123

7.1 The Discovery of $\widehat{f_6}$ 123

7.2 #P-Hardness Conditions and Two Properties of $\widehat{f_6}$ 139

7.3 #P-Hardness of Holant$^b(\mathcal{F})$ 144

7.3.1 Parity Condition 145

7.3.2 Norm Condition 147

7.3.3 Support Condition 175

7.3.4 Affine Signature Condition 189

8 Final Obstacle: An 8-ary Signature with the Strong Bell Property 197

8.1 The Discovery of f_8 197

8.2 Holant Problems with Limited Appearance 219

8.3 The Induction Proof: $2n \geqslant 10$ 223

8.4 Proof of the Real Holant Dichotomy 224

9 Trichotomy for Planar Six-Vertex Models 226

9.1 Background 226

9.2 Preliminaries 229

9.2.1 Problem Definition 229

9.2.2 Planar Gadget Construction 230

9.2.3 More on Polynomial Interpolation 233

9.2.4 Matchgate Signatures 238

9.2.5 Known Dichotomies and Hardness Results 241

9.3 Trichotomy Theorem, Proof Outline and Sample Problems 242

9.4 Case II: One Zero Pair 248

9.5 Case III: $\mathsf{N} = 2$ with No Zero Pair or $\mathsf{N} = 1$ with Zero in an Outer Pair 272

9.6 Case IV: $\mathsf{N} = 1$ with Zero in the Inner Pair or $\mathsf{N} = 0$ 277

9.7 Proof of the Trichotomy Theorem 299

10 Conclusion and Outlook 300

Bibliography 302

Chapter 1

Introduction

Counting problems arise in many different fields, e.g., statistical physics, economics and machine learning. In order to study the complexity of counting problems, several natural frameworks have been proposed. Two well studied frameworks are counting constraint satisfaction problems (#CSP) and counting graph homomorphisms (#GH). #GH is a special case of #CSP. These frameworks are expressive enough so that they can express many natural counting problems, e.g., counting satifiability, hard-core models, Ising models and spin systems [67, 46, 5, 47, 43, 55], but also specific enough so that complete complexity classifications can be established.

Such complexity classification results are usually stated as dichotomy results: For a large family of problems in a certain framework, each of them is either in FP or #P-hard. The #P class [67, 68] is the quantitative version of the NP class. A #P problem corresponds to its NP-version by changing the question from asking the existence of a solution to asking the number of solutions. FP is the class of #P problems that are polynomial-time computable (tractable). By a straightforward adoption of Ladder's theorem [52], complexity dichotomy does not hold for the #P class in general assuming FP≠#P, and concrete artificial #P-intermediate (properly between FP and #P-hard) problems can be designed. However, so far there is no natural counting problem that is proved to be #P-intermediate. Furthermore, many natural problems, such as problems expressible as #CSP and #GH, are indeed either in FP or #P-hard. Full complexity dichotomies have been established for #CSP and #GH problems defined by arbitrary complex-valued constraint functions over general domain [11, 38, 12, 17, 15, 37, 13, 42, 16]. These dichotomy results are important in theory as they tend to give a unified explanation for the tractability of certain problems and a reasonable basis for the conjecture that the remaining problems are intractable. They are also important in practice as they lead to novel efficient algorithms for many types of natural problems.

Despite the significance and wide application of #CSP and #GH, they are not known to be able to encompass some pivotal counting problems, such as counting perfect matchings (#PM). In fact, it is proved that #PM cannot be expressed by #GH with arbitrary complex weights [41, 34, 63, 27]. Inspired by holographic transformations [71, 72], a more expressive framework, the Holant problem was introduced by Cai, Lu and Xia [30]. It is a broad class of sum-of-products computation that generalizes #CSP and #GH, and naturally expresses #PM and counting matchings. Other problems expressible as Holant problems include counting weighted Eulerian orientations (#EO problems) [58, 23], computing the partition functions of six-vertex models [61, 25] and eight-vertex models [6, 19], and a host of other, if not almost all, vertex models from statistical physics [7].

Unlike #CSP and #GH, the understanding of Holant problems, even restricted to the Boolean domain, is still limited. In this dissertation, we focus on the complexity classification of Holant problems on the Boolean domain. A Boolean Holant problem Holant($\mathcal{F}$) is parameterized by a set $\mathcal{F}$ of constraint functions (also called signatures) on the Boolean domain. A signature $f \in \mathcal{F}$ of arity $n > 0$ on the Boolean domain is a map $\mathbb{Z}_2^n \to \mathbb{C}$.

Built on the dichotomy for #CSP on the Boolean domain [31], progress has been made in the complexity classification of Boolean Holant problems. When all signatures are restricted to be *symmetric* (the function value depends only on the Hamming weight of the input), a dichotomy for complex-valued Holant problems was established [28].

For asymmetric signatures, the first result is a dichotomy for a restricted class called Holant* problems where all unary signatures are assumed to be available [28]. Later, it was generalized to (first real-valued [32] and then complex-valued [3, 4]) Holant^c problems where two pinning unary signatures are available. In addition, based on the dichotomy for Holant* problems, a dichotomy for non-negative Holant problems was proved [57] without assuming any auxiliary signatures. Simultaneously, progress has been made for Holant problems parameterized by complex-valued signatures of even arities. The base case is a single 4-ary signature which includes six-vertex models and eight-vertex models. (The case that all signatures are binary is known to be tractable.) A dichotomy is proved for complex-valued six-vertex models [25] and later it was generalized to complex-valued eight-vertex models [19].

In the first part of this dissertation, we establish the first Holant dichotomy on the Boolean domain with arbitrary real-valued constraint functions. These constraint functions need not be symmetric nor do we assume any auxiliary functions.

Theorem 1.1. *Let $\mathcal{F}$ be a set of real-valued signatures. If $\mathcal{F}$ satisfies the tractability condition* (T) *stated in Theorem 2.33, then* $\operatorname{Holant}(\mathcal{F})$ *is polynomial-time computable; otherwise, it is #P-hard.*

This theorem is the culmination of a large part of previous research on dichotomy theorems of Holant problems. However, the journey to this theorem is arduous.

First, as a special case of Holant problems, we introduce the framework of counting Eulerian orientation problems (#EO problems). This framework generalizes six-vertex models from arity 4 to general arities. However, quite surprisingly, #EO problems also encompass all #CSP problems on Boolean variables. In Chapter 2, we define the frameworks of #CSP, #EO problems, and Holant problems, and show their connections. In Chapter 3, we introduce some common polynomial-time reductions. In Chapter 4, we prove a dichotomy for #EO problems with complex-valued constraint functions under a symmetry assumption, called *arrow reversal symmetry* (ARS). Under a suitable holographic transformation, these #EO problems with ARS correspond to precisely a class of real valued Holant problems. The dichotomy of #EO problems with ARS will serve as a building block for the dichotomy of real-valued Holant problems.

Then, we start proving the real Holant dichotomy (Theorem 1.1). We first consider the case that $\mathcal{F}$ contains a nonzero signature of odd-arity in Chapter 5. For the case that $\mathcal{F}$ consists of signatures of even arities. We prove the dichotomy by induction on arities of signatures in $\mathcal{F}$. We consider the base cases that $\mathcal{F}$ contains a binary or 4-ary signature in Chapter 6. Then, we give two particularly intriguing signatures of arity 6 and 8 with some extraordinary closure properties related to Bell states [9] in quantum information theory. Their existence presented a formidable obstacle to the induction proof. We deal with them in Chapters 7 and 8 respectively. Finally, in the last two sections of Chapter 8, we give the induction proof for signatures of arity at least 10, and finish the proof of Theorem 1.1. Results in Chapters 4 to 8 are joint work with Jin-Yi Cai and Zhiguo Fu [23, 24, 64].

Theorem 1.1 delineates all real Holant problems that are polynomial-time computable over general graphs. However, a more interesting question is what happens on planar structures, where physicists had discovered some remarkable algorithms, such as the FKT algorithm [66, 49, 48]. By the FKT algorithm, #PM which is #P-hard in general, is polynomial-time computable when restricted to planar graphs. This algorithm was viewed as a great triumph in statistical physics for a long line of research on *exactly solved models* [60, 73, 74, 54, 56, 8].

To extend the reach of the FKT algorithm, Valiant introduced matchgates [69, 70] and holographic transformations to the FKT algorithm [71, 72], and discovered a number of counting problems that are tractable over planar graphs, but #P-hard in general. After several developments on the theory of matchgates [18, 29, 26], Cai and Fu proved that for a large class of counting problems, such as all #CSP problems on Boolean variables, holographic transformations to the FKT algorithm is a universal technique to solve all problems that are tractable over planar graphs but #P-hard in general [20]. Taking into account of the planar restriction, a complexity trichotomy was established for #CSP on the Boolean domain: every problem in this framework is either (1) tractable for every graph, or (2) #P-hard for general graphs but tractable for planar graphs, or (3) #P-hard even for planar graphs.

However, when it comes to Holant problems, there are *new* planar tractable problems that are *not* solvable by a holographic transformation to the FKT algorithm. After carving out this new planar tractable class, a complete complexity classification was proved for planar Boolean Holant problems where all signatures are symmetric [21].

In the second part of this dissertation, we make the first substantive advance towards a classification of planar Holant problems with asymmetric signatures. We consider the complexity classification of planar six-vertex models without assuming ARS. Previously, without being able to account for tractability on planar graphs, a complexity dichotomy was proved in [25]. Due to the presence of nontrivial algorithms, a complete complexity classification in the planar case is much more difficult to achieve. Not only are reductions to FKT expected to give planar tractable cases that are #P-hard in general, but also a more substantial obstacle awaits us. It turns out that there is *another* planar tractable case that had not been discovered for the six-vertex model in all these decades, until our result. We give this new planar tractable case and prove a complete complexity classification of planar six-vertex models in Chapter 9. This result is joint work with Jin-Yi Cai and Zhiguo Fu [22].

We give the following Figure 1 as a partial map of the complexity classification program for Holant problems on the Boolean domain. The ultimate goal is definitely a complete complexity classification for all complex-valued Holant problems. First, without considering the planar restriction, to achieve a classification for complex-valued Holant problems over general graphs, we think a classification for complex-valued #EO problems *without* assuming ARS may serve as a building block. We may also need to generalize the dichotomy for real-valued Holant problems with an odd-ary signature to complex-valued. Secondly, if we take account of the planar restriction, there is still a long way to go. We think a complexity classification of planar eight-vertex models and a complexity classification of planar Holant* problems are the two potential points where one can further explore.

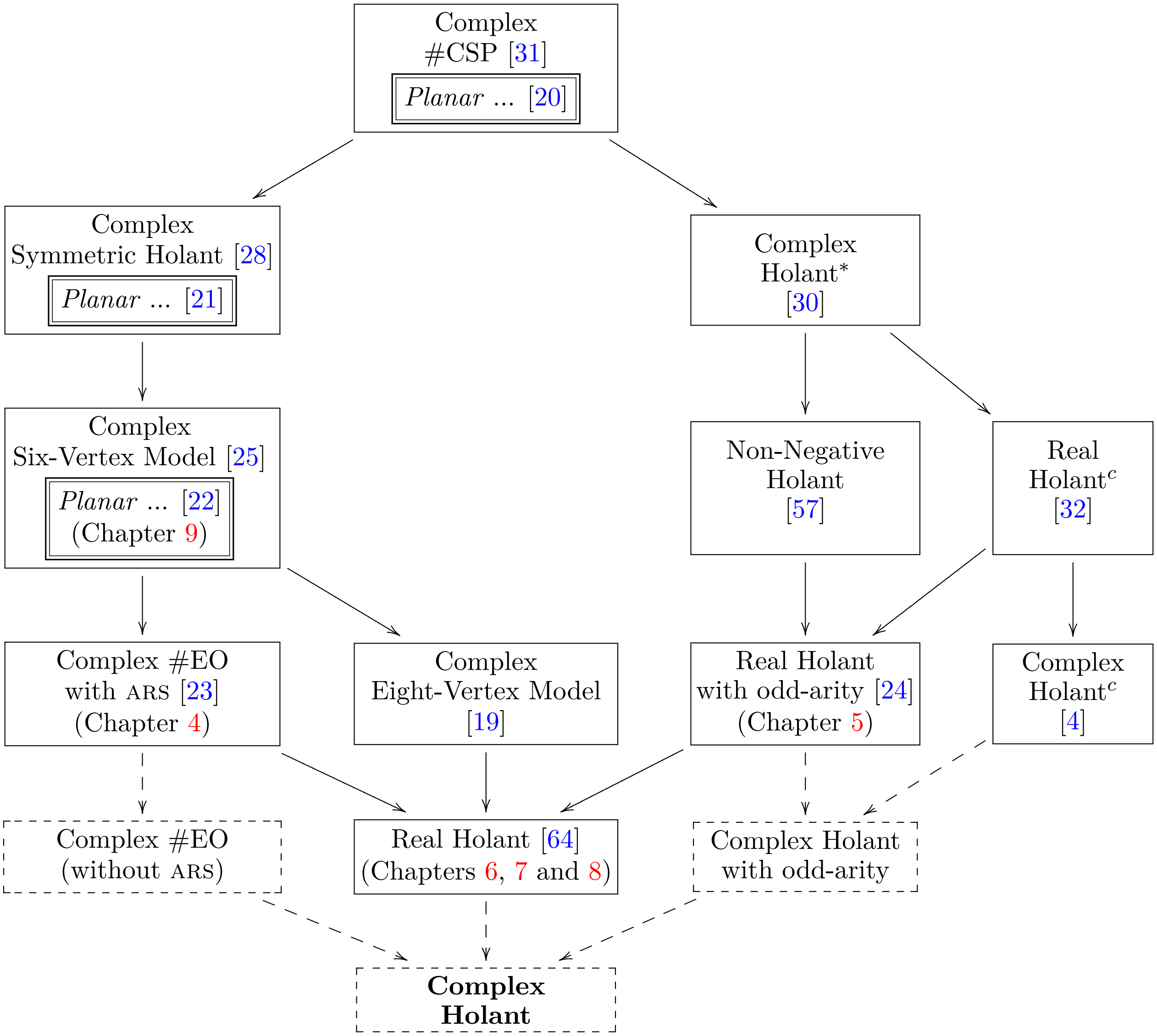


图 1: A partial map of the complexity classification program for Holant problems

Chapter 2

Frameworks of Counting Problems

In this chapter, we define three frameworks of Boolean counting problems that will be studied in this dissertation. They are counting constraint satisfaction problems (#CSP), counting Eulerian orientation problems (#EO problems) and Holant problems. We give some families of signatures that are known to be tractable in these frameworks.

2.1 Counting Constraint Satisfaction Problems (#CSP)

2.1.1 Definition and Examples

Recall that a constraint function (also called a signature) is a map $f : \mathbb{Z}_2^n \to \mathbb{C}$ for some $n > 0$. A (Boolean) counting constraint satisfaction problem #CSP($\mathcal{F}$) is parameterized by a set $\mathcal{F}$ of signatures, and it is defined as follows.

Definition 2.1 (#CSP)**.** *Let $\mathcal{F}$ be any fixed set of signatures. An instance I of* #CSP($\mathcal{F}$) *is a finite set of variables $V = \{x_1, x_2, \ldots, x_n\}$, and a finite set C of clauses. Each clause is a constraint $f \in \mathcal{F}$ of some arity m depending on f together with a sequence of m (not necessarily distinct) variables $x_{i_1}, \ldots x_{i_m} \in V$. The output is the partition function*

$$Z(I) = \sum_{(x_1,\ldots,x_n)\in\mathbb{Z}_2^n} \prod_{(f,x_{i_1},\ldots x_{i_m})\in C} f(x_{i_1}, \ldots x_{i_m}).$$

When $\{f\}$ is a singleton set, we write #CSP($\{f\}$) *as* #CSP(f) *and* #CSP($\{f\}\cup\mathcal{F}$) *as* #CSP($f, \mathcal{F}$)*.*

Many natural combinatorial problems can be expressed by #CSP.

Example 2.2 (Counting Boolean Satisfiability)**.** *The counting Boolean satisfiability problem* (#SAT) *counts the number of satisfying assignments to a given Boolean formula. It can be expressed as*

#CSP($\mathcal{F}$) where $\mathcal{F} = \{\textsc{Or}_k \mid k \geqslant 1\} \cup \{\neq_2\}$, $\textsc{Or}_k$ is the Or *function of arity k and $\neq_2$ is the binary* Disequality *signature with truth table $(0, 1, 1, 0)$.*

Example 2.3 (Counting Independent Sets)**.** *The counting independent set problem (#IS) counts the number of independent sets of a given graph $G = (V, E)$. By viewing each vertex $v \in V$ as a Boolean variable (i.e., $v = 0$ or 1 depending on whether it is selected in an independent set), and each edge $e \in E$ as a binary constraint f_{IS} where $f_{\text{IS}}(0, 0) = f_{\text{IS}}(0, 1) = f_{\text{IS}}(1, 0) = 1$ and $f_{\text{IS}}(1, 1) = 0$, #IS can be expressed as #CSP(f_{IS}).*

The #IS problem is also a basic case of counting graph homomorphisms. Consider the graph $H = (V, E)$ where $V = \{v_0, v_1\}$ and $E = \{(v_0, v_0), (v_0, v_1)\}$. Then, the number of independent sets of a graph G is equal to the number of graph homomorphisms from G to H. In statistical physics, The #IS problem corresponds to the hard-core model, which is a special case of the more general 2-state spin (2-spin) systems. Spin systems are some of the most fundamental statistical physics systems. They model interactions between neighbors on graphs. A 2-spin system is specified by two edge interaction parameters β and γ, and a uniform external field λ, where $\beta, \gamma, \lambda \in \mathbb{C}$. It can be expressed by a #CSP problem with a binary signature and a unary signature.

Example 2.4 (2-Spin systems)**.** *Let f be a binary signature with $f(0, 0) = \beta$, $f(1, 1) = \gamma$ and $f(0, 1) = f(1, 0) = 1$, and g be a unary signature with $g(0) = 0$ and $g(1) = \lambda$. Then, the problem #CSP(f, g) computes the partition function of the 2-spin system specified by (β, γ, λ).*

2.1.2 Existing Dichotomies for #CSP

For a fixed signature set $\mathcal{F}$, the complexity of #CSP($\mathcal{F}$) is measured in terms of the input size of the instance I. When $\mathcal{F}$ is a finite set, this input size is equivalent to n (the number of variables). We may also allow $\mathcal{F}$ to be infinite. In this case, the input size includes the description of the constraints used in the input. A complexity dichotomy was proved for #CSP($\mathcal{F}$) if each $f \in \mathcal{F}$ takes values 0 or 1 [33]. Later, it was generalized to non-negative signature sets [35]. Finally, a full complexity dichotomy was proved for any complex-valued signature sets [31]. Such a dichotomy has an explicit criterion. We introduce the following two families of signatures that define tractable #CSP problems. They are *product-type* signatures and *affine* signatures. We use $=_2$ to denote the binary Equality signature with truth table $(1, 0, 0, 1)$.

Definition 2.5 (Product-type signatures)**.** *A signature on a set of variables X is of* product type *if it can be expressed as a product of unary functions, binary* Equality *functions $=_2$, and binary* Disequality *functions $\neq_2$, each on one or two variables of X. We use $\mathscr{P}$ to denote the set of product-type functions.*

Note that the product in Definition 2.5 are ordinary products of functions (not tensor products); in particular they may be applied on overlapping sets of variables. We give an alternative definition of product-type signatures using tensor products.

Let $\alpha \in \mathbb{Z}_2^n$ be an input of a signature f of arity n. We may use f^α to denote $f(\alpha)$. The support of a signature f is $\mathscr{S}(f) = \{\alpha \in \mathbb{Z}_2^{2n} \mid f^\alpha \neq 0\}$ i.e., the set of inputs on which f is not zero. We say f has support of size k if $|\mathscr{S}(f)| = k$. If $\mathscr{S}(f) = \emptyset$, i.e., f is identically 0, we say f is a zero signature and denote it by $f \equiv 0$. Otherwise, f is a nonzero signature. If $\mathscr{S}(f)$ consists of two antipodal points (i.e., $\mathscr{S}(f) = \{\alpha, \bar{\alpha}\}$), then we say f is an antipodal signature.

Lemma 2.6 ([20])**.** *A signature is of product-type iff it is a zero signature or it is a tensor product of unary signatures and antipodal signatures.*

Let $\mathfrak{i} = \sqrt{-1}$. We define affine signatures.

Definition 2.7 (Affine signatures)**.** *A signature $f(x_1, \ldots, x_n)$ of arity n is* affine *if it has the form*

$$\lambda \cdot \chi_{AX=0} \cdot \mathfrak{i}^{Q(X)},$$

where $\lambda \in \mathbb{C}$, $X = (x_1, x_2, \ldots, x_n, 1)$, A is a matrix over $\mathbb{Z}_2$, $Q(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_4[x_1, x_2, \ldots, x_n]$ is a multilinear polynomial with total degree $d(Q) \leqslant 2$ and the additional requirement that the coefficients of all cross terms are even, i.e., Q has the form

$$Q(x_1, x_2, \ldots, x_n) = a_0 + \sum_{k=1}^{n} a_k x_k + \sum_{1 \leq i < j \leq n} 2b_{ij} x_i x_j,$$

and χ is a 0-1 indicator function such that $\chi_{AX=0}$ is 1 iff $AX = 0$. We use $\mathscr{A}$ to denote the set of all affine signatures.

The following two lemmas follow directly from the definition.

Lemma 2.8. *Let g be a complex-valued binary signature with support of size 4. Then, $g \in \mathscr{A}$ iff g has the signature matrix $M(g) = \lambda \begin{bmatrix} \mathfrak{i}^a & \mathfrak{i}^b \\ \mathfrak{i}^c & \mathfrak{i}^d \end{bmatrix}$, for some nonzero $\lambda \in \mathbb{C}$, $a, b, c, d \in \mathbb{N}$ and $a+b+c+d \equiv 0 \pmod 2$.*

Lemma 2.9. *Let h be a complex-valued unary signature with support of size 2. Then, $h \in \mathscr{A}$ iff h has the form $M(h) = \lambda \begin{bmatrix} \mathfrak{i}^a & \mathfrak{i}^b \end{bmatrix}$, for some nonzero $\lambda \in \mathbb{C}$, and $a, b \in \mathbb{N}$.*

We say a signature f has affine support if $\mathscr{S}(f)$ is an affine linear subspace. Clearly, any affine signature has affine support. Moreover, by Lemma 2.6, we have

Lemma 2.10. *Any signature of product type has affine support.*

证明. Please see Definition 2.22 in Section 2.5 of [20] for a proof. □

When $\mathscr{S}(f)$ is an affine linear space, we can pick a set of free variables such that in $\mathscr{S}(f)$, every variable is an affine linear combination of free variables. Real-valued affine functions satisfy the following congruity or semi-congruity.

Lemma 2.11 ([14]). *Let $f(x_1, \ldots, x_n) = (-1)^{Q(x_1,\ldots,x_n)} \in \mathscr{A}$, and $y = x_n + L(x_1, \ldots, L_{n-1})$ be a linear combination of variables $x_1, \ldots, x_n$ that involves x_n. Define*

$$g(x_1, \ldots, x_{n-1}) = \frac{f_{y=0}(x_1, \ldots, x_{n-1}, y + L)}{f_{y=1}(x_1, \ldots, x_{n-1}, y + L)} = (-1)^{Q(x_1,\ldots,x_{n-1},L)+Q(x_1,\ldots,x_{n-1},L+1)}.$$

Then, g satisfies the following property.

- *(Congruity) $g \equiv 1$ or $g \equiv -1$, or*
- *(Semi-congruity) $g(x_1, \ldots, x_{n-1}) = (-1)^{L(x_1,\ldots,x_{n-1})}$ where $L(x_1, \ldots, x_{n-1}) \in \mathbb{Z}_2[x_1, \ldots, x_{n-1}]$ is an affine linear polynomial (degree $d(L) = 1$).*

In particular, if $d(Q) = 1$, then g has congruity.

Problems defined by $\mathscr{P}$ are tractable by a propagation algorithm, and problems defined by $\mathscr{A}$ are tractable essentially by algebraic cancellation. Together, they exhaust all tractable #CSP [31].

Theorem 2.12. *Let $\mathcal{F}$ be any set of complex-valued signatures. Then #CSP($\mathcal{F}$) is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$, in which cases the problem is tractable.*

We use $\#\mathrm{CSP}_k(\mathcal{F})$ to denote the special case of $\#\mathrm{CSP}(\mathcal{F})$ where every variable appears a multiple of k times. In particular, $\#\mathrm{CSP}_1(\mathcal{F}) = \#\mathrm{CSP}(\mathcal{F})$. We use $\leqslant_T$ (and $\equiv_T$) to denote polynomial-time Turing reductions (and equivalences, respectively). Clearly, $\#\mathrm{CSP}_k(\mathcal{F}) \leqslant_T \#\mathrm{CSP}(\mathcal{F})$. When $k = 2$, a complexity dichotomy was proved for complex-valued $\#\mathrm{CSP}_2(\mathcal{F})$ [32]. Beyond product-type and affine signatures, a new family of tractable signatures was identified. They are *local affine* signatures.

For an invertible 2-by-2 matrix $T \in \mathbf{GL}_2(\mathbb{C})$ and a signature f of arity n, written as a column vector (covariant tensor) $f \in \mathbb{C}^{2^n}$ by listing its truth table, we denote by $Tf = T^{\otimes n} f$. For a signature set $\mathcal{F}$, define $T\mathcal{F} = \{Tf \mid f \in \mathcal{F}\}$ the set of transformed signatures. Let $T_{\alpha^s} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \alpha^s \end{smallmatrix}\right]$ where $\alpha = e^{\frac{\mathrm{i}\pi}{4}} = \frac{1+\mathrm{i}}{\sqrt{2}}$ and s is an integer.

Definition 2.13 (Local affine signatures)**.** *A signature f (written as a column vector) is local-affine if for each $\sigma = s_1 s_2 \ldots s_n \in \mathbb{Z}_2^n$ in the support of f, $(T_{\alpha^{s_1}} \otimes T_{\alpha^{s_2}} \otimes \cdots \otimes T_{\alpha^{s_n}})f \in \mathscr{A}$. We use $\mathscr{L}$ to denote the set of local-affine signatures.*

Theorem 2.14 ([32])**.** *Let $\mathcal{F}$ be any set of complex-valued signatures. Then $\#\mathrm{CSP}_2(\mathcal{F})$ is $\#\mathrm{P}$-hard unless $\mathcal{F} \subseteq \mathscr{A}$, $\mathcal{F} \subseteq \mathscr{P}$, $\mathcal{F} \subseteq \mathscr{L}$ or $T_\alpha \mathcal{F} \subseteq \mathscr{A}$, in which cases the problem is tractable.*

2.2 Counting Eulerian Orientation Problems (#EO Problems)

2.2.1 Definition and Examples

Let G be an undirected Eulerian graph, i.e., every vertex has even degree. An *Eulerian orientation* of G is an orientation of its edges such that at each vertex the number of incoming edges is equal to the number of outgoing edges. Mihail and Winkler showed that counting the number of Eulerian orientations of an undirected Eulerian graph is #P-complete [58]. We consider counting weighted Eulerian orientation problems (#EO problems), formulated as a partition function defined by constraint functions placed at each vertex that represent weightings of various local Eulerian configurations.

We use $\mathrm{wt}(\alpha)$ to denote the Hamming weight of $\alpha \in \mathbb{Z}_2^{2n}$. Let $\mathscr{H}_{2n} = \{\alpha \in \mathbb{Z}_2^{2n} \mid \mathrm{wt}(\alpha) = n\}$. A signature f of arity $2n$ is an *Eulerian orientation* (EO) signature if $\mathscr{S}(f) \subseteq \mathscr{H}_{2n}$. A #EO problem is parameterized by a set $\mathcal{F}$ of EO signatures. An instance of $\#\mathrm{EO}(\mathcal{F})$ is an EO-signature grid

$\Omega = (G, \pi)$, where $G = (V, E)$ is an Eulerian graph without isolated vertex (i.e., every vertex has positive even degree), π labels each $v \in V$ with an EO signature $f_v \in \mathcal{F}$ of arity $\deg(v)$, and labels the incident edges $E(v)$ at v with input variables of f_v. For any Eulerian graph G, let $\text{EO}(G)$ be the set of all Eulerian orientations of G. We view each edge as having two ends, and an orientation of the edge is denoted by assigning 0 to the head and 1 to the tail. An Eulerian orientation corresponds to an assignment to the ends of each edge where the numbers of 0's and 1's at each v are equal. Then a vertex v contributes a weight by the local constraint function f_v evaluated according to the local assignment. Since the support of f_v is on half weighted inputs, only Eulerian orientations contribute nonzero values. Each $\sigma \in \text{EO}(G)$ gives an evaluation $\prod_{v \in V} f_v(\sigma|_{E(v)})$, where $\sigma|_{E(v)}$ assigns 0 to an incoming edge and 1 to an outgoing edge.

Definition 2.15 (#EO problems)**.** *Let $\mathcal{F}$ be any fixed set of EO signatures. The input of* $\#\text{EO}(\mathcal{F})$ *is an* EO-*signature grid* $\Omega = (G, \pi)$ *over* $\mathcal{F}$*; the output is the partition function of* Ω*,*

$$\#\text{EO}_\Omega = \sum_{\sigma \in \text{EO}(G)} \prod_{v \in V} f_v(\sigma|_{E_{(v)}}).$$

When $\{f\}$ *is a singleton set, we write* $\#\text{EO}(\{f\})$ *as* $\#\text{EO}(f)$ *and* $\#\text{EO}(\{f\} \cup \mathcal{F})$ *as* $\#\text{EO}(f, \mathcal{F})$*.*

Example 2.16 (Unweighted #EO problem)**.** *Let* $\mathcal{F}_{\text{EO}} = \{f_2, f_4, \ldots f_{2n}, \ldots\}$*, where* $f_{2n}^\alpha = 1$ *when* $\text{wt}(\alpha) = n$ *and* $f_{2n}^\alpha = 0$ *otherwise. Then* $\#\text{EO}(\mathcal{F}_{\text{EO}})$ *counts the number of Eulerian orientations.*

There are a host of problems in statistical physics that can be formulated as #EO problems. One of the most studied models is the *six-vertex model.* It was introduced by Pauling in 1935 to account for the residual entropy of water ice [61]. Mathematically, it is an #EO problem defined on 4-regular graphs. For more background in physics, please see Chapter 9.

Example 2.17 (Six-vertex models)**.** *Let* f_{six} *be an* EO *signature of arity* 4*, where* $f_{\text{six}}^{0011} = a$*,* $f_{\text{six}}^{1100} = x$*,* $f_{\text{six}}^{0101} = b$*,* $f_{\text{six}}^{1010} = y$*,* $f_{\text{six}}^{0110} = c$*,* $f_{\text{six}}^{1001} = z$*. Then* $\#\text{EO}(f_{\text{six}})$ *is the six-vertex model.*

2.2.2 #EO Problems Encompass #CSP

The #EO problems have an intrinsic significance in the classification program for counting problems. At first glance, the #EO framework may appear to be specialized as it requires all constraint functions to be supported on half weighted inputs. However, surprisingly, it encompasses all Boolean #CSP.

Definition 2.18 (Pairwise opposite). *Let $\mathscr{S} \subseteq \mathbb{Z}_2^{2n}$ be an affine linear subspace. We say $\mathscr{S}$ is pairwise opposite if we can partition the $2n$ variables into n pairs such that on $\mathscr{S}$, two variables of each pair always take opposite values. If $\mathscr{S}$ is pairwise opposite, we fix a pairing. Then each pair under this paring is called an opposite pair.*

Let g be an arbitrary signature of arity $n > 0$ (with no assumption to be EO). We associate g with an EO signature $\widetilde{g}$ of arity $2n$ in the following way. We define

$$\widetilde{g}(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) = \begin{cases} g(x_1, \ldots x_n) & \text{if } x_i \neq x_{i+n} \quad (i \in [n]), \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, $\widetilde{g}$ is an EO signature. Moreover, its support is pairwise opposite, i.e., x_i and x_{n+i} form an opposite pair. We say x_i is in the first half of the inputs of $\widetilde{g}$, while x_{n+i} is in the second half. We define $\widetilde{\mathcal{G}} = \{\widetilde{g} \mid g \in \mathcal{G}\}$ for an arbitrary signature set $\mathcal{G}$. We show that #CSP is expressible in the #EO framework by the following theorem.

Theorem 2.19. *For every signature set $\mathcal{G}$ and the* EO *signature set $\widetilde{\mathcal{G}}$ defined above, we have*

$$\#\mathrm{CSP}(\mathcal{G}) \equiv_T \#\mathrm{EO}(\widetilde{\mathcal{G}}).$$

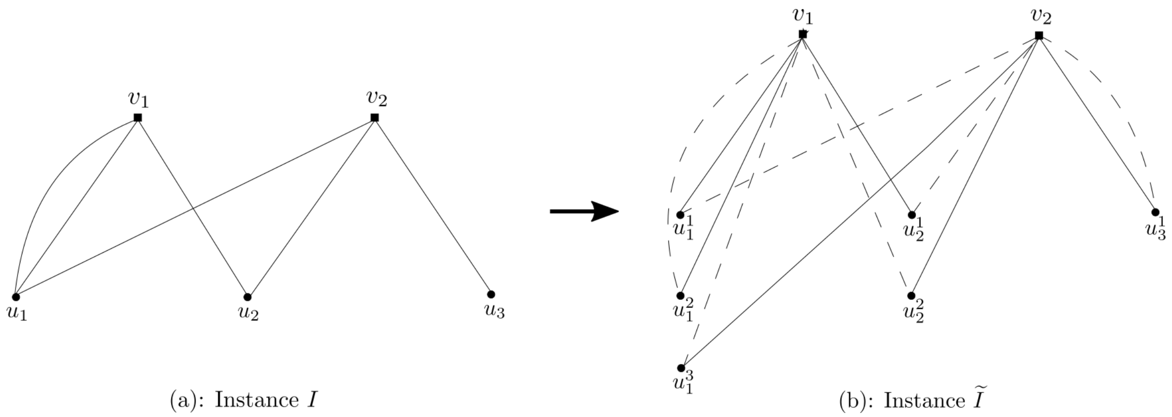
Remark 2.20. *Before we give the proof, we remark that this theorem is not merely stating that for an arbitrary* #CSP($\mathcal{G}$) *problem, one can reduce every instance of* #CSP($\mathcal{G}$) *to an instance of a suitable* #EO($\widetilde{\mathcal{G}}$) *problem. Theorem 2.19 is stronger and categorical: For every signature set $\mathcal{G}$ in the* #CSP *framework, there is a (uniformly constructible) EO signature set $\widetilde{\mathcal{G}}$ such that* #CSP($\mathcal{G}$) *is the same as the #EO problem* #EO($\widetilde{\mathcal{G}}$). *In particular, a complexity dichotomy for #EO problems would generalize the complexity dichotomy for* #CSP *problems on Boolean variables (which is already known).*

证明. We first show that every instance of #CSP($\mathcal{G}$) is expressible canonically as an instance of #EO($\widetilde{\mathcal{G}}$), thus, #CSP($\mathcal{G}$) $\leqslant_T$ #EO($\widetilde{\mathcal{G}}$). Let $G = (U, V, E)$ be a bipartite graph representing an instance I of #CSP($\mathcal{G}$), where each $u \in U$ is a variable and each $v \in V$ is labeled by a constraint function $g \in \mathcal{G}$. We will modify the instance I to an instance $\widetilde{I}$ of #EO($\widetilde{\mathcal{G}}$) that evaluates to the same value, as follows.

1. For every $u \in U$, we create $k = \deg_G(u)$ vertices denoted by u^i ($1 \leqslant i \leqslant k$). (For example, in Figure 2, vertices u_1, u_2 and u_3 are decomposed into 3, 2 and 1 vertices respectively.) Then we connect the k edges originally incident to u to these k new vertices, so that each new vertex is incident to exactly one edge. (To be specific we assume the edges at u in I are ordered from 1 to k, and we connect the i-th edge to u^i. These are edges drawn by solid lines in Figure 2(b).) We denote this graph by G'. Each u^i in G' has degree 1 and the degree of each $v \in V$ does not change.

2. For each edge $e^i = (u^i, v)$ in the graph G', we add an edge $\overline{e}^i = (u^{i+1}, v)$ to G' and we call them a pair. (Here if $\deg_G(u) = k$ then we use u^{k+1} to denote u^1; we will add a multiple edge if $e^{i+1} = (u^{i+1}, v)$ is already in G'. These edges $\overline{e}^i$ are drawn by dashed lines in Figure 2(b).) This defines a graph $\widetilde{G}$. Each u^i in $\widetilde{G}$ has degree 2 and we label it by $\neq_2$. If $\deg_G(v) = n$ and is labeled by the constraint function $g \in \mathcal{G}$, then v in $\widetilde{G}$ has degree $2n$ and we label it by the corresponding $\widetilde{g} \in \widetilde{\mathcal{G}}$. We place the signature $\widetilde{g}$ in a way such that every pair of edges $e^i = (u^i, v)$ and $\overline{e}^i = (u^{i+1}, v)$ incident to the same v appears as an opposite pair in the inputs of the function $\widetilde{g}$, and e^i appears in the first half of the inputs of $\widetilde{g}$ while $\overline{e}^i$ appears in the second half. Recall that $\widetilde{g}$ is defined to be pairwise opposite such that its j-th variable in the first half is paired with its $(n+j)$-th variable in the second half. This defines an instance $\widetilde{I}$ of #EO($\widetilde{\mathcal{G}}$).

We show that $\#\text{EO}_{\widetilde{I}}$ has the same value as the instance I for #CSP($\mathcal{G}$). Consider each variable $u \in U$. Suppose it has $\deg_G(u) = k$ in the instance I. It corresponds to k vertices $u^1, \ldots, u^k$ and $2k$ edges $e^1, \overline{e}^1, \ldots, e^i, \overline{e}^i, \ldots, e^k$ and $\overline{e}^k$. These $2k$ edges form a circuit C_u. For example, in Figure 2, $u_1^1, v_1, u_1^2, v_1, u_1^3, v_2$ back to u_1^1 is such a circuit where the edges are successively $e_1^1, \overline{e}_1^1, e_1^2, \overline{e}_1^2, e_1^3, \overline{e}_1^3$ (edges drawn by solid lines and dashed lines alternate). Note that, for every pair of edges e^i and $\overline{e}^i$, we placed the signature $\widetilde{g}$ such that e^i and $\overline{e}^i$ appear as an opposite pair. Thus, we may assume e^i and $\overline{e}^i$ take opposite values in the evaluation of $\#\text{EO}_{\widetilde{I}}$. Also, since each u^i is labeled by $\neq_2$, we may also assume $\overline{e}^i$ and e^{i+1} take opposite values in the evaluation. (This is really a consequence



(a): Instance I (b): Instance $\widetilde{I}$

图 2: The reduction from #CSP to #EO

of the definition of #EO problems.) Thus, for any (possible) nonzero term in the sum $\#\mathrm{EO}_{\widetilde{I}}$, as a consequence of the support of signatures in $\widetilde{G}$ and $\neq_2$, we know on each circuit C_u all edges must take values $(0,1,0,1,\cdots,0,1)$ or $(1,0,1,0,\cdots,1,0)$, i.e., the values of $0,1$ alternate. Therefore, on the circuit C_u, we have $e^1, e^2, \ldots, e^k$ all take the same 0-1 value, which corresponds to the 0-1 assignment on the variable u in the #CSP instance I. Recall in the definition of $\widetilde{g}$, its value can be determined by the first half of its inputs. By the placement of $\widetilde{g}$, the first half of its inputs are edges in the graph G' (drawn by solid lines). Therefore, the contribution of $\widetilde{g}$ to $\#\mathrm{EO}_{\widetilde{I}}$ is exactly the same as the contribution of g in the #CSP instance I. Thus, these two instances have the same value.

For the other direction, we first note that $\#\mathrm{CSP}(\mathcal{G} \cup \{\neq_2\}) \leqslant_T \#\mathrm{CSP}(\mathcal{G})$. If $\#\mathrm{CSP}(\mathcal{G})$ is #P-hard, the reduction holds trivially since every #CSP problem can be reduced in P-time to a #P-hard problem. Otherwise, by Theorem 2.12, $\#\mathrm{CSP}(\mathcal{G})$ is tractable and $\mathcal{G} \subseteq \mathscr{A}$ or $\mathscr{P}$. Since $(\neq_2) \in \mathscr{A} \cap \mathscr{P}$, we have $\mathcal{G} \cup \{\neq_2\} \subseteq \mathscr{A}$ or $\mathscr{P}$. Thus, $\#\mathrm{CSP}(\mathcal{G} \cup \{\neq_2\})$ is tractable. Then, again the reduction holds trivially. Then, we will show that $\#\mathrm{EO}(\widetilde{\mathcal{G}}) \leqslant_T \#\mathrm{CSP}(\mathcal{G} \cup \{\neq_2\})$.

Consider an arbitrary instance I' of $\#\mathrm{EO}(\widetilde{\mathcal{G}})$. Because every signature in $\widetilde{\mathcal{G}}$ has the pairing structure among its variables, we can decompose the graph of I' into edge disjoint circuits, by always following the paired variables at each constraint vertex. For each edge disjoint circuit, we choose an arbitrary default orientation. The circuit visits constraint vertices in some order according to the default orientation. The visit follows successive pairs of edges. Recall that as a consequence of the support of constraint functions, on each circuit, all these pairs of edges in the successive order must take the same ordered pair of values $(x, \bar{x})$, where $x \in \{0, 1\}$. Thus, we can define a Boolean variable x from the edges on each such circuit. From this a corresponding instance I for #CSP($\mathcal{G} \cup \{\neq_2\}$) can be obtained that has the same value as I' in #EO($\widetilde{\mathcal{G}}$).

More specifically, suppose $g(x_1, \ldots, x_n) \in \mathcal{G}$ and let $g'(x_1, \ldots, x_n) = g(x_1^{\epsilon_1}, \ldots, x_n^{\epsilon_n})$, where each $x_i^{\epsilon_i}$ is either x_i or $\overline{x_i}$. To discuss the complexity of #CSP($\mathcal{G} \cup \{\neq_2\}$), using $(\neq_2)$ we may assume every function obtained by flipping any number of variables in a function $g \in \mathcal{G}$ is also in $\mathcal{G}$.

Now, consider the default orientation of each circuit. At constraint vertices, the default orientation visits successive pairs of edges corresponding to paired inputs of constraint functions, say, $\{x_j, x_{n+j}\}$. If the default orientation always visits in the order x_j followed by x_{n+j}, then this is exactly how the canonical construction given above and we can recover an instance I for #CSP($\mathcal{G}$) with the same value. If at some constraint $\widetilde{g}$ of arity $2n$ the default orientation happens to visit in the order x_{n+j} followed by x_j, we can use one copy of $\neq_2$ to modify the original function g to get another constraint g', so that the corresponding $\widetilde{g'}$ is just $\widetilde{g}$ with a flip between its variables x_{n+j} and x_j. Then according to the default orientation the visit is in the order x_j followed by x_{n+j}. □

2.3 Holant Problems

2.3.1 Definition and Examples

Both #CSP and #EO problems can be viewed as special cases of Holant problems. Let $\mathcal{F}$ be a set of arbitrary (not necessarily EO) signatures. A (general) signature grid $\Omega = (G, \pi)$ over $\mathcal{F}$ is a tuple, where $G = (V, E)$ is a graph without isolated vertices, π labels each $v \in V$ with a signature $f_v \in \mathcal{F}$ of arity $\deg(v)$, and labels the incident edges $E(v)$ at v with input variables of f_v. We consider all 0-1 edge assignments σ, and each gives an evaluation $\prod_{v \in V} f_v(\sigma|_{E(v)})$, where $\sigma|_{E(v)}$ denotes the restriction of σ to $E(v)$.

Definition 2.21 (Holant problems). *The input to the problem* Holant($\mathcal{F}$) *is a signature grid* $\Omega = (G, \pi)$ *over* $\mathcal{F}$. *The output is the partition function*

$$\text{Holant}(\Omega) = \sum_{\sigma: E(G) \to \{0,1\}} \prod_{v \in V(G)} f_v(\sigma|_{E_{(v)}}).$$

Bipartite Holant problems $\operatorname{Holant}(\mathcal{F} \mid \mathcal{G})$ *are Holant problems over bipartite graphs* $H = (U, V, E)$*, where each vertex in* U *or* V *is labeled by a signature in* $\mathcal{F}$ *or* $\mathcal{G}$ *respectively. When* $\{f\}$ *is a singleton set, we write* $\operatorname{Holant}(\{f\})$ *as* $\operatorname{Holant}(f)$ *and* $\operatorname{Holant}(\{f\} \cup \mathcal{F})$ *as* $\operatorname{Holant}(f, \mathcal{F})$.

We use $=_n$ to denote the Equality signature of arity n, which takes value 1 on the all-0 or all-1 inputs, and 0 elsewhere. (We denote the n-bits all-0 and all-1 strings by $\vec{0}^n$ and $\vec{1}^n$ respectively. We may omit the superscript n when it is clear from the context.) Let $\mathcal{EQ}_k = \{=_k, =_{2k}, \ldots, =_{nk}, \ldots\}$ denotes the set of Equality signatures whose arities are multiples of k. In particular, $\mathcal{EQ} = \mathcal{EQ}_1 = \{=_1, =_2, \ldots, =_n, \ldots\}$ denotes the set of all Equality signatures.

Lemma 2.22 ([14])**.** $\#\mathrm{CSP}_k(\mathcal{F}) \equiv_T \operatorname{Holant}(\mathcal{EQ}_k \mid \mathcal{F})$*. When* $k = 1$ *or* 2*,* $\operatorname{Holant}(\mathcal{EQ}_k \mid \mathcal{F}) \equiv_T \operatorname{Holant}(\mathcal{EQ}_k \cup \mathcal{F})$*.*

The following two reductions are also known [14]. One states that we can realize all $=_k \in \mathcal{EQ}$ once we have $=_3$. The other states that we can realize all $=_{2k} \in \mathcal{EQ}_2$ once we have $=_4$.

Lemma 2.23. $\#\mathrm{CSP}(\mathcal{F}) \leqslant_T \operatorname{Holant}(=_3, \mathcal{F})$*.*

Lemma 2.24. $\#\mathrm{CSP}_2(\mathcal{F}) \leqslant_T \operatorname{Holant}(=_4, \mathcal{F})$*.*

Recall that $\neq_2$ denotes the binary Disequality signature $(0, 1, 1, 0)$. We generalize this notion to signatures of higher arities. A signature f of arity $2n$ is called a Disequality signature of arity $2n$, denoted by $\neq_{2n}$, if $f = 1$ when $(x_1 \neq x_2) \wedge \ldots \wedge (x_{2n-1} \neq x_{2n})$, and 0 otherwise. By permuting its variables the Disequality signature of arity $2n$ also defines $(2n-1)(2n-3)\cdots 1$ functions which we also call Disequality signatures. These signatures are equivalent for the complexity of Holant problems; once we have one we have them all. Let $\mathcal{DEQ} = \{\neq_2, \neq_4, \ldots, \neq_{2n}, \ldots\}$ denote the set of all Disequality signatures.

Now, we show EO problems can be expressed by Holant problems.

Lemma 2.25. *Let* $\mathcal{F}$ *be a set of EO signatures. Then,* $\#\mathrm{EO}(\mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2 \mid \mathcal{F})$*.*

证明. If $\Omega = (G, \pi)$ is an instance of $\#\mathrm{EO}(\mathcal{F})$, we add a middle vertex on each edge of G and label it by $\neq_2$. This defines an instance Ω' of $\operatorname{Holant}(\neq_2 \mid \mathcal{F})$ with a bipartite graph H (which is the edge-vertex incidence graph of G), where every edge of G is broken into two. There is a 1-1 correspondence of the terms in the partition functions $\#\mathrm{EO}_\Omega$ and $\operatorname{Holant}_{\Omega'}$. The process is obviously reversable. □

Since #CSP and #EO problems are special cases of Holant problems, problems that can be expressed as #CSP or #EO problems can also be expressed as Holant problems. Other problems that can be expressed as Holant problems include counting matchings and perfecting matchings and eight-vertex models.

Example 2.26 (Counting perfect matchings)**.** *Let* $\mathcal{F} = \{f_1, f_2, \ldots, f_n, \ldots\}$ *where* $f_n(\alpha) = 1$ *if* $\mathrm{wt}(\alpha) = 1$ *and* $f_n(\alpha) = 0$ *otherwise. Then,* $\operatorname{Holant}(\mathcal{F})$ *counts the number of perfect matching.*

Example 2.27 (Eight-vertex models)**.** *Let* f_{eight} *be a signature of arity* 4*, where* $f_{\text{eight}}^{0011} = a, f_{\text{eight}}^{1100} = a$*,* $f_{\text{six}}^{0101} = f_{\text{six}}^{1010} = b$*,* $f_{\text{six}}^{0110} = f_{\text{six}}^{1001} = c$*, (where* $a, b, c \in \mathbb{R}^{+}$*). Then* $\#\mathrm{EO}(f_{\text{six}})$ *is the classical six-vertex model satisfying* ARS *with real parameters* (a, b, c)*.*

Note that $\#\mathrm{CSP}(\mathcal{F}) \equiv_T \operatorname{Holant}(\mathcal{EQ} \cup \mathcal{F})$. Then, clearly Holant(). Thus, both product-type signatures and affine signatures define tractable Holant problems. However, beyond them, there are extra family of signatures.

Definition 2.28 (Unary and binary signatures)**.** *Let* $\mathscr{T}$ *denote the set of tensor products of unary and binary signatures.*

Theorem 2.29 ([32, 4])**.** *Let* $\mathcal{F}$ *be a set of complex valued signatures. Then* $\operatorname{Holant}(\mathcal{F})$ *is tractable if* $\mathcal{F} \subseteq \mathscr{T}$*,* $\mathcal{F} \subseteq \mathscr{P}$*,* $\mathcal{F} \subseteq \mathscr{A}$*, or* $\mathcal{F} \subseteq \mathscr{L}$*.*

Notice that $(\neq_2) \in \mathscr{T}$, $(\neq_2) \in \mathscr{P}$ and $(\neq_2) \in \mathscr{A}$.

Theorem 2.30. *Let* $\mathcal{F}$ *be a set of complex-valued signatures. Then* $\operatorname{Holant}(\neq_2 \mid \mathcal{F})$ *is tractable if* $\mathcal{F} \subseteq \mathscr{T}$*,* $\mathcal{F} \subseteq \mathscr{P}$ *or* $\mathcal{F} \subseteq \mathscr{A}$*.*

2.3.2 Holographic Transformation

To introduce the idea of holographic transformation, it is convenient to consider bipartite graphs. For a general graph, we can always transform it into a bipartite graph while preserving the Holant value, as follows. For each edge in the graph, we replace it by a path of length two. (This operation is called the *2-stretch* of the graph and yields the edge-vertex incidence graph.) Each new vertex is assigned the binary Equality signature $=_2$. Thus, we have $\operatorname{Holant}(=_2 \mid \mathcal{F}) \equiv_T \operatorname{Holant}(\mathcal{F})$.

For an invertible 2-by-2 matrix $T \in \mathbf{GL}_2(\mathbb{C})$ and a signature f of arity n, written as a column vector (covariant tensor) $f \in \mathbb{C}^{2^n}$, we denote by $Tf = T^{\otimes n} f$ the transformed signature. For a signature set $\mathcal{F}$, define $T\mathcal{F} = \{Tf \mid f \in \mathcal{F}\}$ the set of transformed signatures. For signatures written as row vectors (contravariant tensors) we define fT^{-1} and $\mathcal{F}T^{-1}$ similarly. Whenever we write Tf or $T\mathcal{F}$, we view the signatures as column vectors; similarly for fT^{-1} or $\mathcal{F}T^{-1}$ as row vectors.

Let $T \in \mathbf{GL}_2(\mathbb{C})$. The holographic transformation defined by T is the following operation: given a signature grid $\Omega = (H, \pi)$ of $\operatorname{Holant}(\mathcal{F} \mid \mathcal{G})$, for the same bipartite graph H, we get a new signature grid $\Omega' = (H, \pi')$ of $\operatorname{Holant}(\mathcal{F}T^{-1} \mid T\mathcal{G})$ by replacing each signature in $\mathcal{F}$ or $\mathcal{G}$ with the corresponding signature in $\mathcal{F}T^{-1}$ or $T\mathcal{G}$.

Theorem 2.31 ([72]). *For every $T \in \mathbf{GL}_2(\mathbb{C})$,* $\operatorname{Holant}(\mathcal{F} \mid \mathcal{G}) \equiv_T \operatorname{Holant}(\mathcal{F}T^{-1} \mid T\mathcal{G})$.

Therefore, a holographic transformation does not change the complexity of the Holant problem in the bipartite setting. In particular, if there exists a $T \in \mathrm{GL}_2(\mathbb{C})$ such that $\operatorname{Holant}((=_2)T^{-1} \mid T\mathcal{F})$ is tractable, then $\operatorname{Holant}(=_2 \mid \mathcal{F})$ is also tractable.

Definition 2.32. *We say a signature set $\mathcal{F}$ is $\mathscr{C}$-transformable if there exists a $T \in \mathrm{GL}_2(\mathbb{C})$ such that $(=_2)T^{-1} \in \mathscr{C}$ and $T\mathcal{F} \subseteq \mathscr{C}$.*

Theorem 2.33. *Let $\mathcal{F}$ be a set of complex valued signatures. Then* $\operatorname{Holant}(\mathcal{F})$ *is tractable if*

$$\mathcal{F} \subseteq \mathscr{T}, \quad \mathcal{F} \textit{ is } \mathscr{P}\textit{-transformable}, \quad \mathcal{F} \textit{ is } \mathscr{A}\textit{-transformable}, \quad \textit{or } \mathcal{F} \textit{ is } \mathscr{L}\textit{-transformable}. \tag{T}$$

Notice that $(=_2) \in \mathscr{P} \cap \mathscr{A} \cap \mathscr{L}$. Clearly, If $\mathcal{F} \in \mathscr{P}, \mathscr{A}$ or $\mathscr{L}$, then $\mathcal{F}$ is $\mathscr{P}, \mathscr{A}$ or $\mathscr{L}$-transformable respectively. Also, notice that $(=_2)T_\alpha^{-1} = (1, 0, 0, \mathfrak{i}) \in \mathscr{A}$. If $T_\alpha \mathcal{F} \in \mathscr{A}$, then $\mathcal{F}$ is $\mathscr{A}$-transformable. Thus, if $\mathcal{F}$ does not satisfy condition, then If $\mathcal{F} \notin \mathscr{P}, \mathcal{F} \notin \mathscr{A}$, $\mathcal{F} \notin \mathscr{L}$, and $T_\alpha \mathcal{F} \notin \mathscr{A}$. By dichotomies of #CSP and #CSP$_2$, we have the following #P-hardness result.

Theorem 2.34. *Let $\mathcal{F}$ be a set of complex-valued signatures. If $\mathcal{F}$ does not satisfy condition* (T), *then* $\#\mathrm{CSP}(\mathcal{F})$ *and* $\#\mathrm{CSP}_2(\mathcal{F})$ *are* #P-hard.

Now, we introduce two particular holographic transformations that will be commonly used in this dissertation. One is the transformation defined by real orthogonal matrix. Let $\mathbf{O}_2(\mathbb{R}) \subseteq \mathbb{R}^{2\times 2}$ be the set of all 2-by-2 real orthogonal matrices. We denote $\mathbf{O}_2(\mathbb{R})$ by $\mathbf{O}_2$. For all $Q \in \mathbf{O}_2$, since $(=_2)Q^{-1} = (=_2)$, $\operatorname{Holant}(=_2 \mid \mathcal{F}) \equiv_T \operatorname{Holant}(=_2 \mid Q\mathcal{F})$. The other is the transformation defined by $Z^{-1} = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & -\mathfrak{i} \\ 1 & \mathfrak{i} \end{smallmatrix}\right]$. Note that $(=_2)Z = (\neq_2)$ where $Z = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ \mathfrak{i} & -\mathfrak{i} \end{smallmatrix}\right]$. Thus, $\operatorname{Holant}(=_2 | \mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2 | Z^{-1}\mathcal{F})$. We denote $Z^{-1}\mathcal{F}$ by $\widehat{\mathcal{F}}$ and $Z^{-1}f$ by $\widehat{f}$.

Definition 2.35 (Arrow reversal symmetry)**.** *A (complex-valued) signature f satisfies* arrow reversal symmetry *(*ARS*) if $\overline{f(\alpha)} = f(\overline{\alpha})$ for all α where $\overline{f(\alpha)}$ denotes the complex conjugation of $f(\alpha)$ and $\overline{\alpha}$ denotes the bit-wise complement of α. For real-valued signatures, this is $f(\overline{\alpha}) = f(\alpha)$.*

Arrow reversal symmetry is usually assumed in statistical physics*. In complexity theory, there is a more intrinsic reason for considering the arrow reversal symmetry. Under the holographic transformation by $Z^{-1} = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & -\mathfrak{i} \\ 1 & \mathfrak{i} \end{smallmatrix}\right]$, real-valued signatures translate precisely to complex-valued signatures with the ARS restriction.

Lemma 2.36. *A (complex-valued) signature f is a real-valued signature iff $\widehat{f}$ satisfies* ARS*.*

证明. We first prove that if $\widehat{f}$ satisfies ARS then f is real.

We have $2^{n/2} f = \left[\begin{smallmatrix} 1 & 1 \\ \mathfrak{i} & -\mathfrak{i} \end{smallmatrix}\right]^{\otimes n} \widehat{f}$, and thus for all $(a_1, \ldots, a_n) \in \{0,1\}^n$,

$$2^{n/2} f^{a_1 \ldots a_n} = \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} \widehat{f}^{b_1,\ldots,b_n} \prod_{1\leqslant j\leqslant n} \left\{(-1)^{a_j b_j} \mathfrak{i}^{a_j}\right\}.$$

Then,

$$\begin{aligned} 2^{n/2}\overline{f^{a_1\ldots a_n}} &= \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} \overline{\widehat{f}^{b_1\ldots b_n}} \prod_{1\leqslant j\leqslant n} \left\{(-1)^{a_j b_j}(-\mathfrak{i})^{a_j}\right\} \\ &= \sum_{(c_1,\ldots,c_n)\in\{0,1\}^n} \widehat{f}^{c_1\ldots c_n} \prod_{1\leqslant j\leqslant n} \left\{(-1)^{a_j(1-c_j)}(-\mathfrak{i})^{a_j}\right\} \\ &= 2^{n/2} f^{a_1\ldots a_n}. \end{aligned}$$

Hence, f is real.

Now in the opposite direction, suppose f is real. We have $2^{n/2}\widehat{f} = \left[\begin{smallmatrix} 1 & -\mathfrak{i} \\ 1 & \mathfrak{i} \end{smallmatrix}\right]^{\otimes n} f$, and thus for all $(a_1, \ldots, a_n) \in \{0,1\}^n$,

$$2^{n/2}\widehat{f}^{a_1\ldots a_n} = \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} f^{b_1,\ldots,b_n} \prod_{1\leqslant j\leqslant n} \left\{(-1)^{a_j b_j}(-\mathfrak{i})^{b_j}\right\}.$$

*On a square lattice, when there is no external electric field, physical considerations imply that the model is unchanged by reversing all arrows [8]. This ‘zero field’ model includes the *ice* [61], *KDP* [65] and *F* [62] models as special cases.

So

$$2^{n/2}\widehat{f}^{\overline{a_1}\ldots\overline{a_n}} = \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} f^{b_1,\ldots,b_n} \prod_{1\leqslant j\leqslant n}\left\{(-1)^{(1-a_j)b_j}(-\mathfrak{i})^{b_j}\right\}.$$

Then,

$$\begin{aligned} 2^{n/2}\overline{f^{a_1\ldots a_n}} &= \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} \overline{f^{b_1\ldots b_n}} \prod_{1\leqslant j\leqslant n}\left\{(-1)^{a_jb_j}\mathfrak{i}^{b_j}\right\} \\ &= \sum_{(b_1,\ldots,b_n)\in\{0,1\}^n} \widehat{f}^{b_1\ldots b_n} \prod_{1\leqslant j\leqslant n}\left\{(-1)^{a_jb_j}\mathfrak{i}^{b_j}\right\} \\ &= 2^{n/2}\widehat{f}^{\overline{a_1}\ldots\overline{a_n}}. \end{aligned}$$

Hence, $\widehat{f}$ satisfies ARS. □

For every $Q \in \mathbf{O}_2$, let $\widehat{Q} = Z^{-1}QZ$. Remember that we define $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. Then, we have

$$\widehat{Q}\widehat{\mathcal{F}} = (Z^{-1}QZ)(Z^{-1}\mathcal{F}) = Z^{-1}(Q\mathcal{F}) = \widehat{Q\mathcal{F}}. \tag{2.1}$$

Thus,

$$\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(=_2 \mid \mathcal{F}) \equiv_T \operatorname{Holant}(=_2 \mid Q\mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2 \mid \widehat{Q}\widehat{\mathcal{F}}).$$

Let $\widehat{\mathbf{O}_2} = \{\widehat{Q} = Z^{-1}QZ \mid Q \in \mathbf{O}_2\}$. One can check that $\widehat{\mathbf{O}_2} = \{\left[\begin{smallmatrix}\alpha & 0\\ 0 & \overline{\alpha}\end{smallmatrix}\right], \left[\begin{smallmatrix}0 & \alpha\\ \overline{\alpha} & 0\end{smallmatrix}\right] \mid \alpha \in \mathbb{C}, |\alpha| = 1\}$.

The following result is easy to check.

Lemma 2.37. *Let $\mathcal{F}$ be a set of real-valued signatures. If $\mathcal{F}$ does not satisfy condition* (T), then for every $Q \in \mathbf{O}_2$, $Q\mathcal{F}$ also does not satisfy condition (T). Moreover, $\widehat{\mathcal{F}} \not\subseteq \mathscr{P}$ and $\widehat{\mathcal{F}} \not\subseteq \mathscr{A}$.

2.4 Sample Problems

We give some sample problems to illustrate the general theorems to be achieved.

Problem 1 : Counting independent sets #CSP(f_{IS}) (Example 2.3).

Recall that $f_{\text{IS}} = (1, 1, 1, 0)$. By the dichotomy of #CSP (Theorem 2.12), this problem is #P-complete since $f_{\text{IS}} \notin \mathscr{P}$ and $f_{\text{IS}} \notin \mathscr{A}$. The problem #CSP($f_{\text{IS}}$) is equivalent to Holant($\mathcal{EQ}, f_{\text{IS}}$). Our Holant dichotomy (Theorem 1.1) confirms the #P-completeness.

Problem 2 : The 2-spin system parameterized by $\beta = 1$, $\gamma = -1$, and $\lambda = 1$ (Example 2.4).

This problem can be expressed as #CSP(f, g) where $f = (1, 1, 1, -1)$ and $g = (1, 1)$. By the dichotomy of #CSP (Theorem 2.12), it is tractable since $f, g \in \mathscr{A}$. The problem #CSP(f, g) is equivalent to Holant$(\mathcal{EQ}, f, g)$. Our Holant dichotomy (Theorem 1.1) confirms the tractability.

Problem 3 : Counting unweighted Eulerian orientations #EO$(\mathcal{F}_{\text{EO}})$ (Example 2.16).

Recall that $\mathcal{F}_{\text{EO}} = \{f_2, f_4, \dots f_{2n}, \dots\}$ where $f_{2n}^{\alpha} = 1$ when $\text{wt}(\alpha) = n$ and $f_{2n}^{\alpha} = 0$ otherwise. Mihail and Winkler proved that this problem is #P-complete [58]. The problem #EO$(\mathcal{F}_{\text{EO}})$ is equivalent to Holant$(\neq_2 \mid \mathcal{F}_{\text{EO}})$. Notice that $\mathcal{F}_{\text{EO}}$ satisfies ARS, $\mathcal{F}_{\text{EO}} \nsubseteq \mathscr{P}$ and $\mathcal{F}_{\text{EO}} \nsubseteq \mathscr{A}$. Our #EO dichotomy (Theorem 4.1) and our Holant dichotomy (Theorem 1.1) both confirm the #P-completeness.

When restricted to 4-regular graphs, the above problem is a special case of six-vertex models with parameters $a = x = b = y = c = z = 1$ (Example 2.17). Huang and Lu proved that this problem is #P-complete [45]. Our #EO dichotomy (Theorem 4.1) and our trichotomy for six-vertex models (Theorem 9.21) both confirm the tractablity.

We use Pl-Holant$(\mathcal{F})$ to denote the problem Holant$(\mathcal{F})$ with respect to planar graphs. Compared to the six-vertex model over general graphs, the planar version has new tractable problems due to the FKT algorithm (see Chapter 9) under holographic transformations. This tractable class can give highly nontrivial problems. For example, we consider the following problem.

Problem 4 : SmallPell Pl-Holant(f), where f has the signature matrix

$$M(f) = \begin{bmatrix} 317830805723707970 & -283823304736008960\mathfrak{i} & 283823304736008960\mathfrak{i} & 317830805723707968 \\ -283823304736008960\mathfrak{i} & -253454564065438270 & 253454564065438272 & -283823304736008960\mathfrak{i} \\ 283823304736008960\mathfrak{i} & 253454564065438272 & -253454564065438270 & 283823304736008960\mathfrak{i} \\ 317830805723707968 & -283823304736008960\mathfrak{i} & 283823304736008960\mathfrak{i} & 317830805723707970 \end{bmatrix}.$$

After the holographic transformation by Z^{-1}, we have

$$\text{Pl-Holant}(f) \equiv_T \text{Pl-Holant}(\neq_2 | \widehat{f}),$$

where

$$M(\widehat{f}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 569465989630582080 & 321881208291348 49 & 0 \\ 0 & 321881208291348 49 & 181938015856416 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Since $(32188120829134849, 1819380158564160)$ is a solution of Pell's equation $x^2 - 313y^2 = 1$, we can show that $\widehat{f}$ is a matchgate signature by Matchgate Identities (Lemma 9.7). Our trichotomy for six-vertex models (Theorem 9.21) shows that Pl-Holant(f) can be computed in polynomial time.

In addition to matchgates and matchgates-transformable signatures, Theorem 9.21 gives a new class of tractable problems on planar graphs. They are provably not contained in any previously known tractable classes. For example, we consider the following problem.

Problem 5 : Pl-Holant$(\neq_2 |f)$, where f has the signature matrix $M(f) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & e^{\frac{\mathfrak{i}\pi}{4}} & 0 & 0 \\ 0 & 0 & e^{\frac{\mathfrak{i}7\pi}{4}} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

By Theorem 9.21 (condition 4 (ii)), Pl-Holant$(\neq_2 |f)$ can be computed in polynomial time. Note that f satisfies ARS. Our #EO dichotomy and Holant dichotomy show that Holant$(\neq_2 |f)$ is #P-hard without the planar restriction. It can be shown that f is neither a matchgate signature nor a matchgate transformable signature. Therefore, the tractability is not derivable from the FKT algorithm or a holographic transformation to it.

Chapter 3

Polynomial-Time Reductions

In this chapter, we introduce three kinds of polynomial-time Turing reductions that will be used in this dissertation. They are signature factorization, gadget construction and polynomial interpolation.

3.1 Signature Factorization

Recall that we define all signatures have positive arity and they are complex-valued without other specification. A nonzero signature g *divides* f, denoted by $g \mid f$, if there is a signature h such that $f = g \otimes h$ (with possibly a permutation of variables) or there is a constant λ such that $f = \lambda \cdot g$. In the latter case, if $\lambda \neq 0$, then we also have $f \mid g$ since $g = \frac{1}{\lambda} \cdot f$. For nonzero signatures, if both $g \mid f$ and $f \mid g$, then they are nonzero constant multiples of each other, and we say g is an *associate* of f, denoted by $g \sim f$. In terms of this division relation, we can define *irreducible* signatures and *prime* signatures. We will show that they are equivalent, and this gives us the *unique prime factorization* of signatures [*].

Definition 3.1 (Irreducible signatures). *A nonzero signature f is irreducible if $g \mid f$ implies that $g \sim f$. We say a signature is reducible if it is not irreducible or it is a zero signature. By definition, if a signature f of arity greater than 1 is reducible, then there is a factorization $f = g \otimes h$, for some signatures g and h (of positive arities).*

Definition 3.2 (Prime signatures). *A nonzero signature f is a prime signature, if for any nonzero signatures g and h, $f \mid g \otimes h$ implies that $f \mid g$ or $f \mid h$.*

Lemma 3.3. *The notions of irreducible signatures and prime signatures are equivalent.*

[*] The factorization of signatures is synonymous with the decomposition of multipartite quantum states in quantum information theory. There, the uniqueness of decomposition is usually assumed as a common knowledge. To our best knowledge, we are not aware of any formal proof.

证明. Suppose f is a prime signature. If f is not irreducible, then there is a nonzero signature g such that $g \mid f$ but not $g \sim f$. So there is a signature h (of arity $\geqslant 1$) such that $f = g \otimes h$, up to a permutation of variables ($h \not\equiv 0$ due to $f \not\equiv 0$). Then $f \mid g \otimes h$ and by being a prime, either $f \mid g$ or $f \mid h$. This is impossible because both g and h have lower arity than f.

Now, suppose f is irreducible and let $f \mid g \otimes h$, where g and h are nonzero signatures (of arity $\geqslant 1$). If $f \sim g \otimes h$, then $f = (\lambda g) \otimes h$ for some constant $\lambda \neq 0$. This contradicts f being irreducible. Thus, there is a nonzero signature e (of arity $\geqslant 1$) such that, up to a permutation of variables,

$$e \otimes f = g \otimes h. \tag{3.1}$$

Consider the scope of f, i.e., its set of variables. Suppose it intersects with the scopes of both g and h. Since $e \not\equiv 0$, we can pick an input β of e such that $e^{\beta} = \lambda_1 \neq 0$. By setting the variables in the scope of e to β on both sides of (3.1), we have

$$\lambda_1 \cdot f = g' \otimes h',$$

where g' and h' denote the resulting signatures from g and h respectively, both of which have a non-empty scope, i.e., having arity $\geqslant 1$. This is a contradiction to f being irreducible.

Hence the scope of f is a subset of the scope of either g or h. Suppose it is g, then the scope of h is a subset of the scope of e. Since $h \not\equiv 0$, we can pick an input α of h such that $h^{\alpha} = \lambda_2 \neq 0$. By setting the variables in the scope of h to α on both sides of (3.1), we have

$$e' \otimes f = \lambda_2 \cdot g,$$

where e' denotes the resulting signature by setting α in e. Thus, we have $f \mid g$. Similarly, if the scope of f is a subset of the scope of h, then we have $f \mid h$. □

A prime factorization of a signature f is $f = g_1 \otimes \ldots \otimes g_k$ up to a permutation of variables, where each g_i is a prime signature (irreducible). Start with any nonzero signature, if we keep factoring reducible signatures and induct on arity, any nonzero f has a factorization into irreducible (prime) signatures. The following important lemma says that the prime factorization of a nonzero signature is unique up to the order of the tensor factors and constant scaling factors. It can be proved using Lemma 3.3 and a standard argument, which we omit.

Lemma 3.4 (Unique prime factorization)**.** *Every nonzero signature f has a prime factorization. If f has prime factorizations $f = g_1 \otimes \ldots \otimes g_k$ and $f = h_1 \otimes \ldots \otimes h_\ell$, both up to a permutation of variables, then $k = \ell$ and after reordering the factors we have $g_i \sim h_i$ for all i.*

The following lemma shows that a real reducible signature has a real factorization, and equivalently a reducible signature satisfying ARS has a factorization in which all factors satisfy ARS.

Lemma 3.5. *1. Let f be a nonzero real-valued reducible signature, then there exists a factorization $f = g \otimes h$ such that g and h are both real-valued signatures.*

2. Equivalently, let $\widehat{f}$ be a nonzero reducible signature satisfying ARS*, then there exists a factorization $\widehat{f} = \widehat{g} \otimes \widehat{h}$ such that $\widehat{g}$ and $\widehat{h}$ both satisfy* ARS*.*

证明. We only prove the second part of this lemma. Then, the first part holds by Lemma 2.36. For brevity of notations, we rewrite $\widehat{f}$, $\widehat{g}$ and $\widehat{h}$ as f, g and h. Suppose $f = g \otimes h$. Since $f \not\equiv 0$, there is $\alpha \circ \beta$ such that $f^{\alpha\circ\beta} = g^\alpha \cdot h^\beta \neq 0$. Since f satisfy ARS, we have

$$\overline{g^\alpha} \cdot \overline{h^\beta} = \overline{f^{\alpha\circ\beta}} = f^{\bar{\alpha}\circ\bar{\beta}} = g^{\bar{\alpha}} \cdot h^{\bar{\beta}} \neq 0,$$

and also

$$g^\alpha \cdot h^{\bar{\beta}} = f^{\alpha\circ\bar{\beta}} = \overline{f^{\bar{\alpha}\circ\beta}} = \overline{g^{\bar{\alpha}}} \cdot \overline{h^\beta} \neq 0.$$

Multiply these two equalities, and cancel a nonzero common factor, we have

$$|g^\alpha|^2 = |g^{\bar{\alpha}}|^2.$$

Since g^α and $g^{\bar{\alpha}}$ have the same norm, we can pick a scalar $\lambda = 1/(g^\alpha g^{\bar{\alpha}})^{1/2}$ such that $\overline{\lambda g^\alpha} = \lambda g^{\bar{\alpha}}$. We have $f = (\lambda g) \otimes (\frac{1}{\lambda} h)$ and we will show λg and $\frac{1}{\lambda} h$ satisfy the ARS condition. We rename λg and $\frac{1}{\lambda} h$ by g and h, and now we can assume there is an α such that $\overline{g^\alpha} = g^{\bar{\alpha}} \neq 0$. For any input β of h, we have

$$\overline{g^\alpha} \cdot \overline{h^\beta} = \overline{f^{\alpha\circ\beta}} = f^{\bar{\alpha}\circ\bar{\beta}} = g^{\bar{\alpha}} \cdot h^{\bar{\beta}} = \overline{g^\alpha} \cdot h^{\bar{\beta}},$$

and hence, $\overline{h^{\beta}} = h^{\bar{\beta}}$. Hence $h \not\equiv 0$ satisfies the ARS condition. We can pick a particular β such that $\overline{h^{\beta}} = h^{\bar{\beta}} \neq 0$. Then, for any input α' of g, since f satisfies the ARS condition, we have $\overline{g^{\alpha'}} \cdot \overline{h^{\beta}} = g^{\overline{\alpha'}} \cdot h^{\overline{\beta}} = g^{\overline{\alpha'}} \cdot \overline{h^{\beta}}$, and hence $\overline{g^{\alpha'}} = g^{\overline{\alpha'}}$. That is, g also satisfies ARS. □

In the following, when we say that a real-valued reducible signature f has a factorization $g \otimes h$, we always assume that g and h are real-valued. Equivalently, when we say a signature $\widehat{f}$ satisfying ARS has a factorization $\widehat{g} \otimes \widehat{h}$, we always assume that $\widehat{g}$ and $\widehat{h}$ satisfy ARS.

If a vertex v in a signature grid is labeled by a reducible signature $f = g \otimes h$, we can replace the vertex v by two vertices v_1 and v_2 and label v_1 with g and v_2 with h, respectively. The incident edges of v become incident edges of v_1 and v_2 respectively according to the partition of variables of f in the tensor product of g and h. This does not change the Holant value. On the other hand, Lin and Wang proved that, from a real-valued reducible signature $f = g \otimes h \not\equiv 0$ we can freely replace f by g and h while preserving the complexity of a Holant problem.

Lemma 3.6 ([57]). *If a nonzero real-valued signature f has a real factorization $g \otimes h$, then*

$$\operatorname{Holant}(g, h, \mathcal{F}) \equiv_T \operatorname{Holant}(f, \mathcal{F}) \text{ and } \operatorname{Holant}(\neq_2 \mid \widehat{g}, \widehat{h}, \widehat{F}) \equiv_T \operatorname{Holant}(\neq_2 \mid \widehat{f}, \widehat{\mathcal{F}})$$

for any signature set $\mathcal{F}$ ($\widehat{\mathcal{F}}$). We say g ($\widehat{g}$) and h ($\widehat{h}$) are realizable from f ($\widehat{f}$) by factorization.

For a signature set $\mathcal{F}$, we use $\mathcal{F}^{\otimes k}$ ($k \geqslant 1$) to denote the set $\{\lambda \bigotimes_{i=1}^{k} f_i \mid \lambda \in \mathbb{R}\backslash\{0\}, f_i \in \mathcal{F}\}$. Here, λ denotes a normalization scalar. In this paper, we only dissertation the normalization by nonzero real constants. Note that $\mathcal{F}^{\otimes 1}$ contains all signatures obtained from $\mathcal{F}$ by normalization. We use $\mathcal{F}^{\otimes}$ to denote $\bigcup_{k=1}^{\infty} \mathcal{F}^{\otimes k}$.

3.2 Gadget Construction

One basic tool used throughout the dissertation is gadget construction. An $\mathcal{F}$-gate is similar to a signature grid (G, π) for $\operatorname{Holant}(\mathcal{F})$ except that $G = (V, E, D)$ is a graph with internal edges E and dangling edges D. The dangling edges D define input variables for the $\mathcal{F}$-gate. We denote the regular edges in E by $1, 2, \ldots, m$ and the dangling edges in D by $m + 1, \ldots, m + n$. Then the

$\mathcal{F}$-gate defines a function f

$$f(y_1, \ldots, y_n) = \sum_{\sigma: E \to \{0,1\}} \prod_{v \in V} f_v(\hat{\sigma} \mid_{E(v)})$$

where $(y_1, \ldots, y_n) \in \{0,1\}^n$ is an assignment on the dangling edges, $\hat{\sigma}$ is the extension of σ on E by the assignment $(y_1, \ldots, y_m)$, and f_v is the signature assigned at each vertex $v \in V$. This function f is called the signature of the $\mathcal{F}$-gate. There may be no internal edges in an $\mathcal{F}$-gate at all. In this case, f is simply a tensor product of these signatures f_v, i.e., $f = \bigotimes_{v \in V} f_v$ (with possibly a permutation of variables). We say a signature f is *realizable* from a signature set $\mathcal{F}$ by gadget construction if f is the signature of an $\mathcal{F}$-gate. If f is realizable from a set $\mathcal{F}$, then we can freely add f into $\mathcal{F}$ while preserving the complexity (Lemma 1.3 in [14]).

Lemma 3.7 ([14])**.** *If f is realizable from a set $\mathcal{F}$, then* $\operatorname{Holant}(f, \mathcal{F}) \equiv_T \operatorname{Holant}(\mathcal{F})$.

Recall that we use $=_2$ to denote the binary EQUALITY signature with truth table $(1, 0, 0, 1)$, and $\neq_2$ to the binary DISEQUALITY signature with truth table $(0, 1, 1, 0)$. If we view $\operatorname{Holant}(=_2 \mid \mathcal{F})$ as the edge-vertex incidence graph form of $\operatorname{Holant}(\mathcal{F})$, then it is equivalent to label every edge by $=_2$; similarly in the setting of $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$, every edge is labeled by $\neq_2$. The property of real-value and ARS are closed under gadget constructions using $=_2$ and $\neq_2$ respectively.

Lemma 3.8. *If f is realizable from a real-valued signature set $\mathcal{F}$ (in the setting of* $\operatorname{Holant}(=_2 \mid \mathcal{F})$*), then f is also real-valued. Equivalently, if $\widehat{f}$ is realizable from a signature set $\widehat{\mathcal{F}}$ satisfying* ARS *(in the setting of* $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$*), then $\widehat{f}$ also satisfies* ARS.

We may also write $=_2$ as $=_2^+$ and $\neq_2$ as $\neq_2^+$. We use $=_2^-$ to denote the binary signature $(1, 0, 0, -1)$ and $\neq_2^-$ to denote the binary signature $(0, 1, -1, 0)$. Let $\mathcal{B} = \{=_2^+, =_2^-, \neq_2^+, \neq_2^-\}$. We call them Bell signatures[*]. Let $\widehat{\mathcal{B}} = Z^{-1}\mathcal{B}$. One can check that

$$\widehat{\mathcal{B}} = \left\{\widehat{=_2^+}, \widehat{=_2^-}, \widehat{\neq_2^+}, \widehat{\neq_2^-}\right\} = \{\neq_2, =_2, (-\mathfrak{i}) \cdot =_2^-, \mathfrak{i} \cdot \neq_2^-\}.$$

We introduce the following four gadgets that will commonly used in this dissertation.

[*] These signatures correspond to Bell states $|\Phi^+\rangle = |00\rangle + |11\rangle$, $|\Phi^-\rangle = |00\rangle - |11\rangle$, $|\Psi^+\rangle = |01\rangle + |10\rangle$ and $|\Psi^-\rangle = |01\rangle - |10\rangle$ in quantum information science [9].

3.2.1 Merging Gadget

A basic gadget construction is *merging*. In the setting of Holant($=_2| \mathcal{F}$), given a signature $f \in \mathcal{F}$ of arity n, we can connect two variables x_i and x_j of f using $=_2$, and this operation gives a signature of arity $n-2$. We use $\partial_{ij} f$ or $\partial^+_{ij} f$ to denote this signature and $\partial_{ij} f = f^{00}_{ij} + f^{11}_{ij}$, where f^{ab}_{ij} denotes the signature obtained by setting $(x_i, x_j) = (a, b) \in \{0,1\}^2$. While in the setting of Holant($\neq_2| \widehat{\mathcal{F}}$), the above merging gadget is equivalent to connecting two variables x_i and x_j of $\widehat{f}$ using $\neq_2$. We denote the resulting signature by $\widehat{\partial}_{ij} \widehat{f}$ or $\widehat{\partial}^+_{ij} \widehat{f}$, and we have $\widehat{\partial_{ij} f} = \widehat{\partial}_{ij} \widehat{f} = \widehat{f}^{01}_{ij} + \widehat{f}^{10}_{ij}$. If $\neq_2$ is available (i.e., it either belongs to or can be realized from $\mathcal{F}$) in Holant($=_2| \mathcal{F}$), we can also connect two variables x_i and x_j of f using $\neq_2$. We denote the resulting signature by $\partial^{\widehat{+}}_{ij} f$. The merging gadget $\widehat{\partial}^+_{ij}$ is the same as $\partial^{\widehat{+}}_{ij}$, we use different notations to distinguish whether this gadget is used in the setting of Holant($=_2| \mathcal{F}$) or Holant($\neq| \widehat{\mathcal{F}}$).

Also, if $=^-_2$ and $\neq^-_2$ are available in Holant($=_2| \mathcal{F}$), then we can construct $\partial^-_{ij} f$ and $\partial^{\widehat{-}}_{ij} f$ by connecting x_i and x_j using $=^-_2$ and $\neq^-_2$ respectively. We also call ∂^-_{ij} and $\partial^{\widehat{-}}_{ij}$ merging gadgets. Without other specification, by default a merging gadget refers to ∂_{ij} in the setting of Holant($=_2|$ $\mathcal{F}$). Similarly by default a merging gadget refers to $\widehat{\partial}_{ij}$ in the setting of Holant($\neq_2| \widehat{\mathcal{F}}$).

The following lemma gives a relation between a signature f and signatures $\widehat{\partial}_{ij} f$ realized by merging using $\neq_2$.

Lemma 3.9. *Let f be a signature of arity $n \geqslant 3$. If $f^\alpha \neq 0$ for some $\alpha \in \mathbb{Z}^n_2$ with $\mathrm{wt}(\alpha) \neq 0, n$, then there exists a pair of indices $\{i, j\}$ and some $\beta \in \mathbb{Z}^{n-2}_2$ with $\mathrm{wt}(\beta) = \mathrm{wt}(\alpha) - 1$ such that $(\widehat{\partial}_{ij} f)^\beta \neq 0$. In particular, if for all pairs of indices $\{i, j\}$, $\widehat{\partial}_{ij} f \equiv 0$, then $f^\alpha = 0$ for all α with $\mathrm{wt}(\alpha) \neq 0$ and n; furthermore if f is an* EO *signature, then $f \equiv 0$.*

证明. Suppose there exists some α with $\mathrm{wt}(\alpha) \neq 0, n$ such that $f^\alpha \neq 0$. Clearly, α is not all-0 nor all-1. Since f has arity $n \geqslant 3$, α has length at least 3. Thus, we can find three bits in some order such that on these three bits, α takes value 001 or 110. Without loss of generality, we assume they are the first three bits of α and we denote α by 001δ or 110δ (δ maybe empty). We first consider the case that $\alpha = 001\delta$. Consider another two strings $\beta = 010\delta$ and $\gamma = 100\delta$. Note that if we merge variables x_1 and x_2 of f using $\neq_2$, we get $\partial_{12} f$, its entry $(\partial_{12} f)^{0\delta}$ on the input 0δ (for bit positions 3 to n) is the sum of $f^{010\delta}$ and $f^{100\delta}$. Clearly, $\mathrm{wt}(0\delta) = \mathrm{wt}(\delta) = \mathrm{wt}(\alpha) - 1$. If

$(\partial_{12}f)^{0\delta} = f^{010\delta} + f^{100\delta} \neq 0$, then we are done. Thus, we may assume that

$$(\partial_{12}f)^{0\delta} = f^{010\delta} + f^{100\delta} = 0.$$

Similarly, by merging variables x_1 and x_3 using $\neq_2$, we may assume that

$$(\partial_{13}f)^{0\delta} = f^{001\delta} + f^{100\delta} = 0,$$

and by merging variables x_2 and x_3 using $\neq_2$, we may assume that

$$(\partial_{23}f)^{0\delta} = f^{001\delta} + f^{010\delta} = 0.$$

These three equations have only a trivial solution, $f^{001\delta} = f^{010\delta} = f^{100\delta} = 0$. A contradiction with $f^{\alpha} = f^{001\delta} \neq 0$. Thus, among $(\partial_{12}f)^{0\delta}$, $(\partial_{13}f)^{0\delta}$ and $(\partial_{23}f)^{0\delta}$, at least on is nonzero.

If $\alpha = 110\delta$, the proof is symmetric. □

Merging gadget constructions on disjoint pairs of variables commute. Consider the signature $\partial_{ij}f$ realized by merging variables x_i and x_j of f using $=_2$. We may further merge variables x_u and x_v of $\partial_{ij}f$ for any $\{u, v\}$ disjoint with $\{i, j\}$, and we use $\partial_{(uv)(ij)}f = \partial_{uv}(\partial_{ij}f)$ to denote the realized signature. Note that these two merging operations commute, $\partial_{(uv)(ij)}f = \partial_{(ij)(uv)}f$. (Equivalently, for the merging gadget construction using $\neq_2$ on $\widehat{f}$, we have $\widehat{\partial}_{(uv)(ij)}\widehat{f} = \widehat{\partial}_{(ij)(uv)}\widehat{f}$.) We illustrate the commutativity in the following commutative diagram.

$$\begin{tikzcd}
f \arrow[r, "\partial_{(ij)}"] \arrow[d, "\partial_{(uv)}"'] & \partial_{(ij)}f \arrow[d, "\partial_{(uv)}"] \\
\partial_{(uv)}f \arrow[r, "\partial_{(ij)}"'] & \partial_{(uv)(ij)}f = \partial_{(ij)(uv)}f
\end{tikzcd}$$

Remark 3.10. *We adopt the notation ∂ for the similarity of the merging operation with taking partial derivatives. They both reduce the number of variables, they both are linear, and under mild smoothness conditions we know $\frac{\partial^2 f}{\partial x \partial y} = \frac{\partial^2 f}{\partial y \partial x}$.*

3.2.2 Extending Gadget

Another gadget construction that connects a nonzero binary signature b with a signature f is called *extending*. An extending gadget connects one variable of f with one variable of b using $=_2$ in the setting of $\operatorname{Holant}(=_2|\ \mathcal{F})$, and connects one variable of $\widehat{f}$ with one variable of $\widehat{b}$ using $\neq_2$ in the setting of $\operatorname{Holant}(\neq_2|\ \widehat{\mathcal{F}})$. By extending an irreducible signature using $=_2$ or $\neq_2$, we still get an irreducible signature.

A particular extending gadget is to extend f with binary signatures in $\mathcal{B}^{\otimes 1}$ using $=_2$ in the setting of $\operatorname{Holant}(\mathcal{F})$. We use $\{f\}^{\mathcal{B}}_{=_2}$ to denote the set of signatures realizable by extending some variables of f with binary signatures in $\mathcal{B}^{\otimes 1}$ using $=_2$ (recall that $\mathcal{B}^{\otimes 1}$ allows all nonzero real normalization scalars). Equivalently, this gadget is to extend $\widehat{f}$ with binary signatures in $\widehat{\mathcal{B}}$ using $\neq_2$ in the setting of $\operatorname{Holant}(\neq_2|\ \widehat{\mathcal{F}})$. We use $\{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$ to denote the set of signatures realizable by extending some variables of $\widehat{f}$ with binary signatures in $\widehat{\mathcal{B}}^{\otimes 1}$ using $\neq_2$. If $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$, then we can say that the extending gadget by $\widehat{\mathcal{B}}$ defines a relation between $\widehat{g}$ and $\widehat{f}$. Clearly, by extending variables of $\widehat{f}$ with $\neq_2 \in \widehat{\mathcal{B}}$ (using $\neq_2$), we still get $\widehat{f}$. Thus, $\widehat{f} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. So this relation is reflexive. The following lemma shows that this relation is symmetric and transitive, thus it is an equivalence relation.

Lemma 3.11. *1.* $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$ *iff* $\widehat{f} \in \{\widehat{g}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. *2. If* $\widehat{h} \in \{\widehat{g}\}^{\widehat{\mathcal{B}}}_{\neq_2}$ *and* $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$, *then* $\widehat{h} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$.

证明. Note that for any $\widehat{b} \in \widehat{\mathcal{B}}^{\otimes 1}$, if we connect any variable of $\widehat{b}$ with another arbitrary variable of a copy of the same $\widehat{b}$ using $\neq_2$, then we get $\neq_2$ after normalization. Also, by extending a variable of $\widehat{f}$ with $\neq_2$ (using $\neq_2$), we still get $\widehat{f}$. Suppose that $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$, and it is realized by extending certain variables x_i of $\widehat{f}$ with certain $b_i \in \widehat{\mathcal{B}}$. Then, by extending each of these variables x_i of $\widehat{g}$ with exactly the same $b_i \in \widehat{\mathcal{B}}$, we will get $\widehat{f}$ after normalization. Thus, $\widehat{f} \in \{\widehat{g}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. The other direction is proved by exchanging $\widehat{f}$ and $\widehat{g}$. Thus, $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$ iff $\widehat{f} \in \{\widehat{g}\}^{\widehat{\mathcal{B}}}_{\neq_2}$.

Also, note that for any $\widehat{b^1}, \widehat{b^2} \in \widehat{\mathcal{B}}^{\otimes 1}$, by connecting an arbitrary variable of $\widehat{b^1}$ with an arbitrary variable of $\widehat{b^2}$ using $\neq_2$, we still get a signature in $\widehat{\mathcal{B}}^{\otimes 1}$. Suppose that $\widehat{h}$ is realized by extending some variables x_i of $\widehat{g}$ with some $b^1_i \in \widehat{\mathcal{B}}^{\otimes 1}$. We may assume every variable x_i of $\widehat{g}$ has been so connected as $\neq_2 \in \widehat{\mathcal{B}}^{\otimes 1}$. Similarly we can assume $\widehat{g}$ is realized by extending every variable x_i of $\widehat{f}$ with some $b^2_i \in \widehat{\mathcal{B}}^{\otimes 1}$. Let b_i be the signature realized by connecting b^1_i and b^2_i (using $\neq_2$). Then, $\widehat{h}$ can be realized by extending each variable x_i of $\widehat{f}$ with $b_i \in \widehat{\mathcal{B}}^{\otimes 1}$. Thus, $\widehat{h} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. □

Remark 3.12. *As a corollary, if* $\widehat{g} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$*, then* $\{\widehat{g}\}^{\widehat{\mathcal{B}}}_{\neq_2} = \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$*.*

3.2.3 Mating Gadget

We first give the matrix representation of signatures. A signature f of arity $n \geqslant 2$ can be expressed as a $2^k \times 2^{n-k}$ matrix $M_{S_k}(f)$ where S_k is a set of k many variables among all n variables of f. The matrix $M_{S_k}(f)$ lists all 2^n many entries of f with the assignments of variables in S_k[*] listed in lexicographic order (from $\vec{0}^k$ to $\vec{1}^k$) as row index and the assignments of the other $n-k$ many variables in lexicographic order as column index. In particular, f can be expressed as a $2 \times 2^{n-1}$ matrix $M_i(f)$ which lists the 2^n entries of f with the assignments of variable x_i as row index (from $x_i = 0$ to $x_i = 1$) and the assignments of the other $n-1$ variables in lexicographic order as column index. Then,

$$M_i(f) = \begin{bmatrix} f^{0,00\ldots0} & f^{0,00\ldots1} & \ldots & f^{0,11\ldots1} \\ f^{1,00\ldots0} & f^{1,00\ldots1} & \ldots & f^{1,11\ldots1} \end{bmatrix} = \begin{bmatrix} \mathbf{f}_i^0 \\ \mathbf{f}_i^1 \end{bmatrix},$$

where $\mathbf{f}_i^a$ denotes the row vector indexed by $x_i = a$ in $M_i(f)$. Similarly, f can also be expressed as a $4 \times 2^{n-2}$ matrix with the assignments of two variables x_i and x_j as row index. Then,

$$M_{ij}(f) = \begin{bmatrix} f^{00,00\ldots0} & f^{00,00\ldots1} & \ldots & f^{00,11\ldots1} \\ f^{01,00\ldots0} & f^{01,00\ldots1} & \ldots & f^{01,11\ldots1} \\ f^{10,00\ldots0} & f^{10,00\ldots1} & \ldots & f^{10,11\ldots1} \\ f^{11,00\ldots0} & f^{11,00\ldots1} & \ldots & f^{11,11\ldots1} \end{bmatrix} = \begin{bmatrix} \mathbf{f}_{ij}^{00} \\ \mathbf{f}_{ij}^{01} \\ \mathbf{f}_{ij}^{10} \\ \mathbf{f}_{ij}^{11} \end{bmatrix},$$

where $\mathbf{f}_{ij}^{ab}$ denotes the row vector indexed by $(x_i, x_j) = (a, b)$ in $M_{ij}(f)$. For $=_2$, it has the 2-by-2 signature matrix $M(=_2) = I_2 = \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$. For $\neq_2$, $M(\neq_2) = N_2 = \left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]$.

We can also represent Tf as the matrix $M_{S_k}(Tf)$ with the assignments of variables in S_k as row index and the assignments of the other $n-k$ variables as column index. Then, we have $M_{S_k}(Tf) = T^{\otimes k} M_{S_k}(f) (T^{\mathrm{T}})^{\otimes n-k}$. Similarly, $M_{S_k}(fT^{-1}) = (T^{-1^{\mathrm{T}}})^{\otimes k} M_{S_k}(f)(T^{-1})^{\otimes n-k}$.

Now, we introduce the *mating* gadget. Given a real-valued signature f of arity $n \geqslant 2$, we

[*] Given a set of variables, without other specification, we always list them in the cardinal order i.e., from variables with the smallest index to the largest index.

connect two copies of f in the following manner: Fix a set S of $n-m$ variables among all n variables of f. For each $x_k \in S$, connect x_k of one copy of f with x_k of the other copy using $=_2$. The variables that are not in S are called dangling variables. In this paper, we only consider the case that $m = 1$ or 2. For $m = 1$, there is one dangling variable x_i. Then, the mating construction realizes a signature of arity 2, denoted by $\mathfrak{m}_i f$. It can be represented by matrix multiplication. We have

$$M(\mathfrak{m}_i f) = M_i(f) I_2^{\otimes(n-1)} M_i^{\mathtt{T}}(f) = \begin{bmatrix} \mathbf{f}_i^0 \\ \mathbf{f}_i^1 \end{bmatrix} \begin{bmatrix} \mathbf{f}_i^{0\mathtt{T}} & \mathbf{f}_i^{1\mathtt{T}} \end{bmatrix} = \begin{bmatrix} |\mathbf{f}_i^0|^2 & \langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle \\ \langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle & |\mathbf{f}_i^1|^2, \end{bmatrix} \tag{3.2}$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product and $|\cdot|$ denotes the norm defined by this inner product. (We will use the same notation $\langle \cdot, \cdot \rangle$ to denote the complex inner product (with conjugation) below. The notation is consistent.) Note that $|\langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle|^2 \leqslant |\mathbf{f}_i^0|^2 |\mathbf{f}_i^1|^2$ by the Cauchy-Schwarz inequality. Similarly, in the setting of Holant$(\neq_2 | \widehat{\mathcal{F}})$, the above mating operation is equivalent to connecting variables in S using $\neq_2$. We denote the resulting signature by $\widehat{\mathfrak{m}}_i \widehat{f}$, which is the same as $\widehat{\mathfrak{m}_i f}$, and we have

$$M(\widehat{\mathfrak{m}}_i \widehat{f}) = M_i(\widehat{f}) N_2^{\otimes n-1} M_i^{\mathtt{T}}(\widehat{f}) = \begin{bmatrix} \widehat{\mathbf{f}}_i^0 \\ \widehat{\mathbf{f}}_i^1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes(n-1)} \begin{bmatrix} \widehat{\mathbf{f}}_i^{0\mathtt{T}} & \widehat{\mathbf{f}}_i^{1\mathtt{T}} \end{bmatrix}.$$

Note that (in general complex-valued) $\widehat{f}$ satisfies the ARS since f is real, we have

$$N_2^{\otimes(n-1)} \widehat{\mathbf{f}}_i^{0\mathtt{T}} = (\widehat{f}^{0,11\ldots1}, \widehat{f}^{0,11\ldots0}, \ldots, \widehat{f}^{0,00\ldots0})^{\mathtt{T}} = (\overline{\widehat{f}^{1,00\ldots0}}, \overline{\widehat{f}^{1,00\ldots1}}, \ldots, \overline{\widehat{f}^{1,11\ldots1}}) = \overline{\widehat{\mathbf{f}}_i^1}^{\mathtt{T}}.$$

Thus, we have

$$M(\widehat{\mathfrak{m}}_i \widehat{f}) = \begin{bmatrix} \widehat{\mathbf{f}}_i^0 \\ \widehat{\mathbf{f}}_i^1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes(n-1)} \begin{bmatrix} \widehat{\mathbf{f}}_i^{0\mathtt{T}} & \widehat{\mathbf{f}}_i^{1\mathtt{T}} \end{bmatrix} = \begin{bmatrix} \widehat{\mathbf{f}}_i^0 \\ \widehat{\mathbf{f}}_i^1 \end{bmatrix} \begin{bmatrix} \overline{\widehat{\mathbf{f}}_i^1}^{\mathtt{T}} & \overline{\widehat{\mathbf{f}}_i^0}^{\mathtt{T}} \end{bmatrix} = \begin{bmatrix} \langle \widehat{\mathbf{f}}_i^0, \widehat{\mathbf{f}}_i^1 \rangle & |\widehat{\mathbf{f}}_i^0|^2 \\ |\widehat{\mathbf{f}}_i^1|^2 & \langle \widehat{\mathbf{f}}_i^1, \widehat{\mathbf{f}}_i^0 \rangle \end{bmatrix}. \tag{3.3}$$

If there are two dangling variables x_i and x_j, we use $\mathfrak{m}_{ij} f$ and $\widehat{\mathfrak{m}}_{ij} \widehat{f}$ to denote the signatures realized by mating f using $=_2$ and mating $\widehat{f}$ using $\neq_2$ respectively.

With respect to mating gadgets, we introduce the following orthogonality conditions.

Definition 3.13 (First order orthogonality). *Let f be a complex-valued signature of arity $n \geqslant 2$. It satisfies the* first order orthogonality (1ST-ORTH) *if there exists some $\mu \neq 0$ such that for all* *indices $i \in [n]$, the entries of f satisfy the following equations*

$$|\mathbf{f}_i^0|^2 = |\mathbf{f}_i^1|^2 = \mu, \ \textit{and} \ \langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle = 0.$$

Remark 3.14. *When f is a real-valued signature, the inner product is just the ordinary dot product which can be represented by mating using $=_2$. Thus, f satisfies* 1st-Orth *iff there is some real $\mu \neq 0$ such that for all indices i, $M(\mathfrak{m}_i f) = \mu I_2$. On the other hand, when $\widehat{f}$ is a signature with* ars*, by (3.3), the complex inner product can be represented by mating using $\neq_2$. Thus, $\widehat{f}$ satisfies* 1st-Orth *iff there is some real $\mu \neq 0$ such that for all i, $M(\widehat{\mathfrak{m}}_i \widehat{f}) = \mu N_2$. Moreover, f satisfies* 1st-Orth *iff $\widehat{f}$ satisfies it.*

Lemma 3.15. *Let f be a real-valued signature of arity n. If for all indices $i \in [n]$, $M(\mathfrak{m}_i f) = \mu_i I_2$ for some real $\mu_i \neq 0$, then f satisfies* 1st-Orth *(i.e., all μ_i have the same value). Equivalently, if for all indices $i \in [n]$, $M(\widehat{\mathfrak{m}}_i \widehat{f}) = \mu_i N_2$ for some real $\mu_i \neq 0$, then $\widehat{f}$ satisfies* 1st-Orth.

证明. We prove this lemma in the setting of Holant$(=_2 |\ \mathcal{F})$. For every $M(\mathfrak{m}_i f) = \mu_i \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, if we further connect the two dangling variables x_i of $\mathfrak{m}_i f$, which totally connects the corresponding pairs of variables in two copies of f, we get a value $2\mu_i$. This value does not depend on the particular index i. Thus, all μ_i have the same value for $i \in [n]$. We denote this value by μ. □

Definition 3.16 (Binary orthogonal signature)**.** *A real-valued binary signature $f(x_1, x_2)$ is orthogonal if $M_1(f) M_1^{\mathtt{T}}(f) = \lambda I_2$ for some real $\lambda > 0$.*

Remark 3.17. *Since $M_2(f) = M_1^{\mathtt{T}}(f)$, $M_1(f) M_1^{\mathtt{T}}(f) = \lambda I_2$ iff $M_2(f) M_2^{\mathtt{T}}(f) = \lambda I_2$. Thus, a real-valued binary signature f is orthogonal iff f satisfies* 1st-Orth.

Let $\mathscr{E}_n = \{\alpha \in \mathbb{Z}_2^n \mid \mathrm{wt}(\alpha) \text{ is even}\}$, and $\mathscr{O}_n = \{\alpha \in \mathbb{Z}_2^n \mid \mathrm{wt}(\alpha) \text{ is odd}\}$. A signature f of arity n has even or odd parity if its support $\mathscr{S}(f) \subseteq \mathscr{E}_n$ or $\mathscr{S}(f) \subseteq \mathscr{O}_n$ respectively. In both cases, we say that f has parity.

Lemma 3.18. *A binary signature f is orthogonal or a zero signature iff $\widehat{f}$ has parity and* ars.

证明. Consider $M_1(f)$ and $M_1(\widehat{f}) = M_1(Z^{-1} f) = Z^{-1} M_1(f) (Z^{-1})^{\mathtt{T}}$. Then, $M_1(f) = \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]$ iff $M_1(\widehat{f}) = \left[\begin{smallmatrix} 0 & a+bi \\ a-bi & 0 \end{smallmatrix}\right]$, and $M_1(f) = \left[\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right]$ iff $M_1(\widehat{f}) = \left[\begin{smallmatrix} a-bi & 0 \\ 0 & a+bi \end{smallmatrix}\right]$. Also, $f \equiv 0$ iff $\widehat{f} \equiv 0$ which also has parity. □

Let $\mathcal{O}$ denote the set of all binary orthogonal signatures and the binary zero signature. Then, $\widehat{\mathcal{O}} = Z^{-1}\mathcal{O}$ is the set of all binary signatures with ARS and parity (including the binary zero signature). Note that $\mathcal{B} \subseteq \mathcal{O}$ and $\widehat{\mathcal{B}} \subseteq \widehat{\mathcal{O}}$. For signatures in $\widehat{\mathcal{O}}$, we have the following lemma.

Lemma 3.19. *Let $\widehat{b_1}(x_1, x_2), \widehat{b_2}(y_1, y_2) \in \widehat{\mathcal{O}}$. If by connecting the variable x_1 of $\widehat{b_1}$ and the variable y_1 of $\widehat{b_2}$ using $\neq_2$, we get $\lambda\cdot \neq_2 (x_2, y_2)$ for some $\lambda \in \mathbb{R}\backslash\{0\}$, then $\widehat{b_1} \sim \widehat{b_2}$. Moreover, by connecting the variable x_2 of $\widehat{b_1}$ and the variable y_2 of $\widehat{b_2}$, we will get $\lambda\cdot \neq_2 (x_1, y_1)$.*

证明. We prove this lemma in the setting of Holant$(\mathcal{F})$ after the transformation Z back. Now, $b_1 = Z\widehat{b_1} \in \mathcal{O}$ and $b_2 = Z\widehat{b_2} \in \mathcal{O}$.

Consider matrices $M_1(b_1) = M_2^{\mathtt{T}}(b_1)$ and $M_1(b_2) = M_2^{\mathtt{T}}(b_2)$. Since $b_1, b_2 \in \mathcal{O}$, both $M_1(b_1)$ and $M_1(b_2)$ are real multiples of real orthogonal matrices, of which there are two types, either rotations or reflections. For such matrices X, Y, to get $X^{\mathtt{T}}Y = \lambda I_2$ for some $\lambda \in \mathbb{R}\backslash\{0\}$, X and Y must be either both reflections, or both rotations of the same angle, up to nonzero real multiples. First suppose $M_1(b_1) = \left[\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right]$, reflection. Then by connecting x_1 of b_1 and y_1 of b_2 using $=_2$ we get $\lambda\cdot =_2 (x_2, y_2)$, i.e., $M_1^{\mathtt{T}}(b_1)M_1(b_2) = \lambda I_2$. This implies that b_2 is the same reflection up to a nonzero scalar, i.e., $b_2 \sim b_1$. Similarly, for a rotation $M_1(b_1) = \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]$, $M_1^{\mathtt{T}}(b_1)M_1(b_2) = \lambda I_2$ implies that b_2 is also a rotation of the same angle as b_1 up to a nonzero scalar, thus $b_2 \sim b_1$. In either case, by connecting the variable x_2 of b_1 and the variable y_2 of b_2, we will get

$$M_2^{\mathtt{T}}(b_1)M_2(b_2) = M_1(b_1)M_1^{\mathtt{T}}(b_2) = \lambda I_2.$$

This means that we get the signature $\lambda\cdot =_2 (x_1, y_1)$. The statement of the lemma follows from this after a Z^{-1} transformation. □

Definition 3.20 (Second order orthogonality). *Let f be a complex-valued signature of arity $n \geqslant 4$. It satisfies the* second order orthogonality (2ND-ORTH) *if there exists some $\lambda \neq 0$ such that for all pairs of indices $\{i, j\} \subseteq [n]$, the entries of f satisfy*

$$|\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ij}^{01}|^2 = |\mathbf{f}_{ij}^{10}|^2 = |\mathbf{f}_{ij}^{11}|^2 = \lambda, \qquad \text{and} \qquad \langle \mathbf{f}_{ij}^{ab}, \mathbf{f}_{ij}^{cd} \rangle = 0 \qquad \text{for all } (a,b) \neq (c,d).$$

Remark 3.21. *Similar to the remark of first order orthogonality, f satisfies* 2ND-ORTH *iff there is some $\lambda \neq 0$ such that for all (i,j), $M(\mathfrak{m}_{ij}f) = \lambda I_4 = \lambda I_2^{\otimes 2}$, and $\widehat{f}$ satisfies* 2ND-ORTH *iff there* *is some $\lambda \neq 0$ such that for all (i, j), $M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \lambda N_4 = \lambda N_2^{\otimes 2}$. Moreover, f satisfies* 2nd-Orth *iff $\widehat{f}$ satisfies it. Clearly,* 2nd-Orth *implies* 1st-Orth.

Lemma 3.22. *Let f be a real-valued signature of arity n. If for all indices $\{i, j\} \subseteq [n]$, $M(\mathfrak{m}_{ij}f) = \lambda_{ij}I_4$ for some real $\lambda_{ij} \neq 0$, then f satisfies* 2rd-Orth *(i.e., all λ_{ij} have the same value). Equivalently, if for all indices $\{i, j\} \subseteq [n]$, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \lambda_{ij}N_4$ for some real $\lambda_{ij} \neq 0$, then $\widehat{f}$ satisfies* 2rd-Orth.

证明. We prove this lemma in the setting of Holant$(=_2|\ \mathcal{F})$. For every $M(\mathfrak{m}_{ij}f) = \lambda_{ij}I_4$, if we connect further the two respective pairs of variables of $\mathfrak{m}_{ij}f$, which totally connects two copies of f, we get a value $4\lambda_{ij}$. This value clearly does not depend on the particular indices $\{i, j\}$. We denote the value λ_{ij} by λ. □

3.2.4 Pinning Gadget

If the unary signature $\Delta_0 = (1, 0)$ is available, there is another basic gadget construction called *pining*. Given a signature f of arity n and the unary signature Δ_0, we can connect the variable x_i of f with $\Delta_0 = (1, 0)$, and we get a signature of arity $n - 1$, denoted by f_i^0. Clearly, f_i^0 is realized by setting the variable x_i of f to 0. If by pinning any variable of f, we can only realize the zero signature, then f itself is also "almost" a zero signature.

Lemma 3.23. *Let f be a signature of arity $n \geqslant 2$. If for any index i, by pinning the variable x_i of f to 0, we have $f_i^0 \equiv 0$, then $f^\alpha = 0$ for any $\mathrm{wt}(\alpha) \neq n$. If, furthermore, there is a pair of indices $\{j, k\}$ such that $\partial_{jk}f \equiv 0$, then $f \equiv 0$.*

证明. For any $\mathrm{wt}(\alpha) \neq n$, there is an index i such that $\alpha_i = 0$. By pinning x_i to 0, we get the signature f_i^0. We know f^α is an entry in f_i^0, and then $f^\alpha = 0$ since $f_i^0 \equiv 0$.

Suppose there is a pair of indices $\{j, k\}$ such that $\partial_{jk}f \equiv 0$. Let β denote the string of n bits where $\beta_j = \beta_k = 0$ and $\beta_\ell = 1$ elsewhere, and γ denote the string of n bits 1s. Consider the signature $\partial_{jk}f$. We know $f^\beta + f^\gamma$ is an entry in $\partial_{jk}f$ (when $\partial_{jk}f$ is a constant, we have $f^\beta + f^\gamma = \partial_{jk}f$). We know $f^\beta + f^\gamma = 0$ since $\partial_{jk}f \equiv 0$. Clearly, $\mathrm{wt}(\beta) \neq n$ and we have $f^\beta = 0$. Thus, we have $f^\gamma = 0$. Thus, we have $f \equiv 0$. □

Pinning gadget constructions on different variables also commute. Suppose $i \neq j$. Then, $f_{ij}^{00} = (f_i^0)_j^0 = (f_j^0)_i^0 = f_{ji}^{00}$. Also, the pinning gadget construction and the merging gadget construction on distinct variables commute. Suppose i, j, k are distinct. Then, $(\partial_{jk} f)_i^0 = \partial_{jk}(f_i^0) \not\equiv 0$. The commutativity of merging and pinning gadgets (as well as other gadgets) is a key property in our proof.

We use the following Table 1 to compare notations in $\operatorname{Holant}(=_2 \mid \mathcal{F})$ and $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$. In the left column, we list notations in $\operatorname{Holant}(=_2 \mid \mathcal{F})$ where $\mathcal{F}$ is a set of real-valued signatures, and in the right column, we list corresponding notations in $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ where $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ is the set of complex-valued signatures with ARS. Note that although $\mathcal{EO}$ also satisfies ARS, we will only use it in $\operatorname{Holant}(=_2 \mid \mathcal{F})$. Similarly, we will only use $\mathcal{DEQ}$ in $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ although it is real-valued.

$\operatorname{Holant}(=_2 \mid \mathcal{F})$ where $\mathcal{F}$ is real-valued	$\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ where $\widehat{\mathcal{F}}$ satisfies ARS
$\mathcal{EQ} = \{=_1, =_2, \ldots, =_n, \ldots\}$	N/A
N/A	$\mathcal{DEQ} = \{\neq_2, \neq_4, \ldots, \neq_{2n}, \ldots\}$, $\mathcal{D} = \{\neq_2\}$
$\mathcal{O} = \{$binary orthogonal and zero signatures$\}$	$\widehat{\mathcal{O}} = \{$binary signatures with ARS and parity$\}$
$\mathcal{B} = \{=_2, =_2^-, \neq_2, \neq_2^-\}$	$\widehat{\mathcal{B}} = \{\neq_2, =_2, (-\mathfrak{i}) \cdot =_2^-, \mathfrak{i} \cdot \neq_2^-\}$
a holographic transformation $Q\mathcal{F}$ by $Q \in \mathbf{O}_2$	a holographic transformation $\widehat{Q}\widehat{\mathcal{F}}$ by $\widehat{Q} \in \widehat{\mathbf{O}_2}$
a merging gadget $\partial_{ij} f = f_{ij}^{00} + f_{ij}^{11}$	a merging gadget $\widehat{\partial}_{ij} \widehat{f} = \widehat{f}_{ij}^{01} + \widehat{f}_{ij}^{10}$
extending gadgets $\{f\}_{=_2}^{\mathcal{B}}$ with $\mathcal{B}$	extending gadgets $\{\widehat{f}\}_{\neq_2}^{\widehat{\mathcal{B}}}$ with $\widehat{\mathcal{B}}$
a mating gadget $\mathfrak{m}_{ij} f = M_{ij}(f) I_2^{\otimes n-1} M_{ij}^{\mathtt{T}}(f)$	a mating gadget $\widehat{\mathfrak{m}}_{ij} \widehat{f} = M_{ij}(\widehat{f}) N_2^{\otimes n-1} M_{ij}^{\mathtt{T}}(\widehat{f})$

表 1: Comparisons of notations in $\operatorname{Holant}(=_2 \mid \mathcal{F})$ and $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$

Recall that $\mathcal{F}^{\otimes}$ denotes the set $\{\lambda \bigotimes_{i=1}^{k} f_i \mid \lambda \in \mathbb{R}\backslash\{0\}, k \geqslant 1, f_i \in \mathcal{F}\}$ for any signature set $\mathcal{F}$. We remark that both $\mathcal{O}^{\otimes}$ and $\widehat{\mathcal{O}}^{\otimes}$ contain all zero signatures of even arity since the binary zero signature is in $\mathcal{O}$ and $\widehat{\mathcal{O}}$. However, $\mathcal{B}^{\otimes}$ and $\widehat{\mathcal{B}}^{\otimes}$ do *not* contain any zero signatures.

3.3 Polynomial Interpolation

Polynomial interpolation is a powerful technique to prove #P-hardness for counting problems. We give the following lemmas. For more on polynomial interpolation, please see Section 9.2.3.

Lemma 3.24. *Let g_0 and g be two nonzero binary signatures with $M(g_0) = P^{-1} \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right] P$ and $M(g) = P^{-1} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} P$ for some invertible matrix P. If $\lambda_1\lambda_2 \neq 0$ and $|\frac{\lambda_1}{\lambda_2}| \neq 1$, then*

$$\operatorname{Holant}(g_0, \mathcal{F}) \leqslant_T \operatorname{Holant}(g, \mathcal{F})$$

for any signature set $\mathcal{F}$.

Lemma 3.25. *Let g be a nonzero binary signature with $M(g) = P^{-1} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} P$ for some invertible matrix P, and h be a nonzero unary signature. If $\lambda_1\lambda_2 \neq 0$, $|\frac{\lambda_1}{\lambda_2}| \neq 1$, and h (as a column vector) is not an eigenvector of $M(g)$, then*

$$\operatorname{Holant}(h', g, \mathcal{F}) \leqslant_T \operatorname{Holant}(h, g, \mathcal{F})$$

for any unary signature h' and any signature set $\mathcal{F}$.

Chapter 4

Dichotomy for #EO Problems with Arrow Reversal Symmetry

In this chapter, we prove a complexity dichotomy for #EO problems with arrow reversal symmetry (ARS). Recall that ARS requires $f(\overline{\alpha}) = \overline{f(\alpha)}$ for all α, where $\overline{f(\alpha)}$ denotes the complex conjugation of $f(\alpha)$, and $\overline{\alpha}$ denotes the bit-wise complement of α.

Theorem 4.1. *Let $\mathcal{F}$ be a set of* EO *signatures satisfying* ARS*. Then,* #EO($\mathcal{F}$) *is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$, in which cases it is tractable.*

In this chapter, without other specification we use f to denote a complex-valued EO signature (whose support is on half-weighted inputs) satisfying ARS, and $\mathcal{F}$ to denote a set of such signatures.

4.1 Factorization and Gadget Construction of EO Signatures

In Chapter 3, we introduced certain polynomial-time reductions for general Holant problems. To apply them to #EO problems we need to take care of one subtlety, namely any signature signature realizable from EO signatures (by factorization or gadget construction) is still an EO signature, and hence is suitable for #EO problems.

Lemma 4.2. *Let f be a nonzero reducible* EO *signature satisfying* ARS*. Then, for any factorization $f = g \otimes h$, g and h are both* EO *signatures.*

证明. Since $f \not\equiv 0$, we know $g \not\equiv 0$ and $h \not\equiv 0$ for any factorization $f = g \otimes h$. For a contradiction, suppose there is a factorization $f = g \otimes h$ such that g is not an EO signature. Then, there is an input α of g such that $g^{\alpha} \neq 0$, and $\mathrm{wt}(\alpha) \neq \mathrm{wt}(\bar{\alpha})$. (This is true no matter whether g has even or odd arity.) Since $h \not\equiv 0$, there is an input β of h such that $h^{\beta} \neq 0$. Note that $\alpha \circ \beta$ is an input of f

and we have

$$f^{\alpha\circ\beta} = g^{\alpha} \cdot h^{\beta} \neq 0.$$

Moreover, since f satisfies ARS, we have

$$0 \neq f^{\bar{\alpha}\circ\bar{\beta}} = g^{\bar{\alpha}} \cdot h^{\bar{\beta}}.$$

Then, we know $g^{\bar{\alpha}} \neq 0$, and hence

$$f^{\bar{\alpha}\circ\beta} = g^{\bar{\alpha}} \cdot h^{\beta} \neq 0.$$

However, notice that $\mathrm{wt}(\alpha \circ \beta) = \mathrm{wt}(\alpha) + \mathrm{wt}(\beta) \neq \mathrm{wt}(\bar{\alpha}) + \mathrm{wt}(\beta) = \mathrm{wt}(\bar{\alpha} \circ \beta)$. This implies that $\mathscr{S}(f) \nsubseteq \mathscr{H}_{\mathrm{arity}(f)}$, contradicting f being an EO signature. Thus, for any $f = g \otimes h$, f and g are both EO signatures. □

Remark 4.3. *This lemma does not hold without assuming* ARS*. For example,* $f = (0, 0, 1, 0) = (0, 1) \otimes (1, 0)$*, where* $(0, 0, 1, 0)$ *is an EO signature but* $(0, 1)$ *and* $(1, 0)$ *are not. Also, by Lemma 3.5, if an* EO *signature satisfying* ARS *is reducible, then it can be factorized as a tensor product of* EO *signatures satisfying* ARS*.*

In the following, when we say that a nonzero EO signature f satisfying ARS has a factorization $g \otimes h$, we always assume g and h are EO signatures satisfying ARS. By Lemma 3.6, we have the following reduction.

Lemma 4.4. *If a nonzero* EO *signature* f *satisfying* ARS *has a factorization* $g \otimes h$*, then*

$$\#\mathrm{EO}(\{g, h\} \cup \mathcal{F}) \equiv_T \#\mathrm{EO}(\{f\} \cup \mathcal{F})$$

for any EO *signature set* $\mathcal{F}$*. In this case, we also say* g *and* h *are realizable from* f*.*

Then, we consider gadget constructions of EO signatures. Note that in the framework of #EO problems, edges are labelled by $\neq_2$.

Lemma 4.5. *Any signature realizable from a set* $\mathcal{F}$ *of* EO *signatures satisfying* ARS *is also an* EO *signature satisfying* ARS*.*

证明. By definition $\widehat{\partial}_{ij} f = f_{ij}^{01} + f_{ij}^{10}$. Hence for any EO signature satisfying ARS, after merging any two variables, the realized signature is still an EO signature satisfying ARS. Then, suppose f is realized by a graph G with dangling edges and n vertices labeled by signatures $f_1, f_2, \ldots, f_n \in \mathcal{F}$. We first cut all internal edges in G and get the signature $f' = f_1 \otimes f_2 \otimes \cdots \otimes f_n$. Clearly f' is an EO signature satisfying ARS since all f_i are. Then, f can be realized by *merging* (with $\neq_2$) all cut edges of f' in a sequence. After each merging operation, the realized signature is an EO signature satisfying ARS, and hence f is an EO signature satisfying ARS. □

Having established Lemma 4.5, we have the following reduction.

Lemma 4.6. *If f is realizable from a set $\mathcal{F}$ of* EO *signatures, then* $\#\text{EO}(\{f\} \cup \mathcal{F}) \equiv_T \#\text{EO}(\mathcal{F})$.

4.2 Reduction from Six-Vertex Models to #EO problems

The six-vertex model can be expressed by the problem $\#\text{EO}(f)$ where f is an EO signature of arity 4. The complexity classification of this problem is known even when f does not satisfy ARS (see [25] or Chapter 9 for more details). Here, we restate this result for the setting of signatures with ARS.

Theorem 4.7. *Let f be an* EO *signature of arity* 4 *satisfying* ARS*. Then* $\#\text{EO}(f)$ *is #P-hard unless $f \in \mathscr{P}$.*

For nonzero 4-ary signatures satisfying ARS, we characterize product-type signatures by the following two lemmas.

Lemma 4.8. *Let f be an* EO *signature of arity* 4 *satisfying* ARS*. If f has support size* 2*, then $f \in \mathscr{P}$.*

证明. This lemma directly follows the alternative definition of $\mathscr{P}$ (Lemma 2.6). □

Lemma 4.9. *Let f be an* EO *signature of arity* 4 *satisfying* ARS *with support size* 4*, say f^{α}, f^{β}, $f^{\overline{\alpha}}$ and $f^{\overline{\beta}} \neq 0$ where $\alpha \neq \beta, \overline{\beta}$. Then $f \in \mathscr{P}$ if and only if $|f^{\alpha}| = |f^{\beta}|$.*

证明. Suppose $f \in \mathscr{P}$. Then by Lemma 2.10 it has affine support. Being an EO signature with support size 4, we can show that, after renaming its 4 variables we may assume the support is defined by $(x_1 \neq x_2) \wedge (x_3 \neq x_4)$. No binary equality is used in its definition for being in $\mathscr{P}$, and exactly these two binary disequalities are used. Then f takes values ac, ad, bc, bd on $0101, 0110, 1001, 1010$ for some $a, b, c, d \neq 0$. By ARS, we have $bd = \overline{ac}$ and $ad = \overline{bc}$. It follows that $|a| = |b|$. Similarly $|c| = |d|$. Therefore all nonzero values of f have the same norm. Hence $|f^\alpha| = |f^\beta|$.

Conversely, suppose $f^\alpha = re^{i\varphi}$ and $f^\beta = re^{i\psi}$, for some $r > 0$ and φ, ψ. By renaming variables we may assume $\alpha = 0101$, $\beta = 0110$. Let $a = re^{i\frac{\varphi+\psi}{2}}$, $c = e^{i\frac{\varphi-\psi}{2}}$, Then the unary functions $(a, \bar{a})$ on x_1 and $(c, \bar{c})$ on x_3, times $(x_1 \neq x_2) \wedge (x_3 \neq x_4)$ defines $f \in \mathscr{P}$. □

Now, we wish to leverage the complexity classification of six-vertex models and realize arity 4 signatures from a given set of signatures, to which we can apply the known tractability criteria. We will use the mating gadget to realize signatures of arity 4, then apply the Cauchy-Schwarz inequality. Consider a nonzero signature $f \in \mathcal{F}$. We may assume that f is irreducible. Otherwise we can replace f by its irreducible factors without changing the complexity due to Lemma 4.4. We have the following lemma.

Lemma 4.10. *Let $f \in \mathcal{F}$ be an irreducible* EO *signature of arity $n \geqslant 4$. Then one of the following alternatives holds:*

- *$\#\mathrm{EO}(\mathcal{F})$ is #P-hard, or*
- *$\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_{\mathrm{T}} \#\mathrm{EO}(\mathcal{F})$, or*
- *f satisfies second order orthogonality* (2RD-ORTH)*, i.e., there exists a nonzero constant λ, such that for all pairs of indices $\{i, j\} \subseteq [n]$, $M(\widehat{\mathfrak{m}}_{ij} f) = \lambda N_4$, where $N_4 = \left[\begin{smallmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{smallmatrix}\right]$.*

证明. Since f is irreducible, $f \not\equiv 0$. We consider the signature $\widehat{\mathfrak{m}}_{ij} f$ realized by mating two copies of f for all pairs of distinct indices $\{i, j\} \subseteq [n]$. If $\#\mathrm{EO}(\widehat{\mathfrak{m}}_{ij} f)$ is already #P-hard, then $\#\mathrm{EO}(\mathcal{F})$ is also #P-hard since $\#\mathrm{EO}(\widehat{\mathfrak{m}}_{ij} f) \leqslant_T \#\mathrm{EO}(\mathcal{F})$. Since we already have a complexity dichotomy for arity 4 signatures, we may assume that $\widehat{\mathfrak{m}}_{ij} f$ satisfies the tractability condition and that $\#\mathrm{EO}(\widehat{\mathfrak{m}}_{ij} f)$

is computable in polynomial time for every pair $\{i,j\}$. Notice that

$$M(\widehat{\mathfrak{m}}_{ij}f) = M_{ij}(f)N_2^{\otimes(n-2)}M_{ij}^{\mathtt{T}}(f) = \begin{bmatrix} 0 & 0 & 0 & |\mathbf{f}_{ij}^{00}|^2 \\ 0 & \langle \mathbf{f}_{ij}^{01}, \mathbf{f}_{ij}^{10} \rangle & |\mathbf{f}_{ij}^{01}|^2 & 0 \\ 0 & |\mathbf{f}_{ij}^{10}|^2 & \langle \mathbf{f}_{ij}^{10}, \mathbf{f}_{ij}^{01} \rangle & 0 \\ |\mathbf{f}_{ij}^{11}|^2 & 0 & 0 & 0 \end{bmatrix}. \tag{4.1}$$

If there exists some $\{i,j\}$, such that $\widehat{\mathfrak{m}}_{ij}f \equiv 0$, then $\mathbf{f}_{ij}^{00} = \mathbf{f}_{ij}^{01} = \mathbf{f}_{ij}^{10} = \mathbf{f}_{ij}^{11} \equiv 0$, which implies $f \equiv 0$. A contradiction. So we have $\widehat{\mathfrak{m}}_{ij}f \not\equiv 0$, for all pairs $\{i,j\}$. Then by Theorem 4.7, $\#\mathrm{EO}(\widehat{\mathfrak{m}}_{ij}f)$ is tractable if and only if $\widehat{\mathfrak{m}}_{ij}f \in \mathscr{P}$. By Lemma 2.10, we know $\widehat{\mathfrak{m}}_{ij}f$ has affine support, and being nonzero it has support size either 2 or 4 (by the form in (4.1), the support size is not 1). There are two cases depending on the support size of $\widehat{\mathfrak{m}}_{ij}f$ for all pairs $\{i,j\}$.

1. There exists some pair $\{i,j\}$ such that $\widehat{\mathfrak{m}}_{ij}f$ has support size 2. Then,

   - Either $M(\widehat{\mathfrak{m}}_{ij}f)$ has the form $\lambda_{ij}\left[\begin{smallmatrix} 0&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&0 \end{smallmatrix}\right]$ where $\lambda_{ij} = |\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ij}^{11}|^2 \neq 0$,
   - *or* $M(\widehat{\mathfrak{m}}_{ij}f)$ has the form $\lambda_{ij}\left[\begin{smallmatrix} 0&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&0 \end{smallmatrix}\right]$ where $\lambda_{ij} = |\mathbf{f}_{ij}^{01}|^2 = |\mathbf{f}_{ij}^{10}|^2 \neq 0$.

   The form that $\langle \mathbf{f}_{ij}^{01}, \mathbf{f}_{ij}^{10} \rangle \neq 0$ while $|\mathbf{f}_{ij}^{01}|^2 = 0$ cannot occur since $|\langle \mathbf{f}_{ij}^{01}, \mathbf{f}_{ij}^{10} \rangle| \leqslant |\mathbf{f}_{ij}^{01}||\mathbf{f}_{ij}^{10}|$. In both forms, $\neq_4$ is realizable since $\lambda_{ij} \neq 0$. Thus, $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$.

2. For all pairs $\{i,j\}$, $\widehat{\mathfrak{m}}_{ij}f$ has support size 4. By Lemma 4.9,

   - Either $M(\widehat{\mathfrak{m}}_{ij}f)$ has the form $\lambda_{ij}\left[\begin{smallmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{smallmatrix}\right]$ where $\lambda_{ij} = |\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ij}^{11}|^2 = |\mathbf{f}_{ij}^{01}|^2 = |\mathbf{f}_{ij}^{10}|^2 \neq 0$,
   - *or* $M(\widehat{\mathfrak{m}}_{ij}f)$ has the form $\left[\begin{smallmatrix} 0&0&0&0\\0&\langle \mathbf{f}_{ij}^{01},\mathbf{f}_{ij}^{10}\rangle&|\mathbf{f}_{ij}^{01}|^2&0\\0&|\mathbf{f}_{ij}^{10}|^2&\langle \mathbf{f}_{ij}^{10},\mathbf{f}_{ij}^{01}\rangle&0\\0&0&0&0 \end{smallmatrix}\right]$, where $|\langle \mathbf{f}_{ij}^{01}, \mathbf{f}_{ij}^{10} \rangle|^2 = |\mathbf{f}_{ij}^{01}|^2|\mathbf{f}_{ij}^{10}|^2 \neq 0$.

   Again, the form that $\langle \mathbf{f}_{ij}^{01}, \mathbf{f}_{ij}^{10} \rangle \neq 0$ while $|\mathbf{f}_{ij}^{01}|^2 = 0$ cannot occur. In the first form, four vectors form a set of mutually *orthogonal* vectors of nonzero equal norm. In the second form, by Cauchy-Schwarz, it means that $\mathbf{f}_{ij}^{01} = c\mathbf{f}_{ij}^{10}$ for some $c \in \mathbb{C}$. In addition, we know $|c| = 1$ due to $|\mathbf{f}_{ij}^{01}| = |\mathbf{f}_{ij}^{10}|$ by ARS. Since $|\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ij}^{11}|^2 = 0$, we have $\mathbf{f}_{ij}^{00} = \mathbf{f}_{ij}^{11} = \mathbf{0}$, the all-zero vector. Thus, f is factorizable as a tensor product $f = b(x_i, x_j) \otimes g$, for some g and some binary signature $b(x_i, x_j) = (0, a, \overline{a}, 0)$, a contradiction because f is irreducible.

Thus, in this case, $M(\widehat{\mathfrak{m}}_{ij} f) = \lambda_{ij} N_4$ for all pairs $\{i, j\}$. By Lemma 3.22, f satisfies 2nd-Orth.

We are done with the proof. □

By Lemma 4.10, we have two main cases depending on whether $\neq_4$ can be realized by $\widehat{\mathfrak{m}}_{ij} f$ from $\mathcal{F}$. We give a proof outline to show how they will be handled. We use $\mathcal{E}$ to denote the set of binary EO signatures satisfying ars. Then, $\mathcal{E}^{\otimes} = \bigcup_{k=1}^{\infty} \{\lambda \bigotimes_{i=1}^{k} f_i \mid \lambda \in \mathbb{R}\backslash\{0\}, f_i \in \mathcal{E}\}$ is the set of tensor products of binary EO signatures satisfying ars. Note that $\mathcal{E}$ includes the binary zero signature, and hence $\mathcal{E}^{\otimes}$ includes all zero signatures of even arity. We use $\mathcal{E}_{\not\equiv 0}$ to denote $\{f \in \mathcal{E} \mid f \not\equiv 0\}$, and then $\mathcal{E}^{\otimes}_{\not\equiv 0} = \{f \in \mathcal{E}^{\otimes} \mid f \not\equiv 0\}$. By Lemma 2.6, we have $\mathcal{E}^{\otimes} \subseteq \mathscr{P}$.

1. The signature $\neq_4$ cannot be realized by $\widehat{\mathfrak{m}}_{ij} f$ from $\mathcal{F}$. That is, every irreducible signature (or factor of signatures) in $\mathcal{F}$ satisfies 2nd-Orth.

   We show that this case happens only if $\mathcal{F} \subseteq \mathcal{E}^{\otimes}$ (Theorem 4.22). We want to prove this by induction. The general strategy is to start with any signature $f \in \mathcal{F}$ of arity $2n$ that is *not* in $\mathcal{E}^{\otimes}$, we realize a signature g of arity $2n-2$ that is also *not* in $\mathcal{E}^{\otimes}$, i.e. $\#\mathrm{EO}(\{g\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$ (Lemma 4.20). If we can reduce the arity down to 4 (this is by a sequence of reductions that is constant in length independent of the problem instance size of the graph), then we can show it is impossible for such a signature to satisfy 2nd-Orth. Thus, we can use it to realize $\neq_4$ or a #P-hard signature by Lemma 4.10. However, our induction proof only works when the arity $2n \geqslant 10$ (there is an intrinsic reason for this.) Therefore we must establish the base cases at arity $4, 6$ and 8. Fortunately, using 2nd-Orth, we can prove our theorem for signatures of arity $4, 6$ and 8 separately (Lemma 4.21).

   For the induction proof, we realize signatures of lower arity by merging (using $\neq_2$) to. It naturally reduces the arity by two. Given a signature $f \notin \mathcal{E}^{\otimes}$ of arity $2n \geqslant 10$, if $\widehat{\partial}_{ij} f \notin \mathcal{E}^{\otimes}$ for some $\{i, j\}$, then we are done. So we may assume for every $\{i, j\}$, $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$. we further inquire whether for every $\{i, j\}$, $\widehat{\partial}_{ij} f \not\equiv 0$. If for some $\{i, j\}$, $\widehat{\partial}_{ij} f \equiv 0$, then it turns out to be relatively easy to handle (Lemma 4.11). So we may assume for every $\{i, j\}$, $\widehat{\partial}_{ij} f \not\equiv 0$. We aim to show that there is a binary signature $b(x_u, x_v)$ such that $b(x_u, x_v) \mid f$. If so, the "quotient" gives us a signature not in $\mathcal{E}^{\otimes}$, but of arity $2n-2$, by Lemma 4.4. In some cases we have to replace f by another f' to accomplish that.

Assuming $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ for all $\{i,j\}$, we prove there is a $b(x_u,x_v)$ such that $b(x_u,x_v) \mid f$ or $b(x_u,x_v) \mid f'$ in the following steps:

(a) If there is a binary signature $b(x_u,x_v)$ such that $b(x_u,x_v) \mid \widehat{\partial}_{ij} f$ for every $\{i,j\}$ disjoint with $\{u,v\}$, then $b(x_u,x_v) \mid f$ (Lemma 4.12).

(b) We have assumed $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ for all $\{i,j\}$. Suppose there is one $\widehat{\partial}_{uv} f \equiv 0$. We show that the binary signature $b^{\mathfrak{i}}(x_u,x_v) = (0,\mathfrak{i},-\mathfrak{i},0)$ divides $\widehat{\partial}_{ij} f$ for every $\{i,j\}$ disjoint with $\{u,v\}$ (Lemma 4.13).

(c) Now, we further assume $\widehat{\partial}_{ij} f \not\equiv 0$ for all $\{i,j\}$. We want to show that if a binary signature $b(x_u,x_v)$ divides a "triangle", i.e. $b(x_u,x_v) \mid \widehat{\partial}_{rs} f, \widehat{\partial}_{st} f, \widehat{\partial}_{rt} f$ (we say f satisfies the Δ-property), it divides $\widehat{\partial}_{ij} f$ for every $\{i,j\}$ disjoint with $\{u,v\}$ (Lemma 4.15). To prove this, we need the following delicate lemma.

(d) If a binary signature $b(x_u,x_v)$ divides "two pairs", i.e. $b(x_u,x_v) \mid \widehat{\partial}_{st} f, \widehat{\partial}_{s't'} f$, where $\{s,t\}$ and $\{s',t'\}$ are distinct but not necessarily disjoint, then it divides $\widehat{\partial}_{ij} f$ for any $\{i,j\}$ which is disjoint with $\{u,v\} \cup \{s,t\} \cup \{s',t'\}$ that satisfies $\widehat{\partial}_{(st)(ij)} f \not\equiv 0$ and $\widehat{\partial}_{(s't')(ij)} f \not\equiv 0$ (Lemma 4.14).

(e) Finally, we show that either (i) f satisfies the Δ-property, or (ii) we can realize a signature f', where $f' \notin \mathcal{E}^{\otimes}$ has the same arity as f, such that either $\widehat{\partial}_{ij} f \notin \mathcal{E}^{\otimes}$ for some $\{i,j\}$, or f' satisfies the Δ-property. (Lemma 4.17).

These steps will accomplish the arity reduction inductive step.

This case is handled in Section 4.3. We will see that the unique prime factorization plays an important role in the proof.

2. Otherwise, we have $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_{\mathrm{T}} \#\mathrm{EO}(\mathcal{F})$.

The signature $\neq_4$ can be used to realize any $(\neq_{2k}) \in \mathcal{DEQ}$ (Lemma 4.23), and then the problem $\#\mathrm{EO}(\mathcal{DEQ} \cup \mathcal{F})$ can be expressed as $\operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ (Lemma 4.24). The next idea is to simulate $\#\mathrm{CSP}(\mathcal{G}) \equiv_T \operatorname{Holant}(\mathcal{EQ} \mid \mathcal{G})$ using $\operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ for some $\mathcal{G}$ closely related to $\mathcal{F}$, and we can apply the dichotomy of #CSP (Theorem 2.12) to get hardness results. The challenge is to simulate $\mathcal{EQ}$ using $\mathcal{DEQ}$ and $\mathcal{F}$. After some reflection one can observe that it is *impossible* to realize $\mathcal{EQ}$ by direct gadget constructions. Since signatures in $\mathcal{DEQ}$ and $\mathcal{F}$ are EO signatures satisfying ARS, by Lemma 4.5 any gadget realizable from them is also an EO signature. But clearly, any $(=_k) \in \mathcal{EQ}$ is not an EO signature. However we found an alternative way to simulate $\mathcal{EQ}$ globally, and this is achieved depending crucially on some special properties of $\mathcal{F}$, as follows:

(a) First, using ARS we show that $\#\mathrm{CSP}(|\mathcal{F}|^2) \leqslant_T \mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ (Lemma 4.26), where $|\mathcal{F}|^2$ denotes the set of signatures by taking norm squares of signatures in $\mathcal{F}$, namely $|\mathcal{F}|^2 = \{|f|^2 \mid f \in \mathcal{F}\}$. This directly implies that $\mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ is #P-hard unless every signature in $\mathcal{F}$ has affine support (Corollary 4.27).

(b) Then, consider an EO signature with affine support. We show its support has a special structure called *pairwise opposite* (Definition 4.28 and Lemma 4.30).

(c) Finally, given the support of every signature $f \in \mathcal{F}$ is pairwise opposite, we show $\#\mathrm{CSP}(\mathcal{F}) \leqslant_T \mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ (Lemma 4.31) by a global simulation, and hence the problem $\mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$ (Corollary 4.32).

It follows that, in this case, we have $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F})$ is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$ (Theorem 4.33). This case is handled in Section 4.4. We will introduce the pairwise opposite structure and show the global reductions from #CSP to #EO problems.

As observed earlier $\mathscr{E}^{\otimes} \subseteq \mathscr{P}$. If $\mathcal{F} \subseteq \mathscr{E}^{\otimes}$, then by Lemma 2.25 and Theorem 2.30 $\#\mathrm{EO}(\mathcal{F})$ is tractable. In Section 4.3, we show that if $\mathcal{F} \nsubseteq \mathscr{E}^{\otimes}$ then either $\#\mathrm{EO}(\mathcal{F})$ is #P-hard, or we have $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$. In Section 4.4, we show that $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F})$ is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$, or $\mathcal{F} \subseteq \mathscr{P}$. This completes the proof of Theorem 4.1.

4.3 Interplay of Unique Prime Factorization and Merging Gadgets

In this section, we show that if $\mathcal{F} \nsubseteq \mathscr{E}^{\otimes}$ then either $\#\mathrm{EO}(\mathcal{F})$ is #P-hard or we can realize $\neq_4$, i.e., $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$, and then the results from Section 4.4 take over. Suppose $\mathcal{F} \nsubseteq \mathscr{E}^{\otimes}$, then it contains some signature $f \notin \mathscr{E}^{\otimes}$, and we prove the statement by induction on the arity of f. The general strategy is that we start with any signature f of arity $2n \geqslant 10$ that is *not* in $\mathscr{E}^{\otimes}$, and realize a signature g of arity $2n-2$ that is also *not* in $\mathscr{E}^{\otimes}$. However, this induction only works for arity $2n \geqslant 10$. We prove the base cases of the induction separately, when f has arity 4, 6 or 8.

For the inductive step, we consider $\widehat{\partial}_{ij} f$ for all $\{i,j\}$. If there exists $\{i,j\}$ such that $\widehat{\partial}_{ij} f \notin \mathcal{E}^{\otimes}$, then we can realize $g = \widehat{\partial}_{ij} f$ which has arity $2n-2$, and we are done. Thus, we assume $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ for all $\{i,j\}$. We denote this property by $f \in \widehat{\int}\mathcal{E}^{\otimes}$. Under the assumption that $f \in \widehat{\int}\mathcal{E}^{\otimes}$, our goal is to show that there is a binary signature $b(x_u, x_v)$ such that either $b(x_u, x_v) \mid f$ or there exists another $f' \notin \mathcal{E}^{\otimes}$ realizable from f, such that f' has the same arity as f, and $b(x_u, x_v) \mid f'$. In the second case we may again assume $f' \in \widehat{\int}\mathcal{E}^{\otimes}$, for otherwise we may take $\widehat{\partial}_{ij} f'$ for some $\{i,j\}$. Now we may replace f by f' in the second case. From the factorization $f = b(x_u, x_v) \otimes g$, it follows from the definition of $\mathcal{E}^{\otimes}$ that $g \notin \mathcal{E}^{\otimes}$ since $f \notin \mathcal{E}^{\otimes}$. From the factorization of f, we can realize g from f by Lemma 4.4, and we are done. We carry out our induction proof in the next six lemmas.

For convenience, we use the following notations.

- $\mathcal{E}^{\otimes} = \{$tensor products of one or more binary EO signatures satisfying ARS$\}$.
- $f \in \widehat{\int}\mathcal{E}^{\otimes}$ denotes the property that $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ for all $\{i,j\}$.
- $f \in \widehat{\int}\mathcal{E}^{\otimes}_{\not\equiv 0}$ denotes the property that $\widehat{\partial}_{ij} f \in \mathcal{B}$ and $\widehat{\partial}_{ij} f \not\equiv 0$ for all $\{i,j\}$.
- We say f satisfies the Δ-property, if there exist three distinct indices $\{r,s,t\}$ and a binary signature $b(x_u, x_v)$ such that $\{u,v\} \cap \{r,s,t\} = \emptyset$, and $b(x_u, x_v) \mid \widehat{\partial}_{rs} f, \widehat{\partial}_{st} f, \widehat{\partial}_{rt} f$.

Lemma 4.11. *Suppose $f \in \mathcal{E}^{\otimes}$. Then $\widehat{\partial}_{ij} f \equiv 0$ iff the signature $b^{\mathfrak{i}}(x_i, x_j) = (0, \mathfrak{i}, -\mathfrak{i}, 0)$ divides f.*

证明. If $b^{\mathfrak{i}}(x_i, x_j) | f$, then $f = b^{\mathfrak{i}}(x_i, x_j) \otimes g$, where g is a constant or a signature on variables other than x_i, x_j. We have $\widehat{\partial}_{ij} f = (\mathfrak{i} - \mathfrak{i}) \cdot g \equiv 0$.

Now, suppose $\widehat{\partial}_{ij} f \equiv 0$. If $f \equiv 0$, then it is trivial. Otherwise, $f \not\equiv 0$. Consider the unique prime factorization of f. If x_i and x_j appear in one binary signature $b(x_i, x_j) = (0, a, \bar{a}, 0)$, then $a \neq 0$, and $f = b(x_i, x_j) \otimes g$, where g is a constant or a signature on variables other than x_i, x_j and $g \not\equiv 0$ due to $f \not\equiv 0$. Then, we have $\widehat{\partial}_{ij} f = (a + \bar{a}) g \equiv 0$, which means $a + \bar{a} = 0$. That is, $a = \lambda \mathfrak{i}$ for some $\lambda \in \mathbb{R}$. So, we have $b^{\mathfrak{i}}(x_i, x_j) | f$.

Otherwise, x_i and x_j appear in separate binary signatures $b_1(x_i, x_{i'}) = (0, a, \bar{a}, 0)$ and $b_2(x_j, x_{j'}) = (0, b, \bar{b}, 0)$ in the unique prime factorization of f. That is, $f = b_1(x_i, x_{i'}) \otimes b_2(x_j, x_{j'}) \otimes g$, where g is a constant or a signature on variables other than $x_i, x_{i'}, x_j, x_{j'}$ and $g \not\equiv 0$. Then $\widehat{\partial}_{ij} f = b'(x_{i'}, x_{j'}) \otimes g$ where $b'(x_{i'}, x_{j'}) = (0, \bar{a}b, a\bar{b}, 0) \not\equiv 0$. Hence, $\widehat{\partial}_{ij} f \not\equiv 0$. A contradiction. □

Lemma 4.12. *Let $f \in \widehat{\int}\mathcal{E}^{\otimes}$ be a signature of arity $2n \geqslant 6$. If there exists a binary signature $b(x_u, x_v)$ such that $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$ for all $\{i, j\}$ disjoint with $\{u, v\}$, then $b(x_u, x_v) \mid f$.*

证明. Recall that f_{uv}^{bc} denotes the signature obtained by setting variables (x_u, x_v) of f to $(b, c) \in \{0, 1\}^2$. These are called the pinning operations on $\{u, v\}$. Clearly, for any $\{i, j\}$ disjoint with $\{u, v\}$, the pinning operations on $\{u, v\}$ commute with the merging operation $\widehat{\partial}_{ij}$, and so we have $(\widehat{\partial}_{ij} f)_{uv}^{bc} = \widehat{\partial}_{ij}(f_{uv}^{bc})$.

We may assume the binary signature has the form $b(x_u, x_v) = (0, a, \bar{a}, 0)$, where $a \neq 0$. Consider the signature $f' := \bar{a} f_{uv}^{01} - a f_{uv}^{10}$. It is a signature on variables of f other than x_u and x_v. For any $\{i, j\}$ disjoint with $\{u, v\}$, by merging variables x_i and x_j of f', and recalling that $\widehat{\partial}_{ij}$ is a linear operator, we have

$$\widehat{\partial}_{ij} f' = \widehat{\partial}_{ij}(\bar{a} f_{uv}^{01} - a f_{uv}^{10}) = \bar{a}\widehat{\partial}_{ij}(f_{uv}^{01}) - a\widehat{\partial}_{ij}(f_{uv}^{10}) = \bar{a}(\widehat{\partial}_{ij} f)_{uv}^{01} - a(\widehat{\partial}_{ij} f)_{uv}^{10}.$$

By assumption, $\widehat{\partial}_{ij} f = b(x_u, x_v) \otimes g$, where g is a signature on variables other than x_u, x_v, x_i, x_j. (Since $\widehat{\partial}_{ij} f$ has arity at least 4, g is not a constant.) Then we have

$$\widehat{\partial}_{ij} f' = \bar{a}(\widehat{\partial}_{ij} f)_{uv}^{01} - a(\widehat{\partial}_{ij} f)_{uv}^{10} = \bar{a}(ag) - a(\bar{a}g) \equiv 0.$$

Note that f' is also an EO signature. By Lemma 3.9, we have $f' \equiv 0$, and hence $\bar{a} f_{uv}^{01} \equiv a f_{uv}^{10}$. Moreover, by the factorization of $\widehat{\partial}_{ij} f$, we have $\widehat{\partial}_{ij}(f_{uv}^{00}) = (\widehat{\partial}_{ij} f)_{uv}^{00} \equiv 0$ and $\widehat{\partial}_{ij}(f_{uv}^{11}) = (\widehat{\partial}_{ij} f)_{uv}^{11} \equiv 0$ for any $\{i, j\}$ disjoint with $\{u, v\}$. Also, since $2n \geqslant 6$, $f_{uv}^{00}(\alpha) = f_{uv}^{11}(\alpha) = 0$ when $\mathrm{wt}(\alpha) = 0$ or $2n-2$. By Lemma 3.9 again, we have $f_{uv}^{00} = f_{uv}^{11} \equiv 0$. Hence, $f = (f_{uv}^{00}, f_{uv}^{01}, f_{uv}^{10}, f_{uv}^{11}) = (0, a, \bar{a}, 0) \otimes (\frac{1}{a} f_{uv}^{01})$, and we have $b(x_u, x_v) \mid f$. □

Notice that for arity $2n \geqslant 6$, if $b(x_u, x_v) \mid f$ and thus $f = b(x_u, x_v) \otimes g$, then by the definition of $\mathcal{E}^{\otimes}$, from $f \notin \mathcal{E}^{\otimes}$ we obtain $g \notin \mathcal{E}^{\otimes}$, which has arity $2n - 2$, completing the induction step using Lemma 4.4. Therefore, to apply Lemma 4.12 we want to show that there is a binary signature $b(x_u, x_v)$ such that $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$ for every $\{i, j\}$ disjoint with $\{u, v\}$. We first consider the case that $\widehat{\partial}_{uv} f \equiv 0$ for some $\{u, v\}$.

Lemma 4.13. *Suppose f has arity $\geqslant 4$ and $f \in \int \mathcal{E}^{\otimes}$. If $\widehat{\partial}_{uv} f \equiv 0$ for some $\{u,v\}$, then the binary signature $b^{\mathfrak{i}}(x_u,x_v)=(0,\mathfrak{i},-\mathfrak{i},0)$ satisfies $b^{\mathfrak{i}}(x_u,x_v) \mid \widehat{\partial}_{ij} f$ for all $\{i,j\}$ disjoint with $\{u,v\}$.*

证明. For any $\{i,j\}$ disjoint with $\{u,v\}$, the operations $\widehat{\partial}_{ij}$ and $\widehat{\partial}_{uv}$ commute. Since $\widehat{\partial}_{uv} f \equiv 0$, we have

$$\widehat{\partial}_{uv}(\widehat{\partial}_{ij} f) = \widehat{\partial}_{ij}(\widehat{\partial}_{uv} f) \equiv 0.$$

Since $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$, by Lemma 4.11, we have $b^{\mathfrak{i}}(x_u,x_v) \mid \widehat{\partial}_{ij} f$. □

In the following, for convenience we denote $\widehat{\partial}_{ij}(\widehat{\partial}_{uv} f)$ by $\widehat{\partial}_{(ij)(uv)} f$.

Now, we assume $\widehat{\partial}_{ij} f \in \mathcal{B}$ and $\widehat{\partial}_{ij} f \not\equiv 0$ for all $\{i,j\}$. We denote this property by $f \in \int \mathcal{E}^{\otimes}_{\not\equiv 0}$. Each $\widehat{\partial}_{ij} f$ has a unique prime factorization. We will show that once we can find some binary signature $b(x_u,x_v)$ that divides a "triangle", i.e. $b(x_u,x_v) | \widehat{\partial}_{rs} f, \widehat{\partial}_{st} f, \widehat{\partial}_{rt} f$ for three distinct $\{r,s,t\}$ disjoint with $\{u,v\}$, then it divides $\widehat{\partial}_{ij} f$ for all $\{i,j\}$ disjoint with $\{u,v\}$. We first consider the case that $b(x_u,x_v)$ divides "two pairs". The statement of the following lemma is delicate.

Lemma 4.14. *Let f be a signature of arity $2n \geqslant 8$ and $f \in \int \mathcal{E}^{\otimes}_{\not\equiv 0}$. Suppose there exist two pairs of indices $\{s,t\}$ and $\{s',t'\}$ that are distinct but not necessarily disjoint, and a binary signature $b(x_u,x_v)$, where $\{u,v\} \cap (\{s,t\} \cup \{s',t'\}) = \emptyset$, such that $b(x_u,x_v) \mid \widehat{\partial}_{st} f, \widehat{\partial}_{s't'} f$. Then for any $\{i,j\}$ disjoint with $\{u,v\} \cup \{s,t\} \cup \{s',t'\}$, if $\widehat{\partial}_{(st)(ij)} f \not\equiv 0$ and $\widehat{\partial}_{(s't')(ij)} f \not\equiv 0$, then $b(x_u,x_v) \mid \widehat{\partial}_{ij} f$.*

证明. By hypothesis $f \in \int \mathcal{E}^{\otimes}_{\not\equiv 0}$, so for any $\{i,j\}$, we have $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ and is nonzero, and thus it has a unique factorization with binary prime factors. Let $\{i,j\}$ be disjoint with $\{u,v\} \cup \{s,t\} \cup \{s',t'\}$. Suppose it satisfies the condition $\widehat{\partial}_{(st)(ij)} f \not\equiv 0$ and $\widehat{\partial}_{(s't')(ij)} f \not\equiv 0$. We first prove that x_u and x_v must appear in one single binary prime factor $b'(x_u,x_v)$ in the factorization of $\widehat{\partial}_{ij} f$. That is,

$$\widehat{\partial}_{ij} f = b'(x_u,x_v) \otimes g, \tag{4.2}$$

where $g \not\equiv 0$ is a signature on variables other than x_u, x_v, x_i, x_j. For a contradiction, suppose variables x_u and x_v appear in two distinct binary prime factors $b_1(x_u,x_{u'})$ and $b_2(x_v,x_{v'})$ in the prime factorization of $\widehat{\partial}_{ij} f$. Then,

$$\widehat{\partial}_{ij} f = b_1(x_u,x_{u'}) \otimes b_2(x_v,x_{v'}) \otimes g', \tag{4.3}$$

where $g' \not\equiv 0$ is a signature on variables other than $x_u, x_{u'}, x_v, x_{v'}, x_i, x_j$. By hypothesis, $b(x_u, x_v) \mid \widehat{\partial}_{st} f$, thus $\widehat{\partial}_{st} f = b(x_u, x_v) \otimes h$ for some h on variables other than x_u, x_v, x_s, x_t, which certainly include x_i, x_j. Thus $\widehat{\partial}_{(ij)(st)} f = b(x_u, x_v) \otimes \widehat{\partial}_{ij} h$, and we have $b(x_u, x_v) | \widehat{\partial}_{(ij)(st)} f = \widehat{\partial}_{(st)(ij)} f$. By hypothesis for this $\{i, j\}$ we have $\widehat{\partial}_{(st)(ij)} f \not\equiv 0$. This implies that after merging variables x_s and x_t of $\widehat{\partial}_{ij} f$, x_u and x_v form a nonzero binary signature. By the form (4.3) of $\widehat{\partial}_{ij} f$, the only way x_u and x_v can form a nonzero binary signature in $\widehat{\partial}_{(st)(ij)} f$ is that the merge operation is actually merging $x_{u'}$ and $x_{v'}$. We conclude that $\{s, t\} = \{u', v'\}$. We can repeat the same proof replacing $\{s', t'\}$ for $\{s, t\}$, and since $b(x_u, x_v) \mid \widehat{\partial}_{(s't')(ij)} f$ and $\widehat{\partial}_{(s't')(ij)} f \not\equiv 0$, we have $\{s', t'\} = \{u', v'\}$. Hence, we have $\{s, t\} = \{s', t'\}$. This is a contradiction, and (4.3) does not hold.

Thus (4.2) holds. Since $\{s, t\}$ is disjoint with $\{u, v, i, j\}$, by the form (4.2) of $\widehat{\partial}_{ij} f$, when merging variables x_s and x_t of $\widehat{\partial}_{ij} f$, we actually merge variables x_s and x_t of g and the binary signature $b'(x_u, x_v)$ is not affected. Thus,

$$\widehat{\partial}_{(st)(ij)} f = b'(x_u, x_v) \otimes \widehat{\partial}_{st} g.$$

That is, $b'(x_u, x_v) \mid \widehat{\partial}_{(st)(ij)} f$. By hypothesis we also have $b(x_u, x_v) \mid \widehat{\partial}_{st} f$. By the fact that $\{i, j\}$ is disjoint with $\{u, v, s, t\}$, we have $b(x_u, x_v) \mid \widehat{\partial}_{(ij)(st)} f = \widehat{\partial}_{(st)(ij)} f$. Thus $b(x_u, x_v)$ and $b'(x_u, x_v)$ both divide $\widehat{\partial}_{(st)(ij)} f \not\equiv 0$. By the unique factorization lemma (Lemma 3.4), we have $b(x_u, x_v) = \lambda b'(x_u, x_v)$ for some $\lambda \neq 0$. In particular, by (4.2), $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$. □

Now we come to the pivotal "triangle" lemma. Recall that the Δ-property was defined just before Lemma 4.12. Suppose f satisfies the Δ-property, i.e., there is a binary $b(x_u, x_v)$ that divides a "triangle", $b(x_u, x_v) \mid \widehat{\partial}_{rs} f, \widehat{\partial}_{st} f, \widehat{\partial}_{rt} f$. A key step in the proof of Lemma 4.15 is to show that for any $\{i, j\}$ disjoint with $\{u, v, r, s, t\}$, among the three iterated "derivatives" $\widehat{\partial}_{(rs)(ij)} f, \widehat{\partial}_{(st)(ij)} f$ and $\widehat{\partial}_{(rt)(ij)} f$, at most one of them can be identically zero. Then Lemma 4.14 applies.

Lemma 4.15. *Let $f \in \widehat{\int}\mathcal{E}^{\otimes}_{\not\equiv 0}$ have arity $2n \geqslant 10$. Suppose f satisfies the Δ-property. Then there is a binary signature $b(x_u, x_v)$ such that for any $\{i, j\}$ disjoint with $\{u, v\}$, we have $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$.*

证明. By the Δ-property, there is a binary signature $b(x_u, x_v)$ and $\{r, s, t\}$ disjoint with $\{u, v\}$ such that $b(x_u, x_v) \mid \widehat{\partial}_{rs} f, \widehat{\partial}_{st} f, \widehat{\partial}_{rt} f$. For any $\{i, j\}$ disjoint with $\{u, v\}$, we first consider the case that $\{i, j\}$ is also disjoint with $\{r, s, t\}$. Our idea is to show that among $\widehat{\partial}_{(rs)(ij)} f, \widehat{\partial}_{(st)(ij)} f$ and $\widehat{\partial}_{(rt)(ij)} f$, at most one of them can be a zero signature. This implies that there are two among these that are not identically zero. Then by Lemma 4.14, we have $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$.

By Lemma 4.11, $\widehat{\partial}_{(rs)(ij)} f \equiv 0$ iff the binary signature $b^{\mathfrak{i}}(x_r, x_s) = (0, \mathfrak{i}, -\mathfrak{i}, 0)$ divides $\widehat{\partial}_{ij} f$. Similarly, $\widehat{\partial}_{(st)(ij)} f \equiv 0$ iff $b^{\mathfrak{i}}(x_s, x_t) \mid \widehat{\partial}_{ij} f$, and $\widehat{\partial}_{(rt)(ij)} f \equiv 0$ iff $b^{\mathfrak{i}}(x_r, x_t) \mid \widehat{\partial}_{ij} f$. By hypothesis, $f \in \widehat{\int} \mathcal{E}^{\otimes}_{\not\equiv 0}$, so $\widehat{\partial}_{ij} f \not\equiv 0$. The signature $\widehat{\partial}_{ij} f \in \mathcal{E}^{\otimes}$ has a unique prime factorization. By Lemma 3.4, since the three signatures $b^{\mathfrak{i}}(x_r, x_s), b^{\mathfrak{i}}(x_s, x_t)$ and $b^{\mathfrak{i}}(x_r, x_t)$ are on pairwise overlapping sets of variables, at most one of them can be a tensor factor of $\widehat{\partial}_{ij} f$. Thus, among $\widehat{\partial}_{(rs)(ij)} f, \widehat{\partial}_{(st)(ij)} f$ and $\widehat{\partial}_{(rt)(ij)} f$, at most one of them can be a zero signature, which implies $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$, by Lemma 4.14, for all $\{i, j\}$ disjoint with $\{u, v, r, s, t\}$.

Now suppose $\{i, j\}$ is disjoint with $\{u, v\}$, but not disjoint with $\{r, s, t\}$. In the union $\{i, j\} \cup \{r, s, t\} \cup \{u, v\}$, there are at most 6 distinct indices. Since the arity of f is at least 10, there are three indices $\{r', s', t'\}$ such that $\{r', s', t'\}$ is disjoint with $\{i, j\} \cup \{r, s, t\} \cup \{u, v\}$. Since $\{r', s'\}$ is disjoint with $\{u, v, r, s, t\}$, we can replace $\{i, j\}$ by $\{r', s'\}$ in the proof above for the case when $\{i, j\}$ is disjoint with $\{u, v, r, s, t\}$, and derive $b(x_u, x_v) \mid \widehat{\partial}_{(r's')} f$. By the same reason, we also have $b(x_u, x_v) \mid \widehat{\partial}_{s't'} f$, and $b(x_u, x_v) \mid \widehat{\partial}_{(r't')} f$. In other words we found a new "triangle", that is, f satisfies the Δ-property with the binary signature $b(x_u, x_v)$ and the triple $\{r', s', t'\}$ replacing $\{r, s, t\}$. Note that now $\{i, j\}$ is disjoint with $\{r', s', t'\}$. So, we can apply the proof above with $\{r, s, t\}$ now replaced by $\{r', s', t'\}$, and we conclude that $b(x_u, x_v) \mid \widehat{\partial}_{ij} f$. □

Remark 4.16. *This is the first place we require the arity of f to be at least* 10*.*

We go for the kill in the next lemma.

Lemma 4.17. *Let $f \in \mathcal{F}$ be a signature of arity $2n \geqslant 10$, $f \notin \mathcal{E}^{\otimes}$ and $f \in \widehat{\int} \mathcal{E}^{\otimes}_{\not\equiv 0}$. Then*

- *either f satisfies the Δ-property;*
- *or there is a signature $f' \notin \mathcal{E}^{\otimes}$ that has the same arity as f, such that $\#\mathrm{EO}(f' \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$, and the following hold: either (1) $f' \notin \widehat{\int} \mathcal{E}^{\otimes}$ or (2) f' satisfies the Δ-property.*

证明. Consider $\widehat{\partial}_{(12)} f$. Since $\widehat{\partial}_{(12)} f \in \mathcal{E}^{\otimes}$ and $\widehat{\partial}_{(12)} f \not\equiv 0$, without loss of generality, we may assume in the unique prime factorization of $\widehat{\partial}_{(12)} f$, variables x_3 and x_4 appear in one binary prime factor,

x_5 and x_6 appear in one binary prime factor, and so on. That is,

$$\widehat{\partial}_{(12)}f = b_1(x_3,x_4) \otimes b_2(x_5,x_6) \otimes b_3(x_7,x_8) \otimes b_4(x_9,x_{10}) \otimes \ldots \otimes b_{n-1}(x_{2n-1},x_{2n}). \tag{4.4}$$

Case 1. For all $1 \leqslant k \leqslant n-1$, $b_k(x_{2k+1},x_{2k+2}) \neq$ a scalar multiple of $(0,\mathfrak{i},-\mathfrak{i},0)$.

Then by Lemma 4.11, $\widehat{\partial}_{(34)(12)}f \not\equiv 0$, and clearly, $b_k(x_{2k+1},x_{2k+2}) | \widehat{\partial}_{(34)(12)}f$ for $k \geqslant 2$. In particular, we have

$$b_2(x_5,x_6), b_3(x_7,x_8), b_4(x_9,x_{10}) | \widehat{\partial}_{(34)(12)}f,$$

since f has arity at least 10.

Now consider $\widehat{\partial}_{(34)}f$. We have $\widehat{\partial}_{(34)}f \in \mathcal{E}^{\otimes}$, $\widehat{\partial}_{(34)}f \not\equiv 0$, and $\widehat{\partial}_{(12)(34)}f = \widehat{\partial}_{(34)(12)}f \not\equiv 0$.

- If x_1 and x_2 appear in one binary prime factor $b'_1(x_1,x_2)$ in the unique prime factorization of $\widehat{\partial}_{(34)}f$, then after merging variables x_1 and x_2, the binary signature $b'_1(x_1,x_2)$ becomes a nonzero constant, but all other binary prime factors of $\widehat{\partial}_{(34)}f$ are unchanged and appear in the prime factorization of $\widehat{\partial}_{(12)(34)}f$. By commutativity $\widehat{\partial}_{(12)(34)}f = \widehat{\partial}_{(34)(12)}f$, and by (4.4) the prime factors of $\widehat{\partial}_{(12)(34)}f$ are precisely $b_k(x_{2k+1},x_{2k+2})$, for $2 \leqslant k \leqslant n-1$, we conclude that the unique prime factorization of $\widehat{\partial}_{(34)}f$ has the following form (up to a nonzero constant)

$$\widehat{\partial}_{(34)}f = b'_1(x_1,x_2) \otimes b_2(x_5,x_6) \otimes b_3(x_7,x_8) \otimes b_4(x_9,x_{10}) \otimes \ldots \otimes b_{n-1}(x_{2n-1},x_{2n}).$$

- If x_1 and x_2 appear in two distinct binary prime factors $b''_1(x_1,x_i)$ and $b''_2(x_2,x_j)$ in the unique prime factorization of $\widehat{\partial}_{(34)}f$, then after merging variables x_1 and x_2, from (4.4) we have

$$\widehat{\partial}_{(12)(34)}f = \widehat{\partial}_{(34)(12)}f = c \cdot b_2(x_5,x_6) \otimes b_3(x_7,x_8) \otimes b_4(x_9,x_{10}) \otimes \ldots \otimes b_{n-1}(x_{2n-1},x_{2n})$$

for some nonzero constant c. On the other hand, from the form of $\widehat{\partial}_{(34)}f$, the two variables x_i and x_j form a new nonzero binary $b''(x_i,x_j)$. Thus the pair $\{i,j\}$ is either $\{5,6\}$, or $\{7,8\}$, etc. and we may assume $(i,j)=(5,6)$ by renaming the variables. Thus, we have

$$\widehat{\partial}_{(34)} f = b_1''(x_1, x_5) \otimes b_2''(x_2, x_6) \otimes b_3(x_7, x_8) \otimes b_4(x_9, x_{10}) \otimes \ldots \otimes b_{n-1}(x_{2n-1}, x_{2n}).$$

(In the following proof we can use any b_j, for $4 \leqslant j \leqslant n-1$; for definiteness we set $j = 4$, and since $n \geqslant 5$ this choice b_4 is permissible.) In both cases above, we have $b_4(x_9, x_{10}) | \widehat{\partial}_{(34)} f$, and $\widehat{\partial}_{(78)(34)} f \not\equiv 0$ since $b_3(x_7, x_8) \neq (0, \mathfrak{i}, -\mathfrak{i}, 0)$ by assumption. Moreover, note that in both cases, x_6 and x_7 do not appear as the two variables of a single binary signature tensor factor of $\widehat{\partial}_{(34)} f$. The same is true for x_6 and x_8. This implies that $\widehat{\partial}_{(67)(34)} f \not\equiv 0$ and $\widehat{\partial}_{(68)(34)} f \not\equiv 0$. So we have derived

$$b_4(x_9, x_{10}) \mid \widehat{\partial}_{(34)} f, \quad \widehat{\partial}_{(78)(34)} f \not\equiv 0, \quad \widehat{\partial}_{(67)(34)} f \not\equiv 0, \quad \text{and} \quad \widehat{\partial}_{(68)(34)} f \not\equiv 0.$$

Clearly, by (4.4), we also have

$$b_4(x_9, x_{10}) \mid \widehat{\partial}_{(12)} f, \quad \widehat{\partial}_{(78)(12)} f \not\equiv 0, \quad \widehat{\partial}_{(67)(12)} f \not\equiv 0, \quad \text{and} \quad \widehat{\partial}_{(68)(12)} f \not\equiv 0.$$

Apply Lemma 4.14 three times (with $\{u, v\} = \{9, 10\}, \{s, t\} = \{1, 2\}, \{s', t'\} = \{3, 4\}$, and taking $\{i, j\} = \{6, 7\}, \{7, 8\}, \{6, 8\}$ separately), we have

$$b_4(x_9, x_{10}) \mid \widehat{\partial}_{(67)} f, \widehat{\partial}_{(78)} f, \widehat{\partial}_{(68)} f.$$

Thus f satisfies the Δ-property ($\{u, v\} = \{9, 10\}$ and $\{r, s, t\} = \{6, 7, 8\}$) and we are done.

Case 2. There is a binary signature $b_{k-1}(x_{2k-1}, x_{2k})$ in the factorization of $\widehat{\partial}_{(12)} f$ such that $b_{k-1}(x_{2k-1}, x_{2k})$ = a scalar multiple of $(0, \mathfrak{i}, -\mathfrak{i}, 0)$. Then by Lemma 4.4, we have the reduction $\#\text{EO}((0, \mathfrak{i}, -\mathfrak{i}, 0), f) \leqslant_T \#\text{EO}(f)$. Connecting the variable x_{2k-1} of f with $(0, \mathfrak{i}, -\mathfrak{i}, 0)$, we can realize a signature f'. Consider $\widehat{\partial}_{(12)} f'$. Again the operations commute: it is the same as connecting the variable x_{2k-1} of $\widehat{\partial}_{(12)} f$ with $(0, \mathfrak{i}, -\mathfrak{i}, 0)$. Since $\widehat{\partial}_{(12)} f$ is a tensor product of binary signatures, connecting the variable x_{2k-1} of $\widehat{\partial}_{(12)} f$ with $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ is just connecting the variable x_{2k-1} of the binary $b_{k-1}(x_{2k-1}, x_{2k})$ with $(0, \mathfrak{i}, -\mathfrak{i}, 0)$, which gives a binary $(0, 1, 1, 0)$. That is, $\widehat{\partial}_{(12)} f'$ is still a tensor product of the same binary signatures as in $\widehat{\partial}_{(12)} f$ except that

$b_{k-1}(x_{2k-1}, x_{2k}) = (0, \mathfrak{i}, -\mathfrak{i}, 0)$ is replaced by $b'_{k-1}(x_{2k-1}, x_{2k}) = (0, 1, 1, 0)$. Similarly, for any binary signature $b_{\ell-1}(x_{2\ell-1}, x_{2\ell}) = (0, \mathfrak{i}, -\mathfrak{i}, 0)$ in $\widehat{\partial}_{(12)} f$, we modify it in this way (together all at once). Thus, we can realize a signature f' by connecting some variables with $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ such that

$$\widehat{\partial}_{(12)} f' = b'_1(x_3, x_4) \otimes b'_2(x_5, x_6) \otimes b'_3(x_7, x_8) \otimes b'_4(x_9, x_{10}) \otimes \ldots \otimes b'_{n-1}(x_{2n-1}, x_{2n}),$$

where $b'_k(x_{2k+1}, x_{2k+2}) \neq$ a scalar multiple of $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ for any $1 \leqslant k \leqslant n-1$. Moreover, we know $f' \notin \mathcal{E}^{\otimes}$ since $f \notin \mathcal{E}^{\otimes}$; this follows from the closure property of $\mathcal{E}^{\otimes}$ under the operation of connecting a variable by $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ via $\neq_2$, and the fact that if we connect three times $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ via $\neq_2$ in a chain from f', we get f back: $\left(N \left[\begin{smallmatrix} 0 & \mathfrak{i} \\ -\mathfrak{i} & 0 \end{smallmatrix}\right]\right)^4 = I$.

If $f' \notin \widehat{\int}\mathcal{E}^{\otimes}$, we are done. Otherwise, $f' \in \widehat{\int}\mathcal{E}^{\otimes}$. If there is $\{u, v\}$ such that $\widehat{\partial}_{uv} f' \equiv 0$, then by Lemma 4.13, we have $b^{\mathfrak{i}}(x_u, x_v) \mid \widehat{\partial}_{ij} f'$ for any $\{i, j\}$ disjoint with $\{u, v\}$ where $b^{\mathfrak{i}}(x_u, x_v) = (0, \mathfrak{i}, -\mathfrak{i}, 0)$. Then clearly f' satisfies the Δ-property. Otherwise, $f' \in \widehat{\int}\mathcal{E}^{\otimes}{}_{\neq 0}$. As we just proved in Case 1, now replacing f by f', we have $b'_4(x_9, x_{10}) \mid \widehat{\partial}_{(67)} f', \widehat{\partial}_{(78)} f', \widehat{\partial}_{(68)} f'$. This completes the proof.

□

Remark 4.18. *This proof also requires the arity of f to be at least* 10*.*

Let $\mathcal{D} = \{\neq_2\}$. Then $\mathcal{D}^{\otimes} = \{\lambda \cdot (\neq_2)^{\otimes k} \mid \lambda \in \mathbb{R}\backslash\{0\}, k \geqslant 1\}$ is the set of tensor products of $\neq_2$ up to nonzero real scalars. If f satisfies the property that $f \in \widehat{\int}\mathcal{D}^{\otimes}$ (i.e., $\widehat{\partial}_{ij} f \in \mathcal{D}^{\otimes}$) for any pairs of indices $\{i, j\}$, then we can prove the following stronger result.

Lemma 4.19. *Let $\widehat{f}$ be a $2n$-ary* EO *signature satisfying* ARS*.*

- When $2n = 8$, if for all pairs of indices $\{i, j\}$, $\widehat{\partial}_{ij} \widehat{f} \in \mathcal{D}^{\otimes}$, and there exists some $\neq_2 (x_i, x_j)$ and two pairs of indices $\{u, v\}$ and $\{s, t\}$ where $\{u, v\} \cap \{s, t\} \neq \emptyset$ such that $\neq_2 (x_i, x_j) \mid \widehat{\partial}_{uv} \widehat{f}, \widehat{\partial}_{st} \widehat{f}$, then $\widehat{f} \in \mathcal{D}^{\otimes}$ and $\neq_2 (x_i, x_j) \mid \widehat{f}$.

- When $2n \geqslant 10$, if for all pairs of indices $\{i, j\}$, $\widehat{\partial}_{ij} \widehat{f} \in \mathcal{D}^{\otimes}$, then $\widehat{f} \in \mathcal{D}^{\otimes}$.

Lemma 4.20 (Induction)**.** *If $\mathcal{F}$ contains a signature $f \notin \mathcal{E}^{\otimes}$ of arity $2n \geqslant 10$, then there is a signature $g \notin \mathcal{E}^{\otimes}$ of arity $2n - 2$ such that* $\#\mathrm{EO}(\{g\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$*.*

证明. If $f \notin \widehat{\int}\mathcal{E}^{\otimes}$, then there exists $\{i,j\}$ such that $\widehat{\partial}_{ij}f \notin \mathcal{E}^{\otimes}$, and we are done by choosing $g = \widehat{\partial}_{ij}f$. Thus, we assume $f \in \widehat{\int}\mathcal{E}^{\otimes}$. If $\widehat{\partial}_{uv}f \equiv 0$ for some indices $\{u,v\}$, then by Lemmas 4.13 and 4.12, the binary signature $b^{\mathfrak{i}}(x_u,x_v) = (0,\mathfrak{i},-\mathfrak{i},0)$ divides f. That is, $f = b^{\mathfrak{i}}(x_u,x_v) \otimes g$ where g is a signature of arity $2n-2$, and $g \notin \mathcal{E}^{\otimes}$ since $f \notin \mathcal{E}^{\otimes}$. By Lemma 4.4, we have $\#\mathrm{EO}(\{g\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$. So we may assume $f \in \widehat{\int}\mathcal{E}^{\otimes}_{\neq 0}$. Now we apply Lemma 4.17. If the first alternative of Lemma 4.17 holds, then f satisfies the Δ-property. Then by Lemmas 4.15 and 4.12, there is a binary signature $b(x_u,x_v)$ such that $b(x_u,x_v) \mid f$. This divisibility of f produces a signature not in $\mathcal{E}^{\otimes}$ of arity $2n-2$ similar to what we have just proved, and we are done. If the second alternative of Lemma 4.17 holds, then we have a signature $f' \notin \mathcal{E}^{\otimes}$ having the same arity as f. We have $\#\mathrm{EO}(\{f'\}\cup\mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$. If $f' \notin \widehat{\int}\mathcal{E}^{\otimes}$, then there exists $\{i,j\}$ such that $\widehat{\partial}_{ij}f' \notin \mathcal{E}^{\otimes}$, and we can take $\widehat{\partial}_{ij}f'$ as g, and so we are done. Otherwise, by the conclusion of Lemma 4.17, f' satisfies the Δ-property. Similar to the proof above for f, there is a binary signature $b(x_u,x_v)$ such that $b(x_u,x_v) \mid f'$. This divisibility of f' produces a signature not in $\mathcal{E}^{\otimes}$ of arity $2n-2$. This completes the inductive step. □

Now, we use the orthogonality property to prove the base cases.

Lemma 4.21 (Base cases)**.** *If $\mathcal{F}$ contains a signature $f \notin \mathcal{E}^{\otimes}$ of arity* 4, 6 *or* 8*, then either* $\#\mathrm{EO}(\mathcal{F})$ *is* #P-*hard or* $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F}) \leqslant_T \#\mathrm{EO}(\mathcal{F})$.

证明. Again by Lemma 4.4, we may assume f is irreducible. Otherwise, we just need to analyze each irreducible factor of f. More specifically, if $f \notin \mathcal{E}^{\otimes}$ and f is reducible, then there exists an irreducible factor g of f such that $g \notin \mathcal{E}^{\otimes}$, and g has arity 4 or 6. If we can use g to realize a #P-hard signature or $\neq_4$, we can also use f to do so.

By Lemma 4.10, we may assume that f satisfies the orthogonality. Otherwise, we are done.

Therefore, we have

$$|\mathbf{f}_{ij}^{ab}|^2 = \lambda$$

for any $(a,b) \in \{0,1\}^2$, and any pair $\{i,j\}$. This readily leads to a contradiction for signatures of arity 4 as follows. Suppose f is an irreducible signature on four variables x_1,x_2,x_3,x_4. Let (i,j,k,ℓ) be an arbitrary permutation of $\{1,2,3,4\}$. Consider the vector $\mathbf{f}_{ij}^{00}$. It has only one possible nonzero entry $f_{ijk\ell}^{0011}$ since the support of f is on half weight. Thus,

$$|\mathbf{f}_{ij}^{00}|^2 = |f_{ijk\ell}^{0011}|^2 = \lambda$$

for any $(x_i, x_j, x_k, x_\ell) = (0, 0, 1, 1)$. Since (i, j, k, ℓ) is an arbitrary permutation of $\{1, 2, 3, 4\}$, $f_{ijk\ell}^{0011}$ is an arbitrary entry of f at half weight, and since f is nonzero, every weight two entry of f has the same nonzero norm $\sqrt{\lambda}$. However, Consider the vector $\mathbf{f}_{ij}^{01}$, it has two nonzero entries $f_{ijk\ell}^{0101}$ and $f_{ijk\ell}^{0110}$. Hence,

$$\lambda = |\mathbf{f}_{ij}^{01}|^2 = |f_{ijk\ell}^{0101}|^2 + |f_{ijk\ell}^{0110}|^2 = 2\lambda,$$

which means $\lambda = 0$. This is a contradiction.

Before we go into the technical details of the proof for signatures of arity 6 and 8, we first give some intuitions. By considering the norm-squares of entries in f as unknowns, the orthogonality property of f actually gives a linear system. Our proof is to show that when f has small arity $4, 6, 8$, the solution region of such a system only has the trivial zero point. We illustrate this perspective by the arity 4 case. Suppose f has arity 4. It has $\binom{4}{2} = 6$ possible nonzero entries. These entries satisfy the orthogonality condition. We have

$$|\mathbf{f}_{ij}^{00}|^2 - \lambda = 0, \quad |\mathbf{f}_{ij}^{01}|^2 - \lambda = 0, \quad |\mathbf{f}_{ij}^{10}|^2 - \lambda = 0, \quad |\mathbf{f}_{ij}^{11}|^2 - \lambda = 0$$

for any $\{i, j\} \subset \{1, 2, 3, 4\}$. There are $\binom{4}{2} \times 4 = 24$ many equations in total. If we view these norm-squares of entries $|f^{0011}|^2$, $|f^{0101}|^2$, $|f^{0110}|^2$, $|f^{1001}|^2$, $|f^{1010}|^2$, $|f^{1100}|^2$ (we omit subscripts here) and the value λ as variables, those equations are linear equations on these variables. By ARS, we have $|f^{0011}|^2 = |f^{1100}|^2$, $|f^{0101}|^2 = |f^{1010}|^2$, and $|f^{0110}|^2 = |f^{1001}|^2$. So there are only four variables. Our idea is to show that the matrix of this linear system which has 24 many rows but only 4 columns has full rank. We only need 4 rows to prove this. In our proof for arity 4, we picked the following

4 rows and showed that the induced linear system has full rank:

$$\begin{bmatrix}1 & 0 & 0 & -1\\ 0 & 1 & 0 & -1\\ 0 & 0 & 1 & -1\\ 0 & 1 & 1 & -1\end{bmatrix}\begin{bmatrix}|f^{0011}|^2\\ |f^{0101}|^2\\ |f^{0110}|^2\\ \lambda\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\end{bmatrix}.$$

For the arity 6 case, we will basically show the same thing (i.e., the linear system has only the trivial zero solution) with some carefully chosen rows. For arity 8 case, we will use the fact that the variables take nonnegative values and we show the linear system has no nonnegative solution except the zero solution.

An intuitive reason why this proof could succeed for signatures of small arity is that in these cases, we have more equations than variables, which leads to an over-determined linear system. For the general case of arity n, there are $4\binom{n}{2}$ many equations but $\binom{n}{n/2}/2+1$ many variables. Since $4\binom{n}{2} \ll \binom{n}{n/2}/2+1$ when n is large, this method will not work for large n. This is why we cannot hope to apply this proof to signatures of large arity.

Now, we give the formal proof for signatures of arity 6 and 8. In what follows we assume f has arity $\geqslant 6$. Given a vector $\mathbf{f}_{ij}^{ab}$, we can pick a third variable x_k and separate $\mathbf{f}_{ij}^{ab}$ into two vectors $\mathbf{f}_{ijk}^{ab0}$ and $\mathbf{f}_{ijk}^{ab1}$ according to $x_k = 0$ or 1. By setting $(a,b)=(0,0)$, we have

$$|\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ijk}^{000}|^2 + |\mathbf{f}_{ijk}^{001}|^2 = \lambda. \tag{4.5}$$

Similarly, we consider the vector $\mathbf{f}_{ik}^{00}$ and separate it according to $x_j = 0$ or 1. We have

$$|\mathbf{f}_{ik}^{00}|^2 = |\mathbf{f}_{ijk}^{000}|^2 + |\mathbf{f}_{ijk}^{010}|^2 = \lambda. \tag{4.6}$$

Comparing equations (4.5) and (4.6), we have $|\mathbf{f}_{ijk}^{001}|^2 = |\mathbf{f}_{ijk}^{010}|^2$. Moreover, by ARS, we have $|\mathbf{f}_{ijk}^{010}|^2 = |\mathbf{f}_{ijk}^{101}|^2$. Thus, we have $|\mathbf{f}_{ijk}^{001}|^2 = |\mathbf{f}_{ijk}^{101}|^2$. Note that the vector $\mathbf{f}_{jk}^{01}$ can be separated into two vectors $\mathbf{f}_{ijk}^{001}$ and $\mathbf{f}_{ijk}^{101}$ according to $x_i = 0$ or 1. Therefore,

$$|\mathbf{f}_{jk}^{01}|^2 = |\mathbf{f}_{ijk}^{001}|^2 + |\mathbf{f}_{ijk}^{101}|^2 = \lambda.$$

Thus, we have $|\mathbf{f}_{ijk}^{001}|^2 = |\mathbf{f}_{ijk}^{101}|^2 = \lambda/2$. Then, by equation (4.5), we have $|\mathbf{f}_{ijk}^{000}|^2 = \lambda/2$, and again by ARS, we also have $|\mathbf{f}_{ijk}^{111}|^2 = |\mathbf{f}_{ijk}^{000}|^2 = \lambda/2$. Note that the indices i, j, k can be arbitrary three distinct indices, by symmetry we have

$$|\mathbf{f}_{ijk}^{abc}|^2 = \lambda/2 \tag{4.7}$$

for f of arity $\geqslant 6$, and for all $(x_i, x_j, x_k) = (a, b, c) \in \{0,1\}^3$.

This leads to a contradiction for signatures of arity 6. Suppose f is an irreducible signature on 6 variables $x_1, x_2, \ldots, x_6$. Let (i, j, k, i', j', k') be an arbitrary permutation of $\{1, 2, \ldots, 6\}$. Note that the vector $\mathbf{f}_{ijk}^{000}$ has only one possible nonzero entry $f_{ijki'j'k'}^{000111}$. Thus, by (4.7) we have

$$|\mathbf{f}_{ijk}^{000}|^2 = |f_{ijki'j'k'}^{000111}|^2 = \lambda/2$$

for any $(x_i, x_j, x_k, x_{i'}, x_{j'}, x_{k'}) = (0, 0, 0, 1, 1, 1)$. That is, any entry of f at half weight has the same nonzero norm $\sqrt{\lambda/2}$. However, the vector $\mathbf{f}_{ijk}^{001}$ has $\binom{3}{2} = 3$ nonzero entries. But,

$$\lambda/2 = |\mathbf{f}_{ijk}^{001}|^2 = |f_{ijki'j'k'}^{001011}|^2 + |f_{ijki'j'k'}^{001101}|^2 + |f_{ijki'j'k'}^{001110}|^2 = 3\lambda/2,$$

which means $\lambda = 0$. This is a contradiction.

For signatures of arity 8, we need to go further and use the fact that the norm-square is nonnegative. Given a vector $\mathbf{f}_{ijk}^{abc}$, we can continue to pick a fourth variable x_ℓ and separate $\mathbf{f}_{ijk}^{abc}$ into two vectors $\mathbf{f}_{ijk\ell}^{abc0}$ and $\mathbf{f}_{ijk\ell}^{abc1}$ according to $x_\ell = 0$ or 1. By setting $(a, b, c) = (0, 0, 0)$, we have from (4.7)

$$|\mathbf{f}_{ijk}^{000}|^2 = |\mathbf{f}_{ijk\ell}^{0000}|^2 + |\mathbf{f}_{ijk\ell}^{0001}|^2 = \lambda/2. \tag{4.8}$$

Similarly, we consider the vector $\mathbf{f}_{ij\ell}^{001}$ and separate it according to $x_k = 0$ or 1. We have

$$|\mathbf{f}_{ij\ell}^{001}|^2 = |\mathbf{f}_{ijk\ell}^{0001}|^2 + |\mathbf{f}_{ijk\ell}^{0011}|^2 = \lambda/2. \tag{4.9}$$

Comparing equations (4.8) and (4.9), we have $|\mathbf{f}_{ijk\ell}^{0000}|^2 = |\mathbf{f}_{ijk\ell}^{0011}|^2$. This leads to a contradiction for signatures of arity 8.

Suppose f is an irreducible signature on 8 variables $x_1, x_2, \ldots, x_8$. Let $(i, j, k, \ell, i', j', k', \ell')$ be an arbitrary permutation of $\{1, 2, \ldots, 8\}$. The vector $\mathbf{f}_{ijk\ell}^{0000}$ has only one possible nonzero entry

$f^{00001111}_{ijk\ell i'j'k'\ell'}$. Thus,

$$|\mathbf{f}^{0000}_{ijk\ell}|^2 = |f^{00001111}_{ijk\ell i'j'k'\ell'}|^2. \tag{4.10}$$

The vector $\mathbf{f}^{0011}_{ijk\ell}$ has $\binom{4}{2} = 6$ possible nonzero entries including $f^{00110011}_{ijk\ell i'j'k'\ell'}$. Thus,

$$|\mathbf{f}^{0011}_{ijk\ell}|^2 = |f^{00110011}_{ijk\ell i'j'k'\ell'}|^2 + \Delta, \tag{4.11}$$

where Δ denotes the sum of norm-squares of the other 5 entries in $\mathbf{f}^{0011}_{ijk\ell}$ and we know $\Delta \geqslant 0$. Since the left-hand sides of equations (4.10) and (4.11) are equal, we have

$$|f^{00001111}_{ijk\ell i'j'k'\ell'}|^2 = |f^{00110011}_{ijk\ell i'j'k'\ell'}|^2 + \Delta. \tag{4.12}$$

Similarly, consider vectors $\mathbf{f}^{0000}_{iji'j'}$ and $\mathbf{f}^{0011}_{iji'j'}$. We have $|\mathbf{f}^{0000}_{iji'j'}|^2 = |\mathbf{f}^{0011}_{iji'j'}|^2$. The vector $\mathbf{f}^{0000}_{iji'j'}$ has only one possible nonzero entry. Thus,

$$|\mathbf{f}^{0000}_{iji'j'}|^2 = |f^{00110011}_{ijk\ell i'j'k'\ell'}|^2.$$

The vector $\mathbf{f}^{0011}_{iji'j'}$ has 6 possible nonzero entries. Thus,

$$|\mathbf{f}^{0011}_{iji'j'}|^2 = |f^{00001111}_{ijk\ell i'j'k'\ell'}|^2 + \Delta',$$

where Δ' denotes the sum of norm-squares of the other 5 entries in $\mathbf{f}^{0011}_{iji'j'}$ and we know $\Delta' \geqslant 0$. Thus, we have

$$|f^{00110011}_{ijk\ell i'j'k'\ell'}|^2 = |f^{00001111}_{ijk\ell i'j'k'\ell'}|^2 + \Delta' \tag{4.13}$$

Comparing equations (4.12) and (4.13), we have $\Delta = -\Delta'$, which means $\Delta = \Delta' = 0$ due to $\Delta \geqslant 0$ and $\Delta' \geqslant 0$. Since Δ is the sum of 5 norm-squares, each of which is nonnegative, $\Delta = 0$ means each norm-square in the sum Δ is 0. In particular, $|f^{00111100}_{ijk\ell i'j'k'\ell'}|^2$ is a term in the sum Δ. We have $|f^{00111100}_{ijk\ell i'j'k'\ell'}|^2 = 0$. Since the order of indices is picked arbitrarily, all entries of f are zero. Thus, f is a zero signature. A contradiction. □

Theorem 4.22. *If $\mathcal{F} \not\subseteq \mathcal{E}^{\otimes}$, then either* #EO($\mathcal{F}$) is #P-hard or #EO($\{\neq_4\} \cup \mathcal{F}$) $\leqslant_T$ #EO($\mathcal{F}$).

证明. The base case is Lemma 4.21 and the inductive step is Lemma 4.20. Done by induction. □

4.4 Reduction from #CSP to #EO Problems

In this section, we will show #EO($\{\neq_4\} \cup \mathcal{F}$) is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$, or $\mathcal{F} \subseteq \mathscr{P}$. The first steps are simple; the availability of $\neq_4$ allows us to realize any $(\neq_{2k})$ and therefore all of $\mathcal{DEQ}$.

Lemma 4.23. #EO($\mathcal{DEQ} \cup \mathcal{F}$) $\leqslant_{\mathrm{T}}$ #EO($\{\neq_4\} \cup \mathcal{F}$).

证明. Connecting $\neq_{2k}$ ($k \geqslant 2$) and $\neq_4$ using $\neq_2$ we get $\neq_{2k+2}$. Every occurrence of signatures in $\mathcal{DEQ}$ can be realized by a linear size gadget. Then we have #EO($\mathcal{DEQ} \cup \mathcal{F}$) $\leqslant_{\mathrm{T}}$ #EO($\{\neq_4\} \cup \mathcal{F}$). □

Recall that #EO($\mathcal{DEQ} \cup \mathcal{F}$) is just Holant($\neq_2 | \mathcal{DEQ} \cup \mathcal{F}$) expressed in the Holant framework. We show that after we get $\mathcal{DEQ}$ on the right hand side (RHS) in the above Holant problem, we can also realize $\mathcal{DEQ}$ on the left-hand side (LHS).

Lemma 4.24. Holant($\mathcal{DEQ} \mid \mathcal{F}$) $\leqslant_T$ Holant($\neq_2 | \mathcal{DEQ} \cup \mathcal{F}$)*, which is equivalent to* #EO($\mathcal{DEQ} \cup \mathcal{F}$)*.*

证明. In Holant($\neq_2 | \mathcal{DEQ} \cup \mathcal{F}$) we take $2k$ copies of $\neq_2$ on the LHS and connect one variable of each copy of $\neq_2$ to all $2k$ variables of one copy of $\neq_{2k}$ on the RHS. This gives us the constraint function $\neq_{2k}$ on the LHS. □

Combining Lemmas 4.23 and 4.24, we have the following reduction for genaral Holant problems.

Lemma 4.25. *For any* $\mathcal{G}$*,* Holant($\mathcal{DEQ} \mid \mathcal{G}$) $\leqslant_T$ Holant($\neq_2 | \mathcal{DEQ}, \mathcal{G}$) $\leqslant_T$ Holant($\neq_2 | \neq_4, \mathcal{G}$).

Now, consider an arbitrary instance of Holant($\mathcal{DEQ} \mid \mathcal{F}$); it is given by a bipartite graph. Similar to how we express #CSP($\mathcal{F}$) using Holant($\mathcal{EQ} \mid \mathcal{F}$), in Holant($\mathcal{DEQ} \mid \mathcal{F}$) we can view vertices on the LHS (labeled by $(\neq_{2k}) \in \mathcal{DEQ}$) as variables, and vertices on the RHS (labeled by $f \in \mathcal{F}$) as constraints. However, the difference here is that in this setting, both a variable itself and its negation appear as input variables of constraints, and they always appear the same number of times. More specifically, for a variable vertex x labeled by $\neq_{2k}$, the entire set of $2k$ edges incident to x can be divided into two subsets, each of which consisting of k edges. In each subset, every edge takes the same value, while two edges in different sets always take opposite values. Then, we can view the k edges in one subset as the variable x appearing k times, while another k edges in the other subset as its negation $\overline{x}$ appearing k times.

Recall that signatures $f \in \mathcal{F}$ satisfy ARS. Suppose $f \in \mathcal{F}$ has arity $2n$. Then, consider the function $f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{2n}})$. That is, we replace the input variables by their negations. Then we have $f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{2n}}) = \overline{f(x_1, x_2, \ldots, x_{2n})}$ by ARS. Define the norm square function $|f|^2$, which takes value $|f(x_1, \ldots, x_{2n})|^2$ on input $(x_1, \ldots, x_{2n})$. Then, we have

$$|f|^2(x_1, \ldots, x_{2n}) = f(x_1, \ldots, x_{2n})\overline{f(x_1, \ldots, x_{2n})} = f(x_1, \ldots, x_{2n})f(\overline{x_1}, \ldots, \overline{x_{2n}}),$$

and this gives the following reduction.

Lemma 4.26. *Let* $|\mathcal{F}|^2 = \{|f|^2 \mid f \in \mathcal{F}\}$. *Then* $\#\mathrm{CSP}(|\mathcal{F}|^2) \leqslant_T \operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$.

证明. Given an instance I of $\#\mathrm{CSP}(|\mathcal{F}|^2)$ over m variables. Suppose it contains ℓ occurrences of constraints $|f_i|^2 \in |\mathcal{F}|^2$ $(i \in [\ell])$ of arity $2n_i$, and f_i is applied to the variables $x_{i_1}, \ldots, x_{i_{2n_i}}$. Then

$$\#\mathrm{CSP}(I) = \sum_{x_1,\ldots,x_m \in \mathbb{Z}_2} \prod_{i=1}^{\ell} |f_i|^2(x_{i_1}, \ldots, x_{i_{2n_i}}) = \sum_{x_1,\ldots,x_m \in \mathbb{Z}_2} \prod_{i=1}^{\ell} f_i(x_{i_1}, \ldots, x_{i_{2n_i}}) f_i(\overline{x_{i_1}}, \ldots, \overline{x_{i_{2n_i}}}). \tag{4.14}$$

Notice that in the final form of (4.14), for each variable $x \in \{x_1, \ldots, x_m\}$, both itself and its negation appear as input variables to various constraints $f_i \in \mathcal{F}$. Moreover, there is a one-to-one correspondence between each occurrence of x and that of $\bar{x}$. Thus, x and $\bar{x}$ appear the same number of times. Thus the partition function $\#\mathrm{CSP}(I)$ for the $\#\mathrm{CSP}(|\mathcal{F}|^2)$ problem can be expressed as the partition function of an instance of $\operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ of polynomially bounded size. □

Directly by this reduction, we have the following hardness result. Corollary 4.27 follows from Theorem 2.12.

Corollary 4.27. $\operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ *is #P-hard if there is some* $f \in \mathcal{F}$ *such that* $\mathscr{S}(f)$ *is not affine.*

证明. By the definition of $|f|^2$, we know $\mathscr{S}(|f|^2) = \mathscr{S}(f)$. Thus, there is some $|f|^2 \in |\mathcal{F}|^2$ such that $\mathscr{S}(|f|^2)$ is not affine. This implies that $|\mathcal{F}|^2 \not\subseteq \mathscr{A}$. Moreover, by Lemma 2.10, we also have $|\mathcal{F}|^2 \not\subseteq \mathscr{P}$. By Theorem 2.12, $\#\mathrm{CSP}(|\mathcal{F}|^2)$ is #P-hard and hence, by Lemma 4.26, $\operatorname{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ is #P-hard. □

Now, we may assume every signature $f \in \mathcal{F}$ has affine support. Quite amazingly, if an EO signature has affine support, then its support must have a special structure, called *pairwise opposite*.

We repeat the definition of pairwise opposite here.

Definition 4.28 (Pairwise opposite)**.** *Let $\mathscr{S} \subseteq \mathbb{Z}_2^{2n}$ be an affine linear subspace. We say $\mathscr{S}$ is pairwise opposite if we can partition the $2n$ variables into n pairs such that on $\mathscr{S}$, two variables of each pair always take opposite values. If $\mathscr{S}$ is pairwise opposite, we fix a pairing. Then each pair under this paring is called an opposite pair.*

Example 4.29. *Let $\mathscr{S} = \{(x_1, x_2, \ldots, x_{2n}) \mid x_1, \ldots, x_{2n} \in \mathbb{Z}_2, \overline{x_i} = x_{n+i}\ (i \in [n])\}$. Then $\mathscr{S}$ is pairwise opposite. Moreover, any affine linear subspace of $\mathscr{S}$ is pairwise opposite.*

For instance, let C be the Hamming $(7,4)$-code. We consider its dual Hamming code $C^{\perp}$. $C^{\perp}$ is a linear subspace of $\mathbb{Z}_2^7$ of dimension 3. Let

$$\mathscr{S}_C = \{\alpha \circ \overline{\alpha} \in \mathbb{Z}_2^{14} \mid \alpha \in C^{\perp}\}.$$

Then $\mathscr{S}_C$ is pairwise opposite. This $\mathscr{S}_C$ is introduced in [32] related to a certain tractable family of signatures for a class of Holant problems.

Note that if an affine linear subspace $\mathscr{S} \subseteq \mathbb{Z}_2^{2n}$ is pairwise opposite, then $\mathscr{S} \subseteq \mathscr{H}_{2n}$. Now, we show the other direction is also true. This result should be of independent interest.

Lemma 4.30. *Let $\mathscr{S} \subseteq \mathbb{Z}_2^{2n}$ be an affine linear subspace. If $\mathscr{S} \subseteq \mathscr{H}_{2n}$, then $\mathscr{S}$ is pairwise opposite.*

证明. The lemma is trivially true if $|\mathscr{S}| = 0, 1$. Suppose $\dim(\mathscr{S}) = k \geqslant 1$. We can pick a set of free variables $F = \{x_1, \ldots, x_k\}$, then on $\mathscr{S}$, every variable x is expressible as a unique affine linear combination over $\mathbb{Z}_2$ of these free variables, $x = \lambda_1 x_1 + \ldots + \lambda_k x_k + \lambda_{k+1}$, where $\lambda_1, \ldots, \lambda_{k+1} \in \mathbb{Z}_2$. (If x takes a constant value on $\mathscr{S}$, it is still an affine linear combination of these free variables.)

We separate out all $2n$ variables into two types, those with $\lambda_{k+1} = 0$ (linear form) and those with $\lambda_{k+1} = 1$ (affine, *but not* linear form). If we set all free variables $x_1, \ldots, x_k$ to 0, we get a vector $\alpha \in \mathscr{S}$ with $\mathrm{wt}(\alpha) = n$. Each x of the first type contributes zero and each x of the second type contributes one. Hence among all $2n$ variables, there are exactly n variables of each type, and the chosen free variables are among the first type. Without loss of generality, we may assume variables of the first and second type are $U = \{x_1, \ldots, x_n\}$ and $V = \{x_{n+1}, \ldots, x_{2n}\}$.

For any variable $x = \lambda_1 x_1 + \ldots + \lambda_k x_k + \lambda_{k+1}$, with respect to this unique affine linear expression, let $\Lambda(x) = \{i \in [k] \mid \lambda_i = 1\}$, the set of free variables that do appear in the expression of x. We have,

$$x = \sum_{i \in \Lambda(x)} x_i \quad \text{if } x \in U, \qquad \text{and} \qquad x = 1 + \sum_{i \in \Lambda(x)} x_i \quad \text{if } x \in V.$$

Clearly, for $i \in [k]$, $\Lambda(x_i) = \{i\}$. For any subset $I \subseteq [k]$, we let

$$U^{\subseteq}(I) = \{x \in U \mid I \subseteq \Lambda(x)\}, \qquad \text{and} \qquad U^{=}(I) = \{x \in U \mid \Lambda(x) = I\}.$$

Define $V^{\subseteq}(I)$ and $V^{=}(I)$ analogously, with V in place of U. For any subset $I \subseteq [k]$, let $\alpha^I \in \mathscr{S}$ be the vector determined by setting free variables $x_i = 1$ for $i \in I$ and $x_i = 0$ for $i \in [k] - I$. Within the $2n$ bit positions in the vector α^I, for any variable $x \in U$,

$$x = 1 \quad \text{if } |I \cap \Lambda(x)| \text{ is odd}, \qquad \text{and} \qquad x = 0 \quad \text{otherwise.}$$

Symmetrically for any variable $x \in V$, we have

$$x = 0 \quad \text{if } |I \cap \Lambda(x)| \text{ is odd}, \qquad \text{and} \qquad x = 1 \quad \text{otherwise.}$$

Let $U^{\text{odd}}(I) = \{x \in U \mid |I \cap \Lambda(x)| \text{ is odd}\}$ and $V^{\text{odd}}(I) = \{x \in V \mid |I \cap \Lambda(x)| \text{ is odd}\}$. Since

$$n = \text{wt}(\alpha^I) = |U^{\text{odd}}(I)| + (n - |V^{\text{odd}}(I)|),$$

we have $|U^{\text{odd}}(I)| = |V^{\text{odd}}(I)|$, for all $I \subseteq [k]$.

Claim 1. For all $I \subseteq [k]$,

$$|U^{\text{odd}}(I)| = \sum_{J \subseteq I : J \neq \emptyset} (-2)^{|J|-1} |U^{\subseteq}(J)|.$$

To prove this Claim, we count the contributions of every $x \in U$ to both sides of the equation. For $x \in U$, let $m(x) = |I \cap \Lambda(x)|$. This x contributes one or zero to the LHS, according to whether $m(x)$ is odd or even respectively. On the RHS, its contribution is

$$\sum_{j=1}^{m(x)} (-2)^{j-1} \sum_{J \subseteq I \cap \Lambda(x) : |J| = j} 1 = \sum_{j=1}^{m(x)} (-2)^{j-1} \binom{m(x)}{j} = (-2)^{-1} \left[(1-2)^{m(x)} - 1 \right],$$

which is also precisely one or zero according to whether $m(x)$ is odd or even respectively.

The same statement is true for $V^{\text{odd}}(I)$ replacing U by V, with the same proof.

Claim 2. For all $I \subseteq [k]$,

$$|V^{\text{odd}}(I)| = \sum_{J \subseteq I : J \neq \emptyset} (-2)^{|J|-1} |V^{\subseteq}(J)|.$$

We show next that $|U^{\subseteq}(I)| = |V^{\subseteq}(I)|$ for all $I \subseteq [k]$. If $I = \emptyset$, then $U^{\subseteq}(I) = U$ and $V^{\subseteq}(I) = V$, and so they have the same cardinality, both being n. Inductively, for any $I \subseteq [k]$, suppose we already know that $|U^{\subseteq}(J)| = |V^{\subseteq}(J)|$, for all proper subsets $J \subset I$, then since $|U^{\text{odd}}(I)| = |V^{\text{odd}}(I)|$, by the two Claims we have $|U^{\subseteq}(I)| = |V^{\subseteq}(I)|$ as well, since the coefficient $(-2)^{|I|-1} \neq 0$.

Then, by definition

$$|U^{\subseteq}(I)| = \sum_{I \subseteq J \subseteq [k]} |U^{=}(J)|.$$

By the Möbius inversion formula, we have

$$|U^{=}(I)| = \sum_{I \subseteq J \subseteq [k]} (-1)^{|J|-|I|} |U^{\subseteq}(J)|.$$

Indeed,

$$\sum_{I \subseteq J \subseteq [k]} (-1)^{|J|-|I|} \sum_{J \subseteq J' \subseteq [k]} |U^{=}(J')| = \sum_{I \subseteq J' \subseteq [k]} \sum_{I \subseteq J \subseteq J'} (-1)^{|J|-|I|} |U^{=}(J')|,$$

and for a proper containment $I \subset J'$ the coefficient of $|U^{=}(J')|$ is $(1-1)^{|J'|-|I|} = 0$, and it is 1 for $I = J'$.

The same statement is true for V. Thus, we have $|U^{=}(I)| = |V^{=}(I)|$ for all $I \subseteq [k]$.

This allows us to set up a pairing between U and V such that for each pair of paired variables $(x, y) \in U \times V$, we have $\Lambda(x) = I(y)$. For any $I \subseteq [k]$, we arbitrarily pick a pairing between $U^{=}(I)$ and $V^{=}(I)$. This is achievable because they have the same cardinality. Since the following decompositions for both U and V are disjoint unions

$$U = \bigcup_{I \subseteq [k]} U^{=}(I) \qquad \text{and} \qquad V = \bigcup_{I \subseteq [k]} V^{=}(I),$$

we get a global pairing between U and V, such that for each pair of paired variables $(x, y) \in U \times V$, we have $\Lambda(x) = I(y)$. Recall that on $\mathscr{S}$, since $x \in U$, we have $x = \sum_{i\in\Lambda(x)} x_i$; meanwhile since $y \in V$ we have $y = 1 + \sum_{i\in I(y)} x_i$. It follows that $\overline{x} = y$ on $\mathscr{S}$. □

Now, we are going to simulate #CSP($\mathcal{F}$) using Holant($\mathcal{DEQ} \mid \mathcal{F}$) when $\mathcal{F}$ consists of signatures with affine support. Suppose $f(x_1, \ldots, x_{2n}) \in \mathcal{F}$ has affine support, by Lemma 4.30, we know $\mathscr{S}(f)$ is pairwise opposite. By permuting variables, we may assume for $i \in [n]$, (x_i, x_{n+i}) is paired as an opposite pair. Then, we have the following reduction.

Lemma 4.31. *Suppose $\mathcal{F}$ is a set of* EO *signatures. If every signature $f \in \mathcal{F}$ has affine support, then* #CSP($\mathcal{F}$) $\leqslant_T$ Holant($\mathcal{DEQ} \mid \mathcal{F}$).

证明. Given an instance I of #CSP($\mathcal{F}$) over m variables $V = \{x_1, \ldots, x_m\}$. Suppose it contains ℓ constraints f_i ($i \in [\ell]$) of arity $2n_i$, and f_i is applied to the variables $x_{i_1}, \ldots, x_{i_{2n_i}}$. We define a graph $G = (V, E)$, where V is the variable set and $(x, y) \in E$ if variables x, y appear as an opposite pair in some $\mathscr{S}(f_i)$. Consider all connected components of G. We get a partition of V. Pick a representative variable in each connected component and define $V^{\mathtt{r}}$ to be the set of representative variables. Without loss of generality, we assume $V^{\mathtt{r}} = \{x_1, \ldots, x_{m^{\mathtt{r}}}\}$. For each variable $x \in V$, we use $x^{\mathtt{r}} \in V^{\mathtt{r}}$ to denote its representative variable. By the definition of opposite pairs, for any assignment with a nonzero contribution, we have $x = \overline{x^{\mathtt{r}}}$ if there is a path of odd length from x to $x^{\mathtt{r}}$ and $x = x^{\mathtt{r}}$ if there is a path of even length from x to $x^{\mathtt{r}}$ (if $x^{\mathtt{r}}$ is x itself, we say there is a path of length 0 from $x^{\mathtt{r}}$ to x). If for some x, we have both $x = \overline{x^{\mathtt{r}}}$ and $x = x^{\mathtt{r}}$, (that is, the connected component containing x is not a bipartite graph), then we know #CSP(I) $\equiv 0$ since $x = \bar{x}$ is impossible. Otherwise, for each variable $x \in V$ we have either $x = \overline{x^{\mathtt{r}}}$ or $x = x^{\mathtt{r}}$, but not both.

Then, for any nonzero term in the sum

$$\#\mathrm{CSP}(I) = \sum_{x_1,\ldots,x_m\in\mathbb{Z}_2} \prod_{i=1}^{\ell} f_i(x_{i_1}, \ldots, x_{i_{2n}}),$$

the assignment of all variables in V can be uniquely extended from its restriction on representative variables $V^{\mathtt{r}}$. Moreover, since $\mathscr{S}(f_i)$ is pairwise opposite, for each opposite pair $(x_{i_s}, x_{i_{n+s}})$, we know exactly one variable is equal to $x^{\mathtt{r}}_{i_s}$ while the other one is equal to $\overline{x^{\mathtt{r}}_{i_s}}$. Thus each pair

$(x_{i_s}, x_{i_{n+s}})$ is either $(x^{\mathfrak{r}}_{i_s}, \overline{x^{\mathfrak{r}}_{i_s}})$ or $(\overline{x^{\mathfrak{r}}_{i_s}}, x^{\mathfrak{r}}_{i_s})$. We will write this as $(\widehat{x^{\mathfrak{r}}_{i_s}}, \overline{\widehat{x^{\mathfrak{r}}_{i_s}}})$. Then, we have

$$\#\mathrm{CSP}(I) = \sum_{x_1,\ldots,x_{m^{\mathfrak{r}}}\in\mathbb{Z}_2} \prod_{i=1}^{\ell} f_i(x_{i_1},\ldots,x_{i_{2n_i}}) = \sum_{x_1,\ldots,x_{m^{\mathfrak{r}}}\in\mathbb{Z}_2} \prod_{i=1}^{\ell} f_i(\widehat{x^{\mathfrak{r}}_{i_1}},\ldots,\widehat{x^{\mathfrak{r}}_{i_{n_i}}},\overline{\widehat{x^{\mathfrak{r}}_{i_1}}},\ldots,\overline{\widehat{x^{\mathfrak{r}}_{i_{n_i}}}}). \quad (4.15)$$

The final form of (4.15) is an instance of $\mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$. □

By this reduction, we have the following hardness result.

Corollary 4.32. *If every signature $f \in \mathcal{F}$ has affine support, then* $\mathrm{Holant}(\mathcal{DEQ} \mid \mathcal{F})$ *is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$, or $\mathcal{F} \subseteq \mathscr{P}$.*

Theorem 4.33. $\#\mathrm{EO}(\{\neq_4\} \cup \mathcal{F})$ *is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$, or $\mathcal{F} \subseteq \mathscr{P}$.*

证明. It follows from Lemmas 4.23, 4.24, Corollaries 4.27 and 4.32. □

4.5 Putting Things Together

Combining Theorems 2.30, 4.22 and 4.33, we can finish the proof of the Theorem 4.1.

证明. (of Theorem 4.1) If $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$, then by Theorem 2.30, $\#\mathrm{EO}(\mathcal{F})$ is tractable. Suppose $\mathcal{F} \nsubseteq \mathscr{A}$ and $\mathcal{F} \nsubseteq \mathscr{P}$, then certainly $\mathcal{F} \nsubseteq \mathcal{E}^{\otimes}$ as $\mathcal{E}^{\otimes} \subset \mathscr{P}$. Then Theorems 4.22 and 4.33 complete the proof. □

Chapter 5

Dichotomy for Real Holant Problems with an Odd-ary Signature

From this chapter to Chapter 8, we will prove the complexity dichotomy for real-valued Holant problems. In these chapters, without other specification, we use f to denote a real-valued signature and $\mathcal{F}$ to denote a set of real-valued signatures. We use $\widehat{f} = Z^{-1}f$ to denote a signature satisfying ARS and $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ to denote a set of signatures satisfying ARS. We use Q to denote a matrix in $\mathbf{O}_2$, and $\widehat{Q}$ to denote a matrix in $\widehat{\mathbf{O}_2}$. Clearly, if $\mathcal{F}$ is real-valued, then $Q\mathcal{F}$ is also real-valued. Equivalently, if $\widehat{\mathcal{F}}$ satisfies ARS, then $\widehat{Q}\widehat{\mathcal{F}} = \widehat{Q\mathcal{F}}$ also satisfies ARS.

By Theorem 2.33, if $\mathcal{F}$ satisfies condition (T), then Holant($\mathcal{F}$) is P-time computable. So, we only need to prove that Holant($\mathcal{F}$) or equivalently Holant($\neq_2|\ \widehat{\mathcal{F}}$) is #P-hard when $\mathcal{F}$ does not satisfy condition (T). In this chapter, we consider the case that $\mathcal{F}$ contains a nonzero signature of odd arity.

5.1 Realization of Pinning or Equality Signatures

The problem Holant$^c(\mathcal{F})$ is defined as Holant$(\Delta_0, \Delta_1\mathcal{F})$. A complexity dichotomy of Holant^c problems was first proved for real-valued signatures. Later, it was generalized to complex-valued signatures. Here, we state the dichotomy of Holant^c problems for real-valued signatures. Recall that we define $H = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ be the 2-by-2 Hadamard matrix and $T_{\alpha^s} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \alpha^s \end{smallmatrix}\right]$ where $\alpha = \frac{1+\mathrm{i}}{\sqrt{2}}$.

Theorem 5.1. *Let $\mathcal{F}$ be a set of real valued signatures. Then,* Holant$^c(\mathcal{F})$ *is #P-hard unless $\mathcal{F} \subseteq \mathscr{T}$, $\mathscr{A}$, $\mathscr{P}$, $\mathscr{L}$, $H\mathcal{F} \subseteq \mathscr{P}$, $\widehat{\mathcal{F}} \subseteq \mathscr{P}$ or $T_\alpha\mathcal{F} \subseteq \mathscr{A}$, in which cases* Holant$^c(\mathcal{F})$ *is tractable.*

Remark 5.2. *Note that the above tractability condition implies that $\mathcal{F}$ satisfies condition* (T). *Thus, if a real-valued $\mathcal{F}$ does not satisfy condition* (T), *then* Holant$^c(\mathcal{F})$ *is #P-hard.*

We want to realize the unary signatures Δ_0 and Δ_1 so that we can invoke the dichotomy of Holant^c problems. We first show that under some holographic transformations, either one can use a signature of odd arity to realize the unary signature $\Delta_0 = (1, 0)$, or one can realize some equality signature $(=_k)$ $(k \geqslant 3)$.

Lemma 5.3. *Let $\mathcal{F}$ be a set of real-valued signatures containing a signature f of odd arity. Then, there exists some real orthogonal matrix $Q \in \mathbf{O}_2$ such that*

- $\operatorname{Holant}(\Delta_0, Q\mathcal{F}) \leqslant_T \operatorname{Holant}(\mathcal{F})$ *or*
- $\operatorname{Holant}(\neq_2 | =_{2k+1}, \widehat{Q\mathcal{F}}) \leqslant_T \operatorname{Holant}(\mathcal{F})$*, for some $k \geqslant 1$.*

证明. Suppose f has arity n. We prove our lemma by induction on n.

If $n = 1$, then $f = (a, b)$ where $a, b \in \mathbb{R}$ are not both zero. Let $Q_1 = \frac{1}{\sqrt{a^2+b^2}} \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] \in \mathbf{O}_2$. Note that $\operatorname{Holant}(\mathcal{F})$ is just $\operatorname{Holant}(=_2 | \mathcal{F})$, and $=_2$ is invariant under an orthogonal holographic transformation $(=_2)(Q_1^{-1})^{\otimes 2} = (=_2)$, and $Q_1(a, b)^{\mathsf{T}} = \sqrt{a^2 + b^2}(1, 0)^{\mathsf{T}}$. Thus,

$$\operatorname{Holant}(=_2 | \Delta_0, Q_1\mathcal{F}) \equiv \operatorname{Holant}(=_2 | (a, b), \mathcal{F}).$$

The base case is proved.

We assume our claim is true for $n = 2k - 1$. Now, we consider $n = 2k + 1 \geqslant 3$. If there is a pair of indices $\{i, j\}$ such that $\partial_{ij} f \not\equiv 0$, then we can realize a signature of arity $2k - 1$ from f. By induction hypothesis, we have

$$\operatorname{Holant}(\Delta_0, Q\mathcal{F}) \leqslant_T \operatorname{Holant}(\partial_{ij} f, \mathcal{F}) \leqslant_T \operatorname{Holant}(\mathcal{F}).$$

Otherwise, $\partial_{ij} f \equiv 0$ for all pairs of indices $\{i, j\}$. Thus, we also have $\widehat{\partial}_{ij}\widehat{f} \equiv 0$ for all $\{i, j\}$. Then, by Lemma 3.9, we have $\widehat{f} = a(1, 0)^{\otimes n} + \bar{a}(0, 1)^{\otimes n}$ for some $a \neq 0$. We may normalize the norm $|a|$ to 1. Suppose that $a = e^{\mathrm{i}\theta}$. Let $\widehat{Q_2} = \begin{bmatrix} e^{-\mathrm{i}\theta/n} & 0 \\ 0 & e^{\mathrm{i}\theta/n} \end{bmatrix} \in \widehat{\mathbf{O}}_2$. We have $\widehat{Q_2}^{\otimes n}\widehat{f} = (1, 0)^{\otimes n} + (0, 1)^{\otimes n}$. Thus, a holographic transformation by $\widehat{Q_2}$ and Z^{-1} yields

$$\operatorname{Holant}(\mathcal{F}) \equiv_T \operatorname{Holant}(=_2 | f, \mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2 | \widehat{f}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\neq_2 | =_{2k+1}, \widehat{Q_2}\widehat{\mathcal{F}}).$$

By equation (2.1), $\widehat{Q_2}\widehat{\mathcal{F}} = \widehat{Q_2\mathcal{F}}$. Thus, $\operatorname{Holant}(\neq_2 | =_{2k+1}, \widehat{Q_2\mathcal{F}}) \leqslant_T \operatorname{Holant}(\mathcal{F})$ where $k \geqslant 1$. □

Now, we want to show that both $\operatorname{Holant}(\Delta_0, Q\mathcal{F})$ and $\operatorname{Holant}(\neq_2|=_k, \widehat{Q\mathcal{F}})$ where $k \geqslant 3$ are #P-hard for all $Q \in \mathbf{O}_2$ and all real-valued $\mathcal{F}$ that does not satisfy condition (T). Recall that for all $Q \in \mathbf{O}_2$ and all real-valued $\mathcal{F}$, $Q\mathcal{F}$ is also real-valued that does not satisfy condition (T), $Q\mathcal{F}$ is also a real-valued signature set that does not satisfy condition (T). Thus, it suffices for us to show that $\operatorname{Holant}(\Delta_0, \mathcal{F})$ and $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$ where $k \geqslant 3$ are #P-hard for all real-valued $\mathcal{F}$ that does not satisfy condition (T). We will prove these #P-hardness results in the following two sections.

5.2 #P-Hardness of $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$

Recall that $\mathcal{EQ}_k$ denotes the set of equality signatures of arity nk for all $n \geqslant 1$, i.e., $\mathcal{EQ}_k = \{=_k, =_{2k}, \ldots, =_{nk}, \ldots\}$. The problem $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is defined as $\operatorname{Holant}(\mathcal{EQ}_k \mid \neq_2, \mathcal{G})$. First, we prove the following reduction.

Lemma 5.4. *If $k \geqslant 3$, then $\#\mathrm{CSP}_k(\neq_2, \mathcal{G}) \equiv_T \operatorname{Holant}(\mathcal{EQ}_k \mid \neq_2, \mathcal{G}) \leqslant_T \operatorname{Holant}(\neq_2|=_k, \mathcal{G})$ for any complex-valued signature set $\mathcal{G}$.*

证明. The first equivalence is by definition. For the second reduction, we show that $=_{nk}$ can be realized on the LHS by induction on n. First, we connect one variable of each of k copies of $\neq_2$ on the LHS with the k variables of $=_k$ on the RHS (Figure 3a). This gadget realizes $=_k$ on the LHS.

Then, suppose that $=_{nk}$ is realizable on the LHS. We take one copy of $=_{nk}$ and two copies of $=_k$ on the LHS, and one copy of $=_k$ on the RHS. Remember that $k \geqslant 3$. We connect two variables of $=_k$ on the RHS with one variable of each of the two copies of $=_k$ on the LHS, and connect the other $k-2$ variables of $=_k$ on the RHS with $k-2$ variables of $=_{nk}$ on the LHS (Figure 3b). This gadget realizes $=_{(n+1)k}$ on the LHS.

Also, connecting $k-1$ variables of one copy of $=_k$ on the RHS with $k-1$ variables of another copy of $=_k$ on the RHS using $\neq_2$ on the LHS realizes $\neq_2$ on the RHS. □

Then, we give a dichotomy of $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ for any set $\mathcal{G}$ of complex-valued signatures. Let $\rho = e^{\frac{\mathfrak{i}\pi}{2k}}$ be a $4k$-th primitive root of unity, $T_k = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho \end{smallmatrix}\right]$, and $\mathscr{A}_k^d = T_k^d \mathscr{A}$ for some $d \in [k]$.

Theorem 5.5. *Let $\mathcal{G}$ be a set of complex-valued signatures. $\#\mathrm{CSP}_k(\mathcal{G}, \neq_2)$ is #P-hard unless*

- *$\mathcal{G} \subseteq \mathscr{P}$, or*

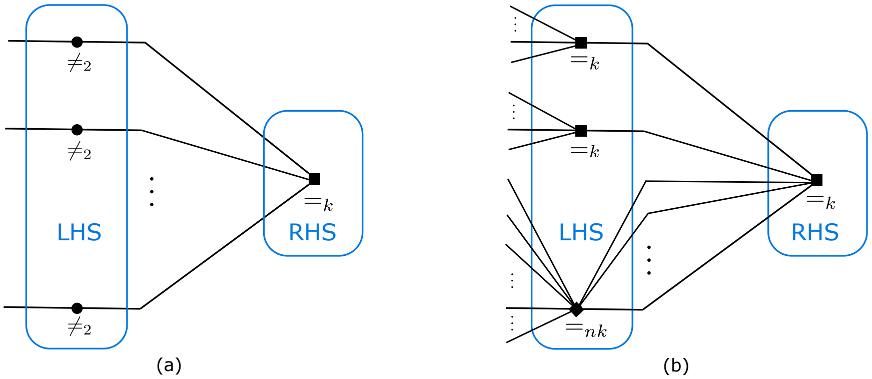


图 3: Gadgets realizing $=_k$ and $=_{(n+1)k}$ on the LHS

- *there exists $d \in [k]$ such that $\mathcal{G} \subseteq \mathscr{A}_k^d$,*

in which cases the problem is tractable.

Before we prove this theorem, we first show that how it gives the #P-hardness of $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$ when $\mathcal{F}$ does not satisfy condition (T).

Corollary 5.6. *Let $\mathcal{F}$ be a set of real-valued signatures. If $\mathcal{F}$ does not satisfy condition* (T)*, then* $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$ *is #P-hard for any $k \geqslant 3$.*

证明. We first prove $\widehat{\mathcal{F}} \not\subseteq \mathscr{P}$ and $\widehat{\mathcal{F}} \not\subseteq \mathscr{A}_k^d$ for any $d \in [k]$ by contraction. If $\widehat{\mathcal{F}} \subseteq \mathscr{P}$, then since $\neq_2 \in \mathscr{P}$, $\mathcal{F}$ is $\mathscr{P}$-transformation. Thus, $\mathcal{F}$ satisfies condition (T). A contradiction. Also, if $\widehat{\mathcal{F}} \subseteq \mathscr{A}_k^d$ for some $d \in [k]$, then since $(T_k^d)^{-1}(\neq_2) = (\neq_2) \in \mathscr{A}$, $\mathcal{F}$ is $\mathscr{A}$-transformation. Still a contradiction.

By Lemma 5.4, $\#\mathrm{CSP}_k(\neq_2, \widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$. By Theorem 5.5, $\#\mathrm{CSP}_k(\neq_2, \widehat{\mathcal{F}})$ is #P-hard. Thus, $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$ is #P-hard. □

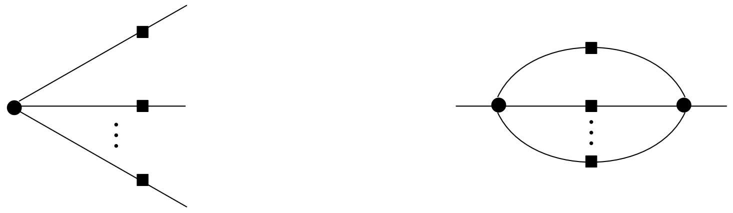
Now, we prove Theorem 5.5. For $k = 1$ or 2, Theorem 5.5 follows from Theorems 2.12 and 2.14 (note that $(\neq_2) \notin \mathscr{L}$). We only need to consider the case that $k \geqslant 3$. Let $\alpha = e^{\frac{\mathfrak{i}\pi}{4}}$ and $\beta = e^{\frac{\mathfrak{i}\pi}{8}}$. Below without other specification, we use ρ to denote a primitive root of unity. Also, we use $[x, 0, \cdots, 0, y]_r$ to denote a general equality signature f of arity r where $f(\vec{0}^r) = a, f(\vec{1}^r) = b$ and f equals 0 otherwise.

Note that

$$\#\,\mathrm{CSP}_k(\neq_2, \mathcal{G}) \equiv_T \operatorname{Holant}(\mathcal{E}Q_k| \neq_2, \mathcal{G}).$$

Moreover, by the following two gadgets, we have $(\neq_2), \mathcal{E}Q_k$ on both sides in $\operatorname{Holant}(\mathcal{E}Q_k| \neq_2, \mathcal{G})$, i.e.,

$$\#\operatorname{CSP}_k(\neq_2, \mathcal{G}) \equiv \operatorname{Holant}(\mathcal{E}Q_k, \neq_2 |\mathcal{E}Q_k, \neq_2, \mathcal{G}). \tag{5.1}$$



(a) Realizing $(=_{nk})$ on RHS (b) Realizing $(\neq_2)$ on LHS

图 4: The squares and circles are labeled by $(\neq_2)$ and $(=_{nk})$ respectively.

The following two lemmas show that in $\#\operatorname{CSP}_k(\neq_2, \mathcal{G})$ the pinning signatures $[1,0]$ and $[0,1]$ are freely available. The first lemma is from [45]. It shows that we have $[1,0]^{\otimes k}, [0,1]^{\otimes k}$ freely in $\#\operatorname{CSP}_k(\mathcal{G})$.

Lemma 5.7. *Let $\mathcal{G}$ be a signature set, then we have*

$$\#\operatorname{CSP}_k(\mathcal{G}, [1,0]^{\otimes k}, [0,1]^{\otimes k}) \le_T \#\operatorname{CSP}_k(\mathcal{G}).$$

The second lemma is from [57]. It shows that we can remove the tensor power of $[1,0]^{\otimes k}, [0,1]^{\otimes k}$ in Lemma 5.7.

Lemma 5.8. *Let $\mathcal{G}$ be a signature set, then we have*

$$\#\operatorname{CSP}_k(\mathcal{G}, [1,0], [0,1]) \le_T \#\operatorname{CSP}_k(\mathcal{G}, [1,0]^{\otimes k}, [0,1]^{\otimes k}).$$

We will prove Theorem 5.5 by induction. If there exists a general equality signature of arity r with $r \nmid k$ in $\mathcal{G}$, then a convenient strategy for induction is allowed as the following lemma shows. Another strategy for induction is presented in Lemma 5.11.

Lemma 5.9. *Let $f = [1, 0, \cdots, 0, a]_r$ with $r \nmid k$ and $a \neq 0$, and $\mathcal{G}$ be a signature set. Then $\#\operatorname{CSP}_k(\mathcal{G}, \neq_2, f)$ is $\#$P-hard except for the following cases*

- *$\mathcal{G} \subseteq \mathscr{P}$;*

- *$\{\mathcal{G}, f\} \subseteq \mathscr{A}_k^d$ for some $d \in [k]$,*

which can be computed in polynomial time.

证明. Note that the lemma has been proved for the cases $k = 1, 2$ by Theorem 2.12 and Theorem 2.14. We will prove the lemma by induction on k in the following. If $r > k$, we can assume that $r = nk + r'$ with $0 < r' < k$. By connecting $(=_{nk})$ to f, we get $[1, 0, \cdots, 0, a]_{r'}$. Thus we can assume that $r < k$ in the following.

Let $k = tr + r_1$ with $0 < r_1 \leq r$. Note that $k > r$, so $t \geq 1$. In $\operatorname{Holant}(\mathcal{EQ}_k, \neq_2 | \mathcal{EQ}_k, \neq_2, f, \mathcal{G})$, connecting ℓt copies of $[1, 0, \cdots, 0, a]_r$ to $(=_{\ell k})$ we get $[1, 0, \cdots, 0, a^{\ell t}]_{\ell r_1}$ on LHS for $\ell = 1, 2, \cdots$, i.e.,

$$\operatorname{Holant}(\mathcal{EQ}_{r_1}^a, \neq_2 | \mathcal{EQ}_k, \neq_2, f, \mathcal{G}) \leq_T \operatorname{Holant}(\mathcal{EQ}_k, \neq_2 | \mathcal{EQ}_k, \neq_2, f, \mathcal{G}),$$

where $\mathcal{EQ}_{r_1}^a = \{[1, 0, \cdots, 0, a^t]_{r_1}, [1, 0, \cdots, 0, a^{2t}]_{2r_1}, \cdots, [1, 0, \cdots, 0, a^{\ell t}]_{\ell r_1}, \cdots\}$. Let $T = \begin{bmatrix} 1 & 0 \\ 0 & a^{\frac{t}{r_1}} \end{bmatrix}$, then $T^{-1}(\mathcal{EQ}_{r_1}^a) = \mathcal{EQ}_{r_1}$. Thus after the holographic transformation using T, we have

$$\operatorname{Holant}(\mathcal{EQ}_{r_1} | T\mathcal{EQ}_k, \neq_2, T^{\otimes r} f, T\mathcal{G}) \leq_T \operatorname{Holant}(\mathcal{EQ}_k, \neq_2 | \mathcal{EQ}_k, \neq_2, f, \mathcal{G}),$$

i.e.,

$$\#\mathrm{CSP}_{r_1}(T\mathcal{EQ}_k, \neq_2, T^{\otimes r} f, T\mathcal{G}) \leq_T \#\mathrm{CSP}_k(\neq_2, f, \mathcal{G}).$$

By induction, if $\{T\mathcal{EQ}_k, T^{\otimes r} f, T\mathcal{G}\} \not\subseteq \mathscr{P}$ and $\{T\mathcal{EQ}_k, T^{\otimes r} f, T\mathcal{G}\} \not\subseteq \mathscr{A}_{r_1}^{d'}$ for any $d' \in [r_1]$, then $\#\mathrm{CSP}_{r_1}(T\mathcal{EQ}_k, \neq_2, T^{\otimes r} f, T\mathcal{G})$ is #P-hard. Thus $\#\mathrm{CSP}_k(\neq_2, f, \mathcal{G})$ is #P-hard.

Otherwise, if $\{T\mathcal{EQ}_k, T^{\otimes r} f, T\mathcal{G}\} \subseteq \mathscr{P}$, then $\mathcal{G} \subseteq \mathscr{P}$ since T is a diagonal matrix. Moreover, if $\{T\mathcal{EQ}_k, T^{\otimes r} f, T\mathcal{G}\} \subseteq \mathscr{A}_{r_1}^{d'}$ for some $d' \in [r_1]$, let $T' = \begin{bmatrix} 1 & 0 \\ 0 & \gamma^{d'} \end{bmatrix}$, where γ is a $4r_1$-th primitive root of unity, i.e., $\gamma^{4r_1} = 1$, then

- $T'^{\otimes k} T^{\otimes k}(=_k) \in \mathscr{A}$,
- $T'^{\otimes r} T^{\otimes r} f \in \mathscr{A}$,
- $T' T\mathcal{G} \subseteq \mathscr{A}$.

Firstly, by $T'^{\otimes k} T^{\otimes k}(=_k) \in \mathscr{A}$, we have $(\gamma^{d'k} a^{\frac{kt}{r_1}})^4 = 1$. This implies that $\gamma^{d'} a^{\frac{t}{r_1}}$ is a $4k$-th root of unity, i.e., there exists $d \in [k]$ such that $\gamma^{d'} a^{\frac{t}{r_1}} = \rho^d$, then $T'T = \begin{bmatrix} 1 & 0 \\ 0 & \rho^d \end{bmatrix}$. Thus $\mathcal{G} \subseteq \mathscr{A}_k^d$ and $f \in \mathscr{A}_k^d$. This finishes the proof. □

Definition 5.10. *Let $f = (f_{i_1 i_2 \cdots i_n}), g = (g_{i_1 i_2 \cdots i_n})$ be two n-ary signatures, then fg is an n-ary signature and $(fg)_{i_1 i_2 \cdots i_n} = f_{i_1 i_2 \cdots i_n} g_{i_1 i_2 \cdots i_n}$ for any $i_1 i_2 \cdots i_n \in \{0,1\}^n$. In particular, $f^k = (f^k_{i_1 i_2 \cdots i_n})$, and for a signature set $\mathcal{G}$, $\mathcal{G}^k = \{f^k | f \in \mathcal{G}\}$.*

The operation in Definition 5.10 is the main tool to do the induction in the proof of Theorem 5.5. More precisely, the following lemma shows that if $f = f_1 f_2 \cdots f_{k'}$ for some $k'|k$, then we can simulate $\#\operatorname{CSP}_{\frac{k}{k'}}(\neq_2, f)$ by $\#\operatorname{CSP}_k(\neq_2, f_1, f_2, \cdots, f_{k'})$. If $f \notin \mathscr{P}$ and $f \notin \mathscr{A}^{d'}_{\frac{k}{k'}}$ for any $d' \in [\frac{k}{k'}]$, then by induction, $\#\operatorname{CSP}_{\frac{k}{k'}}(\neq_2, f)$ is #P-hard. Thus $\#\operatorname{CSP}_k(\neq_2, f_1, f_2, \cdots, f_{k'})$ is #P-hard.

Lemma 5.11. *Let $\mathcal{G}$ be a signature set. Signatures $f_1, f_2, \cdots, f_{k'}$ have the same arity and $f = f_1 f_2 \cdots f_{k'}$, where $k'|k$, then*

$$\#\operatorname{CSP}_{\frac{k}{k'}}(f, \mathcal{G}^{k'}) \leq_T \#\operatorname{CSP}_k(f_1, f_2, \cdots, f_{k'}, \mathcal{G}).$$

证明. In an instance of $\#\operatorname{CSP}_{\frac{k}{k'}}(f, \mathcal{G}^{k'})$, by expanding each variable x to k' copies of x, at the same time replacing each $h^{k'} \in \mathcal{G}^{k'}$ by k' copies of h, and replacing f by $f_1, f_2, \cdots, f_{k'}$, we get an instance of $\#\operatorname{CSP}_k(f_1, f_2, \cdots, f_{k'}, \mathcal{G})$ and its value is same as the value of the instance of $\#\operatorname{CSP}_{\frac{k}{k'}}(f, \mathcal{G}^{k'})$. This finishes the proof. □

By Lemma 5.11, we have

$$\#\operatorname{CSP}(f^k) \leq_T \#\operatorname{CSP}_k(f).$$

If $f^k \notin \mathscr{A}$ and $f^k \notin \mathscr{P}$, by Theorem 2.12, $\#\operatorname{CSP}(f^k)$ is #P-hard. Thus $\#\operatorname{CSP}_k(f)$ is #P-hard and we finish the proof of Theorem 5.5. So in the following, we assume that

$$f^k \in \mathscr{A} \text{ or } f^k \in \mathscr{P} \text{ for each } f \in \mathcal{G}.$$

In particular, the support of f is affine (f^k has the same support as f).

Now we give some definitions for a signature f with affine support.

Definition 5.12. *If f has affine support of rank r, and $X = \{x_{j_1}, x_{j_2}, \cdots, x_{j_r}\}$ is a set of free variables, then $\underline{f_X}$ is the compressed signature of f for X such that $\underline{f_X}(x_{j_1}, x_{j_2}, \cdots, x_{j_r}) = f(x_1, x_2, \cdots, x_n)$, where $(x_1 x_2 \cdots x_n)$ is in the support of f. When it is clear from the context, we omit X and use $\underline{f}$ to denote $\underline{f_X}$.*

Note that if f has affine support, then $f \in \mathscr{A}$ iff $\underline{f} \in \mathscr{A}$.

Definition 5.13. *Suppose f has affine support of rank r with $\{x_1, x_2, \cdots, x_r\}$ as a set of free variables. We use all non-empty combinations $\sum_{j=1}^{r} a_j x_j (a_j \in \mathbb{Z}_2$, not all zero) of $x_1, x_2, \cdots, x_r$ as the names of bundles of f. The type of each bundle is a possibly empty multiset of " $+$ " and " $-$ ", and is defined as follows: For every input variable $x_k (1 \le k \le n)$ of f there is a unique bundle named $\sum_{j=1}^{r} a_j x_j$ such that on the support of f, x_k is either always equal to $\sum_{j=1}^{r} a_j x_j \pmod 2$ or always equal to $\sum_{j=1}^{r} a_j x_j + 1 \pmod 2$. In the former case we add a " $+$ ", and in the latter case we add a " $-$ " to the bundle type for the bundle named $\sum_{j=1}^{r} a_j x_j$, and we say the variable x_k belong to this bundle. All input variables are partitioned into bundles.*

If there exists a set of free variables, without loss of generality, assume that it is $\{x_1, x_2, \cdots, x_r\}$, such that all the bundles have type "+", i.e.,

$$f(x_1(\underbrace{+ + \cdots +}_{n_1})x_2(\underbrace{+ + \cdots +}_{n_2}) \cdots (x_1 + x_2 + \cdots + x_r)(\underbrace{+ + \cdots +}_{n_{12\cdots r}})),$$

where $n_1 + n_2 + \cdots + n_{12\cdots r} = n$, then we say f is monotone and denote its support by

$$(x_1)_{n_1}(x_2)_{n_2} \cdots (x_r)_{n_r}(x_1 + x_2)_{n_{12}} \cdots (x_1 + x_2 + \cdots + x_r)_{n_{12\cdots r}}.$$

If the number of variables in each bundle is a multiple of ℓ for some integer ℓ, then we say f has the ℓ-type support.

Definition 5.14. *, Connecting one variable x_i of a signature to $(=_k)$ using $(\neq_2)$, is equivalent to replace x_i by $(k-1)$ copies of $\bar{x}_i$. We call this operation to be $(k-1)$-*multiple.

If the variables in the same bundle is greater than k, by connecting k variables in this bundle to $(=_k)$, we make these k variables disappear and keep the compressed signature of f unchanged. We call this operation to be collation.

Lemma 5.15. *Let f be a signature of affine support. By doing the operation $(k-1)$-multiple or collation to f we get a new signature g, then $f \in \mathscr{P}$ iff $g \in \mathscr{P}$; $f \in \mathscr{A}_k^d$ iff $g \in \mathscr{A}_k^d$ for any $d \in [k]$.*

证明. We prove the lemma for $(k-1)$-multiple operation to $f \in \mathscr{A}_k^d$ for some $d \in [k]$. Other cases are similar and we omit them here. Note that $(\neq_2) \in \mathscr{A}_k^d$ and $(=_k) \in \mathscr{A}_k^d$ for each $d \in [k]$. Thus

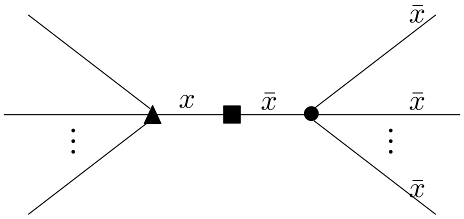


图 5: Transforming the variable x to $k-1$ copies of $\bar{x}$ by connecting $(=_k)$ using $(\neq_2)$. The triangle, square and bullet are labeled by f, $(\neq_2)$ and $(=_k)$ respectively.

if $f \in \mathscr{A}_k^d$ for some d, then $g \in \mathscr{A}_k^d$ by the closure of $\mathscr{A}$. Conversely, note that the variable x of f which is connected to $(=_k)$ using $(\neq_2)$ is flipped into $(k-1)$ copies of $\bar{x}$ in g. By connecting these $(k-1)$ copies of $\bar{x}$ to $(=_k)$ using $(k-1)$ copies of $(\neq_2)$, we get f' that is same as f. Thus if $g \in \mathscr{A}_k^d$, then $f' \in \mathscr{A}_k^d$ and so does f. □

By Lemma 5.15, we can flip the variable $\bar{x}$ to x in the support of f and keep whether f is in the tractable class or not. So in the following we can assume that all the signatures are monotone.

To use Lemma 5.11, we need to construct non-product signature and non-affine signature which is the product $f_1 f_2 \cdots f_{k'}$. Firstly we do this for the non-product case.

By the definition of $\mathscr{P}$, every signature $f \in \mathscr{P}$ has a decomposition as a product of signatures over disjoint of variables, where each factor has support contained in a pair of antipodal points: There exists a partition $X = \{x_1, x_2, \cdots, x_n\} = \bigcup_{j=1}^{\ell} X_j$, and a signature f_j on X_j such that $f(X) = \prod_{j=1}^{\ell} f_j(X_j)$, and for all $1 \leq j \leq \ell$, the support of f_j is contained in $\{\alpha_j, \bar{\alpha_j}\}$ for some $\alpha_j \in \{0,1\}^{|X_j|}$.

The proof of the following lemma totally follows the the proof of Lemma 4.8 and Lemma 4.9 of [32]. We just generalize it from $k=2$ to general k.

Lemma 5.16. *For any $k' \mid k$, if there exists $f \in \mathcal{G}$ such that $f \notin \mathscr{P}$ but $f^{k'} \in \mathscr{P}$, then we can construct $h_1, h_2, \cdots, h_{k'}$ in $\#\operatorname{CSP}_k(\mathcal{G})$, such that $h = h_1 h_2 \cdots h_{k'} \notin \mathscr{P}$.*

证明. Since $[1,0]$ and $[0,1]$ are freely available in $\#\mathrm{CSP}_k(\mathcal{G})$ by Lemma 5.8 and Lemma 5.7, just replacing 2 by k in the proof of Lemma 4.8 and Lemma 4.9 of [32], we can construct a rank-2 signature g from f in $\#\operatorname{CSP}_k(\mathcal{G})$ such that g has the support $(x_1)_{k_1}(x_2)_{k_2}$ and $\underline{g} = (1, a, b, -ab)$ up to a nonzero scalar, where $ab \neq 0$. By pinning all the $x_2 = 0$, we get a signature u_1 which has the support $(x_1)_{k_1}$ and $\underline{u_1} = (1, a)$, and by pinning all the $x_1 = 0$, we get a signature u_2 which has the support $(x_2)_{k_2}$ and $\underline{u_2} = (1, b)$. Let $u = u_1 \otimes u_2$ and $h_1 = g, h_2 = \cdots = h_{k'} = u$, then $h = h_1 h_2 \cdots h_{k'}$ has the compressed signature $(1, a^{k'}, b^{k'}, -a^{k'} b^{k'})$ that is not in $\mathscr{P}$. □

Let $k' = k$ in Lemma 5.11. If $\mathcal{G} \nsubseteq \mathscr{P}$, by Lemma 5.11 and Lemma 5.16, we have

$$\#\operatorname{CSP}(h, \neq_2, \mathcal{G}^k) \leq \#\operatorname{CSP}_k(\neq_2, \mathcal{G}),$$

where $h \notin \mathscr{P}$. If $\mathcal{G}^k \nsubseteq \mathscr{A}$, then $\#\operatorname{CSP}(h, \neq_2, \mathcal{G}^k)$ is #P-hard by Theorem 2.12. This implies that $\#\operatorname{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard. So in the following, we assume that $\mathcal{G}^k \subseteq \mathscr{A}$. Thus we can assume that the compressed signature

$$\underline{f}(x_1, x_2, \cdots, x_r) = \rho^{\sum_{i=1}^{r} a_i x_i + 2\sum_{1 \leq j < k \leq r} a_{jk} x_j x_k + 4H(x_1, x_2, \cdots, x_r)},$$

where $\{x_1, x_2, \cdots, x_r\}$ is a set of free variables and all the monomials in $H(x_1, x_2, \cdots, x_r)$ have degree at least 3.

In the following, we will construct non-affine signature which is the product $f_1 f_2 \cdots f_{k'}$ in $\#\operatorname{CSP}_k(\neq_2, \mathcal{G})$ if $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$. The main idea is to simplify the form of signatures in $\mathcal{G}$ and keep it not contained by $\mathscr{A}_k^d$ for any $d \in [k]$. The following lemma is to reduce the rank of the signatures to at most 3.

Lemma 5.17. *Let $\mathcal{G}$ be a signature set and $f \in \mathcal{G}$ is not in $\mathscr{A}_k^d$ for some $d \in [k]$, then we can construct g in $\#\operatorname{CSP}_k(\neq_2, \mathcal{G})$ such that $g \notin \mathscr{A}_k^d$ and g has rank at most 3, i.e.,*

$$\#\operatorname{CSP}_k(\neq_2, g, \mathcal{G}) \leq_T \#\operatorname{CSP}_k(\neq_2\, \mathcal{G}).$$

证明. Note that $[1, 0], [0, 1]$ are freely available. Without loss of generality, assume that $\{x_1, x_2, \cdots, x_r\}$ is a set of free variables of f. We can assume that the compressed signature

$$\underline{f}(x_1, x_2, \cdots, x_r) = \rho^{Q(x_1, x_2, \cdots, x_r)}$$

up to a nonzero scalar by $f^k \in \mathscr{A}$, where $Q(x_1, x_2, \cdots, x_r)$ is a multilinear polynomial. By the holographic transformation using $T_k^d = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho^d \end{smallmatrix}\right]$, we have

$$\operatorname{Holant}(E_k^d| \neq_2, \widehat{f}, \widehat{\mathcal{G}}, [1,0], [0,1]) \equiv_T \#\operatorname{CSP}_k(\neq_2, f, \mathcal{G}, [1,0], [0,1]),$$

where $\widehat{f} = (T_k^d)^{\otimes arity(f)} f$, $\widehat{\mathcal{G}} = T_k^d \mathcal{G}$, and $E_k^d = \mathcal{EQ}_k (T_k^d)^{-1}$. Since $f \notin \mathscr{A}_k^d$, we have $\widehat{f} \notin \mathscr{A}$. Note that $\widehat{f}$ has the same support as f. The ratio of $f(x_1, x_2, \cdots, x_n)$ and $\widehat{f}(x_1, x_2, \cdots, x_n)$ is a power of ρ for any $(x_1 x_2 \cdots x_n)$ in the support of f. Thus there exists a multilinear polynomial $\widehat{Q}(x_1, x_2, \cdots, x_r)$ such that the compressed signature $\underline{\widehat{f}}(x_1, x_2, \cdots, x_r) = \rho^{\widehat{Q}(x_1, x_2, \cdots, x_r)}$. Assume that

$$\hat{Q}(x_1, x_2, \cdots, x_r) = \sum_{1 \le i \le r} \hat{a}_i x_i + \sum_{1 \le j < \ell \le r} \hat{a}_{j\ell} x_j x_\ell + P(x_1, x_2, \cdots, x_r), \tag{5.2}$$

where $P(x_1, x_2, \cdots, x_r)$ is a polynomial and all the terms have power at least 3. In (5.2),

- If there exists $\hat{a}_i \not\equiv 0 \pmod{k}$, we pin all free variables to 0 by $[1,0]$ except x_i, then we get a rank-1 signature that is not in $\mathscr{A}$.

- If there exists $\hat{a}_{j\ell} \not\equiv 0 \pmod{2k}$, we pin all free variables to 0 by $[1,0]$ except x_j, x_ℓ, then we get a rank-2 signature that is not in $\mathscr{A}$.

- Finally, if $P(x_1, x_2, \cdots, x_r) \not\equiv 0 \pmod{4k}$, suppose the monomial M has the minimum degree, among all monomials in P whose coefficient that is nonzero modulo $4k$. We pin all free variables which are not in M to 0 by $[1,0]$ and pin the variables in M to 1 by $[0,1]$ except 3 of them, then we get a rank-3 signature that is not in $\mathscr{A}$.

If $\hat{a}_i \equiv 0 \pmod{k}$, $\hat{a}_{j\ell} \equiv 0 \pmod{2k}$ for all $\hat{a}_i$ and $\hat{a}_{j\ell}$, and $P(x_1, x_2, \cdots, x_r) \equiv 0 \pmod{4k}$, then $\widehat{f} \in \mathscr{A}$. This is a contradiction. In total, we always can get a non-affine signature of degree at most 3 in $\operatorname{Holant}(E_k^d| \neq_2, \widehat{f}, \widehat{\mathcal{G}}, [1,0], [0,1])$. This implies that we can get a signature $g \notin \mathscr{A}_k^d$ of degree at most 3 in $\#\operatorname{CSP}_k(\neq_2, f, \mathcal{G}, [1,0], [0,1])$. This finishes the proof. □

By Lemma 5.17, we just need to focus on the signatures with arity less than 4.

Lemma 5.18. *If f has k-type support and $f \notin \mathscr{A}_k^{d_0}$ for some $d_0 \in [k]$, then $f \notin \mathscr{A}_k^d$ for any $d \in [k]$.*

证明. Let $\{x_1, x_2, \cdots, x_r\}$ be a set of free variables. We can assume that f has the support $(x_1)_{\ell_1 k} (x_2)_{\ell_2 k} \cdots (x_n)_{\ell_n k}$ since f has k-type support, and $x_i = \sum_{j=1}^r a_{ij} x_j$ for $1 \le i \le n$. Let

$\widehat{f} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho^{d_0} \end{smallmatrix}\right]^{arity(f)} f$, then

$$\widehat{f} = \rho^{d_0 k \sum_{i=1}^{n} \ell_i x_i} f = \mathfrak{i}^{d_0 \sum_{i=1}^{n} \ell_i x_i} f.$$

In the power of $\mathfrak{i}$, by $z \equiv 0 \pmod 2$ (respectively $1 \mod 2$) iff $z^2 \equiv 0 \mod 4$ (respectively $1 \mod 4$), we can substitute x_i by $(\sum_{j=1}^{r} a_{ij} x_j)^2$, i.e.,

$$\underline{\widehat{f}} = \mathfrak{i}^{d_0 \sum_{i=1}^{n} \ell_i (\sum_{j=1}^{r} a_{ij} x_j)^2} \underline{f}.$$

Note that $(\sum_{j=1}^{r} a_{ij} x_j)^2$ is a quadratic polynomial and the coefficients of the cross terms are even. By $\underline{\widehat{f}} \notin \mathscr{A}$, we have $\underline{f} \notin \mathscr{A}$. Then for any $d \in [k]$, let $\widehat{f'} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho^{d} \end{smallmatrix}\right]^{\otimes arity(f)} f$, we have

$$\underline{\widehat{f'}} = \rho^{dk \sum_{i=1}^{n} \ell_i x_i} \underline{f} = \mathfrak{i}^{d \sum_{i=1}^{n} \ell_i (\sum_{j=1}^{r} a_{ij} x_j)^2} \underline{f},$$

which is not in $\mathscr{A}$. □

Assume that f has the k-type support. Note that if $f \notin \mathscr{A}$, then $f \notin \mathscr{A}_k^d$ for $d = k$. Then by Lemma 5.18, $f \notin \mathscr{A}_k^d$ for any $d \in [k]$.

Lemma 5.19. *Let $\mathcal{G}$ be a signature set. If $\mathcal{G} \nsubseteq \mathscr{P}$ and contains a signature $f \notin \mathscr{A}_d^k$ for some $d \in [k]$ which has k-type support, then $\#\mathrm{CSP}_k(\mathcal{G})$ is #P-hard.*

证明. Since $\mathcal{G} \nsubseteq \mathscr{P}$, there exist some signature in $\mathcal{G}$ which is not in $\mathscr{P}$. Then by Lemma 5.16, we can construct $h_1, h_2, \cdots, h_k$ such that $h = h_1 h_2 \cdots h_k \notin \mathscr{P}$. Moreover, since $f \notin \mathscr{A}_d^k$ for some $d \in [k]$, by Lemma 5.18, we have $f \notin \mathscr{A}$. Assume that f has the support $(x_1)_{d_1 k} (x_2)_{d_2 k} \cdots (x_1 + x_2 + \cdots + x_r)_{d_{12\cdots r} k}$. Let $u = (=_{d_1 k}) \otimes (=_{d_2 k}) \otimes \cdots \otimes (=_{d_{12\cdots r} k})$ and $f' = \underbrace{u u \cdots u}_{k-1} f$. Note that f' is identical to f. Thus $f' \notin \mathscr{A}$. By Lemma 5.11, we have

$$\#\,\mathrm{CSP}(h, f') \leq_T \#\,\mathrm{CSP}_k(\mathcal{G}).$$

Since $\{h, f'\} \nsubseteq \mathscr{A}, \mathscr{P}$, by Theorem 2.12, $\#\,\mathrm{CSP}(h, f')$ is #P-hard. Thus $\#\,\mathrm{CSP}_k(\mathcal{G})$ is #P-hard. □

The following lemma shows that if $\mathcal{G}$ contains a rank-2 signature f, then its support and compressed signature has to be of some special form. This is a key point in the proof of Lemma 5.24.

Lemma 5.20. *Let $\mathcal{G}$ be a signature set which contains a rank-2 signature $f \notin \mathscr{A}_k^d$ for some $d \in [k]$, then we have*

- *$\mathcal{G} \subseteq \mathscr{P}$,*
- *or $\mathcal{G} \subseteq \mathscr{A}_k^d$ for some $d \in [k]$,*
- *or $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard;*

otherwise f has the support $(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}$ after collation and the compressed signature is

$$\underline{f}(x_1, x_2) = \mathfrak{i}^{b_1x_1+b_2x_2+b_{12}x_1x_2}.$$

证明. Since f has rank 2, we can assume that f has the support $(x_1)_{k_1}(x_2)_{k_2}(x_1+x_2)_{k_{12}}$. By pinning $x_1 = 0$, we have a rank-1 signature f_1 which has the support $(x_2)_{k_2+k_{12}}$, i.e., $f_1 = [f_1(0,0,\cdots,0), 0, \cdots, 0, f_1(1,1,\cdots,1)]$, where $f_1(0,0,\cdots,0) = \underline{f}(0,0)$ and $f_1(1,1,\cdots,1) = \underline{f}(0,1)$ are both nonzero. Thus up to a scalar, we can assume that $f_1 = [1,0,\cdots,0,x]$ with $x \neq 0$. If $k_2 + k_{12} \not\equiv 0 \pmod{k}$, then we are done by Lemma 5.9. Thus we have

$$k_2 + k_{12} \equiv 0 \pmod{k}. \tag{5.3}$$

Then by pinning $x_2 = 0$, $x_1 + x_2 = 0$ respectively and by the similar argument, we have

$$\begin{aligned} k_1 + k_{12} \equiv 0 \pmod{k}, \\ k_1 + k_2 \equiv 0 \pmod{k}. \end{aligned} \tag{5.4}$$

By (5.3) and the first equation of (5.4), we have $k_1 \equiv k_2 \pmod{k}$. Then by the second equation of (5.4), we have $2k_1 \equiv 0 \pmod{k}$. This implies that $k_1 \equiv 0 \pmod{k}$ or $k_1 \equiv \frac{k}{2} \pmod{k}$. So we have

$$k_1 \equiv k_2 \equiv k_{12} \equiv 0 \pmod{k}, \quad \text{or} \quad k_1 \equiv k_2 \equiv k_{12} \equiv \frac{k}{2} \pmod{k}.$$

If $k_1 \equiv k_2 \equiv k_{12} \equiv 0 \pmod{k}$, then $\mathcal{G} \subseteq \mathscr{P}$ or $\#\mathrm{CSP}(\neq_2, \mathcal{G})$ is #P-hard by Lemma 5.19.

Now we can assume that f has the support $(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}$ after collation. Assume that

$$\underline{f}(x_1, x_2) = \rho^{b'_1x_1+b'_2x_2+b'_{12}x_1x_2}$$

up to a scalar. By pinning $x_2 = 0$ to f, we get the signature $[1, 0, \cdots, 0, \rho^{b'_1}]_k$. If $b'_1 \not\equiv 0 \pmod{k}$, then $[1, 0, \cdots, 0, \rho^{b'_1}] \notin \mathscr{A}$. Note that $[1, 0, \cdots, 0, \rho^{b'_1}]_k$ has the k-type support. Again we have $\mathcal{G} \subseteq \mathscr{P}$ or $\#\mathrm{CSP}(\neq_2, \mathcal{G})$ is #P-hard by Lemma 5.19. Otherwise, we have $b'_1 \equiv 0 \pmod{k}$. Moreover, by pinning $x_2 = 0, x_1 + x_2 = 0$ and using the same argument, we have $b'_2 \equiv 0 \pmod{k}$ and $b'_{12} \equiv 0 \pmod{k}$ respectively. So we have

$$\underline{f}(x_1, x_2) = \mathfrak{i}^{b_1 x_1 + b_2 x_2 + b_{12} x_1 x_2},$$

where b_1, b_2 and b_{12} are integers. □

The following lemma shows that if $\mathcal{G}$ contains a rank-3 signature, then it has special support. This can simplify the proof of Lemma 5.24 greatly.

Lemma 5.21. *Let $\mathcal{G}$ be a signature set which contains a rank-3 signature f, then*

- *$\mathcal{G} \subseteq \mathscr{P}$,*
- *or $\mathcal{G} \subseteq \mathscr{A}_d^k$ for some $d \in [k]$,*
- *or $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard;*

otherwise f has one of the following support after collation:

$$(x_1)_{\epsilon_1 k}(x_2)_{\epsilon_2 k}(x_3)_{\epsilon_3 k}(x_1 + x_2)_{\epsilon_{12} k}(x_1 + x_3)_{\epsilon_{13} k}(x_2 + x_3)_{\epsilon_{23} k}(x_1 + x_2 + x_3)_{\epsilon_{123} k}, \tag{5.5}$$

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}}(x_1 + x_3)_{\frac{k}{2}}(x_2 + x_3)_{\frac{k}{2}}(x_1 + x_2 + x_3)_{\frac{k}{2}}, \tag{5.6}$$

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1 + x_2)_{\epsilon_{12} k}(x_1 + x_3)_{\epsilon_{13} k}(x_2 + x_3)_{\epsilon_{23} k}(x_1 + x_2 + x_3)_{\frac{k}{2}}, \tag{5.7}$$

$$(x_1)_{\epsilon_1 k}(x_2)_{\epsilon_2 k}(x_3)_{\epsilon_3 k}(x_1 + x_2)_{\frac{k}{2}}(x_1 + x_3)_{\frac{k}{2}}(x_2 + x_3)_{\frac{k}{2}}(x_1 + x_2 + x_3)_{\epsilon_{123} k}, \tag{5.8}$$

$$(x_1)_{\frac{k}{4}}(x_2)_{\frac{k}{4}}(x_3)_{\frac{k}{4}}(x_1 + x_2)_{\frac{k}{4}}(x_1 + x_3)_{\frac{k}{4}}(x_2 + x_3)_{\frac{k}{4}}(x_1 + x_2 + x_3)_{\frac{k}{4}}, \tag{5.9}$$

$$(x_1)_{\frac{k}{4}}(x_2)_{\frac{k}{4}}(x_3)_{\frac{k}{4}}(x_1 + x_2)_{\frac{3k}{4}}(x_1 + x_3)_{\frac{3k}{4}}(x_2 + x_3)_{\frac{3k}{4}}(x_1 + x_2 + x_3)_{\frac{k}{4}}, \tag{5.10}$$

$$(x_1)_{\frac{3k}{4}}(x_2)_{\frac{3k}{4}}(x_3)_{\frac{3k}{4}}(x_1 + x_2)_{\frac{k}{4}}(x_1 + x_3)_{\frac{k}{4}}(x_2 + x_3)_{\frac{k}{4}}(x_1 + x_2 + x_3)_{\frac{3k}{4}}, \tag{5.11}$$

$$(x_1)_{\frac{3k}{4}}(x_2)_{\frac{3k}{4}}(x_3)_{\frac{3k}{4}}(x_1 + x_2)_{\frac{3k}{4}}(x_1 + x_3)_{\frac{3k}{4}}(x_2 + x_3)_{\frac{3k}{4}}(x_1 + x_2 + x_3)_{\frac{3k}{4}}, \tag{5.12}$$

where $\epsilon_i = 0$ or 1. In (5.8), at least one of $\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_{123}\}$ is nonzero. Without loss of generality, we assume that $\epsilon_1 \neq 0$ or $\epsilon_{123} \neq 0$ in (5.8).

证明. Assume that f has the support

$$(x_1)_{k_1}(x_2)_{k_2}(x_3)_{k_3}(x_1+x_2)_{k_{12}}(x_1+x_3)_{k_{13}}(x_2+x_3)_{k_{23}}(x_1+x_2+x_3)_{k_{123}}.$$

By pinning $x_1 = 0, x_2 = 0, x_3 = 0$ to f, we get three signatures which have the support

$$\begin{aligned}&(x_2)_{k_2+k_{12}}(x_3)_{k_3+k_{13}}(x_2+x_3)_{k_{23}+k_{123}},\\&(x_1)_{k_1+k_{12}}(x_3)_{k_3+k_{23}}(x_1+x_3)_{k_{13}+k_{123}},\\&(x_1)_{k_1+k_{13}}(x_2)_{k_2+k_{23}}(x_1+x_2)_{k_{12}+k_{123}}\end{aligned}$$

respectively. By (5.3) and (5.4) in the proof of Lemma 5.20, if we have a rank-2 signature whose support is not $\frac{k}{2}$-type, then we can construct a rank-1 signature whose support is not k-type, and we can finish the proof by Lemma 5.9. Otherwise we have

$$\begin{aligned}k_2+k_{12} \equiv k_3+k_{13} \equiv k_{23}+k_{123} \equiv 0 \pmod{\frac{k}{2}},\\k_1+k_{12} \equiv k_3+k_{23} \equiv k_{13}+k_{123} \equiv 0 \pmod{\frac{k}{2}},\\k_1+k_{13} \equiv k_2+k_{23} \equiv k_{12}+k_{123} \equiv 0 \pmod{\frac{k}{2}}.\end{aligned} \tag{5.13}$$

By (5.13) we have

$$k_1 \equiv k_2 \equiv k_3 \equiv k_{123} \equiv -k_{12} \equiv -k_{13} \equiv -k_{23} \pmod{\frac{k}{2}}. \tag{5.14}$$

Moreover, by pinning $x_1 + x_2 = 0$, we get the signature which has the support

$$(x_1)_{k_1+k_2}(x_3)_{k_3+k_{123}}(x_1+x_3)_{k_{13}+k_{23}}$$

and we have

$$k_1+k_2 \equiv k_3+k_{123} \equiv k_{13}+k_{23} \equiv 0 \pmod{\frac{k}{2}}. \tag{5.15}$$

Combining (5.14) and (5.15), we have

$$2k_1 \equiv 2k_{12} \equiv 0 \pmod{\frac{k}{2}}.$$

This implies that $k_1, k_{12} \equiv 0, \frac{k}{2}, \frac{k}{4}$ or $\frac{3k}{4} \pmod{k}$. So after collation, by (5.14),

- if $k_1 \equiv k_{12} \equiv 0 \pmod{k}$, then f has the support (5.5);
- if $k_1 \equiv k_{12} \equiv \frac{k}{2} \pmod{k}$, then f has the support (5.6);
- if $k_1 \equiv \frac{k}{2} \pmod{k}, k_{12} \equiv 0 \pmod{k}$, then f has the support (5.7);
- if $k_1 \equiv 0 \pmod{k}, k_{12} \equiv \frac{k}{2} \pmod{k}$, then f has the support (5.8);
- if $k_1 \equiv k_{12} \equiv \frac{k}{4} \pmod{k}$, then f has the support (5.9);
- if $k_1 \equiv \frac{k}{4} \pmod{k}, k_{12} \equiv \frac{3k}{4} \pmod{k}$, then f has the support (5.10);
- if $k_1 \equiv \frac{3k}{4} \pmod{k}, k_{12} \equiv \frac{k}{4} \pmod{k}$, then f has the support (5.11);
- if $k_1 \equiv k_{12} \equiv \frac{3k}{4} \pmod{k}$, then f has the support (5.12).

In (5.8), if all of $\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_{123}\}$ are zero, then f is rank-2. This is a contradiction. Thus we can assume that $\epsilon_1 \neq 0$ or $\epsilon_{123} \neq 0$ without loss of generality. □

Let f, g be two signatures and there are s and t variables in the bundle (x) of f and (y) of g respectively, where $s + t < 2k$. In the following, we often connected the two bundle by $(=_{2k})$ and produces a variable bundle with $2k - s - t$ variables in the constructed signature as Fig 3 shows. We call the operation to be merging variable bundle (x) and (y) by $(=_{2k})$.

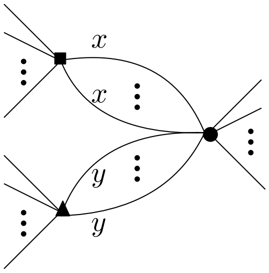


Fig. 3 The square, triangle and bullet is labeled by f, g and $(=_{2k})$ respectively.

For example, if f has the support

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}(x_1+x_3)_{\frac{k}{2}}(x_2+x_3)_{\frac{k}{2}}(x_1+x_2+x_3)_{\frac{k}{2}}$$

and g has the support

$$(y_1)_{\frac{k}{2}}(y_2)_{\frac{k}{2}}(y_1+y_2)_{\frac{k}{2}}.$$

Merging the variable bundle (x_1) and (y_1), (x_2+x_3) and (y_2) using $(=_{2k})$ respectively, produces two new bundle (x'_1) and $(x'_2+x'_3)$ which contain k variables respectively in the constructed signature f'. Moreover, this operation forces $x_1+x_2+x_3=y_1+y_2$. Thus the two bundles $(x_1+x_2+x_3)$, (y_1+y_2) are merged automatically. So f' has the support

$$(x'_1)_k(x'_2)_{\frac{k}{2}}(x'_3)_{\frac{k}{2}}(x'_1+x'_2)_{\frac{k}{2}}(x'_1+x'_3)_{\frac{k}{2}}(x'_2+x'_3)_k(x'_1+x'_2+x'_3)_k,$$

and the compressed signature

$$\underline{f'}(x'_1,x'_2,x'_3)=\underline{g}(x'_1,x'_2+x'_3)\underline{f}(x'_1,x'_2,x'_3). \tag{5.16}$$

For the variables $x_i,x_j,x_k\in\{0,1\}$, note that the variable $(x_i+x_j)\neq x_i+x_j$ and $(x_i+x_j+x_k)\neq x_i+x_j+x_k$ if the computation is not in modulo 2. Thus we use the following two identities

$$(x_i+x_j)=x_i+x_j-2x_ix_j \tag{5.17}$$

and

$$(x_i+x_j+x_k)=x_i+x_j+x_k-2x_ix_j-2x_ix_k-2x_jx_k+4x_ix_jx_k \tag{5.18}$$

when we carry out computation not in modulo 2. For example, in the above example, if f and g have the compressed signatures

$$\underline{f}(x_1,x_2,x_3)=\mathfrak{i}^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+2a_{123}x_1x_2x_3}. \tag{5.19}$$

and

$$\underline{g}(y_1,y_2)=\mathfrak{i}^{b_1y_1+b_2y_2+b_{12}y_1y_2} \tag{5.20}$$

respectively, then f' has the compressed signature

$$\underline{f'}(x'_1, x'_2, x'_3) = \mathfrak{i}^{a_1x'_1+a_2x'_2+a_3x'_3+2a_{12}x'_1x'_2+2a_{13}x'_1x'_3+2a_{23}x'_2x'_3+2a_{123}x'_1x'_2x'_3+b_1x'_1+b_2[x'_2+x'_3]+b_{12}x'_1[x'_2+x'_3]}.$$

In the power of $\mathfrak{i}$, the computation is modulo 4. So the variable $[x'_2 + x'_3] \neq x'_2 + x'_3$ and we use (5.17), i.e.,

$$\underline{f'} = \mathfrak{i}^{a_1x'_1+a_2x'_2+a_3x'_3+2a_{12}x'_1x'_2+2a_{13}x'_1x'_3+2a_{23}x'_2x'_3+2a_{123}x'_1x'_2x'_3+b_1x'_1+b_2(x'_2+x'_3-2x'_2x'_3)+b_{12}x'_1(x'_2+x'_3-2x'_2x'_3)}.$$

We will use the following result repeatedly in the following proof.

Lemma 5.22. *Let g be a rank-2 signature and f be a rank-3 signature. g has the support*

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}},$$

and the compressed signature

$$\underline{g}(x_1, x_2) = \mathfrak{i}^{b_1x_1+b_2x_2+b_{12}x_1x_2}.$$

f has the support

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}}(x_1 + x_3)_{\frac{k}{2}}(x_2 + x_3)_{\frac{k}{2}}(x_1 + x_2 + x_3)_{\frac{k}{2}},$$

and the compressed signature

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+2a_{123}x_1x_2x_3}.$$

Then

- *if b_{12} is even, then $g \in \mathscr{A}_k^d$ for any even $d \in [k]$ and $g \notin \mathscr{A}_k^d$ for any odd $d \in [k]$;*
- *if b_{12} is odd, then $g \in \mathscr{A}_k^d$ for any odd $d \in [k]$ and $g \notin \mathscr{A}_k^d$ for any even $d \in [k]$.*

And

- *if a_{123} is even, then $f \in \mathscr{A}_k^d$ for any even $d \in [k]$ and $f \notin \mathscr{A}_k^d$ for any odd $d \in [k]$;*

- *if a_{123} is odd, then $f \in \mathscr{A}_k^d$ for any odd $d \in [k]$ and $f \notin \mathscr{A}_k^d$ for any even $d \in [k]$.*

证明. We prove the lemma for the rank-3 case. The rank-2 case is similar and we omit it here. Let $\widehat{f} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho^d \end{smallmatrix}\right]^{\otimes arity(f)} f$, then

$$\underline{\widehat{f}}(x_1, x_2, x_3) = \rho^{\frac{dk}{2}(x_1+x_2+x_3+[x_1+x_2]+[x_1+x_3]+[x_2+x_3]+[x_1+x_2+x_3])} f(x_1, x_2, x_3),$$

where $[\cdot]$ denotes the corresponding variable. By (5.17), (5.18), we have

$$\underline{\widehat{f}}(x_1, x_2, x_3) = \rho^{\frac{dk}{2}(4x_1+4x_2+4x_3-4x_1x_2-4x_1x_3-4x_2x_3+4x_1x_2x_3)} f(x_1, x_2, x_3),$$

i.e.,

$$\underline{\widehat{f}}(x_1, x_2, x_3) = \mathfrak{i}^{(2d+a_1)x_1+(2d+a_2)x_2+(2d+a_3)x_3+2(a_{12}-d)x_1x_2+2(a_{13}-d)x_1x_3+2(a_{23}-d)x_2x_3+2(a_{123}+d)x_1x_2x_3}.$$

Note that $\widehat{f} \in \mathscr{A}$ iff $d + a_{123}$ is even. This proves the lemma. □

In Lemma 5.22, if b_{12} in g and a_{123} in f have different parity, then $\{g, f\} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$. Note that $g, f \notin \mathscr{P}$. The following lemma shows that $\#\,\mathrm{CSP}_k(f, g)$ is #P-hard. This is an important base case in the proof of Lemma 5.24.

Lemma 5.23. *Let f be a rank-3 signature which has the support*

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}(x_1+x_3)_{\frac{k}{2}}(x_2+x_3)_{\frac{k}{2}}(x_1+x_2+x_3)_{\frac{k}{2}},$$

and the compressed signature

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+2a_{123}x_1x_2x_3},$$

and g be a rank-2 signature which has the support

$$(y_1)_{\frac{k}{2}}(y_2)_{\frac{k}{2}}(y_1+y_2)_{\frac{k}{2}},$$

and the compressed signature

$$\underline{g}(y_1, y_2) = \mathfrak{i}^{b_1 y_1 + b_2 y_2 + b_{12} y_1 y_2},$$

where $a_{123} + b_{12} \equiv 1 \pmod{2}$. *Then* $\#\,\mathrm{CSP}_k(f, g)$ *is #P-hard.*

证明. We take one copy of $f((x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}(x_1+x_3)_{\frac{k}{2}}(x_2+x_3)_{\frac{k}{2}}(x_1+x_2+x_3)_{\frac{k}{2}})$ and one copy of $g((u_1)_{\frac{k}{2}}(u_2)_{\frac{k}{2}}(u_1+u_2)_{\frac{k}{2}})$. Merging the variable bundle (x_1) and (u_1), (x_2+x_3) and (u_2) by $(=_{2k})$, we get the signature f' which has the support

$$(x_1)_k(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}(x_1+x_3)_{\frac{k}{2}}(x_2+x_3)_k(x_1+x_2+x_3)_k$$

and the compressed signature

$$\underline{f'} = \mathfrak{i}^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+2a_{123}x_1x_2x_3+b_1x_1+b_2(x_2+x_3-2x_2x_3)+b_{12}x_1(x_2+x_3-2x_2x_3)}.$$

Note that the coefficient of $x_1x_2x_3$ is $2(a_{123} - b_{12})$ which is 2 modulo 4.

Similarly, we take another two copies of g: $g_1((v_1)_{\frac{k}{2}}(v_2)_{\frac{k}{2}}(v_1+v_2)_{\frac{k}{2}})$, $g_2((w_1)_{\frac{k}{2}}(w_2)_{\frac{k}{2}}(w_1+w_2)_{\frac{k}{2}})$, and merge the variable bundles $(x_2), (x_1+x_3), (x_3), (x_1+x_2)$ of f' to the variable bundles $(v_1), (v_2), (w_1), (w_2)$ of the these two copies of g by $(=_{2k})$ respectively, Then we get a signature f'' which has the support

$$(x_1)_k(x_2)_k(x_3)_k(x_1+x_2)_k(x_1+x_3)_k(x_2+x_3)_k(x_1+x_2+x_3)_{2k},$$

and

$$\underline{f''}(x_1, x_2, x_3) = \mathfrak{i}^{c_1x_1+c_2x_2+c_3x_3+2c_{12}x_1x_2+2c_{13}x_1x_3+2c_{23}x_2x_3+2c_{123}x_1x_2x_3}$$

where $c_{123} = 2(a_{123} - 3b_{12}) \equiv 2 \pmod{4}$. Thus f'' is not in $\mathscr{A}$. Let

$$h = (=_k) \otimes (=_k) \otimes (=_k) \otimes (=_k) \otimes (=_k) \otimes (=_k) \otimes (=_{2k})$$

and $f''' = f''\underbrace{hh\cdots h}_{k-1}$. Then f''' is identical to f', and by Lemma 5.11, we have

$$\#\,\mathrm{CSP}(f''') \le_T \#\,\mathrm{CSP}_k(f'').$$

Since $f'''$is not in $\mathscr{P} \cup \mathscr{A}$, $\#\operatorname{CSP}(f''')$ is #P-hard by Theorem 2.12. Thus $\#\operatorname{CSP}_k(f, g)$ is #P-hard. □

As we have explained, to use Lemma 5.11, we have to construct signatures which is a product of some same-arity signatures and is not in some tractable class. We have done this for non-product signature in Lemma 5.16. The following Lemma is for the non-affine case. Although we prepare a lot from Lemma 5.17 to Lemma 5.23 for it, the proof is still twisted. In the proof, firstly we consider three special signatures which can not produce rank-2 signature by pinning. Afterward, we can assume that there is a rank-2 signature g in hand. With the help of g and Lemma 5.23, we can handle the remaining cases.

Lemma 5.24. *Let $\mathcal{G}$ be a signature set. Each signature in $\mathcal{G}$ has arity less than 4 and is not in $\mathscr{A}_k^{d_0}$ for some $d_0 \in [k]$. If $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$, then we have*

- *$\mathcal{G} \subseteq \mathscr{P}$,*
- *or $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard,*
- *or in $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ we can construct $f_1, f_2, \cdots, f_{k'}$ which have the same arity for some $k' > 1$ and $k'|k$, such that $h = f_1 f_2 \cdots f_{k'}$ is not in $\mathscr{A}_{\frac{k}{k'}}^{d'}$ for any $d' \in [\frac{k}{k'}]$.*

证明. Firstly, we deal with three special cases.

- Case 1: There exists a rank-3 signature $f \in \mathcal{G}$ which has the support (5.5) and $f \notin \mathscr{A}_k^{d_0}$ for some $d_0 \in [k]$, then we are done by Lemma 5.19.
- Case 2: There exists a rank-1 signature $f \in \mathcal{G}$ and $f \notin \mathscr{A}_k^d$ for some $d \in [k]$. If the arity of f is a multiple of k, then we are done by Lemma 5.19. Otherwise, we are done by Lemma 5.9.
- Case 3: All the signatures in $\mathcal{G}$ have the support (5.6). If there exists $f \in \mathcal{G}$ and $f^2 \notin \mathscr{A}$, then we let $h = f^2$. Note that h has the $\frac{k}{2}$-type support and $h \notin \mathscr{A}$. Thus $h \notin \mathscr{A}_{\frac{k}{2}}^{d'}$ for any $d' \in [\frac{k}{2}]$ by Lemma 5.18 and we are done. Otherwise, For any $f \in \mathcal{G}$, we have $f^2 \in \mathscr{A}$ and we can assume that

$$\underline{f}(x_1, x_2, x_3) = \alpha^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+4a_{123}x_1x_2x_3}.$$

By pinning $x_1 = 0$, we have a rank-2 signature g_1 with the support $(x_2)_k(x_3)_k(x_2+x_3)_k$ and

$$\underline{g_1}(x_2, x_3) = \alpha^{a_2x_2+a_3x_3+2a_{23}x_2x_3}.$$

If $g_1 \notin \mathscr{A}$, then we are done by Lemma 5.19. since g_1 has k-type support. Thus we are done by letting $h = g_1$. Otherwise, we have $a_2 \equiv a_3 \equiv a_{23} \equiv 0 \pmod 2$. Moreover, by pinning $x_2 = 0, x_3 = 0$, we have $a_1 \equiv a_2 \equiv a_3 \equiv a_{12} \equiv a_{13} \equiv a_{23} \equiv 0 \pmod 2$. This implies that

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{\frac{a_1}{2}x_1+\frac{a_2}{2}x_2+\frac{a_3}{2}x_3+a_{12}x_1x_2+a_{13}x_1x_3+a_{23}x_2x_3+2a_{123}x_1x_2x_3}.$$

By Lemma 5.22, since $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$, there at least two signatures $f_1, f_2 \in \mathcal{G}$ and

$$\underline{f}_i(x_1, x_2, x_3) = \mathfrak{i}^{a_1^{(i)}x_1+a_2^{(i)}x_2+a_3^{(i)}x_3+2a_{12}^{(i)}x_1x_2+2a_{13}^{(i)}x_1x_3+2a_{23}^{(i)}x_2x_3+2a_{123}^{(i)}x_1x_2x_3}$$

for $i = 1, 2$, where $a_{123}^{(1)}$ is odd and $a_{123}^{(2)}$ is even. Let $h = f_1f_2$, then h has the $\frac{k}{2}$-type support and

$$\underline{h}(x_1, x_2, x_3) = \mathfrak{i}^{\sum_{i=1}^3(\sum_{u=1}^2 a_i^{(u)})x_i+2\sum_{1\le j<k\le 3}(\sum_{u=1}^2 a_{jk}^{(u)})x_jx_k+2(a_{123}^{(1)}+a_{123}^{(2)})x_1x_2x_3}.$$

Since $a_{123}^{(1)} + a_{123}^{(2)}$ is odd, we have $h \notin \mathscr{A}$. Thus $h \notin \mathscr{A}_{\frac{k}{2}}^{d'}$ for any $d' \in [\frac{k}{2}]$ by Lemma 5.18 and we are done.

Other than these three cases, $\mathcal{G}$ contains at least one rank-2 signature or one rank-3 signature of the support (5.7), (5.8), (5.9), (5.10), (5.11) or (5.12), which is not in $\mathscr{A}_k^d$ for some $d \in [k]$.

- If $\mathcal{G}$ contains a rank-3 signature of the support (5.8) with $\epsilon_{123} \neq 0$, we pin $x_1 + x_2 + x_3 = 0$ and get a rank-2 signature which has the support $(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}}$ after collation.
- If $\mathcal{G}$ contains a rank-3 signature of the support (5.8) with $\epsilon_1 \neq 0$, (5.7), (5.9), (5.10), (5.11) or (5.12), by pinning $x_1 = 0$ we get a rank-2 signature which has the support $(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}}$ after collation.

In total, in the following we can construct a rank-2 signature g which has the support $(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1+$

$x_2)_{\frac{k}{2}}$ in $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$. By Lemma 5.20, we can assume that g has the compressed signature

$$\underline{g}(x_1, x_2) = \mathfrak{i}^{b_1x_1+b_2x_2+b_{12}x_1x_2}.$$

By Lemma 5.22,

- if b_{12} is even, then $g \in \mathscr{A}_k^d$ for any even $d \in [k]$ and $g \notin \mathscr{A}_k^d$ for any odd $d \in [k]$;
- if b_{12} is odd, then $g \in \mathscr{A}_k^d$ for any odd $d \in [k]$ and $g \notin \mathscr{A}_k^d$ for any even $d \in [k]$.

We assume that b_{12} is even in the following. After the holographic transformation using $\left[\begin{smallmatrix}1 & 0\\ 0 & \rho\end{smallmatrix}\right]$, the following proof can work for the case that b_{12} is odd and we omit it here.

With g in $\mathcal{G}$, since $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$, there exists $f \in \mathcal{G}$ such that $f \notin \mathscr{A}_k^d$ for each even $d \in [k]$. Let

$$\overline{\mathcal{G}}^{\text{even}} = \{f \in \mathcal{G} | f \notin \mathscr{A}_k^d \text{ for some even } d \in [k]\}.$$

We prove the lemma for the following separate cases:

- Case (A): there exists one rank-2 signature in $\overline{\mathcal{G}}^{\text{even}}$,
- Case (B): there exists one rank-3 signature in $\overline{\mathcal{G}}^{\text{even}}$, which has the support (5.6), (5.7) or (5.8).
- Case (C): all the signatures in $\overline{\mathcal{G}}^{\text{even}}$ have the support (5.9), (5.10), (5.11) or (5.12).

For Case (A), there exists another rank-2 signature $g' \in \overline{\mathcal{G}}^{\text{even}}$. By Lemma 5.20, we can assume that g' has $\frac{k}{2}$-type support and has the compressed signature

$$\underline{g'} = \mathfrak{i}^{b'_1x_1+b'_2x_2+b'_{12}x_1x_2},$$

By Lemma 5.22, b'_{12} is odd since $g' \notin \mathscr{A}_k^d$ for some even $d \in [k]$. Let $h = gg'$, then the compressed signature

$$\underline{h} = \mathfrak{i}^{(b_1+b'_1)x_1+(b_2+b'_2)x_2+(b_{12}+b'_{12})x_1x_2}.$$

We have $h \notin \mathscr{A}$ since $b_{12} + b'_{12}$ is odd. Moreover, by Lemma 5.18 $h \notin \mathscr{A}_{\frac{k}{2}}^{d'}$ for any $d' \in [\frac{k}{2}]$ since h has $\frac{k}{2}$-type support, and we are done.

For Case (B),

- if there exists a rank-3 signature $f \in \overline{\mathcal{G}}^{\text{even}}$ of the type (5.6), as we have done in the proof of Case 2, we can assume that f has the compressed signature

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{a_1x_1+a_2x_2+a_3x_3+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3+2a_{123}x_1x_2x_3}.$$

  Thus #CSP$_k(g, f)$ is #P-hard by Lemma 5.22 and Lemma 5.23, and #CSP$_k(\neq_2, \mathcal{G})$ is #P-hard;

- assume that there is a signature $f \in \overline{\mathcal{G}}^{\text{even}}$ which has the support (5.7). If $f^2 \notin \mathscr{A}$, then we are done by letting $h = f^2$ since f has $\frac{k}{2}$-type support. Otherwise, we can assume that

$$\underline{f}(x_1, x_2, x_3) = \alpha^{c_1x_1+c_2x_2+c_3x_3+2c_{12}x_1x_2+2c_{13}x_1x_3+2c_{23}x_2x_3+4c_{123}x_1x_2x_3}.$$

  By pinning $x_1 = 0$, we get a rank-2 signature g_2 which has the support

$$(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_2 + x_3)_{\frac{k}{2}}$$

  after collation and the compressed signature

$$\underline{g_2}(x_2, x_3) = \alpha^{c_2x_2+c_3x_3+2c_{23}x_2x_3}.$$

  If $g_2 \notin \mathscr{A}$, then $h = gg_2 \notin \mathscr{A}_{\frac{k}{2}}^{d'}$ for any $d' \in [\frac{k}{2}]$ by Lemma 5.18 and we are done. Otherwise, we have $c_2 \equiv c_3 \equiv c_{23} \equiv 0 \pmod 2$. Similarly, by pinning $x_2 = 0, x_3 = 0$, we have $c_1 \equiv c_2 \equiv c_3 \equiv c_{12} \equiv c_{13} \equiv c_{23} \equiv 0 \pmod 2$. This implies that

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{\frac{c_1}{2}x_1+\frac{c_2}{2}x_2+\frac{c_3}{2}x_3+c_{12}x_1x_2+c_{13}x_1x_3+c_{23}x_2x_3+2c_{123}x_1x_2x_3}.$$

  Let $\widehat{f} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \rho^d \end{smallmatrix}\right]^{\otimes arity(f)} f$. Then

$$\underline{\widehat{f}} = \rho^{d(\frac{k}{2}x_1+\frac{k}{2}x_2+\frac{k}{2}x_3+\epsilon_{12}k[x_1+x_2]+\epsilon_{13}k[x_1+x_3]+\epsilon_{23}[x_2+x_3]+\frac{k}{2}[x_1+x_2+x_3])}\underline{f},$$

where $[\cdot]$ denotes the corresponding variable. By (5.17) and (5.18), we have

$$\underline{\widehat{f}} = \mathfrak{i}^{c_1'x_1+c_2'x_2+c_3'x_3+c_{12}'x_1x_2+c_{13}'x_1x_3+c_{23}'x_2x_3+c_{123}'x_1x_2x_3},$$

where $c_1' = d(1+\epsilon_{12}+\epsilon_{13})+\frac{c_1}{2}, c_2' = d(1+\epsilon_{12}+\epsilon_{23})+\frac{c_2}{2}, c_3' = d(1+\epsilon_{13}+\epsilon_{23})+\frac{c_3}{2}$, $c_{12}' = d(1+2\epsilon_{12})+c_{12}, c_{13}' = d(1+2\epsilon_{13})+c_{13}, c_{23}' = d(1+2\epsilon_{23})+c_{23}, c_{123}' = 2d+2c_{123}$. Note that $f \notin \mathscr{A}_k^d$ for some even d. Thus a_{123} is odd.

Then we take three copies of g and merge the variable bundles $(y_1), (y_2), (y_1+y_2)$ of first copy of g to the variable bundles $(x_1), (x_2), (x_1+x_2)$ of f using $(=_{2k})$ respectively, we get a $\frac{k}{2}$-type signature f' which has the support

$$(x_1)_k(x_2)_k(x_3)_{\frac{k}{2}}(x_1+x_2)_{\frac{k}{2}}(x_1+x_3)_{\epsilon_{13}k}(x_2+x_3)_{\epsilon_{23}k}(x_1+x_2+x_3)_{\frac{k}{2}}$$

after collation and

$$\underline{f'} = \mathfrak{i}^{(\frac{c_1}{2}+b_1)x_1+(\frac{c_2}{2}+b_2)x_2+\frac{c_3}{2}x_3+(c_{12}+b_{12})x_1x_2+c_{13}x_1x_3+c_{23}x_2x_3+2c_{123}x_1x_2x_3};$$

secondly, we merge the variable bundles $(y_1), (y_2), (y_1+y_2)$ of the second copy of g to the variable bundles $(x_1), (x_3), (x_1+x_3)$ of f' using $(=_{2k})$ respectively to construct the signature f''; and then we merge the variable bundles $(y_1), (y_2), (y_1+y_2)$ of the third copy to the variable bundles $(x_2), (x_3), (x_2+x_3)$ of f'' by $(=_{2k})$ respectively. Finally, we get a signature f''' which has the support (5.6) and the compressed signature

$$\underline{f'''} = \mathfrak{i}^{(\frac{c_1}{2}+2b_1)x_1+(\frac{c_2}{2}+b_2+b_1)x_2+(\frac{c_3}{2}+2b_2)x_3+(c_{12}+b_{12})x_1x_2+(c_{13}+b_{12})x_1x_3+(c_{23}+b_{12})x_2x_3+2c_{123}x_1x_2x_3}.$$

Note that c_{123} is odd. So $\#\mathrm{CSP}_k(g, f''')$ is #P-hard by Lemma 5.23 and $\#\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard.

- assume that there is a signature $f \in \overline{\mathcal{G}}^{\text{even}}$ which has the support (5.8) with $\epsilon_1 \neq 0$.

  By the same argument as the case (5.7), we can assume that

$$\underline{f}(x_1, x_2, x_3) = \alpha^{d_1x_1+d_2x_2+d_3x_3+2d_{12}x_1x_2+2d_{13}x_1x_3+2d_{23}x_2x_3+4d_{123}x_1x_2x_3}.$$

Moreover, by pinning $x_1 = 0$ and the same argument as the case (5.7), we have

$$d_2 \equiv d_3 \equiv d_{23} \equiv 0 \pmod 2. \tag{5.21}$$

But we can not pin $x_2 = 0, x_3 = 0$ as the case (5.7) since the bundle $(x_2), (x_3)$ may be empty. Alternatively, we pin $x_1 + x_2 = 0$, then we get a rank-2 signature g_{12} which has the support

$$(x_1)_{(\epsilon_1+\epsilon_2)k}(x_3)_{(\epsilon_3+\epsilon_{123})k}(x_1+x_3)_{(\epsilon_{13}+\epsilon_{23})k}$$

and the compressed signature

$$\underline{g}_{12} = \alpha^{(d_1+d_2+2d_{12})x_1+d_3x_3+2(d_{13}+d_{23}+2d_{123})x_1x_3}.$$

Note that g_{12} has k-type support. If $g_{12} \notin \mathscr{A}$, then we are done by Lemma 5.19. Otherwise, we have

$$d_1 + d_2 + 2d_{12} \equiv d_3 \equiv d_{13} + d_{23} + 2d_{123} \equiv 0 \pmod 2.$$

Combining with (5.21), we have

$$d_1 \equiv d_{13} \equiv 0 \pmod 2.$$

Moreover, by pinning $x_1 + x_3 = 0$ and the same argument, we have $d_{12} \equiv 0 \pmod 2$. This implies that

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{\frac{d_1}{2}x_1+\frac{d_2}{2}x_2+\frac{d_3}{2}x_3+d_{12}x_1x_2+d_{13}x_1x_3+d_{23}x_2x_3+2d_{123}x_1x_2x_3}. \tag{5.22}$$

Then by considering the holographic transformation using $\widehat{f} = \begin{bmatrix} 1 & 0 \\ 0 & \rho^d \end{bmatrix}^{\otimes arity(f)} f$ and the same argument as (5.7), we can assume that d_{123} is odd.

Then we take one copy of $g(y_1, y_2, y_1 + y_2)$ and merge the variable bundles $(y_1), (y_2), (y_1 + y_2)$ to the variable bundles $(x_1 + x_2), (x_1 + x_3), (x_2 + x_3)$ of f using $(=_{2k})$ respectively, we get a

k-type signature $f^{(4)}$ which has the support

$$(x_1)_{\epsilon_1 k}(x_2)_{\epsilon_2 k}(x_3)_{\epsilon_3 k}(x_1+x_2)_k(x_1+x_3)_k(x_2+x_3)_k(x_1+x_2+x_3)_{\epsilon_{123}k}$$

and

$$f^{(4)}(x_1,x_2,x_3)=g(x_1+x_2,x_1+x_3,x_2+x_3)f(x_1,x_2,x_3);$$

i.e.,

$$\underline{f^{(4)}}=\mathfrak{i}^{(\frac{d_1}{2}+b_1+b_2+b_{12})x_1+(\frac{d_2}{2}+b_1)x_2+(\frac{d_3}{2}+b_2)x_3+(d_{12}-2b_1-b_{12})x_1x_2+(d_{13}-2b_2)x_1x_3+d_{23}x_2x_3+2d_{123}x_1x_2x_3}.$$

Note that $f^{(4)}$ has the k-type support. Moreover, $f^{(4)}\notin\mathscr{A}$ since d_{123} is odd. Thus we are done by Lemma 5.19.

- assume that there is a signature $f\in\overline{\mathcal{G}}^{\text{even}}$ which has the support (5.8) with $\epsilon_{123}\neq 0$. By pinning $x_1+x_2+x_3=0, x_1+x_2=0, x_1+x_3=0$ and the same argument as the case $\epsilon_1\neq 0$, we can assume that f has the compressed signature as (5.22). The remaining proof is totally same as the case $\epsilon_1\neq 0$ and we omit it here.

For Case (C), all the signatures in $\overline{\mathcal{G}}^{\text{even}}$ have the $\frac{k}{4}$-type support. For $f\in\overline{\mathcal{G}}^{\text{even}}$, if $f^4\notin\mathscr{A}$, then $h=f^4\notin\mathscr{A}^{d'}_{\frac{k}{4}}$ for any $d'\in[\frac{k}{4}]$ by Lemma 5.18 and we are done. Otherwise, we can assume that

$$\underline{f}(x_1,x_2,x_3)=\beta^{s_1x_1+s_2x_2+s_3x_3+2s_{12}x_1x_2+2s_{13}x_1x_3+2s_{23}x_1x_2x_3+4s_{123}x_1x_2x_3}.$$

Moreover, by pinning $x_1=0$, we get a rank-2 signature g_3 which has the support

$$(x_2)_{\frac{k}{2}}(x_3)_{\frac{k}{2}}(x_2+x_3)_{\frac{k}{2}}$$

and the compressed signature

$$\underline{g_3}=\beta^{s_2x_2+s_3x_3+2s_{23}x_2x_3}.$$

Let $h=gg_3$. Note that h has the $\frac{k}{2}$-type support. If one of $\{s_2,s_3,s_{23}\}$ is nonzero modulo 4, then $h\notin\mathscr{A}$. Thus $h\notin\mathscr{A}^d_{\frac{k}{2}}$ for any $d\in[\frac{k}{2}]$ by Lemma 5.18 and we are done. Otherwise, we have $s_2\equiv s_3\equiv s_{23}\equiv 0 \pmod 4$. Moreover, by pinning $x_2=0, x_3=0$, we have $s_1\equiv s_2\equiv s_3\equiv s_{12}\equiv$

$s_{13} \equiv s_{23} \equiv 0 \pmod 4$ similarly. So we have

$$\underline{f}(x_1, x_2, x_3) = \mathfrak{i}^{\frac{s_1}{4}x_1 + \frac{s_2}{4}x_2 + \frac{s_3}{4}x_3 + \frac{s_{12}}{2}x_1x_2 + \frac{s_{13}}{2}x_1x_3 + \frac{s_{23}}{2}x_2x_3 + s_{123}x_1x_2x_3}.$$

If s_{123} is odd, by pinning $x_3 = 1$, we get a rank-2 signature g_4 whose support is

$$(x_1)_{\frac{k}{2}}(x_2)_{\frac{k}{2}}(x_1 + x_2)_{\frac{k}{2}}$$

after collation and the compressed signature is

$$\underline{g_4} = \mathfrak{i}^{(\frac{s_1}{4} + \frac{s_{13}}{2})x_1 + (\frac{s_2}{4} + \frac{s_{23}}{2})x_2 + (\frac{s_{12}}{2} + s_{123})x_1x_2}$$

up to the scalar $\mathfrak{i}^{\frac{s_3}{4}}$. Let $h = gg_4$, then h has $\frac{k}{2}$-type support and

$$\underline{h} = \mathfrak{i}^{(\frac{s_1}{4} + \frac{s_{13}}{2} + b_1)x_1 + (\frac{s_2}{4} + \frac{s_{23}}{2} + b_2)x_2 + (\frac{s_{12}}{2} + s_{123} + b_{12})x_1x_2}.$$

Note that $\frac{s_{12}}{2}, b_{12}$ are even and s_{123} is odd. Thus $\frac{s_{12}}{2} + s_{123} + b_{12}$ is odd. This implies that $h \notin \mathscr{A}$. Thus $h \notin \mathscr{A}^d_{\frac{k}{2}}$ for any $d \in [\frac{k}{2}]$ by Lemma 5.18 and we are done.

Now we can assume that s_{123} is even. By the same proof as Lemma 5.22, we have the following claim:

- if $s_{123} \equiv 0 \pmod 4$, then $f \notin \mathscr{A}^d_k$ for $d \equiv 2 \pmod 4$ and $f \in \mathscr{A}^d_k$ for $d \equiv 0 \pmod 4$;
- if $s_{123} \equiv 2 \pmod 4$, then $f \notin \mathscr{A}^d_k$ for $d \equiv 0 \pmod 4$ and $f \in \mathscr{A}^d_k$ for $d \equiv 2 \pmod 4$.

Since $\overline{\mathcal{G}}^{\text{even}} \nsubseteq \mathscr{A}^d_k$ for any even $d \in [k]$, there at least two signatures $f_1, f_2 \in \mathcal{G}$ and

$$\underline{f}_i(x_1^{(i)}, x_2^{(i)}, x_3^{(i)}) = \mathfrak{i}^{s_1^{(i)}x_1^{(i)} + s_2^{(i)}x_2^{(i)}sa_3^{(i)}x_3^{(i)} + 2s_{12}^{(i)}x_1^{(i)}x_2^{(i)} + 2s_{13}^{(i)}x_1^{(i)}x_3^{(i)} + 2s_{23}^{(i)}x_2^{(i)}x_3^{(i)} + s_{123}^{(i)}x_1^{(i)}x_2^{(i)}x_3^{(i)}}$$

for $i = 1, 2$, where one of $\{s_{123}^{(1)}, s_{123}^{(2)}\}$ is 0 modulo 4 and another is 2 modulo 4.

If f_1 has the support (5.10) or (5.11), for each bundle of $\{(x_1^{(1)}), (x_2^{(1)}), (x_3^{(1)}), (x_1^{(1)} + x_2^{(1)} + x_3^{(1)})\}$, we connect the variables in it to $(=_k)$ by $\neq_2$ (Note that we can not connect $(=_k)$ to the variable bundle directly by the bipartite restriction), then we get a signature f_1' which has the support (5.9) or (5.12) and

$$\underline{f}_1(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}) = \underline{f'}_1(x_1^{(1)} + 1, x_2^{(1)} + 1, x_3^{(1)} + 1).$$

Thus $f_1 \in \mathscr{A}_k^d$ for some $d \in [k]$ iff $f_1' \in \mathscr{A}_k^d$ for some $d \in [k]$. This implies that we can assume that f_1 has the support (5.9) or (5.12). Similarly, we can assume that f_2 has the support (5.9) or (5.12).

By merging the variable bundle $(a_1x_1^{(1)} + a_2x_2^{(1)} + a_3x_3^{(1)})$ of f_1 to the variable bundle $(a_1x_1^{(2)} + a_2x_2^{(2)} + a_3x_3^{(2)})$ of f_2 for any $a_1, a_2, a_3 \in \{0, 1\}$ by $(=_{2k})$ respectively, we get the signature h which has the compressed signature

$$\underline{h}(x_1, x_2, x_3) = \mathfrak{i}^{\sum_{i=1}^{3}(\sum_{u=1}^{2} s_i^{(u)})x_i + 2\sum_{1\leq j<k\leq 3}(\sum_{u=1}^{2} s_{jk}^{(u)})x_jx_k + (s_{123}^{(1)} + s_{123}^{(2)})x_1x_2x_3}.$$

Since $s_{123}^{(1)} + s_{123}^{(2)}$ is 2 modulo 4, we have $h \notin \mathscr{A}$.

- If f_1, f_2 has the same support, then h has the support (5.6) after collation. Then we are done by Lemma 5.23.
- If one of $\{f_1, f_2\}$ has the supports (5.9), and another has the support (5.12), then h has the k-type support and we are done by Lemma 5.19.

□

Now we are ready to prove Theorem 5.5.

证明. We will prove the theorem by induction on k. Note that the theorem has been proved for the cases $k = 1, 2$ by Theorem 2.12 and Theorem 2.14. In the following we assume that $k \geq 3$.

If $\mathcal{G} \subseteq \mathscr{P}$ or $\mathcal{G} \subseteq \mathscr{A}_k^d$ for some $d \in [k]$, the tractability is obvious. Then we assume that $\mathcal{G} \nsubseteq \mathscr{P}$ and $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$.

Since $\mathcal{G} \nsubseteq \mathscr{A}_k^d$ for any $d \in [k]$, by Lemma 5.17 and Lemma 5.24, #CSP$_k(\neq_2, \mathcal{G})$ is #P-hard, or for some $k'|k$ we can construct $f_1, f_2, \cdots, f_{k'}$, which have the same arity, in #CSP$_k(\neq_2, \mathcal{G})$, such that $h = f_1f_2\cdots f_{k'}$ is not in $\mathscr{A}_{\frac{k}{k'}}^{d'}$ for any $d' \in [\frac{k}{k'}]$.

Moreover, by Lemma 5.16 and $\mathcal{G} \nsubseteq \mathscr{P}$, in #CSP$_k(\neq_2, \mathcal{G})$ we can construct signatures $g_1, g_2, \cdots, g_{k'}$, such that $g = g_1g_2\cdots g_{k'}$ and $g \notin \mathscr{P}$.

Then by Lemma 5.11 we have

$$\#\,\mathrm{CSP}_{\frac{k}{k'}}(\neq_2, g, h) \leq_T \#\,\mathrm{CSP}_k(\neq_2, \mathcal{G}),$$

where $g \notin \mathscr{P}$ and $h \notin \mathscr{A}^{d'}_{\frac{k}{k'}}$ for any $d' \in [\frac{k}{k'}]$. By induction, $\#\,\mathrm{CSP}_{\frac{k}{k'}}(\neq_2, f, g)$ is #P-hard. Thus $\#\,\mathrm{CSP}_k(\neq_2, \mathcal{G})$ is #P-hard. □

5.3 #P-Hardness of $\mathrm{Holant}(\Delta_0, \mathcal{F})$

In the following two sections, we will show that $\mathrm{Holant}(\Delta_0, \mathcal{F})$ is #P-hard if $\mathcal{F}$ does not satisfy condition (T). Since $\mathcal{F}$ does not satisfy condition (T), $\mathcal{F} \nsubseteq \mathscr{T}$. Thus, there is a signature $f \in \mathcal{F}$ of arity $n \geqslant 3$ that is not in $\mathscr{T}$. We will prove our claim by induction on the arity n.

By using Δ_0, we first give two conditions that Δ_1 can be easily realized from a signature of arbitrary arity by pinning (Lemma 5.25) or interpolation (Lemma 5.26). If Δ_1 is realizable, then we have $\mathrm{Holant}^c(\mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F})$. Since $\mathrm{Holant}^c(\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), $\mathrm{Holant}(\Delta_0, \mathcal{F})$ is also #P-hard.

Lemma 5.25. *Let $f \in \mathcal{F}$ be a nonzero signature and $f^{\vec{0}} = 0$. Then* $\mathrm{Holant}^c(\mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F})$.

证明. We prove this by induction on the arity n of f.

If $n = 1$, we have $f = (0, \lambda)$ for some $\lambda \neq 0$ since $f \not\equiv 0$. Clearly, Δ_1 is realizable from f.

Assuming our claim is true when $n = k$, we consider the case that $n = k + 1$. For all indices $i \in [n]$, consider signatures f_i^0 realized from f by pinning variable x_i to 0. We know f_i^0 is signature of arity k and $f_i^0(\vec{0}_k) = f(\vec{0}_{k+1}) = 0$.

- If there is an index i such that $f_i^0 \not\equiv 0$, then by induction hypothesis, we have $\mathrm{Holant}^c(\mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, f_i^0, \mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F})$.
- Otherwise, $f_i^0 \equiv 0$ for all indices i. Then, by Lemma 3.23, we have $f = \lambda(0, 1)^{\otimes n}$ for some $\lambda \neq 0$ since $f \not\equiv 0$. Thus, Δ_1 is realizable from f by factorization (Lemma 3.6).

Thus, we have $\mathrm{Holant}^c(\mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F})$. □

Now for all indices i, we consider signatures $\mathfrak{m}_i f$ realized from f by mating. We give a condition by which Δ_1 can be realized from $\mathfrak{m}_i f$ by interpolation. We show that either $\mathrm{Holant}^c(\mathcal{F}) \leqslant_T$

$\operatorname{Holant}(\Delta_0, \mathcal{F})$, or every irreducible $f \in \mathcal{F}$ satisfies 1ST-ORTH (i.e., there exists some $\mu \neq 0$ such that for all indices i, $M(\mathfrak{m}_i f) = \mu I_2$).

Lemma 5.26. *Let $f \in \mathcal{F}$ be a nonzero real-valued signature of arity $n \geqslant 2$. If f does not satisfy* 1ST-ORTH*, then*

- *there is an unary signature $a(x_i)$ on variable x_i such $a(x_i) \mid f$, or*
- $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$.

证明. Since f does not satisfy 1ST-ORTH, there is an index i such that $M(\mathfrak{m}_i f)$ (as a 2-by-2 matrix) is not the identity matrix up to a scalar ($M(\mathfrak{m}_i f) \neq \mu_i I_2$). We denote

$$M(\mathfrak{m}_i f) = \begin{bmatrix} |\mathbf{f}_i^0|^2 & \langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle \\ \langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle & |\mathbf{f}_i^1|^2 \end{bmatrix} \quad \text{by} \quad \begin{bmatrix} a & b \\ b & c \end{bmatrix}.$$

Since f is real, $M(\mathfrak{m}_i f)$ is real symmetric, and thus diagonalizable with real eigenvalues. We first consider the case that $M(\mathfrak{m}_i f)$ is degenerate. Then, we have $|\langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle|^2 = |\mathbf{f}_i^0|^2 |\mathbf{f}_i^1|^2$, so $\mathbf{f}_i^0$ and $\mathbf{f}_i^1$ are linearly dependent by Cauchy-Schwarz. Since $f \not\equiv 0$, either $\mathbf{f}_i^0$ and $\mathbf{f}_i^1$ is nonzero. Assume $\mathbf{f}_i^0$ is nonzero (the other case is similar). Then, we have $\mathbf{f}_i^1 = c \cdot \mathbf{f}_i^0$ for some constant c. It follows that $f = a(x_i) \otimes \mathbf{f}_i^0$, for a unary signature $a(x_i) = (1, c)$.

Now we assume $M(\mathfrak{m}_i f)$ has rank 2, then we have $a, c > 0$. We consider the value of b.

- If $b = 0$, then $M(\mathfrak{m}_i f) = \left[\begin{smallmatrix} a & 0 \\ 0 & c \end{smallmatrix}\right]$. Clearly, $a \neq c$ since $M(\mathfrak{m}_i f)$ is not I_2 up to a scalar. Given $a \neq c$ and $\frac{a}{c} > 0$, we have $|\frac{a}{c}| \neq 1$. By Lemma 3.24, we can realize $(0,0,0,1) = (0,1)^{\otimes 2}$ from $\mathfrak{m}_i f$ by interpolation. Then, by Lemma 3.6, we can realize $\Delta_1 = (0,1)$ by factorization.
- Otherwise, $b \neq 0$. Clearly, we know $(1,0)^{\mathrm{T}}$ is not an eigenvector of $M(\mathfrak{m}_i f)$. Suppose $M(\mathfrak{m}_i f) = P^{-1} \left[\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right] P$, where λ_1 and λ_2 are two real eigenvalues of $M(\mathfrak{m}_i f)$. Since $M(\mathfrak{m}_i f)$ has rank 2 and $M(\mathfrak{m}_i f)$ is not I_2 up to a scalar, we have $\lambda_1 \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$. Also, by the trace formula, $\lambda_1 + \lambda_2 = a + c > 0$. Thus $\frac{\lambda_1}{\lambda_2} \neq -1$. Then we have $|\frac{\lambda_1}{\lambda_2}| \neq 1$. By Lemma 3.25, we can realize $\Delta_1 = (0,1)$ by interpolation.

Thus, we have $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$. □

Corollary 5.27. *Let $f \in \mathcal{F}$ be an irreducible signature of arity $n \geqslant 2$. If f does not satisfy* 1st-Orth*, then* $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$.

We derive some consequences from 1st-Orth. Consider the vector $\mathbf{f}_i^0$. We can pick a second variable x_j and separate $\mathbf{f}_i^0$ into two vectors $\mathbf{f}_{ij}^{00}$ and $\mathbf{f}_{ij}^{01}$ according to $x_j = 0$ or 1. Then

$$|\mathbf{f}_i^0|^2 = |\mathbf{f}_{ij}^{00}|^2 + |\mathbf{f}_{ij}^{01}|^2 = \mu.$$

Similarly, we have

$$|\mathbf{f}_j^1|^2 = |\mathbf{f}_{ij}^{01}|^2 + |\mathbf{f}_{ij}^{11}|^2 = \mu.$$

Comparing the above two equations, we have

$$|\mathbf{f}_{ij}^{00}|^2 = |\mathbf{f}_{ij}^{11}|^2. \tag{5.23}$$

This is ture for all pairs of indices $\{i, j\}$. Similarly, by considering

$$|\mathbf{f}_j^0|^2 = |\mathbf{f}_{ij}^{00}|^2 + |\mathbf{f}_{ij}^{10}|^2 = \mu,$$

we have

$$|\mathbf{f}_{ij}^{01}|^2 = |\mathbf{f}_{ij}^{10}|^2, \tag{5.24}$$

for all pairs $\{i, j\}$. Also, by definition, for all i,

$$\langle \mathbf{f}_i^0, \mathbf{f}_i^1 \rangle = 0, \tag{5.25}$$

Now, we are ready to prove that $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T) for the base case that $\mathcal{F}$ contains an irreducible signature f arity 3. We show that an irreducible ternary signature satisfying 1st-Orth has some special forms, from which one can realize $=_3$ or $=_4$ after some holographic transformations. Then, we can reduce the problem from $\#\mathrm{CSP}(\mathcal{F})$, or $\#\mathrm{CSP}_2(\mathcal{F})$, or $\operatorname{Holant}(\neq_2|=_3, \widehat{\mathcal{F}})$, to $\operatorname{Holant}(\Delta_0, \mathcal{F})$. This allows us to finish the proof by invoking existing dichotomy results for $\#\mathrm{CSP}(\mathcal{F})$, or $\#\mathrm{CSP}_2(\mathcal{F})$, or the #P-hardness result we showed above for $\operatorname{Holant}(\neq_2|=_k, \widehat{\mathcal{F}})$ where $k \geqslant 3$.

Recall that a binary real-valued signature satisfies 1st-Orth iff it is an orthogonal signature (whose 2-by-2 signature matrix is orthogonal up to a real nonzero scalar). Now we consider the base case that $\mathcal{F}$ contains a ternary signature.

Lemma 5.28 (Base case $n = 3$)**.** *Let $\mathcal{F}$ be a set of real-valued signatures containing a ternary signature $f \notin \mathscr{T}$. Then,* $\operatorname{Holant}(\Delta_0, \mathcal{F})$ *is #P-hard unless $\mathcal{F}$ satisfies conditions* (T)*.*

证明. Since f is a ternary signature and $f \notin \mathscr{T}$, we know f is irreducible. If $f^{000} = 0$ or f does not satisfy 1st-Orth, then by Lemma 5.25 or Lemma 5.27, we have $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$. By Theorem 5.1 and it remark, $\operatorname{Holant}^c(\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard. Therefore, we may assume $f^{000} = 1$ after normalization, and f satisfies 1st-Orth and specially equations (5.23), (5.24), and (5.25).

We consider binary signatures f_1^0, f_2^0 and f_3^0 realized by pinning. If there is an index i such that the binary signature f_i^0 is irreducible and not orthogonal, then by Corollary 5.27 we are done. Otherwise, f_1^0, f_2^0 and f_3^0 are all either reducible or orthogonal. Let N be the number of orthogonal signatures among f_1^0, f_2^0 and f_3^0. According to $N = 0, 1, 2$ or 3, there are four cases.

- $N = 0$. Then f_1^0, f_2^0 and f_3^0 are all reducible. So, f_1^0 is of the form $(1, a, b, ab)$, and so are f_2^0 and f_3^0. Thus f has the following matrix

  $$M_{1,23}(f) = \begin{bmatrix} 1 & a & b & ab \\ c & ac & bc & d \end{bmatrix}.$$

  By the equation $|\mathbf{f}_{12}^{01}|^2 = |\mathbf{f}_{12}^{10}|^2$ from (5.24), we have

  $$b^2 + a^2b^2 = c^2 + a^2c^2.$$

  Then, $(1 + a^2)(b^2 - c^2) = 0$. Being real, we have $1 + a^2 > 0$, and thus $b^2 = c^2$. Similarly by symmetry, we have $a^2 = b^2 = c^2$. By the equation $|\mathbf{f}_{12}^{00}|^2 = |\mathbf{f}_{12}^{11}|^2$ from (5.23), we have

  $$1 + a^2 = b^2c^2 + d^2.$$

Then, $d^2 = 1 + a^2 - a^4$. By the equation $\langle \mathbf{f}_1^0, \mathbf{f}_1^1 \rangle = 0$ from (5.25), we have

$$c + a^2c + b^2c + abd = 0.$$

Then, $c(1 + 2a^2) = -abd$. Taking squares of both sides, we have

$$a^2(1 + 4a^2 + 4a^4) = a^4d^2.$$

Plug in $d^2 = 1 + a^2 - a^4$, and we have

$$a^2(1 + 4a^2 + 4a^4 - a^2 - a^4 + a^6) = a^2(1 + a^2)^3 = 0.$$

Since $1 + a^2 > 0$, we have $a^2 = 0$, and hence $b^2 = c^2 = 0$ and $d^2 = 1$.

- If $d = 1$, then f has the signature matrix $\left[\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$, which is $(=_3)$. Then, by Lemma 2.23, we can realize all equality signatures $(=_k)$. Thus, we have

  $$\#\mathrm{CSP}(\mathcal{F}) \leqslant_T \mathrm{Holant}(=_3, \mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F}).$$

  By Theorem 2.34, we know $\#\mathrm{CSP}(\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\mathrm{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

- Otherwise, $d = -1$. We perform a holographic transformation by the orthogonal matrix $Q_1 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Note that

  $$(=_2)(Q_1^{-1})^{\otimes 2} = (=_2) \qquad \text{and} \qquad Q_1^{\otimes 3} f = (=_3).$$

  Thus, the holographic transformation by Q_1 yields

  $$\mathrm{Holant}(=_2|\, f, \mathcal{F}) \equiv_T \mathrm{Holant}(=_2|=_3, Q_1\mathcal{F}).$$

  Again by Lemma 2.23, we have $\#\mathrm{CSP}(Q_1\mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F})$. By Theorem 2.34, we know that $\#\mathrm{CSP}(Q_1\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\mathrm{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

- $N = 1$. Without loss of generality, we may assume f_1^0 is orthogonal and f_2^0 and f_3^0 are reducible. Then f_1^0 has the form $(1, a, \epsilon a, -\epsilon)$, f_2^0 has the form $(1, a, b, ab)$ and f_3^0 has the form $(1, \epsilon a, b, \epsilon ab)$, for some $\epsilon = \pm 1$. Therefore, for some value x, f has the signature matrix,

  $$M(f) = \begin{bmatrix} 1 & a & \epsilon a & -\epsilon \\ b & ab & \epsilon ab & x \end{bmatrix}.$$

  By the equation $|\mathbf{f}_{12}^{01}|^2 = |\mathbf{f}_{12}^{10}|^2$ from (5.24), we have

  $$(\epsilon a)^2 + (-\epsilon)^2 = b^2 + (ab)^2.$$

  Thus $(1 + a^2)(1 - b^2) = 0$. So $b^2 = 1$. By the equation $|\mathbf{f}_{12}^{00}|^2 = |\mathbf{f}_{12}^{11}|^2$ from (5.23), we have

  $$1 + a^2 = (\epsilon ab)^2 + x^2 = a^2 + x^2.$$

  Then, $x^2 = 1$. By the equation $\langle \mathbf{f}_1^0, \mathbf{f}_1^1 \rangle = 0$ from (5.25), we have

  $$b + a^2 b + \epsilon^2 a^2 b - \epsilon x = 0. \tag{5.26}$$

  Then, $\epsilon x = b(1 + 2a^2)$. Taking squares of both sides, we have $1 = (1 + 2a^2)^2$, which implies that $a = 0$. So by (5.26), we have $b - \epsilon x = 0$, and thus $x = \frac{b}{\epsilon} = \epsilon b$. It follows that $M(f) = \left[\begin{smallmatrix} 1 & 0 & 0 & -\epsilon \\ b & 0 & 0 & \epsilon b \end{smallmatrix}\right]$, with $b^2 = \epsilon^2 = 1$.

  Mating variable x_1 of one copy of f with variable x_1 of another copy of f (with x_2 and x_3 as dangling variables), we get a 4-ary signature $\mathfrak{m}_{23} f$ with the signature matrix

  $$M(\mathfrak{m}_{23} f) = M_{x_2x_3, x_1}(f) M_{x_1, x_2x_3}(f) = \begin{bmatrix} 1 & b \\ 0 & 0 \\ 0 & 0 \\ -\epsilon & \epsilon b \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & -\epsilon \\ b & 0 & 0 & \epsilon b \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} = 2M(=_4).$$

  Therefore, we can realize $(=_4)$, and then by Lemma 2.24 we can realize all equality signatures

$(=_{2k})$ of even arity. Thus,

$$\#\mathrm{CSP}_2(\mathcal{F}) \leqslant_T \mathrm{Holant}(=_4, \mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F}).$$

By Theorem 2.34, we know $\#\mathrm{CSP}_2(\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\mathrm{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

- $N = 2$. Without loss of generality, we may assume f_2^0 and f_3^0 are orthogonal, and f_1^0 is reducible. Then, f_2^0 has the form $(1, \epsilon_1 a, a, -\epsilon_1)$ where $\epsilon_1 = \pm 1$, f_3^0 has the form $(1, \epsilon_2 a, a, -\epsilon_2)$ where $\epsilon_2 = \pm 1$, and f_1^0 has the form $(1, \epsilon_1 a, \epsilon_2 a, \epsilon_1\epsilon_2 a^2)$. Then for some x, f has the form

$$M(f) = \begin{bmatrix} 1 & \epsilon_1 a & \epsilon_2 a & \epsilon_1\epsilon_2 a^2 \\ a & -\epsilon_1 & -\epsilon_2 & x \end{bmatrix}.$$

By the equation $|\mathbf{f}_{12}^{01}|^2 = |\mathbf{f}_{12}^{10}|^2$, we have

$$(\epsilon_2 a)^2 + (\epsilon_1\epsilon_2 a^2)^2 = a^2 + (-\epsilon_1)^2.$$

So we get $a^4 = 1$. Since a is real, we have $a = \pm 1$. By the equation $\langle \mathbf{f}_1^0, \mathbf{f}_1^1 \rangle = 0$, we have

$$a - \epsilon_1^2 a - \epsilon_2^2 a + \epsilon_1\epsilon_2 x = -a + \epsilon_1\epsilon_2 x = 0.$$

Then, $x = \frac{a}{\epsilon_1\epsilon_2} = \epsilon_1\epsilon_2 a$. By mating we get $\mathfrak{m}_{23} f$, and we have

$$M(\mathfrak{m}_{23} f) = \begin{bmatrix} 1 & a \\ \epsilon_1 a & -\epsilon_1 \\ \epsilon_2 a & -\epsilon_2 \\ \epsilon_1\epsilon_2 & \epsilon_1\epsilon_2 a \end{bmatrix} \begin{bmatrix} 1 & \epsilon_1 a & \epsilon_2 a & \epsilon_1\epsilon_2 \\ a & -\epsilon_1 & -\epsilon_2 & \epsilon_1\epsilon_2 a \end{bmatrix} = 2 \begin{bmatrix} 1 & 0 & 0 & \epsilon_1\epsilon_2 \\ 0 & 1 & \epsilon_1\epsilon_2 & 0 \\ 0 & \epsilon_1\epsilon_2 & 1 & 0 \\ \epsilon_1\epsilon_2 & 0 & 0 & 1 \end{bmatrix}.$$

  - If $\epsilon_1\epsilon_2 = 1$, then $\mathfrak{m}_{23} f$ is 2 times the IS-EVEN signature, which takes value 1 on all inputs of even weight, and 0 otherwise. Note that, for $H = \frac{1}{\sqrt{2}} \left[\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right]$ we have

$$(=_2)(H^{-1})^{\otimes 2} = (=_2) \qquad \text{and} \qquad H^{\otimes 4}(\mathfrak{m}_{23} f) = (=_4).$$

Thus, a holographic transformation by H yields

$$\operatorname{Holant}(=_2|\, \mathfrak{m}_{23}f, \mathcal{F}) \equiv_T \operatorname{Holant}(=_2|=_4, H\mathcal{F}).$$

By Lemma 2.24, we have

$$\#\mathrm{CSP}_2(H\mathcal{F}) \leqslant_T \operatorname{Holant}(=_2|=_4, H\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F}).$$

By Theorem 2.34, $\#\mathrm{CSP}_2(H\mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

– Otherwise, $\epsilon_1\epsilon_2 = -1$. Then $g(y_1, y_2, y_3, y_4) = \mathfrak{m}_{23}f$ can be normalized as $\left[\begin{smallmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{smallmatrix}\right]$, where the row index is y_1y_2 and column index is $y_3y_4 \in \{0,1\}^2$, both listed lexicographically. After a permutation of variables, we have $M_{y_1y_3,y_2y_4}(\mathfrak{m}_{23}f) = \left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right]$. Connecting variables y_2, y_4 of a copy of $\mathfrak{m}_{23}f$ with variables y_1, y_3 of another copy of $\mathfrak{m}_{23}f$ respectively, we get a signature with the signature matrix

$$M_{y_1y_3,y_2y_4}(\mathfrak{m}_{23}f)M_{y_1y_3,y_2y_4}(\mathfrak{m}_{23}f) = \left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right] = 2 \left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right].$$

Now perform a holographic transformation by H, and we get $(=_4)$, which implies that $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T).

- $N = 3$. Then for some values a, x and ϵ_1, $\epsilon_2 = \pm 1$, the signature f has the signature matrix

$$M(f) = \begin{bmatrix} 1 & \epsilon_1 a & \epsilon_2 a & -\epsilon_1\epsilon_2 \\ a & -\epsilon_1 & -\epsilon_2 & x \end{bmatrix}.$$

By the equation $\langle \mathbf{f}_1^0, \mathbf{f}_1^1 \rangle = 0$, we have

$$a - \epsilon_1^2 a - \epsilon_2^2 a - \epsilon_1\epsilon_2 x = -a - \epsilon_1\epsilon_2 x = 0.$$

Hence, $x = -\epsilon_1\epsilon_2 a$. A holographic transformation by Z^{-1} yields

$$\operatorname{Holant}(=_2|\, f, \Delta_0, \mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2|\, \widehat{f}, \widehat{\Delta_0}, \widehat{\mathcal{F}}).$$

Note that $\widehat{\Delta_0} = Z^{-1}(1,0)^{\mathtt{T}} = (1,1)^{\mathtt{T}}$, and a simple calculation shows

$$M(\widehat{f}) = Z^{-1}M(f)((Z^{-1})^{\mathtt{T}})^{\otimes 2} = \left[\begin{smallmatrix} 1-ai & 0 \\ 0 & 1+ai \end{smallmatrix}\right] \left[\begin{smallmatrix} (1+\epsilon_1)(1+\epsilon_2) & (1-\epsilon_1)(1+\epsilon_2) & (1+\epsilon_1)(1-\epsilon_2) & (1-\epsilon_1)(1-\epsilon_2) \\ (1-\epsilon_1)(1-\epsilon_2) & (1+\epsilon_1)(1-\epsilon_2) & (1-\epsilon_1)(1+\epsilon_2) & (1+\epsilon_1)(1+\epsilon_2) \end{smallmatrix}\right].$$

- If $\epsilon_1 = \epsilon_2 = 1$, then up to a constant, $M(\widehat{f}) = \left[\begin{smallmatrix} 1-ai & 0 & 0 & 0 \\ 0 & 0 & 0 & 1+ai \end{smallmatrix}\right]$. Let $\widehat{Q_2} = \left[\begin{smallmatrix} \sqrt[3]{1+ai} & 0 \\ 0 & \sqrt[3]{1-ai} \end{smallmatrix}\right]$. Then $(\widehat{Q_2})^{\otimes 3}\widehat{f}$ has the signature matrix $(1+a^2)\left[\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$. Thus, a holographic transformation by $\widehat{Q_2}$ yields

  $$\operatorname{Holant}(\neq_2 |\, \widehat{f}, \widehat{\Delta_0}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\neq_2 | =_3, \widehat{Q_2}\widehat{\Delta_0}, \widehat{Q_2}\widehat{\mathcal{F}}).$$

  Thus, we have

  $$\operatorname{Holant}(\neq_2 | =_3, \widehat{Q_2}\widehat{\Delta_0}, \widehat{Q_2}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F}).$$

  By Corollary 5.6, we know $\operatorname{Holant}(\neq_2 | =_3, \widehat{Q_2}\widehat{\Delta_0}, \widehat{Q_2})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

- Otherwise, $M(\widehat{f})$ has the signature matrix $\left[\begin{smallmatrix} 0 & 0 & 0 & 1-ai \\ 1+ai & 0 & 0 & 0 \end{smallmatrix}\right]$ up to a permutation of variables. Connecting $\widehat{f}$ with $\widehat{\Delta_0} = (1,1)$ using $\neq_2$, we get a binary signature $\widehat{g}$ with matrix

  $$M(\widehat{g}) = [1,1] \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1-ai \\ 1+ai & 0 & 0 & 0 \end{bmatrix} = (1+ai, 0, 0, 1-ai).$$

  Connecting one variable of $\widehat{f}$ with one variable of $\widehat{g}$ using $\neq_2$, we get a signature $\widehat{h}$ with the signature matrix

  $$M(\widehat{h}) = \begin{bmatrix} 1+ai & 0 \\ 0 & 1-ai \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1-ai \\ 1+ai & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} (1+ai)^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & (1-ai)^2 \end{bmatrix}.$$

  Then, a holographic transformation by $\widehat{Q_3} = \begin{bmatrix} \sqrt[3]{(1-ai)^2} & 0 \\ 0 & \sqrt[3]{(1+ai)^2} \end{bmatrix}$ yields

  $$\operatorname{Holant}(\neq_2 |\, \widehat{h}, \widehat{\Delta_0}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\neq_2 | =_3, \widehat{Q_3}\widehat{\Delta_0}, \widehat{Q_3}\widehat{\mathcal{F}}).$$

  Then similarly by Corollary 5.6, we have $\operatorname{Holant}(\Delta_0, \mathcal{F})$ is #P-hard.

Thus, Holant$(\Delta_0, \mathcal{F})$ is #P-hard unless $\mathcal{F}$ satisfies condition (T). □

Now, we consider the inductive step. The general strategy is that we start with a signature $f \in \mathcal{F}$ of arity $n \geqslant 4$ that is not in $\mathscr{T}$, and realize a signature g of arity $n-1$ or $n-2$ by pinning or merging (using $=_2$) that is also not in $\mathscr{T}$. By a sequence of reductions (that is constant in length independent of the problem instance size), we can realize a signature h of arity 3 that is not in $\mathscr{T}$ (the base case). Then we are done.

For all indices i and all pairs of indices $\{j, k\}$, consider f_i^0 and $\partial_{jk} f$. If there exists i or $\{j, k\}$ such that f_i^0 or $\partial_{jk} f \notin \mathscr{T}$, then we can realize $g = f_i^0$ or $\partial_{jk} f$ which has arity $n-1$ or $n-2$, and we are done. Otherwise, f_i^0 and $\partial_{jk} f \in \mathscr{T}$ for all i and all $\{j, k\}$. We denote this property by $f \in \int_{12} \mathscr{T}$. Under the assumption that $f \in \int_{12} \mathscr{T}$, our goal is to show that we can realize Δ_1 and hence we are done by the hardness of Holant$^c(\mathcal{F})$, or there is an unary signature $a(x_u)$ or binary signature $b(x_v, x_w)$ such that $a(x_u) \mid f$ or $b(x_v, x_w) \mid f$. Then, we have $f = a(x_u) \otimes g$ or $f = b(x_v, x_w) \otimes g$ for some g of arity $n-1$ or $n-2$. By the definition of $\mathscr{T}$, we know $g \notin \mathscr{T}$ since $f \notin \mathscr{T}$. By Lemma 3.6, we can realize g by factorization, and we are done. When $n \geqslant 5$, the above induction proof can be achieved by the interplay of the unique factorization, and the commutivity of f_i^0 (pinning) and $\partial_{jk} f$ (merging) operations on disjoint indices (Lemmas 5.30 and 5.31). For $n = 4$, the proof requires more work (Lemma 5.33); we need to combine the induction proof and 1st-Orth to handle it.

We use $\mathscr{T}_1$ to denote the set of tensor products of unary signatures. We denote the property that $f_i^0 \in \mathscr{T}_1$ for all i by $\int_1 \mathscr{T}_1$. We carry out our induction proof by the following lemmas.

Lemma 5.29. *Let f be a signature of arity $n \geqslant 3$. If there exists a nonzero signature g, the scope of which is a subset of the scope of f, such that $g \mid f_i^0$ for all indices i disjoint with the scope of g and furthermore, $g \mid \partial_{jk} f$ for some pair of indices $\{j, k\}$ disjoint with the scope of g, then $g \mid f$. (Note that if $\partial_{jk} f \equiv 0$ then $g \mid \partial_{jk} f$ is satisfied.)*

证明. We may assume f is nonzero, for otherwise the conclusion trivially holds. We now prove this for a unary signature $g = (a, b)$. We assume g is on the variable x_u. Consider the signature $f' = b f_u^0 - a f_u^1$. Clearly, x_j and x_k are in the scope of f'. Thus, f' has arity at least 2. For every

$i \neq u$, we have $f_i^0 = (a, b) \otimes h$ for some h. Then, $(f_i^0)_u^0 = a \cdot h$, $(f_i^0)_u^1 = b \cdot h$, and hence

$$(f')_i^0 = (bf_u^0 - af_u^1)_i^0 = bf_{ui}^{00} - af_{ui}^{10} = b(f_i^0)_u^0 - a(f_i^0)_u^1 = ba \cdot h - ab \cdot h \equiv 0.$$

Moreover, there are indices $j, k \neq u$ such that $g(x_u) \mid \partial_{jk} f$. Then, $\partial_{jk} f = (a, b) \otimes h'$, for some h'. Then, we have $(\partial_{jk} f)_u^0 = a \cdot h'$, $(\partial_{jk} f)_u^1 = b \cdot h'$, and hence

$$\partial_{jk}(f') = \partial_{jk}(bf_u^0 - af_u^1) = b(\partial_{jk} f)_u^0 - a(\partial_{jk} f)_u^1 = ba \cdot h' - ab \cdot h' \equiv 0.$$

By Lemma 3.23, we have $f' \equiv 0$. Thus, we have $f_u^0 : f_u^1 = a : b$, and hence $g(x_u) \mid f$.

For a signature g of arity $\geqslant n - 2$, the proof is essentially the same, which we omit here. □

Lemma 5.30. *Let f be a signature of arity $n \geqslant 5$, $f \notin \mathscr{T}$, $f \in \int_{12} \mathscr{T}$ and $f \in \int_1 \mathscr{T}_1$. Then there is a unary signature $a(x_u)$ such that $a(x_u) \mid f$, or Δ_1 is realizable from f.*

证明. Since $f \notin \mathscr{T}$, f is nonzero. We may further assume $f_i^0 \not\equiv 0$ for all indices i. Otherwise, we have $f^{\vec{0}} = 0$. Then, by Lemma 5.25, we can realize Δ_1. By the same reason, we may further assume $f_{ij}^{00} \not\equiv 0$ for all pairs of indices $\{i, j\}$.

For some arbitrary index r, we consider f_r^0. Since $f_r^0 \in \mathscr{T}_1$, there exists some unary signature $a(x_u)$ such that $a(x_u) \mid f_r^0$. We show $a(x_u) \mid f$. Consider f_i^0 for all indices $i \neq u, r$. Since $f_i^0 \in \mathscr{T}_1$, there is a unary signature $a'(x_u)$ such that $a'(x_u) \mid f_i^0$, and hence we have $a'(x_u) \mid (f_i^0)_r^0$. On the other hand, since $a(x_u) \mid f_r^0$, we also have $a(x_u) \mid (f_r^0)_i^0$. Note that the pinning operations on different variables commute. Thus, we have $(f_r^0)_i^0 = (f_i^0)_r^0$, and we know it is a nonzero signature. Then, by UPF (Lemma 3.4), we have $a(x_u) \sim a'(x_u)$. Thus, $a(x_u) \mid f_i^0$ for all indices $i \neq u$.

Then, we show $a(x_u) \mid \partial_{jk} f$ for some arbitrary pair of indices $j, k \neq u$. If $\partial_{jk} f \equiv 0$, then we have $a(x_u) \mid \partial_{jk} f$ and hence $a(x_u) \mid f$ by Lemma 5.29. Next, we assume $\partial_{jk} f \not\equiv 0$. Similarly, if for some index $i \neq j, k$, we have $(\partial_{jk} f)_i^0 \equiv 0$, then we have $\partial_{jk} f(\vec{0}) = 0$ and hence by Lemma 5.26, we can realize Δ_1. Otherwise, $(\partial_{jk} f)_i^0 \not\equiv 0$ for all $i \notin \{j, k\}$. Recall that $\partial_{jk} f \in \mathscr{T}$. We show the variable x_u must appear in a unary signature in the UPF of $\partial_{jk} f \in \mathscr{T}$.

- For a contradiction, suppose there is an irreducible binary signature $b(x_u, x_v)$ such that $b(x_u, x_v) \mid \partial_{jk} f$. Since f has arity $n \geqslant 5$, we can pick some index $i \notin \{u, v, j, k\}$ such that $b(x_u, x_v) \mid (\partial_{jk} f)_i^0$. Note that $(\partial_{jk} f)_i^0 = \partial_{jk}(f_i^0) \not\equiv 0$ by the commutativity of pinning and merging. Thus, $\partial_{jk}(f_i^0)$ has an irreducible binary tensor divisor $b(x_u, x_v)$. However, $f_i^0 \in \mathscr{T}_1$ and so is $\partial_{jk}(f_i^0)$. By UPF, we get a contradiction.

- Thus, there is a unary signature $a''(x_u)$ such that $a''(x_u) \mid \partial_{jk} f$. Pick some index $i \notin \{u, j, k\}$, and we have $a''(x_u) \mid (\partial_{jk} f)_i^0$. We also have $a(x_u) \mid \partial_{jk}(f_i^0)$ since $a(x_u) \mid f_i^0$. Again, $(\partial_{jk} f)_i^0 = \partial_{jk}(f_i^0) \not\equiv 0$ by commutativity. Then by UPF, we have $a''(x_u) \sim a(x_u)$. Thus, $a(x_u) \mid f$ by Lemma 5.29 and we are done.

□

Lemma 5.31. *Let f be a signature of arity $n \geqslant 5$, $f \notin \mathscr{T}$, $f \in \int \mathscr{T}$ and $f \notin \int_1 \mathscr{T}_1$. Then, there is an irreducible binary signature $b(x_v, x_w)$ such that $b(x_v, x_w) \mid f$, or Δ_1 is realizable from f.*

证明. Since $f \notin \int_1 \mathscr{T}_1$, but $f \in \int \mathscr{T}$, there is some index r such that f_r^0 is nonzero and has an irreducible binary signature factor $b(x_v, x_w)$. We will show this $b(x_v, x_w)$ divides f. Again, we may assume $f_i^0 \not\equiv 0$ and $f_{ij}^{00} \not\equiv 0$ for all i and all $\{i, j\}$. Otherwise, we can realize Δ_1 by Lemma 5.25.

Consider f_i^0 for all indices $i \notin \{v, w, r\}$. Since $f_i^0 \in \mathscr{T}$ and $f_i^0 \not\equiv 0$, there is either a unary signature $a(x_v)$ or an irreducible binary signature $b'(x_v, x_{w'})$ such that $a(x_v) \mid f_i^0$ or $b'(x_v, x_{w'}) \mid f_i^0$. We also have $b(x_v, x_w) \mid (f_r^0)_i^0$ since $b(x_v, x_w) \mid f_r^0$. Again, we have $(f_r^0)_i^0 = (f_i^0)_r^0 \not\equiv 0$. Then by UPF, we know that the unary signature $a(x_v)$ does not exist, and it must be $b'(x_v, x_{w'}) \mid f_i^0$ and $b(x_v, x_w) = b'(x_v, x_{w'})$. Thus, we have $b(x_v, x_w) \mid f_i^0$ for all $i \notin \{v, w\}$.

Then, for an arbitrary pair of indices $\{j, k\}$ disjoint with $\{v, w\}$, we show $b(x_v, x_w) \mid \partial_{jk} f$. Again, we may assume $\partial_{jk} f \not\equiv 0$ (for otherwise $b(x_v, x_w) \mid \partial_{jk} f$ is proved) and furthermore $(\partial_{jk} f)_i^0 \not\equiv 0$ for all i disjoint with $\{j, k\}$, for otherwise, we can realize Δ_1. Since f has arity $n \geqslant 5$, we can pick some index $i \notin \{u, v, j, k\}$ such that $b(x_v, x_w) \mid \partial_{jk}(f_i^0)$ due to $b(x_v, x_w) \mid f_i^0$. Recall that $\partial_{jk} f \in \mathscr{T}$, we consider the UPF of $\partial_{jk} f$. Using a similar argument as in the previous paragraph, we have $b(x_v, x_w) \mid \partial_{jk} f$ by UPF. □

Combining the above two lemmas, we have the following result.

Lemma 5.32 (Inductive step for $n \geqslant 5$). *If $f \in \mathcal{F}$ is a signature of arity $n \geqslant 5$ and $f \notin \mathscr{T}$, then*

- $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$ *or*
- *there is a signature $g \notin \mathscr{T}$ of arity $n-1$ or $n-2$ such that* $\operatorname{Holant}(\Delta_0, g, \mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$.

Now, the only case left for the induction proof is when f is a signature of arity 4. We deal with it by using the 1st-Orth condition.

Lemma 5.33 (Inductive step $n=4$)**.** *Let $f \in \mathcal{F}$ be a signature of arity* 4 *and $f \notin \mathscr{T}$. Then*

- $\operatorname{Holant}^c(\mathcal{F}) \leqslant_T \operatorname{Holant}(=_2|\ \Delta_0, \mathcal{F})$, *or*
- $\#\mathrm{CSP}_2(\mathcal{F}) \leqslant_T \operatorname{Holant}(=_2|=_4, \mathcal{F}) \leqslant_T \operatorname{Holant}(=_2|\ \Delta_0, \mathcal{F})$, *or*
- *there is a signature $g \notin \mathscr{T}$ of arity* 3 *such that* $\operatorname{Holant}(\Delta_0, g, \mathcal{F}) \leqslant_T \operatorname{Holant}(\Delta_0, \mathcal{F})$.

证明. First, we may assume f is irreducible. Otherwise, we consider its irreducible factors. Since $f \notin \mathscr{T}$, it has an irreducible factor g of arity 3 such that $g \notin \mathscr{T}$. By Lemma 3.6, g is realizable from f by factorization, and the lemma is proved. Also we may assume $f^{0000}=1$ after normalization and f satisfies 1st-Orth; otherwise, by Lemma 5.25 and Corollary 5.27, we are done. We consider signatures f_i^0 realized by pinning x_i to 0 in f, for all i. If there is i such that the ternary signature $f_i^0 \notin \mathscr{T}$, then we are done, since f_i^0 has arity 3. Also, since f has arity 4, $\partial_{ij} f$ is a binary signature for any pair of indices $\{i, j\}$. Hence $\partial_{ij} f \in \mathscr{T}$. Thus, we may assume $f \in \int \mathscr{T}$.

- If $f \in \int_1 \mathscr{T}_1$, then there are three unary signatures such that $f_1^0 = a_1(x_2) \otimes a_2(x_3) \otimes a_3(x_4)$. By the same proof in Lemma 5.30, we have $a_2(x_3) \mid f_2^0$ and $a_3(x_4) \mid f_2^0$. Thus, $a_2(x_3) \otimes a_3(x_4) \mid f_2^0$.
- Otherwise, there is an index i such that f_i^0 has an irreducible binary factor. Without loss of generality, we assume that $f_1^0 = a_1(x_2) \otimes b_1(x_3, x_4)$ where $b_1(x_3, x_4)$ is irreducible. By the same proof as in Lemma 5.31, we have $b_1(x_3, x_4) \mid f_2^0$.

Therefore, in both cases, there is a binary signature $b(x_3, x_4)$, which may be reducible, i.e., $b(x_3, x_4) = a_2(x_3) \otimes a_3(x_4)$, such that $b(x_3, x_4) \mid f_1^0$ and $b(x_3, x_4) \mid f_2^0$. Thus, we have

$$f_1^0 = a_1(x_2) \otimes b(x_3, x_4) \qquad \text{and} \qquad f_2^0 = a_1'(x_1) \otimes b(x_3, x_4).$$

By a normalization we may let $b(x_3, x_4) = (1, a, b, c)$, $a_1(x_2) = (1, x)$ and $a_1'(x_1) = (1, y)$. Then, f

has the signature matrix, for some z, z_1, z_2, z_3

$$M_{12,34}(f) = \begin{bmatrix} 1 & a & b & c \\ x & ax & bx & cx \\ y & ay & by & cy \\ z & z_1 & z_2 & z_3 \end{bmatrix}.$$

Then, we consider the signature f_3^0. It has the signature matrix

$$M_{12,4}(f_3^0) = \begin{bmatrix} 1 & a \\ x & ax \\ y & ay \\ z & z_1 \end{bmatrix}.$$

We have $f_3^0 \in \mathscr{T}$, and nonzero. In its unique factorization, if x_2 and x_4 belong to an irreducible binary signature, then $(f_3^0)_1^0$, which has the signature matrix $M_{2,4}(f_{13}^{00}) = [\begin{smallmatrix} 1 & a \\ x & ax \end{smallmatrix}]$, would have been an irreducible binary signature, a contradiction. Similarly x_1 and x_4 do not belong to an irreducible binary signature in the unique factorization of f_3^0. Therefore x_4 appears in a unary signature in the factorization of f_3^0. It follows that $z_1 = az$. Similarly from $f_4^0 \in \mathscr{T}$, we can prove $z_2 = bz$. We also write z_3 as $cz + w$. Thus, we have

$$M_{12,34}(f) = (1, x, y, z)^{\mathtt{T}} \otimes (1, a, b, c) + w((0,1)^{\mathtt{T}})^{\otimes 2} \otimes (0,1)^{\otimes 2}.$$

We know $w \neq 0$ since $f \notin \mathscr{T}$. By pinning any 3 of the 4 variables to 0, we can realize four unary signatures $(1, a), (1, b), (1, x)$ and $(1, y)$. For example, $(1, x)$ can be realized from f by pinning variables x_1, x_3 and x_4 to 0.

- Suppose a, b, x, y are not all zero, say $x \neq 0$. We connect the unary $(1, x)$ with the variable x_2 of f, and we get a signature g with the signature matrix

$$M_{1,34}(g) = \begin{bmatrix} 1 + x^2 & a(1 + x^2) & b(1 + x^2) & c(1 + x^2) \\ y + xz & a(y + xz) & b(y + xz) & c(y + xz) + xw \end{bmatrix}.$$

Clearly, $1+x^2 \neq 0$. By normalization, we have

$$M_{1,34}(g) = \begin{bmatrix} 1 & a & b & c \\ x' & ax' & bx' & cx'+w' \end{bmatrix},$$

where $x' = \frac{y+xz}{1+x^2}$ and $w' = \frac{xw}{1+x^2}$, and $w' \neq 0$ since $xw \neq 0$. Thus

$$g = (1, x')_{x_1} \otimes (1, a, b, c)_{x_3,x_4} + w'(0,1)^{\otimes 3}. \tag{5.27}$$

We claim that $g \notin \mathscr{T}$. Otherwise consider the unique factorization of g in $\mathscr{T}$. By the same proof above for $f_3^0 \in \mathscr{T}$, we can see that x_1 of g cannot appear in an irreducible binary signature, either with x_3 or with x_4, as a tensor factor in the unique prime factorization of g. Hence x_1 must appear in a unary signature in this factorization. This would imply that $w' = 0$, by the form of $M_{1,34}(g)$, a contradiction.

It follows that $g \notin \mathscr{T}$, and we are done.

- Otherwise, $a = b = x = y = 0$. Then, we know

$$M_{12,34}(f) = \begin{bmatrix} 1 & 0 & 0 & c \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ z & 0 & 0 & z_3 \end{bmatrix}.$$

Here, we write z_3 as $cz+w$. By equation (5.23), we have $1+c^2 = z^2+z_3^2$ and $1+z^2 = c^2+z_3^2$. Thus, we have $c^2 = z^2$ and $z_3^2 = 1$. By pinning variables x_1 and x_2 to 0, we can realize the binary signature $(1, 0, 0, c)$. If it is not reducible or orthogonal, then by Lemma 5.26 we can realize Δ_1. Otherwise, we have $c = 0$ or $c = \pm 1$. Similarly, we have $z = 0$ or $z = \pm 1$. As we already have $c^2 = z^2$, we get $c = z = 0$ or $c^2 = z^2 = 1$. We consider the signature $\mathfrak{m}_{34} f$

realized by mating variables x_3, x_4 of f. We have

$$M(\mathfrak{m}_{34}f) = M_{12,34}(f)(M_{12,34}(f))^{\mathtt{T}} = \begin{bmatrix} 1+c^2 & 0 & 0 & z+cz_3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ z+cz_3 & 0 & 0 & z^2+z_3^2 \end{bmatrix}.$$

If $c = z = 0$, then we have $M(\mathfrak{m}_{34}f) = \left[\begin{smallmatrix} 1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1 \end{smallmatrix}\right] = M(=_4)$. Otherwise, $c^2 = z^2 = 1$. Also, we know $z_3 \neq cz$ since $f \notin \mathscr{T}$. Note that $z_3^2 = 1$ and $(cz)^2 = 1$. This implies that $z_3 = -cz$. Then, we have $z + cz_3 = z - c^2 z = z - z = 0$. Thus, we have $M(\mathfrak{m}_{34}f) = \left[\begin{smallmatrix} 2&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&2 \end{smallmatrix}\right] = 2M(=_4)$. Therefore, we can realize $(=_4)$ from f, and then by Lemma 2.24 we can realize all equality signatures $=_{2k}$ of even arity. Thus, we have

$$\#\mathrm{CSP}_2(\mathcal{F}) \leqslant_T \mathrm{Holant}(=_4, \mathcal{F}) \leqslant_T \mathrm{Holant}(\Delta_0, \mathcal{F}).$$

This completes the proof of the lemma.

□

Theorem 5.34. $\mathrm{Holant}(\Delta_0, \mathcal{F})$ *is #P-hard unless $\mathcal{F}$ satisfies the tractable condition* (T)*.*

证明. Assume $\mathcal{F}$ does not satisfy condition (T). Then $\mathcal{F} \nsubseteq \mathscr{T}$. There is a signature $f \in \mathcal{F}$ of arity $n \geqslant 3$ that is not in $\mathscr{T}$. If $n = 3$, then by Lemma 5.28, we are done.

Suppose our statement is true for $3 \leqslant n \leqslant k$. Consider $n = k+1 \geqslant 4$. By Lemmas 5.32 and 5.33, we have $\mathrm{Holant}^c(\mathcal{F})$, or $\#\mathrm{CSP}_2(\mathcal{F})$, or $\mathrm{Holant}(=_2|\ \Delta_0, g, \mathcal{F}) \leqslant_T \mathrm{Holant}(=_2|\ \Delta_0, \mathcal{F})$ for some $g \notin \mathscr{T}$ of arity $k-1$ or k at least 3. By Theorem 2.34 and the induction hypothesis, we know $\mathrm{Holant}^c(\mathcal{F})$, $\#\mathrm{CSP}_2(\mathcal{F})$ and $\mathrm{Holant}(=_2|\ \Delta_0, g, \mathcal{F})$ are all #P-hard when $\mathcal{F}$ does not satisfy condition (T), and hence $\mathrm{Holant}(=_2|\ \Delta_0, \mathcal{F})$ is #P-hard. □

5.4 Putting Things Together

Theorem 5.35. *Let $\mathcal{F}$ be a set of real-valued signatures containing a nonzero signature of odd arity. If $\mathcal{F}$ satisfies condition* (T)*, then* $\mathrm{Holant}(\mathcal{F})$ *is polynomial-time computable; otherwise,* $\mathrm{Holant}(\mathcal{F})$

is #P-hard.

证明. The tractability is known by Theorem 2.33.

We prove #P-hardness when $\mathcal{F}$ does not satisfy condition (T). By Lemma 5.3, There exists some real orthogonal matrix $Q \in \mathbf{O}_2$ such that $\operatorname{Holant}(=_2\mid \Delta_0, Q\mathcal{F}) \leqslant_T \operatorname{Holant}(=_2\mid \mathcal{F})$ or $\operatorname{Holant}(\neq_2\mid=_{2k+1}, \widehat{Q\mathcal{F}}) \leqslant_T \operatorname{Holant}(=_2\mid \mathcal{F})$. Since $\mathcal{F}$ does not satisfy condition (T), $Q\mathcal{F}$ also does not satisfy it. Then by Theorem 5.34 and Corollary 5.6, we have $\operatorname{Holant}(=_2\mid \Delta_0, Q\mathcal{F})$ and $\operatorname{Holant}(\neq_2\mid=_{2k+1}, \widehat{Q}\widehat{\mathcal{F}})$ are both #P-hard. Hence, $\operatorname{Holant}(=_2\mid \mathcal{F})$ is #P-hard. □

Chapter 6

Building Blocks of Even Arity: Binary and 4-ary Signatures

Since now, we consider the complexity of Holant($\mathcal{F}$) for $\mathcal{F}$ consisting of signatures of even arity. Suppose that $\mathcal{F}$ does not satisfy (T). Then, $\mathcal{F} \nsubseteq \mathscr{T}$. Recall that $\mathcal{O}^{\otimes}$ denotes the set of tensor products of binary orthogonal signatures and the binary zero signature. Clearly, since $\mathcal{O}^{\otimes} \subseteq \mathscr{T}$, $\mathcal{F} \nsubseteq \mathcal{O}^{\otimes}$. Thus, $\mathcal{F}$ contains a signature $f \notin \mathcal{O}^{\otimes}$. We will prove that Holant($\mathcal{F}$) is #P-hard when $\mathcal{F}$ does not satisfy (T) by induction on the arity of f. In this chapter, we deal with the base cases that $\mathcal{F}$ contains a binary or 4-ary nonzero signature that is not in $\mathcal{O}^{\otimes}$.

6.1 First and Second Order Orthogonality

Recall that a real-valued signature f of arity n satisfies 1ST-ORTH iff there exists $\mu \neq 0$ such that for all indices $i \in [n]$, $M(\mathfrak{m}_i f) = \mu I_2$. Suppose that $\mathcal{F}$ does not satisfy condition (T). We first show that every nonzero $f \in \mathcal{F}$ (of arity not necessarily 2 or 4) satisfies 1ST-ORTH, or otherwise we get the #P-hardness of Holant($\mathcal{F}$) by realizing a unary signature.

Lemma 6.1. *Suppose that $\mathcal{F}$ is a set of real-valued signatures and $\mathcal{F}$ does not satisfy condition (T). If $\mathcal{F}$ contains a signature f that does not satisfy* 1ST-ORTH, *then* Holant($\mathcal{F}$) *is #P-hard.*

证明. Consider $\mathfrak{m}_i f$ for all indices i. Clearly, $M(\mathfrak{m}_i f) = M_i(f)M_i^{\mathtt{T}}(f)$ is a real symmetric positive semi-definite matrix, which is diagonalizable with two non-negative real eigenvalues $\lambda_i \geqslant \mu_i \geqslant 0$. These two eigenvalues are not both zero since f is real valued and $f \not\equiv 0$, and so $M(\mathfrak{m}_i f) \neq 0$. Thus, $\lambda_i \neq 0$. Then, $|\frac{\mu_i}{\lambda_i}| = 1$ iff $\lambda_i = \mu_i$. In other words, $|\frac{\mu_i}{\lambda_i}| = 1$ iff $M(\mathfrak{m}_i f) = \mu_i I_2$ for some real $\mu_i \neq 0$.

Since f does not satisfy 1ST-ORTH, by Lemma 3.15, there is an index i such that $M(\mathfrak{m}_i f) \neq \mu_i I_2$

for any real $\mu_i \neq 0$. Thus, $M(\mathfrak{m}_i f)$ has two eigenvalues with different norms. By Lemma 3.24, we can realize a nonzero binary signature g such that $M(g)$ is degenerate. This implies that g can be factorized as a tensor product of two nonzero unary signatures. By Lemma 3.6, we can realize a nonzero unary signature and hence by Theorem 5.35, Holant$(\mathcal{F})$ is #P-hard. □

For real-valued $\mathcal{F}$ that does not satisfy condition (T), assuming that every $f \in \mathcal{F}$ satisfies 1st-Orth, we further show that every irreducible $f \in \mathcal{F}$ of arity at least 4 satisfies 2nd-Orth, or otherwise Holant$(\mathcal{F})$ is #P-hard. The proof is based on dichotomies of #CSP problems, #EO problems and eight-vertex models. The eight-vertex model can be expressed by the problem Holant$(\neq_2 \mid f)$ where f is a 4-ary signature with even parity. The complexity classification of this problem is known even when f does not satisfy ars [19]. Here, we restate this result for signatures with ars.

Theorem 6.2. *Let $\widehat{f}$ be a complex-valued signature with matrix form $M(\widehat{f}) = \left[\begin{smallmatrix} c & 0 & 0 & a \\ 0 & d & b & 0 \\ 0 & \overline{b} & \overline{d} & 0 \\ \overline{a} & 0 & 0 & \overline{c} \end{smallmatrix}\right]$. Then,* Holant$(\neq_2 \mid \widehat{f})$ *is #P-hard if*

- *$\widehat{f}$ has support 6, or*
- *$\widehat{f}$ has support 4 and the nonzero entries of $M(\widehat{f})$ do not have the same norm, or*
- *$\widehat{f}$ has support 8, all nonzero entries of $M(\widehat{f})$ are positive real numbers and are not all equal.*

Otherwise, Holant$(\neq_2 \mid \widehat{f})$ *is tractable.*

Since #EO problems and eight-vertex models are defined as special cases of the problem Holant$(\neq_2 \mid \widehat{\mathcal{F}})$, for convenience, we will consider the problem Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ which is equivalent to Holant$(\mathcal{F})$. Recall that $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ satisfies ars, and a signature $\widehat{f}$ with ars satisfies 2nd-Orth iff there exists $\lambda \neq 0$ such that for all pairs of indices $\{i, j\} \subseteq [n]$, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \lambda N_4$.

We first consider that case that $\mathcal{DEQ}$ is available, where $\mathcal{DEQ} = \{\neq_2, \ldots, \neq_{2k}, \ldots\}$ is the set of all disequality signatures.

Lemma 6.3. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T). *Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. Then,* Holant$(\mathcal{DEQ} \mid \widehat{\mathcal{F}})$ *is #P-hard.*

证明. Since $\mathcal{F}$ does not satisfy condition (T), by Lemma 2.37, $\widehat{\mathcal{F}} \not\subseteq \mathscr{P}$ and $\widehat{\mathcal{F}} \not\subseteq \mathscr{A}$. If $\widehat{\mathcal{F}}$ is a set of EO signatures, then EO$(\widehat{\mathcal{F}}) \equiv_T$ Holant$(\neq_2 \mid \widehat{\mathcal{F}}) \leqslant_T$ Holant$(\mathcal{DEQ} \mid \mathcal{F})$. By Theorem 4.1, when

$\widehat{\mathcal{F}} \not\subseteq \mathscr{P}$ and $\widehat{\mathcal{F}} \not\subseteq \mathscr{A}$, $\operatorname{EO}(\widehat{\mathcal{F}})$ is #P-hard, and hence $\operatorname{Holant}(\mathcal{DEQ} \mid \widehat{\mathcal{F}})$ is #P-hard. Thus, we may assume that there is a signature $\widehat{f} \in \widehat{\mathcal{F}}$ whose support is not half-weighted. Suppose that $\widehat{f}$ has arity $2n$. Since $\mathscr{S}(\widehat{f}) \not\subseteq \mathscr{H}_{2n}$, by ARS, there is an $\alpha \in \mathbb{Z}_2^{2n}$ with $\operatorname{wt}(\alpha) = k < n$ such that $\widehat{f}(\alpha) \neq 0$. We first show that we can realize a signature $\widehat{g}$ of arity $2n - 2k$ such that $\widehat{g}(\vec{0}) \neq 0$. If $\operatorname{wt}(\alpha) = k = 0$, then we are done. Otherwise, we have $n > k \geqslant 1$. Thus, $2n \geqslant 4$ and α has length at least 4. By Lemma 3.9, there is a pair of indices $\{i, j\}$ such that $\widehat{\partial}_{ij}\widehat{f}(\beta) \neq 0$ for some $\operatorname{wt}(\beta) = k - 1$. Clearly, $\widehat{\partial}_{ij}\widehat{f}$ has arity $2n - 2$. Since $0 \leqslant k - 1 < (2n-2)/2$, $\widehat{\partial}_{ij}\widehat{f}$ is not an EO signature. Now we can continue this process, and by a chain of merging gadgets using $\neq_2$, we can realize a signature $\widehat{g}$ of arity $2m = 2n - 2k$ such that $\widehat{g}(\vec{0}) \neq 0$. Denote by $a = \widehat{g}(\vec{0})$.

Then, we connect all $2m$ variables of $\widehat{g}$ with $2m$ variables of $\neq_{4m}$ that always take the same value in $\mathscr{S}(\neq_{4m})$ using $\neq_2$. We get a signature $\widehat{h}$ of arity $2m$ where $\widehat{h}(\vec{0}) = a$, $\widehat{h}(\vec{1}) = \bar{a}$ by ARS, and $\widehat{h}(\gamma) = 0$ elsewhere. Then, consider the holographic transformation by $\widehat{Q} = \left[\begin{smallmatrix} \sqrt[2m]{\bar{a}} & 0 \\ 0 & \sqrt[2m]{a} \end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$. It transforms $\widehat{h}$ to $\neq_{2m}$, but does not change $\mathcal{DEQ}$. Thus,

$$\operatorname{Holant}(\mathcal{DEQ} \mid \widehat{h}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\mathcal{DEQ} \mid =_{2m}, \widehat{Q}\widehat{\mathcal{F}}).$$

If $2m = 2$, then we can show that

$$\#\operatorname{CSP}_2(\neq_2, \widehat{Q}\widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\mathcal{EQ}_2 \mid \neq_2, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\mathcal{DEQ} \mid =_2, \widehat{Q}\widehat{\mathcal{F}}).$$

If $2m > 2$, then by Lemma 5.4, we have

$$\#\operatorname{CSP}_{2m}(\neq_2, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2 \mid =_{2m}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\mathcal{DEQ} \mid =_{2m}, \widehat{Q}\widehat{\mathcal{F}}).$$

Thus, for all $2m \geqslant 2$, $\#\operatorname{CSP}_{2m}(\neq_2, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\mathcal{DEQ} \mid =_{2m}, \widehat{Q}\widehat{\mathcal{F}})$. Recall that $\widehat{Q}\widehat{\mathcal{F}} = \widehat{Q\mathcal{F}}$. Since $\mathcal{F}$ does not satisfy condition (T), $Q\mathcal{F}$ also does not satisfy it. By Theorem 5.5, $\#\operatorname{CSP}_{2m}(\neq_2, \widehat{Q\mathcal{F}})$ is #P-hard when $Q\mathcal{F}$ does not satisfy condition (T). Thus, $\operatorname{Holant}(\mathcal{DEQ} \mid =_{2m}, \widehat{Q}\widehat{\mathcal{F}})$ is #P-hard, and then $\operatorname{Holant}(\mathcal{DEQ} \mid \widehat{\mathcal{F}})$ is #P-hard. □

Then, we consider 4-ary signatures $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ realized by mating using $\neq_2$. We show that they have even parity. Then, we can invoke the existing dichotomy of eight-vertex models.

Lemma 6.4. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. If $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ contains a signature $\widehat{f}$ of arity $2n \geqslant 4$, then*

- $\operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$ *is #P-hard, or*
- *for all pairs of indices $\{i, j\}$, there exists a nonzero binary signature $\widehat{b}_{ij} \in \widehat{\mathcal{O}}$ such that $\widehat{b}_{ij}(x_i, x_j) \mid \widehat{f}$ or $M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \lambda_{ij} N_4$ for some real $\lambda_{ij} \neq 0$.*

证明. If $\widehat{f} \equiv 0$, then the lemma holds trivially since for all $\{i, j\}$ and any $\widehat{b}_{ij} \neq 0$, $\widehat{b}_{ij}(x_i, x_j) \mid \widehat{f}$. Thus, we may assume that $f \not\equiv 0$.

If $\widehat{f}$ does not satisfy 1st-Orth, then f does not satisfy it. By Lemma 6.1, $\operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(=_2|\, \mathcal{F})$ is #P-hard. Thus, we may assume that $\widehat{f}$ satisfies 1st-Orth. Then, for all indices i, we have

$$M(\widehat{\mathfrak{m}}_i\widehat{f}) = \begin{bmatrix} \langle \widehat{\mathbf{f}}_i^0, \widehat{\mathbf{f}}_i^1 \rangle & |\widehat{\mathbf{f}}_i^0|^2 \\ |\widehat{\mathbf{f}}_i^1|^2 & \langle \widehat{\mathbf{f}}_i^1, \widehat{\mathbf{f}}_i^0 \rangle \end{bmatrix} = \mu \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

For any variable x_i, we may take another variable x_j ($j \neq i$) and partition the sum in the inner product $\langle \widehat{\mathbf{f}}_i^0, \widehat{\mathbf{f}}_i^1 \rangle = 0$ into two sums depending on whether $x_j = 0$ or 1. Also, by ars we have

$$\langle \widehat{\mathbf{f}}_i^0, \widehat{\mathbf{f}}_i^1 \rangle = \langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{10} \rangle + \langle \widehat{\mathbf{f}}_{ij}^{01}, \widehat{\mathbf{f}}_{ij}^{11} \rangle = \langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{10} \rangle + \langle \overline{\widehat{\mathbf{f}}_{ij}^{10}}, \overline{\widehat{\mathbf{f}}_{ij}^{00}} \rangle = 2\langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{10} \rangle = 0.$$

Thus, for all pairs of indices $\{i, j\}$, $\langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{10} \rangle = 0$ and $\langle \widehat{\mathbf{f}}_{ij}^{01}, \widehat{\mathbf{f}}_{ij}^{11} \rangle = 0$. (Note that by exchanging i and j we also have $\langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{01} \rangle = 0$ and $\langle \widehat{\mathbf{f}}_{ij}^{10}, \widehat{\mathbf{f}}_{ij}^{11} \rangle = 0$.) Also by ars, we have $|\widehat{\mathbf{f}}_{ij}^{00}|^2 = |\overline{\widehat{\mathbf{f}}_{ij}^{11}}|^2 = |\widehat{\mathbf{f}}_{ij}^{11}|^2$ and $|\widehat{\mathbf{f}}_{ij}^{01}|^2 = |\overline{\widehat{\mathbf{f}}_{ij}^{10}}|^2 = |\widehat{\mathbf{f}}_{ij}^{10}|^2$.

Now, consider $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ for all pairs of indices $\{i, j\}$.

$$M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \begin{bmatrix} \widehat{\mathbf{f}}_{ij}^{00} \\ \widehat{\mathbf{f}}_{ij}^{01} \\ \widehat{\mathbf{f}}_{ij}^{10} \\ \widehat{\mathbf{f}}_{ij}^{11} \end{bmatrix} \begin{bmatrix} \overline{\widehat{\mathbf{f}}_{ij}^{11}}^{\mathrm{T}} & \overline{\widehat{\mathbf{f}}_{ij}^{10}}^{\mathrm{T}} & \overline{\widehat{\mathbf{f}}_{ij}^{01}}^{\mathrm{T}} & \overline{\widehat{\mathbf{f}}_{ij}^{00}}^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} \langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{11} \rangle & 0 & 0 & |\widehat{\mathbf{f}}_{ij}^{00}|^2 \\ 0 & \langle \widehat{\mathbf{f}}_{ij}^{01}, \widehat{\mathbf{f}}_{ij}^{10} \rangle & |\widehat{\mathbf{f}}_{ij}^{01}|^2 & 0 \\ 0 & |\widehat{\mathbf{f}}_{ij}^{10}|^2 & \langle \widehat{\mathbf{f}}_{ij}^{10}, \widehat{\mathbf{f}}_{ij}^{01} \rangle & 0 \\ |\widehat{\mathbf{f}}_{ij}^{11}|^2 & 0 & 0 & \langle \widehat{\mathbf{f}}_{ij}^{11}, \widehat{\mathbf{f}}_{ij}^{00} \rangle \end{bmatrix}.$$

Note that $|\langle \widehat{\mathbf{f}}_{ij}^{00}, \widehat{\mathbf{f}}_{ij}^{11} \rangle| \leqslant |\widehat{\mathbf{f}}_{ij}^{00}| \cdot |\widehat{\mathbf{f}}_{ij}^{11}|$ by Cauchy-Schwarz inequality. Clearly, $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ has even parity, and thus it represents a signature of the eight-vertex model. If there exists a pair of indices $\{i, j\}$ such that $\operatorname{Holant}(\neq_2|\, \widehat{\mathfrak{m}}_{ij}\widehat{f})$ is #P-hard, then we are done since $\operatorname{Holant}(\neq_2|\, \widehat{\mathfrak{m}}_{ij}\widehat{f}) \leqslant_T \operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$.

Thus, we may assume all $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ belong to the tractable family for eight-vertex models. Clearly, by observing its antidiagonal entries of the matrix $M(\widehat{\mathfrak{m}}_{ij}\widehat{f})$, we have $\widehat{\mathfrak{m}}_{ij}\widehat{f} \not\equiv 0$ since $\widehat{f} \not\equiv 0$. By Theorem 6.2, there are three possible cases.

- There exists a pair $\{i, j\}$ such that $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ has support of size 2. By Cauchy-Schwarz inequality, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f})$ is either of the form $\lambda_{ij}\left[\begin{smallmatrix} 0&0&0&1\\ 0&0&0&0\\ 0&0&0&0\\ 1&0&0&0 \end{smallmatrix}\right]$ where $\lambda_{ij} = |\widehat{\mathbf{f}}^{00}_{ij}|^2 = |\widehat{\mathbf{f}}^{11}_{ij}|^2 \neq 0$ or $\lambda_{ij}\left[\begin{smallmatrix} 0&0&0&0\\ 0&0&1&0\\ 0&1&0&0\\ 0&0&0&0 \end{smallmatrix}\right]$ where $\lambda_{ij} = |\widehat{\mathbf{f}}^{01}_{ij}| = |\widehat{\mathbf{f}}^{10}_{ij}| \neq 0$. In both cases, $\neq_4$ is realizable since $\lambda_{ij} \neq 0$. The form that $\langle \widehat{\mathbf{f}}^{01}_{ij}, \widehat{\mathbf{f}}^{10}_{ij} \rangle \neq 0$ while $|\widehat{\mathbf{f}}^{01}_{ij}|^2 = |\widehat{\mathbf{f}}^{10}_{ij}|^2 = 0$ cannot occur since $|\langle \widehat{\mathbf{f}}^{01}_{ij}, \widehat{\mathbf{f}}^{10}_{ij} \rangle| \leqslant |\widehat{\mathbf{f}}^{01}_{ij}||\widehat{\mathbf{f}}^{10}_{ij}|$. Also, the form that $\langle \widehat{\mathbf{f}}^{00}_{ij}, \widehat{\mathbf{f}}^{11}_{ij} \rangle \neq 0$ while $|\widehat{\mathbf{f}}^{00}_{ij}|^2 = |\widehat{\mathbf{f}}^{11}_{ij}|^2 = 0$ cannot occur. Since $\neq_4$ is available, by Lemma 4.25, $\operatorname{Holant}(\mathcal{DEQ} \mid \widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(=_2 \mid \widehat{\mathcal{F}})$. By Lemma 6.3, $\operatorname{Holant}(=_2 \mid \widehat{\mathcal{F}})$ is #P-hard.

- There exists a pair $\{i, j\}$ such that $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ has support of size 8. We can rename the four variables of $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ in a cyclic permutation. We use $\widehat{g}$ to denote this signature. Then $M(\widehat{g}) = M_{12}(\widehat{g}) = \left[\begin{smallmatrix} c&0&0&d\\ 0&a&b&0\\ 0&b&a&0\\ \bar{d}&0&0&\bar{c} \end{smallmatrix}\right]$ where a and b are positive real numbers and c and d are nonzero complex numbers. Consider the signature $\widehat{\mathfrak{m}}_{12}\widehat{g}$ realized by mating $\widehat{g}$. We denote it by $\widehat{h}$. Then,

  $$M(\widehat{h}) = M(\widehat{g})N_4M^{\mathrm{T}}(\widehat{g}) = \begin{bmatrix} 2cd & 0 & 0 & |c|^2+|d|^2 \\ 0 & 2ab & a^2+b^2 & 0 \\ 0 & a^2+b^2 & 2ab & 0 \\ |c|^2+|d|^2 & 0 & 0 & 2\bar{c}\bar{d} \end{bmatrix} = \begin{bmatrix} c' & 0 & 0 & d' \\ 0 & a' & b' & 0 \\ 0 & b' & a' & 0 \\ d' & 0 & 0 & \bar{c'} \end{bmatrix},$$

  where a', b', and d' are positive real numbers and c' is a nonzero complex number. Suppose that the argument of c' is θ, i.e., $c' = |c'|e^{\mathrm{i}\theta}$.

  Consider the holographic transformation by $\widehat{Q} = \left[\begin{smallmatrix} e^{-\mathrm{i}\theta/4} & 0\\ 0 & e^{\mathrm{i}\theta/4} \end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$. Then,

  $$\operatorname{Holant}(\neq_2 \mid \widehat{h}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\neq_2 \mid \widehat{Q}\widehat{h}, \widehat{Q}\widehat{\mathcal{F}}).$$

  Note that $M(\widehat{Q}\widehat{h}) = \left[\begin{smallmatrix} |c'|&0&0&d'\\ 0&a'&b'&0\\ 0&b'&a'&0\\ d'&0&0&|c'| \end{smallmatrix}\right]$ where all entries are positive real numbers. Notice that all weight 2 entries of $\widehat{h}$ are unchanged in $\widehat{Q}\widehat{h}$. By Theorem 6.2, $\operatorname{Holant}(\neq_2 \mid \widehat{Q}\widehat{h})$ is #P-hard unless $a' = b' = |c'| = d'$. Thus, we may assume that $M(\widehat{Q}\widehat{h}) = \left[\begin{smallmatrix} 1&0&0&1\\ 0&1&1&0\\ 0&1&1&0\\ 1&0&0&1 \end{smallmatrix}\right]$ up to normalization. Notice that $M(Z(\widehat{Q}\widehat{h})) = Z^{\otimes 2}M(\widehat{Q}\widehat{h})(Z^{\mathrm{T}})^{\otimes 2} = \left[\begin{smallmatrix} 1&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{smallmatrix}\right]$, which is the arity-4 equality ($=_4$).

Consider the holographic transformation by Z which transfers $\neq_2$ back to $=_2$. Remember that $\widehat{Q} = Z^{-1}QZ$. Then, $Z(\widehat{Q}\widehat{\mathcal{F}}) = Z(Z^{-1}QZ)(Z^{-1}\mathcal{F}) = Q\mathcal{F}$. Since $\widehat{Q} \in \widehat{\mathbf{O}_2}$, we have $Q \in \mathbf{O}_2$. Thus,

$$\operatorname{Holant}(\neq_2 |\ \widehat{Q}\widehat{h}, \widehat{Q}\widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(=_2|=_4, Q\mathcal{F}).$$

By Lemma 2.24, $\#\text{CSP}_2(Q\mathcal{F}) \leqslant_T \operatorname{Holant}(=_2|=_4, Q\mathcal{F})$. Since $\mathcal{F}$ does not satisfy condition (T) and $Q \in \mathbf{O}_2$, $Q\mathcal{F}$ also does not satisfy condition (T). By Theorem 2.34, $\#\text{CSP}_2(Q\mathcal{F})$ is #P-hard. Thus, $\operatorname{Holant}(\neq_2|\ \widehat{\mathcal{F}})$ is #P-hard.

- For all $\{i, j\}$, $\widehat{\mathfrak{m}}_{ij}\widehat{f}$ has support of size 4. By Cauchy-Schwarz inequality, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f})$ is of the form $\begin{bmatrix} b & 0 & 0 & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a & 0 & 0 & \bar{b} \end{bmatrix}$ or $\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & b & a & 0 \\ 0 & a & \bar{b} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ where $a^2 - |b|^2 = 0$, or the form $\lambda_{ij} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ where $\lambda_{ij} = |\widehat{\mathbf{f}}_{ij}^{00}|^2 = |\widehat{\mathbf{f}}_{ij}^{01}| \neq 0$. If $M(\mathfrak{m}_{ij}\widehat{f}) = \lambda_{ij}N_4$, then we are done. Otherwise, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f})$ has rank one. Hence, $M_{ij}(\widehat{f})$ also has rank one. Then, by observing the form of $M(\widehat{\mathfrak{m}}_{ij}\widehat{f})$ especially the all zero rows, $\widehat{f}$ can be factorized as $\widehat{b}_{ij}(x_i, x_j) \otimes \widehat{g}$ where $\widehat{b}_{ij} \in \widehat{\mathcal{O}}$ and $\widehat{g}$ is a signature on the other $n-2$ variables. Thus, we are done.

The lemma is proved. □

Remark 6.5. *We give a restatement of Lemma 6.4 in the setting of* $\operatorname{Holant}(\mathcal{F})$*. Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Let $f \in \mathcal{F}$ be a signature of arity $2n \geqslant 4$. Then,* $\operatorname{Holant}(\mathcal{F})$ *is #P-hard, or for all pairs of indices $\{i, j\}$, there exists a nonzero binary signature $b_{ij} \in \mathcal{O}$ such that $b_{ij}(x_i, x_j) \mid f$ or $M(\mathfrak{m}_{ij}f) = \lambda_{ij}I_4$ for some real $\lambda_{ij} \neq 0$.*

Now for an irreducible signature $\widehat{f}$ of arity $2n \geqslant 4$, we show that it satisfies 2ND-ORTH or we get #P-hardness.

Lemma 6.6. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition* (T)*. Let $\widehat{f} \in \widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ be an irreducible signature of arity $2n \geqslant 4$. If $\widehat{f}$ does not satisfy* 2ND-ORTH*, then* $\operatorname{Holant}(\neq|\ \widehat{\mathcal{F}})$ *is #P-hard.*

证明. Since $\widehat{f}$ is irreducible, by Lemma 6.4, $M(\widehat{\mathfrak{m}}_{ij}\widehat{f}) = \lambda_{ij}N_4$ for all $\{i, j\}$. Now, we show all λ_{ij} have the same value. If we connect further the two respective pairs of variables of $\mathfrak{m}_{ij}f$, which totally connects two copies of f, we get a value $4\lambda_{ij}$. This value clearly does not depend on the particular indices $\{i, j\}$. We denote the value λ_{ij} by λ. This value is nonzero because $\widehat{f}$ is irreducible. □

We derive some consequences from the condition 2nd-Orth for signatures with ars. Suppose that $\widehat{f}$ satisfies 2nd-Orth. First, by definition we have $|\widehat{\mathbf{f}}_{ij}^{ab}|^2 = \lambda$ for any $(x_i, x_j) = (a, b) \in \{0,1\}^2$. Given a vector $\widehat{\mathbf{f}}_{ij}^{ab}$, we can pick a third variable x_k and partition $\widehat{\mathbf{f}}_{ij}^{ab}$ into two vectors $\widehat{\mathbf{f}}_{ijk}^{ab0}$ and $\widehat{\mathbf{f}}_{ijk}^{ab1}$ according to $x_k = 0$ or 1. By setting $(a, b) = (0, 0)$, we have

$$|\widehat{\mathbf{f}}_{ij}^{00}|^2 = |\widehat{\mathbf{f}}_{ijk}^{000}|^2 + |\widehat{\mathbf{f}}_{ijk}^{001}|^2 = \lambda. \tag{6.1}$$

Similarly, we consider the vector $\widehat{\mathbf{f}}_{ik}^{00}$ and partition it according to $x_j = 0$ or 1. We have

$$|\widehat{\mathbf{f}}_{ik}^{00}|^2 = |\widehat{\mathbf{f}}_{ijk}^{000}|^2 + |\widehat{\mathbf{f}}_{ijk}^{010}|^2 = \lambda. \tag{6.2}$$

Comparing equations (6.1) and (6.2), we have $|\widehat{\mathbf{f}}_{ijk}^{001}|^2 = |\widehat{\mathbf{f}}_{ijk}^{010}|^2$. Moreover, by ars, we have $|\widehat{\mathbf{f}}_{ijk}^{010}|^2 = |\widehat{\mathbf{f}}_{ijk}^{101}|^2$. Thus, we have $|\widehat{\mathbf{f}}_{ijk}^{001}|^2 = |\widehat{\mathbf{f}}_{ijk}^{101}|^2$. Note that the vector $\widehat{\mathbf{f}}_{jk}^{01}$ is partitioned into two vectors $\widehat{\mathbf{f}}_{ijk}^{001}$ and $\widehat{\mathbf{f}}_{ijk}^{101}$ according to $x_i = 0$ or 1. That is

$$|\widehat{\mathbf{f}}_{jk}^{01}|^2 = |\widehat{\mathbf{f}}_{ijk}^{001}|^2 + |\widehat{\mathbf{f}}_{ijk}^{101}|^2 = \lambda.$$

Thus, we have $|\widehat{\mathbf{f}}_{ijk}^{001}|^2 = |\widehat{\mathbf{f}}_{ijk}^{101}|^2 = \lambda/2$. Then, by equation (6.1), we have $|\widehat{\mathbf{f}}_{ijk}^{000}|^2 = \lambda/2$, and again by ars, we also have $|\widehat{\mathbf{f}}_{ijk}^{111}|^2 = |\widehat{\mathbf{f}}_{ijk}^{000}|^2 = \lambda/2$. Note that indices i, j, k are picked arbitrarily, by symmetry, we have

$$|\widehat{\mathbf{f}}_{ijk}^{abc}|^2 = \lambda/2 \tag{6.3}$$

for all $(x_i, x_j, x_k) = (a, b, c) \in \{0,1\}^3$.

Given a vector $\widehat{\mathbf{f}}_{ijk}^{abc}$, we can continue to pick a fourth variable x_ℓ and partition $\widehat{\mathbf{f}}_{ijk}^{abc}$ into two vectors $\widehat{\mathbf{f}}_{ijk\ell}^{abc0}$ and $\widehat{\mathbf{f}}_{ijk\ell}^{abc1}$ according to $x_\ell = 0$ or 1. By setting $(a, b, c) = (0, 0, 0)$, we have from (6.3)

$$|\widehat{\mathbf{f}}_{ijk}^{000}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{0000}|^2 + |\widehat{\mathbf{f}}_{ijk\ell}^{0001}|^2 = \lambda/2. \tag{6.4}$$

Similarly, we consider the vector $\widehat{\mathbf{f}}_{ij\ell}^{001}$ and partition it according to $x_k = 0$ or 1. We have

$$|\widehat{\mathbf{f}}_{ij\ell}^{001}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{0001}|^2 + |\widehat{\mathbf{f}}_{ijk\ell}^{0011}|^2 = \lambda/2. \tag{6.5}$$

Comparing equations (6.4) and (6.5), and also by ARS, we have

$$|\widehat{\mathbf{f}}_{ijk\ell}^{0000}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{0011}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{1100}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{1111}|^2 \tag{6.6}$$

for all indices $\{i, j, k, \ell\}$. Similarly, we can get

$$|\widehat{\mathbf{f}}_{ijk\ell}^{0001}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{0010}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{1101}|^2 = |\widehat{\mathbf{f}}_{ijk\ell}^{1110}|^2. \tag{6.7}$$

By the definition of second order orthogonality, we also have

$$\langle \widehat{\mathbf{f}}_{ij}^{ab}, \widehat{\mathbf{f}}_{ij}^{cd} \rangle = 0 \tag{6.8}$$

for all variables x_i, x_j and $(a, b) \neq (c, d)$.

Equations (6.6), (6.7) and (6.8) will be used frequently in the analysis of signatures satisfying ARS and 2ND-ORTH. This is also a reason why we consider the problem in the setting under the Z^{-1} transformation, Holant($\neq_2 |\, \widehat{\mathcal{F}}$), where we can express these consequences of 2ND-ORTH elegantly, instead of Holant($\mathcal{F}$) which is logically equivalent. By combining 2ND-ORTH and ARS of the signature $\widehat{f}$, we get these simply expressed, thus easily applicable, conditions in terms of norms and inner products.

6.2 The Induction Proof: Base Cases $2n \leqslant 4$

In this section, we introduce the induction framework and handle the base cases (Lemmas 6.7 and 6.8). Recall that $\widehat{\mathcal{O}}$ denotes the set of binary signatures with ARS and parity (including the binary zero signature), and $\widehat{\mathcal{O}}^{\otimes}$ denotes the set of tensor products of signatures in $\widehat{\mathcal{O}}$. Since $\mathcal{F}$ does not satisfy condition (T), $\widehat{\mathcal{F}} \not\subseteq \mathscr{T}$. Also, since $\widehat{\mathcal{O}}^{\otimes} \subseteq \mathscr{T}$, $\widehat{\mathcal{F}} \not\subseteq \widehat{\mathcal{O}}^{\otimes}$. Thus, there is a nonzero signature $\widehat{f} \in \widehat{\mathcal{F}}$ of arity $2n$ such that $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$. We want to achieve a proof of #P-hardness by induction on $2n$. We first consider the base that $2n = 2$. Notice that a nonzero binary signature

$\widehat{f}$ satisfies 1ST-ORTH iff its matrix form (as a 2-by-2 matrix) is orthogonal. Thus, $\widehat{f} \notin \widehat{\mathcal{O}}$ implies that it does not satisfy 1ST-ORTH. Then, we have the following result.

Lemma 6.7. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. If $\mathcal{F}$ contains a binary signature $f \notin \mathcal{O}^{\otimes}$, then* $\operatorname{Holant}(\mathcal{F})$ *is #P-hard. Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. Equivalently, if $\widehat{\mathcal{F}}$ contains a binary signature $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then* $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is #P-hard.*

证明. We prove this lemma in the setting of $\operatorname{Holant}(\mathcal{F})$. Since $\mathcal{O}^{\otimes}$ contains the binary zero signature, $f \notin \mathcal{O}^{\otimes}$ implies that $f \not\equiv 0$. If f is reducible, then it is a tensor product of two nonzero unary signatures. By Lemma 3.6, we can realize a nonzero unary signature by factorization, and we are done by Theorem 5.35. Otherwise, f is irreducible. Since $f \notin \mathcal{O}^{\otimes}$, f does not satisfy 1ST-ORTH. By Lemma 6.1, $\operatorname{Holant}(\mathcal{F})$ is #P-hard. □

Then, the general induction framework is that we start with a signature $\widehat{f}$ of arity $2n \geqslant 4$ that is not in $\widehat{\mathcal{O}}^{\otimes}$, and realize a signature $\widehat{g}$ of arity $2k \leqslant 2n-2$ that is also not in $\widehat{\mathcal{O}}^{\otimes}$, or otherwise we can directly show $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard. If we can reduce the arity down to 2 (by a sequence of reductions of length independent of the problem instance size), then we have a binary signature $\widehat{b} \notin \widehat{\mathcal{O}}$. By Lemma 6.7, we are done.

For the inductive step, we first consider the case that $\widehat{f}$ is reducible. Suppose that $\widehat{f} = \widehat{f_1} \otimes \widehat{f_2}$. If $\widehat{f_1}$ or $\widehat{f_2}$ have odd arity, then we can realize a signature of odd arity by factorization and we are done. Otherwise, $\widehat{f_1}$ and $\widehat{f_2}$ have even arity. Since $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, we know $\widehat{f_1}$ and $\widehat{f_2}$ cannot both be in $\widehat{\mathcal{O}}^{\otimes}$. Then, we can realize a signature of lower arity that is not in $\widehat{\mathcal{O}}^{\otimes}$ by factorization. We are done. Thus, in the following we may assume that $\widehat{f}$ is irreducible. Then, we may further assume that $\widehat{f}$ satisfies 2ND-ORTH. Otherwise, we get #P-hardness by Lemma 6.6. We use merging with $\neq_2$ to realize signatures of arity $2n-2$ from $\widehat{f}$. Consider $\widehat{\partial}_{ij}\widehat{f}$ for all pairs of indices $\{i, j\}$. If there exists a pair $\{i, j\}$ such that $\widehat{\partial}_{ij}\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then we can realize $\widehat{g} = \widehat{\partial}_{ij}\widehat{f}$ which has arity $2n-2$, and we are done. Thus, we may assume $\widehat{\partial}_{ij}\widehat{f} \in \widehat{\mathcal{O}}^{\otimes}$ for all $\{i, j\}$. We denote this property by $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$. We want to achieve our induction proof based on these two properties: 2ND-ORTH and $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$. We consider the case that $2n = 4$.

Lemma 6.8. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy* *condition* (T). *Let* $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. *If* $\widehat{\mathcal{F}}$ *contains a* 4*-ary signature* $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, *then* $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is* #*P-hard.*

证明. Since $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, $f \not\equiv 0$. First, we may assume that $\widehat{f}$ is irreducible. Otherwise, we can realize a nonzero unary signature or a binary signature that is not in $\widehat{\mathcal{O}}$. Then, by Theorem 5.35 and Lemma 6.7, we have #P-hardness. Since $\widehat{f}$ is irreducible, we may further assume that $\widehat{f}$ satisfies 2nd-Orth. Otherwise, by Lemma 6.6, we get #P-hardness.

We consider binary signatures $\widehat{\partial}_{ij}\widehat{f}$ realized from $\widehat{f}$ by merging using $\neq_2$. Under the assumption that $\widehat{f}$ satisfies 2nd-Orth, we will show that there exits a pair $\{i,j\}$ such that $\widehat{\partial}_{ij}\widehat{f} \notin \widehat{\mathcal{O}}$. Then by Lemma 6.7, we are done. For a contradiction, suppose that $\widehat{f} \in \int\widehat{\mathcal{O}}$ i.e., $\widehat{\partial}_{ij}\widehat{f} \in \widehat{\mathcal{O}}$ for all pairs $\{i,j\}$. Since $\widehat{f}$ satisfies 2nd-Orth, by equations (6.6) and (6.7), we have $|\widehat{\mathbf{f}}^{0000}_{ijk\ell}| = |\widehat{\mathbf{f}}^{0011}_{ijk\ell}| = |\widehat{\mathbf{f}}^{1111}_{ijk\ell}|$ and $|\widehat{\mathbf{f}}^{0001}_{ijk\ell}| = |\widehat{\mathbf{f}}^{1110}_{ijk\ell}|$ respectively for any permutation (i,j,k,ℓ) of $(1,2,3,4)$. Thus all entries of $\widehat{f}$ on inputs of even weight $\{0,2,4\}$ have the same norm, and all entries of $\widehat{f}$ on inputs of odd weight $\{1,3\}$ have the same norm. We denote by ν_0 and ν_1 the norm squares of entries on inputs of even weight and odd weight, respectively.

Then, we consider the equation $\langle \widehat{\mathbf{f}}^{01}_{12}, \widehat{\mathbf{f}}^{10}_{12}\rangle = 0$ from (6.8) by taking $(i,j) = (1,2)$. We have

$$\langle \widehat{\mathbf{f}}^{01}_{12}, \widehat{\mathbf{f}}^{10}_{12}\rangle = \widehat{f}^{0100}\overline{\widehat{f}^{1000}} + \widehat{f}^{0101}\overline{\widehat{f}^{1001}} + \widehat{f}^{0110}\overline{\widehat{f}^{1010}} + \widehat{f}^{0111}\overline{\widehat{f}^{1011}} = 0.$$

(Here for clarity, we omitted the subscript 1234 of $\widehat{f}^{abcd}_{1234}$.) By ars, we have $\widehat{f}^{0111}\overline{\widehat{f}^{1011}} = \overline{\widehat{f}^{1000}}\widehat{f}^{0100}$ and $\widehat{f}^{0110}\overline{\widehat{f}^{1010}} = \overline{\widehat{f}^{1001}}\widehat{f}^{0101}$. Thus, we have

$$\widehat{f}^{0100}\overline{\widehat{f}^{1000}} + \widehat{f}^{0101}\overline{\widehat{f}^{1001}} = 0. \tag{6.9}$$

Note that by taking norm, $|\widehat{f}^{0100}\overline{\widehat{f}^{1000}}| = \nu_1$ and $|\widehat{f}^{0101}\overline{\widehat{f}^{1001}}| = \nu_0$. Then, it follows that $\nu_0 = \nu_1$. Thus, all entries of $\widehat{f}$ have the same norm. We normalize the norm to be 1 since $\widehat{f} \not\equiv 0$.

Consider $\widehat{\partial}_{12}\widehat{f}$. We have

$$\widehat{\partial}_{12}\widehat{f} = (\widehat{f}^{0100} + \widehat{f}^{1000}, \quad \widehat{f}^{0101} + \widehat{f}^{1001}, \quad \widehat{f}^{0110} + \widehat{f}^{1010}, \quad \widehat{f}^{0111} + \widehat{f}^{1011}),$$

and by assumption $\widehat{\partial}_{12}\widehat{f} \in \widehat{\mathcal{O}}$. Thus, at least one of the two entries $\widehat{f}^{0100} + \widehat{f}^{1000}$ and $\widehat{f}^{0101} + \widehat{f}^{1001}$

is equal to zero. If $\widehat{f}^{0100} + \widehat{f}^{1000} = 0$, then we have

$$\widehat{f}^{0100}\overline{\widehat{f}^{1000}} = (-\widehat{f}^{1000})\overline{\widehat{f}^{1000}} = -|\widehat{f}^{1000}|^2 = -1.$$

Then, by equation (6.9), we have $\widehat{f}^{0101}\overline{\widehat{f}^{1001}} = 1$. Otherwise, $\widehat{f}^{0101} + \widehat{f}^{1001} = 0$. Then, we have $\widehat{f}^{0101}\overline{\widehat{f}^{1001}} = -1$ while $\widehat{f}^{0100}\overline{\widehat{f}^{1000}} = 1$. Thus, among these two products $\widehat{f}^{0100}\overline{\widehat{f}^{1000}}$ and $\widehat{f}^{0101}\overline{\widehat{f}^{1001}}$, exactly one is equal to 1, while the other is -1. Then, we have

$$\widehat{f}^{0100}\overline{\widehat{f}^{1000}}\widehat{f}^{0101}\overline{\widehat{f}^{1001}} = -1.$$

Similarly, by considering $\widehat{\partial}_{23}\widehat{f}$ and $\widehat{\partial}_{31}\widehat{f}$ respectively, we have

$$\widehat{f}^{0010}\overline{\widehat{f}^{0100}}\widehat{f}^{0011}\overline{\widehat{f}^{0101}} = -1, \qquad \text{and} \qquad \widehat{f}^{1000}\overline{\widehat{f}^{0010}}\widehat{f}^{1001}\overline{\widehat{f}^{0011}} = -1.$$

Multiply these three products, we have

$$|\widehat{f}^{0100}|^2|\widehat{f}^{0010}|^2|\widehat{f}^{1000}|^2|\widehat{f}^{0101}|^2|\widehat{f}^{0011}|^2|\widehat{f}^{1001}|^2 = (-1)^3 = -1.$$

A contradiction! □

Remark 6.9. *In this proof, we showed that there is no irreducible 4-ary signature $\widehat{f}$ that satisfies both* 2ND-ORTH *and* $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$.

If Lemma 6.8 were to hold for signatures of arity $2n \geqslant 6$, i.e., there is no irreducible signature $\widehat{f}$ of $2n \geqslant 6$ such that $\widehat{f}$ satisfies both 2ND-ORTH and $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$, then the induction proof holds and we are done. We show that this is true for signatures of arity $2n \geqslant 10$ in Section 8.3. However, there are extraordinary signatures of arity 6 and 8 with special closure properties (Bell properties) such that they satisfy both 2ND-ORTH and $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$.

Chapter 7

First Major Obstacle: 6-ary Signatures with the Bell Property

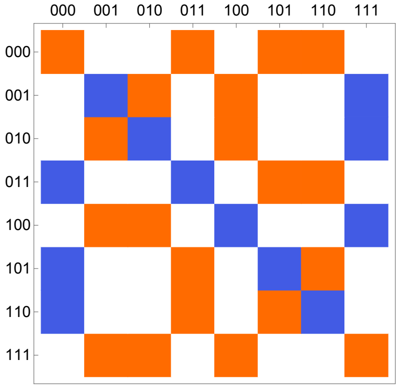
In this chapter, we consider the case that $\widehat{\mathcal{F}}$ contains a 6-ary signature that is not in $\widehat{\mathcal{O}}^{\otimes}$. We give a signature $\widehat{f_6}$ with extraordinary closure properties called the Bell property. The existence of $\widehat{f_6}$ presented a formidable obstacle to the induction proof. In order to handle the signature $\widehat{f_6}$, we introduce Holant^b problems where the four binary Bell signatures are available. We prove a #P-hardness result for Holant$^b(f_6, \mathcal{F})$.

7.1 The Discovery of $\widehat{f_6}$

We consider the following 6-ary signature $\widehat{f_6}$. Let $\widehat{f_6} = \chi_S \cdot (-1)^{x_1x_2+x_2x_3+x_1x_3+x_1x_4+x_2x_5+x_3x_6}$, where χ_S is the indicator function on the set $S = \mathscr{S}(\widehat{f_6}) = \mathscr{E}_6 = \{\alpha \in \mathbb{Z}_2^6 \mid \mathrm{wt}(\alpha) \equiv 0 \bmod 2\}$. One can check that $\widehat{f_6}$ is irreducible, and $\widehat{f_6}$ satisfies both 2nd-Orth and $\widehat{f} \in \int \widehat{\mathcal{O}}^{\otimes}$. $\widehat{f_6}$ has the following matrix form

$$M_{123,456}(\widehat{f_6}) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{7.1}$$

We use Figure 6 to visualize this matrix. A block with orange color denotes an entry $+1$ and a block with blue color denotes an entry -1. Other blank blocks are zeros.



	000	001	010	011	100	101	110	111
000	🟧			🟧		🟧	🟧	
001		🟦	🟧		🟧			🟦
010		🟧	🟦		🟧			🟦
011	🟦			🟦		🟧	🟧	
100		🟧	🟧		🟦			🟦
101	🟦			🟧		🟦	🟧	
110	🟦			🟧		🟧	🟦	
111		🟧	🟧		🟧			🟧

图 6: A visualization of $\widehat{f_6}$

In this subsection, we show how this extraordinary signature $\widehat{f_6}$ was discovered. We prove that if $\widehat{\mathcal{F}}$ contains a 6-ary signature $\widehat{f}$ where $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then $\operatorname{Holant}(\neq_2 |\, \widehat{\mathcal{F}})$ is #P-hard or $\widehat{f_6}$ is realizable from $\widehat{f}$ after a holographic transformation by some $\widehat{Q} \in \widehat{\mathbf{O}_2}$ (Theorem 7.5). The general strategy of this proof is to show that we can realize signatures with special properties from $\widehat{f}$ step by step (Lemmas 7.1, 7.2, 7.3 and 7.4), and finally we can realize $\widehat{f_6}$, or else we can realize signatures that lead to #P-hardness. So this $\widehat{f_6}$ emerges as essentially the unique (and true) obstacle to our proof of #P-hardness in this setting.

Lemma 7.1. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ contains a 6-ary signature $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then* $\operatorname{Holant}(\neq_2 |\, \widehat{\mathcal{F}})$ *is #P-hard, or an irreducible 6-ary signature $\widehat{f}'$ is realizable from $\widehat{f}$, where $\widehat{f}'(\alpha) = 0$ for all α with* $\operatorname{wt}(\alpha) = 2$ *or* 4*. Moreover, $\widehat{f}'$ is realizable by extending variables of $\widehat{f}$ with nonzero binary signatures in $\widehat{\mathcal{O}}$ that are realizable by factorization from $\widehat{\partial}_{12}\widehat{f}$.*

证明. Since $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, $\widehat{f} \not\equiv 0$. Again, we may assume that $\widehat{f}$ is irreducible. Otherwise, by factorization, we can realize a nonzero signature of odd arity, or a signature of arity 2 or 4 that is not in $\widehat{\mathcal{O}}^{\otimes}$. Then by Theorem 5.35, or Lemmas 6.7 or 6.8, we get #P-hardness. Under the assumption that $\widehat{f}$ is irreducible, we may further assume that $\widehat{f}$ satisfies 2ND-ORTH by Lemma 6.6. Also, we may assume that $\widehat{f} \in \int \widehat{\mathcal{O}}^{\otimes}$. Otherwise, there is a pair of indices $\{i, j\}$ such that the 4-ary signature $\widehat{\partial}_{ij}\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$. Then by Lemma 6.8, $\operatorname{Holant}(\neq_2 |\, \widehat{\mathcal{F}})$ is #P-hard.

If for all pairs of indices $\{i,j\}$, $\widehat{\partial}_{ij}\widehat{f}\equiv 0$, then by Lemma 3.9, we have $\widehat{f}(\alpha)=0$ for all α with $\text{wt}(\alpha)\neq 0$ and 6. Since $f\not\equiv 0$, clearly such a signature does not satisfy 2nd-Orth. Contradiction. Otherwise, there is a pair of indices $\{i,j\}$ such that $\widehat{\partial}_{ij}\widehat{f}\not\equiv 0$. By renaming variables, without loss of generality, we assume that $\widehat{\partial}_{12}\widehat{f}\not\equiv 0$. Since $\widehat{\partial}_{12}\widehat{f}\in\widehat{\mathcal{O}}^{\otimes}$, in the UPF of $\widehat{\partial}_{12}\widehat{f}$, by renaming variables we assume that variables x_3 and x_4 appear in one nonzero binary signature $\widehat{b_1}(x_3,x_4)\in\widehat{\mathcal{O}}^{\otimes}$, and variables x_5 and x_6 appear in the other nonzero binary signature $\widehat{b_2}(x_5,x_6)\in\widehat{\mathcal{O}}^{\otimes}$. Thus, we have

$$\widehat{\partial}_{12}\widehat{f}=\widehat{b_1}(x_3,x_4)\otimes\widehat{b_2}(x_5,x_6)\not\equiv 0.$$

By Lemma 3.6, we know that these two binary signatures $\widehat{b_1}$ and $\widehat{b_2}$ are realizable by factorization. Note that for a nonzero binary signature $\widehat{b_i}(x_{2i+1},x_{2i+2})\in\widehat{\mathcal{O}}$ $(i\in\{1,2\})$, if we connect the variable x_{2i+1} of two copies of $\widehat{b_i}(x_{2i+1},x_{2i+2})$ using $\neq_2$ (mating two binary signatures), then we get $\neq_2$ up to a nonzero scalar. We consider the following gadget construction G_1 on $\widehat{f}$. Recall that in the setting of $\text{Holant}(\neq\mid\widehat{\mathcal{F}})$, variables are connected using $\neq_2$. For $i\in\{1,2\}$, by a slight abuse of variable names, we connect the variable x_{2i+1} of $\widehat{f}$ with the variable x_{2i+1} of $\widehat{b_i}(x_{2i+1},x_{2i+2})$. We get a signature $\widehat{f'}$ of arity 6. Such a gadget construction does not change the irreducibility of f. Thus, $\widehat{f'}$ is irreducible. Again, we may assume that $\widehat{f'}\in\int\widehat{\mathcal{O}}^{\otimes}$ and $\widehat{f'}$ satisfies 2nd-Orth. Otherwise, we are done.

Consider $\widehat{\partial}_{12}\widehat{f'}$. Since the above gadget construction G_1 does not touch variables x_1 and x_2 of f, the operation of forming G_1 commutes with the merging operation $\widehat{\partial}_{12}$. Thus, $\widehat{\partial}_{12}\widehat{f'}$ can be realized by performing the gadget construction G_1 on $\widehat{\partial}_{12}\widehat{f}$, which connects each binary signature $\widehat{b_i}$ $(i\in\{1,2\})$ of $\widehat{\partial}_{12}\widehat{f}$ with another copy of itself using $\neq_2$ (in the mating fashion). Then, each $\widehat{b_i}$ in $\widehat{\partial}_{12}\widehat{f}$ is changed to $\neq_2$ up to a nonzero real scalar. After normalization and renaming variables, we have

$$\widehat{\partial}_{12}\widehat{f'}=(\neq_2)(x_3,x_4)\otimes(\neq_2)(x_5,x_6).$$

Since $\widehat{\partial}_{12}\widehat{f'}\in\mathcal{D}^{\otimes}$, for any $\{i,j\}$ disjoint with $\{1,2\}$ we have $\widehat{\partial}_{(ij)(12)}\widehat{f'}\in\mathcal{D}^{\otimes}$, and hence $\widehat{\partial}_{ij}\widehat{f'}\not\equiv 0$.

Now, we show that for all pairs of indices $\{i,j\}$, $\widehat{\partial}_{ij}\widehat{f'}$ has even parity. We first consider the case that $\{i,j\}$ is disjoint with $\{1,2\}$. Connect variables x_i and x_j of $\widehat{\partial}_{12}\widehat{f'}$ using $\neq_2$. Since $\widehat{\partial}_{12}\widehat{f'}$ has even parity, a merging gadget using $\neq_2$ will change the parity from even to odd. Thus, $\widehat{\partial}_{(ij)(12)}\widehat{f'}$ has odd parity. Consider $\widehat{\partial}_{ij}\widehat{f'}$. Remember that $\widehat{\partial}_{ij}\widehat{f'}\not\equiv 0$ since $\widehat{\partial}_{(ij)(12)}\widehat{f'}\not\equiv 0$. Since $\widehat{f'}\in\int\widehat{\mathcal{O}}^{\otimes}$, We have $\widehat{\partial}_{ij}\widehat{f'} \in \mathcal{O}^{\otimes}$. Thus, $\widehat{\partial}_{ij}\widehat{f'}$ has (either odd or even) parity. For a contradiction, suppose that it has odd parity. Then, $\widehat{\partial}_{(12)(ij)}\widehat{f'}$ has even parity since it is realized by merging using $\neq_2$. A signature that has both even parity and odd parity is identically zero. Thus $\widehat{\partial}_{(12)(ij)}\widehat{f'}$ is the zero signature. However, since $\widehat{\partial}_{(ij)(12)}\widehat{f'} \in \mathcal{D}^{\otimes}$, it is not the zero signature. Contradiction. Therefore, $\widehat{\partial}_{ij}\widehat{f'}$ has even parity for all $\{i,j\}$ disjoint with $\{1,2\}$.

Then, consider $\widehat{\partial}_{ij}\widehat{f'}$ for $\{i,j\}\cap\{1,2\} \neq \emptyset$. If $\{1,2\} = \{i,j\}$, then clearly, $\widehat{\partial}_{12}\widehat{f'}$ has even parity. Otherwise, without loss of generality, we may assume that $i = 1$ and $j \neq 2$. Consider $\widehat{\partial}_{1j}\widehat{f'}$ for $3 \leqslant j \leqslant 6$. If it is a zero signature, then it has even parity. Otherwise, $\widehat{\partial}_{1j}\widehat{f'} \not\equiv 0$. Since $\widehat{\partial}_{1j}\widehat{f'} \in \widehat{\mathcal{O}}^{\otimes}$, we assume that it has the following UPF

$$\widehat{\partial}_{1j}\widehat{f'} = \widehat{b'_1}(x_2, x_u) \otimes \widehat{b'_2}(x_v, x_w).$$

By connecting variables x_u and x_v of $\widehat{\partial}_{1j}\widehat{f'}$ using $\neq_2$, we get $\widehat{\partial}_{(uv)(1j)}\widehat{f'}$. Since the merging gadget connects two nonzero binary signatures in $\widehat{\mathcal{O}}$, the resulting signature is a nonzero binary signature. Thus, $\widehat{\partial}_{(uv)(1j)}\widehat{f'} \not\equiv 0$. Notice that $\{u,v\}$ is disjoint with $\{1,2\}$. As showed above, $\widehat{\partial}_{uv}\widehat{f'}$ has even parity. Then, $\widehat{\partial}_{(1j)(uv)}\widehat{f'}$ has odd parity. For a contradiction, suppose that $\widehat{\partial}_{1j}\widehat{f'}$ has odd parity. Then $\widehat{\partial}_{(uv)(1j)}\widehat{f'}$ has even parity. But a nonzero signature $\widehat{\partial}_{(uv)(1j)}\widehat{f'}$ cannot have both even parity and odd parity. Contradiction. Thus, $\widehat{\partial}_{1j}\widehat{f'}$ has even parity.

We have proved that $\widehat{\partial}_{ij}\widehat{f'}$ has even parity for all pairs of indices $\{i,j\}$. In other words, for all pairs of indices $\{i,j\}$ and all $\beta \in \mathbb{Z}_2^4$ with $\mathrm{wt}(\beta) = 1$ or 3, we have $(\widehat{\partial}_{ij}\widehat{f'})(\beta) = 0$. Then, by Lemma 3.9, $\widehat{f'}(\alpha) = 0$ for all α with $\mathrm{wt}(\alpha) = 2$ or 4. Clearly, $\widehat{f'}$ is realized by extending $\widehat{f}$ with nonzero binary signatures in $\widehat{\mathcal{O}}$ that are realized by factorization from $\widehat{\partial}_{12}\widehat{f}$. □

Lemma 7.2. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T). *Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ contains an irreducible 6-ary signature $\widehat{f'}$ where $\widehat{f'}(\alpha) = 0$ for all α with $\mathrm{wt}(\alpha) = 2$ or 4, then* $\operatorname{Holant}(\neq_2|\ \widehat{\mathcal{F}})$ *is #P-hard, or $\mathscr{S}(\widehat{f'}) = \mathscr{O}_6 = \{\alpha \in \mathbb{Z}_2^6 \mid \mathrm{wt}(\alpha)$ is odd$\}$ and all nonzero entries of $\widehat{f'}$ have the same norm.*

证明. Since $\widehat{f'}$ is irreducible, again we may assume that $\widehat{f'}$ satisfies 2ND-ORTH and $\widehat{f'} \in \widehat{\int\mathcal{O}}^{\otimes}$. Let $\{i,j,k,\ell\}$ be an arbitrarily chosen subset of indices from $\{1,\ldots,6\}$, and $\{m,n\}$ be the other two indices. Then by equation (6.7), and the condition that $\widehat{f'}$ vanishes at weight 2 and 4, we have

$$|\widehat{\mathbf{f}'}^{0001}_{ijk\ell}|^2 = |\widehat{f'}^{000100}_{ijk\ell mn}|^2 + |\widehat{f'}^{000111}_{ijk\ell mn}|^2 = |\widehat{f'}^{001000}_{ijk\ell mn}|^2 + |\widehat{f'}^{001011}_{ijk\ell mn}|^2 = |\widehat{\mathbf{f}'}^{0010}_{ijk\ell}|^2. \tag{7.2}$$

Also, by considering indices $\{k, \ell, m, n\}$, we have

$$|\widehat{\mathbf{f}'}^{0100}_{k\ell mn}|^2 = |\widehat{f'}^{000100}_{ijk\ell mn}|^2 + |\widehat{f'}^{110100}_{ijk\ell mn}|^2 = |\widehat{f'}^{001000}_{ijk\ell mn}|^2 + |\widehat{f'}^{111000}_{ijk\ell mn}|^2 = |\widehat{\mathbf{f}'}^{1000}_{k\ell mn}|^2. \tag{7.3}$$

By ARS, we have

$$|\widehat{f'}^{000111}_{ijk\ell mn}|^2 = |\widehat{f'}^{111000}_{ijk\ell mn}|^2, \tag{7.4}$$

and

$$|\widehat{f'}^{001011}_{ijk\ell mn}|^2 = |\widehat{f'}^{110100}_{ijk\ell mn}|^2. \tag{7.5}$$

By calculating (7.2) + (7.3) − (7.4) − (7.5), we have

$$|\widehat{f'}^{000100}_{ijk\ell mn}|^2 = |\widehat{f'}^{001000}_{ijk\ell mn}|^2. \tag{7.6}$$

By (7.2) − (7.6), we have

$$|\widehat{f'}^{000111}_{ijk\ell mn}|^2 = |\widehat{f'}^{001011}_{ijk\ell mn}|^2. \tag{7.7}$$

From (7.6), since the indices (i, j, k, ℓ, m, n) can be an arbitrary permutation of $(1, 2, 3, 4, 5, 6)$, for all α, $\beta \in \mathbb{Z}_2^6$ with $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta) = 1$, we have $|\widehat{f'}(\alpha)| = |\widehat{f'}(\beta)|$. The same statement holds for $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta) = 3$, by (7.7).

Let $a = |\widehat{f'}(\vec{0}^6)|$; by ARS, $a = |\widehat{f'}(\vec{1}^6)|$ as well. It is the norm of entries of $\widehat{f'}$ on input of Hamming weight 0 and 6. We use b to denote the norm of entries of $\widehat{f'}$ on inputs of Hamming weight 1. By ARS, b is also the norm of entries of $\widehat{f'}$ on inputs of Hamming weight 5. We use c to denote the norm of entries of $\widehat{f'}$ on inputs of Hamming weight 3. Remember that by assumption, $|\widehat{f'}(\alpha)| = 0$ if $\mathrm{wt}(\alpha) = 2$ or 4.

By equation (6.6), we have

$$|\widehat{\mathbf{f}'}^{0000}_{1234}|^2 = a^2 + 2b^2 = |\widehat{\mathbf{f}'}^{0011}_{1234}|^2 = 2c^2.$$

Clearly, we have $0 \leqslant a, b \leqslant c$. If $c = 0$, then $a = b = 0$ which implies that $\widehat{f'}$ is a zero signature. This is a contradiction since $\widehat{f'}$ is irreducible. Therefore $c \neq 0$. We normalize c to 1. Then

$$a^2 + 2b^2 = 2.$$

We will show that $b = 1$ and $a = 0$. This will finish the proof of the lemma. For a contradiction, suppose that $b < 1$, then we also have $a > 0$.

Consider signatures $\widehat{f'}^{01}_{12}$, $\widehat{f'}^{10}_{12}$ and $\widehat{\partial}_{12}\widehat{f'} = \widehat{f'}^{01}_{12} + \widehat{f'}^{10}_{12}$. Since $\widehat{f'}(\alpha) = 0$ for all α with $\text{wt}(\alpha) = 2$ or 4, $\widehat{f'}^{01}_{12}(\beta) = 0$ and $\widehat{f'}^{10}_{12}(\beta) = 0$ for all β with $\text{wt}(\beta) = 1$ or 3. Thus, $\widehat{f'}^{01}_{12}$ and $\widehat{f'}^{10}_{12}$ have even parity. We also consider the complex inner product $\langle \widehat{\mathbf{f'}}^{01}_{12}, \widehat{\mathbf{f'}}^{10}_{12} \rangle$. First we build the following table.

$\widehat{f'}^{01}_{12}$	$\widehat{f'}^{010000}$	$\widehat{f'}^{010011}$	$\widehat{f'}^{010101}$	$\widehat{f'}^{010110}$	$\widehat{f'}^{011001}$	$\widehat{f'}^{011010}$	$\widehat{f'}^{011100}$	$\widehat{f'}^{011111}$
$\widehat{f'}^{10}_{12}$	$\widehat{f'}^{100000}$	$\widehat{f'}^{100011}$	$\widehat{f'}^{100101}$	$\widehat{f'}^{100110}$	$\widehat{f'}^{101001}$	$\widehat{f'}^{101010}$	$\widehat{f'}^{101100}$	$\widehat{f'}^{101111}$
$\widehat{\partial}_{12}\widehat{f'}$	s_1	s_2	s_3	s_4	$\overline{s_4}$	$\overline{s_3}$	$\overline{s_2}$	$\overline{s_1}$
$\langle \widehat{\mathbf{f'}}^{01}_{12}, \widehat{\mathbf{f'}}^{10}_{12} \rangle$	p_1	p_2	p_3	p_4	p_4	p_3	p_2	p_1

表 2: Entries of $\widehat{f'}^{01}_{12}$, $\widehat{f'}^{10}_{12}$, $\widehat{\partial}_{12}\widehat{f'}$ and pairwise product terms in $\langle \widehat{\mathbf{f'}}^{01}_{12}, \widehat{\mathbf{f'}}^{10}_{12} \rangle$ on even-weighed inputs

In Table 2, we call these four rows by Row 1, 2, 3 and 4 respectively and these nine columns by Column 0, 1, ...and 8 respectively. We use $T_{i,j}$ to denote the cell in Row i and Column j. Table 2 is built as follows.

- In Row 1 and Row 2, we list the entries of signatures $\widehat{f'}^{01}_{12}$ and $\widehat{f'}^{10}_{12}$ that are on even-weighted inputs (excluding the first two bits that are pinned) respectively. Note that, those that did not appear are 0 entries on odd-weighted inputs (excluding the first two bits that are pinned) of the signatures $\widehat{f'}^{01}_{12}$ and $\widehat{f'}^{10}_{12}$, since $\widehat{f'}^{01}_{12}$ and $\widehat{f'}^{10}_{12}$ have even parity.

- In Row 3, we list the corresponding entries of the signature $\widehat{\partial}_{12}\widehat{f'} = \widehat{f'}^{01}_{12} + \widehat{f'}^{10}_{12}$, i.e., $T_{3,j} = T_{1,j} + T_{2,j}$ for $1 \leqslant j \leqslant 8$.

- In Row 4, we list the corresponding items in the complex inner product $\langle \widehat{\mathbf{f'}}^{01}_{12}, \widehat{\mathbf{f'}}^{10}_{12} \rangle$, i.e., $T_{4,j} = T_{1,j} \cdot \overline{T_{2,j}}$ for $1 \leqslant j \leqslant 8$.

For $1 \leqslant j \leqslant 8$, we consider the entry in $T_{1,j}$ and the entry in $T_{2,9-j}$. By ARS, we have $T_{1,j} = \overline{T_{2,9-j}}$ because their corresponding inputs are complement of each other. Thus,

$$T_{3,j} = T_{1,j} + T_{2,j} = \overline{T_{2,9-j}} + \overline{T_{1,9-j}} = \overline{T_{3,9-j}},$$

and

$$T_{4,j} = T_{1,j} \cdot \overline{T_{2,j}} = \overline{T_{2,9-j}} \cdot T_{2,9-j} = T_{4,9-j}.$$

We use $s_1, \ldots, s_4$ to denote the values in $T_{3,1}, \ldots, T_{3,4}$ and $p_1, \ldots, p_4$ to denote the values in $T_{4,1}, \ldots, T_{4,4}$. Correspondingly, the values in $T_{3,5}, \ldots, T_{3,8}$ are $\overline{s_4}, \ldots, \overline{s_1}$ and the values in $T_{4,5}, \ldots, T_{4,8}$ are $p_4, \ldots, p_1$. We also use x_j and y_j $(1 \leqslant j \leqslant 8)$ to denote the entries in $T_{1,j}$ and $T_{2,j}$ respectively.

By 2ND-ORTH, we have $\langle \widehat{\mathbf{f}'}^{01}_{12}, \widehat{\mathbf{f}'}^{10}_{12} \rangle = 2(p_1 + p_2 + p_3 + p_4) = 0$. Also we have $|p_1| = b^2$ and $|p_2| = |p_3| = |p_4| = 1$. Notice the fact that if $x_i + y_i = 0$, then $x_i \cdot \overline{y_i} = x_i \cdot \overline{-x_i} = -|x_i|^2 = -|x_i \cdot \overline{y_i}|$. Thus, if $s_1 = 0$ then $p_1 = -|p_1| = -b^2$ and for any $i = 2, 3, 4$, if $s_i = 0$ then $p_i = -1$. Note that $\widehat{\partial}_{12}\widehat{f'}(\beta) = \widehat{f'}^{01}_{12}(\beta) + \widehat{f'}^{10}_{12}(\beta) = 0$ for all β with $\text{wt}(\beta) = 1$ or 3. Among all 16 entries of $\widehat{\partial}_{12}\widehat{f'}$, $s_1, \ldots, s_4, \overline{s_4}, \ldots, \overline{s_1}$ are those that are possibly nonzero. Since $\widehat{\partial}_{12}\widehat{f'} \in \widehat{\mathcal{O}}^{\otimes}$, it has support of size either 4 or 0. Thus, among s_1, s_2, s_3 and s_4, either exactly two of them are zero or they are all zero. There are three possible cases.

- $s_1 = s_2 = s_3 = s_4 = 0$. Then $p_1 + p_2 + p_3 + p_4 = -b^2 - 3 \leqslant -3 \neq 0$. Contradiction.

- $s_1 \neq 0$ and two of s_2, s_3 and s_4 are zero. Without loss of generality, we may assume that $s_2 = s_3 = 0$. Then $p_2 = p_3 = -1$. Since $p_1 + p_2 + p_3 + p_4 = 0$, we have $p_1 + p_4 = -p_2 - p_3 = 2$. Then, $2 = |p_1 + p_4| \leqslant |p_1| + |p_4| = b^2 + 1 < 2$. Contradiction.

- $s_1 = 0$ and one of s_2, s_3 and s_4 is zero. Without loss of generality, we may assume that $s_2 = 0$. Then $p_1 = -b^2$ and $p_2 = -1$. Thus, $p_3 + p_4 = -p_1 - p_2 = 1 + b^2 < 2$. Let $\theta = \arccos \frac{1+b^2}{2}$. We know that $0 < \theta < \frac{\pi}{2}$. Recall that $|p_3| = |p_4| = 1$. Thus, $p_3 = e^{\pm \mathrm{i}\theta}$ and $p_4 = e^{\mp \mathrm{i}\theta}$ (and $p_3 = \overline{p_4}$).

Let $P = \{-1, e^{\mathrm{i}\theta}, e^{-\mathrm{i}\theta}\}$. Thus, $p_2, p_3, p_4 \in P$. Otherwise, we get a contradiction.

Now, we consider signatures $\widehat{\partial}_{ij}\widehat{f'}$ for all pairs of indices $\{i, j\}$. By symmetry, the same conclusion holds. In other words, let $\{i, j\}$ be an arbitrarily chosen pair of indices from $\{1, \ldots, 6\}$ and

$\{k, \ell, m, n\}$ be the other four indices, and let $\beta \in \mathbb{Z}_2^4$ be an assignment on variables (x_k, x_ℓ, x_m, x_n) with $\mathrm{wt}(\beta) = 2$. Then, we have $\widehat{f'}^{01\beta}_{ijk\ell mn} \cdot \overline{\widehat{f'}^{10\beta}_{ijk\ell mn}} \in P$. Since the indices (i, j, k, ℓ, m, n) can be an arbitrary permutation of $(1, 2, 3, 4, 5, 6)$, we have $\widehat{f'}(\alpha) \cdot \overline{\widehat{f'}(\alpha')} \in P$ for any two assignments α and α' on the six variables where $\mathrm{wt}(\alpha) = \mathrm{wt}(\alpha') = 3$ and $\mathrm{wt}(\alpha \oplus \alpha') = 2$, because for any such two strings α and α', there exist two bit positions on which α and α' take values 01 and 10 respectively.

We consider the following three inputs $\alpha_1 = 100011$, $\alpha_2 = 010011$ and $\alpha_3 = 001011$ of $\widehat{f'}$. We have $\widehat{f'}(\alpha_1) \cdot \overline{\widehat{f'}(\alpha_2)} = q_{12} \in P$, $\widehat{f'}(\alpha_2) \cdot \overline{\widehat{f'}(\alpha_3)} = q_{23} \in P$ and $\widehat{f'}(\alpha_1) \cdot \overline{\widehat{f'}(\alpha_3)} = q_{13} \in P$. Recall that $|\widehat{f'}(\alpha_2)| = 1$ since $\mathrm{wt}(\alpha_2) = 3$. Then,

$$q_{12} \cdot q_{23} = \widehat{f'}(\alpha_1) \cdot \overline{\widehat{f'}(\alpha_2)} \cdot \widehat{f'}(\alpha_2) \cdot \overline{\widehat{f'}(\alpha_3)} = |\widehat{f'}(\alpha_2)|^2 \cdot \widehat{f'}(\alpha_1) \cdot \overline{\widehat{f'}(\alpha_3)} = q_{13} \in P.$$

However, since $0 < \theta < \frac{\pi}{2}$, it is easy to check that for any two (not necessarily distinct) elements in P, their product is not in P. Thus, we get a contradiction. This proves that $b = c = 1$ and $a = 0$.

Therefore we have proved that, $\mathscr{S}(\widehat{f'}) = \mathscr{O}_6$, and all its nonzero entries have the same norm that is normalized to 1. □

Lemma 7.3. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T). *Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ contains an irreducible 6-ary signature $\widehat{f'}$ where $\mathscr{S}(\widehat{f'}) = \mathscr{O}_6$ and $|\widehat{f'}(\alpha)| = 1$ for all $\alpha \in \mathscr{S}(\widehat{f'})$, then* Holant$(\neq_2|\ \widehat{\mathcal{F}})$ *is #P-hard, or after a holographic transformation by some $\widehat{Q} = \left[\begin{smallmatrix} \bar{\rho} & 0 \\ 0 & \rho \end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$ where $\rho = e^{i\delta}$ and $0 \leqslant \delta < \pi/2$, an irreducible 6-ary signature $\widehat{f''}$ and $=_2$ are realizable from $\widehat{f'}$ where $\mathscr{S}(\widehat{f''}) = \mathscr{O}_6$ and there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathscr{S}(\widehat{f''})$, $\widehat{f''}(\alpha) = \pm\lambda$, i.e.,* Holant$(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T$ Holant$(\neq_2|\ \widehat{\mathcal{F}})$ *where $\widehat{f''} = \widehat{Q}\widehat{f'}$. Moreover, the nonzero binary signature $(\rho^2, 0, 0, \overline{\rho^2}) \in \widehat{\mathcal{O}}$ is realizable from $\widehat{\partial}_{ij}\widehat{f'}$ for some $\{i, j\}$.*

证明. Again, we may assume that $\widehat{f'}$ satisfies 2nd-Orth and $\widehat{f'} \in \int\widehat{\mathcal{O}}^{\otimes}$. We first show that there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathscr{S}(\widehat{f'})$ with $\mathrm{wt}(\alpha) = 3$, $\widehat{f''}(\alpha) = \pm\lambda$, or else we get #P-hardness.

Let's revisit Table 2. Now we have $|p_1| = |p_2| = |p_3| = |p_4| = 1$. Recall that for $1 \leqslant i \leqslant 4$, $s_i = 0$ implies that $p_i = -1$. Since $\widehat{\partial}_{12}\widehat{f'} \in \widehat{\mathcal{O}}^{\otimes 2}$, it has support of size 4 or 0. Thus, among s_1, s_2, s_3 and s_4, either exactly two of them are zero or they are all zero. If they are all zero, then we have $p_1 + p_2 + p_3 + p_4 = -4 \neq 0$. This is a contradiction to our assumption that $\widehat{f'}$ satisfies 2nd-Orth.

Thus, exactly two of s_1, s_2, s_3 and s_4 are zeros. Suppose that they are s_i and s_j. Recall that we use x_i and y_i ($1 \leqslant i \leqslant 8$) to denote the entries in Row 1 and Row 2 of Table 2. Thus $|x_i| = |y_i| = 1$, for $1 \leqslant i \leqslant 8$. Since $s_i = x_i + y_i = 0$ and $s_j = x_j + y_j = 0$, we have $x_i = -y_i$, and $x_j = -y_j$. Also, since $s_i = s_j = 0$, we have $p_i = p_j = -1$. Let $\{\ell, k\} = \{1, 2, 3, 4\} \backslash \{i, j\}$. Then, by 2nd-Orth, we have $p_\ell + p_k = -p_i - p_j = 2$. Since $|p_\ell| = |p_k| = 1$, we have $p_\ell = p_k = 1$. Note that $p_\ell = x_\ell \cdot \overline{y_\ell} = 1$ and also $1 = |y_\ell| = y_\ell \cdot \overline{y_\ell}$. Thus, we have $x_\ell = y_\ell$. Similarly, $x_k = y_k$. Thus, for all $1 \leqslant i \leqslant 8$, $x_i = \pm y_i$. Consider $\widehat{\partial}_{ij}\widehat{f'}$ for all pairs of indices $\{i, j\}$. By symmetry, the same conclusion holds. Thus, $\widehat{f}(\alpha) = \pm\widehat{f}(\alpha')$ for any two inputs α and α' on the six variables where $\mathrm{wt}(\alpha) = \mathrm{wt}(\alpha') = 3$ and $\mathrm{wt}(\alpha \oplus \alpha') = 2$. In particular, we have

$$\widehat{f'}^{000111} = \varepsilon_1 \widehat{f'}^{001011} = \varepsilon_2 \widehat{f'}^{011001} = \varepsilon_3 \widehat{f'}^{111000},$$

where $\varepsilon_1, \varepsilon_2, \varepsilon_3 = \pm 1$ independently. By ARS, we have $\widehat{f'}^{000111} = \overline{\widehat{f'}^{111000}}$.

- If $\widehat{f'}^{000111} = \widehat{f'}^{111000} = \overline{\widehat{f'}^{111000}}$, then $\widehat{f'}^{111000} = \pm 1$.
- If $\widehat{f'}^{000111} = -\widehat{f'}^{111000} = \overline{\widehat{f'}^{111000}}$, then $\widehat{f'}^{111000} = \pm\mathfrak{i}$.

Thus, there exists $\lambda = 1$ or $\mathfrak{i}$ such that $\widehat{f'}^{000111} = \pm\lambda$ and $\widehat{f'}^{111000} = \pm\lambda$. Consider any $\alpha \in \mathbb{Z}_2^6$ with $\mathrm{wt}(\alpha) = 3$. If $\alpha \in \{000111, 111000\}$, then clearly, $\widehat{f'}(\alpha) = \pm\lambda$. Otherwise, either $\mathrm{wt}(\alpha \oplus 000111) = 2$ or $\mathrm{wt}(\alpha \oplus 111000) = 2$. Then, $\widehat{f'}(\alpha) = \pm\lambda$. Thus, there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathbb{Z}_2^6$ with $\mathrm{wt}(\alpha) = 3$, $\widehat{f'}(\alpha) = \pm\lambda$.

Since $\widehat{f'}(\alpha) \neq 0$ for all α with $\mathrm{wt}(\alpha) = 1$, by Lemma 3.9, there exists a pair of indices $\{i, j\}$ such that $(\widehat{\partial}_{ij}\widehat{f'})^{0000} \neq 0$. Since $\widehat{\partial}_{ij}\widehat{f'} \in \mathcal{O}^{\otimes}$, it is of the form $(a, 0, 0, \bar{a}) \otimes (b, 0, 0, \bar{b})$, where $ab \neq 0$, since no other factorization form in $\mathcal{O}^{\otimes}$ has a nonzero value at 0000. By Lemma 3.6, we can realize the signature $\widehat{g} = (a, 0, 0, \bar{a})$. Here, we can normalize a to $e^{\mathfrak{i}\theta}$ where $0 \leqslant \theta < \pi$. Then, let $\rho = e^{\mathfrak{i}\theta/2}$. Clearly, $0 \leqslant \theta/2 < \pi/2$. Consider a holographic transformation by $\widehat{Q} = \left[\begin{smallmatrix} \bar{\rho} & 0 \\ 0 & \rho \end{smallmatrix}\right]$. Note that $(\neq_2)(\widehat{Q}^{-1})^{\otimes 2} = (\neq_2)$ and $\widehat{Q}^{\otimes 2}\widehat{g} = (1, 0, 0, 1)$. The holographic transformation by $\widehat{Q}$ does not change $\neq_2$, but transfers $\widehat{g} = (a, 0, 0, \bar{a})$ to $(=_2) = (1, 0, 0, 1)$. Thus, we have

$$\operatorname{Holant}(\neq_2 |\, \widehat{g}, \widehat{f'}, \widehat{\mathcal{F}}) \equiv_T \operatorname{Holant}(\neq_2 | =_2, \widehat{Q}\widehat{f'}, \widehat{Q}\widehat{\mathcal{F}}).$$

We denote $\widehat{Q}\widehat{f'}$ by $\widehat{f''}$. Note that $\widehat{Q}$ does not change those entries of $\widehat{f'}$ that are on half-weighted inputs. Thus, for all α with $\mathrm{wt}(\alpha) = 3$, we have $\widehat{f''}(\alpha) = \pm\lambda$ for some $\lambda = 1$ or $\mathfrak{i}$. Also, $\widehat{Q}$ does not change the parity and irreducibility of $\widehat{f'}$. Thus $\widehat{f''}$ has odd parity and $\widehat{f''}$ is irreducible. Again, we may assume that $\widehat{f''}$ satisfies 2ND-ORTH and $\widehat{f''} \in \int\widehat{\mathcal{O}}^{\otimes}$. Otherwise, we are done.

In the problem $\mathrm{Holant}(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}})$, we can connect two $\neq_2$ on the LHS using $=_2$ on the RHS, and then we can realize $=_2$ on the LHS. Thus, we can use $=_2$ to merge variables of $\widehat{f''}$. Therefore, we may further assume $\widehat{f''} \in \int\widehat{\mathcal{O}}^{\otimes}$, i.e., $\partial_{ij}\widehat{f''} \in \widehat{\mathcal{O}}^{\otimes}$ for all pairs of indices $\{i, j\}$; otherwise, there exist two variables of $\widehat{f''}$ such that by merging these two variables using $=_2$, we can realize a 4-ary signature that is not in $\widehat{\mathcal{O}}^{\otimes}$, and then by Lemma 6.8 we are done.

Consider the signature $\partial_{12}\widehat{f''} = \widehat{f''}^{00}_{12} + \widehat{f''}^{11}_{12}$ and the inner product $\langle \widehat{\mathbf{f}''}^{00}_{12}, \widehat{\mathbf{f}''}^{11}_{12}\rangle$. Same as Table 2, we build the following Table 3.

$\widehat{f''}^{00}_{12}$	$\widehat{f''}^{000001}$	$\widehat{f''}^{000010}$	$\widehat{f''}^{000100}$	$\widehat{f''}^{000111}$	$\widehat{f''}^{001000}$	$\widehat{f''}^{001011}$	$\widehat{f''}^{001101}$	$\widehat{f''}^{001110}$
$\widehat{f''}^{11}_{12}$	$\widehat{f''}^{110001}$	$\widehat{f''}^{110010}$	$\widehat{f''}^{110100}$	$\widehat{f''}^{110111}$	$\widehat{f''}^{111000}$	$\widehat{f''}^{111011}$	$\widehat{f''}^{111101}$	$\widehat{f''}^{111110}$
$\partial_{12}\widehat{f''}$	t_1	t_2	t_3	t_4	$\overline{t_4}$	$\overline{t_3}$	$\overline{t_2}$	$\overline{t_1}$
$\langle \widehat{\mathbf{f}''}^{00}_{12}, \widehat{\mathbf{f}''}^{11}_{12}\rangle$	q_1	q_2	q_3	q_4	q_4	q_3	q_2	q_1

表 3: Entries of $\widehat{f''}^{00}_{12}$, $\widehat{f''}^{11}_{12}$, $\partial_{12}\widehat{f''}$ and pair-wise product terms in $\langle \widehat{\mathbf{f}''}^{00}_{12}, \widehat{\mathbf{f}''}^{11}_{12}\rangle$ on odd-weighed inputs

Same as the proof of $x_i = \pm y_i$ for Table 2, we have $\widehat{f''}^{000001} = \pm\widehat{f''}^{110001}$. Since $\widehat{f''}^{110001} = \pm\lambda$, $\widehat{f''}^{000001} = \pm\lambda$, (here $\pm$ can be either $\pm$ or $\mp$). Consider $\partial_{ij}\widehat{f''}$ for all pairs of indices $\{i, j\}$. By symmetry, the same conclusion holds. Thus, for every $\alpha \in \mathbb{Z}_2^6$ with $\mathrm{wt}(\alpha) = 1$, $\widehat{f''}(\alpha) = \pm\lambda$. Therefore, using ARS, there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathscr{S}(\widehat{f''})$, $\widehat{f''}(\alpha) = \pm\lambda$, and we have the reduction

$$\mathrm{Holant}(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \mathrm{Holant}(\neq_2|\,\widehat{\mathcal{F}})$$

for some $\widehat{Q} \in \widehat{\mathbf{O}_2}$. Clearly, $\widehat{f''} = \widehat{Q}\widehat{f'}$ where $\widehat{Q} = \left[\begin{smallmatrix}\bar{\rho} & 0\\ 0 & \rho\end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$, and the nonzero binary signature $(\rho^2, 0, 0, \overline{\rho^2}) \in \widehat{\mathcal{O}}$ is realizable from $\widehat{\partial}_{ij}\widehat{f'}$ for some $\{i, j\}$. □

Finally, we go for the kill in the next lemma. Recall the signature $\widehat{f_6}$ defined in (7.1). This *Lord of Intransigence* at arity 6 makes its appearance in Lemma 7.4.

Lemma 7.4. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ contains an irreducible* 6*-ary signature $\widehat{f''}$ where $\mathscr{S}(\widehat{f''}) = \mathscr{O}_6$, and there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathscr{S}(\widehat{f''})$, $\widehat{f''}(\alpha) = \pm\lambda$, then* $\operatorname{Holant}(\neq_2|=_2, \widehat{\mathcal{F}})$ *is #P-hard, or $\widehat{f_6}$ is realizable from $\widehat{f''}$ and $=_2$, i.e.,* $\operatorname{Holant}(\neq_2|\,\widehat{f_6}, \widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|=_2, \widehat{\mathcal{F}})$*. Moreover, $\widehat{f_6}$ is realizable by extending variables of $\widehat{f''}$ with binary signatures in $\widehat{\mathcal{B}}$, i.e., $\widehat{f_6} \in \{\widehat{f''}\}^{\widehat{\mathcal{B}}}_{\neq_2}$.*

证明. Again, we may assume that $\widehat{f''}$ satisfies 2nd-Orth and $\widehat{f''} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$. Since $=_2$ is available on the RHS, given any signature $\widehat{f} \in \widehat{\mathcal{F}}$, we can extend any variable x_i of $\widehat{f}$ with $=_2 \in \widehat{\mathcal{B}}$ using $\neq_2$. This gives a signature $\widehat{g}$ where $\widehat{g}_i^0 = \widehat{f}_i^1$ and $\widehat{g}_i^1 = \widehat{f}_i^0$. We call this extending gadget construction the flipping operation on variable x_i. Clearly, it does not change the reducibility or irreducibility of $\widehat{f}$. But it changes the parity of $\widehat{f}$ if $\widehat{f}$ has parity. Once a signature $\widehat{f}$ is realizable, we can modify it by flipping some of its variables.

We first show that we can realize a signature $\widehat{f^*}$ from $\widehat{f''}$ having support $\mathscr{S}(\widehat{f^*}) = \mathscr{E}_6 = \{\alpha \in \mathbb{Z}_2^6 \mid \operatorname{wt}(\alpha) \equiv 0 \mod 2\}$, and $\widehat{f^*}(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(\widehat{f^*})$. Remember that $=_2$ is available. If we connect $=_2$ with an arbitrary variable of $\widehat{f''}$ using $\neq_2$, we will change the parity of $\widehat{f''}$ from odd to even. If $\widehat{f''}(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(\widehat{f''})$, then $\widehat{f^*}$ can be realized by flipping an arbitrary variable of $\widehat{f''}$. Otherwise, $\widehat{f''}(\alpha) = \pm\mathfrak{i}$ for all $\alpha \in \mathscr{S}(\widehat{f''})$. Consider $\widehat{\partial}_{12}\widehat{f''}$. Look at Table 3. We use x_i and y_i $(1 \leqslant i \leqslant 8)$ to denote entries in Row 1 and 2. As we have showed, $x_i = \pm y_i$. Thus, $t_i = \pm 2\mathfrak{i}$ or 0 for $1 \leqslant i \leqslant 4$. Remember that if $t_i = 0$ (i.e., $x_i = -y_i$), then $q_i = x_i \cdot \overline{y_i} = -x_i \cdot \overline{x_i} = -|x_i|^2 = -1$. If $t_i = 0$ for all $1 \leqslant i \leqslant 4$, then

$$\langle \widehat{\mathbf{f''}}_{12}^{00}, \widehat{\mathbf{f''}}_{12}^{11} \rangle = 2(q_1 + q_2 + q_3 + q_4) = -4 \neq 0.$$

This contradicts with our assumption that $\widehat{f''}$ satisfies 2nd-Orth. Thus, t_i $(1 \leqslant i \leqslant 4)$ are not all zeros. Then $(\widehat{\partial}_{12}\widehat{f''}) \not\equiv 0$. Thus, $\mathscr{S}(\widehat{\partial}_{12}\widehat{f''}) \neq \emptyset$ and $(\widehat{\partial}_{12}\widehat{f''})(\alpha) = \pm 2i$ for all $\alpha \in \mathscr{S}(\widehat{\partial}_{12}\widehat{f''})$.

Since $\widehat{\partial}_{12}\widehat{f''} \in \widehat{\mathcal{O}}^{\otimes}$ and it has even parity, $\widehat{\partial}_{12}\widehat{f''}$ is of the form $2 \cdot (a, 0, 0, \bar{a}) \otimes (b, 0, 0, \bar{b})$ or $2 \cdot (0, a, \bar{a}, 0) \otimes (0, b, \bar{b}, 0)$, where the norms of a and b are normalized to 1. In both cases, we have $ab, \bar{a}b, a\bar{b}, \bar{a}\bar{b} \in \{\mathfrak{i}, -\mathfrak{i}\}$. Thus, $ab \cdot \bar{a}b = (a\bar{a})b^2 = b^2 = \pm 1$. Then, $b = \pm 1$ or $\pm\mathfrak{i}$. If $b = \pm 1$, then $a = a\bar{b} \cdot b = \pm\mathfrak{i}$. Similarly, if $b = \pm\mathfrak{i}$, then $a = a\bar{b} \cdot b = \pm 1$. Thus, among a and b, exactly one is $\pm\mathfrak{i}$. Thus, by factorization we can realize the binary signature $\widehat{g} = (\mathfrak{i}, 0, 0, -\mathfrak{i})$ or $(0, \mathfrak{i}, -\mathfrak{i}, 0)$ up to a scalar -1. Connecting an arbitrary variable of $\widehat{f}$ with a variable of $\widehat{g}$, we can get a signature which has parity and all its nonzero entries have value ±1. If the resulting signature has even parity, then we get the desired $\widehat{f^*}$. If it has odd parity, then we can flip one of its variables to change the parity. Thus, we can realize a signature $\widehat{f^*}$ by extending variables of $\widehat{f''}$ with binary signatures in $\widehat{\mathcal{B}}^{\otimes}$ such that $\mathscr{S}(\widehat{f^*}) = \mathscr{E}_6$, and $\widehat{f^*}(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(\widehat{f^*})$.

Consider the following 16 entries of $\widehat{f^*}$. In Table 4, we list 16 entries of $\widehat{f^*}$ with $x_1x_2x_3 = 000, 011, 101, 110$ as the row index and $x_4x_5x_6 = 000, 011, 101, 110$ as the column index. We also view these 16 entries in Table 4 as a 4-by-4 matrix denoted by $M_r(\widehat{f^*})$, and we call it the representative matrix of $\widehat{f^*}$. Note that for any $\alpha \in \mathscr{S}(\widehat{f^*})$ such that the entry $\widehat{f^*}(\alpha)$ does not appear in $M_r(\widehat{f^*})$, $\widehat{f^*}(\overline{\alpha})$ appears in $M_r(\widehat{f^*})$. Since $\widehat{f^*}(\alpha) = \pm 1 \in \mathbb{R}$, $\overline{\widehat{f^*}(\alpha)} = \widehat{f^*}(\alpha)$. By ARS, $\widehat{f^*}(\overline{\alpha}) = \overline{\widehat{f^*}(\alpha)} = \widehat{f^*}(\alpha)$. Thus, the 16 entries of the matrix $M_r(\widehat{f^*})$ listed in Table 4 gives a complete account for all the 32 nonzero entries of $\widehat{f^*}$.

$x_4x_5x_6$ $x_1x_2x_3$	000 (Col 1)	011 (Col 2)	101 (Col 3)	110 (Col 4)
000 (Row 1)	$\widehat{f^*}^{000000}$	$\widehat{f^*}^{000011}$	$\widehat{f^*}^{000101}$	$\widehat{f^*}^{000110}$
011 (Row 2)	$\widehat{f^*}^{011000}$	$\widehat{f^*}^{011011}$	$\widehat{f^*}^{011101}$	$\widehat{f^*}^{011110}$
101 (Row 3)	$\widehat{f^*}^{101000}$	$\widehat{f^*}^{101011}$	$\widehat{f^*}^{101101}$	$\widehat{f^*}^{101110}$
110 (Row 4)	$\widehat{f^*}^{110000}$	$\widehat{f^*}^{110011}$	$\widehat{f^*}^{110101}$	$\widehat{f^*}^{110110}$

表 4: Representative entries of $\widehat{f^*}$

We use $(m_{ij})_{i,j=1}^{4}$ to denote the 16 entries of $M_r(\widehat{f^*})$. We claim that any two rows of $M_r(\widehat{f^*})$ are orthogonal; this follows from the fact that $\widehat{f^*}$ satisfies 2nd-Orth and ARS. For example, consider the first two rows of $M_r(\widehat{f^*})$. By 2nd-Orth, the inner product $\langle \widehat{\mathbf{f}^*}^{00}_{23}, \widehat{\mathbf{f}^*}^{11}_{23} \rangle$ for the real-valued $\widehat{f^*}$ is

$$\sum_{(x_1,x_4,x_5,x_6)\in\mathbb{Z}_2^4} \widehat{f^*}^{x_1 00 x_4x_5x_6}\widehat{f^*}^{x_1 11 x_4x_5x_6} = 0,$$

where the sum has 8 nonzero product terms. The first 4 terms given by $x_1 = 0$ are the pairwise products $m_{1j}m_{2j}$, for $1 \leqslant j \leqslant 4$. The second 4 terms are, by ARS, the pairwise products $m_{2j}m_{1j}$ in the reversal order of $1 \leqslant j \leqslant 4$, where we exchange row 1 with row 2 on the account of flipping the summation index x_1 from 0 to 1, and simultaneously flipping both x_2 and x_3. This shows that

$\sum_{j=1}^{4} m_{1j}m_{2j} = 0$. Similarly any two columns of $M_r(\widehat{f^*})$ are orthogonal.

Also, we consider the inner product $\langle \widehat{\mathbf{f}^*}^{00}_{14}, \widehat{\mathbf{f}^*}^{11}_{14} \rangle = 0$. It is computed using the following 16 entries in $M_r(\widehat{f^*})$, listed in Table 5.

$\widehat{f^*}^{000000}$ $= m_{11}$	$\widehat{f^*}^{000011}$ $= m_{12}$	$\widehat{f^*}^{010010}$ $= m_{33}$	$\widehat{f^*}^{010001}$ $= m_{34}$	$\widehat{f^*}^{001010}$ $= m_{43}$	$\widehat{f^*}^{001001}$ $= m_{44}$	$\widehat{f^*}^{011000}$ $= m_{21}$	$\widehat{f^*}^{011011}$ $= m_{22}$
$\widehat{f^*}^{100100}$ $= m_{22}$	$\widehat{f^*}^{100111}$ $= m_{21}$	$\widehat{f^*}^{110110}$ $= m_{44}$	$\widehat{f^*}^{110101}$ $= m_{43}$	$\widehat{f^*}^{101110}$ $= m_{34}$	$\widehat{f^*}^{101101}$ $= m_{33}$	$\widehat{f^*}^{111100}$ $= m_{12}$	$\widehat{f^*}^{111111}$ $= m_{11}$

表 5: Pair-wise product terms in $\langle \widehat{\mathbf{f}^*}^{00}_{14}, \widehat{\mathbf{f}^*}^{11}_{14} \rangle$ on even-weighed inputs

Let $M_r(\widehat{f^*})_{[1,2]}$ be the 2-by-2 submatrix of $M_r(\widehat{f^*})$ by picking the first two rows and the first two columns, and $M_r(\widehat{f^*})_{[3,4]}$ be the 2-by-2 submatrix of $M_r(\widehat{f^*})$ by picking the last two rows and the last two columns. Indeed,

$$\begin{aligned}\langle \widehat{\mathbf{f}^*}^{00}_{14}, \widehat{\mathbf{f}^*}^{11}_{14} \rangle &= 2(\operatorname{perm}(M_r(\widehat{f^*})_{[1,2]}) + \operatorname{perm}(M_r(\widehat{f^*})_{[3,4]})) \\ &= 2(m_{11}m_{22} + m_{12}m_{21} + m_{33}m_{44} + m_{34}m_{43}) = 0.\end{aligned}$$

Then, we show that by renaming or flipping variables of $\widehat{f^*}$, we may modify $\widehat{f^*}$ to realize a signature whose representative matrix is obtained by performing row permutation, column permutation, or matrix transpose on $M_r(\widehat{f^*})$. First, if we exchange the names of variables (x_1, x_2, x_3) with variables (x_4, x_5, x_6), then the representative matrix $M_r(\widehat{f^*})$ will be transposed. Next, consider the group $\mathfrak{G}$ of permutations on the rows $\{1, 2, 3, 4\}$ effected by any sequence of operations of renaming and flipping variables in $\{x_1, x_2, x_3\}$. By renaming variables in $\{x_1, x_2, x_3\}$, we can switch any two rows among Row 2, 3 and 4. Thus S_3 on $\{2, 3, 4\}$ is contained in $\mathfrak{G}$. Also, if we flip both variables x_2 and x_3 of $\widehat{f^*}$, then for the realized signature, its representative matrix can be obtained by switching both the pair Row 1 and Row 2, and the pair Row 3 and Row 4 of $M_r(\widehat{f^*})$. Thus, the permutation $(12)(34) \in \mathfrak{G}$. It follows that $\mathfrak{G} = S_4$. Thus, by renaming or flipping variables of $\widehat{f^*}$, we can permute any two rows or any two columns of $M_r(\widehat{f^*})$, or transpose $M_r(\widehat{f^*})$. For the resulting signature, we may assume that its representative matrix A also satisfy $\operatorname{perm}(A_{[1,2]}) + \operatorname{perm}(A_{[3,4]}) = 0$, and any two rows of A are orthogonal and any two columns of A are orthogonal. Otherwise, we get #P-hardness. In the following, without loss of generality, we may modify $M_r(\widehat{f^*})$ by permuting any two rows or any two columns, or taking transpose. We show that it will give $M_r(\widehat{f_6})$, after a normalization by ±1. In other words, $\widehat{f_6}$ is realizable from $\widehat{f^*}$ by renaming or flipping variables, up to a normalization by ±1.

Consider any two rows, Row i and Row j, of $M_r(\widehat{f^*})$. Recall that every entry of $M_r(\widehat{f^*})$ is ± 1. We say that Row i and Row j differ in Column k if $m_{ik} \neq m_{jk}$, which implies that $m_{ik} = -m_{jk}$; otherwise, they are equal $m_{ik} = m_{jk}$. In the former case, $m_{ik} \cdot m_{jk} = -1$, and in the latter case $m_{ik} \cdot m_{jk} = 1$. Since Row i and Row j are orthogonal, they differ in exactly two columns and are equal in the other two columns. Similarly, for any two columns of $M_r(\widehat{f^*})$, they differ in exactly two rows and are equal in the other two rows. Depending on the number of -1 entries in each row and column of $M_r(\widehat{f^*})$, we consider the following two cases.

- Every row and column of $M_r(\widehat{f^*})$ has an odd number of -1 entries.

  Consider Row 1. It has either exactly three -1 entries or exactly one -1 entry. If it has three -1 entries, then we modify $M_r(\widehat{f^*})$ by multiplying the matrix with -1. This does not change the parity of the number of -1 entries in each row and each column. By such a modification, Row 1 has exactly one -1 entry. By permuting columns, we may assume that Row 1 is $(-1, 1, 1, 1)$. Consider the number of -1 entries in Rows 2, 3 and 4.

  - If they all have exactly one -1 entry, by orthogonality, the unique column locations of the -1 entry in each row must be pairwise distinct. Then, by possibly permuting rows 2, 3 and 4 we may assume that the matrix $M_r(\widehat{f^*})$ has the following form

    $$M_r(\widehat{f^*}) = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

    Then, $\operatorname{perm}(M_r(\widehat{f^*})_{[1,2]}) + \operatorname{perm}(M_r(\widehat{f^*})_{[3,4]}) = 2 + 2 = 4 \neq 0$. Contradiction.

  - Otherwise, among Rows 2, 3 and 4, there is one that has three -1 entries. By permuting rows, we may assume that Row 2 has three -1 entries. Since Row 2 and Row 1 differ in two columns, the only $+1$ entry in Row 2 is not in Column 1. By possibly permuting Columns 2, 3 and 4, without loss of generality, we may assume that Row 2 is $(-1,1,-1,-1)$. Then, we consider Column 3 and Column 4. Since every column has an odd number of -1 entries and $m_{13} = 1$ and $m_{23} = -1$, we have $m_{33} = m_{43}$, both $+1$ or -1. Similarly, $m_{34} = m_{44}$. Also, since Column 3 and Column 4 differ in exactly two rows, and $m_{13} = m_{14}$ and $m_{23} = m_{24}$, we have $m_{33} = -m_{34}$ and $m_{43} = -m_{44}$. Thus, $M_r(\widehat{f^*})_{[3,4]} = \pm \left[\begin{smallmatrix} 1 & -1 \\ 1 & -1 \end{smallmatrix}\right]$. In both cases, we have $\operatorname{perm}(M_r(\widehat{f^*})_{[1,2]}) = -2$. Notice that $M_r(\widehat{f^*})_{[1,2]} = \left[\begin{smallmatrix} -1 & 1 \\ -1 & 1 \end{smallmatrix}\right]$. Thus, $\operatorname{perm}(M_r(\widehat{f^*})_{[1,2]}) + \operatorname{perm}(M_r(\widehat{f^*})_{[3,4]}) = -4 \neq 0$. Contradiction.

- There is a row or a column of $M_r(\widehat{f^*})$ such that it has an even number of -1 entries. By transposing $M_r(\widehat{f^*})$, we may assume that it is a row, say Row i. For any other Row j, it differs with Row i in exactly two columns. Thus, Row j also has an even number of -1 entries. If all four rows of $M_r(\widehat{f^*})$ have exactly two -1 entries, then one can check that there are two rows such that one row is a scalar (± 1) multiple of the other, thus not orthogonal; this is a contradiction. Thus, there exists a row in which the number of -1 entries is 0 or 4. By permuting rows, we may assume that it is Row 1. Also, by possibly multiplying $M_r(\widehat{f^*})$ with -1, we may assume that all entries of Row 1 are $+1$. Thus, Row 1 is $(1,1,1,1)$.

  By orthogonality, all other rows have exactly two -1 entries. By permuting columns (which does not change Row 1), we may assume that Row 2 is $(-1,-1,1,1)$. Then, consider Row 3. It also has exactly two -1 entries. Moreover, since Row 2 and Row 3 differ in 2 columns, among m_{31} and m_{32}, exactly one is -1. By permuting Column 1 and Column 2 (which does not change Row 1 and Row 2), we may assume that $m_{31} = -1$. Also, among m_{33} and m_{34}, exactly one is -1. By permuting Column 3 and Column 4 (still this will not change Row 1 and Row 2), we may assume that $m_{33} = -1$. Thus, Row 3 is $(-1,1,-1,1)$. Finally, consider Row 4. It also has two -1 entries. One can easily check that Row 4 has two possible forms,

$(-1,1,1,-1)$ or $(1,-1,-1,1)$. If Row 4 is $(1,-1,-1,1)$, then,

$$M_r(\widehat{f^*}) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Thus, $\operatorname{perm}(M_r(\widehat{f^*})_{[12]}) + \operatorname{perm}(M_r(\widehat{f^*})_{[34]}) = -4 \neq 0$. Contradiction.

Thus, Row 4 is $(-1,1,1,-1)$. Then

$$M_r(\widehat{f^*}) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}.$$

This gives the desired $M_r(\widehat{f_6})$.

Therefore, $\widehat{f_6}$ is realizable from $\widehat{f^*}$.

Since $\widehat{f_6}$ is realized from $\widehat{f^*}$ by flipping (and permuting) variables, i.e., extending some variables of $\widehat{f^*}$ with $=_2$ (using $\neq_2$), we have $\widehat{f_6} \in \{\widehat{f^*}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. Since $\widehat{f^*}$ is realized from $\widehat{f''}$ by extending some variables of $\widehat{f''}$ with signatures in $\widehat{\mathcal{B}}$, we have $\widehat{f^*} \in \{\widehat{f''}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. By Lemma 3.11, we have $\widehat{f_6} \in \{\widehat{f''}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. □

Theorem 7.5. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition (T). Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$ If $\widehat{\mathcal{F}}$ contains a 6-ary signature $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then*

- $\operatorname{Holant}(\neq_2|\,\widehat{\mathcal{F}})$ *is #P-hard, or*
- *there exists some $\widehat{Q} \in \widehat{\mathbf{O}_2}$ such that* $\operatorname{Holant}(\neq_2|\,\widehat{f_6}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|\,\widehat{\mathcal{F}})$.

证明. By Lemmas 7.1, 7.2 and 7.3, $\operatorname{Holant}(\neq_2|\,\widehat{\mathcal{F}})$ is #P-hard, or $\operatorname{Holant}(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|\,\widehat{\mathcal{F}})$ for some $\widehat{Q}$ where $Q \in \widehat{\mathbf{O}_2}$, and some irreducible 6-ary signature $\widehat{f''}$ where $\mathscr{S}(\widehat{f''}) = \mathscr{E}_6$ and there exists $\lambda = 1$ or $\mathfrak{i}$ such that for all $\alpha \in \mathscr{S}(\widehat{f''})$, $\widehat{f''}(\alpha) = \pm\lambda$. Remember that $\widehat{Q}\widehat{\mathcal{F}} = \widehat{Q\mathcal{F}}$ where $Q = Z\widehat{Q}Z^{-1} \in \mathbf{O}_2$. Clearly, $Q\mathcal{F}$ is a set of real-valued signatures of even arity. Since $\mathcal{F}$ does not satisfy condition (T), by Lemma 2.37, $Q\mathcal{F}$ also does not satisfy it. Then, by

Lemma 7.4, $\operatorname{Holant}(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}})$ is #P-hard, or $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|{=_2}, \widehat{f''}, \widehat{Q}\widehat{\mathcal{F}})$. Thus, $\operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$ is #P-hard, or $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$. □

Remark 7.6. *Theorem 7.5 can be more succinctly stated as simply that a reduction*

$$\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$$

exists, because when $\operatorname{Holant}(\neq_2|\, \widehat{\mathcal{F}})$ *is #P-hard, the reduction exists trivially. However in keeping with the cadence of the other lemmas and theorems in this subsection, we list them as two cases.*

Now, we want to show that $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{Q}\widehat{\mathcal{F}})$ is #P-hard for all $\widehat{Q} \in \widehat{\mathbf{O}_2}$ and all $\widehat{\mathcal{F}}$ where $\mathcal{F} = Z\widehat{\mathcal{F}}$ is a real-valued signature set that does not satisfy condition (T). If so, then we are done. Recall that for all $\widehat{Q} \in \widehat{\mathbf{O}_2}$, $\widehat{Q}\widehat{\mathcal{F}} = \widehat{Q\mathcal{F}}$ for some $Q \in \mathbf{O}_2$. Moreover, for all $Q \in \mathbf{O}_2$, and all real-valued $\mathcal{F}$ that does not satisfy condition (T), $Q\mathcal{F}$ is also a real-valued signature set that does not satisfy condition (T). Thus, it suffices for us to show that $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{\mathcal{F}})$ is #P-hard for all real-valued $\mathcal{F}$ that does not satisfy condition (T).

7.2 #P-Hardness Conditions and Two Properties of $\widehat{f_6}$

In this section, we give three conditions (Lemmas 7.7, 7.9 and 7.10) which can quite straightforwardly lead to the #P-hardness of $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{\mathcal{F}})$. We will extract two properties from $\widehat{f_6}$, the non-$\widehat{\mathcal{B}}$ hardness (Definition 7.8) and the realizability of $\widehat{\mathcal{B}}$ (Lemma 7.13). Later, we will prove the #P-hardness of $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{\mathcal{F}})$ based on these two properties.

Lemma 7.7. *Suppose that* $\mathcal{F}$ *is a set of real-valued signatures of even arity and* $\mathcal{F}$ *does not satisfy condition (T). Let* $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$*. If* $\widehat{\mathcal{F}}$ *contains a nonzero binary signature* $\widehat{b} \notin \widehat{\mathcal{B}}^{\otimes}$*, then* $\operatorname{Holant}(\neq_2|\, \widehat{f_6}, \widehat{\mathcal{F}})$ *is #P-hard.*

证明. If $\widehat{b} \notin \widehat{\mathcal{O}}^{\otimes}$, then by Lemma 6.7, we are done. Otherwise, $\widehat{b} \in \widehat{\mathcal{O}}^{\otimes}$. Thus, $\widehat{b} = (a, 0, 0, \bar{a})$ or $\widehat{b} = (0, a, \bar{a}, 0)$. Since $\widehat{b} \not\equiv 0$, $a \neq 0$. We normalize the norm of a to 1. Since $\widehat{b} \notin \widehat{\mathcal{B}}^{\otimes}$, $a \neq \pm 1$ or $\pm \mathfrak{i}$. We first consider the case that $\widehat{b}(y_1, y_2) = (0, a, \bar{a}, 0)$. Connecting variables x_1 and x_2 of $\widehat{f_6}$ with variables y_2 and y_1 of $\widehat{b}$ using $\neq_2$, we get a 4-ary signature $\widehat{g}$. We list the truth table of $\widehat{g}$ indexed by the assignments of variables (x_3, x_4, x_5, x_6) from 0000 to 1111.

$$\widehat{g} = (0, a + \bar{a}, -a + \bar{a}, 0, a - \bar{a}, 0, 0, -a - \bar{a}, -a - \bar{a}, 0, 0, -a + \bar{a}, 0, a - \bar{a}, a + \bar{a}, 0).$$

Since a has norm 1, and $a \neq \pm 1$ or $\pm \mathfrak{i}$, $|a \pm \bar{a}| \neq 0$. Thus, $|\mathscr{S}(\widehat{g})| = 8$. Clearly, every 4-ary signature that is in $\widehat{\mathcal{O}}^{\otimes}$ has support of size 0 or 4. Thus, $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$. By Lemma 6.8, $\operatorname{Holant}(\neq_2 | \widehat{f}_6, \widehat{\mathcal{F}})$ is #P-hard. We prove the case $\widehat{b}(y_1, y_2) = (a, 0, 0, \bar{a})$ similarly. By connecting variables x_1 and x_2 of $\widehat{f}_6$ with variables y_1 and y_2 of $\widehat{b}$ using $\neq_2$, we also get a 4-ary signature that is not in $\widehat{\mathcal{O}}^{\otimes}$. The lemma is proved. □

Definition 7.8. *We say a signature set $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard, if for any nonzero binary signature $\widehat{b} \notin \widehat{\mathcal{B}}^{\otimes}$, the problem* $\operatorname{Holant}(\neq_2 | \widehat{b}, \widehat{\mathcal{F}})$ *is #P-hard. Correspondingly, we say that a signature set $\mathcal{F}$ is non-$\mathcal{B}$ hard, if for any nonzero binary signature $b \notin \mathcal{B}^{\otimes}$, the problem* $\operatorname{Holant}(b, \mathcal{F})$ *is #P-hard.*

Clearly, Lemma 7.7 says that $\{\widehat{f}_6\} \cup \widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard for any $\widehat{\mathcal{F}}$ (where $\mathcal{F} = Z\widehat{\mathcal{F}}$ is a real-valued signature set that does not satisfy condition (T)). Before we give the other two #P-hardness conditions, we first explain why we introduce the notion of non-$\widehat{\mathcal{B}}$ hardness. We will extract two properties from $\widehat{f}_6$ to prove the #P-hardness of $\operatorname{Holant}(\neq_2 | \widehat{f}_6, \widehat{\mathcal{F}})$. These are the non-$\widehat{\mathcal{B}}$ hardness and the realizability of $\widehat{\mathcal{B}}$. From Lemma 7.13* we get the redutcion $\operatorname{Holant}(\neq_2 | \widehat{f}_6, \widehat{\mathcal{B}} \cup \widehat{\mathcal{F}}) \leqslant \operatorname{Holant}(\neq_2 | \widehat{f}_6, \widehat{\mathcal{F}})$. We will show that for any non-$\widehat{\mathcal{B}}$ hard set $\widehat{\mathcal{F}}$ where $\mathcal{F}$ does not satisfy condition (T), $\operatorname{Holant}(\neq_2 | \widehat{\mathcal{B}} \cup \widehat{\mathcal{F}})$ is #P-hard (Theorem 7.38). This directly implies that $\operatorname{Holant}(\neq_2 | \widehat{f}_6, \widehat{\mathcal{F}})$ is #P-hard when $\mathcal{F}$ does not satisfy condition (T). This slightly more general Theorem 7.38 will also be used when dealing with signatures of arity 8. Now, let us continue to give two more #P-hardness conditions without assuming the availability of $\mathcal{B}$ (Lemma 7.9 and 7.10).

Lemma 7.9. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard and $\widehat{\mathcal{F}}$ contains a nonzero 4-ary signature $\widehat{f} \notin \widehat{\mathcal{B}}^{\otimes}$, then* $\operatorname{Holant}(\neq_2 | \widehat{\mathcal{F}})$ *is #P-hard.*

证明. If $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then by Lemma 6.8, we are done. Otherwise, $\widehat{f} = \widehat{b_1} \otimes \widehat{b_2}$, where the binary signatures $\widehat{b_1}, \widehat{b_2} \in \widehat{\mathcal{O}}^{\otimes}$. Since $\widehat{f} \notin \widehat{\mathcal{B}}^{\otimes}$, $\widehat{b_1}$ and $\widehat{b_2}$ are not both in $\widehat{\mathcal{B}}^{\otimes}$. Then, we can realize a binary signature that is not in $\widehat{\mathcal{B}}^{\otimes}$ by factorization. Since $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard, we are done. □

*This lemma and the following Theorem 7.38 are stated and proved in the setting of $\operatorname{Holant}(\mathcal{F})$.

Let $H = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right]$. Then $\widehat{H} = Z^{-1}HZ = \begin{bmatrix} \frac{(1+\mathrm{i})}{\sqrt{2}} & 0 \\ 0 & \frac{(1-\mathrm{i})}{\sqrt{2}} \end{bmatrix} = \left[\begin{smallmatrix} e^{\mathrm{i}\pi/4} & 0 \\ 0 & e^{-\mathrm{i}\pi/4} \end{smallmatrix}\right]$. Let $\widehat{f_6^H} = \widehat{H}\widehat{f_6}$. Let $\widehat{\mathcal{F}_6} = \{\widehat{f_6}\}^{\widehat{B}}_{\neq_2}$ be the set of signature realizable by extending variables of $\widehat{f_6}$ with binary signatures in $\widehat{\mathcal{B}}$ using $\neq_2$, and $\widehat{\mathcal{F}_6^H} = \{\widehat{f_6^H}\}^{\widehat{B}}_{\neq_2}$ be the set of signature realizable by extending variables of $\widehat{f_6^H}$ with binary signatures in $\widehat{\mathcal{B}}$ using $\neq_2$. One can check that $\widehat{\mathcal{F}_6^H} = \widehat{H}\widehat{\mathcal{F}_6} \neq \widehat{\mathcal{F}_6}$.

Lemma 7.10. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition (T). Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard and $\widehat{\mathcal{F}}$ contains a nonzero 6-ary signature $\widehat{f} \notin \widehat{\mathcal{B}}^{\otimes} \cup \widehat{\mathcal{F}_6} \cup \widehat{\mathcal{F}_6^H}$, then* Holant$(\neq_2|\,\widehat{\mathcal{F}})$ *is #P-hard.*

证明. If $\widehat{f}$ is reducible, since $\widehat{f} \notin \widehat{\mathcal{B}}^{\otimes}$, then by factorization, we can realize a nonzero signature of odd arity or a nonzero signature of arity 2 or 4 that is not in $\widehat{\mathcal{B}}^{\otimes}$. If we have a nonzero signature of odd arity, then we are done by Theorem 5.35. If we have a nonzero signature of 2, then we are done because $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard. If we have a nonzero signature of 4, then we are done by Lemma 7.9. Now we assume that $\widehat{f}$ is irreducible. In particular, being irreducible, $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$. For a contradiction, suppose that Holant$(\neq_2|\,\widehat{\mathcal{F}})$ is not #P-hard. Then, by Theorem 7.5, $\widehat{f_6}$ is realizable from $\widehat{f}$. Remember that we realize $\widehat{f_6}$ from $\widehat{f}$ by realizing $\widehat{f'}$, $\widehat{f''}$ and $\widehat{f^*}$ (Lemmas 7.1, 7.3 and 7.4). We will trace back this process and show that they are all in $\widehat{\mathcal{F}_6} \cup \widehat{\mathcal{F}_6^H}$, which contradicts with the condition that $\widehat{f} \notin \widehat{\mathcal{F}_6} \cup \widehat{\mathcal{F}_6^H}$.

1. First, by Lemma 7.4, $\widehat{f_6} \in \{\widehat{f''}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. Then, by Lemma 3.11, $\widehat{f''} \in \{\widehat{f_6}\}^{\widehat{\mathcal{B}}}_{\neq_2} = \widehat{\mathcal{F}_6}$.

2. Then, by Lemma 7.3, $\widehat{f''} = \widehat{Q}\widehat{f'}$ for some $\widehat{Q} = \left[\begin{smallmatrix} e^{-\mathrm{i}\delta} & 0 \\ 0 & e^{\mathrm{i}\delta} \end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$ where $0 \leqslant \delta < \pi/2$, and the binary signature $\widehat{b} = (e^{\mathrm{i}2\delta}, 0, 0, e^{-\mathrm{i}2\delta})$ is realizable from $\widehat{f'}$ where $\widehat{f'}$ is realizable from $\widehat{f}$. Thus, $\widehat{b}$ is realizable from $\widehat{\mathcal{F}}$. If $e^{\mathrm{i}2\delta} \neq \pm 1$ or $\pm\mathfrak{i}$, then $\widehat{b} \notin \widehat{\mathcal{B}}^{\otimes}$. Since $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard, we get #P-harness. Contradiction. Otherwise, since $0 \leqslant \delta < \pi/2$, $e^{\mathrm{i}2\delta} = 1$ or $\mathfrak{i}$ and then, $\delta = 0$ or $\pi/4$. If $\delta = 0$, then $e^{\mathrm{i}\delta} = e^{-\mathrm{i}\delta} = 1$ and $\widehat{f''} = \widehat{Q}\widehat{f'} = \widehat{f'}$. Thus, $\widehat{f'} \in \widehat{\mathcal{F}_6}$. If $\delta = \pi/4$, then $\widehat{f'} = \widehat{Q}^{-1}\widehat{f''}$ where $\widehat{Q}^{-1} = \left[\begin{smallmatrix} e^{\mathrm{i}\pi/4} & 0 \\ 0 & e^{-\mathrm{i}\pi/4} \end{smallmatrix}\right] = \widehat{H}$. Since $\widehat{f''} \in \widehat{\mathcal{F}_6}$, $\widehat{f'} = \widehat{H}\widehat{f''} \in \widehat{H}\widehat{\mathcal{F}_6} = \widehat{\mathcal{F}_6^H}$.

3. Finally, by Lemma 7.1, $\widehat{f'}$ is realized by extending variables of $\widehat{f}$ with nonzero binary signatures realized from $\widehat{\partial}_{12}\widehat{f}$. If we can realize a nonzero binary signature that is not in $\widehat{\mathcal{B}}^{\otimes 1}$ from $\widehat{\partial}_{12}\widehat{f}$ by factorization, then since $\widehat{\mathcal{F}}$ is non-$\widehat{\mathcal{B}}$ hard, we get #P-hardness. Contradiction. Thus, we may assume that all nonzero binary signatures realizable from $\widehat{\partial}_{12}\widehat{f}$ are in $\widehat{\mathcal{B}}^{\otimes 1}$. Then, $\widehat{f'}$ is

realized by extending variables of $\widehat{f}$ with nonzero binary signatures in $\widehat{\mathcal{B}}^{\otimes 1}$. Thus, $\widehat{f'} \in \{\widehat{f}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. By Lemma 3.11, $\widehat{f} \in \{\widehat{f'}\}^{\widehat{\mathcal{B}}}_{\neq_2}$. Since $\widehat{f'} \in \widehat{\mathcal{F}_6}$ or $\widehat{\mathcal{F}^H_6}$, $\widehat{f} \in \widehat{\mathcal{F}_6}$ or $\widehat{\mathcal{F}^H_6}$. Contradiction.

Thus, $\operatorname{Holant}(\neq_2|\,\widehat{\mathcal{F}})$ is #P-hard if $\widehat{\mathcal{F}}$ contains a nonzero 6-ary signature $\widehat{f} \notin \widehat{\mathcal{B}}^{\otimes} \cup \widehat{\mathcal{F}_6} \cup \widehat{\mathcal{F}^H_6}$. □

We go back to real-valued Holant problems under the Z-transformation. Consider the problem $\operatorname{Holant}(f_6, \mathcal{F})$ where

$$f_6 = Z\widehat{f_6} = \chi_S \cdot (-1)^{x_1+x_2+x_3+x_1x_2+x_2x_3+x_1x_3+x_1x_4+x_2x_5+x_3x_6}$$

and $S = \mathscr{S}(f_6) = \mathscr{E}_6$. The signature f_6 has a quite similar matrix form to $\widehat{f_6}$.

$$M_{123,456}(f_6) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 & -1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & -1 & -1 & 0 & 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & -1 \end{bmatrix}.$$

Since $\widehat{f^H_6} = \widehat{H}\widehat{f_6} = \widehat{Hf_6}$, $f^H_6 = Z\widehat{f^H_6} = Hf_6$. Also, since $\widehat{\mathcal{F}_6} = \{\widehat{f_6}\}^{\widehat{\mathcal{B}}}_{\neq_2}$, $\mathcal{F}_6 = Z\widehat{\mathcal{F}_6} = \{f_6\}^{\mathcal{B}}_{=_2}$ is the set of signatures realizable by extending variables of f_6 with binary signatures in $\mathcal{B}$ using $=_2$. Similarly, since $\widehat{\mathcal{F}^H_6} = \{\widehat{f^H_6}\}^{\widehat{\mathcal{B}}}_{\neq_2}$, $\mathcal{F}^H_6 = Z\widehat{\mathcal{F}^H_6} = \{f_6\}^{\mathcal{B}}_{=_2}$ is the set of signatures realizable by extending variables of f^H_6 with binary signatures in $\mathcal{B}$ using $=_2$. Notice that $f_6 \in \mathscr{A}$ and $\mathcal{B} \subseteq \mathscr{A}$. Thus, $\mathcal{F}_6 \subseteq \mathscr{A}$. Also, the binary signature $(1, 1, -1, 1)$ with a signature matrix H is in $\mathscr{A}$. Thus, $f^H_6 \in \mathscr{A}$ and then $\mathcal{F}^H_6 \subseteq \mathscr{A}$. Also, $\mathscr{S}(f_6) = \mathscr{E}_6$ and one can check that $\mathscr{S}(f^H_6) = \mathscr{O}_6$. Thus, for every $f \in \mathcal{F}_6 \cup \mathcal{F}^H_6$, $\mathscr{S}(f) = \mathscr{E}_6$ or $\mathscr{O}_6$. Since f_6 and f^H_6 satisfy 2nd-Orth, one can easily check that every $f \in \mathcal{F}_6 \cup \mathcal{F}^H_6$ satisfies 2nd-Orth.

We want to show that $\operatorname{Holant}(f_6, \mathcal{F}) \equiv_T \operatorname{Holant}(\neq_2|\,\widehat{f_6}, \widehat{\mathcal{F}})$ is #P-hard for all real-valued $\mathcal{F}$ that does not satisfy condition (T). By Lemma 7.7, $\{f_6\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard. We restate Lemmas 7.9 and 7.10 in the setting of $\operatorname{Holant}(\mathcal{F})$ for non-$\mathcal{B}$ hard $\mathcal{F}$.

Corollary 7.11. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition* (T)*, and $\mathcal{F}$ is non-$\mathcal{B}$ hard. Then,* Holant$(\mathcal{F})$ *is #P-hard if $\mathcal{F}$ contains a nonzero signature f of arity at most 6 where $f \notin \mathcal{B}^{\otimes} \cup \mathcal{F}_6 \cup \mathcal{F}_6^H$.*

Remark 7.12. *Notice that $\mathcal{B}^{\otimes} \cup \mathcal{F}_6 \cup \mathcal{F}_6^H \subseteq \mathscr{A}$. Thus, for any non-$\mathcal{B}$ hard set $\mathcal{F}$,* Holant$(\mathcal{F})$ *is #P-hard if $\mathcal{F}$ contains a nonzero signature f of arity at most 6 where $f \notin \mathscr{A}$.*

Now, we show that all four binary signatures in $\mathcal{B}$ are realizable from f_6.

Lemma 7.13. Holant$(\mathcal{B}, f_6, \mathcal{F}) \leqslant$ Holant$(f_6, \mathcal{F})$.

证明. Consider $\partial_{12} f_6$. Notice that

$$\begin{bmatrix} \mathbf{f_6}_{12}^{00} \\ \mathbf{f_6}_{12}^{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & 0 & -1 & -1 & 0 & -1 & 0 & 0 & -1 \end{bmatrix}.$$

Thus, $\partial_{12} f_6(x_3, x_4, x_5, x_6) = {f_6}_{12}^{00} + {f_6}_{12}^{11}$ has the truth table $(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, -1, 0, -1, 0, 0, 0)$. In other words, $\partial_{12} f_6(0011) = 1$, $\partial_{12} f_6(0101) = 1$, $\partial_{12} f_6(1010) = -1$, $\partial_{12} f_6(1100) = -1$, and $\partial_{12} f_6 = 0$ elsewhere. Then,

$$\mathscr{S}(\partial_{12} f_6) = \{(x_3, x_4, x_5, x_6) \in \mathbb{Z}_2^4 \mid x_3 \neq x_6 \wedge x_4 \neq x_5\},$$

and

$$\partial_{12} f_6(x_3, x_4, x_5, x_6) = (\neq_2^-)(x_3, x_6) \otimes (\neq_2)(x_4, x_5).$$

Thus, by factorization we can realize $\neq_2^-$ and $\neq_2$. Then connecting a variable of $\neq_2^-$ with a variable of $\neq_2$ (using $=_2$), we will get $=_2^-$. Thus, $\mathcal{B}$ is realizable from f_6. □

We define the problem Holant$^b(\mathcal{F})$ to be Holant$(\mathcal{B} \cup \mathcal{F})$. For all $\{i, j\}$ and every $b \in \mathcal{B}$, consider signatures $\partial_{ij}^b f_6$ (i.e., $\partial_{ij}^+ f_6$, $\partial_{ij}^{\hat{+}} f_6$, $\partial_{ij}^- f_6$ and $\partial_{ij}^{\hat{-}} f_6$) realized by merging variables x_i and x_j of f_6 using the binary signature b. If there were one that is not in $\mathcal{B}^{\otimes 2}$, then by Corollary 7.11, we would be done. However, f_6 satisfies the following Bell property.

Definition 7.14 (Bell property)**.** *An irreducible signature f satisfies the Bell property if for all pairs of indices $\{i, j\}$ and every $b \in \mathcal{B}$, $\partial_{ij}^b f \in \mathcal{B}^{\otimes}$. (Here, ∂_{ij}^b denotes the merging gadget using b.)*

It can be directly checked that

Lemma 7.15. *Every signature in $\mathcal{F}_6 \cup \mathcal{F}_6^H$ satisfies the Bell property.*

Now consider all possible gadget constructions. If we could realize a signature of arity at most 6 that is not in $\mathcal{B}^{\otimes} \cup \mathcal{F}_6 \cup \mathcal{F}_6^H$ from $\mathcal{B}$ and f_6 by any possible gadget, then by Corollary 7.11 there would be a somewhat more straightforward proof to our dichotomy theorem for the case of arity 6. However, after many failed attempts, we believe there is a more intrinsic reason why this approach cannot work. The following conjecture formulates this difficulty. This truly makes f_6 the *Lord of Intransigence* at arity 6.

Conjecture 7.16. *All nonzero signatures of arity at most* 6 *realizable from* $\mathcal{B} \cup \{f_6\}$ *are in* $\mathcal{B}^{\otimes} \cup \mathcal{F}_6$*. Also, all signatures of arity at most* 6 *realizable from* $\mathcal{B} \cup \{f_6^H\}$ *are in* $\mathcal{B}^{\otimes} \cup \mathcal{F}_6^H$*.*

So to prove the #P-hardness of $\operatorname{Holant}^b(f_6, \mathcal{F})$, we have to make additional use of $\mathcal{F}$. In particular, we need to use a non-affine signature in $\mathcal{F}$.

7.3 #P-Hardness of $\operatorname{Holant}^b(\mathcal{F})$

In this section, we prove that for all real-valued non-$\mathcal{B}$ hard set $\mathcal{F}$ that does not satisfy condition (T), $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard (Theorem 7.38). For any real-valued set $\mathcal{F}$ that does not satisfy condition (T), the set $\{f_6\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard, and since $\mathcal{B}$ is realizable from f_6, $\operatorname{Holant}(f_6, \mathcal{F})$ is #P-hard by Theorem 7.38. Combining with Theorem 7.5, we show that $\operatorname{Holant}(\neq_6 | \widehat{\mathcal{F}})$ is #P-hard if $\widehat{\mathcal{F}}$ contains a 6-ary signature that is not in $\widehat{\mathcal{O}}^{\otimes}$ (Lemma 7.40).

Since $\mathcal{F}$ does not satisfy condition (T), $\mathcal{F} \not\subseteq \mathscr{A}$. Thus, it contains a signature f of arity $2n$ that is not in $\mathscr{A}$. In the following, we will prove the #P-hardness of $\operatorname{Holant}^b(\mathcal{F})$ where $\mathcal{F}$ is non-$\mathcal{B}$ hard by induction on $2n \geqslant 2$. For the base cases $2n \leqslant 6$, by Corollary 7.11 and the Remark after that, $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard. Then, starting with a signature of arity $2n \geqslant 8$ that is not in $\mathscr{A}$, we want to realize a signature of lower arity $2k \leqslant 2n - 2$ that is also not in $\mathscr{A}$, or else we get #P-hardness directly. If we can reduce the arity down to at most 6, then we are done.

Let $f \notin \mathscr{A}$ be a nonzero signature of arity $2n \geqslant 8$. We first show that if f does not have parity, then we get #P-hardness (Lemma 7.17). Then, suppose that f has parity. If f is reducible, since f has even arity (as we assumed so starting from Chapter 6), it is a tensor product of two signatures of odd arity, or a tensor product of two signatures of even arity which are not both in $\mathscr{A}$ since $f \notin \mathscr{A}$. Thus, by factorization, we can realize a nonzero signature of odd arity and we get #P-hardness by Theorem 5.35, or we can realize a signature of lower even arity that is not in $\mathscr{A}$. Thus, we may assume that f is irreducible. Then by Lemma 6.6 and the Remark after Definition 3.20 we may assume f satisfies 2ND-ORTH.

Consider signatures $\partial^{b}_{ij} f$ (i.e., $\partial^{+}_{ij} f$, $\partial^{-}_{ij} f$, $\partial^{\widehat{+}}_{ij} f$ and $\partial^{\widehat{-}}_{ij} f$) realized by merging variables x_i and x_j of f using $b \in \mathcal{B}$ for all pairs of indices $\{i, j\}$ and every $b \in \mathcal{B}$. If there is one signature that is not in $\mathscr{A}$, then we have realized a signature of arity $2n-2$ that is not in $\mathscr{A}$. Otherwise, $\partial^{b}_{ij} f \in \mathscr{A}$ for all $\{i, j\}$ and every $b \in \mathcal{B}$. We denote this property by $f \in \int_{\mathcal{B}} \mathscr{A}$. Now, assuming that f has parity, f satisfies 2ND-ORTH and $f \in \int_{\mathcal{B}} \mathscr{A}$, we would like to reach a contradiction by showing that this would force f itself to belong to $\mathscr{A}$. However, quite amazingly, there do exist non-affine signatures that satisfy these stringent conditions. We will show how they are discovered and handled (Lemmas 7.27, 7.35 and 7.37).

In this section, all signatures are real-valued. When we say an entry of a signature has norm a, we mean it takes value $\pm a$. Since $\mathcal{B}$ is available in $\operatorname{Holant}^{b}(\mathcal{F})$, if a signature f is realizable in $\operatorname{Holant}^{b}(\mathcal{F})$, then we can realize all signatures in $\{f\}^{\mathcal{B}}_{=_2}$ that are realizable by extending f with $\mathcal{B}^{\otimes 1}$ (using $=_2$). If we extend the variable x_i of f with $\neq_2$, then we will get a signature g where $g^0_i = f^1_i$ and $g^1_i = f^0_i$. This is a flipping operation on the variable x_i. If we extend the variable x_i of f with $=^{-}_{2}$, then we will get a signature g where $g^0_i = f^0_i$ and $g^1_i = -f^1_i$. We call this a negating operation on the variable x_i. In the following, once f is realizable in $\operatorname{Holant}^{b}(\mathcal{F})$, we may modify it by flipping or negating. This will not change the complexity of the problem.

7.3.1 Parity Condition

We first show that if $\mathcal{F}$ contains a signature that does not have parity, then we can get #P-hardness.

Lemma 7.17. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition (T), $\mathcal{F}$ is non-$\mathcal{B}$ hard and $\mathcal{F}$ contains a signature f of arity $2n$. If f does not have parity, then* $\operatorname{Holant}^{b}(\mathcal{F})$ *is #P-hard.*

证明. We prove this lemma by induction on $2n$. We first consider the base case that $2n = 2$. Since

f has no parity, $f \notin \mathcal{B}$. Since $\mathcal{F}$ is non-$\mathcal{B}$ hard, $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard.

Now, suppose that $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard when $2n = 2k \geqslant 2$. Consider the case that $2n = 2k+2 \geqslant 4$. We will show that we can realize a signature g of arity $2k$ with no parity from f, i.e., $\operatorname{Holant}^b(g, \mathcal{F}) \leqslant_T \operatorname{Holant}^b(\mathcal{F})$. Then by the induction hypothesis, we have $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard when $2n = 2k+2$.

Since f has no parity, $f \not\equiv 0$. It has at least a nonzero entry. By flipping variables of f, we may assume that $f(\vec{0}^{2n}) = x \neq 0$. We denote $\vec{0}^{2n}$ by $\alpha = 000\delta$ where $\delta = \vec{0}^{2n-3}$. Since f has no parity and $f(\vec{0}^{2n}) \neq 0$, there exists an input α' with $\operatorname{wt}(\alpha') \equiv 1 \pmod 2$ such that $f(\alpha') = x' \neq 0$. Since $2n \geqslant 4$, we can find three bits of α' such that on these three bits, the values of α' are the same. By renaming variables of f which gives a permutation of α', without loss of generality, we may assume that these are the first three bits, i.e, $\alpha'_1 = \alpha'_2 = \alpha'_3$.

We first consider the case that $\alpha'_1\alpha'_2\alpha'_3 = 000$. Then, $\alpha' = 000\delta'$ for some $\delta' \in \mathbb{Z}_2^{2n-3}$ where $\operatorname{wt}(\delta') = \operatorname{wt}(000\delta') = \operatorname{wt}(\alpha') \equiv 1 \pmod 2$. We consider the following six entries of f.

$$x = f(000\delta), x' = f(000\delta'), y = f(011\delta), y' = f(011\delta'), z = f(101\delta), z' = f(101\delta').$$

Consider signatures $\partial^+_{23}f$ and $\partial^-_{23}f$ realized by connecting variables x_2 and x_3 of f using $=^+_2$ and $=^-_2$ respectively. Clearly, $\partial^+_{23}f$ and $\partial^-_{23}f$ have arity $2n-2$. If one of them has no parity, then we are done. Thus, we may assume that $\partial^+_{23}f$ and $\partial^-_{23}f$ both have parity. Note that $x+y$ and $x'+y'$ are entries of the signature $\partial^+_{23}f$ on inputs 0δ and $0\delta'$ respectively. Clearly, $\operatorname{wt}(0\delta) = 0$ and $\operatorname{wt}(0\delta') \equiv 1 \pmod 2$. Since $\partial^+_{23}f$ has parity, at least one of $x+y$ and $x'+y'$ is zero. Thus, we have $(x+y)(x'+y') = 0$. Also, note that $x-y$ and $x'-y'$ are entries of the signature $\partial^-_{23}f$ on inputs 0δ and $0\delta'$ respectively. Then, since $\partial^-_{23}f$ has parity, similarly we have $(x-y)(x'-y') = 0$. Thus,

$$(x+y)(x'+y') + (x-y)(x'-y') = 2(xx'+yy') = 0. \tag{7.8}$$

Consider signatures $\partial^+_{13}f$ and $\partial^-_{13}f$ realized by connecting variables x_1 and x_3 of f using $=_2$ and $=^-_2$ respectively. Again if one of them has no parity, then we are done. Suppose that $\partial^+_{13}f$ and $\partial^-_{13}f$ both have parity. Then, $(x+z)(x'+z') = 0$ since $x+z$ and $x'+z'$ are entries of $\partial^+_{13}f$ on inputs 0δ and $0\delta'$ respectively. Similarly, $(x-z)(x'-z')=0$. Thus,

$$(x+z)(x'+z')+(x-z)(x'-z')=2(xx'+zz')=0. \tag{7.9}$$

Consider signatures $\partial^{\widehat{+}}_{12}f$ and $\partial^{\widehat{-}}_{12}f$ realized by connecting variables x_1 and x_2 of f using $\neq_2$ and $\neq_2^-$ respectively. Again if one of them has no parity, then we are done. Suppose that $\partial^{\widehat{+}}_{12}f$ and $\partial^{\widehat{-}}_{12}f$ both have parity. Then, $(y+z)(y'+z')=0$ since $y+z$ and $y'+z'$ are entries of $\partial^{\widehat{+}}_{12}f$ on inputs 1δ and $1\delta'$ respectively, and $\text{wt}(1\delta)=1$ and $\text{wt}(1\delta')\equiv 0(\text{mod}2)$. Similarly, $(y-z)(y'-z')=0$. Thus,

$$(y+z)(y'+z')+(y-z)(y'-z')=2(yy'+zz')=0. \tag{7.10}$$

Then, consider (7.8) + (7.9) − (7.10). We have $xx'=0$. However, since $x=f(\vec{0}^{2n})\neq 0$ and $x'=f(\alpha')\neq 0$, $xx'\neq 0$. Contradiction.

For the case that $\alpha'_1\alpha'_2\alpha'_3=111$, we have $\alpha'=111\delta'$ for some $\delta'\in\mathbb{Z}_2^{2n-3}$ where $\text{wt}(\delta')=\text{wt}(111\delta')-3=\text{wt}(\alpha')-3\equiv 0 \pmod 2$. We consider the following six entries of f.

$$x=f(000\delta), x'=f(111\delta'), y=f(011\delta), y'=f(100\delta'), z=f(101\delta), z'=f(010\delta').$$

We still consider signatures $\partial^{+}_{23}f$, $\partial^{-}_{23}f$, $\partial^{+}_{13}f$, $\partial^{-}_{13}f$, $\partial^{\widehat{+}}_{12}f$ and $\partial^{\widehat{-}}_{12}f$ and suppose that they all have parity. Then, similar to the above proof of the case $\alpha'_1\alpha'_2\alpha'_3=000$, we can show that $xx'=0$. Contradiction.

Thus, among $\partial^{+}_{23}f$, $\partial^{-}_{23}f$, $\partial^{+}_{13}f$, $\partial^{-}_{13}f$, $\partial^{\widehat{+}}_{12}f$ and $\partial^{\widehat{-}}_{12}f$, at least one does not have parity. Thus, we realized a $2k$-ary signature with no parity. By our induction hypothesis, we are done. □

7.3.2 Norm Condition

Under the assumptions that f has parity, f satisfies 2nd-Orth and $f\in\int_{\mathcal{B}}\mathscr{A}$, we consider whether all nonzero entries of f have the same norm. In Lemma 7.27, we will show that the answer is yes, but only for signatures of arity $2n\geqslant 10$ (this lemma does not require $\mathcal{F}$ to be non-$\mathcal{B}$ hard). For a signature f of arity $2n=8$, we show that either all nonzero entries of f have the same norm, or one of the following signatures g_8 or g'_8 is realizable. These two signatures are defined by

$g_8 = \chi_S - 4 \cdot f_8$ and $g'_8 = q_8 - 4 \cdot f_8$, where

$$S = \mathscr{S}(q_8) = \mathscr{E}_8, \quad q_8 = \chi_S (-1)^{\sum_{1 \leqslant i < j \leqslant 8} x_i x_j} \quad \text{and}$$

$$f_8 = \chi_T \text{ with } T = \mathscr{S}(f_8) = \{(x_1, x_2, \ldots, x_8) \in \mathbb{Z}_2^8 \mid \begin{array}{l} x_1 + x_2 + x_3 + x_4 = 0,\ x_5 + x_6 + x_7 + x_8 = 0, \\ x_1 + x_2 + x_5 + x_6 = 0,\ x_1 + x_3 + x_5 + x_7 = 0\}. \end{array} \tag{7.11}$$

It is here the function f_8 makes its first appearance, we dub it the *Queen of the Night*. Clearly, $g_8, g'_8 \notin \mathscr{A}$ since their nonzero entries have two different norms 1 and 3. One can check that g_8 and g'_8 have parity, g_8 and g'_8 satisfy 2ND-ORTH and $g_8, g'_8 \in \int_{\mathcal{B}} \mathscr{A}$. Thus, one cannot get a non-affine signature by connecting two variables of g_8 or g'_8 using signatures in $\mathcal{B}$. However, fortunately by merging two arbitrary variables of g_8 using $=_2$ and two arbitrary variables of g'_8 using $=_2^-$, we can get 6-ary irreducible signatures that do not satisfy 2ND-ORTH. Thus, we get #P-hardness.

The following Lemma 7.21 regarding the independence number of a family of special graphs is at the heart of the discovery of the signature g_8. It should be of independent interest.

Definition 7.18. *Define the graphs G_{2n} and H_{2n} as follows. The vertex set $V(G_{2n})$ is the set $\mathscr{E}_{2n}$ of all even weighted points in $\mathbb{Z}_2^{2n}$. The vertex set $V(H_{2n})$ is the set $\mathscr{O}_{2n}$ of all odd weighted points in $\mathbb{Z}_2^{2n}$. Two points $u, v \in \mathscr{E}_{2n}$ (or $\mathscr{O}_{2n}$) are connected by an edge iff* $\text{wt}(u \oplus v) = 2$.

Let $\alpha(G_{2n})$ be the independence number of G_{2n} i.e, the size of a maximum independent set of G_{2n}, and $\alpha(H_{2n})$ be the independence number of H_{2n}. Let $S \subseteq [2n]$. We define φ_S be a mapping that flips the values on bits in S for all $u \in \mathscr{E}_{2n}$. In other words, suppose that $u' = \varphi_S(u)$. Then, $u'_i = \overline{u_i}$ if $i \in S$ and $u'_i = u_i$ if $i \notin S$ where u'_i and u_i are values of u and u on bit i respectively. For all S, clearly $\text{wt}(u \oplus v) = 2$ iff $\text{wt}(\varphi_S(u) \oplus \varphi_S(v)) = 2$. When $|S|$ is odd, $\varphi_S(\mathscr{E}_{2n}) = \mathscr{O}_{2n}$. One can easily check that φ_S gives an isomorphism between G_{2n} and H_{2n}. When $|S|$ is even, $\varphi_S(\mathscr{E}_{2n}) = \mathscr{E}_{2n}$. Then, φ_S gives an automorphism of G_{2n}. Also, by permuting these $2n$ bits, we can get an automorphism of G_{2n}. In fact, the automorphism group of G_{2n} is generated by these operations.

Lemma 7.19. *Let $2n \geqslant 6$. Every automorphism ψ of G_{2n} is a product $\varphi_S \circ \pi$ for some automorphism π induced by a permutation of $2n$ bits, and an automorphism φ_S given by flipping the values on some bits in a set S of even cardinality.*

证明. Let ψ be an arbitrary automorphism of G_{2n}. Suppose $\psi(\vec{0}^{2n}) = u$. Let $S \subseteq [2n]$ be the index set where $u_i = 1$. Then $|S| = \mathrm{wt}(u)$ is even, and $\psi' = \varphi_S \circ \psi$ fixes $\vec{0}^{2n}$. Consider $\psi'(v)$ for all $v \in \mathscr{E}_{2n}$ of $\mathrm{wt}(v) = 2$. Since ψ' is an automorphism fixing $\vec{0}^{2n}$, $\psi'(v)$ has weight 2. We denote by e_{ij} the $2n$-bit string with $\mathrm{wt}(e_{ij}) = 2$ having 1's on bits i and j, for $1 \leqslant i < j \leqslant 2n$. Then, $e_{12} = 11\vec{0}^{2n-2}$. By a suitable permutation π of the variables, we have $\pi \circ \psi'(e_{12}) = e_{12}$, while still fixing $\vec{0}^{2n}$. We will show that $\pi \circ \psi' = \pi \circ \varphi_S \circ \psi$ is the identity mapping, i.e., $\pi \circ \varphi_S \circ \psi = 1_{G_{2n}}$. Then, $\psi = \varphi_S^{-1} \circ \pi^{-1}$. We are done.

For simplicity of notations, we reuse ψ to denote $\pi \circ \psi'$ in the following and we show that $\psi = 1_{G_{2n}}$. Consider e_{1i}, for $3 \leqslant i \leqslant 2n$. Note that $\psi(e_{1i})$ is some e_{st} and must have Hamming distance 2 to e_{12}. It is easy to see that the only possibilities are $s \in \{1, 2\}$ and $t > 2$, i.e., from e_{12} we flip exactly one bit in $\{1, 2\}$ and another bit in $\{3, \ldots, 2n\}$. Suppose there are $i \neq i'$ ($i, i' \geqslant 3$) such that $\psi(e_{1i}) = e_{1t}$ and $\psi(e_{1i'}) = e_{2t'}$. Since $\mathrm{wt}(e_{1i} \oplus e_{1i'}) = 2$, we must have $t = t'$. Since $2n \geqslant 6$, we can pick another $i'' \geqslant 3$ such that $i'' \neq i$ and i'. Then, this leads to a contradiction since $e_{1i''}$ must either be mapped to e_{1t} if $\psi(e_{1i''}) = e_{1t''}$, or be mapped to e_{2t} if $\psi(e_{1i''}) = e_{2t''}$; neither is possible. Thus either $\psi(e_{1i})$ is some e_{1t} for all $3 \leqslant i \geqslant 2n$, or is some e_{2t} for all $3 \leqslant i \geqslant 2n$. By a permutation of $\{1, 2\}$ (which maintains the property that ψ fixes $\vec{0}^{2n}$ and e_{12}) we may assume it is the former. Then the mapping $i \mapsto t$ given by $\psi(e_{1i}) = e_{1t}$ for $3 \leqslant i \geqslant 2n$ defines a permutation of the variables for $3 \leqslant i \geqslant 2n$ (which again maintains the property that ψ fixes $\vec{0}^{2n}$ and e_{12}) and, after a permutation of the variables we may now assume that ψ fixes $\vec{0}^{2n}$ and all e_{1i}. For any $1 \leqslant i < j \leqslant 2n$, we have $\mathrm{wt}(\psi(e_{ij})) = 2$ and $\psi(e_{ij})$ has distance 2 from both $\psi(e_{1i}) = e_{1i}$ and $\psi(e_{1j}) = e_{1j}$. Then $\psi(e_{ij})$ must be obtained from e_{1i} by flipping exactly one bit in $\{1, i\}$ and another bit out of $\{1, i\}$. However, it cannot flip bit i which would result in some e_{1t} for some $t > 2$, because ψ already fixed e_{1t}. Thus, it flips bit 1 but not bit i. Similarly in view of e_{1j}, we must flip bit 1 but not bit j. Hence $\psi(e_{ij}) = e_{ij}$, and therefore ψ fixes all v with Hamming weight $\mathrm{wt}(v) \leqslant 2$.

Inductively assume ψ fixes all v of $\mathrm{wt}(v) \leqslant 2k$, for some $k \geqslant 1$. If $k < n$ we prove that ψ also fixes all v of $\mathrm{wt}(v) = 2k + 2$. For notational simplicity we may assume $v = \vec{1}^{2k+2}\vec{0}^{2n-2k-2}$. As $2k + 2 \geqslant 4$, we can choose $u = \vec{1}^{2k}00\vec{0}^{2n-2k-2}$ and $w = 00\vec{1}^{2k}\vec{0}^{2n-2k-2}$, and the two 00 in u and w among the first $2k + 2$ bits are in disjoint bit positions. Clearly $\mathrm{wt}(\psi(v)) \geqslant 2k + 2$ since all strings of wt $\leqslant 2k$ are fixed. Also since $\psi(v)$ has Hamming distance 2 from $\psi(u) = u$ and $\psi(w) = w$, it has weight exactly $2k+2$, and is obtained from u by flipping two bits from 00 to 11 in positions $> 2k$, as well as obtained from w by flipping two bits from 00 to 11 in positions in $\{1,2\} \cup \{t \mid t > 2k+2\}$. In particular, it is 1 in positions 1 to $2k$ (in view of u), and it is also 1 in positions 3 to $2k+2$. But together these positions cover all bits 1 to $2k+2$. Thus $\psi(v) = v$. This completes the induction, and proves the lemma for all $2n \geqslant 6$. □

Remark 7.20. *The condition $2n \geqslant 6$ in Lemma 7.19 is necessary. Here is a counter example for $2n = 4$: ψ fixes 0000 and 1111, and it maps α to $\overline{\alpha}$ for all $\alpha \in \{0,1\}^4$ with $\mathrm{wt}(\alpha) = 2$. If ψ were to be expressible as $\varphi_S \circ \pi$, then since $\psi(0000) = 0000$, we have $S = \emptyset$. Then by $\psi(0011) = 1100$ and $\psi(0101) = 1010$, the permutation π must map variable x_1 to x_4. However this violates $\psi(1001) = 0110$.*

Lemma 7.21. *Let $\{G_{2n}\}$ be the sequence of graphs defined above.*

- *If $2n = 8$, then $\alpha(G_8) = \frac{1}{8}|\mathscr{E}_8| = 2^4$, and the maximum independent set I_8 of G_8 is unique up to an automorphism, where*

$$\begin{aligned}I_8 =\{&00000000, 00001111, 00110011, 00111100, 01010101, 01011010, 01100110, 01101001,\\ &10010110, 10011001, 10100101, 10101010, 11000011, 11001100, 11110000, 11111111\}.\end{aligned}$$

- *If $2n \geqslant 10$, then $\alpha(G_{2n}) < \frac{1}{8}|\mathscr{E}_{2n}| = 2^{2n-4}$.*

证明. We first consider the case $2n = 6$. One can check that the following set

$$I_6 = \{000000, 001111, 110011, 111100\}$$

is an independent set of G_6. Thus, $\alpha(G_6) \geqslant 4$. Next, we show that $\alpha(G_6) = 4$ and I_6 is the unique maximum independent set of $\alpha(G_6)$ up to an automorphism.

Let J_6 be an maximum independent set of G_6. Clearly, $|J_6| \geqslant 4$. After an automorphism of G_6 by flipping some bits, we may assume that $\vec{0}^6 \in J_6$. Then for any $u \in \mathscr{E}_6$ with $\mathrm{wt}(u) = 2$, $u \notin J_6$. If $\vec{1}^6 \in J_6$, then for any $u \in \mathscr{E}_6$ with $\mathrm{wt}(u) = 4$, $u \notin J_6$. Thus, J_6 is maximal with $|J_6| = 2 < 4$, a contradiction. Thus, we have $\vec{1}^6 \notin J_6$. Then all vertices in J_6, except $\vec{0}^6$ have hamming weight 4. After an automorphism by permuting bits (this will not change $\vec{0}^6$), we may assume that $u = 001111 \in J_6$. Consider some other $v \in J_6$ with $\mathrm{wt}(v) = 4$. If $v_1v_2 = 01$ or 10, then $\mathrm{wt}(v_3v_4v_5v_6) = 3$. Thus, $\mathrm{wt}(u \oplus v) = \mathrm{wt}(00 \oplus v_1v_2) + \mathrm{wt}(1111 \oplus v_3v_4v_5v_6) = 1 + 1 = 2$. Contradiction. The only $v \in J_6$ with $\mathrm{wt}(v) = 4$, and $v_1v_2 = 00$ is $v = 001111 = u$. Thus, $v_1v_2 = 11$, i.e., both bits of v are 1 where u is 00. After an automorphism by permuting bits in $\{3, 4, 5, 6\}$ (this will not change $\vec{0}^6$ and u), we may assume that $v = 110011 \in J_6$. For any other $w \in J_6$ with $\mathrm{wt}(w) = 4$, we must have $w_1w_2 = 11$ (by the same proof for the pair (u, v) applied to (u, w)), and also $w_3w_4 = 11$ (by the same proof for the pair (u, v) applied to (v, w)). Thus, $w = 111100$. Then, $J_6 = \{\vec{0}^6, u, v, w\} = I_6$ is maximal. Thus, $\alpha(G_6) = 4$ and I_6 is the unique maximum independent set of $\alpha(G_6)$ up to an automorphism.

Consider $2n = 8$. One can check that I_8 is an independent set of G_8. Thus, $\alpha(G_8) \geqslant 16$. We use G_8^{ab} to denote the subgraph of G_8 induced by vertices $\{u \in \mathscr{E}_8 \mid u_1u_2 = ab\}$ for $(a, b) \in \mathbb{Z}_2^2$. Clearly, G_8^{00} and G_8^{11} are isomorphic to G_6, and G_8^{01} and G_8^{10} are isomorphic to H_6. Since H_6 is isomorphic to G_6, G_8^{01} and G_8^{10} are also isomorphic to G_6. Let J_8 be a maximum independent set of G_8. Clearly, $|J_8| \geqslant |I_8| = 16$. Also, we use J_8^{ab} to denote the subset $\{u \in J_8 \mid u_1u_2 = ab\}$ for $(a, b) \in \mathbb{Z}_2^2$. Similarly, we can define I_8^{ab}. Since J_8 is an independent set of G_8, clearly, for every $(a, b) \in \mathbb{Z}_2^2$, J_8^{ab} is an independent set of G_8^{ab}. Since G_8^{ab} is isomorphic to G_6 and $\alpha(G_6) = 4$, thus $|J_8^{ab}| \leqslant 4$. Then $|J_8| \leqslant 16$. Thus, $|J_8| = 16$, and $|J_8^{ab}| = 4$ for every $(a, b) \in \mathbb{Z}_2^2$. Since the maximum independent set of G_6 is unique up to an automorphism of G_6, which can be extended to an automorphism of G_8 by fixing the first two bits, we may assume that

$$J_8^{00} = I_8^{00} = \{00000000, 00001111, 00110011, 00111100\}$$

after an automorphism of G_8.

Then, consider J_8^{01}. We show that for any $u \in J_8^{01}$, $u_3 \neq u_4$, $u_5 \neq u_6$ and $u_7 \neq u_8$. Otherwise, by switching the pair of bits $\{3, 4\}$ with $\{5, 6\}$ or $\{7, 8\}$ (this will not change J_8^{00}), we may assume that $u_3 = u_4$. Then $\mathrm{wt}(u_1u_2u_3u_4)$ is odd. Since $\mathrm{wt}(u)$ is even, $\mathrm{wt}(u_5u_6u_7u_8)$ is odd. Thus, either $u_5 = u_6$ or $u_7 = u_8$. Still by switching the pair $\{5, 6\}$ with $\{7, 8\}$ (again this will not change J_8^{00}), we may assume that $u_5 = u_6$. Then since $\mathrm{wt}(u_5u_6u_7u_8)$ is odd, we have $u_7 \neq u_8$. Then, one can check that there exists some $v \in J_8^{00}$ such that $v_3v_4v_5v_6 = u_3u_4u_5u_6$. Since $v_1 = v_2$ and $u_1 \neq u_2$, $\mathrm{wt}(u_1u_2 \oplus v_1v_2) = 1$. Also since $v_7 = v_8$ and $u_7 \neq u_8$, $\mathrm{wt}(u_7u_8 \oplus v_7v_8) = 1$. Thus,

$\mathrm{wt}(u \oplus v) = \mathrm{wt}(u_1u_2 \oplus v_1v_2) + \mathrm{wt}(u_7u_8 \oplus v_7v_8) = 2$. This means that the vertices u and v are connected in the graph G_8, a contradiction. Thus, for any $u \in J_8^{01}$, $u_3 \neq u_4$, $u_5 \neq u_6$ and $u_7 \neq u_8$. By permuting bit 3 with bit 4, bit 5 with bit 6, and bit 7 with bit 8 (this will not change J_8^{00}), we may assume that $01010101 \in J_8^{01}$. Consider some other $w \in J_8^{01}$. Since $w_{2i+1} \neq w_{2i+2}$ for any $i = 1, 2$ or 3, the pair $w_{2i+1}w_{2i+2} = 01$ or 10. Among these three pairs, let k denote the number of pairs that are 01. If $k = 3$, then $w = 01010101$. Contraction. If $k = 2$, then $\mathrm{wt}(01010101 \oplus w) = 2$. Contradiction. If $k = 0$, then $w = 01101010$. One can check that $\{01010101, 01101010\}$ is already a maximal independent set of G_8^{01} and it has size $2 < 4$. Contradiction. Thus, $k = 1$. Then, w can take $\binom{3}{1}$ possible values. Thus,

$$J_8^{01} \subseteq I_8^{01} = \{01010101, 01011010, 01100110, 01101001\}.$$

Since, $|J_8^{01}| = 4$, $J_8^{01} = I_8^{01}$.

Consider some $u \in J_8^{10}$. Similar to the proof of J_8^{01}, we can show that $u_3 \neq u_4$, $u_5 \neq u_6$ and $u_7 \neq u_8$. Thus, u can take 2^3 possible values. Moreover, for any $01u' \in J_8^{01}$, $10u' \notin J_8^{10}$. Thus, there are only four remaining values that u can take. Then,

$$J_8^{10} \subseteq I_8^{10} = \{10010110, 10011001, 10100101, 10101010\}.$$

Since $|J_8^{10}| = 4$, $J_8^{10} = I_8^{10}$.

Finally, consider J_8^{11}. We show that for any $u \in J_8^{11}$, $u_3 = u_4$, $u_5 = u_6$ and $u_7 = u_8$. Otherwise, by permuting the pair of bits $\{3, 4\}$ with $\{5, 6\}$ or $\{7, 8\}$ (one can check that this will not change J_8^{01} and J_8^{10}), we may assume that $u_3 \neq u_4$. Since $\mathrm{wt}(u)$ is even, between $\mathrm{wt}(u_5u_6)$ and $\mathrm{wt}(u_7u_8)$, exactly one is even and the other is odd. By permuting the pair of bits $\{5, 6\}$ with $\{7, 8\}$, we may further assume that $u_5 \neq u_6$ and $u_7 = u_8$. Then, one can check that there exists some $v \in J_8^{01}$ such that $u_3u_4u_5u_6 = v_3v_4v_5v_6$. Since $u_1 = u_2$ and $v_1 \neq v_2$, $\mathrm{wt}(u_1u_2 \oplus v_1v_2) = 1$. Also since $u_7 = u_8$ and $v_7 \neq v_8$, $\mathrm{wt}(u_7u_8 \oplus v_7v_8) = 1$. Thus, $\mathrm{wt}(u \oplus v) = \mathrm{wt}(u_1u_2 \oplus v_1v_2) + \mathrm{wt}(u_7u_8 \oplus v_7v_8) = 2$. Contradiction. Thus, for any $u \in J_8^{11}$, it can take 2^3 possible values. Moreover, for any $00u' \in J_8^{00}$, we have $11u' \notin J_8^{11}$. Thus, there are only four remaining values that u can take. Then,

$$J_8^{11} \subseteq I_8^{11} = \{11000011, 11001100, 11110000, 11111111\}.$$

Thus, after an automorphism, $J_8 = I_8$. In other words, I_8 is the unique maximum independent set of G_8 up to an automorphism.

Now, we consider the case $2n \geqslant 10$. For every $(a,b) \in \mathbb{Z}_2^2$, we define G_{2n}^{ab} to be the subgraph of G_{2n} induced by $\{u \in G_{2n} \mid u_1u_2 = ab\}$, and it is isomorphic to G_{2n-2}. Thus,

$$\alpha(G_{2n}) \leqslant \alpha(G_{2n}^{00}) + \alpha(G_{2n}^{01}) + \alpha(G_{2n}^{10}) + \alpha(G_{2n}^{11}) = 4\alpha(G_{2n-2}).$$

Then, $\alpha(G_{2n-2}) < 2^{(2n-2)-4}$ will imply that $\alpha(G_{2n}) < 2^{2n-4}$. Thus, in order to prove $\alpha(G_{2n}) < 2^{2n-4}$ for all $2n \geqslant 10$, it suffices to prove that $\alpha(G_{10}) < 2^{10-4}$. For a contradiction, suppose that $\alpha(G_{10}) \geqslant 2^{10-4}$. Let I be a maximum independent set of G_{10}. Then, $|I| \geqslant 2^6$. We define $I^{ab} = \{u \in I \mid u_1u_2 = ab\}$ for every $(a,b) \in \mathbb{Z}_2$. Since G_{10}^{ab} is isomorphic to G_8 and $\alpha(G_8) = 2^4$, $|I^{ab}| \leqslant 2^4$ for every $(a,b) \in \mathbb{Z}_2^2$. Then, $|I| \leqslant 4 \cdot 2^4$. Thus, $|I| = 2^6$ and $|I^{ab}| = 2^4$ for every $(a,b) \in \mathbb{Z}_2^2$. Since the maximum independent set of G_8 is unique up to an automorphism of G_8 which can be extended to an automorphism of G_{10} by fixing the first two bits, we may assume that $I^{00} = \{00u \mid u \in I_8\}$.

Consider I^{01}. Since $|I^{01}| \neq 0$, there exists some $01v \in I^{01}$. Since $\text{wt}(v)$ is odd, among $\text{wt}(v_3v_4)$, $\text{wt}(v_5v_6)$, $\text{wt}(v_7v_8)$ and $\text{wt}(v_9v_{10})$, there is an odd number (either one or three) of pairs such that $\text{wt}(v_{2i+1}v_{2i+2})$ $(1 \leqslant i \leqslant 4)$ is odd, i.e., $v_{2i+1} \neq v_{2i+2}$. In other words, there are exactly three pairs among v_3v_4, v_5v_6, v_7v_8 and v_9v_{10} such that the values inside each pair are all equal with each other or all distinct with each other. By permuting these pairs of bits $\{3,4\}$, $\{5,6\}$, $\{7,8\}$ and $\{9,10\}$ (this will not change I^{00}), we may assume that either $v_3 = v_4$, $v_5 = v_6$, $v_7 = v_8$ and $v_9 \neq v_{10}$, or $v_3 \neq v_4$, $v_5 \neq v_6$, $v_7 \neq v_8$ and $v_9 = v_{10}$. In both cases, one can check that there exists some $00u \in I^{00}$ such that $u_i = v_i$ for $i \in \{3,\ldots,8\}$. Moreover, $u_9 = u_{10}$ if $v_9 \neq v_{10}$, and $u_9 \neq u_{10}$ if $v_9 = v_{10}$. Then, $\text{wt}(00u \oplus 01v) = \text{wt}(00 \oplus 01) + \text{wt}(u_9u_{10} \oplus v_9v_{10}) = 2$. This contradiction proves that $\alpha(G_{10}) < 2^{10-4}$, and the lemma is proved. □

Remark 7.22. *We remark that $I_8 = \mathscr{S}(f_8)$. Later, we will see that the signature f_8, this Queen of the Night, and its support $\mathscr{S}(f_8)$ have even more extraordinary properties.*

We consider a particular gadget construction that will be used in our proof. Let h_4 be a 4-ary signature with signature matrix $M_{12,34}(h_4) = H_4 = \left[\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{smallmatrix}\right]$. Notice that $H_4H_4^{\mathtt{T}} = H_4H_4 = 2I_4$, and h_4 is an affine signature. The following is called an H_4 gadget construction on f, denoted by ${}^{H_4}_{ij}f$. This is the signature obtained by connecting variables x_3 and x_4 of h_4 with variables x_i and x_j of f using $=_2$, respectively. Note that ${}^{H_4}_{ij}f$ is not necessarily realizable from f since h_4 may not be available. However, we will analyze the structure of f by analyzing ${}^{H_4}_{ij}f$. For convenience, we consider $(i,j)=(1,2)$ and we use $\widetilde{f}$ to denote ${}^{H_4}_{12}f$. The following results (Lemmas 7.23 and 7.24) about $\widetilde{f}={}^{H_4}_{12}f$ hold for all ${}^{H_4}_{ij}f$ by replacing $\{1,2\}$ with $\{i,j\}$. Note that $\widetilde{f}$ has the following signature matrix

$$M_{12}(\widetilde{f})=\begin{bmatrix}\widetilde{\mathbf{f}}^{00}_{12}\\ \widetilde{\mathbf{f}}^{01}_{12}\\ \widetilde{\mathbf{f}}^{10}_{12}\\ \widetilde{\mathbf{f}}^{11}_{12}\end{bmatrix}=H_4M_{12}(f)=\begin{bmatrix}\mathbf{f}^{00}_{12}+\mathbf{f}^{11}_{12}\\ \mathbf{f}^{01}_{12}+\mathbf{f}^{10}_{12}\\ \mathbf{f}^{01}_{12}-\mathbf{f}^{10}_{12}\\ \mathbf{f}^{00}_{12}-\mathbf{f}^{11}_{12}\end{bmatrix}=\begin{bmatrix}\partial^{+}_{12}\mathbf{f}\\ \partial^{\widehat{+}}_{12}\mathbf{f}\\ \partial^{\widehat{-}}_{12}\mathbf{f}\\ \partial^{-}_{12}\mathbf{f}\end{bmatrix}.$$

We give the following relations between f and $\widetilde{f}$.

Lemma 7.23. *1. If f has even parity then $\widetilde{f}$ also has even parity.*

2. If $f\in\mathscr{A}$, then $\widetilde{f}\in\mathscr{A}$.

3. If $M(\mathfrak{m}_{12}f)=\lambda I_4$ for some real $\lambda\neq 0$, then $M(\mathfrak{m}_{12}\widetilde{f})=2\lambda I_4$.

4. If $\partial^{+}_{12}f,\partial^{-}_{12}f,\partial^{\widehat{+}}_{12}f,\partial^{\widehat{-}}_{12}f\in\mathscr{A}$, then $\widetilde{f}^{00}_{12}$, $\widetilde{f}^{01}_{12}$, $\widetilde{f}^{10}_{12}$, $\widetilde{f}^{11}_{12}\in\mathscr{A}$.

5. For $\{u,v\}$ disjoint with $\{1,2\}$ and $b\in\mathcal{B}$, if $\partial^{b}_{uv}f\in\mathscr{A}$, then $\partial^{b}_{uv}\widetilde{f}\in\mathscr{A}$.

证明. Since h_4 has even parity and $h_4\in\mathscr{A}$, the first and second propositions hold.

If $M(\mathfrak{m}_{12}f)=\lambda I_4$, then $M(\mathfrak{m}_{12}\widetilde{f})=M_{12}(\widetilde{f})M^{\mathtt{T}}_{12}(\widetilde{f})=H_4M_{12}(f)M^{\mathtt{T}}_{12}(f)H^{\mathtt{T}}_4=\lambda H_4I_4H^{\mathtt{T}}_4=2\lambda I_4$. The third proposition holds.

By the matrix form $M_{12}(\widetilde{f})$, the fourth proposition holds.

Since the H_4 gadget construction only touches variables x_1 and x_2 of f, it commutes with merging gadgets on variables other than x_1 and x_2. Thus $\partial^{b}_{ij}\widetilde{f}=\widetilde{\partial^{b}_{ij}f}$. For all $b\in\mathcal{B}$ and all $\{i,j\}$ disjoint with $\{1,2\}$, if $\partial^{b}_{ij}f\in\mathscr{A}$ where $\partial^{b}_{ij}f$ are signatures realized by connecting variables x_i and x_j of f using b, then $\partial^{b}_{ij}\widetilde{f}=\widetilde{\partial^{b}_{ij}f}\in\mathscr{A}$. The last proposition holds. □

Clearly, if $f\in\int_{\mathcal{B}}\mathscr{A}$, then $\widetilde{f}^{00}_{12}$, $\widetilde{f}^{01}_{12}$, $\widetilde{f}^{10}_{12}$, $\widetilde{f}^{11}_{12}\in\mathscr{A}$. Thus, for every $(a,b)\in\mathbb{Z}^2_2$, if $\widetilde{f}^{ab}_{12}\not\equiv 0$, then its nonzero entries have the same norm, denoted by n_{ab}. Let $n_{ab}=0$ if $\widetilde{f}^{ab}_{12}\equiv 0$. We have the following results regarding these norms n_{ab}.

Lemma 7.24. *Let f be an irreducible signature of arity $2n \geqslant 6$. Suppose that f has even parity, f satisfies* 2nd-Orth *and $f \in \int_{\mathcal{B}} \mathscr{A}$.*

1. *For any $(a, b), (c, d) \in \mathbb{Z}_2^2$, there exists some $k \in \mathbb{Z}$ such that $n_{ab} = \sqrt{2}^k n_{cd} \neq 0$, and $n_{ab} = n_{cd}$ iff $|\mathscr{S}(\widetilde{f}_{12}^{ab})| = |\mathscr{S}(\widetilde{f}_{12}^{cd})|$.*

2. *Furthermore, if $\widetilde{f}_{12}^{00}(\vec{0}^{2n-2}) \neq 0$ and $n_{00} > n_{11}$, then $\mathscr{S}(\widetilde{f}_{12}^{11}) = \mathscr{E}_{2n-2}$[*] and $n_{ab} = n_{11}$ or $2n_{11}$ for every $(a, b) \in \mathbb{Z}_2^2$; in particular, $n_{00} = 2n_{11}$. Symmetrically, if $\widetilde{f}_{12}^{11}(\vec{0}^{2n-2}) \neq 0$ and $n_{00} < n_{11}$, then $\mathscr{S}(\widetilde{f}_{12}^{00}) = \mathscr{E}_{2n-2}$ and $n_{ab} = n_{00}$ or $2n_{00}$ for every $(a, b) \in \mathbb{Z}_2^2$, and $n_{11} = 2n_{00}$.*

证明. Since f satisfies 2nd-Orth, $M(\mathfrak{m}_{12} f) = \lambda I_4$ for some real $\lambda \neq 0$. Then, by Lemma 7.23, $M(\mathfrak{m}_{12} \widetilde{f}) = 2\lambda I_4 \neq 0$. Thus, $|\widetilde{f}_{12}^{ab}|^2 = 2\lambda \neq 0$ for every $(a, b) \in \mathbb{Z}_2^2$. Also, since $f \in \int_{\mathcal{B}} \mathscr{A}$, by Lemma 7.23, for every $(a, b) \in \mathbb{Z}_2^2$, $\widetilde{f}_{12}^{ab} \in \mathscr{A}$. Thus, $\mathscr{S}(\widetilde{f}_{12}^{ab})$ is affine and $|\mathscr{S}(\widetilde{f}_{12}^{ab})| = 2^{k_{ab}}$ for some integer $k_{ab} \geqslant 0$. Note that

$$|\widetilde{f}_{12}^{ab}|^2 = n_{ab}^2 \cdot |\mathscr{S}(\widetilde{f}_{12}^{ab})| = n_{ab}^2 \cdot 2^{k_{ab}} \neq 0.$$

Thus, for any $(a, b), (c, d) \in \mathbb{Z}_2^2$, $n_{ab}^2 \cdot 2^{k_{ab}} = n_{cd}^2 \cdot 2^{k_{cd}} \neq 0$. Then, $n_{ab} = \sqrt{2}^k n_{cd} \neq 0$ where $k = k_{cd} - k_{ab} \in \mathbb{Z}$. Clearly, $k = 0$ iff $|\mathscr{S}(\widetilde{f}_{12}^{ab})| = 2^{k_{ab}} = 2^{k_{cd}} = |\mathscr{S}(\widetilde{f}_{12}^{cd})|$.

Now we prove the second part of this lemma. We give the proof for the case that $\widetilde{f}_{12}^{00}(\vec{0}^{2n-2}) \neq 0$ and $n_{00} > n_{11}$. The proof of the case that $\widetilde{f}_{12}^{11}(\vec{0}^{2n-2}) \neq 0$ and $n_{00} < n_{11}$ is symmetric. We first show that $\mathscr{S}(\widetilde{f}_{12}^{11}) = \mathscr{E}_{2n-2}$. For a contradiction, suppose that $\mathscr{S}(\widetilde{f}_{12}^{11}) \neq \mathscr{E}_{2n-2}$. Since f has even parity, by Lemma 7.23, $\widetilde{f}$ has even parity. Then, $\widetilde{f}_{12}^{11}$ also has even parity. Thus, $\mathscr{S}(\widetilde{f}_{12}^{11}) \subsetneq \mathscr{E}_{2n-2}$. There exists $\theta \in \mathscr{E}_{2n-2}$ such that $\theta \notin \mathscr{S}(\widetilde{f}_{12}^{11})$. Also, since $n_{11} \neq 0$, $\widetilde{f}_{12}^{11} \not\equiv 0$. Then, $\mathscr{S}(\widetilde{f}_{12}^{11}) \neq \emptyset$ and there exists $\delta \in \mathscr{E}_{2n-2}$ such that $\delta \in \mathscr{S}(\widetilde{f}_{12}^{11})$. Then, we can find a pair $\alpha, \beta \in \mathscr{E}_{2n-2}$ where $\text{wt}(\alpha \oplus \beta) = 2$ such that one is in $\mathscr{S}(\widetilde{f}_{12}^{11})$ and the other one is not in $\mathscr{S}(\widetilde{f}_{12}^{11})$.

- If $\text{wt}(\alpha) \neq \text{wt}(\beta)$, then clearly the difference between their Hamming weights is 2 since $\text{wt}(\alpha \oplus \beta) = 2$. Thus, α and β differ in two bits i, j on which one takes value 00 and the other takes value 11.

[*] Here, $\mathscr{E}_{2n-2} = \{(x_3, \ldots, x_8) \in \mathbb{Z}_2^6 \mid x_3 + \cdots + x_8 = 0\}$. When context is clear, we do not specify the variables of $\mathscr{E}_{2n-2}$ and also $\mathscr{O}_{2n-2}$.

- If $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$, then they differ in two bits i, j on which one takes value 01 and the other takes value 10. Without loss of generality, we assume that $\alpha_i\alpha_j = 01$ and $\beta_i\beta_j = 10$. They take the same value on other bits. Since $\alpha, \beta \in \mathscr{E}_{2n-2}$ and $2n \geqslant 6$, they have even Hamming weight and length at least 4. Thus, there is another bit k such that on this bit, $\alpha_k = \beta_k = 1$. Consider $\gamma \in \mathscr{E}_{2n-2}$ where $\gamma_i\gamma_j\gamma_k = 000$ and γ takes the same value as α and β on other bits. Clearly, $\mathrm{wt}(\gamma) + 2 = \mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$. If $\gamma \in \mathscr{S}(\widetilde{f}_{12}^{11})$, then between α and β, we pick the one that is not in $\mathscr{S}(\widetilde{f}_{12}^{11})$. Otherwise, we pick the one that is in $\mathscr{S}(\widetilde{f}_{12}^{11})$. In both cases, we can get a pair of inputs in $\mathscr{E}_{2n-2}$ such that one is in $\mathscr{S}(\widetilde{f}_{12}^{11})$ and the other is not in $\mathscr{S}(\widetilde{f}_{12}^{11})$, and they have Hamming distance 2 as well as different Hamming weights.

Thus, we can always find a pair $\alpha, \beta \in \mathscr{E}_{2n-2}$ where $\mathrm{wt}(\alpha \oplus \beta) = 2$ and α, β differ in two bits i, j on which one takes value 00 and the other takes value 11, such that one is in $\mathscr{S}(\widetilde{f}_{12}^{11})$ and the other is not in $\mathscr{S}(\widetilde{f}_{12}^{11})$. Clearly, $\{i, j\}$ is disjoint with $\{1, 2\}$.

Consider signatures $\partial_{ij}^{+}\widetilde{f}$ and $\partial_{ij}^{-}\widetilde{f}$. Then, $\widetilde{f}(11\alpha) + \widetilde{f}(11\beta)$ is an entry of $\partial_{ij}^{+}\widetilde{f}$, and $\widetilde{f}(11\alpha) - \widetilde{f}(11\beta)$ is an entry of $\partial_{ij}^{-}\widetilde{f}$. Since between $\widetilde{f}(11\alpha)$ and $\widetilde{f}(11\beta)$, exactly one is nonzero and it has norm n_{11}, we have

$$|\widetilde{f}(11\alpha) + \widetilde{f}(11\beta)| = |\widetilde{f}(11\alpha) - \widetilde{f}(11\beta)| = n_{11}.$$

Thus, both $\partial_{ij}^{+}\widetilde{f}$ and $\partial_{ij}^{-}\widetilde{f}$ have an entry with norm n_{11}. Let $\delta \in \mathscr{E}_{2n}$ where $\delta_i\delta_j = 11$ and δ takes value 0 on other bits. Then, clearly, $\widetilde{f}(\vec{0}^{2n}) + \widetilde{f}(\delta)$ is an entry of $\partial_{ij}^{+}\widetilde{f}$, and $\widetilde{f}(\vec{0}^{2n}) - \widetilde{f}(\delta)$ is an entry of $\partial_{ij}^{-}\widetilde{f}$.

- If $\widetilde{f}(\delta) \neq 0$, then $|\widetilde{f}(\delta)| = n_{00}$ since $\delta_1\delta_2 = 00$. Since $\widetilde{f}(\vec{0}^{2n}) \neq 0$, $|\widetilde{f}(\vec{0}^{2n})| = n_{00}$. Thus, between $\widetilde{f}(\vec{0}^{2n}) + \widetilde{f}(\delta)$ and $\widetilde{f}(\vec{0}^{2n}) - \widetilde{f}(\delta)$, one has norm $2n_{00}$ and the other is zero. Therefore, between $\partial_{ij}^{+}\widetilde{f}$ and $\partial_{ij}^{-}\widetilde{f}$, one signature has an entry with norm $2n_{00}$. Remember that both $\partial_{ij}^{+}\widetilde{f}$ and $\partial_{ij}^{-}\widetilde{f}$ have an entry with norm n_{11}. Clearly, $2n_{00} > n_{11}$. Thus, between $\partial_{ij}^{+}\widetilde{f}$ and $\partial_{ij}^{-}\widetilde{f}$, there is a signature that has two entries with different norms. Clearly, such a signature is not in $\mathscr{A}$. However, since $f \in \int_{\mathcal{B}} \mathscr{A}$, by Lemma 7.23, $\partial_{ij}^{+}\widetilde{f}, \partial_{ij}^{-}\widetilde{f} \in \mathscr{A}$. Contradiction.

- If $\widetilde{f}(\delta) = 0$, then $|\widetilde{f}(\vec{0}^{2n}) + \widetilde{f}(\delta)| = |\widetilde{f}(\vec{0}^{2n})| = n_{00} > n_{11}$. Thus, $\partial_{ij}^{+}\widetilde{f}$ has two nonzero entries with different norms n_{00} and n_{11}. Then, $\partial_{ij}^{+}\widetilde{f} \notin \mathscr{A}$. Contradiction.

Thus, $\mathscr{S}(\widetilde{f}_{12}^{11}) = \mathscr{E}_{2n-2}$.

Then, we show that $n_{ab} = n_{11}$ or $2n_{11}$ for any $(a, b) \in \mathbb{Z}_2^2$. Clearly, we may assume that $(a, b) \neq (1, 1)$. For a contradiction, suppose that $n_{ab} \neq n_{11}$ and $2n_{11}$. First, we show that $|\mathscr{S}(\widetilde{f}^{ab}_{12})| < 2^{2n-3}$ and $n_{ab} > n_{11}$. Since f has parity, $\widetilde{f}^{ab}_{12}$ also has parity (either even or odd depending on whether $\text{wt}(ab) = 0$ or 1). Thus $|\mathscr{S}(\widetilde{f}^{ab}_{12})| \leqslant |\mathscr{E}_{2n-2}| = |\mathscr{O}_{2n-2}| = 2^{2n-3}$. If the equality holds, then $n_{ab} = n_{11}$ since $n^2_{ab}|\mathscr{S}(\widetilde{f}^{ab}_{12})| = n^2_{11}|\mathscr{S}(\widetilde{f}^{11}_{12})|$ and $|\mathscr{S}(\widetilde{f}^{11}_{12})| = 2^{2n-3}$. Contradiction. Thus, $|\mathscr{S}(\widetilde{f}^{ab}_{12})| < 2^{2n-3}$ and also $n_{ab} > n_{11}$.

Depending on whether f^{ab}_{12} has even parity or odd parity, we can pick a pair of inputs α, β with $\text{wt}(\alpha \oplus \beta) = 2$ from $\mathscr{E}_{2n-2}$ or $\mathscr{O}_{2n-2}$ such that exactly one is in $\mathscr{S}(f^{ab}_{12})$ and the other is not in $\mathscr{S}(f^{ab}_{12})$. Suppose that α and β differ in bits i, j. Depending on whether $\alpha_i = \alpha_j$ or $\alpha_i \neq \alpha_j$, we can connect variables x_i and x_j of $\widetilde{f}$ using $=_2^+$ and $=_2^-$, or $\neq_2^+$ and $\neq_2^-$. We will get two signatures $\partial^+_{ij}\widetilde{f}$ and $\partial^-_{ij}\widetilde{f}$, or $\partial^{\widehat{+}}_{ij}\widetilde{f}$ and $\partial^{\widehat{-}}_{ij}\widetilde{f}$. We consider the case that $\alpha_i = \alpha_j$. For the case that $\alpha_i \neq \alpha_j$, the analysis is the same by replacing $\partial^+_{ij}\widetilde{f}$ and $\partial^-_{ij}\widetilde{f}$ with $\partial^{\widehat{+}}_{ij}\widetilde{f}$ and $\partial^{\widehat{-}}_{ij}\widetilde{f}$ respectively.

Consider signatures $\partial^+_{ij}\widetilde{f}$ and $\partial^-_{ij}\widetilde{f}$. Then, $\widetilde{f}(ab\alpha) + \widetilde{f}(ab\beta)$ is an entry of $\partial^+_{ij}\widetilde{f}$, and $\widetilde{f}(ab\alpha) - \widetilde{f}(ab\beta)$ is an entry of $\partial^-_{ij}\widetilde{f}$. Since between α and β, exactly one is in $\mathscr{S}(f^{ab}_{12})$, between $\widetilde{f}(ab\alpha)$ and $\widetilde{f}(ab\beta)$, exactly one is nonzero and it has norm n_{ab}. Thus,

$$|\widetilde{f}(ab\alpha) + \widetilde{f}(ab\beta)| = |\widetilde{f}(ab\alpha) - \widetilde{f}(ab\beta)| = n_{ab}.$$

Both $\partial^+_{ij}\widetilde{f}$ and $\partial^-_{ij}\widetilde{f}$ have an entry with norm n_{ab}.

Let $\alpha', \beta' \in \mathscr{E}_{2n-2}$ where $\alpha'_i\alpha'_j = \alpha_i\alpha_j$, $\alpha'_k = \alpha'_i \oplus \alpha'_j$ for some $k \neq i, j$[*] and α' takes value 0 on other bits, and $\beta'_i\beta'_j = \beta_i\beta_j$, $\beta'_k = \beta'_i \oplus \beta'_j$ for the same $k \neq i, j$ and β' takes value 0 on other bits. Clearly, α' and β' differ in bits i and j and they differ in the same way as α and β. Then, $\widetilde{f}(11\alpha') + \widetilde{f}(11\beta')$ is an entry of $\partial^+_{ij}\widetilde{f}$, and $\widetilde{f}(11\alpha') - \widetilde{f}(11\beta')$ is an entry of $\partial^-_{ij}\widetilde{f}$. Since $\mathscr{S}(\widetilde{f}^{11}_{12}) = \mathscr{E}_{2n-2}$, both $\widetilde{f}(11\alpha')$ and $\widetilde{f}(11\beta')$ are nonzero and they have norm n_{11}. Thus, between $\widetilde{f}(11\alpha') + \widetilde{f}(11\beta')$ and $\widetilde{f}(11\alpha') - \widetilde{f}(11\beta')$, exactly one is zero and the other has norm $2n_{11}$. Thus, between signatures $\partial_{ij}\widetilde{f}$ and $\partial^-_{ij}\widetilde{f}$, there is a signature that has two entries with different norms $2n_{11}$ and n_{ab}. Such a signature is not in $\mathscr{A}$. However, since $f \in \int_{\mathcal{B}}\mathscr{A}$, by Lemma 7.23, $\partial_{ij}\widetilde{f}, \partial^-_{ij}\widetilde{f} \in \mathscr{A}$. Contradiction. Thus, $n_{ab} = n_{11}$ or $2n_{11}$ for any $(a, b) \in \mathbb{Z}_2^2$. □

[*] Since $2n - 2 \geqslant 4$, such a k exists. Here, $\alpha'_k = 0$ since $\alpha_i = \alpha_j$ in this case under discussion. For the case that $\alpha_i \neq \alpha_j$, we have $\alpha'_k = 1$.

We also give the following results about multilinear polynomials $F(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$. We use $d(F)$ to denote the total degree of F. For $\{i, j\} \subseteq \{1, \ldots, n\} = [n]$, we use $F_{ij}^{ab} \in Z_2[\{x_1, \ldots, x_n\} \backslash \{x_i, x_j\}]$ to denote the polynomial obtained by setting $(x_i, x_j) = (a, b)$ in F.

Definition 7.25. *Let $F(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$ be a multilinear polynomial. We say F is a complete quadratic polynomial if $d(F) = 2$ and for all $\{i, j\} \subseteq [n]$, the quadratic term $x_i x_j$ appears in F. We say F is a complete cubic polynomial if $d(F) = 3$ and for all $\{i, j, k\} \subseteq [n]$, the cubic term $x_i x_j x_k$ appears in F.*

Lemma 7.26. *Let $F(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$ be a multilinear polynomial.*

1. *If for all $\{i, j\} \subseteq [n]$, $F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1, and $F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1, then $d(F) \leqslant 2$. Moreover, if $d(F) = 2$, then F is a complete quadratic polynomial.*

2. *If for all $\{i, j\} \subseteq [n]$, $d(F_{ij}^{00} + F_{ij}^{11}) \leqslant 1$, and $d(F_{ij}^{01} + F_{ij}^{10}) \leqslant 1$, then $d(F) \leqslant 3$. Moreover, if $d(F) = 3$, then F is a complete cubic polynomial.*

证明. We prove the first part. The proof for the second part is similar which we omit here.

For all $\{i, j\} \subseteq [n]$, we write $F \in \mathbb{Z}_2[x_1, \ldots, x_n]$ as a polynomial of variables x_i and x_j.

$$F = X_{ij} x_i x_j + Y_{ij} x_i + Z_{ij} x_j + W_{ij}$$

where $X_{ij}, Y_{ij}, Z_{ij}, W_{ij} \in \mathbb{Z}_2[\{x_3, \ldots, x_n\} \backslash \{x_i, x_j\}]$. Then,

$$F_{ij}^{00} = W_{ij} \quad \text{and} \quad F_{ij}^{11} = X_{ij} + Y_{ij} + Z_{ij} + W_{ij}.$$

Thus, $X_{ij} + Y_{ij} + Z_{ij} = F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1. Also,

$$F_{ij}^{01} = Z_{ij} + W_{ij} \quad \text{and} \quad F_{ij}^{10} = Y_{ij} + W_{ij}.$$

Thus, $Y_{ij} + Z_{ij} = F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1. Then, $X_{ij} \equiv 0$ or 1 for all $\{i, j\}$. Thus, $d(F) \leqslant 2$.

Suppose that $d(F) = 2$. then F has at least a quadratic term $x_u x_v$ $(u \neq v)$. Without loss of generality, we assume that the term $x_1 x_2$ appears in F. We first show that for all $2 \leqslant j \leqslant n$, the quadratic term $x_1 x_j$ appears in F. Since $x_1 x_2$ is already in F, we may assume that $3 \leqslant j$. We write F as a polynomial of variables x_2 and x_j.

$$F = X_{2j}x_2x_j + Y_{2j}x_2 + Z_{2j}x_j + W_{2j},$$

where $X_{2j}, Y_{2j}, Z_{2j}, W_{2j}$ do not involve x_2 and x_j. Since x_1x_2 appears in F, x_1 appears in Y_{2j}. As we have proved above, $Y_{2j} + Z_{2j} \equiv 0$ or 1. Thus, x_1 also appears in Z_{2j}, which means that x_1x_j appears in F. Then, for all $2 \leqslant j \leqslant n$, x_1x_j appears in F.

Then, for all $2 \leqslant i < j \leqslant n$, we write F as a polynomial of variables x_1 and x_i.

$$F = X_{1i}x_1x_i + Y_{1i}x_1 + Z_{1i}x_i + W_{1i},$$

where $X_{1i}, Y_{1i}, Z_{1i}, W_{1i}$ do not involve x_1 and x_i. Since x_1x_j appears in F, x_j appears in Y_{1i}. Since $Y_{1i} + Z_{1i} \equiv 0$ or 1, x_j also appears in Z_{1i}. Thus, x_ix_j appears in F. Then, for all $2 \leqslant i < j \leqslant n$, the quadratic term x_ix_j appears in F. Thus, for all $\{i, j\} \subseteq [n]$, x_ix_j appears in F. □

Now, we are ready to take a major step towards Theorem 7.38.

Lemma 7.27. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T). *If $\mathcal{F}$ contains an irreducible $2n$-ary signature f with parity where $2n \geqslant 8$, then*

- $\text{Holant}^b(\mathcal{F})$ *is #P-hard, or*
- *there is a signature $g \notin \mathscr{A}$ of arity $2k < 2n$ that is realizable from f and $\mathcal{B}$, or*
- *after normalization, $f(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(f)$.*

证明. Since f is irreducible, we may assume that it satisfies 2nd-Orth. Otherwise, we get #P-hardness by Lemma 6.6. Also, we may assume that $f \in \int_{\mathcal{B}} \mathscr{A}$. Otherwise, we can realize a signature of arity $2n - 2$ that is not in $\mathscr{A}$ by merging f using some $b \in \mathcal{B}$.

For any four entries x, y, z, w of f on inputs $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2^{2n}$ written in the form of a 2-by-2 matrix $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right] = \begin{bmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{bmatrix}$, we say that such a matrix is a *distance-2 square* if there exist four bits i, j, k, ℓ such that $\alpha_i\alpha_j = \beta_i\beta_j = \overline{\gamma_i\gamma_j} = \overline{\delta_i\delta_j}$, $\alpha_k\alpha_\ell = \gamma_k\gamma_\ell = \overline{\beta_k\beta_\ell} = \overline{\delta_k\delta_\ell}$ and α, β, γ and δ take the same values on other bits. An equivalent description is that

$$\delta = \alpha \oplus \beta \oplus \gamma, \quad \text{wt}(\alpha \oplus \beta) = 2, \quad \text{wt}(\alpha \oplus \gamma) = 2 \quad \text{and} \quad \text{wt}(\alpha \oplus \delta) = 4. \tag{7.12}$$

Indeed (7.12) is clearly satisfied by any distance-2 square. Conversely, suppose (7.12) holds. If we flip any bit i in all α, β, γ and δ, both (7.12) and the bitwise description are invariant, and thus we may assume $\alpha = \vec{0}^{2n}$. By $\text{wt}(\alpha \oplus \gamma) = 2$, there exist two bits i, j such that $\gamma_i\gamma_j = 11$, and γ takes 0 on other bits. By $\text{wt}(\alpha \oplus \beta) = 2$, there exits two bits k, ℓ such that $\beta_k\beta_\ell = 11$, and β takes 0 on other bits. Since $\delta = \alpha \oplus \beta \oplus \gamma$, $\text{wt}(\beta \oplus \gamma) = \text{wt}(\alpha \oplus \delta) = 4$. Thus, the bits i, j, k, ℓ are distinct four bits. Then, $\delta_i\delta_j\delta_k\delta_\ell = 1111$ and δ takes 0 on other bits. Thus, α, β, γ and δ satisfy the bitwise description of distance-2 squares.

We give an example of such a distance-2 square. Let

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{bmatrix} = \begin{bmatrix} f(00010\theta) & f(00100\theta) \\ f(11010\theta) & f(11100\theta) \end{bmatrix}$$

where $\theta \in \mathbb{Z}_2^{2n-4}$ is an arbitrary binary string of length $2n-4$. In this example, $(i, j) = (1, 2)$ and $(k, \ell) = (3, 4)$. We show next that such a distance-2 square $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ has the property described in (7.13) $\sim$ (7.16).

By connecting variables x_1 and x_2 of f using $=_2^+$ and $=_2^-$ respectively, we get signatures $\partial_{12}^+ f$ and $\partial_{12}^- f$. By our assumption, $\partial_{12}^+ f$ and $\partial_{12}^- f$ are affine signatures. Note that, $x + z$ and $y + w$ are entries of $\partial_{12}^+ f$ on inputs 01θ and $10\theta \in \mathbb{Z}_2^{2n-2}$. Since $\partial_{12}^+ f \in \mathscr{A}$, if $x+z$ and $y+w$ are both nonzero, then they have the same norm. Thus, we have $(x+z)(y+w) = 0$ or $(x+z)^2 = (y+w)^2$. Similarly, $x - z$ and $y - w$ are entries of $\partial_{12}^- f \in \mathscr{A}$. Thus, we have $(x-z)(y-w) = 0$ or $(x-z)^2 = (y-w)^2$.

Also, by connecting variables x_3 and x_4 of f using $\neq_2$ and $\neq_2^-$ respectively, we get signatures $\partial_{34}^{\widehat{+}} f$ and $\partial_{34}^{\widehat{-}} f$ that are affine signatures. Note that, $x + y$ and $z + w$ are entries of $\partial_{34}^{\widehat{+}} f$ on inputs 00θ and 11θ. Since $\partial_{34}^{\widehat{+}} f \in \mathscr{A}$, we have $(x+y)(z+w) = 0$ or $(x+y)^2 = (z+w)^2$. Similarly, $x - y$ and $z - w$ are entries of $\widehat{\partial}_{34}^{-} f$. Then, we have $(x-y)(z-w) = 0$ or $(x-y)^2 = (z-w)^2$.

Now, consider an arbitrary distance-2 square $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right] = \left[\begin{smallmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{smallmatrix}\right]$. Depending on whether $\alpha_i = \alpha_j$ or $\alpha_i \neq \alpha_j$, we can use $=_2^+$ and $=_2^-$, or $\neq_2^+$ and $\neq_2^-$ respectively, to connect variables x_i and x_j of f to produce two signatures $\partial_{ij}^+ f$ and $\partial_{ij}^- f$, or $\partial_{ij}^{\widehat{+}} f$ and $\partial_{ij}^{\widehat{-}} f$ in either case, such that $x \pm z$ and $y \pm w$ are both entries of the resulting two signatures. Since the two resulting signatures are in affine, we have

$$(x+z)(y+w) = 0 \quad \text{or} \quad (x+z)^2 = (y+w)^2, \tag{7.13}$$

and

$$(x-z)(y-w)=0 \quad \text{or} \quad (x-z)^2=(y-w)^2. \tag{7.14}$$

Similarly, by connecting variables x_k and x_ℓ of f using either $=_2^{\pm}$ or $\neq_2^{\pm}$, we have

$$(x+y)(z+w)=0 \quad \text{or} \quad (x+y)^2=(z+w)^2 \tag{7.15}$$

and

$$(x-y)(z-w)=0 \quad \text{or} \quad (x-y)^2=(z-w)^2. \tag{7.16}$$

Now, we show that by solving equations (7.13) $\sim$ (7.16), every distance-2 square has one of the following forms (after normalization, row or column permutation, multiplying a -1 scalar of one row or one column, and taking transpose)

$$\underbrace{\begin{bmatrix}0&0\\0&0\end{bmatrix}, \begin{bmatrix}1&0\\0&0\end{bmatrix}, \begin{bmatrix}1&1\\0&0\end{bmatrix}, \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\1&1\end{bmatrix}, \begin{bmatrix}1&1\\1&-1\end{bmatrix},}_{\text{type I}} \quad \underbrace{\begin{bmatrix}1&a\\a&1\end{bmatrix}(a>1),}_{\text{type II}} \quad \text{or} \quad \underbrace{\begin{bmatrix}1&1\\3&-1\end{bmatrix}}_{\text{type III}}.$$

We say that the first six forms are type I, and the other two are type II and type III respectively. These forms listed above are canonical forms of each type.

Let $\left[\begin{smallmatrix}x&y\\z&w\end{smallmatrix}\right]$ be a distance-2 square. Consider

$$p=(x+y)(z+w)(x+z)(y+w)(x-y)(z-w)(x-z)(y-w).$$

- If $p=0$, then among its eight factors (four sums and four differences), at least one factor is zero. By taking transpose and row permutation, we may assume that $x+y=0$ or $x-y=0$. If $x+y=0$, then by multiplying the column $\left[\begin{smallmatrix}y\\w\end{smallmatrix}\right]$ with -1, we can modify this distance-2 square to get $x-y=0$. Thus, we may assume that $x-y=0$. If $x=y=0$, then by (7.13), we have $z=0$ or $w=0$, or $z=\pm w$. Thus, after normalizing operations of row and column permutation and multiplication by -1, we reach the following canonical forms $\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right]$ or $\left[\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right]$. Otherwise, $x=y\neq 0$. Consider $q=(x+z)(y+w)(x-z)(y-w)$.
    - If $q=0$, then among its four factors (two sums and two differences), at least one is zero.

By column permutation on the matrix $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ and multiplying the row (z, w) with -1 (which does not change the values of x and y), we may assume that $x - z = 0$. Thus, $x = y = z \neq 0$. We normalize their values to 1. Then by (7.13), $1 + w = 0$ or $1 + w = \pm 2$. Thus, $w = -1, 1$ or -3. If $w = \pm 1$, then $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ has the canonical form $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$. If $w = -3$, then $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -3 \end{smallmatrix}\right]$ which has the canonical form $\left[\begin{smallmatrix} 1 & 1 \\ 3 & -1 \end{smallmatrix}\right]$ (Type III).

- If $q \neq 0$, then $(x + z)(y + w) \neq 0$ and $(x - z)(y - w) \neq 0$. By equations (7.13) and (7.14), $(x + z)^2 = (y + w)^2$ and $(x - z)^2 = (y - w)^2$. Thus, $xz = yw$. Since $x = y \neq 0$, $z = w$. If $z = w = 0$, then this gives the canonical form $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. Otherwise, $z = w \neq 0$. Then $z + w \neq 0$ and hence by (7.15), $z + w = \pm(x + y)$. Since $z = w$ and $x = y$, we get $z = \pm x$. Thus, $x + z = 0$ or $x - z = 0$. Contradiction.

- If $p \neq 0$, then all its eight factors are nonzero. Thus by (7.13) $\sim$ (7.16), $(x + z)^2 = (y + w)^2$, $(x - z)^2 = (y - w)^2$, $(x + y)^2 = (z + w)^2$ and $(x - y)^2 = (z - w)^2$. By solving these equations, we have $x^2 = w^2$, $y^2 = z^2$, and $xy = zw$. If $x = y = z = w = 0$, then it gives the canonical form $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$. Otherwise, by permuting rows and columns, we may assume that $x \neq 0$ and $|x|$ is the smallest among the norms of nonzero entries in $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$. We normalize x to 1. Since $x^2 = w^2$, we get $w = \pm 1$. By multiplying the row (z, w) with -1 (which does not change $xy = zw$), we may assume that $w = 1$. Then, $xy = zw$ implies that $y = z$. If $y = z = 0$, then $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ has the canonical form $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Otherwise, since $|x| = 1$ is the smallest norm among nonzero entries, $y = z = \pm a$ where $a \geqslant 1$. If $a = 1$ (i.e., $y = z = \pm 1$), then $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ has the canonical form $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. If $a > 1$, then $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ has the canonical form of Type II.

Thus, every distance-2 square has a canonical form of Type I, II or III.

Note that given a particular distance-2 square of f, by normalization, and renaming or flipping or negating variables of f, we can always modify this distance-2 square to get its canonical form. Clearly, for signatures of arity at least 4, distance-2 squares exist. We consider the following two cases according to which types of distance-2 squares appear in f.

Case 1. All distance-2 squares in f are of type I.

We show that (after normalization) $f(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(f)$. Since $f \not\equiv 0$, it has at least one nonzero entry. By normalization, we may assume that 1 is the smallest norm of all nonzero entries of f. Then by flipping variables of f, we may assume that $f(\vec{0}^{2n}) = 1$. For a contradiction, suppose that there is some $\beta \in \mathscr{S}(f)$ such that $f(\beta) \neq \pm 1$. Then by our assumption that 1 is the smallest norm and $|f(\beta)| \neq 1$, we have $|f(\beta)| > 1$. Also, since f has parity and $\vec{0}^{2n} \in \mathscr{S}(f)$, f has even parity. Thus, $\text{wt}(\beta) \equiv 0 \pmod 2$. By renaming variables of f, we may assume that $\beta = \vec{1}^{2m}\vec{0}^{2n-2m}$, for some $m \geqslant 1$. (This does not affect the normalization $f(\vec{0}^{2n}) = 1$). Then, we show that for all $\alpha = \delta\vec{0}^{2n-2m}$ where $\delta \in \mathbb{Z}_2^{2m}$, $f(\alpha) = \pm 1$. We prove this by induction on $\text{wt}(\delta)$. This will lead to a contradiction when $\text{wt}(\delta) = 2m$, since $|f(\beta)| = |f(\vec{1}^{2m}\vec{0}^{2n-2m})| \neq 1$.

Since $f(\vec{0}^{2n}) = 1$, we may assume $\text{wt}(\delta) \geqslant 2$. We first consider the base case that $\text{wt}(\delta) = 2$. By renaming the first $2m$ variables, without loss of generality, we may assume that $\delta = 11\vec{0}^{2m-2}$ and then $\alpha = 11\vec{0}^{2n-2} = 11000\vec{0}^{2n-4}$. This renaming will not change β. Consider the following distance-2 square

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} f(0000\vec{0}^{2n-4}) & f(1100\vec{0}^{2n-4}) \\ f(0011\vec{0}^{2n-4}) & f(1111\vec{0}^{2n-4}) \end{bmatrix}.$$

Recall our assumption that every distance-2 square is of type I. Here $x = f(\vec{0}^{2n})$, and $y = f(\alpha)$. Since $x = 1$, $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ being of type I implies that $y = 0$ or ± 1 (the normalization steps include possibly multiplying a row or a column by -1). We want to show that $|y| = 1$; for a contradiction, suppose that $y = 0$. We consider the following two extra entries of f, where $\overline{\delta} = 00\vec{1}^{2m-2}$.

$$x' = f(\overline{\delta}\vec{0}^{2n-2m}) = f(00\vec{1}^{2m-2}\vec{0}^{2n-2m}) \quad \text{and} \quad y' = f(\beta) = f(11\vec{1}^{2m-2}\vec{0}^{2n-2m}).$$

By connecting variables x_1 and x_2 of f using $=_2$ and $=_2^-$, we get signatures $\partial_{12}f$ and ∂_{12}^-f respectively. Note that both $x + y$ and $x' + y'$ are entries of $\partial_{12}f$. Since $\partial_{12}f \in \mathscr{A}$, we have $(x+y)(x'+y') = 0$ or $(x+y)^2 = (x'+y')^2$. We can also consider ∂_{12}^-f and get $(x-y)(x'-y') = 0$ or $(x-y)^2 = (x'-y')^2$. Since $x = 1$ and $y = 0$, we have

$$\Big[x' + y' = 0 \;\text{ or }\; (x'+y')^2 = 1\Big] \quad \text{and} \quad \Big[x' - y' = 0 \;\text{ or }\; (x'-y')^2 = 1\Big].$$

Recall that $|y'| = |f(\beta)| > 1$. Clearly $x' + y' = 0$ and $x' - y' = 0$ cannot be both true, otherwise $y' = 0$. Suppose one of them is true, then $x' = \pm y'$. And at least one of $(x'+y')^2 = 1$ or $(x'-y')^2 = 1$ holds. So either $|x' + y'| = 1$ or $|x' - y'| = 1$. Substituting $x' = \pm y'$ we reach a contradiction to

$|y'| > 1$. So neither $x' + y' = 0$ nor $x' - y' = 0$ holds. Then $(x' + y')^2 = 1$ and $(x' - y')^2 = 1$. Subtracting them, we get $x'y' = 0$, and since $y' \neq 0$, we get $x' = 0$. But then this contradicts $|y'| > 1$ and $(x' + y')^2 = 1$. Therefore, $y \neq 0$. Then, $y = \pm 1$. Thus, $y = f(\delta\vec{0}^{2n-2m}) = \pm 1$ for all δ with $\mathrm{wt}(\delta) = 2$.

If $2m = 2$, then the induction is finished. Otherwise, $2m > 2$. Inductively for some $2k \geqslant 2$, we assume that $f(\theta\vec{0}^{2n-2m}) = \pm 1$ for all $\theta \in \mathbb{Z}_2^{2m}$ with $\mathrm{wt}(\theta) \leqslant 2k < 2m$. Let δ be such that $\mathrm{wt}(\delta) = 2k + 2 \leqslant 2m$ and we show that $f(\delta\vec{0}^{2n-2m}) = \pm 1$. Since $\mathrm{wt}(\delta) = 2k + 2 \geqslant 4$, we can find four bits of δ such that the values of δ are 1 on these four bits. Without loss of generality, we assume that they are the first four bits, i.e. $\delta = 1111\delta'$ where $\delta' \in \mathbb{Z}_2^{2m-4}$. Consider the following distance-2 square

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} f(0000\delta'\vec{0}^{2n-2m}) & f(0011\delta'\vec{0}^{2n-2m}) \\ f(1100\delta'\vec{0}^{2n-2m}) & f(1111\delta'\vec{0}^{2n-2m}) \end{bmatrix}.$$

Clearly, three entries in this distance-2 square have input strings of weight at most $2k$, namely $\mathrm{wt}(0000\delta'\vec{0}^{2n-2m}) = 2k - 2$, and $\mathrm{wt}(0011\delta'\vec{0}^{2n-2m}) = \mathrm{wt}(1100\delta'\vec{0}^{2n-2m}) = 2k$. By our induction hypothesis, $x, y, z \in \{1, -1\}$. Then, since the distance-2 square $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ is of type I, we have $w = f(\delta\vec{0}^{2n-2m}) = \pm 1$. The induction is complete. This finishes the proof of Case 1.

Case 2. There is a type II or type III distance-2 square in f.

This is the case where signatures g_8 and g_8' appear. We handle this case in two steps.

Step 1. We show that after flipping variables of f, $\mathscr{S}(f) = \mathscr{E}_{2n}$, and after normalization $f(\alpha) = \pm 1$ or ± 3 for all $\alpha \in \mathscr{S}(f)$. Let $\mathscr{S}_3(f) = \{\alpha \in \mathscr{S}(f) \mid f(\alpha) = \pm 3\}$. We also show that $|\mathscr{S}_3(f)| = 2^{2n-4} = \frac{1}{8}|\mathscr{S}(f)|$, and for any distinct $\alpha, \beta \in \mathscr{S}_3(f)$, $\mathrm{wt}(\alpha \oplus \beta) \geqslant 4$.

We first consider the case that there is a Type II distance-2 square in f. We show that the only possible Type II distance-2 square in f has the canonical form $\left[\begin{smallmatrix} 1 & 3 \\ 3 & 1 \end{smallmatrix}\right]$. Suppose that a distance-2 square of Type II appears in f. By flipping and negating variables, we modify f such that this distance-2 square is in its canonical form $\left[\begin{smallmatrix} 1 & a \\ a & 1 \end{smallmatrix}\right]$ $(a > 1)$. Also, by flipping variables and renaming variables, we may assume that this distance-2 square appears on inputs α, β, γ and δ where

$$\begin{bmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{bmatrix} = \begin{bmatrix} f(0000\vec{0}^{2n-4}) & f(0011\vec{0}^{2n-4}) \\ f(1100\vec{0}^{2n-4}) & f(1111\vec{0}^{2n-4}) \end{bmatrix} = \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix}.$$

Then, we consider the entries of $\widetilde{f}$ on inputs α, β, γ and δ. We have

$$\begin{bmatrix} \widetilde{f}(\alpha) & \widetilde{f}(\beta) \\ \widetilde{f}(\gamma) & \widetilde{f}(\delta) \end{bmatrix} = \begin{bmatrix} f(\alpha)+f(\gamma) & f(\beta)+f(\delta) \\ f(\alpha)-f(\gamma) & f(\beta)-f(\delta) \end{bmatrix} = \begin{bmatrix} 1+a & 1+a \\ 1-a & a-1 \end{bmatrix}.$$

Since $a>1$, clearly $1+a\neq 0$, $1-a\neq 0$ and $|1+a|>|1-a|$. Since f has parity and $f(\vec{0}^{2n})=1$, f has even parity. By Lemma 7.24(2), $\mathscr{S}(\widetilde{f}^{11}_{12})=\mathscr{E}_{2n-2}$ and $|1+a|=2|1-a|$. Since $a>1$, we have $1+a=2(a-1)$. Then, $a=3$. Thus, the only possible Type II distance-2 square in f has the canonical form $\left[\begin{smallmatrix}1 & 3\\ 3 & 1\end{smallmatrix}\right]$.

Under the assumption that a Type II distance-2 square appears in f and $\left[\begin{smallmatrix}f(\alpha) & f(\beta)\\ f(\gamma) & f(\delta)\end{smallmatrix}\right]=\left[\begin{smallmatrix}1 & 3\\ 3 & 1\end{smallmatrix}\right]$, we have $\left[\begin{smallmatrix}\widetilde{f}(\alpha) & \widetilde{f}(\beta)\\ \widetilde{f}(\gamma) & \widetilde{f}(\delta)\end{smallmatrix}\right]=\left[\begin{smallmatrix}4 & 4\\ -2 & 2\end{smallmatrix}\right]$. As showed above, by Lemma 7.24(2), $\mathscr{S}(\widetilde{f}^{11}_{12})=\mathscr{E}_{2n-2}$ and $n_{01}, n_{10}=2$ or 4. We first prove

Claim 1. *$\mathscr{S}(f^{00}_{12})=\mathscr{S}(f^{11}_{12})=\mathscr{E}_{2n-2}$, $f^{00}_{12}(\theta), f^{11}_{12}(\theta)=\pm 3$ or ± 1 for all $\theta\in\mathscr{E}_{2n-2}$, and $|\mathscr{S}_3(f^{00}_{12})|+|\mathscr{S}_3(f^{11}_{12})|=2^{2n-5}$.*

Remember that $\widetilde{f}^{00}_{12}, \widetilde{f}^{11}_{12}\in\mathscr{A}$. For any of them, its nonzero entries have the same norm. Since $\widetilde{f}(\alpha)=\widetilde{f}(00\vec{0}^{2n-2})=1+3=4$ and $\mathscr{S}(\widetilde{f}^{00}_{12})\subseteq\mathscr{E}_{2n-2}$, for every $\theta\in\mathscr{E}_{2n-2}$, $\widetilde{f}(00\theta)=\pm 4$ or 0. Also, since $\widetilde{f}(\gamma)=\widetilde{f}(11\vec{0}^{2n-2})=1-3=-2$, and $\mathscr{S}(\widetilde{f}^{11}_{12})=\mathscr{E}_{2n-2}$, for every $\theta\in\mathscr{E}_{2n-2}$, $\widetilde{f}(11\theta)=\pm 2$. Then,

$$f(00\theta)=\frac{\widetilde{f}(00\theta)+\widetilde{f}(11\theta)}{2}=\frac{(\pm 4)+(\pm 2)}{2} \quad \text{or} \quad \frac{0+(\pm 2)}{2}.$$

Thus, $f(00\theta)=\pm 3$ or ± 1 for every $\theta\in\mathscr{E}_{2n-2}$. Also,

$$f(11\theta)=\frac{\widetilde{f}(00\theta)-\widetilde{f}(11\theta)}{2}=\frac{(\pm 4)-(\pm 2)}{2} \quad \text{or} \quad \frac{0-(\pm 2)}{2}.$$

Thus, $f(11\theta)=\pm 3$ or ± 1 for every $\theta\in\mathscr{E}_{2n-2}$. Additionally note that, for any $\theta\in\mathscr{E}_{2n-2}$ if $\widetilde{f}(00\theta)=\pm 4$, then of the two values $f(00\theta)$ and $f(11\theta)$, exactly one is ± 3 and the other one is ± 1; if $\widetilde{f}(00\theta)=0$, then $f(00\theta)=\pm 1$ and $f(11\theta)=\pm 1$. Since

$$|\widetilde{f}^{00}_{12}|^2=4^2\cdot|\mathscr{S}(\widetilde{f}^{00}_{12})|=|\widetilde{f}^{11}_{12}|^2=2^2\cdot|\mathscr{S}(\widetilde{f}^{11}_{12})|=2^2\cdot|\mathscr{E}_{2n-2}|,$$

we have $|\mathscr{S}(\widetilde{f}^{00}_{12})|=|\mathscr{E}_{2n-2}|/4=2^{2n-5}$. Thus, there are exactly 2^{2n-5} entries of $\widetilde{f}^{00}_{12}$ having value

± 4, which give arise to exactly 2^{2n-5} many entries of value ± 3 among all entries of f_{12}^{00} and f_{12}^{11}. Claim 1 has been proved.

Next, we prove

Claim 2. *$\mathscr{S}(f_{12}^{01}) = \mathscr{S}(f_{12}^{10}) = \mathscr{O}_{2n-2}$, $f_{12}^{01}(\theta), f_{12}^{10}(\theta) = \pm 3$ or ± 1 for all $\theta \in \mathscr{O}_{2n-2}$, and $|\mathscr{S}_3(f_{12}^{01})| + |\mathscr{S}_3(f_{12}^{10})| = 2^{2n-5}$.*

We have $\widetilde{f}(\vec{0}^{2n}) = 4$. We have $n_{00} = 4$ and $n_{11} = 2$. Also recall that we have showed that $n_{01}, n_{10} = 2$ or 4, by Lemma 7.24(2). There are three cases.

- $n_{01} = n_{10} = 2$. Since $n_{11} = n_{01} = 2$ and

  $$|\widetilde{f}_{12}^{11}|^2 = n_{11}^2 \cdot |\mathscr{S}(\widetilde{f}_{12}^{11})| = n_{01}^2 \cdot |\mathscr{S}(\widetilde{f}_{12}^{01})| = |\widetilde{f}_{12}^{01}|^2,$$

  we have

  $$|\mathscr{S}(\widetilde{f}_{12}^{01})| = |\mathscr{S}(\widetilde{f}_{12}^{11})| = |\mathscr{E}_{2n-2}| = 2^{2n-3}.$$

  Since $\widetilde{f}$ has even parity, $\mathscr{S}(\widetilde{f}_{12}^{01}) \subseteq \mathscr{O}_{2n-2}$. As $|\mathscr{O}_{2n-2}| = 2^{2n-3}$, we get $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{O}_{2n-2}$. Similarly, we can show that $\mathscr{S}(\widetilde{f}_{12}^{10}) = \mathscr{O}_{2n-2}$. Let $\zeta = 0110\vec{0}^{2n-4}$ and $\eta = 1010\vec{0}^{2n-4}$. Then, $\widetilde{f}(\zeta) = \pm 2$ and $\widetilde{f}(\eta) = \pm 2$. Note that

  $$f(\zeta) = \frac{\widetilde{f}(\zeta) + \widetilde{f}(\eta)}{2} \quad \text{and} \quad f(\eta) = \frac{\widetilde{f}(\zeta) - \widetilde{f}(\eta)}{2}.$$

  If $\widetilde{f}(\zeta) = \widetilde{f}(\eta)$, then $f(\zeta) = \pm 2$ and $f(\eta) = 0$. If $\widetilde{f}(\zeta) = -\widetilde{f}(\eta)$, then $f(\zeta) = 0$ and $f(\eta) = \pm 2$. We first consider the case that $f(\zeta) = \pm 2$. Let $\xi = 1001\vec{0}^{2n-4}$. Consider the following distance-2 square.

  $$\begin{bmatrix} f(\alpha) & f(\zeta) \\ f(\xi) & f(\delta) \end{bmatrix} = \begin{bmatrix} f(0000\vec{0}^{2n-4}) & f(0110\vec{0}^{2n-4}) \\ f(1001\vec{0}^{2n-4}) & f(1111\vec{0}^{2n-4}) \end{bmatrix} = \begin{bmatrix} 1 & \pm 2 \\ * & 1 \end{bmatrix}.$$

  Clearly, it is not of type I nor type III. Also, it is not of type II with the canonical form $\left[\begin{smallmatrix} 1 & 3 \\ 3 & 1 \end{smallmatrix}\right]$. Contradiction. If $f(\eta) = \pm 2$, then similarly by considering the distance-2 square $\left[\begin{smallmatrix} f(\alpha) & f(\eta) \\ f(\tau) & f(\delta) \end{smallmatrix}\right]$ where $\tau = 0101\vec{0}^{2n-4}$, we get a contradiction.

- $n_{01} = n_{10} = 4$. We still consider

$$f(\zeta) = \frac{\widetilde{f}(\zeta) + \widetilde{f}(\eta)}{2} \quad \text{and} \quad f(\eta) = \frac{\widetilde{f}(\zeta) - \widetilde{f}(\eta)}{2}, \quad \text{where } \zeta = 0110\vec{0}^{2n-4} \text{ and } \eta = 1010\vec{0}^{2n-4}.$$

  Then, as ζ has leading bits 01 and η has leading bits 10,

$$f(\zeta) = \frac{(\pm 4) + (\pm 4)}{2}, \frac{(\pm 4) + 0}{2} \text{ or } \frac{0+0}{2} \quad \text{and} \quad f(\eta) = \frac{(\pm 4) - (\pm 4)}{2}, \pm\frac{(\pm 4) - 0}{2} \text{ or } \frac{0-0}{2}.$$

  Thus, $f(\zeta), f(\eta) = \pm 4, \pm 2$ or 0. If $f(\zeta)$ or $f(\eta) = \pm 4, \pm 2$, then by considering the distance-2 square $\left[\begin{smallmatrix} f(\alpha) & f(\zeta) \\ f(\xi) & f(\delta) \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} f(\alpha) & f(\eta) \\ f(\tau) & f(\delta) \end{smallmatrix}\right]$, we still get a contradiction. Thus we have $f(\zeta) = f(\eta) = 0$. Then, consider the signature ${}^{H_4}_{23}f$, denoted by $\widetilde{f'}$. Since f has even parity, f satisfies 2nd-Orth and $f \in \int_{\mathcal{B}} \mathscr{A}$, $\widetilde{f'}$ has even parity, $\widetilde{f'}^{00}_{23}, \widetilde{f'}^{01}_{23}, \widetilde{f'}^{10}_{23}, \widetilde{f'}^{11}_{23} \in \mathscr{A}$. Let $n'_{00}, n'_{01}, n'_{10}$ and n'_{11} denote the norms of nonzero entries in $\widetilde{f'}^{00}_{23}, \widetilde{f'}^{01}_{23}, \widetilde{f'}^{10}_{23}$, and $\widetilde{f'}^{11}_{23}$ respectively. Notice that

$$\widetilde{f'}(\alpha) = \widetilde{f'}(\vec{0}^{2n}) = f(0000\vec{0}^{2n-4}) + f(0110\vec{0}^{2n-4}) = f(\alpha) + f(\zeta) = 1 + 0 = 1.$$

  Thus, $n'_{00} = 1$. Also, notice that

$$\widetilde{f'}(\gamma) = \widetilde{f'}(1100\vec{0}^{2n-4}) = f(1010\vec{0}^{2n-4}) - f(1100\vec{0}^{2n-4}) = f(\eta) - f(\gamma) = 0 - 3 = -3.$$

  Thus, $n'_{10} = 3$. But by Lemma 7.24(1), $n'_{00} = \sqrt{2}^k n'_{10}$ for some $k \in \mathbb{Z}$. However, clearly, $3 \neq \sqrt{2}^k$ for any $k \in \mathbb{Z}$. Contradiction.

- Therefore exactly one of n_{01} and n_{10} is 2 and the other is 4. Let $(a, b) = (0, 1)$ or $(1, 0)$ be such that $n_{ab} = 2$. Since $n_{11} = 2$ and $|\mathscr{S}(\widetilde{f}^{11}_{12})| = |\mathscr{E}_{2n-2}|{=}2^{2n-3}$, we have $|\mathscr{S}(\widetilde{f}^{ab}_{12})| = 2^{2n-3}$. Since $\widetilde{f}$ has even parity, $\widetilde{f}^{ab}_{12}$ has odd parity, thus $\mathscr{S}(\widetilde{f}^{ab}_{12}) = \mathscr{O}_{2n-2}$. Then, similar to the proof of f^{00}_{12} and f^{11}_{12}, we can show that for every $\theta \in \mathscr{O}_{2n-2}$, $f^{01}_{12}(\theta), f^{10}_{12}(\theta) = \pm 3$ or ± 1. Also, among f^{01}_{12} and f^{10}_{12}, exactly 2^{2n-5} many entries are ± 3.

This completes the proof of Claim 2.

Thus, combining Claim 1 and Claim 2, $\mathscr{S}(f) = \mathscr{E}_{2n}$, $f(\alpha) = \pm 1$ or ± 3 for all $\alpha \in \mathscr{S}(f)$, and $|\mathscr{S}_3(f)| = 2^{2n-4} = \frac{1}{8}|\mathscr{S}(f)|$. Also remember that by our assumption, $f(\vec{0}^{2n}) = 1$.

Now, we show that for any distinct $\alpha, \beta \in \mathscr{S}_3(f)$, $\text{wt}(\alpha \oplus \beta) \geqslant 4$. For a contradiction, suppose that $\alpha, \beta \in \mathscr{S}_3(f)$ and $\mathrm{wt}(\alpha \oplus \beta) = 2$, and they differ at bits i and j. By renaming variables, without loss of generality, we may assume that $\{i, j\} = \{1, 2\}$. This renaming does not change the value of $f(\vec{0}^{2n}) = 1$. Since $f(11\vec{0}^{2n-2}) = \pm 1$ or ± 3, of the values $f(00\vec{0}^{2n-2}) + f(11\vec{0}^{2n-2})$ and $f(00\vec{0}^{2n-2}) - f(11\vec{0}^{2n-2})$, which are respectively an entry of $\widetilde{f}_{12}^{00}$ and an entry of $\widetilde{f}_{12}^{11}$, at least one has norm 2. Thus, among n_{00} and n_{11}, at least one is 2. Since $f(\alpha) = \pm 3$ and $f(\beta) = \pm 3$, among $f(\alpha) + f(\beta)$ and $f(\alpha) - f(\beta)$, exactly one has norm 6 and the other has norm 0. Clearly, $f(\alpha) + f(\beta)$ and $f(\alpha) - f(\beta)$ are entries of $\widetilde{f}$ since α and β differ at bits 1 and 2. Thus, among n_{00}, n_{01}, n_{10} and n_{11}, one has norm 6. By Lemma 7.24(1), $2 = \sqrt{2}^k \cdot 6$ for some $k \in \mathbb{N}$. Contradiction. This proves that for any distinct $\alpha, \beta \in \mathscr{S}_3(f)$, $\mathrm{wt}(\alpha \oplus \beta) \geqslant 4$.

We have established the goal laid out in Step 1 of Case 2 under the assumption that there is a Type II distance-2 square in f.

Finally, within Step 1 of Case 2, we consider the case that a type III distance-2 square appears in f. By flipping and negating variables, we modify f such that this distance-2 square is in its canonical form $\left[\begin{smallmatrix} 1 & 3 \\ 1 & -1 \end{smallmatrix}\right]$. Also, by flipping variables and renaming variables, still we may assume that this distance-2 square appears on inputs α, β, γ and δ where

$$\begin{bmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{bmatrix} = \begin{bmatrix} f(0000\vec{0}^{2n-4}) & f(0011\vec{0}^{2n-4}) \\ f(1100\vec{0}^{2n-4}) & f(1111\vec{0}^{2n-4}) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 3 & -1 \end{bmatrix}.$$

Then, we consider the entries of $\widetilde{f}$ on inputs α, β, γ and δ. We have

$$\begin{bmatrix} \widetilde{f}(\alpha) & \widetilde{f}(\beta) \\ \widetilde{f}(\gamma) & \widetilde{f}(\delta) \end{bmatrix} = \begin{bmatrix} f(\alpha) + f(\gamma) & f(\beta) + f(\delta) \\ f(\alpha) - f(\gamma) & f(\beta) - f(\delta) \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ -2 & 2 \end{bmatrix}.$$

Then exactly in the same way as the above proof when $\left[\begin{smallmatrix} \widetilde{f}(\alpha) & \widetilde{f}(\beta) \\ \widetilde{f}(\gamma) & \widetilde{f}(\delta) \end{smallmatrix}\right] = \left[\begin{smallmatrix} 4 & 4 \\ -2 & 2 \end{smallmatrix}\right]$, we can show that the same result holds. Thus, $\mathscr{S}(f) = \mathscr{E}_{2n}$, $f(\alpha) = \pm 1$ or ± 3 for all $\alpha \in \mathscr{S}(f)$, $|\mathscr{S}_3(f)| = 2^{2n-4} = \frac{1}{8}|\mathscr{S}(f)|$, and for any distinct $\alpha, \beta \in \mathscr{S}(f)$ with $\mathrm{wt}(\alpha \oplus \beta) = 2$, α and β cannot be both in $\mathscr{S}_3(f)$.

This finishes the proof of Step 1 of Case 2.

Step 2. Now we show that either g_8 or g'_8 is realizable from f. We will show that they are both irreducible and do not satisfy 2nd-Orth, which gives #P-hardness.

We define a graph G_{2n} with vertex set $\mathscr{E}_{2n}$, and there is an edge between α and β if $\operatorname{wt}(\alpha \oplus \beta) = 2$. I.e., we view every $\alpha \in \mathscr{E}_{2n}$ as a vertex, and the edges are distance 2 neighbors in Hamming distance. Then, $\mathscr{S}_3(f)$ is an independent set of G_{2n}. Remember that $2n \geqslant 8$ by the hypothesis of the lemma. If $2n \geqslant 10$, then by Lemma 7.21, $|\mathscr{S}_3(f)| < \frac{1}{8}|\mathscr{S}(f)|$. Contradiction. Thus, $2n = 8$. After renaming and flipping variables, we may assume that $\mathscr{S}_3(f) = I_8 = \mathscr{S}(f_8)$. For brevity of notation, let $S = \mathscr{E}_8$ and $T = \mathscr{S}(f_8)$. We can pick $(x_1, \ldots, x_7)$ as a set of free variables of $S = \mathscr{E}_8$. Then, there exists a multilinear polynomial $F(x_1, \ldots, x_7) \in \mathbb{Z}_2[x_1, \ldots, x_7]$, and a multilinear polynomial $G(x_1, \ldots, x_8) \in \mathbb{Z}_2[x_1, \ldots, x_8]$ that is viewed as a representative for its image in the quotient algebra $\mathbb{Z}_2[x_1, \ldots, x_8]/(P_1, P_2, P_3, P_4)$ where P_1, P_2, P_3, P_4 are the four linear polynomials in (7.11) such that T is decided by $P_1 = P_2 = P_3 = P_4 = 0$, such that

$$f = \chi_S(-1)^{F(x_1,\ldots,x_7)} + 4\chi_T(-1)^{G(x_1,\ldots,x_8)}.$$

We note that such multilinear polynomials $F(x_1, \ldots, x_7)$ and $G(x_1, \ldots, x_8)$ exist: For any point in $S \setminus T$ we can choose a unique value $s \in \mathbb{Z}_2$ which represents the ± 1 value of f as $(-1)^s$, and for any point in $T \subseteq S$ we can choose unique values $t \in \mathbb{Z}_2$ and $s' \in \mathbb{Z}_2$ such that $(-1)^{s'} + 4(-1)^t$ represents the ± 3 value of f.

For $\{i, j\} \subseteq [7] = \{1, \ldots, 7\}$, remember that $F_{ij}^{ab} \in Z_2[\{x_1, \ldots, x_7\} \backslash \{x_i, x_j\}]$ is the function obtained by setting $(x_i, x_j) = (a, b)$ in F. Similarly, we can define G_{ij}^{ab} with respect to $P_1 = P_2 = P_3 = P_4 = 0$ (any assignment of $(x_i, x_j) = (a, b)$ is consistent with $P_1 = P_2 = P_3 = P_4 = 0$ which defines T). We make the following claim about F_{ij}^{ab}.

Claim 3. *For all $\{i, j\} \subseteq [7]$, $F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1, and also $F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1.*

We first show how this claim will let us realize g_8 or g_8', and lead to #P-hardness. Then, we give a proof of Claim 3. By Claim 3 and Lemma 7.26, the degree $d(F) \leqslant 2$.

- If $d(F) \leqslant 1$, then F is an affine linear combination of variables $x_1, \ldots, x_7$, i.e., $F = \lambda_0 + \sum_{i=1}^{7} \lambda_i x_i$ where $\lambda_i \in \mathbb{Z}_2$ for $0 \leqslant i \leqslant 7$. Notice that if we negate the variable x_i of f, we will get a signature $f'(x_1, \ldots, x_8) = (-1)^{x_i} f(x_1, \ldots, x_8)$. For every x_i appearing in F (i.e., $\lambda_i = 1$), we negate the variable x_i of f. Also, if $\lambda_0 = 1$, then we normalize f by a scalar -1.

Then, we get a signature

$$f' = \chi_S \cdot 1 + 4\chi_T(-1)^{G'(x_1,\dots,x_8)}.$$

This will not change the support of f and also norms of entries of f. Thus, $f'(\alpha) = \pm 3$ or ± 1 for all $\alpha \in \mathscr{S}(f') = \mathscr{E}_8$. Then, for every $\alpha \in T$, $f'(\alpha) = 1 + 4(-1)^{G'(\alpha)} = \pm 3$, which implies that $(-1)^{G'(\alpha)} = -1$ and $f'(\alpha) = -3$, because $1 + 4 = 5$ cannot be an entry of f'. Therefore, $f' = \chi_S - 4\chi_T = g_8$. Thus, g_8 is realizable from f.

By merging variables x_1 and x_5 of g_8 using $=_2$, we can get a 6-ary signature h. We rename variables x_2, x_3, x_4 to x_1, x_2, x_3 and variables x_6, x_7, x_8 to x_4, x_5, x_6 (The choice of merging x_1 and x_5 is just for a simple renaming of variables). Then after normalization by a scalar $1/2$, h has the following signature matrix

$$M_{123,456}(h) = A = \begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & -1 \end{bmatrix}.$$

Consider the inner product $\langle \mathbf{h}_{14}^{00}, \mathbf{h}_{14}^{11} \rangle$. One can check that

$$\langle \mathbf{h}_{14}^{00}, \mathbf{h}_{14}^{11} \rangle = \sum_{1 \leqslant i,j \leqslant 4} A_{i,j} \cdot A_{i+4,j+4} = 8 \neq 0.$$

(This is the sum of pairwise products of every entry in the upper left 4×4 submatrix of A with the corresponding entry of the lower right 4×4 submatrix of A.) In fact, notice that $h(\overline{\alpha}) = \overline{h(\alpha)} = h(\alpha)$. By considering the representative matrix $M_r(h)$ of h (see Table 4), we have

$$M_r(h) = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

Then,

$$\langle \mathbf{h}_{14}^{00}, \mathbf{h}_{14}^{11} \rangle = 2(\mathrm{perm}(M_r(h)_{[1,2]}) + \mathrm{perm}(M_r(h)_{[3,4]})) = 2(2+2) = 8 \neq 0.$$

Also, since $\mathscr{S}(h) = \mathscr{E}_6$, it is easy to see that h is irreducible. Since h does not satisfy 2nd-Orth, we get #P-hardness.

- If $d(F) = 2$, then by Lemma 7.26, for all $\{i, j\} \subseteq [7]$, x_ix_j appears in F. Then, $F = \sum_{1 \leqslant i<j \leqslant 7} x_ix_j + L$ where L is an affine linear combination of variables $x_1, \ldots, x_7$. Since on the support $\mathscr{S}(f) = \mathscr{E}_8$, $x_1 + \cdots + x_8 = 0$, and on Boolean inputs $x_8^2 = x_8$, we can substitute F by $F' = F + x_8(x_1 + \cdots + x_8) - (x_8^2 - x_8) = \sum_{1 \leqslant i<j \leqslant 8} x_ix_j + L + x_8$ (all arithmetic mod 2). This will not change the signature f. Then, by negating variables of f that appear as linear terms in F' and normalization with a scalar ±1, we get a signature

$$f' = \chi_S(-1)^{\sum_{1 \leqslant i<j \leqslant 8} x_ix_j} + 4\chi_T(-1)^{G'(x_1,\ldots,x_8)} = q_8 + 4\chi_T(-1)^{G'(x_1,\ldots,x_8)}.$$

where $q_8 = \chi_S(-1)^{\sum_{1 \leqslant i<j \leqslant 8} x_ix_j}$ (see form (7.11)). For every $\alpha \in T$, since $\mathrm{wt}(\alpha) = 0, 4$ or 8, it is easy to see that $q_8(\alpha) = (-1)^{\binom{\mathrm{wt}(\alpha)}{2}} = 1$. Thus, $(-1)^{G'(\alpha)}$ must be -1 in order to get $1 - 4 = -3$, of norm 3 for f'. The other choice would give $1 + 4 = 5$ to be an entry of f', a contradiction. Therefore, $f'(\alpha) = q_8 - 4\chi_T = g'_8$. Thus, g'_8 is realizable from f.

By merging variables x_1 and x_5 of g'_8 using $=_2^-$, we can get a 6-ary signature h'. After renaming variables (same as we did for h) and normalization by a scalar $-1/2$, we have

$$M_{123,456}(h') = B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & -1 \end{bmatrix}.$$

Consider the inner product $\langle \mathbf{h'}^{00}_{14}, \mathbf{h'}^{11}_{14} \rangle$. One can check that

$$\langle \mathbf{h'}^{00}_{14}, \mathbf{h'}^{11}_{14} \rangle = \sum_{1 \leqslant i,j \leqslant 4} B_{i,j} \cdot B_{i+4,j+4} = -8 \neq 0.$$

Also, since $\mathscr{S}(h') = \mathscr{E}_6$, it is easy to see that h' is irreducible. Since h' does not satisfy 2nd-Orth, we get #P-hardness.

This completes the proof of Step 2, and the proof of the lemma, modulo Claim 3.

Now, we prove Claim 3 that for all $\{i,j\} \subseteq [7]$, $F^{00}_{ij} + F^{11}_{ij} \equiv 0$ or 1 and $F^{01}_{ij} + F^{10}_{ij} \equiv 0$ or 1. For simplicity of notation, we prove this for $\{i,j\} = \{1,2\}$. The proof for arbitrary $\{i,j\}$ is the same by replacing $\{1,2\}$ by $\{i,j\}$. Since $f \in \int_{\mathcal{B}} \mathscr{A}$, $\widetilde{f}^{00}_{12}, \widetilde{f}^{01}_{12}, \widetilde{f}^{10}_{12}, \widetilde{f}^{11}_{12} \in \mathscr{A}$. Remember all nonzero entries in $\widetilde{f}^{ab}_{12}$ have the same norm, denoted by n_{ab}. We first show that between $\widetilde{f}^{00}_{12}$ and $\widetilde{f}^{11}_{12}$, exactly one has support $\mathscr{E}_{2n-2}$ and its nonzero entries have norm 2 and the other has nonzero entries of norm 4, and between $\widetilde{f}^{01}_{12}$ and $\widetilde{f}^{10}_{12}$, exactly one has support $\mathscr{O}_{2n-2}$ and its nonzero entries have norm 2 and the other has nonzero entries of norm 4. (This is not what we have proved in Step 1 where $\{1,2\}$ is a pair of particularly chosen indices. Here $\{1,2\}$ means an arbitrary pair $\{i,j\}$.)

Consider $f^{00}_{12}(\vec{0}^6)$ and $f^{11}_{12}(\vec{0}^6)$. By Step 1 of Case 2 and Lemma 7.21, we may assume that $\mathscr{S}_3(f) = \mathscr{S}(f_8)$ (after flipping and renaming variables). We have $00\vec{0}^6 \in \mathscr{S}_3(f)$ and $11\vec{0}^6 \notin \mathscr{S}_3(f)$. Thus, $f^{00}_{12}(\vec{0}^6) = \pm 3$ and $f^{11}_{12}(\vec{0}^6) = \pm 1$. (This is true when replacing $\{1,2\}$ by an arbitrary pair of indices $\{i,j\}$.) Thus, between

$$\widetilde{f}_{12}^{00}(\vec{0}^6) = f_{12}^{00}(\vec{0}^6) + f_{12}^{11}(\vec{0}^6) \quad \text{and} \quad \widetilde{f}_{12}^{11}(\vec{0}^6) = f_{12}^{00}(\vec{0}^6) - f_{12}^{11}(\vec{0}^6),$$

one has norm 2 and the other has norm 4. They are both nonzero. Then, between n_{00} and n_{11}, one is 2 and the other is 4. By Lemma 7.24(2), between $\widetilde{f}_{12}^{00}$ and $\widetilde{f}_{12}^{11}$, the one whose nonzero entries have norm 2 has support $\mathscr{E}_6$, and moreover n_{01} and $n_{10} = 2$ or 4. Since there exists $(a,b) = (0,0)$ or $(1,1)$ such that

$$|\widetilde{f}_{12}^{ab}|^2 = n_{ab}^2 \cdot |\mathscr{S}(\widetilde{f}_{12}^{ab})| = 2^2 \cdot |\mathscr{E}_6|,$$

for $\widetilde{f}_{12}^{cd}$ where $(c,d) = (0,1)$ or $(1,0)$, if $n_{cd} = 2$, then $|\mathscr{S}(\widetilde{f}_{12}^{cd})| = |\mathscr{E}_6| = |\mathscr{O}_6|$. Since $\widetilde{f}_{12}^{cd}$ has odd parity, $\mathscr{S}(\widetilde{f}_{12}^{cd}) \subseteq \mathscr{O}_6$. Thus, $|\mathscr{S}(\widetilde{f}_{12}^{cd})| = 2^{2n-3}$ implies that $\mathscr{S}(\widetilde{f}_{12}^{cd}) = \mathscr{O}_6$.

- If $n_{01} = n_{10} = 2$, then $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{S}(\widetilde{f}_{12}^{10}) = \mathscr{O}_6$. For an arbitrary $\theta \in \mathscr{O}_6$,

  $$f(01\theta) = \frac{\widetilde{f}(01\theta) + \widetilde{f}(10\theta)}{2} = \frac{(\pm 2) + (\pm 2)}{2} \quad \text{and} \quad f(10\theta) = \frac{\widetilde{f}(01\theta) - \widetilde{f}(10\theta)}{2} = \frac{(\pm 2) - (\pm 2)}{2}.$$

  Thus, between $f(01\theta)$ and $f(10\theta)$, exactly one has norm 2 and the other has norm 0. This gives a contradiction since every nonzero entry of f has norm 1 or 3.

- If $n_{01} = n_{10} = 4$, then still consider $f(01\theta)$ and $f(10\theta)$ for an arbitrary $\theta \in \mathscr{O}_6$. We know that $f(01\theta), f(10\theta) = \pm 4, \pm 2$ or 0. The case that $f(01\theta) = 0$ or $f(10\theta) = 0$ cannot occur since $\mathscr{S}(f) = \mathscr{E}_{2n}$ and clearly, $01\theta, 10\theta \in \mathscr{E}_{2n}$. Thus, $f(01\theta), f(10\theta) = \pm 4, \pm 2$. Still, we get a contradiction since every nonzero entry of f has norm 1 or 3.

- Thus, between n_{01} and n_{10}, one is 2 and the other is 4.

Then, between $\widetilde{f}_{12}^{01}$ and $\widetilde{f}_{12}^{10}$, exactly one has support $\mathscr{O}_6$ and its nonzero entries have norm 2, and the other has nonzero entries of norm 4.

Now, we show that $F_{12}^{00} + F_{12}^{11} \equiv 0$ or 1. We first consider the case that between $\widetilde{f}_{12}^{00}$ and $\widetilde{f}_{12}^{11}$, $\widetilde{f}_{12}^{11} = f_{12}^{00} - f_{12}^{11}$ is the signature whose support is $\mathscr{E}_6$ and nonzero entries have norm 2; the case where it is $\widetilde{f}_{12}^{00}$ will be addressed shortly. Let S_0 be the subspace in $\mathbb{Z}_2^6$ obtained by setting $x_1 = x_2 = 0$ in $S = \mathscr{S}(f) = \mathscr{E}_8$, and S_1 be the subspace in $\mathbb{Z}_2^6$ obtained by setting $x_1 = x_2 = 1$. Similarly, we can define T_0 and T_1, replacing S in the definition by $T = \mathscr{S}_3(f) = I_8$. Clearly,

$S_0 = S_1 = \{(x_3, \ldots, x_8) \in \mathbb{Z}_2^6 \mid x_3 + \cdots x_8 = 0\} = \mathscr{E}_6$. Also, one can check that T_0 is disjoint with T_1. Then

$$f_{12}^{00} = \chi_{S_0}(-1)^{F_{12}^{00}(x_3,\ldots,x_7)} + 4\chi_{T_0}(-1)^{G_{12}^{00}(x_3,\ldots,x_8)},$$

and

$$f_{12}^{11} = \chi_{S_1}(-1)^{F_{12}^{11}(x_3,\ldots,x_7)} + 4\chi_{T_1}(-1)^{G_{12}^{11}(x_3,\ldots,x_8)}.$$

Thus,

$$\widetilde{f}_{12}^{11} = \chi_{\mathscr{E}_6}((-1)^{F_{12}^{00}(x_3,\ldots,x_7)} - (-1)^{F_{12}^{11}(x_3,\ldots,x_7)}) + 4\chi_{T_0}(-1)^{G_{12}^{00}(x_3,\ldots,x_8)} - 4\chi_{T_1}(-1)^{G_{12}^{11}(x_3,\ldots,x_8)}.$$

Since $\mathscr{S}(\widetilde{f}_{12}^{11}) = \mathscr{E}_6$ and $n_{11} = 2$, $\widetilde{f}_{12}^{11}(\theta) = \pm 2$ for every $\theta \in \mathscr{E}_6$. If $\theta \notin T_0 \cup T_1$, then

$$\widetilde{f}_{12}^{11}(\theta) = (-1)^{F_{12}^{00}(\theta)} - (-1)^{F_{12}^{11}(\theta)} = \pm 2.$$

If $\theta \in T_0 \cup T_1$, then it belongs to exactly one of T_0 or T_1,

$$\widetilde{f}_{12}^{11}(\theta) = (-1)^{F_{12}^{00}(\theta)} - (-1)^{F_{12}^{11}(\theta)} + 4a = \pm 2,$$

where $a = \pm 1$. In this case, the sum of the first two terms is still $(-1)^{F_{12}^{00}(\theta)} - (-1)^{F_{12}^{11}(\theta)} = \pm 2$, because the only other possible value for $(\pm 1) - (\pm 1)$ is 0 and then we would have $4a = \pm 2$, a contradiction. Thus, for every $(x_3, \ldots, x_7) \in \mathbb{Z}_2^5$ which decides every $(x_3, \ldots, x_8) \in \mathscr{E}_6$ by $x_8 = x_3 + \cdots + x_7$,

$$(-1)^{F_{12}^{00}(x_3,\ldots,x_7)} - (-1)^{F_{12}^{11}(x_3,\ldots,x_7)} = \pm 2.$$

This implies that

$$(-1)^{F_{12}^{00}(x_3,\ldots,x_7)} = -(-1)^{F_{12}^{11}(x_3,\ldots,x_7)}.$$

Thus,

$$(-1)^{F_{12}^{00}(x_3,\ldots,x_7)+F_{12}^{11}(x_3,\ldots,x_7)} = -1.$$

Then, $F_{12}^{00} + F_{12}^{11} \equiv 1$.

Now we address the case that (between $\widetilde{f}_{12}^{00}$ and $\widetilde{f}_{12}^{11}$) it is $\widetilde{f}_{12}^{00} = f_{12}^{00} + f_{12}^{11}$ the signature whose support is $\mathscr{E}_6$ and nonzero entries have norm 2. Then similarly for every $(x_3, \dots, x_7) \in \mathbb{Z}_2^5$, which determines every $(x_3, \dots, x_8) \in \mathscr{E}_6$,

$$(-1)^{F_{12}^{00}(x_3,\dots,x_7)} + (-1)^{F_{12}^{11}(x_3,\dots,x_7)} = \pm 2.$$

This implies that

$$(-1)^{F_{12}^{00}(x_3,\dots,x_7)} = (-1)^{F_{12}^{11}(x_3,\dots,x_7)}.$$

Thus,

$$(-1)^{F_{12}^{00}(x_3,\dots,x_7)+F_{12}^{11}(x_3,\dots,x_7)} = 1$$

Then, $F_{12}^{00} + F_{12}^{11} \equiv 0$.

We have proved that, $F_{12}^{00} + F_{12}^{11} \equiv 0$ or 1.

Also, consider $\widetilde{f}_{12}^{01}$ and $\widetilde{f}_{12}^{10}$. One of them is a signature whose support is $\mathscr{O}_{2n-2}$ and nonzero entries have norm 2. Then similarly, for every $(x_3, \dots, x_7) \in \mathbb{Z}^5$ which decides every $(x_3, \dots, x_8) \in \mathscr{O}_6$ by $x_8 = 1 + x_3 + \cdots + x_7$,

$$(-1)^{F_{12}^{01}(x_3,\dots,x_7)} + (-1)^{F_{12}^{10}(x_3,\dots,x_7)} = \pm 2,$$

or

$$(-1)^{F_{12}^{01}(x_3,\dots,x_7)} - (-1)^{F_{12}^{10}(x_3,\dots,x_7)} = \pm 2.$$

Then, $F_{12}^{01} + F_{12}^{10} \equiv 0$ or $F_{12}^{01} + F_{12}^{10} \equiv 1$. The above proof holds for all $\{i, j\} \subseteq [7]$. Thus, for all $\{i, j\} \subseteq [7]$, $F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1, and $F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1. □

Remark 7.28. *The above proof does not require $\mathcal{F}$ to be non-$\mathcal{B}$ hard.*

7.3.3 Support Condition

Then, by further assuming that nonzero entries of f have the same norm, we show that f has affine support or we can get the #P-hardness for non-$\mathcal{B}$ hard set $\mathcal{F}$ (Lemma 7.35). Here, we do require $\mathcal{F}$ to be non-$\mathcal{B}$ hard.

We first give one more result about $\widetilde{f}$. Remember that if $f \in \int_{\mathcal{B}} \mathscr{A}$, then $\widetilde{f}_{12}^{00}$, $\widetilde{f}_{12}^{01}$, $\widetilde{f}_{12}^{10}$,

$\widetilde{f}_{12}^{11} \in \mathscr{A}$, and n_{ab} denotes the norm of nonzero entries of $\widetilde{f}_{12}^{ab}$. Let $\widetilde{\mathcal{B}} = \left\{\widetilde{=_2^+}, \widetilde{=_2^-}, \widetilde{\neq_2^+}, \widetilde{\neq_2^-}\right\}$ where $\widetilde{=_2^+} = (2,0,0,0)$, $\widetilde{=_2^-} = (0,0,0,2)$, $\widetilde{\neq_2^+} = (0,2,0,0)$ and $\widetilde{\neq_2^-} = (0,0,2,0)$. Signatures in $\widetilde{\mathcal{B}}$ are obtained by performing the H_4 gadget construction on binary signatures in $\mathcal{B}$.

Lemma 7.29. *Let f be an irreducible signature of arity $2n \geqslant 6$ with the following properties.*

1. *f has even parity, f satisfies* 2ND-ORTH, *and $f \in \int_{\mathcal{B}} \mathscr{A}$;*
2. *for all $\{i,j\}$ disjoint with $\{1,2\}$ and every $b \in \mathcal{B}$, either $M(\mathfrak{m}_{12}(\partial_{ij}^b f)) = \lambda_{ij}^b I_4$ for some real $\lambda_{ij}^b \neq 0$, or there exists a nonzero binary signature $g_{ij}^b \in \mathcal{B}$ such that $g_{ij}^b(x_1,x_2) \mid \partial_{ij}^b f$.*

If $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{S}(\widetilde{f}_{12}^{10})$, $n_{00} > n_{01} > 0$, then $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{O}_{2n-2}$.

证明. We first analyze the second property of f, i.e., the property about $\partial_{ij}^b f$.

- If $M(\mathfrak{m}_{12}(\partial_{ij}^b f)) = \lambda_{ij}^b I_4$, by Lemma 7.23, then $M(\mathfrak{m}_{12}(\widetilde{\partial_{ij}^b f})) = 2\lambda_{ij}^b I_4$. Since $\{i,j\}$ is disjoint with $\{1,2\}$, the H_4 gadget on variables x_1 and x_2 commutes with the merging gadget on variables x_i and x_j. Thus, $\widetilde{\partial_{ij}^b f} = \partial_{ij}^b \widetilde{f}$. Let $(\partial_{ij}^b \widetilde{f})_{12}^{ab}$ be the signature obtained by setting variables x_1 and x_2 of $\partial_{ij}^b \widetilde{f}$ to a and b, and $\partial_{ij}^b(\widetilde{f}_{12}^{ab})$ be the signature obtained by merging variables x_i and x_j of $\widetilde{f}_{12}^{ab}$. Again, since $\{1,2\}$ and $\{i,j\}$ are disjoint, $(\partial_{ij}^b \widetilde{f})_{12}^{ab} = \partial_{ij}^b(\widetilde{f}_{12}^{ab})$. We denote them by $\partial_{ij}^b \widetilde{f}_{12}^{ab}$. Then, since $M(\mathfrak{m}_{12}(\widetilde{\partial_{ij}^b f})) = M(\mathfrak{m}_{12}(\partial_{ij}^b \widetilde{f})) = 2\lambda_{ij}^b I_4$,

$$|\partial_{ij}^b \widetilde{\mathbf{f}}_{12}^{00}|^2 = |\partial_{ij}^b \widetilde{\mathbf{f}}_{12}^{01}|^2 = |\partial_{ij}^b \widetilde{\mathbf{f}}_{12}^{10}|^2 = |\partial_{ij}^b \widetilde{\mathbf{f}}_{12}^{11}|^2 = 2\lambda_{ij}^b \neq 0.$$

- If $g_{ij}^b(x_1,x_2) \mid \partial_{ij}^b f$, i.e, $\partial_{ij}^b f = g_{ij}^b(x_1,x_2) \otimes h$, then $\widetilde{\partial_{ij}^b f} = \partial_{ij}^b \widetilde{f} = \widetilde{g_{ij}^b}(x_1,x_2) \otimes h$. Since $g_{ij}^b \in \mathcal{B}$, $\widetilde{g_{ij}^b} \in \widetilde{\mathcal{B}}$. By the form of signatures in $\widetilde{\mathcal{B}}$, among $\partial_{ij}^b \widetilde{f}_{12}^{00}$, $\partial_{ij}^b \widetilde{f}_{12}^{01}$, $\partial_{ij}^b \widetilde{f}_{12}^{10}$ and $\partial_{ij}^b \widetilde{f}_{12}^{11}$, at most one is a nonzero signature.

Combining the above two cases we have that, among $\partial_{ij}^b \widetilde{f}_{12}^{00}$, $\partial_{ij}^b \widetilde{f}_{12}^{01}$, $\partial_{ij}^b \widetilde{f}_{12}^{10}$ and $\partial_{ij}^b \widetilde{f}_{12}^{11}$, if at least two of them are nonzero signatures then they are all nonzero signatures.

Now, we show that $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{O}_{2n-2}$. Since f has even parity, $\widetilde{f}$ also has even parity. Then, $\widetilde{f}_{12}^{01}$ has odd parity, i.e., $\mathscr{S}(\widetilde{f}_{12}^{01}) \subseteq \mathscr{O}_{2n-2}$. For a contradiction, suppose that $\mathscr{S}(\widetilde{f}_{12}^{01}) \subsetneq \mathscr{O}_{2n-2}$. Since $n_{01} > 0$, $\mathscr{S}(\widetilde{f}_{12}^{01}) \neq \emptyset$. Then, we can pick a pair of inputs $\alpha, \beta \in \mathscr{O}_{2n-2}$ with $\operatorname{wt}(\alpha \oplus \beta) = 2$ such that $\alpha \in \mathscr{S}(\widetilde{f}_{12}^{01})$ and $\beta \notin \mathscr{S}(\widetilde{f}_{12}^{01})$. Also, since $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{S}(\widetilde{f}_{12}^{10})$, $\alpha \in \mathscr{S}(\widetilde{f}_{12}^{10})$ and $\beta \notin \mathscr{S}(\widetilde{f}_{12}^{10})$.

Thus, $|\widetilde{f}^{01}_{12}(\alpha)| = n_{01}$ and $|\widetilde{f}^{01}_{12}(\beta)| = 0$, and $|\widetilde{f}^{10}_{12}(\alpha)| = n_{10}$ and $|\widetilde{f}^{10}_{12}(\beta)| = 0$. Suppose that α and β differ in bits i and j. Clearly, $\{i, j\}$ is disjoint with $\{1, 2\}$. Depending whether $\alpha_i = \alpha_j$ or $\alpha_i \neq \alpha_j$, we connect variables x_i and x_j of $\widetilde{f}$ using $=^{+}_{2}$ or $\neq^{+}_{2}$. We get signatures $\partial^{+}_{ij}\widetilde{f}$ or $\partial^{\widehat{+}}_{ij}\widetilde{f}$ respectively. We consider the case that $\alpha_i = \alpha_j$; in this case $\{\alpha_i\alpha_j, \beta_i\beta_j\} = \{00, 11\}$. For the case that $\alpha_i \neq \alpha_j$, the analysis is the same by replacing $\partial^{+}_{ij}\widetilde{f}$ with $\partial^{\widehat{+}}_{ij}\widetilde{f}$.

Consider $\partial^{+}_{ij}\widetilde{f}$. Then, because $\{\alpha_i\alpha_j, \beta_i\beta_j\} = \{00, 11\}$, $\widetilde{f}^{01}_{12}(\alpha)+\widetilde{f}^{01}_{12}(\beta)$ and $\widetilde{f}^{10}_{12}(\alpha)+\widetilde{f}^{10}_{12}(\beta)$ are entries of $\partial^{+}_{ij}\widetilde{f}$; more precisely, they are entries of $\partial^{+}_{ij}\widetilde{f}^{01}_{12}$ and $\partial^{+}_{ij}\widetilde{f}^{10}_{12}$ respectively. Since $\widetilde{f}^{01}_{12}(\beta) = \widetilde{f}^{10}_{12}(\beta) = 0$, we have

$$|\widetilde{f}^{01}_{12}(\alpha) + \widetilde{f}^{01}_{12}(\beta)| = |\widetilde{f}^{01}_{12}(\alpha)| = n_{01} \neq 0, \quad \text{and} \quad |\widetilde{f}^{10}_{12}(\alpha) + \widetilde{f}^{10}_{12}(\beta)| = |\widetilde{f}^{10}_{12}(\alpha)| = n_{10} \neq 0.$$

Thus, $\partial^{+}_{ij}\widetilde{f}^{01}_{12}$ has a nonzero entry with norm n_{01}, and then $\partial^{+}_{ij}\widetilde{f}^{01}_{12} \not\equiv 0$. Also, we have $\partial^{+}_{ij}\widetilde{f}^{10}_{12} \not\equiv 0$. Thus at least two among $\partial^{+}_{ij}\widetilde{f}^{00}_{12}$, $\partial^{+}_{ij}\widetilde{f}^{01}_{12}$, $\partial^{+}_{ij}\widetilde{f}^{10}_{12}$ and $\partial^{+}_{ij}\widetilde{f}^{10}_{12}$ are nonzero, it follows that all of them are nonzero signatures.

Then $\partial^{+}_{ij}\widetilde{f}^{00}_{12} \not\equiv 0$. Let $\partial^{+}_{ij}\widetilde{f}^{00}_{12}(\gamma)$ be a nonzero entry of $\partial^{+}_{ij}\widetilde{f}^{00}_{12}$. Then, $\partial^{+}_{ij}\widetilde{f}^{00}_{12}(\gamma) = \widetilde{f}^{0000}_{12ij}(\gamma) + \widetilde{f}^{0011}_{12ij}(\gamma) \neq 0$.[*] Clearly, $\widetilde{f}^{0000}_{12ij}(\gamma)$ and $\widetilde{f}^{0011}_{12ij}(\gamma)$ are entries of $\widetilde{f}^{00}_{12}$, and they have norm n_{00} or 0. Thus, $\partial^{+}_{ij}\widetilde{f}^{00}_{12}(\gamma)$ has norm $2n_{00}$ or n_{00}. Also, $\partial^{+}_{ij}\widetilde{f}^{00}_{12}(\gamma)$ is an entry of $\partial^{+}_{ij}\widetilde{f}$ on the input 00γ. Thus, $\partial^{+}_{ij}\widetilde{f}$ has a nonzero entry with norm $2n_{00}$ or n_{00}. Since $n_{00} > n_{01}$, both $2n_{00}$ and n_{00} are not equal to n_{01}. Thus, $\partial^{+}_{ij}\widetilde{f}$ has two nonzero entries with different norms. Such a signature is not in $\mathscr{A}$. However, since $f \in \int_{\mathcal{B}}\mathscr{A}$, by Lemma 7.23, $\partial^{+}_{ij}\widetilde{f} \in \mathscr{A}$. Contradiction. Thus, $\mathscr{S}(\widetilde{f}^{01}_{12}) = \mathscr{O}_{2n-2}$. □

We also give a result about the edge partition of complete graphs into two complete tripartite subgraphs. This result should also be of independent interest. We say a graph $G = (V, E)$ is tripartite if $V = V_1 \sqcup V_2 \sqcup V_3$ and every $e \in E$ is between distinct V_i and V_j. Here $\sqcup$ denotes disjoint union. The parts V_i are allowed to be empty. It is a complete tripartite graph if every pair between distinct V_i and V_j is an edge.

Definition 7.30. *Let K_n be the complete graph on n vertices. We say K_n has a* tripartite 2-partition *if there exist complete tripartite subgraphs T_1 and T_2 such that $\{E(T_1), E(T_2)\}$ is a partition of $E(K_n)$, i.e., $E(K_n) = E(T_1) \sqcup E(T_2)$. We say T_1 and T_2 are witnesses of a tripartite*

[*] For the case that $\alpha_i \neq \alpha_j$, $\partial^{+}_{ij}\widetilde{f}^{00}_{12}(\gamma) = \widetilde{f}^{0000}_{12ij}(\gamma) + \widetilde{f}^{0011}_{12ij}(\gamma)$ will be replced by $\partial^{\widehat{+}}_{ij}\widetilde{f}^{00}_{12}(\gamma) = \widetilde{f}^{0001}_{12ij}(\gamma) + \widetilde{f}^{0010}_{12ij}(\gamma)$.

2-partition of K_n.

Lemma 7.31. *K_n has a tripartite 2-partition iff $n \leqslant 5$. For $n = 5$, up to an automorphism of K_5, there is a unique tripartite 2-partition where T_1 is a triangle on $\{v_1, v_2, v_3\}$ and T_2 is the complete tripartite graph with parts $\{v_1, v_2, v_3\}$, $\{v_4\}$ and $\{v_5\}$.*

证明. Let T be a complete tripartite graph. Let $G_{2,1}$ be the union of K_2 and an isolated vertex. We first prove the following two claims.

Claim 1. *$G_{2,1}$ is not an induced subgraph of T.*

For a contradiction, suppose $G_{2,1} = (V, E)$ is an induced subgraph of T, where $V = \{v_1, v_2, v_3\}$, and $E = \{(v_1, v_2)\}$. Then, v_1 and v_2 belong to distinct parts of T. Since $(v_1, v_3), (v_2, v_3) \notin E(T)$, v_1 and v_3 belong to the same part of T, and so are v_2 and v_3. Thus, v_1 and v_2 belong to the same part of T. This contradiction proves Claim 1.

Claim 2. *K_4 is not an induced subgraph of T.*

For a contradiction, suppose K_4 on $V = \{v_1, v_2, v_3, v_4\}$ is an induced subgraph of T. Then, for any two distinct vertices $v_i, v_j \in V$, the edge $(v_i, v_j) \in K_4$ shows that v_i and v_j belong to distinct parts in T. But T has at most three distinct nonempty parts. This contradiction proves Claim 2.

Now, we prove this lemma. The cases $n = 1, 2, 3$ are trivial. When $n = 4$, we have the following two tripartite 2-partitions of K_4, with $V(T_1) = \{v_1\} \sqcup \{v_2\} \sqcup \{v_3\}$ and $V(T_2) = \{v_1, v_2, v_3\} \sqcup \{v_4\} \sqcup \emptyset$, or alternatively with $V(T_1') = \{v_1\} \sqcup \{v_2\} \sqcup \emptyset$ and $V(T_2') = \{v_1, v_2\} \sqcup \{v_3\} \sqcup \{x_4\}$.

We consider $n \geqslant 5$. Suppose K_n has a tripartite 2-partition with complete tripartite subgraphs $T_1 = (V_1, E_1)$ and $T_2 = (V_2, E_2)$. We write (A_i, B_i, C_i) for the three parts of T_i, $i = 1, 2$.

Clearly $V = V_1 \cup V_2$, as all vertices of V must appear in either T_1 or T_2, for otherwise any edge incident to $v \in V \setminus (V_1 \cup V_2)$ is not in $E_1 \cup E_2$. If all parts of both T_1 and T_2 have size at most 1, then $|E_1 \sqcup E_2| \leqslant 6 < |K_5| \leqslant |K_n|$, a contradiction. So at least one part, say A_1, has size $|A_1| \geqslant 2$, and we let $a, a' \in A_1$. Then, $(a, a') \notin E_1$. Thus, $(a, a') \in E_2$ and $a, a' \in V_2$.

We show that $(V_1 \setminus A_1) \cap (V_2 \setminus A_1) = \emptyset$. Otherwise, there exists $v \in (V_1 \setminus A_1) \cap (V_2 \setminus A_1)$. Then, edges $(v, a), (v, a') \in E_1$. Thus, among edges $(v, a), (v, a')$ and (a, a') of K_n, (a, a') is the only one in T_2. Since $v, a, a' \in V_2$, $G_{2,1}$ is an induced subgraph of T_2. A violation of Claim 1.

If both $V_1 \setminus A_1$ and $V_2 \setminus A_1$ are nonempty, then an edge in K_n between $u \in V_1 \setminus A_1$ and $v \in V_2 \setminus A_1$ is in neither E_1 nor E_2, since $u \notin V_2$ and $v \notin V_1$. This is a contradiction. If $V_1 \setminus A_1 = \emptyset$, then $E_1 = \emptyset$, and then all edges of K_n belong to T_2, which violates Claim 2. So $V_2 \setminus A_1 = \emptyset$. Since $V = V_1 \cup V_2$, $V_2 \setminus A_1 = \emptyset$ implies that $V = V_1$.

Clearly $V_1 \setminus A_1 = B_1 \sqcup C_1$. If $|B_1| \geqslant 2$, then there exists some $\{u, v\} \subseteq B_1 \subseteq V_1 \setminus A_1$, which is disjoint from V_2. Thus $\{u, v\} \notin E_1 \sqcup E_2$, a contradiction. Hence $|B_1| \leqslant 1$. Similarly $|C_1| \leqslant 1$. Finally, if $|A_1| \geqslant 4$, then there is a K_4 inside A_1 which must be an induced subgraph of T_2, a violation of Claim 2. Thus $|A_1| \leqslant 3$. It follows that $n \leqslant 5$ since $V = V_1 = A_1 \sqcup B_1 \sqcup C_1$. If $n = 5$, then $|A_1| = 3$ and $|B_1| = |C_1| = 1$. After relabeling vertices, we may assume that $A_1 = \{v_1, v_2, v_3\}$, $B_1 = \{v_4\}$ and $C_1 = \{v_5\}$. Then, we have $A_2 = \{v_1\}$, $B_2 = \{v_2\}$ and $C_2 = \{v_3\}$. This gives the unique tripartite 2-partition of K_5. □

We will apply Lemma 7.31 to multilinear $\mathbb{Z}_2$-polynomials. Remember that we take the reduction of polynomials in $\mathbb{Z}_2[x_1, \ldots, x_n]$ modulo the ideal generated by $\{x_i^2 - x_i \mid i \in [n]\}$ replacing any F by its unique multilinear representative.

Definition 7.32. *Let $F(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$ be a complete quadratic polynomial. We say F has a twice-linear 2-partition if there exist $L_1, L_2, L_3, L_4 \in \mathbb{Z}_2[x_1, \ldots, x_n]$ where $d(L_1) = d(L_2) = d(L_3) = d(L_4) \leqslant 1$ such that $F = L_1 \cdot L_2 + L_3 \cdot L_4$.*

Lemma 7.31 gives the following result about multilinear $\mathbb{Z}_2$-polynomials.

Lemma 7.33. *Let $F(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$ be a complete quadratic polynomial. For $n \geqslant 6$, F does not have a twice-linear 2-partition. For $n = 5$, F has a twice-linear 2-partition $F = L_1 \cdot L_2 + L_3 \cdot L_4$ iff (after renaming variables) the cross terms of $L_1 \cdot L_2$ and $L_3 \cdot L_4$ correspond to the unique tripartite 2-partition of K_5, and we have $L_1 \cdot L_2 = (x_1 + x_2 + a)(x_2 + x_3 + b)$ and $L_3 \cdot L_4 = (x_1 + x_2 + x_3 + x_4 + c)(x_1 + x_2 + x_3 + x_5 + d)$ for some $a, b, c, d \in \mathbb{Z}_2$.*

证明. We first analyze the quadratic terms that appear in a product of two linear polynomials. We use $x_i \in L$ to denote that a linear term x_i appears in a linear polynomial L. Let L_1 and L_2 be two linear polynomials.

Let $U_1 = \{x_i \mid x_i \in L_1, x_i \notin L_2\}$, $U_2 = \{x_i \mid x_i \in L_1, x_i \in L_2\}$, and $U_3 = \{x_i \mid x_i \notin L_1, x_i \in$

$L_2\}$. Then,

$$L_1 = \sum_{x_i \in U_1} x_i + \sum_{x_j \in U_2} x_j + a, \quad \text{and} \quad L_2 = \sum_{x_j \in U_2} x_j + \sum_{x_k \in U_3} x_k + b$$

for some $a, b \in \mathbb{Z}_2^2$. The quadratic terms in $L_1 \cdot L_2$ are from

$$\Big(\sum_{x_i \in U_1} x_i + \sum_{x_j \in U_2} x_j\Big) \cdot \Big(\sum_{x_j \in U_2} x_j + \sum_{x_k \in U_3} x_k\Big)$$

which are enumerated in

$$\sum_{x_i \in U_1, x_j \in U_2} x_i x_j + \sum_{x_i \in U_1, x_k \in U_3} x_i x_k + \sum_{x_j \in U_2, x_k \in U_3} x_j x_k.$$

Note that each term x_i^2 for $i \in U_2$ is replaced by x_i (thus no longer counted as a quadratic term) as we calculate modulo the ideal generated by $\{x_i^2 - x_i \mid i \in [n]\}$, and every pairwise cross product term $x_i x_j$ for $i, j \in U_2$ and $i \neq j$ disappears since it appears exactly twice.

If we view variables $x_1, \ldots, x_n$ as n vertices and each quadratic term $x_i x_j$ as an edge between vertices x_i and x_j, then the quadratic terms in $L_1 \cdot L_2$ are the edges of a complete tripartite subgraph T of K_n (the parts of a tripartite graph could be empty) and $V(T) = U_1 \sqcup U_2 \sqcup U_3$. Therefore, $L_1 \cdot L_2$ is one of the two terms of a twice-linear 2-partition of a complete quadratic polynomial over n variables iff T is one tripartite complete graph in a tripartite 2-partition of the complete graph K_n. By Lemma 7.31, a tripartite 2-partition does not exist for K_n when $n \geqslant 6$. Thus, F does not have twice-linear partition when $n \geqslant 6$. When $n = 5$, the tripartite 2-partition of K_5 is unique up to relabeling. One tripartite complete graph of this tripartite 2-partition is a triangle, and we may assume it is on $\{x_1, x_2, x_3\}$. Then, we take $L_1 \cdot L_2 = (x_1 + x_2 + a)(x_2 + x_3 + b)$ for some $a, b \in \mathbb{Z}_2^2$, and $L_3 \cdot L_4 = (x_1 + x_2 + x_3 + x_4 + c)(x_1 + x_2 + x_3 + x_5 + d)$ for some $c, d \in \mathbb{Z}_2^2$. Thus, a complete quadratic polynomial $F(x_1, \ldots, x_5)$ over 5 variables has a twice-linear 2-partition iff (after renaming variables) $F = L_1 \cdot L_2 + L_3 \cdot L_4$. □

Now, we are ready to make a further major step towards Theorem 7.38. We first give a preliminary result.

Lemma 7.34. *Let f be a $2n$-ary signature, where $2n \geqslant 4$. If $f \in \int_{\mathcal{B}} \mathscr{A}$ and $|f(\alpha)| = 1$ for all $\alpha \in \mathscr{S}(f)$, then for all $\{i, j\} \subseteq [2n]$, $\mathscr{S}(f_{ij}^{00}) = \mathscr{S}(f_{ij}^{11})$ or $\mathscr{S}(f_{ij}^{00}) \cap \mathscr{S}(f_{ij}^{11}) = \emptyset$, and*

$\mathscr{S}(f^{01}_{ij}) = \mathscr{S}(f^{10}_{ij})$ or $\mathscr{S}(f^{01}_{ij}) \cap \mathscr{S}(f^{10}_{ij}) = \emptyset$.

证明. We first prove that for all $\{i,j\} \subseteq [2n]$, $\mathscr{S}(f^{00}_{ij}) = \mathscr{S}(f^{11}_{ij})$ or $\mathscr{S}(f^{00}_{ij}) \cap \mathscr{S}(f^{11}_{ij}) = \emptyset$. For a contradiction, suppose that there exist $\alpha, \beta \in \mathbb{Z}_2^{2n-2}$ such that $\alpha \in \mathscr{S}(f^{00}_{ij}) \cap \mathscr{S}(f^{11}_{ij})$ and $\beta \in \mathscr{S}(f^{00}_{ij}) \Delta \mathscr{S}(f^{11}_{ij})$, where Δ denotes the symmetric difference between two sets. Consider signatures $\partial^{+}_{ij} f$ and $\partial^{-}_{ij} f$. Then, $f^{00}_{ij}(\alpha) + f^{11}_{ij}(\alpha)$ and $f^{00}_{ij}(\beta) + f^{11}_{ij}(\beta)$ are entries of $\partial^{+}_{ij} f$, and $f^{00}_{ij}(\alpha) - f^{11}_{ij}(\alpha)$ and $f^{00}_{ij}(\beta) - f^{11}_{ij}(\beta)$ are entries of $\partial^{-}_{ij} f$. Since $\alpha \in \mathscr{S}(f^{00}_{ij}) \cap \mathscr{S}(f^{11}_{ij})$, $f^{00}_{ij}(\alpha) = \pm 1$ and $f^{11}_{ij}(\alpha) = \pm 1$. Then between $f^{00}_{ij}(\alpha) + f^{11}_{ij}(\alpha)$ and $f^{00}_{ij}(\alpha) - f^{11}_{ij}(\alpha)$, exactly one has norm 2 and the other is 0. However, since $\beta \in \mathscr{S}(f^{00}_{ij}) \Delta \mathscr{S}(f^{11}_{ij})$, between $f^{00}_{ij}(\beta)$ and $f^{11}_{ij}(\beta)$, exactly one is 0 and the other has norm 1. Thus, $|f^{00}_{ij}(\beta) + f^{11}_{ij}(\beta)| = |f^{00}_{ij}(\beta) - f^{11}_{ij}(\beta)| = 1$. Then, between $\partial^{+}_{ij} f$ and $\partial^{-}_{ij} f$, there is a signature that has an entry of norm 1 and an entry of norm 2. Clearly, such a signature is not in $\mathscr{A}$. However, since $f \in \int_{\mathcal{B}} \mathscr{A}$, we have $\partial^{+}_{ij} f$, $\partial^{-}_{ij} f \in \mathscr{A}$. Contradiction.

By considering signatures $\partial^{\widehat{+}}_{ij} f$ and $\partial^{\widehat{-}}_{ij} f$, similarly we can show that $\mathscr{S}(f^{01}_{ij}) = \mathscr{S}(f^{10}_{ij})$ or $\mathscr{S}(f^{01}_{ij}) \cap \mathscr{S}(f^{10}_{ij}) = \emptyset$. □

The next lemma is a major step.

Lemma 7.35. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition (T), and $\mathcal{F}$ is non-$\mathcal{B}$ hard. If $\mathcal{F}$ contains an irreducible $2n$-ary signature f with parity where $2n \geqslant 8$, then*

- $\operatorname{Holant}^b(\mathcal{F})$ *is #P-hard, or*
- *there is a signature $g \notin \mathscr{A}$ of arity $2k < 2n$ that is realizable from f and $\mathcal{B}$, or*
- *f has affine support.*

证明. Again, we may assume that f satisfies 2ND-ORTH and $f \in \int_{\mathcal{B}} \mathscr{A}$. Also, by Lemma 7.27, we may assume that $f(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(f)$ after normalization.

For any four distinct binary strings $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2^{2n}$ with $\alpha \oplus \beta \oplus \gamma = \delta$, we define a *score* $T(\alpha, \beta, \gamma, \delta) = (t_1, t_2, t_3)$ which are the values of $\operatorname{wt}(\alpha \oplus \beta) = \operatorname{wt}(\gamma \oplus \delta), \operatorname{wt}(\alpha \oplus \gamma) = \operatorname{wt}(\beta \oplus \delta)$ and $\operatorname{wt}(\alpha \oplus \delta) = \operatorname{wt}(\beta \oplus \gamma)$ ordered from the smallest to the largest. We order the scores lexicographically, i.e., we say $T = (t_1, t_2, t_3) < T' = (t'_1, t'_2, t'_3)$ if $t_1 < t'_1$, or $t_2 < t'_2$ when $t_1 = t'_1$, or $t_3 < t'_3$ when $t_1 = t'_1$ and $t_2 = t'_2$. Note that since $\alpha, \beta, \gamma, \delta$ are distinct, the smallest value of the score T is

$(2,2,2)$. We say that $(\alpha, \beta, \gamma, \delta)$ where $\alpha \oplus \beta \oplus \gamma = \delta$ forms a *non-affine quadrilateral* of f if exactly three of them are in $\mathscr{S}(f)$ and the fourth is not.

For a contradiction, suppose that $\mathscr{S}(f)$ is not affine. Then, f has at least a non-affine quadrilateral. Among all non-affine quadrilaterals of f, we pick the one $(\alpha, \beta, \gamma, \delta)$ with the minimum score $T_{\min} = T(\alpha, \beta, \gamma, \delta) = (t_1, t_2, t_3)$. Without loss of generality, we may assume that among α, β, γ and δ, δ is the one that is not in $\mathscr{S}(f)$.

We first consider the case that $(2,2,2) < T_{\min}$. We prove that we can realize a non-affine signature from f by merging. Depending on the values of $T_{\min}$, there are three cases.

- $t_1 \geqslant 4$. Without loss of generality, we may assume that $t_1 = \mathrm{wt}(\alpha \oplus \beta)$. (Note that even though we have named δ as the one not belonging to $\mathscr{S}(f)$, since $\alpha \oplus \beta \oplus \gamma \oplus \delta = 0$, we can name them so that $t_1 = \mathrm{wt}(\alpha \oplus \beta)$.) Then, there are at least four bits on which α and β differ. Among these four bits, there are at least two bits on which γ is identical to α or β. Without loss of generality, we assume that these are the first two bits and $\gamma_1\gamma_2 = \alpha_1\alpha_2$. We have $\beta_1\beta_2 = \overline{\alpha_1\alpha_2}$, and as $\delta = \alpha \oplus \beta \oplus \gamma$, we have $\delta_1\delta_2 = \overline{\alpha_1\alpha_2}$. Also by flipping variables, we may assume that $\alpha = \vec{0}^{2n} = 00\vec{0}^{2n-2}$. Then, $\beta = 11\beta^*$, $\gamma = 00\gamma^*$ and $\delta = 11\delta^*$ where $\beta^*, \gamma^*, \delta^* \in \mathbb{Z}_2^{2n-2}$ and $\delta^* = \beta^* \oplus \gamma^*$. We consider the following eight inputs of f.

$$\begin{array}{cccc} \alpha = 00\alpha^* & \alpha' = 11\alpha^* & \beta' = 00\beta^* & \beta = 11\beta^* \\ \gamma = 00\gamma^* & \gamma' = 11\gamma^* & \delta' = 00\delta^* & \delta = 11\delta^* \end{array}$$

  Note that $\gamma' = \alpha \oplus \alpha' \oplus \gamma$, and $\mathrm{wt}(\alpha \oplus \alpha') = 2 < t_1$. Then,

$$T(\alpha, \alpha', \gamma, \gamma') < T(\alpha, \beta, \gamma, \delta).$$

  By our assumption that $T(\alpha, \beta, \gamma, \delta)$ is the minimum score among all non-affine quadrilaterals of f, $(\alpha, \alpha', \gamma, \gamma')$ is not a non-affine quadrilateral of f. Since $\alpha, \gamma \in \mathscr{S}(f)$, α' and γ' are either both in $\mathscr{S}(f)$ or both not in $\mathscr{S}(f)$. Also, note that $\gamma' = \alpha' \oplus \beta \oplus \delta$, and $\mathrm{wt}(\alpha' \oplus \beta) = \mathrm{wt}(\alpha \oplus \beta) - 2 = t_1 - 2 < t_1$. Then,

$$T(\alpha', \beta, \gamma', \delta) < T(\alpha, \beta, \gamma, \delta).$$

Again since $T(\alpha,\beta,\gamma,\delta)$ is the minimum score among all non-affine quadrilaterals of f, $(\alpha',\beta,\gamma',\delta)$ is not a non-affine quadrilateral. Since $\beta\in\mathscr{S}(f)$ and $\delta\notin\mathscr{S}(f)$, α' and γ' are not both in $\mathscr{S}(f)$. Thus, $\alpha',\gamma'\notin\mathscr{S}(f)$. Similarly, $(\beta',\beta,\delta',\delta)$ and $(\alpha,\beta',\gamma,\delta')$ are not non-affine quadrilaterals of f, since their scores are less than $T(\alpha,\beta,\gamma,\delta)$. Since $\beta\in\mathscr{S}(f)$ and $\delta\notin\mathscr{S}(f)$, we cannot have both $\beta',\delta'\in\mathscr{S}(f)$ from considering $(\beta',\beta,\delta',\delta)$, and then from $(\alpha,\beta',\gamma,\delta')$, we cannot have exactly one of β',δ' is in $\mathscr{S}(f)$. Thus, both $\beta',\delta'\notin\mathscr{S}(f)$. In other words, we have $f(\alpha')=f(\beta')=f(\gamma')=f(\delta')=0$.

Consider the signature $\partial_{12}f$. Then, $f(\alpha)+f(\alpha')$, $f(\beta)+f(\beta')$, $f(\gamma)+f(\gamma')$ and $f(\delta)+f(\delta')$ are entries of $\partial_{12}f$ on inputs α^*, β^*, γ^* and δ^* respectively. Since $f(\alpha)+f(\alpha')=f(\alpha)\neq 0$, $f(\beta)+f(\beta')=f(\beta)\neq 0$ and $f(\gamma)+f(\gamma')=f(\gamma)\neq 0$, $\alpha^*,\beta^*,\gamma^*\in\mathscr{S}(\partial_{12}f)$. Meanwhile we have $f(\delta)+f(\delta')=0+0=0$, thus $\delta^*\notin\mathscr{S}(\partial_{12}f)$. Thus, $(\alpha^*,\beta^*,\gamma^*,\delta^*)$ is a non-affine quadrilateral of $\partial_{12}f$. Then, $\partial_{12}f$ is a non-affine signature of arity $2n-2$. Contradiction.

- $t_1=2$ and $t_2\geqslant 4$. Without loss of generality, we assume that $\text{wt}(\alpha\oplus\gamma)=2$ and $\text{wt}(\alpha\oplus\beta)=t_2\geqslant 4$. (Again, using $\alpha\oplus\beta\oplus\gamma\oplus\delta=0$, a moment reflection shows that this is indeed without loss of generality, even though we have named $\delta\notin\mathscr{S}(f)$.) Again by flipping variables, we may assume that $\alpha=\vec{0}^{2n}$. Then, $\text{wt}(\gamma)=2$ and $\text{wt}(\beta)\geqslant 4$. Take four bits where $\beta_i=1$, for at most two of these we can have $\gamma_i=1$, thus there exist two other bits of these four bits (we may assume that they are the first two bits) such that $\gamma_1\gamma_2=00$ and $\beta_1\beta_2=11$. Then, $\alpha=00\alpha^*$, $\beta=11\beta^*$, $\gamma=00\gamma^*$, and $\delta=11\delta^*$ by $\delta=\alpha\oplus\beta\oplus\gamma$, where $\beta^*,\gamma^*,\delta^*\in\mathbb{Z}_2^{2n-2}$, $\text{wt}(\beta^*)\geqslant 2$, $\text{wt}(\gamma^*)=2$ and $\delta^*=\beta^*\oplus\gamma^*$. Still, we consider the following eight inputs of f.

$$\begin{array}{cccc}\alpha=00\alpha^* & \alpha'=11\alpha^* & \beta'=00\beta^* & \beta=11\beta^*\\ \gamma=00\gamma^* & \gamma'=11\gamma^* & \delta'=00\delta^* & \delta=11\delta^*\end{array}$$

Note that $\text{wt}(\alpha\oplus\gamma)=2$ and $\text{wt}(\alpha\oplus\alpha')=2<t_2$. Then,

$$T(\alpha,\alpha',\gamma,\gamma')<T(\alpha,\beta,\gamma,\delta).$$

Then similarly since $T(\alpha,\beta,\gamma,\delta)$ is the minimum, $(\alpha,\alpha',\gamma,\gamma')$ is not a non-affine quadrilateral. Since $\alpha,\gamma\in\mathscr{S}(f)$, α' and γ' are either both in $\mathscr{S}(f)$ or both not in it. Also, note that

$\text{wt}(\alpha' \oplus \gamma') = 2$ and $\text{wt}(\alpha' \oplus \beta) = \text{wt}(\alpha \oplus \beta) - 2 = t_2 - 2 < t_2$. Then,

$$T(\alpha', \beta, \gamma', \delta) < T(\alpha, \beta, \gamma, \delta).$$

Thus, $(\alpha', \beta, \gamma', \delta)$ is not a non-affine quadrilateral. Since $\beta \in \mathscr{S}(f)$ and $\delta \notin \mathscr{S}(f)$, α' and γ' are not both in $\mathscr{S}(f)$. Thus, $\alpha', \gamma' \notin \mathscr{S}(f)$. Similarly, by considering $(\beta', \beta, \delta', \delta)$ and $(\alpha, \beta', \gamma, \delta')$, we know that they are not non-affine quadrilaterals. Thus, $\beta', \delta' \notin \mathscr{S}(f)$. In other words, we have $f(\alpha') = f(\beta') = f(\gamma') = f(\delta') = 0$. Still consider the signature $\partial_{12} f$. We have $\partial_{12} f \notin \mathscr{A}$. Contradiction.

- $t_1 = 2$, $t_2 = 2$ and $t_3 = 4$. In this case, by the definition of distance-2 squares (equation (7.12)), $\left[\begin{smallmatrix} f(\alpha) & f(\beta) \\ f(\gamma) & f(\delta) \end{smallmatrix}\right]$ forms a distance-2 square. Clearly, it is not of type I, II or III since exactly one entry of this square is zero. As proved in Lemma 7.27, since f has a distance-2 square that is not type I, II or III, then we can realize a non-affine signature by merging. Contradiction.

Now, we consider the case that $T_{\min} = (2, 2, 2)$.

Then, we show that $|\mathscr{S}(f)| = 2^{2n-2}$. We consider the non-affine quadrilateral $(\alpha, \beta, \gamma, \delta)$ with score $T = (2, 2, 2)$. By renaming and flipping variables, without loss of generality, we may assume that

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 000\vec{0}^{2n-3} & 011\vec{0}^{2n-3} \\ 110\vec{0}^{2n-3} & 101\vec{0}^{2n-3} \end{bmatrix},$$

and δ is the only one among four that is not in $\mathscr{S}(f)$. By normalization, we may assume that $f(\alpha) = 1$. If $f(\gamma) = -1$, then we negate the variable x_1 of f. This keeps f_1^0 unchanged but changes f_1^1 to $-f_1^1$, so this does not change the value of $f(\alpha)$, but changes the value of $f(\gamma)$ to 1. Thus, without loss of generality, we may assume that $f(\alpha) = f(\gamma) = 1$. Clearly, f has even parity. Consider the signature $\widetilde{f}$ by the H_4 gadget applied on variables x_1 and x_2 of f. We have $\widetilde{f}_{12}^{00}(\vec{0}^{2n-2}) = f(\alpha) + f(\gamma) = 2$ and $\widetilde{f}_{12}^{01}(1\vec{0}^{2n-3}) = f(\beta) + f(\delta) = f(\beta)$ since $f(\delta) = 0$. Remember that since $f \in \int_{\mathcal{B}} \mathscr{A}$, by Lemma 7.23, for all $(a, b) \in \mathbb{Z}_2^2$, $\widetilde{f}_{12}^{ab} \in \mathscr{A}$ and we use n_{ab} to denote the norm of its nonzero entries. Thus, $n_{00} = 2$ and $n_{01} = 1$. Also, we have $f(\beta) \neq 0$ which is the same as $1\vec{0}^{2n-3} \in \mathscr{S}(f_{12}^{01})$, and $f(\delta) = 0$ which is the same as $1\vec{0}^{2n-3} \notin \mathscr{S}(f_{12}^{10})$. By Lemma 7.34,

$\mathscr{S}(f_{12}^{01}) \cap \mathscr{S}(f_{12}^{10}) = \emptyset$. Remember that $\widetilde{f}_{12}^{01} = f_{12}^{01} + f_{12}^{10}$ and $\widetilde{f}_{12}^{10} = f_{12}^{01} - f_{12}^{10}$. Then,

$$\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{S}(f_{12}^{01}) \cup \mathscr{S}(f_{12}^{10}) = \mathscr{S}(\widetilde{f}_{12}^{10}).$$

Consider signatures $\partial_{ij}^{b} f$ for all $\{i,j\}$ disjoint with $\{1,2\}$ and every $b \in \mathcal{B}$. By Lemma 6.4 and its remark, we may assume that either $M(\mathfrak{m}_{12}(\partial_{ij}^{b} f)) = \lambda_{ij}^{b} I_4$ for some real $\lambda_{ij}^{b} \neq 0$, or there exists a nonzero binary signature $g_{ij}^{b} \in \mathcal{O}$ such that $g_{ij}^{b}(x_1, x_2) \mid \partial_{ij}^{b} f$. Otherwise, we get #P-hardness.

Consider the case that $g_{ij}^{b}(x_1, x_2) \mid \partial_{ij}^{b} f$. If $\partial_{ij}^{b} f \equiv 0$, then we can let $g_{ij}^{b} \in \mathcal{B}$ since a zero signature can be divided by any nonzero binary signature. If $\partial_{ij}^{b} f \not\equiv 0$, we can realize g_{ij}^{b} by factorization. If $g_{ij}^{b} \notin \mathcal{B}^{\otimes 1}$, then we get #P-hardness since $\mathcal{F}$ is non-$\mathcal{B}$ hard. Thus, we may assume that $g_{ij}^{b} \in \mathcal{B}$ after normalization. Therefore, for all $\{i,j\}$ disjoint with $\{1,2\}$ and every $b \in \mathcal{B}$, we may assume that either $M(\mathfrak{m}_{12}(\partial_{ij}^{b} f)) = \lambda_{ij}^{b} I_4$ for some real $\lambda_{ij}^{b} \neq 0$, or there exists a nonzero binary signature $g_{ij}^{b} \in \mathcal{B}$ such that $g_{ij}^{b}(x_1, x_2) \mid \partial_{ij}^{b} f$. Then, by Lemma 7.29, $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{O}_{2n-2}$. Thus, $|\mathscr{S}(\widetilde{f}_{12}^{01})| = 2^{2n-3}$.

Now consider again the signature f. Since f satisfies 2ND-ORTH, and all its nonzero entries have norm 1, for any $(a,b) \in \mathbb{Z}_2^2$, $|\mathbf{f}_{12}^{ab}|^2 = |\mathscr{S}(f_{12}^{ab})|$. Then,

$$|\mathscr{S}(f_{12}^{00})| = |\mathscr{S}(f_{12}^{01})| = |\mathscr{S}(f_{12}^{10})| = |\mathscr{S}(f_{12}^{11})|.$$

Remember that $\mathscr{S}(f_{12}^{01}) \cap \mathscr{S}(f_{12}^{10}) = \emptyset$, and $\mathscr{S}(\widetilde{f}_{12}^{01}) = \mathscr{S}(f_{12}^{01}) \cup \mathscr{S}(f_{12}^{10})$. Then, $\mathscr{S}(f_{12}^{00})$ and $\mathscr{S}(f_{12}^{01})$ form an equal size partition of $\mathscr{S}(\widetilde{f}_{12}^{01})$. Thus, $|\mathscr{S}(f_{12}^{01})| = |\mathscr{S}(f_{12}^{10})| = \frac{1}{2}|\mathscr{S}(\widetilde{f}_{12}^{01})| = 2^{2n-4}$. Also, $|\mathscr{S}(f_{12}^{00})| = |\mathscr{S}(f_{12}^{11})| = 2^{2n-4}$. Therefore,

$$|\mathscr{S}(f)| = |\mathscr{S}(f_{12}^{00})| + |\mathscr{S}(f_{12}^{01})| + |\mathscr{S}(f_{12}^{10})| + |\mathscr{S}(f_{12}^{11})| = 4 \cdot 2^{2n-4} = 2^{2n-2}.$$

Since all nonzero entries of f have norm 1, $|\mathbf{f}|^2 = |\mathscr{S}(f)| = 2^{2n-2}$. Also, since f satisfies 2ND-ORTH, for all $\{i,j\} \in [2n]$ and all $(a,b) \in \mathbb{Z}_2^2$, $|\mathbf{f}_{ij}^{ab}| = \frac{1}{4}|\mathbf{f}|^2 = 2^{2n-4}$.

We denote $\mathscr{S}(f)$ by S. Since f has even parity, for every $(x_1, \ldots, x_{2n}) \in S$, $x_1 + \cdots + x_{2n} = 0$, i.e., $S \subseteq \mathscr{E}_{2n}$. Let $F(x_1, \ldots, x_{2n-1}) \in \mathbb{Z}_2[x_1, \ldots, x_{2n-1}]$ be the multilinear polynomial such that

$$F(x_1, \ldots, x_{2n-1}) = \begin{cases} 1, & (x_1, \ldots, x_{2n-1}, x_{2n}) \in S \\ 0, & (x_1, \ldots, x_{2n-1}, x_{2n}) \notin S \end{cases} \quad \text{where} \quad x_{2n} = \sum_{i=1}^{2n-1} x_i.$$

Then, $S = \{(x_1, \ldots, x_{2n}) \in \mathscr{E}_{2n} \mid F(x_1, \ldots, x_{2n-1}) = 1\}$.

Now, we show that for all $\{i, j\} \subseteq [2n-1]$, $F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1, and also $F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1. For simplicity of notations, we prove this for $\{i, j\} = \{1, 2\}$. The proof for arbitrary $\{i, j\}$ is the same by replacing $\{1, 2\}$ by $\{i, j\}$. Consider

$$S_0 = \mathscr{S}(f_{12}^{00}) = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid F_{12}^{00}(x_3, \ldots, x_{2n-1}) = 1\},$$

and

$$S_1 = \mathscr{S}(f_{12}^{11}) = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid F_{12}^{11}(x_3, \ldots, x_{2n-1}) = 1\}.$$

Then,

$$S_0 \cap S_1 = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid F_{12}^{00} \cdot F_{12}^{11} = 1\},$$

and

$$S_0 \cup S_1 = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid F_{12}^{00} + F_{12}^{11} + F_{12}^{00} \cdot F_{12}^{11} = 1\}.$$

By Lemma 7.34, $S_0 = S_1$ or $S_0 \cap S_1 = 0$.

- If $S_0 = S_1$, then for every $(x_3, \ldots, x_{2n-1}) \in \mathbb{Z}_2^{2n-3}$ which decides every $(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2}$ by $x_{2n} = x_3 + \cdots + x_{2n-1}$,

  $$F_{12}^{00}(x_3, \ldots, x_{2n-1}) = F_{12}^{11}(x_3, \ldots, x_{2n-1}).$$

  Thus, $F_{12}^{00} + F_{12}^{11} \equiv 0$.

- If $S_0 \cap S_1 = \emptyset$, then since $|S_0| = |S_1| = 2^{2n-4}$ (which is still true when replacing $\{1, 2\}$ by an arbitrary $\{i, j\}$), $|S_0 \cup S_1| = |S_0| + |S_1| = 2^{2n-3}$. Since $S_0 \cup S_1 \subseteq \mathscr{E}_{2n-2}$ and $|\mathscr{E}_{2n-2}| = 2^{2n-3}$, $S_0 \cup S_1 = \mathscr{E}_{2n-2}$. Thus, for every $(x_3, \ldots, x_{2n-1}) \in \mathbb{Z}_2^{2n-3}$ which decides every $(x_3, \ldots, x_{2n}) \in$

$\mathscr{E}_{2n-2}$ by $x_{2n} = x_3 + \cdots + x_{2n-1}$,

$$F_{12}^{00}(x_3, \ldots, x_{2n-1}) \cdot F_{12}^{11}(x_3, \ldots, x_{2n-1}) = 0,$$

and

$$F_{12}^{00}(x_3, \ldots, x_{2n-1}) + F_{12}^{11}(x_3, \ldots, x_{2n-1}) + F_{12}^{00} \cdot F_{12}^{11}(x_3, \ldots, x_{2n-1}) = 1.$$

Thus, $F_{12}^{00} + F_{12}^{11} \equiv 1$.

Similarly, we can show that $F_{12}^{01} + F_{12}^{10} \equiv 0$ or 1. Therefore, for all $\{i, j\} \subseteq [2n-1]$, $F_{ij}^{00} + F_{ij}^{11} \equiv 0$ or 1 and $F_{ij}^{01} + F_{ij}^{10} \equiv 0$ or 1. By Lemma 7.26, $d(F) \leqslant 2$.

If $d(F) \leqslant 1$, then clearly, $S = \{(x_1, \ldots, x_{2n}) \in \mathscr{E}_{2n} \mid F(x_1, \ldots, x_{2n-1}) = 1\}$ is an affine linear space. Thus, f has affine support. Otherwise, $d(F) = 2$. By Lemma 7.26, F is a complete quadratic polynomial. Consider signatures f_{12}^{00} and f_{12}^{11}. Remember that $f(000\vec{0}^{2n-3}) = f(110\vec{0}^{2n-3}) = 1$. Thus, $\vec{0}^{2n-2} \in S_0 \cap S_1 \neq \emptyset$. Then, $S_0 = S_1$. Let

$$S_+ = \{\alpha \in S_0 \mid f_{12}^{00}(\alpha) = f_{12}^{11}(\alpha)\} \text{ and } S_- = \{\alpha \in S_0 \mid f_{12}^{00}(\alpha) = -f_{12}^{11}(\alpha)\}.$$

Then, as f takes ±1 values on its support, $S_+ = \mathscr{S}(\partial_{12}^+ f)$ and $S_- = \mathscr{S}(\partial_{12}^- f)$. Since $\partial_{12}^+ f, \partial_{12}^- f \in \mathscr{A}$, S_+ and S_- are affine linear subspaces of $\mathscr{E}_{2n-2}$. Also, by 2nd-Orth, $\langle \mathbf{f}_{12}^{00}, \mathbf{f}_{12}^{11} \rangle = |S_+| - |S_-| = 0$. Thus, $|S_+| = |S_-| = \frac{1}{2}|S_0| = 2^{2n-5}$. Since $|\mathscr{E}_{2n-2}| = 2^{2n-3}$, S_+ is a an affine linear subspaces of $\mathscr{E}_{2n-2}$ decided by two affine linear constraints $L_1^+ = 1$ and $L_2^+ = 1$. (Here both L_1^+ and L_2^+ are *affine* linear forms which may have nonzero constant terms, but we write the constraints as $L_1^+ = 1$ and $L_2^+ = 1$.) In other words,

$$S_+ = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid L_1^+ = 1 \text{ and } L_2^+ = 1\} = \{(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2} \mid L_1^+ \cdot L_2^+ = 1\}.$$

Since for every $(x_3, \ldots, x_{2n}) \in \mathscr{E}_{2n-2}$, $x_3 + \cdots + x_{2n} = 0$, we may substitute the appearance of x_{2n} in L_1^+ and L_2^+ by $x_3 + \cdot + x_{2n-1}$. Thus, we may assume that $L_1^+, L_2^+ \in \mathbb{Z}_2[x_3, \ldots, x_{2n-1}]$, and $d(L_1^+) = d(L_2^+) = 1$. Similarly, there exist $L_1^-, L_2^- \in \mathbb{Z}_2[x_3, \ldots, x_{2n-1}]$ with $d(L_1^-) = d(L_2^-) = 1$

such that

$$S_- = \{(x_3, \dots, x_{2n}) \in \mathscr{E}_{2n-2} \mid L_1^- = 1 \text{ and } L_2^- = 1\} = \{(x_3, \dots, x_{2n}) \in \mathscr{E}_{2n-2} \mid L_1^- \cdot L_2^- = 1\}.$$

Clearly, $S_+ \cap S_- = \emptyset$. Then

$$S_+ \cup S_- = \{(x_3, \dots, x_{2n}) \in \mathscr{E}_{2n-2} \mid L_1^+ \cdot L_2^+ + L_1^- \cdot L_2^- = 1\}.$$

Remember that

$$S_0 = S_+ \cup S_- = \{(x_3, \dots, x_{2n}) \in \mathscr{E}_{2n-2} \mid F_{12}^{00} = 1\}.$$

Thus, $L_1^+ \cdot L_2^+ + L_1^- \cdot L_2^- = F_{12}^{00}$. Since for all $1 \leqslant i < j \leqslant 2n-1$, the quadratic term x_ix_j appears in F, for all $3 \leqslant i < j \leqslant 2n-1$, the quadratic term x_ix_j appears in F_{12}^{00}. Thus, $F_{12}^{00} \in \mathbb{Z}_2[x_3, \dots, x_{2n-1}]$ is a complete quadratic polynomial over $2n-3$ variables and it has a twice-linear 2-partition. Since $2n \geqslant 8$, $2n-3 \geqslant 5$. By Lemma 7.33, we have $2n-3 = 5$, and after renaming variables,

$$F = (x_3 + x_4 + a)(x_4 + x_5 + b) + (x_3 + x_4 + x_5 + x_6 + c)(x_3 + x_4 + x_5 + x_7 + d)$$

where $a, b, c, d \in \mathbb{Z}_2$. Without loss of generality, we may assume that $L_1^+ \cdot L_2^+ = (x_3 + x_4 + a)(x_4 + x_5 + b)$. Then,

$$S_+ = \mathscr{S}(\partial_{12}^+ f) = \{(x_3, \dots, x_8) \in \mathscr{E}_{2n-2} \mid x_3 = x_4 + a \text{ and } x_4 = x_5 + b\},$$

for some $a, b \in \mathbb{Z}_2$.

Clearly $\partial_{12}^+ f$ is a 6-ary signature and $|\mathscr{S}(\partial_{12}^+ f)| = 2^{5-2} = 2^3$. We show that $\partial_{12}^+ f \notin \mathcal{B}^{\otimes 3} \cup \mathcal{F}_6 \cup \mathcal{F}_6^H$. Then, by Corollary 7.11, we get #P-hardness. Since the support of a signature in $\mathcal{F}_6 \cup \mathcal{F}_6^H$ is either $\mathscr{E}_6$ or $\mathscr{O}_6$ whose sizes are both 2^5. Thus, $\partial_{12}^+ f \notin \mathcal{F}_6 \cup \mathcal{F}_6^H$. For any 6-ary signature g in $\mathcal{B}^{\otimes 3}$, its 6 variables can be divided into three independent pairs such that on the support $\mathscr{S}(g)$, the values of variables inside each pair do not rely on the values of variables of other pairs. Thus, if we pick any three variables in $\mathscr{S}(g)$, the degree of freedom of them is at least 2; more precisely, there are at least 4 assignments on these three variables which can be extended to an input in $\mathscr{S}(g)$. However, in $\mathscr{S}(\partial_{12}^+ f)$, the degree of freedom of variables x_3, x_4, x_5 is only 1, namely there are only two assignments on x_3, x_4, x_5 that can be extended to an input in $\mathscr{S}(\partial_{12}^{+} f)$. Thus, $\partial_{12}^{+} f \notin \mathcal{B}^{\otimes 3}$. This completes the proof of Lemma 7.35. □

7.3.4 Affine Signature Condition

Finally, by further assuming that f has affine support, we consider whether f itself is an affine signature. We prove that this is true only for signature of arity $2n \geqslant 10$. For signature f of arity $2n = 8$, we show that either $f \in \mathscr{A}$ or the following signature is realizable.

$$h_8 = \chi_T \cdot (-1)^{x_1x_2x_3 + x_1x_2x_5 + x_1x_3x_5 + x_2x_3x_5}, \text{ where } T = \mathscr{S}(h_8) = \mathscr{S}(f_8).$$

Note that in the support $\mathscr{S}(f_8)$ (see its definition (7.11) for this *Queen of the Night* f_8), by taking x_1, x_2, x_3, x_5 as free variables, the remaining 4 variables are mod 2 sums of $\binom{4}{3}$ subsets of $\{x_1, x_2, x_3, x_5\}$. Clearly, h_8 is not affine, but it has affine support and all its nonzero entries have the same norm. One can check that h_8 satisfies 2ND-ORTH and $h_8 \in \int_{\mathcal{B}} \mathscr{A}$. But fortunately, we show that by merging h_8, we can realize a 6-ary signature that is not in $\mathcal{B}^{\otimes} \cup \mathcal{F}_6 \cup \mathcal{F}_6^H$. By Corollary 7.11, we are done.

After we give one more result about multilinear boolean polynomials, we make our final step towards Theorem 7.38.

Lemma 7.36. *Let $F(x_1, \dots, x_n) \in \mathbb{Z}_2[x_1, \dots, x_n]$ be a complete cubic polynomial, $L(x_2, \dots, x_n) \in \mathbb{Z}_2[x_2, \dots, x_n]$ and $d(L) \leqslant 1$. If we substitute x_1 by $x_{n+1} + L(x_2, \dots, x_n)$ in F to get F', and suppose $F'(x_2, \dots, x_{n+1}) = F(x_{n+1} + L, x_2, \dots, x_n) \in \mathbb{Z}_2[x_2, \dots, x_{n+1}]$ is also a complete cubic polynomial, then*

- *If $n \geqslant 5$, then L must be a constant $\epsilon = 0$ or 1.*
- *If $n = 4$, then L must be either ϵ, or of the form $x_i + x_j + \epsilon$, for some $\epsilon = 0$ or 1, for some $\{i, j\} \in \{2, 3, 4\}$.*

证明. Since $F(x_1, \dots, x_n)$ is a complete cubic polynomial, we can write it as

$$F(x_1, \dots, x_n) = x_1 \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j + \sum_{2 \leqslant i < j < k \leqslant n} x_i x_j x_k + G(x_1, \dots, x_n)$$

where $d(G) \leqslant 2$. Then,

$$F'(x_2, \ldots, x_n, x_{n+1}) = (x_{n+1} + L) \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j + \sum_{2 \leqslant i < j < k \leqslant n} x_i x_j x_k + G(x_{n+1} + L, \ldots, x_n).$$

Let $G'(x_2, \ldots, x_n, x_{n+1}) = G(x_{n+1} + L, \ldots, x_n)$. Since $d(L) \leqslant 1$ and $d(G) \leqslant 2$, $d(G') \leqslant 2$. Then, there is no cubic term in $G'(x_2, \ldots, x_n, x_{n+1})$. Since $F'(x_2, \ldots, x_n, x_{n+1})$ is a complete cubic polynomial over variables $(x_2, \ldots, x_n, x_{n+1})$ and $x_{n+1} \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j + \sum_{2 \leqslant i < j < k \leqslant n} x_i x_j x_k$ already gives every cubic term over $(x_2, \ldots, x_n, x_{n+1})$ exactly once, there is no cubic term in $L \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j$ (after taking module 2). If $L \equiv 0$ or 1, then we are done. Otherwise, there is a variable that appears in L. Without loss of generality, we may assume that $x_2 \in L$ (i.e., x_2 appears in L).

Let $Q(x_3, \ldots, x_n) = \sum_{3 \leqslant i < j \leqslant n} x_i x_j \in \mathbb{Z}_2[x_3, \ldots, x_n]$. Since $n \geqslant 4$, we have $Q \not\equiv 0$. For every $x_i x_j \in Q$, since $x_2 \in L$, the cubic term $x_2 x_i x_j$ will appear in $L \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j$. To cancel it, exactly one between $x_i \cdot x_2 x_j$ and $x_j \cdot x_2 x_i$ must also appear in $L \cdot \sum_{2 \leqslant i < j \leqslant n} x_i x_j$. Thus, exactly one between x_i and x_j appears in L.

If $n \geqslant 5$, then $x_3 x_4, x_4 x_5, x_3 x_5 \in Q$. Thus, exactly one between x_3 and x_4 is in L, exactly one between x_4 and x_5 is in L, and exactly one between x_3 and x_5 is in L. Clearly, this is a contradiction.

If $n = 4$, then $Q = x_3 x_4$. Either x_3 or x_4 appears in L. Thus, L is a sum of two variables among $\{x_2, x_3, x_4\}$ plus a constant 0 or 1. □

Lemma 7.37. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition (T), and $\mathcal{F}$ is non-$\mathcal{B}$ hard. If $\mathcal{F}$ contains an irreducible $2n$-ary signature f with parity where $2n \geqslant 8$, then*

- $\operatorname{Holant}^b(\mathcal{F})$ *is #P-hard, or*
- *there is a signature $g \notin \mathscr{A}$ of arity $2k < 2n$ that is realizable from f and $\mathcal{B}$, or*
- *$f \in \mathscr{A}$.*

证明. Again, we may assume that f satisfies 2ND-ORTH and $f \in \int_{\mathcal{B}} \mathscr{A}$. Also by Lemmas 7.27 and 7.35, we may assume that $f(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(f)$ and $\mathscr{S}(f)$ is an affine linear space. Let $\{x_1, \ldots, x_m\}$ be a set of free variables of $\mathscr{S}(f)$. Then, on the support $\mathscr{S}(f)$, every variable x_i

$(1 \leqslant i \leqslant 2n)$ is expressible as a unique affine linear combination over $\mathbb{Z}_2$ of these free variables, i.e., $x_i = L_i(x_1, \ldots, x_m) = \lambda_i^0 + \lambda_i^1 x_1 + \ldots + \lambda_i^m x_m$, where $\lambda_i^0, \ldots, \lambda_i^m \in \mathbb{Z}_2$. Clearly, for $1 \leqslant i \leqslant m$, $L(x_i) = x_i$. Then,

$$\begin{aligned}\mathscr{S}(f) &= \{(x_1, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n} \mid x_1 = L_1, \ldots, x_{2n} = L_{2n}\}\\ &= \{(x_1, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n} \mid x_{m+1} = L_{m+1}, \ldots, x_{2n} = L_{2n}\}.\end{aligned}$$

Also, let $I(x_i) = \{1 \leqslant k \leqslant m \mid \lambda_i^k = 1\}$. Clearly, for $1 \leqslant i \leqslant m$, $I(x_i) = \{i\}$. For $m+1 \leqslant i \leqslant 2n$, we show that $|I_{x_i}| \geqslant 2$. For a contradiction, suppose that there exists $m+1 \leqslant i \leqslant 2n$ such that $|I_{x_i}| = 0$ or 1. If $|I_{x_i}| = 0$, then x_i takes a constant value in $\mathscr{S}$. Then, among f_i^0 and f_i^1, one is a zero signature. Thus, f is reducible. Contradiction. If $|I_{x_i}| = 1$, then $x_i = x_k$ or $x_k + 1$ for some free variable x_k. Then, among f_{ik}^{00}, f_{ik}^{01}, f_{ik}^{10} and f_{ik}^{11}, two are zero signatures. Thus, f does not satisfy 2nd-Orth. Contradiction.

Since $f(\alpha) = \pm 1$ for all $\alpha \in \mathscr{S}(f)$ and each $\alpha \in \mathscr{S}(f)$ can be uniquely decided by its value on the first m free variables, there exists a unique multilinear boolean polynomial $F(x_1, \ldots, x_m) \in \mathbb{Z}_2[x_1, \ldots, x_m]$ such that

$$f(x_1, \ldots, x_m, \ldots, x_{2n}) = \chi_S (-1)^{F(x_1, \ldots, x_m)}$$

where $S = \mathscr{S}(f)$. If $d(F) \leqslant 2$, then clearly $f \in \mathscr{A}$. We are done. Thus, we may assume that $d(F) > 2$ and hence $m > 2$. Remember that F_{ij}^{ab} denotes the polynomial obtained by setting variables (x_i, x_j) of F to $(a, b) \in \mathbb{Z}_2^2$. Then, $f_{ij}^{ab} = (-1)^{F_{ij}^{ab}}$ on $\mathscr{S}(f)$. We will show that for all $i, j \in [m]$, $d(F_{ij}^{00} + F_{ij}^{11}) \leqslant 1$ and $d(F_{ij}^{01} + F_{ij}^{10}) \leqslant 1$. For brevity of notation, we prove this for $\{i, j\} = \{1, 2\}$. The proof for arbitrary $\{i, j\}$ is the same by replacing $\{1, 2\}$ with $\{i, j\}$. We first show that $d(F_{ij}^{00} + F_{ij}^{11}) \leqslant 1$. We use S_0 to denote $\mathscr{S}(f_{ij}^{00})$ and S_1 to denote $\mathscr{S}(f_{ij}^{11})$. By Lemma 7.34, there are two cases, $S_0 = S_1$ or $S_0 \cap S_1 = \emptyset$.

- Suppose that $S_0 = S_1$. For convenience, we use L_i^0 to denote $(L_i)_{12}^{00}$ and L_i^1 to denote $(L_i)_{12}^{11}$. Then,

$$\begin{aligned}S_0 =& \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_{m+1} = L_{m+1}^0, \ldots, x_{2n} = L_{2n}^0\}\\ S_1 =& \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_{m+1} = L_{m+1}^1, \ldots, x_{2n} = L_{2n}^1\}.\end{aligned}$$

So $L_i^0 \equiv L_i^1$ for all $i \geqslant m+1$. Thus, either $\{1,2\} \subseteq I(x_i)$ or $\{1,2\} \cap I(x_i) = \emptyset$ for $i \geqslant m+1$. Let $S_+ = \{\alpha \in S_0 \mid f_{ij}^{00}(\alpha) = f_{ij}^{11}(\alpha)\}$ and $S_- = \{\alpha \in S_0 \mid f_{ij}^{00}(\alpha) = -f_{ij}^{11}(\alpha)\}$. Then, $\langle \mathbf{f}_{ij}^{00}, \mathbf{f}_{ij}^{11} \rangle = 1 \cdot |S_+| - 1 \cdot |S_-| = 0$. Since $S_0 = S_+ \cup S_-$, $|S_+| = |S_-| = \frac{1}{2}|S_0|$. Note that $\mathscr{S}(\partial_{12} f) = S_+$ and $\mathscr{S}(\partial_{12}^- f) = S_-$. By our assumption that $f \in \int_{\mathcal{B}} \mathscr{A}$, $\partial_{12} f, \partial_{12}^- f \in \mathscr{A}$. Thus, both S_+ and S_- are affine linear subspaces of $S_0 = S_1$. Since $|S_+| = |S_-| = |S_0|/2$, there exists an (affine) linear polynomial $L(x_3, \ldots, x_{2n})$ such that

$$S_+ = \{(x_3, \ldots, x_{2n}) \in S_0 \mid L(x_3, \ldots, x_{2n}) = 0\},$$

and

$$S_- = \{(x_3, \ldots, x_{2n}) \in S_0 \mid L(x_3, \ldots, x_{2n}) = 1\}.$$

For $(x_3, \ldots, x_{2n}) \in S_0$, and $i \geqslant m+1$, we can substitute the variable x_i that appears in $L(x_3, \ldots, x_{2n})$ with $L_i^0 \equiv L_i^1$. Then, we get an (affine) linear polynomial $L'(x_3, \ldots, x_m) \in \mathbb{Z}_2[x_1, \ldots, x_m]$ such that $L'(x_3, \ldots, x_m) = L(x_3, \ldots, x_m, x_{m+1}, \ldots, x_{2n})$ for $(x_3, \ldots, x_{2n}) \in S_0$. Thus,

$$S_+ = \{(x_3, \ldots, x_{2n}) \in S_0 \mid L'(x_3, \ldots, x_m) = 0\},$$

and

$$S_- = \{(x_3, \ldots, x_{2n}) \in S_0 \mid L'(x_3, \ldots, x_m) = 1\}.$$

Note that as $|S_+| = |S_-| > 0$, the affine linear polynomial L' is non-constant, i.e., $d(L') = 1$. Then, for every $(x_3, \ldots, x_m) \in \mathbb{Z}_2^{m-2}$,

$$(-1)^{F_{12}^{00}(x_3, \ldots, x_m)} = (-1)^{F_{12}^{11}(x_3, \ldots, x_m)} \text{ if } L'(x_3, \ldots, x_m) = 0$$

and

$$(-1)^{F_{12}^{00}(x_3, \ldots, x_m)} = -(-1)^{F_{12}^{11}(x_3, \ldots, x_m)} \text{ if } L'(x_3, \ldots, x_m) = 1.$$

Thus,

$$(-1)^{F_{12}^{00}(x_3, \ldots, x_m) + F_{12}^{11}(x_3, \ldots, x_m)} = (-1)^{L'(x_3, \ldots, x_m)}.$$

Therefore, $F_{12}^{00}(x_3, \ldots, x_m) + F_{12}^{11}(x_3, \ldots, x_m) \equiv L'(x_3, \ldots, x_m)$. Then, $d(F_{12}^{00} + F_{12}^{11}) = 1$.

- Suppose that $S_0 \cap S_1 = \emptyset$. Then, there exists a variable x_i where $i \geqslant m+1$ such that between $\{1,2\}$, exactly one index is in $I(x_i)$. Without loss of generality, we may assume that $i = m+1$, $1 \in I(x_{m+1})$ and $2 \notin I(x_{m+1})$. Then, $x_{m+1} = x_1 + K(x_3, \ldots, x_m)$ where $K \in \mathbb{Z}_2[x_3, \ldots, x_m]$ is an (affine) linear polynomial. Consider S_0.

$$S_0 = \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_1 = x_2 = 0, x_{m+1} = x_1 + K, x_{m+2} = L_{m+2} \ldots, x_{2n} = L_{2n}\}.$$

Since $x_1 = x_2$ on S_0, for every $i \geqslant m+2$, if x_1 or x_2 appear in L_i, we substitute each one of them with $x_{m+1} + K$. We get a linear polynomial $K_i \in \mathbb{Z}_2[x_3, \ldots, x_m, x_{m+1}]$. Then, for every $(x_3, \ldots, x_{2n}) \in S_0$, $L_i = K_i$. Thus,

$$S_0 = \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_{m+1} + K = 0, x_{m+2} = K_{m+2} \ldots, x_{2n} = K_{2n}\}.$$

Similarly, we have

$$S_1 = \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_{m+1} + K = 1, x_{m+2} = K_{m+2} \ldots, x_{2n} = K_{2n}\}.$$

Let $S_\cup = S_0 \cup S_1$. Then,

$$S_\cup = \{(x_3, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n-2} \mid x_{m+2} = K_{m+2} \ldots, x_{2n} = K_{2n}\}.$$

Thus, we can pick $x_3, \ldots, x_m, x_{m+1}$ as a set of free variables of $S_\cup$.

Consider $g = \partial_{12} f$. Clearly, $\mathscr{S}(g) = S_\cup$ since $S_0 \cap S_1 = \emptyset$. Then, there exists a unique multilinear boolean polynomial $G(x_3, \ldots, x_{m+1}) \in \mathbb{Z}_2[x_3, \ldots, x_{m+1}]$ such that

$$g(x_3, \ldots, x_{2n}) = \chi_{S_\cup} \cdot (-1)^{G(x_3, \ldots, x_{m+1})}.$$

For every $(x_3, \ldots, x_{2n}) \in S_0$ that is uniquely decided by $(0, 0, x_3, \ldots, x_m) \in \{(0,0)\} \times \mathbb{Z}_2^{m-2}$, $x_{m+1} = K(x_3, \ldots, x_m)$ and $f_{12}^{00}(x_3, \ldots, x_{2n}) = g(x_3, \ldots, x_{2n})$. Thus, for every $(x_3, \ldots, x_m) \in \mathbb{Z}_2^{m-2}$,

$$(-1)^{F_{12}^{00}(x_3, \ldots, x_m)} = (-1)^{G(x_3, \ldots, x_m, K)}.$$

Also, for every $(x_3, \ldots, x_{2n}) \in S_1$ that is uniquely decided by $(1, 1, x_3, \ldots, x_m) \in \{(1, 1)\} \times \mathbb{Z}_2^{m-2}$, $x_{m+1} = K(x_3, \ldots, x_m) + 1$, and $f_{12}^{11}(x_3, \ldots, x_{2n}) = g(x_3, \ldots, x_{2n})$. Thus, for every $(x_3, \ldots, x_m) \in \mathbb{Z}_2^{m-2}$,

$$(-1)^{F_{12}^{11}(x_3,\ldots,x_m)} = (-1)^{G(x_3,\ldots,x_m,K+1)}.$$

Thus, $F_{12}^{00}(x_3, \ldots, x_m) \equiv G(x_3, \ldots, x_m, K)$ and $F_{12}^{11}(x_3, \ldots, x_m) \equiv G(x_3, \ldots, x_m, K + 1)$.

Since $f \in \int_{\mathcal{B}} \mathscr{A}$, $g = \partial_{12} f \in \mathscr{A}$. Thus,

$$g'(x_3, \ldots, x_m, x_{m+1}) = (-1)^{G(x_3,\ldots,x_m,x_{m+1})}$$

is also in $\in \mathscr{A}$. Let $y = x_{m+1} + K(x_3, \ldots, x_m) \in \mathbb{Z}[x_3, \ldots, x_{m+1}]$ be an affine linear combination of variables $x_3, \ldots, x_{m+1}$. Since $g \in \mathscr{A}$, by Lemma 2.11,

$$d[G(x_3, \ldots, x_m, K) + G(x_3, \ldots, x_m, K + 1)] \leqslant 1.$$

Thus, $d(F_{12}^{00} + F_{12}^{11}) \leqslant 1$. Also if $d(G) = 1$, then by Lemma 2.11

$$d(F_{12}^{00} + F_{12}^{11}) = 0, \text{ i.e., } F_{12}^{00} + F_{12}^{11} \equiv 0 \text{ or } 1. \tag{7.17}$$

Similarly, we can show that $d(F_{12}^{01} + F_{12}^{10}) \leqslant 1$. Thus, for all $i, j \in [m]$, $d(F_{ij}^{00} + F_{ij}^{11}) \leqslant 1$ and $d(F_{ij}^{01} + F_{ij}^{10}) \leqslant 1$. By Lemma 7.26, $d(F) \leqslant 3$.

If $d(F) \leqslant 2$, then clearly $f \in \mathscr{A}$. We are done. Otherwise, $d(F) = 3$ and by Lemma 7.26, F is a complete cubic multilinear polynomial over m variables. If we pick another set X of m free variables and substitute variables of F by variables in X, then we will get a cubic multilinear polynomial F' over variables in X. Same as the analysis of F, F' is also a complete cubic polynomial. In particular, consider the variable x_{m+1}. Recall that $|I(x_{m+1})| \geqslant 2$. Without loss of generality, we assume that $1 \in I(x_{m+1})$. Then, $x_{m+1} = x_1 + L(x_2, \ldots, x_m)$ where $L(x_2, \ldots, x_m)$ is an affine linear combination of variables $x_2, \ldots, x_m$. We substitute x_1 in F by $x_{m+1} + L$, and we get a complete cubic multilinear polynomial $F'(x_2, \ldots, x_{m+1}) \in \mathbb{Z}_2[x_2, \ldots, x_{m+1}]$. By Lemma 7.36, if $m \geqslant 5$, then $x_{m+1} = x_1$ or $x_{m+1} = \overline{x_1}$. Thus, $I(x_{m+1}) = \{1\}$. This contradicts with $|I(x_{m=1})| \geqslant 2$. Thus, $m \leqslant 4$.

If $m = 4$, then by Lemma 7.36, $x_5 = x_1 + \epsilon$, or $x_5 = x_1 + x_i + x_j + \epsilon$, where $\epsilon = 0$ or 1, for some $2 \leqslant i < j \leqslant 4$. Since $|I(x_5)| \geqslant 2$, the case that $x_5 = x_1 + \epsilon$ is impossible. Similarly, for $i \geqslant m + 2$, the variable x_i is a sum of three variables in $\{x_1, x_2, x_3, x_4\}$ plus a constant 0 or 1. If there exist x_i and x_j for $5 \leqslant i < j \leqslant 2n$ such that $I(x_i) = I(x_j)$. Then, $x_i = x_j$ or $\overline{x_j}$. Thus, among f^{00}_{ij}, f^{01}_{ij}, f^{10}_{ij} and f^{11}_{ij}, two are zero signatures. Thus, f does not satisfy 2nd-Orth. Contradiction. Thus, $I(x_i) \neq I(x_j)$ for any $5 \leqslant i < j \leqslant 2n$. There are only $\binom{4}{3} = 4$ ways to pick three variables from $\{x_1, x_2, x_3, x_4\}$. Thus, $2n \leqslant 4 + 4 = 8$. By the hypothesis $2n \geqslant 8$ of the lemma, we have $2n = 8$. Clearly, $|\mathscr{S}(f)| = 2^4 = 16$. Due to 2nd-Orth, for all $\{i, j\} \in [8]$, $|\mathscr{S}(f^{00}_{ij})| = |\mathscr{S}(f^{01}_{ij})| = |\mathscr{S}(f^{10}_{ij})| = |\mathscr{S}(f^{11}_{ij})| = 4$.

- If there exists $\{i, j\}$ such that $\mathscr{S}(f^{00}_{ij}) = \mathscr{S}(f^{11}_{ij})$, then for any point α in $\mathscr{S}(f^{00}_{ij}) = \mathscr{S}(f^{11}_{ij})$, regardless whether $f^{00}_{ij}(\alpha) = f^{11}_{ij}(\alpha)$ or $f^{00}_{ij}(\alpha) = -f^{11}_{ij}(\alpha)$, either $\alpha \in \mathscr{S}(\partial^+_{ij} f)$ or $\alpha \in \mathscr{S}(\partial^-_{ij} f)$. Thus,

  $$\mathscr{S}(\partial^+_{ij} f) \cup \mathscr{S}(\partial^-_{ij} f) = \mathscr{S}(f^{00}_{ij}) = \mathscr{S}(f^{11}_{ij}).$$

  Also, by 2nd-Orth,

  $$\langle \mathbf{f}^{00}_{ij}, \mathbf{f}^{11}_{ij} \rangle = |\mathscr{S}(\partial^-_{ij} f)| - |\mathscr{S}(\partial^+_{ij} f)| = 0.$$

  Thus, $|\mathscr{S}(\partial^+_{ij} f)| = |\mathscr{S}(\partial^-_{ij} f)| = 2$. Note that every 6-ary signature in $\mathcal{B}^{\otimes}$ has support of size 8, and every signature in $\mathcal{F}_6$ and $\mathcal{F}^H_6$ has support of size 32. Thus, $\partial^+_{ij} f \notin \mathcal{B} \cup \mathcal{F}_6 \cup \mathcal{F}^H_6$. Then, by Corollary 7.11, we get #P-hardness. Similarly, if there exists $\{i, j\}$ such that $\mathscr{S}(f^{01}_{ij}) = \mathscr{S}(f^{10}_{ij})$, then we have $|\mathscr{S}(\widehat{\partial}^{+}_{ij} f)| = |\mathscr{S}(\widehat{\partial}^{-}_{ij} f)| = 2$. Thus, $\widehat{\partial}^{+}_{ij} f \notin \mathcal{B}^{\otimes} \cup \mathcal{F}_6 \cup \mathcal{F}^H_6$. Again, we get #P-hardness.

- Otherwise, for all $\{i, j\} \in [8]$, $\mathscr{S}(f^{00}_{ij}) \cap \mathscr{S}(f^{11}_{ij}) = \emptyset$ and $\mathscr{S}(f^{01}_{ij}) \cap \mathscr{S}(f^{10}_{ij}) = \emptyset$. Then, $\mathscr{S}(\partial^+_{ij} f) = \mathscr{S}(f^{00}_{ij}) \cup \mathscr{S}(f^{11}_{ij})$. Thus, $|\mathscr{S}(\partial^+_{ij} f)| = 8$. Clearly, $\partial^+_{ij} f \notin \mathcal{F}_6 \cup \mathcal{F}^H_6$. If $\partial^+_{ij} f \notin \mathcal{B}^{\otimes 3}$, then we get #P-hardness. For a contradiction, suppose that $\partial^+_{ij} f \in \mathcal{B}^{\otimes 3}$. Then,

  $$\partial^+_{ij} f = \chi_{\mathscr{S}(\partial^+_{ij} f)} (-1)^{G^+_{ij}} \quad \text{where} \quad d(G^+_{ij}) = 1.$$

  As we proved above in equation (7.17), $F^{00}_{ij} + F^{11}_{ij} \equiv 0$ or 1. Similarly, suppose $\widehat{\partial}^{+}_{ij} f \in \mathcal{B}^{\otimes 3}$, and we can show that $F^{01}_{ij} + F^{10}_{ij} \equiv 0$ or 1. Thus, for all $\{i, j\} \subseteq [8]$, $F^{00}_{ij} + F^{11}_{ij} \equiv 0$ or 1 and $F^{01}_{ij} + F^{10}_{ij} \equiv 0$ or 1. Then, by Lemma 7.26, $d(F) \leqslant 2$. Contradiction.

Suppose that $m = 3$. Remember that for $4 \leqslant i \leqslant 2n$, $|I(x_i)| \geqslant 2$. Thus, x_i is a sum of at least two variables in $\{x_1, x_2, x_3\}$ plus a constant 0 or 1. Again, if there exist x_i and x_j for $4 \leqslant i < j \leqslant 2n$ such that $I(x_i) = I(x_j)$, then among f_{ij}^{00}, f_{ij}^{01}, f_{ij}^{10} and f_{ij}^{11}, two are zero signatures. Contradiction. Thus, $I(x_i) \neq I(x_j)$ for any $4 \leqslant i < j \leqslant 2n$. There are $\binom{3}{2} + \binom{3}{3} = 4$ different ways to pick at least two variables from $\{x_1, x_2, x_3\}$. Thus, $2n \leqslant 3 + 4 = 7$. Contradiction. □

Theorem 7.38. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity, $\mathcal{F}$ does not satisfy condition* (T)*, and $\mathcal{F}$ is non-$\mathcal{B}$ hard. Then,* $\operatorname{Holant}^b(\mathcal{F})$ *is #P-hard.*

证明. Since $\mathcal{F}$ does not satisfy condition (T), $\mathcal{F}$ contains a signature $f \notin \mathscr{A}$. Suppose that f has arity $2n$. We prove this theorem by induction on $2n$.

If $2n = 2, 4$ or 6, then by Corollary 7.11 and its remark, $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard.

Inductively assume for some $2k \geqslant 6$, $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard when $2n \leqslant 2k$. We consider the case that $2n = 2k + 2 \geqslant 8$. First, suppose that f is reducible. If it is a tensor product of two signatures of odd arity, then we can realize a signature of odd arity by factorization. We get #P-hardness by Theorem 5.35. Otherwise, it is a tensor product of two signatures of even arity that are not both in $\mathscr{A}$ since $f \notin \mathscr{A}$. Then, we can realize a non-affine signature of arity $2m \leqslant 2k$ by factorization. By our induction hypothesis, we get #P-hardness. Thus, we may assume that f is irreducible. If f has no parity, then we get #P-hardness by Lemma 7.17. Thus, we may also assume that f has parity. Then by Lemma 7.37, $\operatorname{Holant}^b(\mathcal{F})$ is #P-hard, or we can realize a non-affine signature of arity $2m \leqslant 2k$. By our induction hypothesis, we get #P-hardness. □

Since $\mathcal{B}$ is realizable from f_6 and $\{f_6\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard for any real-valued $\mathcal{F}$ that does not satisfy condition (T), we have the following result.

Lemma 7.39. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Then,* $\operatorname{Holant}^b(f_6, \mathcal{F})$ *is #P-hard.*

Combining Theorem 7.5 and Lemma 7.39, we have the following result. This concludes Chapter 7, and we are done with the arity 6 case.

Lemma 7.40. *Suppose that $\mathcal{F}$ is a set of real-valued signatures of even arity and $\mathcal{F}$ does not satisfy condition* (T)*. Let $\widehat{\mathcal{F}} = Z^{-1}\mathcal{F}$. If $\widehat{\mathcal{F}}$ contains a signature $\widehat{f}$ of arity 6 and $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then* $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is #P-hard.*

Chapter 8

Final Obstacle: An 8-ary Signature with the Strong Bell Property

We have seen some extraordinary properties of the signature f_8. Now, we formally analyze it. The existence of f_8 presented a more formidable obstacle to the induction proof. In order to handle it, We introduce Holant problems with limited appearances and give a novel reduction from $\operatorname{Holant}^b(f_8, \mathcal{F})$ to $\operatorname{Holant}(f_8, \mathcal{F})$. We prove a #P-hardness result for $\operatorname{Holant}(f_8, \mathcal{F})$. Finally, we show that our induction proof works for signatures of arity $2n \geqslant 10$. This finishes the proof of the dichotomy for real-valued Holant problems.

8.1 The Discovery of f_8

Remember that $f_8 = \chi_T$ where

$$\begin{aligned}
T =& \mathscr{S}(f_8) = \{(x_1, x_2, \dots, x_8) \in \mathbb{Z}_2^8 \mid \ x_1 + x_2 + x_3 + x_4 = 0,\ x_5 + x_6 + x_7 + x_8 = 0, \\
& \qquad\qquad\qquad\qquad\qquad\qquad\quad x_1 + x_2 + x_5 + x_6 = 0,\ x_1 + x_3 + x_5 + x_7 = 0\}. \\
=& \{00000000, 00001111, 00110011, 00111100, 01010101, 01011010, 01100110, 01101001, \\
& \ 10010110, 10011001, 10100101, 10101010, 11000011, 11001100, 11110000, 11111111\}.
\end{aligned} \tag{8.1}$$

One can see that $\mathscr{S}(f_8)$ has the following structure: the sums of the first four variables, and the last four variables are both even; the assignment of the first four variables are either identical to, or complement of the assignment of the last four variables. Another interesting description of $\mathscr{S}(f_8)$ is as follows: One can take 4 variables, called them y_1, y_2, y_3, y_4. Then on the support the remaining 4 variables are mod 2 sums of $\binom{4}{3}$ subsets of $\{y_1, y_2, y_3, y_4\}$, and y_1, y_2, y_3, y_4 are free variables. (However, the 4 variables (y_1, y_2, y_3, y_4) cannot be taken as (x_1, x_2, x_3, x_4) in the above description (8.1). But one *can* take $(y_1, y_2, y_3, y_4) = (x_1, x_2, x_3, x_5)$. More specifically, one can take any 3 variables x_i, x_j, x_k from $\{x_1, \ldots, x_8\}$ first as free variables, which excludes one unique other x_ℓ from the remainder set $X' = \{x_1, \ldots, x_8\} \setminus \{x_i, x_j, x_k\}$, and *then* one can take any one variable $x_r \in X'$ as the 4th free variable. *Then* the remaining 4 variables are the mod 2 sums of $\binom{4}{3}$ subsets of the 4 free variables $\{x_i, x_j, x_k, x_r\}$, and in particular $x_\ell = x_i + x_j + x_k$, on $\mathscr{S}(f_8)$.) We give the following Figure 7 to visualize the signature matrix $M_{1234}(f_8)$. A block with orange color denotes an entry $+1$. Other blank blocks are zeros.

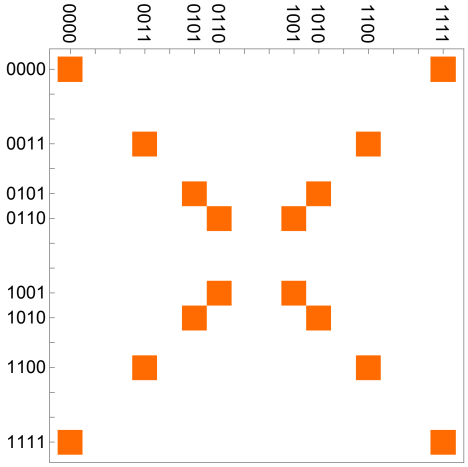


图 7: A visualization of f_8, which happens to be the same as $\widehat{f_8} = Z^{-1} f_8$

One can check that f_8 satisfies both 2ND-ORTH and $f_8 \in \int \mathcal{O}^{\otimes}$. Also, f_8 is unchanged under the holographic transformation by Z^{-1}, i.e., $\widehat{f_8} = Z^{-1} f_8 = f_8$. Now, we show how this extraordinary signature $\widehat{f_8}$ was discovered. We use the notation $\widehat{f_8}$ since we consider the problem $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ for complex-valued $\widehat{\mathcal{F}}$ satisfying ARS. We prove that if $\widehat{\mathcal{F}}$ contains an 8-ary signature $\widehat{f}$ where $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard or $\widehat{f_8}$ is realizable from $\widehat{f}$ (Theorem 8.6).

Remember that $\mathcal{D} = \{\neq_2\}$. Then $\mathcal{D}^{\otimes} = \{\lambda \cdot (\neq_2)^{\otimes n} \mid \lambda \in \mathbb{R}\backslash\{0\}, n \geqslant 1\}$ is the set of tensor products of binary disequalities $\neq_2$ up to a nonzero real scalar. If for all pairs of indices $\{i, j\}$, $\widehat{\partial}_{ij} \widehat{f} \in \mathcal{D}^{\otimes}$, then we say $\widehat{f} \in \int \mathcal{D}^{\otimes}$. Clearly, if $\widehat{f} \in \mathcal{D}^{\otimes}$ and $\widehat{f}$ has arity greater than 2, then $\widehat{f} \in \int \mathcal{D}^{\otimes}$. We first show the following result for signatures of arity at least 8.

Lemma 8.1. *Let $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$ be a signature of arity $2n \geqslant 8$ in $\widehat{\mathcal{F}}$. Then,*

- $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is #P-hard, or*

- *there is a signature $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$ of arity $2k \leqslant 2n-2$ that is realizable from $\widehat{f}$, or*
- *there is an irreducible signature $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$ of arity $2n$ that is realizable from $\widehat{f}$.*

证明. Since $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, $\widehat{f} \not\equiv 0$. Again, we may assume that $\widehat{f}$ is irreducible. Otherwise, by factorization, we can realize a nonzero signature of odd arity and we get #P-hardness by Theorem 5.35, or we can realize a signature of lower even arity that is not in $\widehat{\mathcal{O}}^{\otimes}$ and we are done. Under the assumption that $\widehat{f}$ is irreducible, we may further assume that $\widehat{f}$ satisfies 2ND-ORTH by Lemma 6.6. Consider signatures $\widehat{\partial}_{ij}\widehat{f}$ for all pairs of indices $\{i,j\}$. If there exists a pair $\{i,j\}$ such that $\widehat{\partial}_{ij}\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, then let $\widehat{g} = \widehat{\partial}_{ij}\widehat{f}$, and we are done. Thus, we may also assume that $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$.

If for all pairs of indices $\{i,j\}$, we have $\widehat{\partial}_{ij}\widehat{f} \equiv 0$. Then, by Lemma 3.9, $\widehat{f}(\alpha) = 0$ for all α with $\mathrm{wt}(\alpha) \neq 0$ or $2n$. Since $f \not\equiv 0$ and by ARS, $|\widehat{f}(\vec{0}^{2n})| = |\widehat{f}(\vec{1}^{2n})| \neq 0$. Clearly, such a signature does not satisfy 2ND-ORTH. Contradiction. Thus, without loss of generality, we assume that $\widehat{\partial}_{12}\widehat{f} \not\equiv 0$. Since $\widehat{\partial}_{12}\widehat{f} \in \widehat{\mathcal{O}}^{\otimes}$, without loss of generality, we may assume that in the UPF of $\widehat{\partial}_{12}\widehat{f}$, variables x_3 and x_4 appear in one binary signature $b_1(x_3, x_4)$, x_5 and x_6 appear in one binary signature $b_2(x_5, x_6)$ and so on. Thus, we have

$$\widehat{\partial}_{12}\widehat{f} = \widehat{b_1}(x_3, x_4) \otimes \widehat{b_2}(x_5, x_6) \otimes \widehat{b_3}(x_7, x_8) \otimes \ldots \otimes \widehat{b_{n-1}}(x_{2n-1}, x_{2n}).$$

By Lemma 3.6, all these binary signatures $\widehat{b_1}$, $\widehat{b_2}$, ..., $\widehat{b_{n-1}}$ are realizable from f by factorization. Note that for nonzero binary signatures $\widehat{b_i}(x_{2i+1}, x_{2i+2})$ $(1 \leqslant i \leqslant n-1)$, if we connect the variable x_{2i+1} of two copies of $\widehat{b_i}(x_{2i+1}, x_{2i+2})$ using $\neq_2$ (mating two binary signatures), then we get $\neq_2$ up to a scalar. We consider the following gadget construction on $\widehat{f}$. Recall that in the setting of $\mathrm{Holant}(\neq \mid \widehat{\mathcal{F}})$, variables are connected using $\neq_2$. For $1 \leqslant i \leqslant n-1$, by a slight abuse of names of variables, we connect the variable x_{2i+1} of $\widehat{f}$ with the variable x_{2i+1} of $\widehat{b_i}(x_{2i+1}, x_{2i+2})$ using $\neq_2$. We get a signature $\widehat{f'}$ of arity $2n$. (Note that, as a complexity reduction using factorization (Lemma 3.6), we can only apply it a constant number of times. However, the arity $2n$ of $\widehat{f}$ is considered a constant, as $\widehat{f} \in \widehat{\mathcal{F}}$, which is independent of the input size of a signature grid to the problem $\mathrm{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$.) We denote this gadget construction by G_1 and we write $\widehat{f'}$ as $G_1 \circ \widehat{f}$. G_1 is constructed by extending variables of $\widehat{f}$ using binary signatures realized from $\widehat{\partial}_{12}\widehat{f}$. It does not change the irreducibility of $\widehat{f}$. Thus, $\widehat{f'}$ is irreducible since $\widehat{f}$ is irreducible. Similarly, we may assume that $\widehat{f'} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$. Otherwise, we are done.

Consider the signature $\widehat{\partial}_{12}\widehat{f'}$. Since the above gadget construction G_1 does not touch variables x_1 and x_2 of f, G_1 commutes with the merging gadget $\widehat{\partial}_{12}$. (Succinctly, the commutativity can be expressed as $\widehat{\partial}_{12}\widehat{f'} = \widehat{\partial}_{12}(G_1 \circ \widehat{f}) = G_1 \circ \widehat{\partial}_{12}\widehat{f}$.) Thus, $\widehat{\partial}_{12}\widehat{f'}$ can be realized by performing the gadget construction G_1 on $\widehat{\partial}_{12}\widehat{f}$, which connects each binary signature $\widehat{b_i}(x_{2i+1}, x_{2i+2})$ in the UPF of $\widehat{\partial}_{12}\widehat{f}$ with another copy of $\widehat{b_i}(x_{2i+1}, x_{2i+2})$ (in the mating fashion). Thus, each binary signature $\widehat{b_i}$ in $\widehat{\partial}_{12}\widehat{f}$ is changed to $\neq_2$ up to a nonzero scalar after this gadget construction G_1. After normalization and renaming variables, we have

$$\widehat{\partial}_{12}\widehat{f'} = (\neq_2)(x_3, x_4) \otimes (\neq_2)(x_5, x_6) \otimes (\neq_2)(x_7, x_8) \otimes \ldots \otimes (\neq_2)(x_{2n-1}, x_{2n}). \tag{8.2}$$

Thus, $\widehat{\partial}_{12}\widehat{f'} \in \mathcal{D}^{\otimes}$. Moreover, for all pairs of indices $\{i, j\}$ disjoint with $\{1, 2\}$, we have

$$\widehat{\partial}_{(ij)(12)}\widehat{f'} \in \mathcal{D}^{\otimes}, \quad \text{and hence} \quad \widehat{\partial}_{(ij)(12)}\widehat{f'} \not\equiv 0. \tag{8.3}$$

A fortiori, for all pairs of indices $\{i, j\}$ disjoint with $\{1, 2\}$, $\widehat{\partial}_{ij}\widehat{f'} \not\equiv 0$.

Now, we show that we can realize an irreducible signature $\widehat{f^*}$ of arity $2n$ from $\widehat{f'}$ such that $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$. We first prove the following claim.

> **Claim.** *Let $\widehat{h} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$ be a signature of arity $2n \geqslant 8$. If $\widehat{\partial}_{ij}\widehat{h} \in \mathcal{D}^{\otimes}$ for all $\{i, j\}$ disjoint with $\{1, 2\}$, then $\widehat{h} \in \widehat{\int}\mathcal{D}^{\otimes}$.*

Clearly, we only need to show that $\widehat{\partial}_{1k}\widehat{h} \in \mathcal{D}^{\otimes}$ for all $2 \leqslant k \leqslant 2n$. Then, by symmetry we also have $\widehat{\partial}_{2k}\widehat{h} \in \mathcal{D}^{\otimes}$ for $k = 1$ and all $3 \leqslant k \leqslant 2n$. This will prove $\widehat{h} \in \widehat{\int}\mathcal{D}^{\otimes}$. Consider $\widehat{\partial}_{1k}\widehat{h}$ for an arbitrary $2 \leqslant k \leqslant 2n$. Since for all $\{i, j\}$ disjoint with $\{1, 2\}$, we have $\widehat{\partial}_{ij}\widehat{h} \in \mathcal{D}^{\otimes}$, a fortiori for all $\{i, j\}$ disjoint with $\{1, 2\} \cup \{k\}$,

$$\widehat{\partial}_{(1k)(ij)}\widehat{h} \in \mathcal{D}^{\otimes}. \tag{8.4}$$

Since $\widehat{h}$ has arity $2n \geqslant 8$, we can pick a pair of indices $\{i, j\}$ disjoint with $\{1, 2\} \cup \{k\}$. Since $\widehat{\partial}_{(1k)(ij)}\widehat{h} \in \mathcal{D}^{\otimes}$, which is nonzero, a fortiori we have $\widehat{\partial}_{1k}\widehat{h} \not\equiv 0$. So we may consider the UPF of $\widehat{\partial}_{1k}\widehat{h}$, which is known to be in $\widehat{\mathcal{O}}^{\otimes}$. For a contradiction, suppose that there is a binary signature $\widehat{b_1}$ (as a factor of $\widehat{\partial}_{1k}\widehat{h}$) such that $\widehat{b_1}$ is not an associate of $\neq_2$. Among the two variables in the scope of $\widehat{b_1}$, at least one is not x_2. We pick such a variable x_s where $x_s \neq x_2$. Then, we consider another binary signature $\widehat{b_2}$ in the UPF of $\widehat{\partial}_{1k}\widehat{h}$.

- If $\widehat{b_2} = \lambda \cdot \neq_2$, for some nonzero scalar λ, then we pick a variable x_t in the scope of $\widehat{b_2}$ that is not x_2. Consider $\widehat{\partial}_{(st)(1k)}\widehat{h}$. When merging variables x_s and x_t of $\widehat{\partial}_{1k}\widehat{h}$, we connect the variable x_s of $\widehat{b_1}$ with the variable x_t of $\lambda \cdot \neq_2$, and the resulting binary signature is just $\lambda \cdot \widehat{b_1}$, which is not an associate of $\neq_2$. Thus, we have $\widehat{\partial}_{(st)(1k)}\widehat{h} \notin \mathcal{D}^{\otimes}$.

- Otherwise, $\widehat{b_2}$ is not an associate of $\neq_2$. Since $\widehat{\partial}_{1k}\widehat{h}$ has arity $2n-2 \geqslant 6$, we can find another binary signature $\widehat{b_3}$ in the UPF of $\widehat{\partial}_{1k}\widehat{h}$. We pick a variable x_t in the scope of $\widehat{b_3}$ that is not x_2. Consider $\widehat{\partial}_{(st)(1k)}\widehat{h}$. Now, when merging variables x_s and x_t of $\widehat{\partial}_{1k}\widehat{h}$, the binary signature $\widehat{b_2}$ is untouched. Thus, we have $\widehat{b_2} \mid \widehat{\partial}_{(st)(1k)}\widehat{h}$, which implies that $\widehat{\partial}_{(st)(1k)}\widehat{h} \notin \mathcal{D}^{\otimes}$.

Note that in both cases, $\{s,t\} \cap (\{1,2\} \cup \{k\}) = \emptyset$. Therefore the two cases above both contradict (8.4) by picking $\{i,j\} = \{s,t\}$. Thus, $\widehat{\partial}_{1k}\widehat{h} \in \mathcal{D}^{\otimes}$ for all $2 \leqslant k \leqslant 2n$. Then similarly, we can show that $\widehat{\partial}_{2k}\widehat{h} \in \mathcal{D}^{\otimes}$ for all $3 \leqslant k \leqslant 2n$. This finishes the proof of our Claim.

Remember that $\widehat{\partial}_{ij}\widehat{f'} \not\equiv 0$ for all $\{i,j\}$ disjoint with $\{1,2\}$. We consider the UPF of $\widehat{\partial}_{ij}\widehat{f'}$. Since $\widehat{f'} \in \int\widehat{\mathcal{O}}^{\otimes}$, there are two cases depending on whether variables x_1 and x_2 appear in one binary signature or two distinct binary signatures.

Case 1. For every $\{i,j\}$ disjoint with $\{1,2\}$, in the UPF of $\widehat{\partial}_{ij}\widehat{f'}$, x_1 and x_2 appear in one nonzero binary signature $\widehat{b_{ij}}(x_1,x_2) \in \widehat{\mathcal{O}}$. In other words, for every $\{i,j\}$ disjoint with $\{1,2\}$,

$$\widehat{\partial}_{ij}\widehat{f'} = \widehat{b_{ij}}(x_1,x_2) \otimes \widehat{g_{ij}}, \quad \text{for some } \widehat{g_{ij}} \not\equiv 0.$$

(These factors $\widehat{b_{ij}}$ and $\widehat{g_{ij}}$ are nonzero since $\widehat{\partial}_{ij}\widehat{f'} \not\equiv 0$.) Then, $\widehat{g_{ij}} \sim \widehat{\partial}_{(12)(ij)}\widehat{f'}$, and by (8.3), we have $\widehat{g_{ij}} \in \mathcal{D}^{\otimes}$. Also for $\{k,\ell\}$ disjoint with both $\{i,j\}$ and $\{1,2\}$, $\widehat{\partial}_{(k\ell)(ij)}\widehat{f'} \not\equiv 0$ since $\widehat{\partial}_{(12)(k\ell)(ij)}\widehat{f'} = \widehat{\partial}_{(ij)(k\ell)(12)}\widehat{f'} \not\equiv 0$.

We first show that for any two pairs $\{i,j\} \neq \{k,\ell\}$ that are both disjoint with $\{1,2\}$, $\widehat{b_{ij}}(x_1,x_2) \sim \widehat{b_{k\ell}}(x_1,x_2)$. If $\{i,j\}$ is disjoint with $\{k,\ell\}$, then $\widehat{b_{ij}}(x_1,x_2) \mid \widehat{\partial}_{(k\ell)(ij)}\widehat{f'}$ and $\widehat{b_{k\ell}}(x_1,x_2) \mid \widehat{\partial}_{(ij)(k\ell)}\widehat{f'}$. Since $\widehat{\partial}_{(k\ell)(ij)}\widehat{f'} = \widehat{\partial}_{(ij)(k\ell)}\widehat{f'} \not\equiv 0$, by Lemma 3.4, we have $\widehat{b_{ij}}(x_1,x_2) \sim \widehat{b_{k\ell}}(x_1,x_2)$. Otherwise, $\{i,j\}$ and $\{k,\ell\}$ are not disjoint. Since $\widehat{f'}$ has arity $\geqslant 8$, we can find another pair of indices $\{s,t\}$ such that it is disjoint with $\{1,2\} \cup \{i,j\} \cup \{k,\ell\}$. Then, by the above argument, we have $\widehat{b_{ij}}(x_1,x_2) \sim \widehat{b_{st}}(x_1,x_2)$, and $\widehat{b_{st}}(x_1,x_2) \sim \widehat{b_{k\ell}}(x_1,x_2)$. Thus, $\widehat{b_{ij}}(x_1,x_2) \sim \widehat{b_{k\ell}}(x_1,x_2)$. We can use a binary signature $\widehat{b}(x_1,x_2)$ to denote these binary signature $\widehat{b_{ij}}(x_1,x_2)$ for all $\{i,j\}$ disjoint with

$\{1,2\}$. Then, $\widehat{b}(x_1,x_2) \mid \widehat{\partial}_{ij}\widehat{f'}$ for all $\{i,j\}$ disjoint with $\{1,2\}$. Also, $\widehat{b}(x_1,x_2)$ is realizable from $\widehat{f'}$ by merging and factorization.

Then, we consider the following gadget construction G_2 on $\widehat{f'}$. By a slight abuse of variable names, we connect the variable x_1 of $\widehat{f'}$ with the variable x_1 of $\widehat{b}(x_1,x_2)$ and we get a signature $\widehat{f^*}$. Clearly, G_2 is constructed by extending variables of $\widehat{f'}$. It does not change the irreducibility of $\widehat{f'}$. Thus, $\widehat{f^*}$ is irreducible. Again, we may assume that $\widehat{f^*} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$. Consider $\widehat{\partial}_{ij}\widehat{f^*}$ for all $\{i,j\}$ disjoint with $\{1,2\}$. Since the above gadget construction G_2 only touches the variable x_1 of f', it commutes with the merging operation $\widehat{\partial}_{ij}$. Thus, $\widehat{\partial}_{ij}\widehat{f^*}$ can be realized by performing the gadget construction G_2 on $\widehat{\partial}_{ij}\widehat{f'}$, i.e., connecting the binary signature $\widehat{b}(x_1,x_2)$ in the UPF of $\widehat{\partial}_{ij}\widehat{f'}$ with itself (in the mating fashion), which changes $\widehat{b}(x_1,x_2)$ to $\neq_2$ up to some nonzero scalar λ_{ij}. Thus, for all $\{i,j\}$ disjoint with $\{1,2\}$, after renaming variables, we have

$$\widehat{\partial}_{ij}\widehat{f^*} = \lambda_{ij}\cdot(\neq_2)(x_1,x_2)\otimes\widehat{g_{ij}} \in \mathcal{D}^{\otimes}.$$

Thus, $\widehat{\partial}_{ij}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $\{i,j\}$ disjoint with $\{1,2\}$. By our Claim, $\widehat{f^*} \in \int\mathcal{D}^{\otimes}$. We are done with Case 1.

Case 2. There is a pair of indices $\{i,j\}$ disjoint with $\{1,2\}$ such that x_1 and x_2 appear in two distinct nonzero binary signatures $\widehat{b'_1}(x_1,x_u)$ and $\widehat{b'_2}(x_2,x_v)$ in the UPF of $\widehat{\partial}_{ij}\widehat{f'}$. In other words, there exits $\{i,j\}$ such that

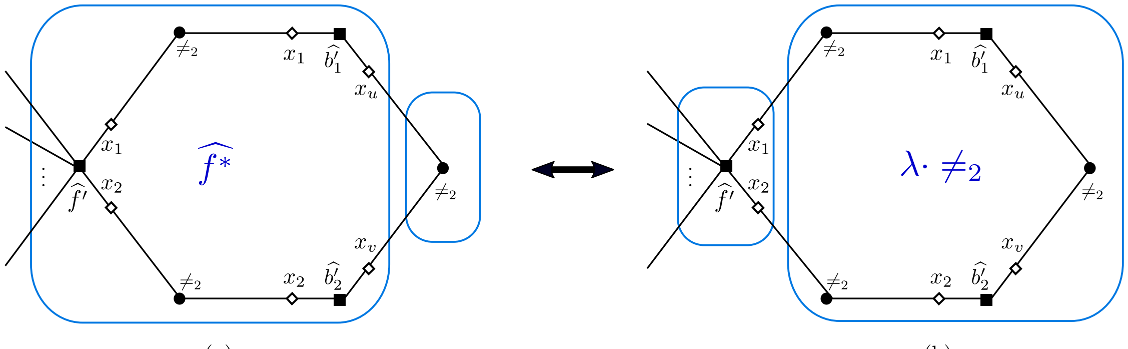
$$\widehat{\partial}_{ij}\widehat{f'} = \widehat{b'_1}(x_1,x_u)\otimes\widehat{b'_2}(x_2,x_v)\otimes\widehat{h_{ij}}, \text{ for some } \widehat{h_{ij}} \not\equiv 0. \tag{8.5}$$

Since $\widehat{h_{ij}} \mid \widehat{\partial}_{(12)(ij)}\widehat{f'}$ and $\widehat{\partial}_{(12)(ij)}\widehat{f'} \in \mathcal{D}^{\otimes}$, we have $\widehat{h_{ij}} \in \mathcal{D}^{\otimes}$. Also, after merging variables x_1 and x_2 (using $\neq_2$) in $\widehat{\partial}_{ij}\widehat{f'}$, variables x_u and x_v form a binary disequality up to a nonzero scalar (this binary signature on x_u and x_v must be a binary disequality because we already know $\widehat{\partial}_{(12)(ij)}\widehat{f'} \in \mathcal{D}^{\otimes}$). In other words, by connecting the variable x_1 of $\widehat{b'_1}(x_1,x_u)$ and the variable x_2 of $\widehat{b'_2}(x_2,x_v)$ (using $\neq_2$), we get $\lambda\cdot \neq_2 (x_u,x_v)$ for some $\lambda \neq 0$. By Lemma 3.19, we have $\widehat{b'_1} \sim \widehat{b'_2}$. Also, connecting the variable x_u of $\widehat{b'_1}$ and the variable x_v of $\widehat{b'_2}$ (using $\neq_2$) will give the binary signature $\lambda\cdot \neq_2 (x_1,x_2)$ as well.

We consider the following gadget construction G_3 on $\widehat{f'}$. By a slight abuse of variable names, we connect variables x_1 and x_2 of $\widehat{f'}$ with the variable x_1 of $\widehat{b'_1}$ and x_2 of $\widehat{b'_2}$ using $\neq_2$ respectively. We get a signature $\widehat{f^*}$. Again, $\widehat{f^*}$ is irreducible since the gadget construction G_3 does not change the irreducibility of $\widehat{f'}$. Also, we may assume that $\widehat{f^*} \in \widehat{\int\mathcal{O}}^{\otimes}$. Otherwise, we are done. Consider $\widehat{\partial}_{ij}\widehat{f^*}$. Similarly, by the commutitivity of the gadget construction G_3 and the merging gadget $\widehat{\partial}_{ij}$, $\widehat{\partial}_{ij}\widehat{f^*}$ can be realized by connecting variables x_1 and x_2 of $\widehat{\partial}_{ij}\widehat{f'}$ with the variable x_1 of $\widehat{b'_1}$ and the variable x_2 of $\widehat{b'_2}$ respectively. After renaming variables, we have

$$\widehat{\partial}_{ij}\widehat{f^*} = \lambda_{ij} \cdot (\neq_2)(x_1, x_u) \otimes (\neq_2)\,(x_2, x_v) \otimes \widehat{h}_{ij} \in \mathcal{D}^{\otimes}. \tag{8.6}$$

We now show that $\widehat{\partial}_{12}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Note that it is realized in the following way; we first connect variables x_1 and x_2 of $\widehat{f'}$ with the variable x_1 of $\widehat{b'_1}(x_1, x_u)$ and the variable x_2 of $\widehat{b'_2}(x_2, x_v)$ respectively (using $\neq_2$) to get $\widehat{f^*}$, and then after renaming variables x_u and x_v to x_1 and x_2 respectively, we merge them using $\neq_2$ (see Figure 8(a)). By associativity of gadget constructions, we can change the order; we first connect the variable x_u of $\widehat{b'_1}(x_1, x_u)$ with the variable x_v of $\widehat{b'_2}(x_2, x_v)$ (using $\neq_2$), and then we use the resulting binary signature to connect variables x_1 and x_2 of $\widehat{f'}$ (edges are connected using $\neq_2$). Note that connecting x_u of $\widehat{b'_1}(x_1, x_u)$ with x_v of $\widehat{b'_2}(x_2, x_v)$ gives $\lambda\cdot \neq_2$ up to a nonzero scalar λ, and $\lambda\cdot \neq_2$ is unchanged by extending both of its two variables with $\neq_2$ (see Figure 8(b)). Thus, $\widehat{\partial}_{12}\widehat{f^*}$ is actually realized by merging x_1 and x_2 of $\widehat{f'}$ (using $\neq_2$) up to a nonzero scalar. Thus, we have $\widehat{\partial}_{12}\widehat{f^*} \sim \widehat{\partial}_{12}\widehat{f'}$, and hence $\widehat{\partial}_{12}\widehat{f^*} \in \mathcal{D}^{\otimes}$, by the form (8.2) of $\widehat{\partial}_{12}\widehat{f'}$.



(a) (b)

图 8: Gadget constructions of $\widehat{\partial}_{12}\widehat{f^*}$ and $\widehat{\partial}_{12}\widehat{f'}$

Then, we show that $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all pairs of indices $\{s, t\}$ disjoint with $\{1, 2, i, j\}$ and $\{s, t\} \neq \{u, v\}$ where u and v are named in (8.6). Clearly, $\widehat{\partial}_{st}\widehat{f^*} \not\equiv 0$ since $\widehat{\partial}_{(st)(12)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. We first show that in the UPF of $\widehat{\partial}_{st}\widehat{f^*}$, x_1 and x_2 appear in two distinct nonzero binary signatures. Otherwise, for a contradiction, suppose that there is a nonzero binary signature $\widehat{b}^*(x_1,x_2)$ such that $\widehat{b}^*(x_1,x_2) \mid \widehat{\partial}_{st}\widehat{f^*}$. Then, $\widehat{b}^*(x_1,x_2) \mid \widehat{\partial}_{(ij)(st)}\widehat{f^*} = \widehat{\partial}_{(st)(ij)}\widehat{f^*} \not\equiv 0$. By the form (8.6) of $\widehat{\partial}_{ij}\widehat{f^*}$, the only way that x_1 and x_2 can form a nonzero binary signature in $\widehat{\partial}_{(st)(ij)}\widehat{f^*}$ is that the merging gadget is actually merging x_u and x_v. Thus, $\{s,t\}=\{u,v\}$. Contradiction. Therefore, for some i' and j', we have

$$\widehat{\partial}_{st}\widehat{f^*} = \widehat{b^*_{st1}}(x_1,x_{i'}) \otimes \widehat{b^*_{st2}}(x_2,x_{j'}) \otimes \widehat{h_{st}}, \tag{8.7}$$

for some $\widehat{b^*_{st1}}(x_1,x_{i'}), \widehat{b^*_{st2}}(x_2,x_{j'}), \widehat{h_{st}} \not\equiv 0$ since $\widehat{\partial}_{st}\widehat{f^*} \not\equiv 0$. Since $\widehat{h_{st}} \mid \widehat{\partial}_{(12)(st)}\widehat{f^*}$ and $\widehat{\partial}_{(12)(st)}\widehat{f^*} \in \mathcal{D}^{\otimes}$, we have $\widehat{h_{st}} \in \mathcal{D}^{\otimes}$. Also, by Lemma 3.19, $\widehat{b^*_{st1}} \sim \widehat{b^*_{st2}}$. For a contradiction, suppose that $\widehat{\partial}_{st}\widehat{f^*} \notin \mathcal{D}^{\otimes}$, then $\widehat{b^*_{st1}}(x_1,x_{i'}) \not\sim (\neq_2)$, and $\widehat{b^*_{st2}}(x_2,x_{j'}) \not\sim (\neq_2)$. Consider the signature $\widehat{\partial}_{(st)(ij)}\widehat{f^*}$. Since $\{s,t\} \neq \{u,v\}$, by the form (8.6) of $\widehat{\partial}_{ij}\widehat{f^*}$, x_1 and x_2 appear in two binary signatures in the UPF of $\widehat{\partial}_{(st)(ij)}\widehat{f^*}$. Remember that $\widehat{\partial}_{(st)(ij)}\widehat{f^*} = \widehat{\partial}_{(ij)(st)}\widehat{f^*}$. By the form (8.7) of $\widehat{\partial}_{st}\widehat{f^*}$, if $\{i',j'\}=\{i,j\}$, then, after merging x_i and x_j of $\widehat{\partial}_{st}\widehat{f^*}$, x_1 and x_2 will form a new binary signature in $\widehat{\partial}_{(ij)(st)}\widehat{f^*}$. Contradiction. Thus, $\{i',j'\} \neq \{i,j\}$. Then, when merging x_i and x_j of $\widehat{\partial}_{st}\widehat{f^*}$, among $\widehat{b^*_{st1}}(x_1,x_{i'})$ and $\widehat{b^*_{st2}}(x_2,x_{j'})$, at least one binary signature is untouched. Thus, $\widehat{\partial}_{(ij)(st)}\widehat{f^*}$ has a factor that is not an associate of $\neq_2$. A contradiction with $\widehat{\partial}_{(ij)(st)}\widehat{f^*} \in \mathcal{D}^{\otimes}$, which is a consequence of (8.6). Thus, $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$.

Then, we show that $\widehat{\partial}_{uv}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Recall the form (8.6) of $\widehat{\partial}_{ij}\widehat{f^*}$. Clearly, $\{u,v\}$ is disjoint with $\{1,2,i,j\}$. Also, $\widehat{\partial}_{uv}\widehat{f^*} \not\equiv 0$ since $\widehat{\partial}_{(ij)(uv)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Consider the UPF of $\widehat{\partial}_{uv}\widehat{f^*}$.

- If x_1 and x_2 appear in one nonzero binary signature $\widehat{b^*_{uv}}(x_1,x_2)$, then

  $$\widehat{\partial}_{uv}\widehat{f^*} = \widehat{b^*_{uv}}(x_1,x_2) \otimes \widehat{g_{uv}} \qquad \text{for some } \widehat{g_{uv}} \not\equiv 0.$$

  Then, we have $\widehat{g_{uv}} \sim \widehat{\partial}_{(12)(uv)}\widehat{f^*} \in \mathcal{D}^{\otimes}$ since $\widehat{\partial}_{12}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Also, since $\widehat{b^*_{uv}}(x_1,x_2) \mid \widehat{\partial}_{(ij)(uv)}\widehat{f^*} \in \mathcal{D}^{\otimes}$, we have $\widehat{b^*_{uv}}(x_1,x_2) \in \mathcal{D}^{\otimes}$. Hence, $\widehat{\partial}_{uv}\widehat{f^*} \in \mathcal{D}^{\otimes}$.

- If x_1 and x_2 appear in two distinct nonzero binary signatures $\widehat{b^*_{uv1}}(x_1,x_{i'})$ and $\widehat{b^*_{uv2}}(x_2,x_{j'})$, then

  $$\widehat{\partial}_{uv}\widehat{f^*} = \widehat{b^*_{uv1}}(x_1,x_{i'}) \otimes \widehat{b^*_{uv2}}(x_2,x_{j'}) \otimes \widehat{h_{uv}} \qquad \text{for some } \widehat{h_{uv}} \not\equiv 0.$$

Then, we have $\widehat{h_{uv}} \in \mathcal{D}^{\otimes}$ since $\widehat{\partial}_{(12)(uv)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. By the form (8.6) of $\widehat{\partial}_{ij}\widehat{f^*}$, after merging variables x_u and x_v of $\widehat{\partial}_{ij}\widehat{f^*}$, variables x_1 and x_2 form a binary $\neq_2$ in $\widehat{\partial}_{(uv)(ij)}\widehat{f^*} = \widehat{\partial}_{(ij)(uv)}\widehat{f^*}$. On the other hand, by the form of $\widehat{\partial}_{uv}\widehat{f^*}$, the only way that x_1 and x_2 form a binary after merging two variables in $\widehat{\partial}_{uv}\widehat{f^*}$ is to merge $x_{i'}$ and $x_{j'}$. Thus, we have $\{i', j'\} = \{i, j\}$. Since $\widehat{f^*}$ has arity $2n \geqslant 8$, we can find another pair of indices $\{s, t\}$ disjoint with $\{1, 2, i, j, u, v\}$. When merging variables x_s and x_t in $\widehat{\partial}_{uv}\widehat{f^*}$, binary signatures $\widehat{b^*_{uv1}}(x_1, x_{i'})$ and $\widehat{b^*_{uv2}}(x_2, x_{j'})$ are untouched. Thus, we have $\widehat{b^*_{uv1}}(x_1, x_{i'}) \otimes \widehat{b^*_{uv2}}(x_2, x_{j'}) \mid \widehat{\partial}_{(st)(uv)}\widehat{f^*}$. As showed above, we have $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$ and then $\widehat{\partial}_{(st)(uv)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Thus, $\widehat{b^*_{uv1}}(x_1, x_{i'}) \otimes \widehat{b^*_{uv2}}(x_2, x_{j'}) \in \mathcal{D}^{\otimes}$ and then $\widehat{\partial}_{uv}\widehat{f^*} \in \mathcal{D}^{\otimes}$.

So far, we have shown that $\widehat{\partial}_{12}\widehat{f^*} \in \mathcal{D}^{\otimes}$, $\widehat{\partial}_{ij}\widehat{f^*} \in \mathcal{D}^{\otimes}$ and $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $\{s, t\}$ disjoint with $\{1, 2, i, j\}$. If we can further show that $\widehat{\partial}_{ik}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $k \neq 1, 2, i, j$, and then symmetrically $\widehat{\partial}_{jk}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $k \neq 1, 2, i, j$, then $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $\{s, t\}$ disjoint with $\{1, 2\}$. Thus, by our Claim, $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$. This will finish the proof of Case 2.

Now we prove $\widehat{\partial}_{ik}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $k \neq 1, 2, i, j$. Since $\widehat{\partial}_{(ik)(12)}\widehat{f^*} \in \mathcal{D}^{\otimes}$, we have $\widehat{\partial}_{ik}\widehat{f^*} \not\equiv 0$. So we can consider the UPF of $\widehat{\partial}_{ik}\widehat{f^*}$.

- If x_1 and x_2 appear in one nonzero binary signature, then

  $$\widehat{\partial}_{ik}\widehat{f^*} = \widehat{b^*_{ik}}(x_1, x_2) \otimes \widehat{g_{ik}} \qquad \text{for some } \widehat{g_{ik}} \in \mathcal{D}^{\otimes}.$$

  Here, $\widehat{g_{ik}} \in \mathcal{D}^{\otimes}$ since $\widehat{\partial}_{(ik)(12)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Since $\widehat{f^*}$ has arity $2n \geqslant 8$, we can pick a pair of indices $\{s, t\}$ disjoint with $\{1, 2, i, j, k\}$, and merge variables x_s and x_t of $\widehat{\partial}_{ik}\widehat{f^*}$. Then, $\widehat{b^*_{ik}}(x_1, x_2) \mid \widehat{\partial}_{(st)(ik)}\widehat{f^*}$. Since $\widehat{\partial}_{st}\widehat{f^*} \in \mathcal{D}^{\otimes}$, $\widehat{\partial}_{(st)(ik)}\widehat{f^*} = \widehat{\partial}_{(ik)(st)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Thus, $\widehat{b^*_{ik}}(x_1, x_2) \in \mathcal{D}^{\otimes}$ and then $\widehat{\partial}_{ik}\widehat{f^*} \in \mathcal{D}^{\otimes}$.

- If x_1 and x_2 appear in two nonzero distinct binary signatures, then

  $$\widehat{\partial}_{ik}\widehat{f^*} = \widehat{b^*_{ik1}}(x_1, x_p) \otimes \widehat{b^*_{ik2}}(x_2, x_q) \otimes \widehat{h_{ik}} \qquad \text{for some } \widehat{h_{ik}} \in \mathcal{D}^{\otimes}.$$

  Again, here $\widehat{h_{ik}} \in \mathcal{D}^{\otimes}$ since $\widehat{\partial}_{(ik)(12)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. By connecting variables x_1 and x_2 of $\widehat{\partial}_{ik}\widehat{f^*}$, x_p and x_q will form a binary disequality up to a nonzero scalar (this binary signature is disequality because we know that $\widehat{\partial}_{(ik)(12)}\widehat{f^*} \in \mathcal{D}^{\otimes}$). By Lemma 3.19, as the type of binary signatures, $\widehat{b^*_{ik1}} \sim \widehat{b^*_{ik2}}$. Between x_p and x_q, at least one of them is not x_j; suppose that it is x_p. We pick a variable x_r in the scope of $\widehat{h_{ik}}$ that is also not x_j (such a variable x_r exists as $2n \geqslant 8$). Then, by merging x_p and x_r of $\widehat{\partial}_{ik}\widehat{f^*}$, the binary signature $\widehat{b^*_{ik2}}(x_2, x_q)$ is untouched. Since $\{p, r\}$ is disjoint with $\{1, 2, i, j\}$, we have $\widehat{b^*_{ik2}}(x_2, x_q) \mid \widehat{\partial}_{(ik)(pr)}\widehat{f^*} \in \mathcal{D}^{\otimes}$. Thus, we have $\widehat{b^*_{ik2}}(x_2, x_q) \in \mathcal{D}^{\otimes}$ and so does $\widehat{b^*_{ik1}}(x_1, x_p)$, since we have shown that they are associates as the type of binary signatures. Thus, $\widehat{\partial}_{ik}\widehat{f^*} \in \mathcal{D}^{\otimes}$.

As remarked earlier, by symmetry, we also have $\widehat{\partial}_{jk}\widehat{f^*} \in \mathcal{D}^{\otimes}$ for all $k \neq 1, 2, i, j$. Thus, we are done with Case 2.

Thus, an irreducible signature $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$ of arity $2n$ is realized from $\widehat{f}$. □

Remark 8.2. *Since $\widehat{f^*}$ is realized from $\widehat{f}$ by gadget construction, $\widehat{f^*}$ satisfies* ARS *as $\widehat{f}$ does.*

We first give a condition (Lemma 8.4) in which we can quite straightforwardly get the #P-hardness of Holant($\neq\mid \widehat{f}, \widehat{\mathcal{F}}$) by 2ND-ORTH given $\widehat{f} \in \widehat{\int}\mathcal{D}^{\otimes}$ is an irreducible 8-ary signature.

Lemma 8.3. *Let $\widehat{f} = a(1,0)^{\otimes 2n} + \bar{a}(0,1)^{\otimes 2n} + (\neq_2)(x_i, x_j) \otimes \widehat{g_{\rm h}}$ be an irreducible $2n$-ary signature, where $2n \geqslant 4$ and $\widehat{g_{\rm h}}$ is a nonzero* EO *signature (i.e., with half-weighted support) of arity $2n-2$. Then, $\widehat{f}$ does not satisfy* 2ND-ORTH.

证明. By renaming variables, without loss of generality, we may assume that $\{i, j\} = \{1, 2\}$.

For any input $00\beta \neq \vec{0}^{2n}$ of $\widehat{f}$, we have $\widehat{f}(00\beta) = (\neq_2)(0,0) \cdot \widehat{g_{\rm h}}(\beta) = 0$. Thus,

$$|\widehat{f}^{00}_{12}|^2 = \sum_{\beta \in \mathbb{Z}_2^{2n-2}} |\widehat{f}(00\beta)|^2 = |\widehat{f}(\vec{0}^{2n})|^2.$$

On the other hand, since both $(\neq_2)(x_1, x_2)$ and $\widehat{g_{\rm h}}$ are nonzero EO signatures, $(\neq_2)(x_1, x_2) \otimes \widehat{g_{\rm h}}$ is a nonzero EO signature. Then, we can pick an input $01\gamma \in \mathbb{Z}_2^{2n}$ with ${\rm wt}(01\gamma) = n$ such that $\widehat{f}(01\gamma) = (\neq_2)(0,1) \cdot \widehat{g_{\rm h}}(\gamma) \neq 0$. Since $\gamma \in \mathbb{Z}_2^{2n-2}$, and ${\rm wt}(\gamma) = n - 1 \geqslant 1$, there exists a bit γ_i in γ such that $\gamma_i = 0$. Without loss of generality, we may assume that $01\gamma = 010\gamma'$. Then,

$$|\widehat{f}^{00}_{13}|^2 \geqslant |\widehat{f}(\vec{0}^{2n})|^2 + |\widehat{f}(010\gamma')|^2 > |\widehat{f}(\vec{0}^{2n})|^2 = |\widehat{f}^{00}_{12}|^2.$$

Note that the constant λ for the norm squares must be the same for all index pairs $\{i, j\} \subseteq [2n]$ in order to satisfy 2ND-ORTH in Definition 3.20. Thus, $\widehat{f}$ does not satisfy 2ND-ORTH. □

Lemma 8.4. *Let $\widehat{f} \in \widehat{\int\mathcal{D}}^{\otimes}$ be an irreducible 8-ary signature in $\widehat{\mathcal{F}}$. If there exists a binary disequality $(\neq_2)(x_i, x_j)$ and two pairs of indices $\{u, v\}$ and $\{s, t\}$ where $\{u, v\} \cap \{s, t\} \neq \emptyset$ such that $(\neq_2)(x_i, x_j) \mid \widehat{\partial}_{uv}\widehat{f}$ and $(\neq_2)(x_i, x_j) \mid \widehat{\partial}_{st}\widehat{f}$, then* $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is #P-hard.*

证明. For all pairs of indices $\{i, j\}$, since $\widehat{\partial}_{ij}\widehat{f} \in \mathcal{D}^{\otimes}$, $\mathscr{S}(\widehat{\partial}_{ij}\widehat{f})$ is on half-weight. By Lemma 3.9, we have $\widehat{f}(\alpha) = 0$ for all $\mathrm{wt}(\alpha) \neq 0, 4, 8$. Suppose that $\widehat{f}(\vec{0}^8) = a$ and by ARS $\widehat{f}(\vec{1}^8) = \bar{a}$. We can write $\widehat{f}$ in the following form

$$\widehat{f} = a(1, 0)^{\otimes 8} + \bar{a}(0, 1)^{\otimes 8} + \widehat{f}_{\mathrm{h}},$$

where $\widehat{f}_{\mathrm{h}}$ is an EO signature of arity 8.

Clearly, $\widehat{\partial}_{ij}\widehat{f} = \widehat{\partial}_{ij}\widehat{f}_{\mathrm{h}}$ for all $\{i, j\}$. Then, $\widehat{f}_{\mathrm{h}} \in \widehat{\int\mathcal{D}}^{\otimes}$ since $\widehat{f} \in \widehat{\int\mathcal{D}}^{\otimes}$. In addition, since there exists a binary disequality $(\neq_2)(x_i, x_j)$ and two pairs of indices $\{u, v\}$ and $\{s, t\}$ where $\{u, v\} \cap \{s, t\} \neq \emptyset$ such that $(\neq_2)(x_i, x_j) \mid \widehat{\partial}_{uv}\widehat{f}_{\mathrm{h}}, \widehat{\partial}_{st}\widehat{f}_{\mathrm{h}}$, by Lemma 4.19, $\widehat{f}_{\mathrm{h}} \in \mathcal{D}^{\otimes}$ and $(\neq_2)(x_i, x_j) \mid \widehat{f}_{\mathrm{h}}$. Thus,

$$\widehat{f} = a(1, 0)^{\otimes 8} + \bar{a}(0, 1)^{\otimes 8} + (\neq_2)(x_i, x_j) \otimes \widehat{g}_{\mathrm{h}},$$

where $\widehat{g}_{\mathrm{h}} \in \mathcal{D}^{\otimes}$ is a nonzero EO signature or arity 6 since $\widehat{f}_{\mathrm{h}} \in \mathcal{D}^{\otimes}$. By Lemma 8.3, $\widehat{f}$ does not satisfy 2ND-ORTH. Thus, $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard by Lemma 6.6. □

For signatures in $\mathcal{D}^{\otimes}$, we give the following property. Now we adopt the following notation for brevity. We use (i, j) to denote the binary disequality $(\neq_2)(x_i, x_j)$ on variables x_i and x_j.

Lemma 8.5. *Let $\widehat{f} \in \mathcal{D}^{\otimes}$ be a signature of arity at least 6. If there exist $\{u, v\} \neq \{s, t\}$ such that $(i, j) \mid \widehat{\partial}_{uv}\widehat{f}$ and $(i, j) \mid \widehat{\partial}_{st}\widehat{f}$, then $(i, j) \mid \widehat{f}$.*

证明. For a contradiction, suppose that $(i, j) \nmid \widehat{f}$. Thus x_i and x_j appear in two separate disequalities in the UPF of $\widehat{f}$. Since $\widehat{f} \in \mathcal{D}^{\otimes}$, there exists $\{\ell, k\}$ such that $(i, \ell) \otimes (j, k) \mid \widehat{f}$. By merging two variables of $\widehat{f}$, the only way to make x_i and x_j to form a binary disequality is by merging x_ℓ and x_k. By the hypothesis of the lemma, $\{\ell, k\} = \{u, v\} = \{s, t\}$. Contradiction. □

Theorem 8.6. *Let $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$ be a signature of arity 8 in $\widehat{\mathcal{F}}$. Then*

- $\operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$ *is #P-hard, or*

- *there exists some $\widehat{Q} \in \widehat{\mathbf{O}_2}$ such that* $\operatorname{Holant}(\neq_2 \mid \widehat{f}_8, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2 \mid \widehat{\mathcal{F}})$.

证明. By Lemma 8.1, we may assume that an irreducible signature $\widehat{f^*}$ of arity 8 where $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$ is realizable from $\widehat{f}$, and $\widehat{f^*}$ also satisfies ARS. Otherwise, Holant($\neq_2|\ \widehat{\mathcal{F}}$) is #P-hard or we can realize a signature $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$ of arity 2, 4 or 6. Then, by Lemmas 6.7, 6.8 and 7.40, we get #P-hardness. We will show that $\widehat{f_8}$ is realizable from $\widehat{f^*}$, or otherwise we get #P-hardness. For brevity of notation, we rename $\widehat{f^*}$ by $\widehat{f}$. We first show that after renaming variables by applying a suitable permutation to $\{1, 2, \ldots, 8\}$, for all $\{i, j\} \subseteq \{1, 2, 3, 4\}$, $(\ell, k) \mid \widehat{\partial}_{ij}\widehat{f}$ where $\{\ell, k\} = \{1, 2, 3, 4\}\backslash\{i, j\}$. Furthermore, we show that either Holant($\neq_2|\ \widehat{\mathcal{F}}$) is #P-hard, or

$$(5,6) \mid \widehat{\partial}_{12}\widehat{f}, \quad (5,7) \mid \widehat{\partial}_{13}\widehat{f}, \quad (6,7) \mid \widehat{\partial}_{23}\widehat{f}, \text{ and } \quad (1,2) \mid \widehat{\partial}_{56}\widehat{f} \text{ or } (1,3) \mid \widehat{\partial}_{56}\widehat{f}. \tag{8.8}$$

Consider $\widehat{\partial}_{12}\widehat{f}$. Since $\widehat{f} \in \widehat{\int}\mathcal{D}^{\otimes}$, $\widehat{\partial}_{12}\widehat{f} \in \mathcal{D}^{\otimes}$. By renaming variables, without loss of generality, we may assume that

$$\widehat{\partial}_{12}\widehat{f} = \lambda_{12} \cdot (3,4) \otimes (5,6) \otimes (7,8), \tag{8.9}$$

for some $\lambda_{12} \in \mathbb{R} \setminus \{0\}$. Then, consider $\widehat{\partial}_{34}\widehat{f}$. $\widehat{\partial}_{56}\widehat{f}$, and $\widehat{\partial}_{78}\widehat{f}$. There are two cases.

- Case 1. $(1,2) \mid \widehat{\partial}_{34}\widehat{f}, \widehat{\partial}_{56}\widehat{f}$ and $\widehat{\partial}_{78}\widehat{f}$. Then we can write $\widehat{\partial}_{56}\widehat{f} = (1,2) \otimes \widehat{h}$ for some $\widehat{h} \in \mathcal{D}^{\otimes}$. Clearly, $\widehat{h} \sim \widehat{\partial}_{(12)(56)}\widehat{f}$. By the form (8.9) and commutativity, $\widehat{\partial}_{(12)(56)}\widehat{f} \sim (3,4) \otimes (7,8)$. Thus, $\widehat{h} \sim (3,4) \otimes (7,8)$. Then, for some $\lambda_{56} \in \mathbb{R} \setminus \{0\}$,

  $$\widehat{\partial}_{56}\widehat{f} = \lambda_{56} \cdot (1,2) \otimes (3,4) \otimes (7,8). \tag{8.10}$$

  Similarly, we have

  $$\widehat{\partial}_{78}\widehat{f} = \lambda_{78} \cdot (1,2) \otimes (3,4) \otimes (5,6),$$

  and

  $$\widehat{\partial}_{34}\widehat{f} = \lambda_{34} \cdot (1,2) \otimes (5,6) \otimes (7,8),$$

  for some $\lambda_{78}, \lambda_{34} \in \mathbb{R} \setminus \{0\}$.

  Let $\widehat{g} = (1,2) \otimes (3,4)$. Let $\{i, j\} \subseteq \{1, 2, 3, 4\}$ and $\{\ell, k\} = \{1, 2, 3, 4\}\backslash\{i, j\}$. If we merge variables x_i and x_j of $\widehat{g}$, i.e., if we form $\widehat{\partial}_{ij}\widehat{g}$, then clearly variables x_ℓ and x_k will form a disequality. Thus, for all $\{i, j\} \subseteq \{1, 2, 3, 4\}$, $(\ell, k) \mid \widehat{\partial}_{ij}\widehat{g}$. Then, $(\ell, k) \mid \widehat{\partial}_{ij}\widehat{g} \otimes (7,8) \sim \widehat{\partial}_{(ij)(56)}\widehat{f}$ by (8.10), and similarly $(\ell, k) \mid \widehat{\partial}_{ij}\widehat{g} \otimes (5,6) \sim \widehat{\partial}_{(ij)(78)}\widehat{f}$. By Lemma 8.5, $(\ell, k) \mid \widehat{\partial}_{ij}\widehat{f}$.

- Case 2. Among $\widehat{\partial}_{34}\widehat{f}$, $\widehat{\partial}_{56}\widehat{f}$, and $\widehat{\partial}_{78}\widehat{f}$, there is at least one signature that is not divisible by $(1,2)$. Without loss of generality, suppose that $(1,2) \nmid \widehat{\partial}_{56}\widehat{f}$. Since $\widehat{\partial}_{56}\widehat{f} \in \mathcal{D}^{\otimes}$, there exists $\{u,v\}$ disjoint from $\{1,2,5,6\}$ such that $(1,u) \otimes (2,v) \mid \widehat{\partial}_{56}\widehat{f}$. Then, by merging variables x_1 and x_2 of $\widehat{\partial}_{56}\widehat{f}$, we have $(u,v) \mid \widehat{\partial}_{(12)(56)}\widehat{f}$; comparing it to $\widehat{\partial}_{(56)(12)}\widehat{f}$ using the form of (8.9) and by unique factorization we get $\{u,v\} = \{3,4\}$ or $\{7,8\}$. Without loss of generality (i.e., this is still within the freedom of our naming variables subject to the choices made so far), we may assume that $\{u,v\} = \{3,4\}$ and furthermore, $u = 3$ and $v = 4$. Then, for some $\lambda'_{56} \in \mathbb{R} \setminus \{0\}$,
$$\widehat{\partial}_{56}\widehat{f} = \lambda'_{56} \cdot (1,3) \otimes (2,4) \otimes (7,8). \tag{8.11}$$
Then, consider $\widehat{\partial}_{78}\widehat{f}$. We show that $(5,6) \mid \widehat{\partial}_{78}\widehat{f}$. Otherwise, there exists $\{s,t\}$ disjoint from $\{5,6,7,8\}$ such that $(5,s) \otimes (6,t) \mid \widehat{\partial}_{78}\widehat{f}$. By merging two variables of $\widehat{\partial}_{78}\widehat{f}$, the only way to make x_5 and x_6 form a binary disequality is to merge x_s and x_t. By the form (8.9), $(5,6) \mid \widehat{\partial}_{(12)(78)}\widehat{f}$. Thus, $\{s,t\} = \{1,2\}$. From $(5,s) \otimes (6,t) \mid \widehat{\partial}_{78}\widehat{f}$, and $\{s,t\} = \{1,2\}$ we know that x_1 and x_2 will form a binary disequality in $\widehat{\partial}_{(56)(78)}\widehat{f}$. Thus, $(1,2) \mid \widehat{\partial}_{(56)(78)}\widehat{f}$. However, by (8.11) $\widehat{\partial}_{(56)(78)}\widehat{f} \sim (1,3) \otimes (2,4)$. This is a contradiction to UPF. Thus, $\widehat{\partial}_{78}\widehat{f} = (5,6) \otimes \widehat{g'}$ and $\widehat{g'} \sim \widehat{\partial}_{(56)(78)}\widehat{f} \sim (1,3) \otimes (2,4)$. Then, for some $\lambda'_{78} \in \mathbb{R} \setminus \{0\}$,
$$\widehat{\partial}_{78}\widehat{f} = \lambda'_{78} \cdot (1,3) \otimes (2,4) \otimes (5,6). \tag{8.12}$$
Let $\{i,j\} \subseteq \{1,2,3,4\}$ and $\{\ell,k\} = \{1,2,3,4\} \backslash \{i,j\}$. If we merge variables x_i and x_j of $\widehat{g'}$, which is an associate of $(1,3) \otimes (2,4)$, then clearly variables x_ℓ and x_k will form a disequality. Thus, for all $\{i,j\} \subseteq \{1,2,3,4\}$, $(\ell,k) \sim \widehat{\partial}_{ij}\widehat{g'}$. Then, $(\ell,k) \mid \widehat{\partial}_{ij}\widehat{g'} \otimes (7,8) \sim \widehat{\partial}_{(ij)(56)}\widehat{f}$ (by (8.11)) and $(\ell,k) \mid \widehat{\partial}_{ij}\widehat{g'} \otimes (5,6) \sim \widehat{\partial}_{(ij)(78)}\widehat{f}$ (by (8.12)). By Lemma 8.5, $(\ell,k) \mid \widehat{\partial}_{ij}\widehat{f}$.

Thus, in both cases, we have $(\ell,k) \mid \widehat{\partial}_{ij}\widehat{f}$ where $\{i,j\} \sqcup \{\ell,k\} = \{1,2,3,4\}$ is an arbitrary disjoint union of two pairs. Now, we show that in both cases, (with possibly switching the names x_7 and x_8, which we are still free to do), we can have
$$(5,6) \mid \widehat{\partial}_{12}\widehat{f}, \quad (5,7) \mid \partial_{13}\widehat{f}, \quad (6,7) \mid \widehat{\partial}_{23}\widehat{f}. \tag{8.13}$$
Clearly, by the form (8.9), we have $(5,6) \mid \widehat{\partial}_{12}\widehat{f}$. Consider $\partial_{13}\widehat{f}$. We already know that

$(2,4) \mid \partial_{13}\widehat{f}$ (in both cases). If $(5,6) \mid \widehat{\partial}_{13}\widehat{f}$, then since $(5,6) \mid \widehat{\partial}_{12}\widehat{f}$ and $\{1,2\} \cap \{1,3\} \neq \emptyset$, by Lemma 8.4, Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard. Thus, $(5,7) \mid \widehat{\partial}_{13}\widehat{f}$ or $(5,8) \mid \widehat{\partial}_{13}\widehat{f}$. By renaming variables x_7 and x_8, we may assume that in both cases

$$\widehat{\partial}_{13}\widehat{f} = (2,4) \otimes (5,7) \otimes (6,8). \tag{8.14}$$

This renaming will not change any of the above forms of $\widehat{\partial_{ij}}\widehat{f}$. Consider $\widehat{\partial}_{23}\widehat{f}$. We already have $(1,4) \mid \widehat{\partial}_{23}\widehat{f}$. We know $\widehat{\partial}_{23}\widehat{f} \in \mathcal{D}^{\otimes}$, and so in its UPF, $(6,r) \mid \widehat{\partial}_{23}\widehat{f}$, for some $r \in [8] \setminus \{1,2,3,4,6\}$. If $(5,6) \mid \widehat{\partial}_{23}\widehat{f}$, then since $(5,6) \mid \widehat{\partial}_{12}\widehat{f}$ and $\{1,2\} \cap \{2,3\} \neq \emptyset$, by Lemma 8.4, we get #P-hardness. If $(6,8) \mid \widehat{\partial}_{23}\widehat{f}$, then since $(6,8) \mid \widehat{\partial}_{13}\widehat{f}$ by (8.14) and $\{1,3\} \cap \{2,3\} \neq \emptyset$, again by Lemma 8.4, we get #P-hardness. Thus, we may assume that $r = 7$ and $(6,7) \mid \widehat{\partial}_{23}\widehat{f}$. Therefore, we have established (8.13) in both cases. Furthermore, in Case 1, we have $(1,2) \mid \widehat{\partial}_{56}\widehat{f}$ by form (8.10), and in Case 2, we have $(1,3) \mid \widehat{\partial}_{56}\widehat{f}$ by form (8.11).

Now, we show that for any $\alpha \in \mathbb{Z}_2^4$ with $\mathrm{wt}(\alpha) = 1$, $\widehat{f}^{\alpha}_{1234} \equiv 0$. Since $(3,4) \mid \widehat{\partial}_{12}\widehat{f}$, $(\widehat{\partial}_{12}\widehat{f})^{00}_{34} \equiv 0$. Since $\{1,2\}$ is disjoint with $\{3,4\}$,

$$(\widehat{\partial}_{12}\widehat{f})^{00}_{34} = \widehat{\partial}_{12}(\widehat{f}^{00}_{34}) = \widehat{f}^{0100}_{1234} + \widehat{f}^{1000}_{1234} \equiv 0. \tag{8.15}$$

Since $(1,4) \mid \widehat{\partial}_{23}\widehat{f}$,

$$(\widehat{\partial}_{23}\widehat{f})^{00}_{14} = \widehat{\partial}_{23}(\widehat{f}^{00}_{14}) = \widehat{f}^{0010}_{1234} + \widehat{f}^{0100}_{1234} \equiv 0. \tag{8.16}$$

Since $(1,3) \mid \widehat{\partial}_{24}\widehat{f}$,

$$(\widehat{\partial}_{13}\widehat{f})^{00}_{24} = \widehat{\partial}_{13}(\widehat{f}^{00}_{24}) = \widehat{f}^{0010}_{1234} + \widehat{f}^{1000}_{1234} \equiv 0. \tag{8.17}$$

Comparing (8.15), (8.16) and (8.17), we have

$$\widehat{f}^{1000}_{1234} = \widehat{f}^{0100}_{1234} = \widehat{f}^{0010}_{1234} \equiv 0.$$

Since $(2,3) \mid \widehat{\partial}_{14}\widehat{f}$,

$$(\widehat{\partial}_{14}\widehat{f})^{00}_{23} = \widehat{\partial}_{14}(\widehat{f}^{00}_{23}) = \widehat{f}^{0001}_{1234} + \widehat{f}^{1000}_{1234} \equiv 0.$$

Plug in $\widehat{f}^{1000}_{1234} \equiv 0$, we have $\widehat{f}^{0001}_{1234} \equiv 0$. Thus for any $\alpha \in \mathbb{Z}_2^4$ with $\mathrm{wt}(\alpha) = 1$, we have $\widehat{f}^{\alpha}_{1234} \equiv 0$.

Also, for $\alpha \in \mathbb{Z}_2^4$ with $\text{wt}(\alpha) = 3$ and any $\beta \in \mathbb{Z}_2^4$, by ARS we have,

$$\widehat{f}_{1234}^{\alpha}(\beta) = \overline{\widehat{f}_{1234}^{\overline{\alpha}}(\overline{\beta})} = 0$$

since $\text{wt}(\overline{\alpha}) = 1$. Thus, for any $\alpha \in \mathbb{Z}_2^4$ with $\text{wt}(\alpha) = 3$, we also have $\widehat{f}_{1234}^{\alpha} \equiv 0$.

Let $\alpha \in \mathbb{Z}_2^4$ be an assignment of the first four variables of f, and $\beta \in \mathbb{Z}_2^4$ be an assignment of the last four variables of f. Thus, for any $\alpha, \beta \in \mathbb{Z}_2^4$, $\widehat{f}(\alpha\beta) = 0$ if $\text{wt}(\alpha) = 1$ or 3. Also, since $\widehat{f} \in \widehat{\int}\mathcal{D}^{\otimes}$, by Lemma 3.9, $\widehat{f}(\alpha\beta) = 0$ if $\text{wt}(\alpha) + \text{wt}(\beta) \neq 0, 4$ and 8. Then, we show that for any $\alpha\beta \in \mathscr{S}(\widehat{f})$,

$$|\widehat{f}(\alpha\beta)| = |\widehat{f}(\overline{\alpha}\beta)| = |\widehat{f}(\alpha\overline{\beta})| = |\widehat{f}(\overline{\alpha}\overline{\beta})|.$$

By ARS, $|\widehat{f}(\alpha\beta)| = |\widehat{f}(\overline{\alpha}\overline{\beta})|$ and $|\widehat{f}(\overline{\alpha}\beta)| = |\widehat{f}(\alpha\overline{\beta})|$. So, we only need to show that

$$|\widehat{f}(\alpha\beta)| = |\widehat{f}(\alpha\overline{\beta})|. \tag{8.18}$$

Pick an arbitrary $\{i, j\} \subseteq \{1, 2, 3, 4\}$ and an arbitrary $\{u, v\} \subseteq \{5, 6, 7, 8\}$. Let $\{\ell, k\} = \{1, 2, 3, 4\} \backslash \{i, j\}$ and $\{s, t\} = \{5, 6, 7, 8\} \backslash \{u, v\}$. Since $\widehat{f}$ satisfies 2ND-ORTH, by equation (6.6), we have $|\widehat{\mathbf{f}}_{ijuv}^{0000}|^2 = |\widehat{\mathbf{f}}_{ijuv}^{0011}|^2$. Since $\widehat{f}(\alpha\beta) = 0$ if $\text{wt}(\alpha) = 1$ or 3, or $\text{wt}(\alpha) + \text{wt}(\beta) \neq 0, 4$ and 8, we get the equation,

$$|\widehat{f}_{ij\ell kuvst}^{00000000}|^2 + |\widehat{f}_{ij\ell kuvst}^{00110011}|^2 = |\widehat{f}_{ij\ell kuvst}^{00111100}|^2 + |\widehat{f}_{ij\ell kuvst}^{00001111}|^2. \tag{8.19}$$

Note that for $|\widehat{\mathbf{f}}_{ijuv}^{0000}|^2$, since we set $x_i x_j = 00$, the only possible nonzero terms are for $x_\ell x_k = 00$ or 11; furthermore, as we also set $x_u x_v = 00$, then $x_s x_t = 00$ if $x_\ell x_k = 00$, and $x_s x_t = 11$ if $x_\ell x_k = 11$. The situation is similar for $|\widehat{\mathbf{f}}_{ijuv}^{0011}|^2$.

Also, by considering $|\widehat{\mathbf{f}}_{ijst}^{0000}|^2 = |\widehat{\mathbf{f}}_{ijst}^{0011}|^2$, we have

$$|\widehat{f}_{ij\ell kuvst}^{00000000}|^2 + |\widehat{f}_{ij\ell kuvst}^{00111100}|^2 = |\widehat{f}_{ij\ell kuvst}^{00110011}|^2 + |\widehat{f}_{ij\ell kuvst}^{00001111}|^2. \tag{8.20}$$

Comparing equations (8.19) and (8.20), we have

$$|\widehat{f}_{ij\ell kuvst}^{00000000}|^2 = |\widehat{f}_{ij\ell kuvst}^{00001111}|^2, \quad \text{and} \quad |\widehat{f}_{ij\ell kuvst}^{00110011}|^2 = |\widehat{f}_{ij\ell kuvst}^{00111100}|^2.$$

Also, by ARS,

$$|\widehat{f}^{11111111}_{ij\ell kuvst}|^2 = |\widehat{f}^{11110000}_{ij\ell kuvst}|^2.$$

As (i,j,k,ℓ) is an arbitrary permutation of $(1,2,3,4)$ and (u,v,s,t) is an arbitrary permutation of $(5,6,7,8)$, and $\widehat{f}(\alpha\beta)$ vanishes if $\mathrm{wt}(\alpha)+\mathrm{wt}(\beta) \neq 0, 4$ and 8, the above have established (8.18) for any $\alpha, \beta \in \mathbb{Z}_2^4$. Hence, for all $\alpha, \beta \in \mathbb{Z}_2^4$,

$$|\widehat{f}(\alpha\beta)| = |\widehat{f}(\overline{\alpha}\beta)| = |\widehat{f}(\alpha\overline{\beta})| = |\widehat{f}(\overline{\alpha}\overline{\beta})|.$$

Note that $\widehat{f}$ has at most $4 + \binom{4}{2}\cdot\binom{4}{2} = 40$ many possibly non-zero entries. In terms of norms, these 40 entries can be represented by $\widehat{f}^{\vec{0}^8}$ and the following 9 entries in Table 6. In other words, for every $\alpha\beta \in \mathbb{Z}_2^8$ where $\mathrm{wt}(\alpha) \equiv \mathrm{wt}(\beta) \equiv 0 \pmod 2$ and $\mathrm{wt}(\alpha)+\mathrm{wt}(\beta) \equiv 0 \pmod 4$, exactly one entry among $\widehat{f}(\alpha\beta)$, $\widehat{f}(\overline{\alpha}\beta)$, $\widehat{f}(\alpha\overline{\beta})$ and $\widehat{f}(\overline{\alpha}\overline{\beta})$ appears in Table 6. We also view these 9 entries in Table 6 as a 3-by-3 matrix denoted by $M = (m_{ij})_{i,j=1}^3$.

$x_1x_2x_3x_4$ \ $x_5x_6x_7x_8$	$\alpha_1 = 0110$ (Col 1)	$\alpha_2 = 1010$ (Col 2)	$\alpha_3 = 1100$ (Col 3)
$\alpha_1 = 0110$ (Row 1)	$m_{11} = \widehat{f}^{01100110}$	$m_{12} = \widehat{f}^{01101010}$	$m_{13} = \widehat{f}^{01101100}$
$\alpha_2 = 1010$ (Row 2)	$m_{21} = \widehat{f}^{10100110}$	$m_{22} = \widehat{f}^{10101010}$	$m_{23} = \widehat{f}^{10101100}$
$\alpha_3 = 1100$ (Row 3)	$m_{31} = \widehat{f}^{11000110}$	$m_{32} = \widehat{f}^{11001010}$	$m_{33} = \widehat{f}^{11001100}$

表 6: Representative entries of $\widehat{f}$ in terms of norms

Let $\widehat{f}^{\vec{0}^8} = a$. First we show that

$$|m_{i,1}|^2 + |m_{i,2}|^2 + |m_{i,3}|^2 = |a|^2, \quad \text{for } i = 1,2,3. \tag{8.21}$$

and

$$|m_{1,j}|^2 + |m_{2,j}|^2 + |m_{3,j}|^2 = |a|^2, \quad \text{for } j = 1,2,3. \tag{8.22}$$

Let (i,j,k) be an arbitrary permutation of $(1,2,3)$. Again, by equation (6.6), $|\widehat{\mathbf{f}}^{0110}_{ijk8}|^2 = |\widehat{\mathbf{f}}^{0000}_{ijk8}|^2$. Then, we have

$$|\widehat{f}^{01100110}_{ijk45678}|^2 + |\widehat{f}^{01101010}_{ijk45678}|^2 + |\widehat{f}^{01101100}_{ijk45678}|^2 = |\widehat{f}^{00000000}_{ijk45678}|^2 = |a|^2.$$

By taking $(i,j,k)=(1,2,3),(2,1,3)$ and $(3,1,2)$, we get equations (8.21) for $i=1,2,3$ respectively. Similarly, by considering $|\widehat{\mathbf{f}}_{4ijk}^{0110}|^2=|\widehat{\mathbf{f}}_{4ijk}^{0000}|^2$ where (i,j,k) is an arbitrary permutation of $(5,6,7)$, we get equations (8.22).

Also, since $(5,6)\mid\widehat{\partial}_{12}\widehat{f}$, we have $\widehat{\partial}_{12}\widehat{f}(x_3,\ldots,x_8)=0$ if $x_5=x_6$. Notice that

$$m_{13}+m_{23}=\widehat{f}^{01101100}+\widehat{f}^{10101100}$$

is an entry of $\widehat{\partial}_{12}\widehat{f}$ on the input 101100. Thus, $m_{13}+m_{23}=0$. Also, since $(5,7)\mid\widehat{\partial}_{13}\widehat{f}$, we have

$$m_{12}+m_{32}=0.$$

Since $(6,7)\mid\widehat{\partial}_{23}\widehat{f}$, we have

$$m_{21}+m_{31}=0.$$

Let $x=|m_{13}|=|m_{23}|$, $y=|m_{12}|=|m_{32}|$, and $z=|m_{21}|=|m_{31}|$. Plug x, y, z into equations (8.21) and (8.22). We have

$$\begin{aligned}|m_{11}|^2+y^2+x^2=&\quad|m_{11}|^2+z^2+z^2\\=z^2+|m_{22}|^2+x^2=&\quad y^2+|m_{22}|^2+y^2\\=z^2+y^2+|m_{33}|^2=&\quad x^2+x^2+|m_{33}|^2.\end{aligned}$$

Thus, $x=y=z$ and $|m_{11}|=|m_{22}|=|m_{33}|$. Consider

$$m_{11}+m_{21}=\widehat{f}^{01100110}+\widehat{f}^{10100110}\quad\text{and}\quad m_{12}+m_{22}=\widehat{f}^{01101010}+\widehat{f}^{10101010}.$$

They are entries of $\widehat{\partial}_{12}\widehat{f}$ on inputs 100110 and 101010. By form (8.9) of $\widehat{\partial}_{12}\widehat{f}$, we have

$$m_{11}+m_{21}=m_{12}+m_{22}\in\mathbb{R}\backslash\{0\}.$$

Remember that we also have $(1,2)\mid\widehat{\partial}_{56}\widehat{f}$ or $(1,3)\mid\widehat{\partial}_{56}\widehat{f}$.

We first consider the case that $(1,3)\mid\widehat{\partial}_{56}\widehat{f}$. Then

$$m_{21}+m_{22}=\widehat{f}^{10100110}+\widehat{f}^{10101010}=0.$$

Thus,

$$m_{11}+m_{21}=m_{12}-m_{21}\in\mathbb{R}\backslash\{0\}.$$

Since $|m_{12}|=|m_{21}|$, $|m_{22}|=|m_{11}|$ and $m_{21}+m_{22}=0$,

$$|m_{12}|=|m_{21}|=|m_{22}|=|m_{11}|.$$

Thus, $m_{11}=\overline{m_{21}}$ and $m_{12}=-\overline{m_{21}}$. Let $\mathfrak{Re}(x)$ the real part of a number x. Then,

$$\mathfrak{Re}(m_{11})+\mathfrak{Re}(m_{21})=2\mathfrak{Re}(m_{21})=\mathfrak{Re}(m_{12})-\mathfrak{Re}(m_{21})=-2\mathfrak{Re}(m_{21}).$$

Thus, $\mathfrak{Re}(m_{21})=0$. Then, $\mathfrak{Re}(m_{11})=\mathfrak{Re}(m_{21})=0$. Thus, $m_{11}+m_{21}\notin\mathbb{R}\backslash\{0\}$ since $\mathfrak{Re}(m_{11}+m_{21})=0$. Contradiction.

Now, we consider the case that $(1,2)\mid\widehat{\partial}_{56}\widehat{f}$. Then

$$m_{31}+m_{32}=\widehat{f}^{11000110}+\widehat{f}^{11001010}=0.$$

Since $m_{12}+m_{32}=0$ and $m_{21}+m_{31}=0$, we have $m_{12}=-m_{21}$. Thus, we have

$$m_{11}+m_{21}=m_{12}+m_{22}=m_{22}-m_{21}\in\mathbb{R}\backslash\{0\}.$$

Taking the imaginary part, $\mathfrak{Im}(m_{11})+\mathfrak{Im}(m_{21})=\mathfrak{Im}(m_{22})-\mathfrak{Im}(m_{21})=0$. Adding the two, we get $\mathfrak{Im}(m_{11})+\mathfrak{Im}(m_{22})=0$, and thus, $m_{11}+m_{22}\in\mathbb{R}$. Since $|m_{11}|=|m_{22}|$, $m_{11}=\overline{m_{22}}$. Then, $\mathfrak{Re}(m_{11})=\mathfrak{Re}(m_{22})$. Also, since $m_{11}+m_{21}=m_{22}-m_{21}\in\mathbb{R}\backslash\{0\}$,

$$\mathfrak{Re}(m_{11})+\mathfrak{Re}(m_{21})=\mathfrak{Re}(m_{22})-\mathfrak{Re}(m_{21})=\mathfrak{Re}(m_{11})-\mathfrak{Re}(m_{21})\neq 0.$$

Thus, $\mathfrak{Re}(m_{21})=0$, and $\mathfrak{Re}(m_{11})\neq 0$. Suppose that $m_{21}=d\mathfrak{i}$ for some $d\in\mathbb{R}$. Then there exists $c\in\mathbb{R}\backslash\{0\}$ such that $m_{11}=c-d\mathfrak{i}$ and then $m_{22}=c+d\mathfrak{i}$. Remember that $m_{21}+m_{31}=0$. Thus, $m_{31}=-d\mathfrak{i}$. Consider

$$m_{11}+m_{31}=\widehat{f}^{01100110}+\widehat{f}^{11000110}=c-2d\mathfrak{i}.$$

It is an entry of the signature $\widehat{\partial}_{13}\widehat{f}$. Since $\widehat{\partial}_{13}\widehat{f}\in\mathcal{D}^{\otimes}$, $c-2d\mathfrak{i}\in\mathbb{R}$. Thus, $d=0$. Then, $m_{21}=0$

and $m_{11} \in \mathbb{R}$. Thus,

$$x = |m_{13}| = |m_{23}| = y = |m_{12}| = |m_{32}| = z = |m_{21}| = |m_{31}| = 0,$$

and

$$|m_{11}| = |m_{22}| = |m_{33}| = |a| = |\widehat{f}(\vec{0})|.$$

Since $\widehat{f} \not\equiv 0$, $a \neq 0$. Thus,

$$\mathscr{S}(\widehat{f}) = \{\delta\delta, \delta\overline{\delta}, \overline{\delta}\delta, \overline{\delta\delta} \in \mathbb{Z}_2^8 \mid \delta = 0000, \alpha_1, \alpha_2, \alpha_3\},$$

where $\alpha_1, \alpha_2, \alpha_3$ are named in Table 6. It is easy to see that $\mathscr{S}(\widehat{f}) = \mathscr{S}(\widehat{f_8})$. Since $m_{11} \in \mathbb{R}$, and $|m_{11}| = |a| \neq 0$, we can normalize it to 1. Since, $\widehat{\partial}_{12}\widehat{f} \in \mathcal{D}^{\otimes}$, we have

$$1 = \widehat{f}(\alpha_1\alpha_1) + \widehat{f}(\alpha_2\alpha_1) = \widehat{f}(\alpha_1\alpha_2) + \widehat{f}(\alpha_2\alpha_2) = \widehat{f}(\alpha_1\overline{\alpha_1}) + \widehat{f}(\alpha_2\overline{\alpha}_1) = \widehat{f}(\alpha_1\overline{\alpha_2}) + \widehat{f}(\alpha_2\overline{\alpha}_2).$$

Since, $\widehat{f}(\alpha_2\alpha_1) = \widehat{f}(\alpha_1\alpha_2) = \widehat{f}(\alpha_2\overline{\alpha}_1) = \widehat{f}(\alpha_1\overline{\alpha_2}) = 0$,

$$\widehat{f}(\alpha_1\alpha_1) = \widehat{f}(\alpha_2\alpha_2) = \widehat{f}(\alpha_1\overline{\alpha}_1) = \widehat{f}(\alpha_2\overline{\alpha_2}) = 1.$$

Similarly, since $\widehat{\partial}_{13}\widehat{f} \in \mathcal{D}^{\otimes}$,

$$\widehat{f}(\alpha_1\alpha_1) = \widehat{f}(\alpha_3\alpha_3) = \widehat{f}(\alpha_1\overline{\alpha}_1) = \widehat{f}(\alpha_3\overline{\alpha_3}) = 1.$$

By ARS, we have

$$1 = \overline{\widehat{f}(\alpha_1\alpha_1)} = \widehat{f}(\overline{\alpha_1\alpha_1}) = \widehat{f}(\overline{\alpha_1}\alpha_1) = \widehat{f}(\overline{\alpha_2\alpha_2}) = \widehat{f}(\overline{\alpha_2}\alpha_2) = \widehat{f}(\overline{\alpha_3\alpha_3}) = \widehat{f}(\overline{\alpha_3}\alpha_3).$$

Also, since $\widehat{\partial}_{15}\widehat{f} \in \mathcal{D}^{\otimes}$,

$$1 = \widehat{f}(\alpha_1\overline{\alpha_1}) = \widehat{f}^{01101001} + \widehat{f}^{11100001} = \widehat{f}^{00001111} + \widehat{f}^{10000111} = \widehat{f}^{00001111}.$$

Then, by ARS, $\widehat{f}^{11110000} = \overline{\widehat{f}^{00001111}} = 1$. Thus, $\widehat{f}(\gamma) = 1$ for any $\gamma \in \mathscr{S}(\widehat{f})$ with $\mathrm{wt}(\gamma) = 4$.

Remember that $\widehat{f}(\vec{0}^8) = a$ where $|a| = 1$. Then, $\widehat{f}(\vec{1}^8) = \bar{a}$ by ARS. Suppose that $a = e^{\mathfrak{i}\theta}$. Let $\widehat{Q} = \left[\begin{smallmatrix} \rho & 0 \\ 0 & \bar{\rho} \end{smallmatrix}\right] \in \widehat{\mathbf{O}_2}$ where $\rho = e^{-\mathfrak{i}\theta/8}$. Consider the holographic transformation by $\widehat{Q}$. $\widehat{Q}$ does not change the entries of $\widehat{f}$ on half-weighed inputs, but change the values of $\widehat{f}(\vec{0}^8)$ and $\widehat{f}(\vec{1}^8)$ to 1. Thus, $\widehat{Q}\widehat{f} = \widehat{f_8}$. Then, $\operatorname{Holant}(\neq_2|\ \widehat{f_8}, \widehat{Q}\widehat{\mathcal{F}}) \leqslant_T \operatorname{Holant}(\neq_2|\ \widehat{\mathcal{F}})$. □

Now, we want to show that $\operatorname{Holant}(\neq_2|\ \widehat{f_8}, \widehat{Q}\widehat{\mathcal{F}})$ is #P-hard for all $\widehat{Q} \in \widehat{\mathbf{O}_2}$ and all $\widehat{\mathcal{F}}$ where $\mathcal{F} = Z\widehat{\mathcal{F}}$ is a real-valued signature set that does not satisfy condition (T). If so, then we are done. Recall that for all $\widehat{Q} \in \widehat{\mathbf{O}_2}$, $\widehat{Q}\widehat{\mathcal{F}} = \widehat{Q\mathcal{F}}$ for some $Q \in \mathbf{O}_2$. Moreover, for all $Q \in \mathbf{O}_2$, and all real-valued $\mathcal{F}$ that does not satisfy condition (T), $Q\mathcal{F}$ is also a real-valued signature set that does not satisfy condition (T). Thus, it suffices for us to show that $\operatorname{Holant}(\neq_2|\ \widehat{f_8}, \widehat{\mathcal{F}})$ is #P-hard for all real-valued $\mathcal{F}$ that does not satisfy condition (T).

The following Lemma shows that $\widehat{f_8}$ gives non-$\widehat{\mathcal{B}}$ hardness (Definition 7.8).

Lemma 8.7. *$\operatorname{Holant}(\neq_2|\ \widehat{f_8}, \widehat{\mathcal{F}})$ is #P-hard if $\widehat{\mathcal{F}}$ contains a nonzero binary signature $\widehat{b} \notin \widehat{\mathcal{B}}^{\otimes}$. Equivalently, $\operatorname{Holant}(f_8, \mathcal{F})$ is #P-hard if $\mathcal{F}$ contains a nonzero binary signature $b \notin \mathcal{B}^{\otimes}$.*

证明. We prove this lemma in the setting of $\operatorname{Holant}(\neq_2|\ \widehat{f_8}, \widehat{\mathcal{F}})$. If $\widehat{b} \notin \widehat{\mathcal{O}}^{\otimes}$, then by Lemma 6.7, we get #P-hardness. Thus, we may assume that $\widehat{b} \in \widehat{\mathcal{O}}^{\otimes}$. Then, $\widehat{b}$ has parity. We first consider the case that $\widehat{b}$ has even parity, i.e., $\widehat{b} = (a, 0, 0, \bar{a})$. Since $\widehat{b} \not\equiv 0$, $a \neq 0$. We can normalize a to $e^{\mathfrak{i}\theta}$ where $0 \leqslant \theta < \pi$. Then $\bar{a} = e^{-\mathfrak{i}\theta}$. Since $\widehat{b} \notin \widehat{\mathcal{B}}$, $a \neq \pm 1$ and $a \neq \pm \mathfrak{i}$. Thus, $\theta \neq 0$ and $\theta \neq \frac{\pi}{2}$.

We connect variables x_1 and x_5 of $\widehat{f_8}$ with the two variables of $\widehat{b}$ (using $\neq_2$), and we get a 6-ary signature denoted by $\widehat{g}$. We rename variables x_2, x_3, x_4 of $\widehat{g}$ to x_1, x_2, x_3 and variables x_6, x_7, x_8 to x_4, x_5, x_6. Then, $\widehat{g}$ has the following signature matrix

$$M_{123,456}(\widehat{g}) = \begin{bmatrix} e^{-\mathfrak{i}\theta} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{\mathfrak{i}\theta} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{\mathfrak{i}\theta} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{-\mathfrak{i}\theta} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{\mathfrak{i}\theta} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{-\mathfrak{i}\theta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & e^{-\mathfrak{i}\theta} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{\mathfrak{i}\theta} \end{bmatrix}.$$

Now, we show that $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$. For a contradiction, suppose that $\widehat{g} \in \widehat{\mathcal{O}}^{\otimes}$. Notice that $\mathscr{S}(\widehat{g}) = \{(x_1, \ldots, x_6) \in \mathbb{Z}_2^6 \mid x_1 = x_4,\ x_2 = x_5 \text{ and } x_3 = x_6\}$. Then, we can write $\widehat{g}$ as

$$\widehat{g} = \widehat{b_1}(x_1, x_4) \otimes \widehat{b_2}(x_2, x_5) \otimes \widehat{b_3}(x_3, x_6),$$

where $\widehat{b_1} = (e^{\mathrm{i}\theta_1}, 0, 0, e^{-\mathrm{i}\theta_1})$, $\widehat{b_2} = (e^{\mathrm{i}\theta_2}, 0, 0, e^{-\mathrm{i}\theta_2})$ and $\widehat{b_3} = (e^{\mathrm{i}\theta_3}, 0, 0, e^{-\mathrm{i}\theta_3})$. Then notice that

$$\widehat{g}^{000000} = e^{-\mathrm{i}\theta} = \widehat{b_1}(0,0) \cdot \widehat{b_2}(0,0) \cdot \widehat{b_3}(0,0) = e^{\mathrm{i}(\theta_1+\theta_2+\theta_3)},$$

and

$$\widehat{g}^{011011} = e^{-\mathrm{i}\theta} = \widehat{b_1}(0,0) \cdot \widehat{b_2}(1,1) \cdot \widehat{b_3}(1,1) = e^{\mathrm{i}(\theta_1-\theta_2-\theta_3)}.$$

By multiplying the above two equations, we have

$$e^{-\mathrm{i}2\theta} = e^{\mathrm{i}(\theta_1+\theta_2+\theta_3)} \cdot e^{\mathrm{i}(\theta_1-\theta_2-\theta_3)} = e^{\mathrm{i}2\theta_1}.$$

Also, notice that

$$\widehat{g}^{001001} = e^{\mathrm{i}\theta} = \widehat{b_1}(0,0) \cdot \widehat{b_2}(0,0) \cdot \widehat{b_3}(1,1) = e^{\mathrm{i}(\theta_1+\theta_2-\theta_3)},$$

and

$$\widehat{g}^{010010} = e^{\mathrm{i}\theta} = \widehat{b_1}(0,0) \cdot \widehat{b_2}(1,1) \cdot \widehat{b_3}(0,0) = e^{\mathrm{i}(\theta_1-\theta_2+\theta_3)}.$$

By multiplying them, we have

$$e^{\mathrm{i}2\theta} = e^{\mathrm{i}(\theta_1+\theta_2-\theta_3)} \cdot e^{\mathrm{i}(\theta_1-\theta_2+\theta_3)} = e^{\mathrm{i}2\theta_1}.$$

Thus, $e^{\mathrm{i}2\theta} = e^{-\mathrm{i}2\theta}$. Then, $e^{\mathrm{i}4\theta} = 1$. Since, $\theta \in [0, \pi)$, $\theta = 0$ or $\frac{\pi}{2}$. Contradiction. Thus, $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$. By Lemma 7.40, we get #P-hardness.

Now, suppose that $\widehat{b}$ has odd parity, i.e., $\widehat{b}(y_1, y_2) = (0, e^{\mathrm{i}\theta}, e^{-\mathrm{i}\theta}, 0)$ where $\theta \in [0, \pi)$ after normalization. We still consider the 6-ary signature $\widehat{g'}$ that is realized by connecting variables x_1 and x_5 of $\widehat{f_8}$ with the two variables y_1 and y_2 of $\widehat{b}$ (using $\neq_2$). Then, after renaming variables, $\widehat{g'}$

has the following signature matrix

$$M_{123,456}(\widehat{g'}) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{-\mathrm{i}\theta} \\ 0 & 0 & 0 & 0 & 0 & 0 & e^{\mathrm{i}\theta} & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{\mathrm{i}\theta} & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{-\mathrm{i}\theta} & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{\mathrm{i}\theta} & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{-\mathrm{i}\theta} & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{-\mathrm{i}\theta} & 0 & 0 & 0 & 0 & 0 & 0 \\ e^{\mathrm{i}\theta} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Similarly, we can show that $\widehat{g'} \notin \widehat{\mathcal{O}}^{\otimes}$. Thus, by Lemma 7.40, we get #P-hardness. □

We go back to real-valued Holant problems under the Z-transformation. Consider the problem $\operatorname{Holant}(f_8, \mathcal{F})$. Remember that $f_8 = \widehat{f_8}$. We observe that, by Lemma 8.7 the set $\{f_8\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard, according to Definition 7.8. Then if we apply Theorem 7.38 to the set $\{f_8\} \cup \mathcal{F}$ we see that $\operatorname{Holant}^b(f_8, \mathcal{F})$ is #P-hard. Now *if we were able to show* that $\mathcal{B}$ is realizable from f_8 then we would be done, since by Theorem 8.6, we either already have the #P-hardness for $\operatorname{Holant}(\mathcal{F})$, or we can realize f_8 from $\mathcal{F}$, and thus the following reduction chain holds

$$\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(\mathcal{F}).$$

Thus we get the #P-hardness of $\operatorname{Holant}(\mathcal{F})$ in either way.

However, since f_8 has even parity and all its entries are non-negative, all gadgets realizable from f_8 have even parity and have non-negative entries. Thus, $=_2^-$, $\neq_2$ and $\neq_2^-$ *cannot* be realized from f_8 by gadget construction. In fact, f_8 satisfies the following strong Bell property.

Definition 8.8. *A signature f satisfies the strong Bell property if for all pairs of indices $\{i, j\}$, and every $b \in \mathcal{B}$, the signature $\partial_{ij}^b f$ realized by merging x_i and x_j of f using b is in $\{b\}^{\otimes}$.*

8.2 Holant Problems with Limited Appearance

In this section, *not using gadget construction* but critically based on the strong Bell property of f_8, we prove that $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$ in a novel way. We define the following Holant problems with limited appearance.

Definition 8.9. *Let $\mathcal{F}$ be a signature set containing a signature f. The problem* $\operatorname{Holant}(f^{\leqslant k}, \mathcal{F})$ *contains all instances of* $\operatorname{Holant}(\mathcal{F})$ *where the signature f appears at most k times.*

Lemma 8.10. *For any $b \in \mathcal{B}$,* $\operatorname{Holant}(b, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b^{\leqslant 2}, f_8, \mathcal{F})$.

证明. Consider an instance Ω of $\operatorname{Holant}(b, f_8, \mathcal{F})$. Suppose that b appears n times in Ω. If $n \leqslant 2$, then Ω is already an instance of $\operatorname{Holant}(b^{\leqslant 2}, f_8, \mathcal{F})$. Otherwise, $n \geqslant 3$. Consider the gadget $\partial^b_{ij} f_8$ realized by connecting two variables x_i and x_j of f_8 using b. (This gadget uses b only once.) Since f_8 satisfies the strong Bell property, $\partial^b_{ij} f_8 = b^{\otimes 3}$. Thus, by replacing three occurrences of b in Ω by $\partial^b_{ij} f_8$, we can reduce the number of occurrences of b by 2. We carry out this replacement a linear number of times to obtain an equivalent instance of $\operatorname{Holant}(b^{\leqslant 2}, f_8, \mathcal{F})$, of size linear in Ω. □

Now, we are ready to prove the reduction $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$. Note that if $\operatorname{Holant}(f_8, \mathcal{F})$ is #P-hard, then the reduction holds trivially. For any $b \in \mathcal{B}$, if we connect a variable of b with a variable of another copy of b using $=_2$, we get $\pm(=_2)$. Also, for any $b_1, b_2 \in \mathcal{B}$ where $b_1 \neq b_2$ if we connect the two variables of b_1 with the two variables of b_2, we get a value 0.

Lemma 8.11. $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$.

证明. We prove this reduction in two steps.

Step 1. There exists a signature $b_1 \in \mathcal{B} \backslash \{=_2\}$ such that $\operatorname{Holant}(b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$.

We consider *all* binary and 4-ary signatures realizable by gadget constructions from $\{f_8\} \cup \mathcal{F}$. If a binary signature $g \notin \mathcal{B}$ is realizable from $\{f_8\} \cup \mathcal{F}$, then by Lemma 8.7, $\operatorname{Holant}(f_8, \mathcal{F})$ is #P-hard, and we are done. If a binary signature $g \in \mathcal{B} \backslash \{=_2\}$ is realizable from $\{f_8\} \cup \mathcal{F}$, then we are done by choosing $b_1 = g$. So we may assume that all binary signatures g realizable from $\{f_8\} \cup \mathcal{F}$ are $=_2$ (up to a scalar) or the zero binary signature, i.e., $g = \mu \cdot (=_2)$ for some $\mu \in \mathbb{R}$. Similarly, if a nonzero 4-ary signature $h \notin \mathcal{B}^{\otimes 2}$ is realizable, then we have $\operatorname{Holant}(f_8, \mathcal{F})$ is #P-hard, by Lemma 7.9, as Lemma 8.7 says the set $\{f_8\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard. If a nonzero 4-ary signature $h \in \mathcal{B}^{\otimes 2} \backslash \{=_2\}^{\otimes 2}$ is realizable, then we can realize a binary signature $b_1 \in \mathcal{B}\backslash\{=_2\}$ by factorization, and we are done. Thus, we may assume that all 4-ary signatures h realizable from $\{f_8\} \cup \mathcal{F}$ are $(=_2)^{\otimes 2}$ or the 4-ary zero signature, i.e., $h = \lambda \cdot (=_2)^{\otimes 2}$ for some $\lambda \in \mathbb{R}$.

Now, let b_1 be a signature in $\mathcal{B}\backslash\{=_2\}$. We show that $\operatorname{Holant}(b_1^{\leqslant 2}, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$. Consider an instance Ω of $\operatorname{Holant}(b_1^{\leqslant 2}, f_8, \mathcal{F})$.

- If b_1 does not appear in Ω, then Ω is already an instance of $\operatorname{Holant}(f_8, \mathcal{F})$.

- If b_1 appears exactly once in Ω (we may assume it does connect to itself), then we may consider *the rest of* Ω *that connects to* b_1 as a gadget realized from $\{f_8\} \cup \mathcal{F}$, which must have signature $\lambda \cdot (=_2)$, for some $\lambda \in \mathbb{R}$. Connecting the two variables of b_1 by $(=_2)$ for every $b_1 \in \mathcal{B}\backslash\{=_2\}$ will always gives 0. Thus, $\operatorname{Holant}(\Omega) = 0$.

- Suppose b_1 appears exactly twice in Ω. It is easy to handle when the two copies of b_1 form a gadget of arity 0 or 2 to the rest of Ω. We may assume they are connected to the rest of Ω in such a way that the rest of Ω forms a 4-ary gadget h realized from $\{f_8\} \cup \mathcal{F}$. We can name the four dangling edges of h in any specific ordering as (x_1, x_2, x_3, x_4). Then

  $$h(x_1, x_2, x_3, x_4) = \lambda \cdot (=_2)(x_1, x_j) \otimes (=_2)(x_k, x_\ell)$$

  for some partition $\{1, 2, 3, 4\} = \{1, j\} \sqcup \{k, \ell\}$, and some $\lambda \in \mathbb{R}$. (Note that while we have named four specific dangling edges as (x_1, x_2, x_3, x_4), the specific partition $\{1, 2, 3, 4\} = \{1, j\} \sqcup \{k, \ell\}$ and the value λ are unknown at this point.) We consider the following three instances Ω_{12}, Ω_{13}, and Ω_{14}, where Ω_{1s} ($s \in \{2, 3, 4\}$) is the instance formed by merging variables x_1 and x_s of h using $=_2$, and merging the other two variables of h using $=_2$ (see Figure 9 where $h_1 = h_2 = (=_2)$ and $h = \lambda \cdot h_1 \otimes h_2$). Since h is a gadget realized from $\{f_8\} \cup \mathcal{F}$, Ω_{12}, Ω_{13}, and Ω_{14} are instances of $\operatorname{Holant}(f_8, \mathcal{F})$. Note that $\operatorname{Holant}(\Omega_{1s}) = 4\lambda$ when $s = j$ and $\operatorname{Holant}(\Omega_{1s}) = 2\lambda$ otherwise. Thus, by computing $\operatorname{Holant}(\Omega_{1s})$ for $s \in \{2, 3, 4\}$, we can get λ, and if $\lambda \neq 0$ the partition $\{1, j\} \sqcup \{k, \ell\}$ of the four variables. Thus we can get the exact structure of the 4-ary gadget h. In either case (whether $\lambda = 0$ or not), we can compute the value of $\operatorname{Holant}(\Omega)$.

Thus, $\operatorname{Holant}(b_1^{\leqslant 2}, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$. By Lemma 8.10, $\operatorname{Holant}(b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$.

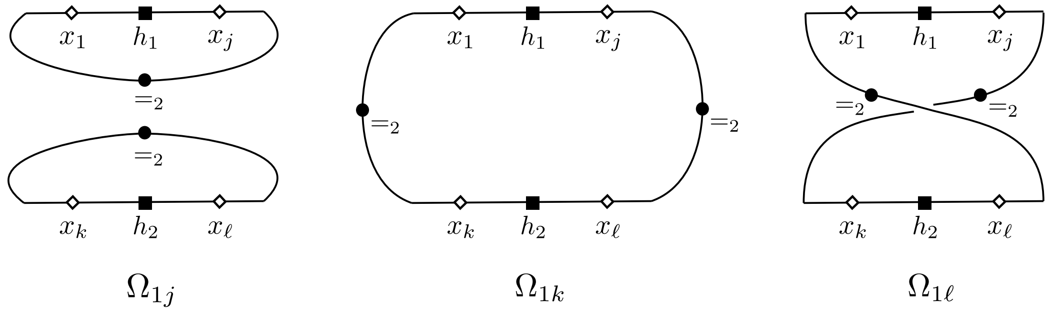


图 9: Instances Ω_{1j}, Ω_{1k} and $\Omega_{1\ell}$

Step 2. For any $b_1 \in \mathcal{B}\backslash\{=_2\}$, we have $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F})$.

We show that we can get another $b_2 \in \mathcal{B}\backslash\{=_2, b_1\}$, i.e., for some binary signature $b_2 \in \mathcal{B}\backslash\{=_2, b_1\}$ we have the reduction $\operatorname{Holant}(b_2, b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F})$. Then, by connecting one variable of b_1 and one variable of b_2 using $=_2$, we get the third signature in $\mathcal{B}\backslash\{b_1, b_2\}$. Then, the lemma is proved. The proof is similar to the proof in Step 1. We consider *all* binary and 4-ary gadgets realizable from $\{b_1, f_8\} \cup \mathcal{F}$. Still, we may assume that all realizable binary signatures are of the form $\mu \cdot (=_2)$ or $\mu \cdot b_1$ for some $\mu \in \mathbb{R}$, and all realizable 4-ary signatures are of form $\lambda \cdot (=_2)^{\otimes 2}$, $\lambda \cdot b_1^{\otimes 2}$ or $\lambda \cdot (=_2) \otimes b_1$ for some $\lambda \in \mathbb{R}$. Otherwise, we can show that $\operatorname{Holant}(b_1, f_8, \mathcal{F})$ is #P-hard or we realize a signature $b_2 \in \mathcal{B}\backslash\{=_2, b_1\}$ directly by gadget construction.

Then, let b_2 be an arbitrary signature in $\mathcal{B}\backslash\{=_2, b_1\}$. We show that

$$\operatorname{Holant}(b_2^{\leqslant 2}, b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F}).$$

Consider an instance Ω of $\operatorname{Holant}(b_2^{\leqslant 2}, b_1, f_8, \mathcal{F})$. If b_2 does not appear in Ω, then Ω is already an instance of $\operatorname{Holant}(b_1, f_8, \mathcal{F})$. If b_2 appears exactly once in Ω, then it is connected with a binary gadget g where $g = \mu \cdot (=_2)$ or $g = \mu \cdot b_1$. In both cases, the evaluation is 0. Thus, $\operatorname{Holant}(\Omega) = 0$. Suppose b_2 appears exactly twice in Ω. Again it is easy to handle the case if the rest of Ω forms a gadget of arity 0 or 2 to the two occurrences of b_2. So we may assume the two occurrences of b_2 are connected to a 4-ary gadget $h = \lambda \cdot (=_2)^{\otimes 2}$, $\lambda \cdot b_1^{\otimes 2}$ or $\lambda \cdot (=_2) \otimes b_1$. We denote the four variables of h by (x_1, x_2, x_3, x_4), by an arbitrary ordering of the four dangling edges. Then $h(x_1, x_2, x_3, x_4) = \lambda \cdot h_1(x_1, x_j) \otimes h_2(x_k, x_\ell)$ where $h_1, h_2 \in \{=_2, b_1\}$, for some λ and $\{j, k, \ell\} = \{2, 3, 4\}$. (Note that at the moment the values λ and j, k, ℓ are unknown.) We consider the following three instances Ω_{12}, Ω_{13} and Ω_{14}, where Ω_{1s} ($s \in \{2, 3, 4\}$) is the instance formed by connecting variables x_1 and x_s of h using $=_2$, and connecting the other two variables of h using $=_2$ (again see Figure 9). Clearly, Ω_{12}, Ω_{13} and Ω_{14} are instances of $\operatorname{Holant}(b_1, f_8, \mathcal{F})$. Consider the evaluations of these instances. We have three cases.

- If $h_1 = h_2 = (=_2)$, then $\operatorname{Holant}(\Omega_{1s}) = 4\lambda$ when $s = j$ and $\operatorname{Holant}(\Omega_{1s}) = 2\lambda$ when $s \neq j$.
- If $h_1 = h_2 = b_1$, then $\operatorname{Holant}(\Omega_{1s}) = 0$ when $s = j$. If $M(b_1)$ is the 2 by 2 matrix form for the binary signature b_1 where we list its first variable as row index and second variable as column index, then we have $\operatorname{Holant}(\Omega_{1k}) = \lambda \cdot \operatorname{tr}(M(b_1)M(b_1)^{\mathtt{T}})$, and $\operatorname{Holant}(\Omega_{1\ell}) = \lambda \cdot \operatorname{tr}(M(b_1)^2)$, where tr denotes trace. For $b_1 = (=_2^-)$ or $(\neq_2^+)$, the matrix $M(b_1)$ is symmetric, and the value $\operatorname{Holant}(\Omega_{1s}) = 2\lambda$ in both cases $s = k$ or $s = \ell$. For $b_1 = (\neq_2^-)$, $M(b_1)^{\mathtt{T}} = -M(b_1)$, and we have $\operatorname{Holant}(\Omega_{1k}) = 2\lambda$, and $\operatorname{Holant}(\Omega_{1\ell}) = -2\lambda$.
- If one of h_1 and h_2 is $=_2$ and the other is b_1, then $\operatorname{Holant}(\Omega_{1s}) = 0$ for all $s \in \{j, k, \ell\}$.

Thus, if the values of $\operatorname{Holant}(\Omega_{1s})$ for $s \in \{2, 3, 4\}$ are not all zero, then $\lambda \neq 0$ and the third case is impossible, and we can tell whether h is in the form $\lambda \cdot (=_2)^{\otimes 2}$ or $\lambda \cdot (b_1)^{\otimes 2}$. Moreover we can get the exact structure of h, i.e., the value λ and the decomposition form of h_1 and h_2. Otherwise, the values of $\operatorname{Holant}(\Omega_{1s})$ for $s \in \{2, 3, 4\}$ are all zero. Then we can write $h = \lambda \cdot (=_2)(x_1, x_j) \otimes b_1(x_k, x_\ell)$ or $h = \lambda \cdot b_1(x_1, x_j) \otimes (=_2)(x_k, x_\ell)$, including possibly $\lambda = 0$, which means $h \equiv 0$. (Note that if $\lambda \neq 0$, this uniquely identifies that we are in the third case; if $\lambda = 0$ then this form is still formally valid, even though we cannot say this uniquely identifies the third case. But when $\lambda = 0$ all three cases are the same, i.e., $h \equiv 0$.) At this point we still do not know the exact value of λ and the decomposition form of h.

We further consider the following three instances Ω'_{12}, Ω'_{13} and Ω'_{14}, where Ω'_{1s} ($s \in \{2, 3, 4\}$) is the instance formed by connecting variables x_1 and x_s of h using b_1, and connecting the other two variables of h using $=_2$. (In other words, we replace the labeling $=_2$ of the edge that is connected to the variable x_1 in each instance illustrated in Figure 9 by b_1.) It is easy to see that Ω'_{12}, Ω'_{13} and Ω'_{14} are instances of $\operatorname{Holant}(b_1, f_8, \mathcal{F})$. Consider the evaluations of these instances.

- If $h_1 = (=_2)(x_1, x_j)$, then $\operatorname{Holant}(\Omega'_{1s}) = 0$ when $s = j$. Also we have $\operatorname{Holant}(\Omega_{1k}) = \lambda \cdot \operatorname{tr}(M(b_1)^2)$, and $\operatorname{Holant}(\Omega_{1\ell}) = \lambda \cdot \operatorname{tr}(M(b_1)M(b_1)^{\mathtt{T}})$. For $b_1 = (=_2^-)$ or $\neq_2^+$, the matrix

$M(b_1)$ is symmetric, and the value $\operatorname{Holant}(\Omega_{1s}) = 2\lambda$ in both cases $s = k$ or $s = \ell$. For $b_1 = (\neq_2^-)$, $M(b_1)^{\mathtt{T}} = -M(b_1)$, and we have $\operatorname{Holant}(\Omega_{1k}) = -2\lambda$, and $\operatorname{Holant}(\Omega_{1\ell}) = 2\lambda$.

- If $h_1 = b_1(x_1, x_j)$, then $\operatorname{Holant}(\Omega'_{1s}) = 4\lambda$ when $s = j$ and $\operatorname{Holant}(\Omega'_{1s}) = 2\lambda$ when $s \neq j$.

Thus, by further computing $\operatorname{Holant}(\Omega'_{1s})$ for $s \in \{2, 3, 4\}$, we can get the exact structure of h.

Therefore, by querying $\operatorname{Holant}(b_1, f_8, \mathcal{F})$ at most 6 times, we can compute h exactly. Then, we can compute $\operatorname{Holant}(\Omega)$ easily. Thus, $\operatorname{Holant}(b_2^{\leqslant 2}, b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F})$. By Lemma 8.10, $\operatorname{Holant}(b_2, b_1, f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F})$. The other signature in $\mathcal{B} \backslash \{=_2, b_1, b_2\}$ can be realized by connecting b_1 and b_2. Thus, $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(b_1, f_8, \mathcal{F})$.

Therefore, $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$. □

Since $\operatorname{Holant}^b(f_8, \mathcal{F}) \leqslant_T \operatorname{Holant}(f_8, \mathcal{F})$ and $\{f_8\} \cup \mathcal{F}$ is non-$\mathcal{B}$ hard for any real-valued $\mathcal{F}$ that does not satisfy condition (T), by Theorem 7.38, we have the following result.

Lemma 8.12. $\operatorname{Holant}(f_8, \mathcal{F})$ *is #P-hard.*

Combining Theorem 8.6 and Lemma 8.12, we have the following result.

Lemma 8.13. *If* $\widehat{\mathcal{F}}$ *contains a signature* $\widehat{f}$ *of arity* 8 *and* $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, *then* $\operatorname{Holant}(\neq_2 | \widehat{\mathcal{F}})$ *is #P-hard.*

8.3 The Induction Proof: $2n \geqslant 10$

Now, we show that our induction framework works for signatures of arity $2n \geqslant 10$.

Lemma 8.14. *If* $\widehat{\mathcal{F}}$ *contains a signature* $\widehat{f}$ *of arity* $2n \geqslant 10$ *and* $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$, *then,*

- $\operatorname{Holant}(\neq_2 | \widehat{\mathcal{F}})$ *is #P-hard, or*
- *a signature* $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$ *of arity* $2k \leqslant 2n - 2$ *is realizable from* $\widehat{f}$.

证明. By Lemma 8.1, we may assume that an irreducible signature $\widehat{f^*}$ of arity $2n \geqslant 10$ where $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$ is realizable, and $\widehat{f^*}$ satisfies ARS. We show that $\widehat{f^*}$ does not satisfy 2ND-ORTH, and hence we get #P-hardness.

For all pairs of indices $\{i, j\}$, since $\widehat{\partial}_{ij}\widehat{f^*} \in \mathcal{D}^{\otimes}$, $\mathscr{S}(\widehat{\partial}_{ij}\widehat{f^*})$ is on half-weight. By Lemma 3.9, we have $\widehat{f^*}(\alpha) = 0$ for all $\operatorname{wt}(\alpha) \neq 0, n, 2n$. Suppose that $\widehat{f^*}(\vec{0}^{2n}) = a$ and $\widehat{f^*}(\vec{1}^{2n}) = \bar{a}$ by ARS. We can write $\widehat{f^*}$ in the following form

$$\widehat{f^*} = a(1,0)^{\otimes 2n} + \bar{a}(0,1)^{\otimes 2n} + \widehat{f^*_{\mathrm{h}}}.$$

where $\widehat{f^*_{\mathrm{h}}}$ is an EO signature of arity $2n \geqslant 10$.

Clearly, $\partial_{ij}\widehat{f^*} = \partial_{ij}\widehat{f^*_{\mathrm{h}}}$ for all $\{i,j\}$. Then, $\widehat{f^*_{\mathrm{h}}} \in \widehat{\int}\mathcal{D}^{\otimes}$ since $\widehat{f^*} \in \widehat{\int}\mathcal{D}^{\otimes}$. Since $\widehat{f^*_{\mathrm{h}}}$ is an EO signature of arity at least 10 and $\widehat{f^*_{\mathrm{h}}} \in \widehat{\int}\mathcal{D}^{\otimes}$, by Lemma 4.19, we have $\widehat{f^*_{\mathrm{h}}} \in \mathcal{D}^{\otimes}$. Recall that all signatures in $\mathcal{D}^{\otimes}$ are nonzero by definition. Pick some $\{i,j\}$ such that $(\neq_2)(x_i,x_j) \mid \widehat{f^*_{\mathrm{h}}}$. Then,

$$\widehat{f^*} = a(1,0)^{\otimes 2n} + \bar{a}(0,1)^{\otimes 2n} + \widehat{b}^*(x_i,x_j) \otimes \widehat{g^*_{\mathrm{h}}},$$

where $\widehat{g^*_{\mathrm{h}}} \in \mathcal{D}^{\otimes}$ is a nonzero EO signature since $\widehat{f^*_{\mathrm{h}}} \in \mathcal{D}^{\otimes}$. By Lemma 8.3, $\widehat{f^*}$ does not satisfy 2nd-Orth. Thus, Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard by Lemma 6.6. □

Remark 8.15. *Indeed, following from our proof, we can also show that there is no irreducible signature $\widehat{f}$ of arity $2n \geqslant 10$ that satisfies both* 2nd-Orth *and $\widehat{f} \in \widehat{\int}\widehat{\mathcal{O}}^{\otimes}$.*

8.4 Proof of the Real Holant Dichotomy

Finally, we give the proof of Theorem 1.1. We restate it here.

Theorem 8.16. *Let $\mathcal{F}$ be a set of real-valued signatures. If $\mathcal{F}$ satisfies the tractability condition* (T) *in Theorem 2.33, then* Holant$(\mathcal{F})$ *is polynomial-time computable; otherwise,* Holant$(\mathcal{F})$ *is #P-hard.*

证明. By Theorem 2.33, if $\mathcal{F}$ satisfies condition (T), then Holant$(\mathcal{F})$ is P-time computable. Suppose that $\mathcal{F}$ does not satisfy condition (T). If $\mathcal{F}$ contains a nonzero signature of odd arity, then by Theorem 5.35, Holant$(\mathcal{F})$ is #P-hard. We show Holant$(\neq_2 \mid \widehat{\mathcal{F}}) \equiv_T$ Holant$(\mathcal{F})$ is #P-hard when $\mathcal{F}$ is a set of signatures of even arity. Since $\mathcal{F}$ does not satisfy condition (T), $\widehat{\mathcal{F}} \not\subseteq \mathscr{T}$. Since $\widehat{\mathcal{O}}^{\otimes} \subseteq \mathscr{T}$, there is a signature $\widehat{f} \in \widehat{\mathcal{F}}$ of arity $2n$ such that $\widehat{f} \notin \widehat{\mathcal{O}}^{\otimes}$. We prove this theorem by induction on $2n$.

When $2n \leqslant 8$, by Lemmas 6.7, 6.8, 7.40, 8.13, Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard.

Inductively, suppose for some $2k \geqslant 8$, if $2n \leqslant 2k$, then Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard. We consider $2n = 2k+2 \geqslant 10$. By Lemma 8.14, Holant$(\neq_2 \mid \widehat{\mathcal{F}})$ is #P-hard, or Holant$(\neq \mid \widehat{g}, \widehat{\mathcal{F}}) \leqslant_T$ Holant$(\neq \mid \widehat{\mathcal{F}})$

for some $\widehat{g} \notin \widehat{\mathcal{O}}^{\otimes}$ of arity $\leqslant 2k$. By the induction hypothesis, Holant($\neq\mid \widehat{g}, \widehat{\mathcal{F}}$) is #P-hard. Thus, Holant($\neq_2\mid \widehat{\mathcal{F}}$) is #P-hard. □

Chapter 9

Trichotomy for Planar Six-Vertex Models

In this chapter, we consider the complexity of Holant problems over planar graphs. We give a new family of six-vertex models that are #P-hard in general, but tractable over planar graphs. We prove a complete complexity classification for planar six-vertex models.

9.1 Background

The six-vertex model has a long history in physics. Pauling in 1935 introduced the six-vertex model to account for the residual entropy of water ice [61]. Consider a large number of oxygen and hydrogen atoms in a 1 to 2 ratio. Each oxygen atom (O) is connected by a bond to four other neighboring oxygen atoms (O), and each bond is occupied by one hydrogen atom (H). Physical constraint requires that each (H) is closer to exactly one of the two neighboring (O). Pauling argued [61] that, furthermore, the allowed configurations are such that at each oxygen (O) site, exactly two hydrogen (H) are closer to it, and the other two are farther away. This can be naturally represented by a 4-regular graph. The constraint on the placement of hydrogen atoms (H) can be represented by an orientation of the edges of the graph, such that at every vertex (O), the in-degree and out-degree are both 2. In other words, this is an *Eulerian orientation* [58, 23]. Since there are $\binom{4}{2} = 6$ local valid configurations, this is called the six-vertex model. In addition to water ice, potassium dihydrogen phosphate KH_2PO_4 (KDP) also satisfies this model.

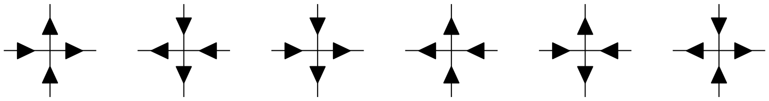


图 10: Valid configurations of the six-vertex model

The valid local configurations of the six-vertex model are illustrated in Figure 10. The energy E of the system is determined by six parameters $\epsilon_1, \epsilon_2, \ldots, \epsilon_6$ associated with each type of local configuration. If there are n_i sites in local configurations of type i, then $E = n_1\epsilon_1 + n_2\epsilon_2 + \ldots + n_6\epsilon_6$. Then the partition function is $Z_{\text{Six}} = \sum e^{-E/k_B T}$, where the sum is over all valid configurations, k_B is Boltzmann's constant, and T is the system's temperature. This is a *sum-of-product* computation where the sum is over all Eulerian orientations of the graph, and the product is over all vertices where each contributes a factor $c_i = c^{\epsilon_i}$ if it is in configuration i ($1 \le i \le 6$) for some constant c.

Some choices of the parameters are well-studied. For modeling ice ($\epsilon_1 = \ldots = \epsilon_6 = 0$) on the square $N \times N$ lattice graph, Lieb [56] famously showed that, the value of the "partition function per vertex" $W = Z^{1/N^2}$ approaches $\left(\frac{4}{3}\right)^{3/2} \approx 1.5396007\ldots$ (Lieb's square ice constant). This matched experimental data 1.540 ± 0.001 so well that it is considered a triumph. Other well-known six-vertex models include: the KDP model of a ferroelectric ($\epsilon_1 = \epsilon_2 = 0$, and $\epsilon_3 = \epsilon_4 = \epsilon_5 = \epsilon_6 > 0$), the Rys F model of an antiferroelectric ($\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 > 0$, and $\epsilon_5 = \epsilon_6 = 0$). Historically these are widely considered among the most significant applications ever made of statistical mechanics to real substances. In classical statistical mechanics the parameters are real numbers. However, it's meaningful to consider parameters over complex values. In quantum theory the parameters are generally complex valued. Even in classical theory, for example, Baxter generalized the parameters to complex values to develop the "commuting transfer matrix" for tackling the six-vertex model [7]. Some other models can be transformed to a six-vertex model with complex weights. There are books with sections (e.g., see section 2.5.2 of [44]) that are dedicated to this, for example, the Hamiltonian of a one dimensional spin chain is simply an extension of the Hamiltonian of a six-vertex model with complex Boltzmann weights.

The six-vertex model has broad connections to combinatorics. The resolution of the famous *Alternating Sign Matrix* conjecture is one example [50, 59, 75, 51, 10]. Also, the Tutte polynomial on a planar graph at the point $(3, 3)$ is precisely $1/2$ of Z_{Six} on its medial graph which is also a planar graph with a specific weight assignment [53].

Although Pauling most likely did not think of it in such terms, the six-vertex model can be expressed perfectly as a family of Holant problems with 6 parameters, expressed by signatures of arity 4. Previously, without being able to account for the planar restriction, it has been proved [25] that there is a complexity dichotomy where the problem on general graphs is either in P or #P-hard. However, the more interesting problem is what happens on planar structures where physicists had discovered some remarkable algorithms, such as the FKT algorithm [66, 49, 48]. Due to the presence of nontrivial algorithms, a complete complexity classification in the planar case is more difficult to achieve. Not only are reductions to FKT expected to give planar P-time computable cases that are #P-hard in general, but also a more substantial obstacle awaits us. It turns out that there is *another* planar P-time computable case that had not been discovered for the six-vertex model in all these decades, till now. (Since our algorithm and its proof that it runs in P-time is valid for all planar graphs, this certainly also applies to the grid case, which is traditionally the main concern for physicists.)

The main theorem in this chapter is a complexity trichotomy for the six-vertex model: According to the 6 parameters from $\mathbb{C}$, the partition function Z_{Six} is either (1) computable in P-time, or (2) #P-hard on general graphs but computable in P-time on planar graphs, or (3) remains #P-hard on planar graphs. The classification has an explicit criterion. The planar tractable class (2) includes those that depend on FKT, and a previously unknown family. Functions that are expressible as matchgates (denoted by $\mathscr{M}$) or those that are transformable to matchgates (denoted by $\widehat{\mathscr{M}}$) do constitute a family of Z_{Six} in class (2). This follows from the FKT and Valiant's holographic algorithms [72].* However, beyond these, we discover an additional family of P-time computable Z_{Six} on planar graphs. The P-time tractability is via a non-local reduction to P-time computable #CSP, where the variables in #CSP correspond to carefully defined circuits in G. The fact that this #CSP problem is in P depends crucially on the global topological constraint imposed by the planarity of G (but the #CSP instances that this produces is not planar in general.) The new tractable class provably cannot be subsumed by FKT (even with a holographic transformation).

After carving out this last tractable family, we prove that everything else is #P-hard, even for the planar case. A powerful tool in hardness proofs is interpolation [67]. Typically an interpolation proof can succeed when certain quantities (such as ratios of eigenvalues) are not roots of unity, lest the iteration repeat after a bounded number of steps. A sufficient condition is that these quantities have complex norm not equal to 1. However, for some constraint functions, we can show that

*It was known [40, 39] that on the grid graph the parameter settings that satisfy $cz = ax + by$ (using notations in Section 9.2) is P-time computable; in our theory this is in $\mathscr{M}$, and the proof is: It follows by Matchgate Identities [14].

these constructions only produce such quantities of norm equal to 1. To overcome this difficulty we introduce a new technique in hardness proofs: Möbius transformations.* We explore properties of Möbius transformations that map unit circle to unit circle on $\mathbb{C}$, and obtain a suitable Möbius transformation that generates an infinite group. This allows our interpolation proof to succeed.

9.2 Preliminaries

9.2.1 Problem Definition

We use Pl-Holant$(\mathcal{F})$ to denote the restriction of Holant$(\mathcal{F})$ to planar signature grids. Similarly, Pl-Holant $(\mathcal{F} \mid \mathcal{G})$ denotes the Holant problem over signature grids with a planar bipartite graph. Also, we use Pl-#CSP$(\mathcal{F})$ to denote the restriction of #CSP$(\mathcal{F})$ to planar signature grids. Still, we have Pl-#CSP$(\mathcal{F}) \equiv_T$ Pl-Holant $(\mathcal{EQ} \mid \mathcal{F})$.

A signature f of arity 4 has the signature matrix $M(f) = M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} \\ f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ f_{1000} & f_{1010} & f_{1001} & f_{1011} \\ f_{1100} & f_{1110} & f_{1101} & f_{1111} \end{smallmatrix}\right]$. (We use f_α to denote the entry $f(\alpha)$ in this chapter.) Notice the order reversal x_4x_3; this is for the convenience of composing these signatures in a planar fashion. If (i, j, k, ℓ) is a permutation of $(1, 2, 3, 4)$, then the 4×4 matrix $M_{x_ix_j,x_\ell x_k}(f)$ lists the 16 values with row index $x_ix_j \in \{0,1\}^2$ and column index $x_\ell x_k \in \{0,1\}^2$ in lexicographic order.

The planar six-vertex model is Pl-Holant$(\neq_2 \mid f)$, where $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$. The *outer matrix* of $M(f)$ is the submatrix $\left[\begin{smallmatrix} M(f)_{1,1} & M(f)_{1,4} \\ M(f)_{4,1} & M(f)_{4,4} \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & a \\ x & 0 \end{smallmatrix}\right]$, and is denoted by $M_{\text{Out}}(f)$. The *inner matrix* of $M(f)$ is $\left[\begin{smallmatrix} M(f)_{2,2} & M(f)_{2,3} \\ M(f)_{3,2} & M(f)_{3,3} \end{smallmatrix}\right] = \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right]$, and is denoted by $M_{\text{In}}(f)$. A binary signature g has the signature matrix $M(g) = M_{x_1,x_2}(g) = \left[\begin{smallmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{smallmatrix}\right]$. Switching the order, $M_{x_2,x_1}(g) = \left[\begin{smallmatrix} g_{00} & g_{10} \\ g_{01} & g_{11} \end{smallmatrix}\right]$. Recall that a signature is symmetric if its value depends only on the Hamming weight of its input. A symmetric signature f of arity k can be expressed as $[f_0, f_1, \ldots, f_k]$, where f_w is the value of f on inputs of Hamming weight w.

*Möbius transformations were previously used in the design of quantum algorithms for approximating the Potts model [1]. Here we use Möbius transformations in a different way, which is for hardness proofs. These Möbius transformations are maps on $\mathbb{C}$; they are unrelated to Möbius inversions for partial orders, e.g., as used in [36].

9.2.2 Planar Gadget Construction

Recall the definition of gadget construction in Section 3.2. We say a gadget construction is planar if the underlying graph G is a planar graph, and the dangling edges, ordered counterclockwise corresponding to the order of the input variables, are in the outer face in a planar embedding. A planar gadget can be used in a planar signature grid as if it is just a single vertex with the particular signature. Using planar gadget construction, we can reduce one planar Holant problem to another. Suppose g is the signature of some planar $\mathcal{F}$-gate. Then Pl-Holant$(\mathcal{F}, g) \leq_T$ Pl-Holant$(\mathcal{F})$.

In this chapter, we focus on planar graphs, and we assume the edges incident to a vertex are ordered counterclockwise. When connecting two signatures, we need to keep the counterclockwise order of the edges incident to each vertex. Given a signature f with signature matrix $M_{x_1x_2,x_4x_3}(f)$, we can rotate it to obtain, for any cyclic permutations (i, j, k, ℓ) of $(1, 2, 3, 4)$, the signature f' with signature matrix $M_{x_1x_2,x_4x_3}(f') = M_{x_ix_j,x_\ell x_k}(f)$. There are four cyclic permutations of $(1, 2, 3, 4)$, so correspondingly, a signature f has four rotated forms, with 4×4 signature matrices $M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} 0&0&0&a\\ 0&b&c&0\\ 0&z&y&0\\ x&0&0&0 \end{smallmatrix}\right]$, $M_{x_2x_3,x_1x_4}(f) = \left[\begin{smallmatrix} 0&0&0&y\\ 0&a&z&0\\ 0&c&x&0\\ b&0&0&0 \end{smallmatrix}\right]$, $M_{x_3x_4,x_2x_1}(f) = \left[\begin{smallmatrix} 0&0&0&x\\ 0&y&c&0\\ 0&z&b&0\\ a&0&0&0 \end{smallmatrix}\right]$, and $M_{x_4x_1,x_3x_2}(f) = \left[\begin{smallmatrix} 0&0&0&b\\ 0&x&z&0\\ 0&c&a&0\\ y&0&0&0 \end{smallmatrix}\right]$. These are denoted as f, $f^{\frac{\pi}{2}}$, f^{π} and $f^{\frac{3\pi}{2}}$, respectively. Thus $M_{x_1x_2,x_4x_3}(f^{\frac{\pi}{2}}) = M_{x_2x_3,x_1x_4}(f)$, etc. Without other specification, $M(f)$ denotes $M_{x_1x_2,x_4x_3}(f)$. Once we get one form, all four rotation forms can be freely used. In the proof, after one construction, we may use this property to get a similar construction and conclude by quoting this rotational symmetry. Note that no matter in which signature matrix, the pair (c, z) (and only (c, z)) is always in the inner matrix. We call (c, z) the inner pair, and (a, x), (b, y) the outer pairs.

We introduce three common planar gadgets we will use in this chapter. The first gadget construction is as follows. Suppose f_1 and f_2 have signature matrices $M_{x_ix_j,x_\ell x_k}(f_1)$ and $M_{x_sx_t,x_vx_u}(f_2)$, where (i, j, k, ℓ) and (s, t, u, v) are permutations of $(1, 2, 3, 4)$. By connecting x_ℓ with x_s, x_k with x_t, both using Disequality ($\neq_2$), we get a signature of arity 4 with the signature matrix $M_{x_ix_j,x_\ell x_k}(f_1)N_2M_{x_sx_t,x_vx_u}(f_2)$ by matrix product with row index x_ix_j and column index x_vx_u (See Figure 11).

A binary signature g has the signature vector $g(x_1, x_2) = (g_{00}, g_{01}, g_{10}, g_{11})^T$, and also $g(x_2, x_1) = (g_{00}, g_{10}, g_{01}, g_{11})^T$. Without other specification, g denotes $g(x_1, x_2)$. Let f be a signature of arity 4 with the signature matrix $M_{x_ix_j,x_\ell x_k}(f)$ and (s, t) be a permutation of $(1, 2)$.

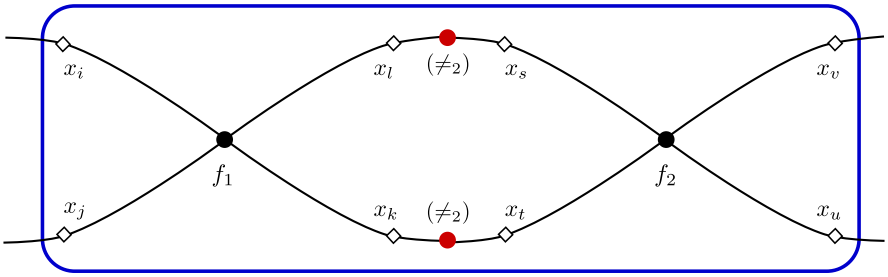


图 11: Connect variables x_ℓ, x_k of f_1 with variables x_s, x_t of f_2 both using $(\neq_2)$.

The second gadget construction is essentially a merging gadget defined as follows. By connecting x_ℓ with x_s and x_k with x_t, both using Disequality $(\neq_2)$, we get a binary signature with the signature matrix $M_{x_ix_j,x_kx_\ell}Ng(x_s,x_t)$ as a matrix product with index x_ix_j (See Figure 12). If $g_{00}=g_{11}$, then $N(g_{00},g_{01},g_{10},g_{11})^T=(g_{11},g_{10},g_{01},g_{00})^T=(g_{00},g_{10},g_{01},g_{11})^T$, and similarly,

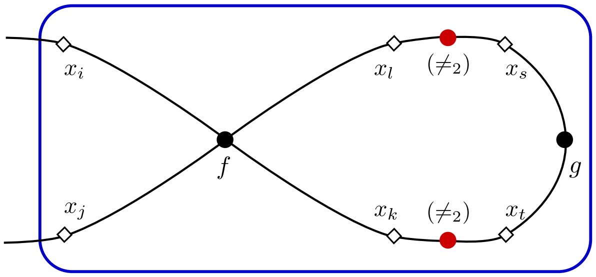


图 12: Connect variables x_ℓ, x_k of f with variables x_s, x_t of g both using $(\neq_2)$.

$N(g_{00},g_{10},g_{01},g_{11})^T=(g_{00},g_{01},g_{10},g_{11})^T$. Therefore, $M_{x_ix_j,x_\ell x_k}Ng(x_s,x_t)=M_{x_ix_j,x_\ell x_k}g(x_t,x_s)$, which means that connecting variables x_ℓ, x_k of f with, respectively, variables x_s, x_t of g using N is equivalent to connecting them directly without N. Hence, in the setting Pl-Holant$(\neq_2|\ f,g)$ we can form $M_{x_ix_j,x_\ell x_k}(f)g(x_t,x_s)$, which is technically $M_{x_ix_j,x_\ell x_k}Ng(x_s,x_t)$, provided that $g_{00}=g_{11}$. Note that for a binary signature g, we can rotate it by 180° without violating planarity, and so both $g(x_s,x_t)$ and $g(x_t,x_s)$ can be freely used once we get one of them.

A signature f of arity 4 also has the 2×8 signature matrix

$$M_{x_1,x_2x_4x_3}(f)=\begin{bmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} & f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ f_{1000} & f_{1010} & f_{1001} & f_{1011} & f_{1100} & f_{1110} & f_{1101} & f_{1111} \end{bmatrix}.$$

Suppose the signature matrix of g is $M_{x_s,x_t}(g)$ and the signature matrix of f is $M_{x_i,x_jx_\ell x_k}(f)$.

Our third gadget construction is essentially an extending gadget defined as follows. By connecting x_t with x_i using Disequality $(\neq_2)$, we get a signature h of arity 4 with the signature matrix $M_{x_s,x_t}(g)M(\neq_2)M_{x_i,x_jx_\ell x_k}(f)$ by matrix product with row index x_s and column index $x_jx_\ell x_k$ (See Figure 13). We may change this form to a signature matrix with row index x_sx_j and column index $x_\ell x_k$. In particular, if $M_{y_1,y_2}(g) = \left[\begin{smallmatrix} 0 & 1 \\ t & 0 \end{smallmatrix}\right]$, then connecting y_2 with x_1 via $(\neq_2)$ gives

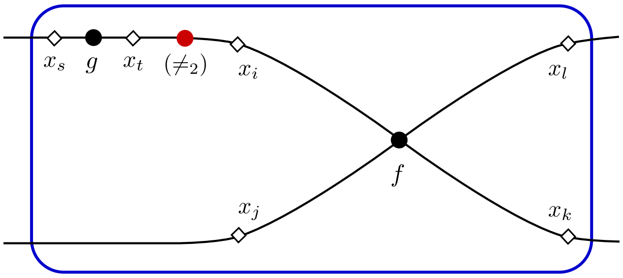


图 13: Connect variable x_t of g with variable x_i of f using $(\neq_2)$.

$$\begin{aligned} M_{y_1,x_2x_4x_3}(h) &= M_{y_1,y_2}(g)M(\neq_2)M_{x_1,x_2x_4x_3}(f) \\ &= \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} & f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ f_{1000} & f_{1010} & f_{1001} & f_{1011} & f_{1100} & f_{1110} & f_{1101} & f_{1111} \end{bmatrix} \\ &= \begin{bmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} & f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ tf_{1000} & tf_{1010} & tf_{1001} & tf_{1011} & tf_{1100} & tf_{1110} & tf_{1101} & tf_{1111} \end{bmatrix}. \end{aligned}$$

If we rename the variable y_1 by x_1, then

$$M_{x_1x_2,x_4x_3}(h) = \begin{bmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} \\ f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ tf_{1000} & tf_{1010} & tf_{1001} & tf_{1011} \\ tf_{1100} & tf_{1110} & tf_{1101} & tf_{1111} \end{bmatrix}.$$

That is, the new signature has the matrix obtained from multiplying t to the last two rows of $M_{x_1x_2,x_4x_3}(f)$ corresponding to $x_1 = 1$. Similarly we can modify the last two columns of

$M_{x_1x_2,x_4x_3}(f)$. Given $g = (0, 1, t, 0)^T$, we call the modification from $M_{x_1x_2,x_4x_3}(f)$ to

$$\begin{bmatrix} f_{0000} & f_{0010} & f_{0001} & f_{0011} \\ f_{0100} & f_{0110} & f_{0101} & f_{0111} \\ tf_{1000} & tf_{1010} & tf_{1001} & tf_{1011} \\ tf_{1100} & tf_{1110} & tf_{1101} & tf_{1111} \end{bmatrix}$$

the operation of t scaling on $x_1 = 1$. Similarly we call the modification from $M_{x_1x_2,x_4x_3}(f)$ to

$$\begin{bmatrix} f_{0000} & f_{0010} & tf_{0001} & tf_{0011} \\ f_{0100} & f_{0110} & tf_{0101} & tf_{0111} \\ f_{1000} & f_{1010} & tf_{1001} & tf_{1011} \\ f_{1100} & f_{1110} & tf_{1101} & tf_{1111} \end{bmatrix}$$

the operation of t scaling on $x_4 = 1$.

9.2.3 More on Polynomial Interpolation

We use polynomial interpolation in a more involved way to prove the following reductions.

Lemma 9.1. *Let f be a 4-ary signature with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $b \neq 0$ is not a root of unity. Let χ_1 be a 4-ary signature with the signature matrix $M(\chi_1) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Then for any signature set $\mathcal{F}$ containing f, we have*

$$\text{Pl-Holant}(\neq_2 |\, \mathcal{F} \cup \{\chi_1\}) \leqslant_T \text{Pl-Holant}(\neq_2 |\, \mathcal{F}).$$

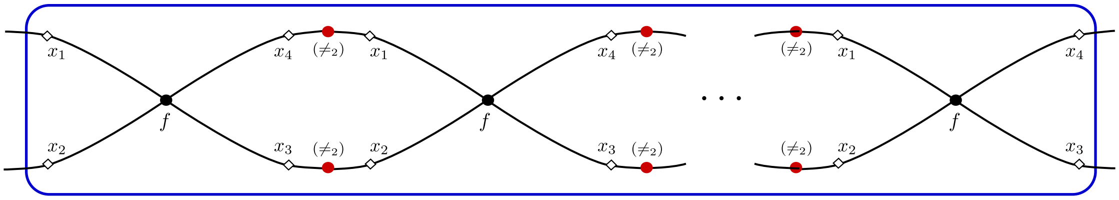


图 14: A chain of $2s + 1$ many copies of f linked by double Disequality N

Proof. We construct a series of gadgets f_{2s+1} by a chain of $2s+1$ many copies of f linked by the double Disequality N (See Figure 14). Clearly f_{2s+1} has the following signature matrix

$$M(f_{2s+1}) = M(f)(N_2 M(f))^{2s} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & b^{2s+1} & 0 & 0 \\ 0 & 0 & b^{2s+1} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

The matrix $M(f_{2s+1})$ has a good form for polynomial interpolation. Suppose χ_1 appears m times in an instance Ω of Pl-Holant($\neq_2$| $\mathcal{F} \cup \{\chi_1\}$). We replace each appearance of χ_1 by a copy of the gadget f_{2s+1} to get an instance Ω_{2s+1} of Pl-Holant($\neq_2$| $\mathcal{F} \cup \{f_{2s+1}\}$), which is also an instance of Pl-Holant($\neq_2$| $\mathcal{F}$). We divide Ω_{2s+1} into two parts. One part consists of m signatures f_{2s+1} and its signature is represented by $(M(f_{2s+1}))^{\otimes m}$. Here we rewrite $(M(f_{2s+1}))^{\otimes m}$ as a column vector. The other part is the rest of Ω_{2s+1} and its signature is represented by A which is a tensor expressed as a row vector. Then, the Holant value of Ω_{2s+1} is the dot product $\langle A, (M(f_{2s+1}))^{\otimes m}\rangle$, which is a summation over $4m$ bits. That is, a sum over all $0, 1$ values for the $4m$ edges connecting the two parts. We can stratify all $0, 1$ assignments of these $4m$ bits having a nonzero evaluation of a term in Pl-Holant$_{\Omega_{2s+1}}$ into the following categories:

- There are i many copies of f_{2s+1} receiving inputs 0011 or 1100;
- There are j many copies of f_{2s+1} receiving inputs 0110 or 1001;

where $i + j = m$.

For any assignment in the category with parameter (i, j), the evaluation of $(M(f_{2s+1}))^{\otimes m}$ is clearly $b^{(2s+1)j}$. Let a_{ij} be the summation of values of the part A over all assignments in the category (i, j). Note that a_{ij} is independent from the value of s since we view the gadget f_{2s+1} as a block. Since $i + j = m$, we can denote a_{ij} by a_j. Then, we rewrite the dot product summation and get

$$\text{Pl-Holant}_{\Omega_{2s+1}} = \langle A, (M(f_{2s+1}))^{\otimes m}\rangle = \sum_{0 \leqslant j \leqslant m} a_j b^{(2s+1)j}.$$

Under this stratification, the Holant value of Pl-Holant$(\Omega, \neq_2 | \mathcal{F} \cup \{\chi_1\})$ can be represented as

$$\text{Pl-Holant}_\Omega = \langle A, (M(\chi_1))^{\otimes m} \rangle = \sum_{0 \leqslant j \leqslant m} a_j.$$

Since $b \neq 0$ is not a root of unity, the linear equation system has a nonsingular Vandermonde matrix

$$\begin{bmatrix} b^0 & b^1 & \cdots & b^m \\ (b^3)^0 & (b^3)^1 & \cdots & (b^3)^m \\ \vdots & \vdots & \vdots & \vdots \\ (b^{2m+1})^0 & (b^{2m+1})^1 & \cdots & (b^{2m+1})^m \end{bmatrix}.$$

By oracle querying the values of Pl-Holant$_{\Omega_{2s+1}}$, we can solve the coefficients a_j in polynomial time and obtain the value of $p(x) = \sum\limits_{0 \leqslant j \leqslant m} a_j x^j$ for any x. Let $x = 1$, we get Pl-Holant$_\Omega$. Therefore, we have Pl-Holant$(\neq_2 | \mathcal{F} \cup \{\chi_1\}) \leqslant_T$ Pl-Holant$(\neq_2 | \mathcal{F})$. □

Corollary 9.2. *Let f be a 4-ary signature with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ -1 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $b \neq 0$ is not a root of unity. Let χ_2 be a 4-ary signature with the signature matrix $M(\chi_2) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Then for any signature set $\mathcal{F}$ containing f, we have*

$$\text{Pl-Holant}(\neq_2 | \mathcal{F} \cup \{\chi_2\}) \leqslant_T \text{Pl-Holant}(\neq_2 | \mathcal{F}).$$

Proof. We still construct a series of gadgets f_{2s+1} by a chain of odd many copies of f linked by the double Disequality N. Clearly f_{2s+1} has the following signature matrix

$$M(f_{2s+1}) = M(f)(N_2 M(f))^{2s} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & b^{2s+1} & 0 & 0 \\ 0 & 0 & b^{2s+1} & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

Suppose χ_2 appears m times in an instance Ω of Pl-Holant$(\neq_2 | f \cup \chi_2)$. We replace each appearance of χ_2 by a copy of the gadget f_{2s+1} to get an instance Ω_{2s+1} of Pl-Holant$(\neq_2 | \mathcal{F} \cup \{f_{2s+1}\})$. In the same way as in the proof of Lemma 9.1, we divide Ω_{2s+1} into two parts. One part is represented by

$(M(f_{2s+1}))^{\otimes m}$ and the other part is represented by A. Then, the Holant value of Ω_{2s+1} is the dot product $\langle A, (M(f_{2s+1}))^{\otimes m}\rangle$. We can stratify all $0,1$ assignments of these $4m$ bits having a nonzero evaluation of a term in Pl-Holant$_{\Omega_{2s+1}}$ into the following categories:

- There are i many copies of f_{2s+1} receiving inputs 0011;
- There are j many copies of f_{2s+1} receiving inputs 0110 or 1001;
- There are k many copies of f_{2s+1} receiving inputs 1100;

where $i + j + k = m$.

For any assignment in those categories with parameters (i, j, k) where $k \equiv 0 \pmod 2$, the evaluation of $(M(f_{2s+1}))^{\otimes m}$ is clearly $(-1)^k b^{(2s+1)j} = b^{(2s+1)j}$. And for any assignment in those categories with parameters (i, j, k) where $k \equiv 1 \pmod 2$, the evaluation of $(M(f_{2s+1}))^{\otimes m}$ is clearly $(-1)^k b^{(2s+1)j} = -b^{(2s+1)j}$. Since $i + j + k = m$, the index i is determined by j and k. Let a_{j0} be the summation of values of the part A over all assignments in those categories (i, j, k) where $k \equiv 0 \pmod 2$, and a_{j1} be the summation of values of the part A over all assignments in those categories (i, j, k) where $k \equiv 1 \pmod 2$. Note that a_{j0} and a_{j1} are independent from the value of s. Let $a_j = a_{j0} - a_{j1}$. Then, we rewrite the dot product summation and get

$$\text{Pl-Holant}_{\Omega_{2s+1}} = \langle A, (M(f_{2s+1}))^{\otimes m}\rangle = \sum_{0\leqslant j\leqslant m} (a_{j0}b^{(2s+1)j} - a_{j1}b^{(2s+1)j}) = \sum_{0\leqslant j\leqslant m} a_j b^{(2s+1)j}.$$

Under this stratification, the Holant value of Pl-Holant $(\Omega; \neq_2 \mid f \cup \chi_2)$ can be represented as

$$\text{Pl-Holant}_{\Omega} = \langle A, (M(\chi_2))^{\otimes m}\rangle = \sum_{0\leqslant j\leqslant m} (a_{j0} - a_{j1}) = \sum_{0\leqslant j\leqslant m} a_j.$$

Since $b \neq 0$ is not a root of unity, the Vandermonde coefficient matrix has full rank. Hence we can solve for all the values a_j in polynomial time and obtain the value $\sum\limits_{0\leqslant j\leqslant m} a_j$, and so we get Pl-Holant$_\Omega$. Therefore, we have Pl-Holant$(\neq_2 \mid \mathcal{F} \cup \{\chi_2\}) \leqslant_T$ Pl-Holant$(\neq_2 \mid \mathcal{F})$. □

Lemma 9.3. *Let $g = (0, 1, t, 0)^T$ be a binary signature, where $t \neq 0$ is not a root of unity. Then for any binary signature g' of the form $(0, 1, t', 0)^T$ and any signature set $\mathcal{F}$ containing g, we have*

$$\text{Pl-Holant}\left(\neq_2 \mid \mathcal{F} \cup \{g'\}\right) \leqslant_T \text{Pl-Holant}\left(\neq_2 \mid \mathcal{F}\right).$$

Inductively, for any finite signature set $\mathcal{B}$ consisting of binary signatures of the form $(0, 1, t', 0)^T$ and any signature set $\mathcal{F}$ containing g, we have

$$\text{Pl-Holant}\,(\neq_2|\ \mathcal{F} \cup \mathcal{B}) \leqslant_T \text{Pl-Holant}\,(\neq_2|\ \mathcal{F})\,.$$

Proof. Note that $M(g) = [\begin{smallmatrix} 0 & 1 \\ t & 0 \end{smallmatrix}]$. Connecting the variable x_2 of a copy of g with the variable x_1 of another copy of g using $(\neq_2)$, we get a signature g_2 with the signature matrix

$$M(g_2) = M_{x_1,x_2}(g) M(\neq_2) M_{x_1,x_2}(g) = \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ t^2 & 0 \end{bmatrix}.$$

That is, $g_2 = (0, 1, t^2, 0)^T$. Recursively, we can construct $g_s = (0, 1, t^s, 0)^T$ for $s \geq 1$. Here, g_1 denotes g. Given an instance Ω' of Pl-Holant $(\neq_2|\ \mathcal{F} \cup \{g'\})$, in the same way as in the proof of Lemma 9.1, we can replace each appearance of g' by g_s and get an instance Ω_s of Pl-Holant $(\neq_2|\ \mathcal{F})$. Similarly, the Holant value of Ω_s can be represented as

$$\text{Pl-Holant}_{\Omega_s} = \sum_{0 \leqslant j \leqslant m} a_j (t^s)^j,$$

while the Holant value of Ω' can be represented as

$$\text{Pl-Holant}_{\Omega'} = \sum_{0 \leqslant j \leqslant m} a_j (t')^j.$$

Since $t \neq 0$ is not a root of unity, all t^s are distinct, and so the Vandermonde coefficient matrix has full rank. Hence, we can solve for all a_j, and then compute $\sum\limits_{0 \leqslant j \leqslant m} a_j (t')^j$. So we get $\text{Pl-Holant}_{\Omega'}$. Therefore, we have Pl-Holant$(\neq_2|\ \mathcal{F} \cup \{g'\}) \leqslant_T$ Pl-Holant$(\neq_2|\ \mathcal{F})$. The second part of this lemma follows directly by the first part. □

Remark 9.4. *Note that the reason why the interpolation can succeed is that we can construct polynomially many binary signatures g_s of the form $(0, 1, t_s, 0)^T$, where all t_s are distinct such that the Vandermonde coefficient matrix has full rank. According to this, we have the following corollary.*

Corollary 9.5. *Given a signature set $\mathcal{F}$, if we can use $\mathcal{F}$ to construct polynomially many distinct* *binary signatures $g_s = (0,1,t_s,0)^T$, then for any finite signature set $\mathcal{B}$ consisting of binary signatures of the form $(0,1,t',0)^T$, we have*

$$\text{Pl-Holant}\,(\neq_2 \mid \mathcal{F} \cup \mathcal{B}) \leqslant_T \text{Pl-Holant}\,(\neq_2 \mid \mathcal{F})\,.$$

In Lemma 9.37, we will show how to construct polynomially many distinct binary signatures $g_s = (0,1,t_s,0)^T$ using Möbius transformations [2]. A Möbius transformation of the extended complex plane $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, the complex plane plus a point at infinity, is a rational function of the form $\mathfrak{z} \mapsto \dfrac{a\mathfrak{z}+b}{c\mathfrak{z}+d}$ of a complex variable $\mathfrak{z}$, where the coefficients a,b,c,d are complex numbers satisfying $\det\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = ad - bc \neq 0$. It is a bijective conformal map. In particular, a Möbius transformation mapping the unit circle $S^1 = \{z \mid |z| = 1\}$ to itself is of the form $\varphi(\mathfrak{z}) = e^{i\theta}\dfrac{(\mathfrak{z}+\alpha)}{1+\bar{\alpha}\mathfrak{z}}$ denoted by $\mathcal{M}(\alpha, e^{i\theta})$, where $|\alpha| \neq 1$, or $\varphi(\mathfrak{z}) = e^{i\theta}/\mathfrak{z}$. When $|\alpha| < 1$, it maps the interior of S^1 to the interior, while when $|\alpha| > 1$, it maps the interior of S^1 to the exterior. A Möbius transformation is completely determined by its values on any 3 distinct points of $\widehat{\mathbb{C}}$.

An interpolation proof based on a lattice structure will be given in Lemma 9.34, where the following lemma is used.

Lemma 9.6. *[25] Suppose $\alpha, \beta \in \mathbb{C} - \{0\}$, and the lattice $L = \{(j,k) \in \mathbb{Z}^2 \mid \alpha^j\beta^k = 1\}$ has the form $L = \{(ns, nt) \mid n \in \mathbb{Z}\}$, where $s,t \in \mathbb{Z}$ and $(s,t) \neq (0,0)$. Let ϕ and ψ be any numbers satisfying $\phi^s\psi^t = 1$. If we are given the values $N_\ell = \sum_{j,k \geq 0,\ j+k \leq m} (\alpha^j\beta^k)^\ell x_{j,k}$ for $\ell = 1, 2, \ldots \binom{m+2}{2}$, then we can compute $\sum_{j,k \geq 0,\ j+k \leq m} \phi^j\psi^k x_{j,k}$ in polynomial time.*

9.2.4 Matchgate Signatures

Matchgates were introduced by Valiant [70, 69] to give polynomial-time algorithms for a collection of counting problems over planar graphs. As the name suggests, problems expressible by matchgates can be reduced to computing a weighted sum of perfect matchings. The latter problem is tractable over planar graphs by Kasteleyn's algorithm [48], a.k.a. the FKT algorithm [66, 49]. These counting problems are naturally expressed in the Holant framework using *matchgate signatures*. We use $\mathscr{M}$ to denote the set of all matchgate signatures; thus Pl-Holant($\mathscr{M}$) is tractable, as well as Pl-Holant($\neq_2 \mid \mathscr{M}$). For signatures of arity at most 4, the matchgate signatures are characterized by the following lemma.

Lemma 9.7 ([69, 14])**.** *If f has arity $\leqslant 3$, then $f \in \mathscr{M}$ iff f satisfies the Parity Condition.*

If f has arity 4 and f satisfies the even Parity Condition, i.e.,

$$M_{x_1x_2,x_4x_3}(f) = \begin{bmatrix} f_{0000} & 0 & 0 & f_{0011} \\ 0 & f_{0110} & f_{0101} & 0 \\ 0 & f_{1010} & f_{1001} & 0 \\ f_{1100} & 0 & 0 & f_{1111} \end{bmatrix},$$

then $f \in \mathscr{M}$ iff

$$\det M_{\text{Out}}(f) = \det M_{\text{In}}(f).$$

By this matchgate identity, we have the following corollary.

Corollary 9.8. *Given a signature f of arity 4, two 2-by-2 matrices $D_\lambda = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \lambda \end{smallmatrix}\right]$ $(\lambda \neq 0)$ and $M(\neq_2) = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, if $f \in \mathscr{M}$, then $D_\lambda f$ and $M(\neq_2)f \in \mathscr{M}$.*

Proof. Since $f \in \mathscr{M}$, by Lemma 9.7 we know f satisfies the Parity Condition. We only consider that f satisfies even parity. The proof for f satisfying odd parity is similar and we omitted it here. Suppose f has the signature matrix $M(f) = \left[\begin{smallmatrix} d & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & w \end{smallmatrix}\right]$. Then, we have $M(D_\lambda f) = \left[\begin{smallmatrix} d & 0 & 0 & \lambda^2 a \\ 0 & \lambda^2 b & \lambda^2 c & 0 \\ 0 & \lambda^2 z & \lambda^2 y & 0 \\ \lambda^2 x & 0 & 0 & \lambda^4 w \end{smallmatrix}\right]$ and $M(M(\neq_2)f) = \left[\begin{smallmatrix} w & 0 & 0 & x \\ 0 & y & z & 0 \\ 0 & c & b & 0 \\ a & 0 & 0 & d \end{smallmatrix}\right]$. Clearly, $D_\lambda f$ and $M(\neq_2)f$ also satisfy even parity. Moreover, we have

$$\det M_{\text{Out}}(D_\lambda f) = \lambda^4 \det M_{\text{Out}}(f), \det M_{\text{In}}(D_\lambda f) = \lambda^4 \det M_{\text{In}}(f),$$

and

$$\det M_{\text{Out}}(M(\neq_2)f) = \det M_{\text{Out}}(f), \det M_{\text{In}}(M(\neq_2)f) = \det M_{\text{In}}(f).$$

Since $\det M_{\text{Out}}(f) = \det M_{\text{In}}(f)$, we have

$$\det M_{\text{Out}}(D_\lambda f) = \det M_{\text{In}}(D_\lambda f), \text{ and } \det M_{\text{Out}}(M(\neq_2)f) = \det M_{\text{In}}(M(\neq_2)f).$$

That is, $D_\lambda f$ and $M(\neq_2)f \in \mathscr{M}$. □

Holographic transformations extend the reach of the FKT algorithm further, as stated below.

By Definition 2.32, a signature set $\mathcal{F}$ is $\mathscr{M}$-transformable if there exists a $T \in \mathrm{GL}_2(\mathbb{C})$ such that $(=_2)(T^{-1})^{\otimes 2} \in \mathscr{M}$ and $T\mathcal{F} \subseteq \mathscr{M}$.

Theorem 9.9. *Let $\mathcal{F}$ be any set of complex-valued signatures in Boolean variables. If $\mathcal{F}$ is $\mathscr{M}$-transformable, then* Pl-Holant$(\neq_2|\ \mathcal{F})$ *is tractable.*

Let $\widehat{\mathscr{M}} = H\mathscr{M}$, where $H = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$. We will show that for the six-vertex model, $\mathscr{M}$-transformable signatures are exactly characterized by $\mathscr{M}$ and $\widehat{\mathscr{M}}$. We first give the following simple lemma.

Lemma 9.10. *For any signature f with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$, and a 2-by-2 matrix $D_\lambda = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \lambda \end{smallmatrix}\right]$, where $\lambda \neq 0$, we have $f \in \widehat{\mathscr{M}}$ iff $(D_\lambda)^{\otimes 4} f \in \widehat{\mathscr{M}}$.*

Proof. Note that $M((D_\lambda)^{\otimes 4} f) = \begin{bmatrix} 0 & 0 & 0 & \lambda^2 a \\ 0 & \lambda^2 b & \lambda^2 c & 0 \\ 0 & \lambda^2 z & \lambda^2 y & 0 \\ \lambda^2 x & 0 & 0 & 0 \end{bmatrix} = \lambda^2 M(f)$. That is, $(D_\lambda)^{\otimes 4} f = \lambda^2 f$. Thus, $f \in \widehat{\mathscr{M}}$ is equivalent to $(D_\lambda)^{\otimes 4} f = \lambda^2 f \in \widehat{\mathscr{M}}$. □

Lemma 9.11. *A signature f with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$ is $\mathscr{M}$-transformable iff $f \in \widehat{\mathscr{M}}$.*

Proof. The reverse direction is obvious, since $(\neq_2)I^{\otimes 2} \in \mathscr{M}$, and $(\neq_2)H^{\otimes 2} \in \mathscr{M}$.

Suppose f is $\mathscr{M}$-transformable. By definition, there is $T \in \mathrm{GL}_2(\mathbb{C})$ such that

$$(0,1,1,0)T^{\otimes 2} \in \mathscr{M} \quad \text{and} \quad (T^{-1})^{\otimes 4} f \in \mathscr{M}.$$

Let $T = \left[\begin{smallmatrix} \lambda & \mu \\ \nu & \xi \end{smallmatrix}\right]$. We have

$$(0,1,1,0)T^{\otimes 2} = (2\lambda\nu, \lambda\xi + \mu\nu, \lambda\xi + \mu\nu, 2\mu\xi) \in \mathscr{M}.$$

By Lemma 9.7, we have $\lambda\nu = \mu\xi = 0$ or $\lambda\xi + \mu\nu = 0$.

If $\lambda\nu = \mu\xi = 0$, since $T \in \mathrm{GL}_2(\mathbb{C})$, we have $\mu = \nu = 0$ while $\lambda, \xi \neq 0$, or $\lambda = \xi = 0$ while $\mu, \nu \neq 0$. That is, $T = \left[\begin{smallmatrix} \lambda & 0 \\ 0 & \xi \end{smallmatrix}\right]$ $(\lambda, \xi \neq 0)$, or $T = \left[\begin{smallmatrix} 0 & \mu \\ \nu & 0 \end{smallmatrix}\right]$ $(\mu, \nu \neq 0)$. By normalization, we may assume $\lambda = 1$ or $\mu = 1$. That is,

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \xi \end{bmatrix} (\xi \neq 0), \text{ or } T = \begin{bmatrix} 0 & 1 \\ \nu & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \nu \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (\nu \neq 0).$$

For any $\alpha \neq 0$, we use D_α to denote the matrix $\left[\begin{smallmatrix}1 & 0\\ 0 & \alpha\end{smallmatrix}\right]$ and we know $D_\alpha^{-1} = D_{1/\alpha}$. Then, $T = D_\xi$ or $T = D_\nu M(\neq_2)$. By Corollary 9.8, we know $f \in \mathscr{M}$ given $T^{-1} f \in \mathscr{M}$.

Otherwise, $\lambda\xi + \mu\nu = 0$. Since $T \in \mathrm{GL}_2(\mathbb{C})$, we know $\det T = \lambda\xi - \mu\nu \neq 0$. Thus, $\lambda\xi\mu\nu \neq 0$. By normalization, we may assume $\lambda = 1$ and hence, $\xi = -\mu\nu$. That is

$$T = \begin{bmatrix}1 & \mu\\ \nu & -\mu\nu\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & \nu\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & \mu\end{bmatrix} = D_\nu H D_\mu.$$

Hence, we have $T^{-1} = \frac{1}{2} D_{1/\mu} H D_{1/\nu}$ and we know $D_{1/\mu} H D_{1/\nu} f \in \mathscr{M}$. We have $D_\mu \mathscr{M} = \mathscr{M}$. Hence $H D_{1/\nu} f \in \mathscr{M}$. Thus, we have

$$D_{1/\nu} f \in \widehat{\mathscr{M}}.$$

By Lemma 9.10, we have $f \in \widehat{\mathscr{M}}$ given $D_{1/\nu}^{\otimes 4} f \in \widehat{\mathscr{M}}$. □

For signatures of special forms, we give the following three characterizations of $\widehat{\mathscr{M}}$. They follow directly from the definition.

Lemma 9.12. *A binary signature g with the signature matrix $M(g) = \left[\begin{smallmatrix}g_{00} & g_{01}\\ g_{10} & g_{11}\end{smallmatrix}\right]$ is in $\widehat{\mathscr{M}}$ iff $g_{00} = \epsilon g_{11}$ and $g_{01} = \epsilon g_{10}$, where $\epsilon = \pm 1$.*

Lemma 9.13. *A signature f with the signature matrix $M(f) = \left[\begin{smallmatrix}0 & 0 & 0 & 0\\ 0 & b & c & 0\\ 0 & z & y & 0\\ 0 & 0 & 0 & 0\end{smallmatrix}\right]$ is in $\widehat{\mathscr{M}}$ iff $b = \epsilon y$ and $c = \epsilon z$, where $\epsilon = \pm 1$.*

Lemma 9.14. *If f has the signature matrix $M(f) = \left[\begin{smallmatrix}0 & 0 & 0 & a\\ 0 & b & 0 & 0\\ 0 & 0 & y & 0\\ x & 0 & 0 & 0\end{smallmatrix}\right]$, where $abxy \neq 0$, then $f \notin \widehat{\mathscr{M}}$.*

9.2.5 Known Dichotomies and Hardness Results

Definition 9.15. *A 4-ary signature is non-singular redundant iff in one of its four 4×4 signature matrices, the middle two rows are identical and the middle two columns are identical, and the determinant*

$$\det \begin{bmatrix} f_{0000} & f_{0010} & f_{0011}\\ f_{0100} & f_{0110} & f_{0111}\\ f_{1100} & f_{1110} & f_{1111}\end{bmatrix} \neq 0.$$

Theorem 9.16. *[28] If f is a non-singular redundant signature, then* Pl-Holant$(\neq_2 | f)$ *is #P-hard.*

Theorem 9.17. *[53] Let G be a connected plane graph and $\mathcal{EO}(H)$ be the set of all Eulerian orientations of the medial graph $H = H(G)$ which is a 4-regular planar graph. Then*

$$\sum_{O \in \mathcal{EO}(H)} 2^{\beta(O)} = 2T(G; 3, 3),$$

where T is the Tutte polynomial, and $\beta(O)$ is the number of saddle vertices in the orientation O, i.e., vertices in which the edges are oriented "in, out, in, out" in cyclic order.

Remark 9.18. *Note that $\sum_{O \in \mathcal{EO}(H)} 2^{\beta(O)}$ can be expressed as Pl-Holant($\neq_2 |\, f$) on H, where f has the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Therefore, Pl-Holant($\neq_2 |\, f$) is #P-hard.*

Theorem 9.19. *[20] Let $\mathcal{F}$ be any set of complex-valued signatures in Boolean variables. Then* Pl-#CSP($\mathcal{F}$) *is #P-hard unless $\mathcal{F} \subseteq \mathscr{A}$, $\mathcal{F} \subseteq \mathscr{P}$, or $\mathcal{F} \subseteq \widehat{\mathscr{M}}$, in which case the problem is computable in polynomial time. If $\mathcal{F} \subseteq \mathscr{A}$ or $\mathcal{F} \subseteq \mathscr{P}$, then* #CSP($\mathcal{F}$) *is computable in polynomial time without planarity; otherwise* #CSP($\mathcal{F}$) *is #P-hard.*

Theorem 9.20. *[25] Let f be a 4-ary signature with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$, then* Holant($\neq_2 |\, f$) *is #P-hard except for the following cases:*

- *$f \in \mathscr{P}$;*
- *$f \in \mathscr{A}$;*
- *there is a zero in each pair $(a, x), (b, y), (c, z)$;*

in which cases Holant($\neq_2 |\, f$) *is computable in polynomial time.*

9.3 Trichotomy Theorem, Proof Outline and Sample Problems

Theorem 9.21. *Let f be a signature with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$, where $a, b, c, x, y, z \in \mathbb{C}$. Then* Pl-Holant($\neq_2 |\, f$) *is polynomial time computable in the following cases, and #P-hard otherwise:*

1. *$f \in \mathscr{P}$ or $\mathscr{A}$;*
2. *There is a zero in each pair (a, x), (b, y), (c, z);*

3. $f \in \mathscr{M}$ *or* $\widehat{\mathscr{M}}$*;*

4. $c = z = 0$ *and*

(i). $(ax)^2 = (by)^2$*, or*

(ii). $x = a\mathfrak{i}^\alpha, b = a\sqrt{\mathfrak{i}}^\beta$*, and* $y = a\sqrt{\mathfrak{i}}^\gamma$*, where* $\alpha, \beta, \gamma \in \mathbb{N}$*, and* $\beta \equiv \gamma \pmod 2$;

If f *satisfies condition 1 or 2, then* $\operatorname{Holant}(\neq_2 \mid f)$ *is computable in polynomial time without the planarity restriction; otherwise (the non-planar)* $\operatorname{Holant}(\neq_2 \mid f)$ *is #P-hard.*

Let N be the number of zeros among a, b, c, x, y, z. The following division of all cases into Cases I, II, III and IV may not appear to be the most obvious, but it is done to simplify the organization of the proof. We define:

Case I: There is exactly one zero in each pair.

Case II: There is a zero pair.

Case III: $\mathsf{N} = 2$ and having no zero pair, or $\mathsf{N} = 1$ and the zero is in an outer pair.

Case IV: $\mathsf{N} = 1$ and the zero is in an inner pair, or $\mathsf{N} = 0$.

Cases I, II, III and IV are clearly disjoint. To see that they cover all cases, note that if $\mathsf{N} \geqslant 3$, then either there is a zero pair (in Case II), or $\mathsf{N} = 3$ and each pair has exactly one zero (in Case I). If $\mathsf{N} = 2$, then either it has a zero pair (in Case II), or it has no zero pair (in Case III). If $\mathsf{N} = 1$, then either the single zero is in an outer pair (in Case III), or the single zero is in an inner pair (Case IV). If $\mathsf{N} = 0$ it is in Case IV.

Also note that if $\mathsf{N} = 2$ and it has no zero pair, then the two zeros are in different pairs, which implies that there is a zero in an outer pair. So in Case III, there is a zero in an outer pair regardless $\mathsf{N} = 1$ or $\mathsf{N} = 2$. In Case III an outer pair has exactly one zero, and the other two pairs together have at most one zero.

In Case II, depending on whether the zero pair is inner or outer we have two different connections to #CSP. A previously established connection to #CSP (see [25]) can be adapted in the planar setting to handle the case with a zero outer pair. This connection is a local transformation, and we observe that it preserves planarity. A significantly more involved non-local connection to #CSP is discovered in this paper when the inner pair is zero (and no outer pair is zero). We show that by the support structure of the signature we can define a set of circuits, which forms a partition of the edge set. There are exactly two valid configurations along each such circuit, corresponding to its two cyclic orientations. These circuits may intersect in complicated ways, including self-intersections. But we can define a #CSP problem, where the variables are these circuits, and their edge functions exactly account for the intersections. We show that Pl-Holant($\neq_2 | f$) is equivalent to these #CSP problems, which are *non-planar* in general. However, crucially, because Pl-Holant($\neq_2 | f$) is planar, every two such circuits must intersect an even number of times. Due to the planarity of Pl-Holant($\neq_2 | f$) we can exactly carve out a new class of tractable problems via this non-local #CSP connection, by the kind of constraint functions they produce in the #CSP problems.

For the proof of #P-hardness in this paper, one particularly difficult case is in Lemma 9.37. This is where we introduce Möbius transformations to prove dichotomy theorems for counting problems. In this case, all constructible binary signatures correspond to points on the unit circle S^1, and any iteration of the construction amounts to mapping this point by a Möbius transformation which preserves S^1.

The following is an outline on how Case I to Case IV are handled.

I. There is exactly one zero in each pair. In this case, Holant($\neq_2 | f$) is tractable, proved in [25].

II. There is a zero pair:

1. An outer pair (a, x) or (b, y) is a zero pair. We prove that Pl-Holant($\neq_2 | f$) is tractable if $f \in \mathscr{P}, \mathscr{A}, \mathscr{M}$ or $\widehat{\mathscr{M}}$, and is #P-hard otherwise.

   In this Case II.1, we can rotate the signature f such that the matrix $M_{\mathrm{Out}}(f)$ is the zero matrix. Let $M(\widetilde{f_{\mathrm{In}}}) = M_{\mathrm{In}}(f) \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. We reduce Pl-#CSP($\widetilde{f_{\mathrm{In}}}$) to Pl-Holant ($\neq_2 | f$) via a local replacement (Lemma 9.23). We apply the dichotomy of Pl-#CSP to get #P-hardness (Theorem 9.24). Tractability of Pl-Holant ($\neq_2 | f$) follows from known tractable signatures.

2. The inner pair (c, z) is a zero pair and no outer pair is a zero pair. We prove that Pl-Holant($\neq_2 | f$) is #P-hard unless f satisfies condition 4, in which case it is tractable. This is the non-local reduction described above. The tractable condition 4 is previously unknown. (Curiously, in Case II.2, condition 4 subsumes $f \in \mathscr{M}$.)

III. 1. There are exactly two zeros and they are in different pairs;

2. There is exactly one zero and it is in an outer pair.

We prove that Pl-Holant($\neq_2|\ f$) is #P-hard unless $f \in \mathscr{M}$, in which case it is tractable.

In Case III, there exists an outer pair which contains a single zero. By connecting two copies of the signature f, we can construct a 4-ary signature f_1 such that one outer pair is a zero pair. When $f \notin \mathscr{M}$, we can realize a signature $M(g) = \left[\begin{smallmatrix} 0&0&0&0\\ 0&0&1&0\\ 0&1&0&0\\ 0&0&0&0 \end{smallmatrix}\right]$ by interpolation using f_1 (Lemma 9.32). This g can help us "extract" the inner matrix of $M(f)$. By connecting f and g, we can construct a signature that belongs to Case II. We then prove #P-hardness using the result of Case II (Theorem 9.33).

IV. 1. There is exactly one zero and it is in the inner pair;

2. All values in $\{a, x, b, y, c, z\}$ are nonzero.

We prove that Pl-Holant($\neq_2|\ f$) is #P-hard unless $f \in \mathscr{M}$, in which case it is tractable.

Assume $f \notin \mathscr{M}$. The main idea is to use Möbius transformations. However, there are some settings where we cannot do so, either because we don't have the initial signature to start the process, or the matrix that would define the Möbius transformation is singular. So we first treat the following two special cases.

- If $a = \epsilon x$, $b = \epsilon y$ and $c = \epsilon z$, where $\epsilon = \pm 1$, by interpolation based on a lattice structure, either we can realize a non-singular redundant signature or reduce from the evaluation of the Tutte polynomial at $(3, 3)$, both of which are #P-hard (Lemma 9.34).
- If $\det \left[\begin{smallmatrix} b & c\\ z & y \end{smallmatrix}\right] = 0$ or $\det \left[\begin{smallmatrix} a & z\\ c & x \end{smallmatrix}\right] = 0$, then either we can realize a non-singular redundant signature or a signature that is #P-hard by Lemma 9.34 (Lemma 9.35).

If f does not belong to the above two cases, we want to realize binary signatures of the form $(0, 1, t, 0)^T$, for arbitrary values of t. If this can be done, by carefully choosing the values of t, we can construct a signature that belongs to Case III and it is #P-hard when $f \notin \mathscr{M}$ (Lemma 9.36). We realize binary signatures by connecting f with ($\neq_2$). This corresponds naturally to a Möbius transformation. By discussing the following different forms of binary signatures we get, we can either realize arbitrary $(0, 1, t, 0)^T$ or a signature belonging to Case II.2 that does not satisfy condition 4, therefore is #P-hard (Theorem 9.42).

- If we can get a signature of the form $g = (0, 1, t, 0)^T$ where $t \neq 0$ is not a root of unity, then by connecting a chain of g, we can get polynomially many distinct binary signatures $g_i = (0, 1, t^i, 0)^T$. Then, by interpolation, we can realize arbitrary binary signatures of the form $(0, 1, t', 0)^T$.
- Suppose we can get a signature of the form $(0, 1, t, 0)^T$, where $t \neq 0$ is an n-th primitive root of unity ($n \geqslant 5$). Now, we only have n many distinct signatures $g_i = (0, 1, t^i, 0)^T$. But we can relate f to two Möbius transformations due to $\det \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right] \neq 0$ and $\det \left[\begin{smallmatrix} a & z \\ c & x \end{smallmatrix}\right] \neq 0$. For each Möbius transformation φ, we can realize the signatures $g = (0, 1, \varphi(t^i), 0)^T$. If $|\varphi(t^i)| \neq 0, 1$ or ∞ for some i, then this is treated above, as this $\varphi(t^i)$ is nonzero and not a root of unity. Otherwise, since φ is a bijection on the extended complex plane $\widehat{\mathbb{C}}$, it can map at most two points of S^1 to 0 or ∞. Hence, $|\varphi(t^i)| = 1$ for at least three distinct t^i. But a Möbius transformation is determined by any three distinct points. This implies that φ maps S^1 to itself. Such mappings φ have a known special form $e^{\mathrm{i}\theta} \dfrac{\mathfrak{z} + \alpha}{1 + \bar{\alpha}\mathfrak{z}}$ (or $e^{\mathrm{i}\theta}/\mathfrak{z}$, but the latter form actually cannot occur in our context.) By exploiting its property we can construct a signature f' such that its corresponding Möbius transformation φ' defines an infinite group. This implies that $\varphi'^k(t)$ are all distinct. Then, we can get polynomially many distinct binary signatures $(0, 1, \varphi'^k(t), 0)$, and realize arbitrary binary signatures of the form $(0, 1, t', 0)^T$ (Lemma 9.37).
- Suppose we can get a signature of the form $(0, 1, t, 0)^T$ where $t \neq 0$ is an n-th primitive root of unity ($n = 3, 4$). Then we can either relate it to two Möbius transformations mapping the unit circle to itself, or realize a double pinning $(0, 1, 0, 0)^T = (1, 0)^T \otimes (0, 1)^T$ (Corollary 9.39).
- Suppose we can get a signature of the form $(0, 1, 0, 0)^T$. By connecting f with it, we can get new signatures of the form $(0, 1, t, 0)^T$. Similarly, by analyzing the value of t, we can either realize arbitrary binary signatures of the form $(0, 1, s, 0)^T$, or realize a signature that belongs to Case II.2, which is #P-hard (Lemma 9.40).
- Suppose we can only get signatures of the form $(0, 1, \pm 1, 0)$. That implies $a = \epsilon x$, $b = \epsilon y$ and $c = \epsilon z$, where $\epsilon = \pm 1$. This has been treated before.

As Case I has already been proved tractable in [25], we only deal with Cases II, III and IV, and they are each dealt with in the next three sections. Before we start the proof, we first illustrate the scope of Theorem 9.21 by several concrete problems.

Problem 1 : #EO on 4-Regular Planar Graphs.

Input : A 4-regular planar graph G.

Output : The number of Eulerian orientations of G, i.e., the number of orientations of G such that at every vertex the in-degree and out-degree are equal.

This problem can be expressed as Pl-Holant($\neq_2 |f$), where f has the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Huang and Lu proved this problem is #P-complete [45]. Theorem 9.21 confirms this.

Problem 2 : Pl-$T(G; 3, 3)$.

Input : A planar graph G.

Output : The value of the Tutte polynomial $T(G; x, y)$ at $(3, 3)$.

Let G_m be the medial graph of G, then G_m is a 4-regular planar graph. By Theorem 9.17, we have

$$\sum_{O \in \mathcal{EO}(G_m)} 2^{\beta(O)} = 2T(G; 3, 3),$$

where $\beta(O)$ is the number of saddle vertices in the orientation O. Note that $\sum_{O \in \mathcal{EO}(G_m)} 2^{\beta(O)}$ can be expressed as Pl-Holant($\neq_2 |f$), where f has the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Theorem 9.21 confirms that this problem is #P-hard.

Compared to the six-vertex model over general graphs, the planar version has new tractable problems due to the FKT algorithm under holographic transformations. This tractable class can give highly nontrivial problems. For example, we consider the following problem.

Problem 3 : SmallPell

Input : A planar 4-regular graph G and a 4-ary signature f, where f has the signature matrix

$$M(f) = \begin{bmatrix} 3178308057237079\!70 & -283823304736008960\mathfrak{i} & 283823304736008960\mathfrak{i} & 317830805723707968 \\ -283823304736008960\mathfrak{i} & -253454564065438270 & 253454564065438272 & -283823304736008960\mathfrak{i} \\ 283823304736008960\mathfrak{i} & 253454564065438272 & -253454564065438270 & 283823304736008960\mathfrak{i} \\ 317830805723707968 & -283823304736008960\mathfrak{i} & 283823304736008960\mathfrak{i} & 317830805723707970 \end{bmatrix}.$$

Output : The evaluation of Pl-Holant(f) on G.

By the holographic transformation $Z = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix} 1 & 1 \\ \mathfrak{i} & -\mathfrak{i} \end{smallmatrix}\right]$, we have

$$\text{Pl-Holant}(f) \equiv_T \text{Pl-Holant}(\neq_2 | \widehat{f}),$$

where

$$M(\widehat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 569465989630582080 & 32188120829134849 & 0 \\ 0 & 32188120829134849 & 1819380158564160 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right].$$

Since $(32188120829134849, 1819380158564160)$ is a solution of Pell's equation $x^2 - 313y^2 = 1$, we have $\widehat{f} \in \mathscr{M}$ by Matchgate Identities [69]. By Theorem 9.21, Pl-Holant(f) can be computed in polynomial time.

In addition to matchgates and matchgates-transformable signatures, Theorem 9.21 gives a new class of tractable problems on planar graphs. They are provably not contained in any previously known tractable classes. For example, we consider the following problem.

Problem 4 : Pl-Holant$(\neq_2 |f)$, where f has the signature matrix $M(f) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \sqrt{\mathfrak{i}} & 0 & 0 \\ 0 & 0 & \sqrt{\mathfrak{i}} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

Input : An instance of Pl-Holant$(\neq_2 |f)$.

Output : The evaluation of this instance.

By Theorem 9.21 (condition 4 (ii)), Pl-Holant$(\neq_2 |f)$ can be computed in polynomial time. Note that Holant$(\neq_2 |f)$ is #P-hard without the planar restriction. It can be shown that f is neither in $\mathscr{M}$ nor $\mathscr{M}$-transformable. By Lemma 9.7 we know $f \notin \mathscr{M}$, and by Lemma 9.14 we know $f \notin \widehat{\mathscr{M}}$. By Lemma 9.11, this implies f is neither in $\mathscr{M}$ nor $\mathscr{M}$-transformable.

Therefore, the tractability is not derivable from the Kasteleyn's algorithm or a holographic transformation to it. Hence, condition 4 of Theorem 9.21 defines a new component of planar tractability complementing the Kasteleyn's algorithm. *Furthermore*, it is an essential component because with it the picture is complete.

9.4 Case II: One Zero Pair

If an outer pair is a zero pair, by rotational symmetry, we may assume (a, x) is a zero pair.

Definition 9.22. *Given a 4-ary signature f with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{9.1}$$

we denote by $\widetilde{f}_{\text{In}}$ the binary signature with $M(\widetilde{f}_{\text{In}}) = M_{\text{In}}(f) \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c & b \\ y & z \end{smallmatrix}\right]$. Given a set $\mathcal{F}$ consisting of signatures of the form (9.1), we define $\widetilde{\mathcal{F}}_{\text{In}} = \{\widetilde{f}_{\text{In}} \mid f \in \mathcal{F}\}$.

Lemma 9.23. *For any set $\mathcal{F}$ of signatures of the form (9.1),*

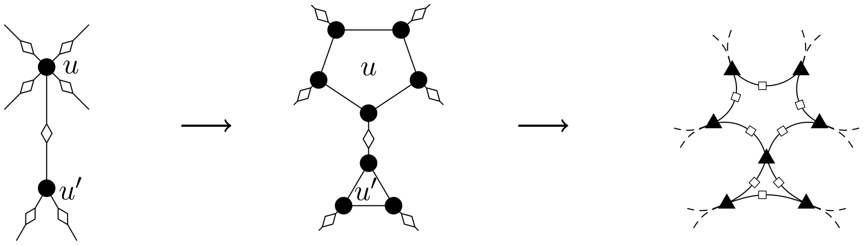
$$\text{Pl-\#CSP}(\widetilde{\mathcal{F}}_{\text{In}}) \leqslant_T \text{Pl-Holant}\left(\neq_2 \mid \mathcal{F}\right).$$

Proof. We adapt a proof from [25], making sure that the reduction preserves planarity. This need to preserve planarity necessitates the twist introduced in the definition of $\widetilde{f}_{\text{In}}$ and $\widetilde{\mathcal{F}}_{\text{In}}$. We prove this reduction in two steps. In each step, we begin with a signature grid and end with a new signature grid such that the Holant values of both signature grids are the same.

For step one, let $G = (U, V, E)$ be a planar bipartite graph representing an instance of

$$\text{Pl-\#CSP}(\widetilde{\mathcal{F}}_{\text{In}}) = \text{Pl-Holant}\left(\mathcal{EQ} \mid \widetilde{\mathcal{F}}_{\text{In}}\right),$$

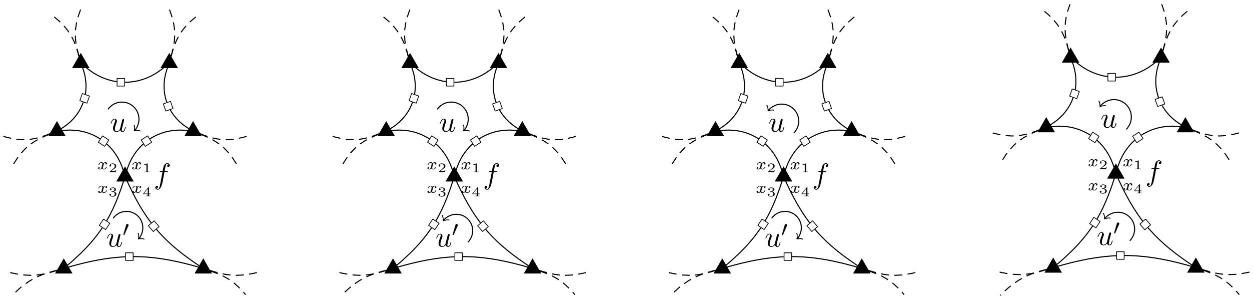
where each $u \in U$ is a variable, and each $v \in V$ has degree two and is labeled by some $\widetilde{f}_{\text{In}} \in \widetilde{\mathcal{F}}_{\text{In}}$. We define a cyclic order of the edges incident to each vertex $u \in U$, and split u into $k = \deg(u)$ vertices. Then we connect the k edges originally incident to u to these k new vertices so that each vertex is incident to exactly one edge. We also connect these k new vertices in a cycle according to the cyclic order (see Figure 15b). Thus, in effect we have replaced u by a cycle of length $k = \deg(u)$. (If $k = 1$ then there is a self-loop. If $k = 2$ then the cycle consists of two parallel edges.) Each of k vertices has degree 3, and we label them by $(=_3)$. This defines a signature grid for a planar holant problem, since the construction preserves planarity. Also clearly this does not change the value of the partition function. The resulting graph has the following properties: (1) every vertex has either degree 2 or degree 3; (2) each degree 2 vertex is connected to degree 3 vertices; (3) each



(a) (b) (c)

图 15: The reduction from #Pl-CSP($\widetilde{f}_{\text{In}}$) to Pl-Holant($\neq_2$| f). The circle vertices are labeled by ($=_d$), where d is the degree of the corresponding vertex, the diamond vertices are labeled by $\widetilde{f}_{\text{In}}$, the triangle vertices are labeled by f, and the square vertices are labeled by ($\neq_2$).

degree 3 vertex is connected to exactly one degree 2 vertex.



(a) $\widetilde{f}_{\text{In}00} \leftrightarrow f_{0101}=c$

(b) $\widetilde{f}_{\text{In}01} \leftrightarrow f_{0110}=b$

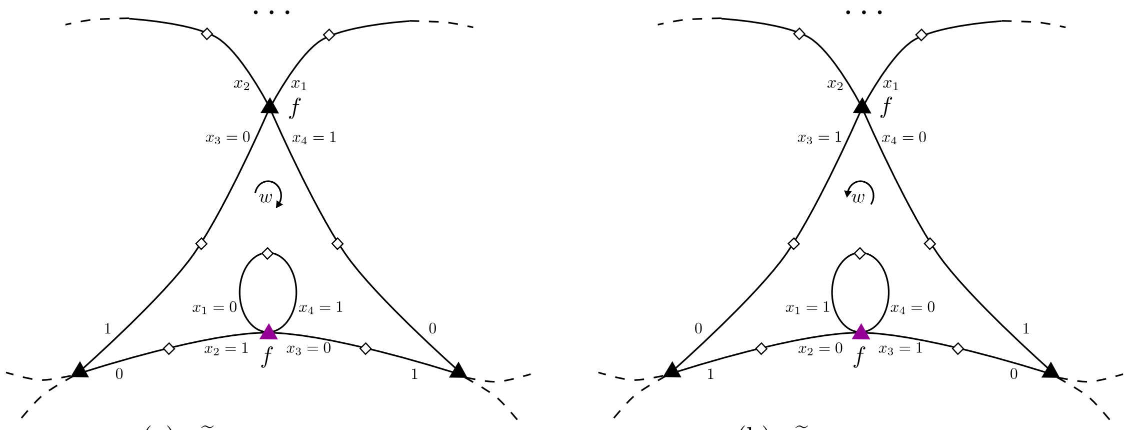
(c) $\widetilde{f}_{\text{In}10} \leftrightarrow f_{1001}=y$

(d) $\widetilde{f}_{\text{In}11} \leftrightarrow f_{1010}=z$

图 16: Assign input variables of f with $M(f) = \begin{bmatrix} 0&0&0&0 \\ 0&b&c&0 \\ 0&z&y&0 \\ 0&0&0&0 \end{bmatrix}$. Suppose the binary signature g is applied to (the ordered pair) (u, u'). The variables u and u' have been replaced by cycles of length deg(u) and deg(u') respectively. For the cycle C_u representing a variable u, we associate the value $u = 0$ with a clockwise orientation, and $u = 1$ with a counterclockwise orientation. Then by the support of f, which is contained in $(x_1 \neq x_2) \wedge (x_3 \neq x_4)$, (x_1, x_2) can only take assignment $(0, 1)$ or $(1, 0)$, and similarly (x_3, x_4) can only take assignment $(0, 1)$ or $(1, 0)$. We associate $(x_1, x_2) = (0, 1)$ to $u = 0$ (clockwise orientation), and $(x_1, x_2) = (1, 0)$ to $u = 1$ (counterclockwise orientation). Consistently, $(x_3, x_4) = (0, 1)$ when $u' = 0$, and $(x_3, x_4) = (1, 0)$ when $u' = 1$.

Now step two. For every $v \in V$, v has degree 2 and is labeled by some $\widetilde{f}_{\text{In}} \in \widetilde{\mathcal{F}}_{\text{In}}$. We contract the two edges incident to v to produce a new vertex v'. The resulting graph $G' = (V', E')$ is 4-regular and planar. We put a node on every edge of G' (these are all edges of the cycles created in step one) and label it by ($\neq_2$) (see Figure 15c). Next, we assign a copy of the corresponding

f to every $v' \in V'$. The input variables x_1, x_2, x_3, x_4 are carefully assigned at each copy of f (as illustrated in Figure 16) such that there are exactly two configurations to each original cycle, which correspond to cyclic orientations, due to the $(\neq_2)$ on it and the support set of f. These cyclic orientations correspond to the $\{0,1\}$ assignments at the original variable $u \in U$. Under this one-to-one correspondence, the value of $\widetilde{f}_{\text{In}}$ is perfectly mirrored by the value of f. Therefore, we have Pl-#CSP$(\widetilde{\mathcal{F}}_{\text{In}}) \leqslant_T$ Pl-Holant$\,(\neq_2 \mid \mathcal{F})$.



(a) $\widetilde{f}_{\text{In}00} \leftrightarrow f_{0101} = c$

(b) $\widetilde{f}_{\text{In}11} \leftrightarrow f_{1010} = z$

图 17: A self-loop on the cycle representing variable w is created for each constraint $\widetilde{f}_{\text{In}}(w, w)$. This creates a degree 4 vertex labeled by f, with four input variables (x_1, x_2, x_3, x_4) as described. Note that the self-loop is created locally on the cycle such that it does not affect anything having to do with other cycles. Base on the support of f, the values $x_1 \neq x_2$ and $x_3 \neq x_4$. By the $(\neq)$ on the loop, we also have $x_1 \neq x_4$. Hence $(x_1, x_2) = (x_3, x_4) = (0, 1)$ or $(1, 0)$. It is clear that the former corrresponds to $w = 0$ (clockwise orientation), and the latter corrresponds to $w = 1$ (counterclockwise orientation). This is consistent with the association in Figure 16.

There is also the possibility that the binary constraint $\widetilde{f}_{\text{In}}$ is applied to a single variable, say w, resulting in a unary constraint that takes value $\widetilde{f}_{\text{In}}(0, 0) = c$ if $w = 0$ and $\widetilde{f}_{\text{In}}(1, 1) = z$ if $w = 1$. To reflect that, we simply introduce a self-loop on the cycle representing the variable w for every such occurrence, as illustrated in Figure 17. It is clear that the values c and z are perfectly mirrored by the values that the local copy f takes under the two orientations for the cycle corresponding to $w = 0$ and 1. □

Theorem 9.24. *Let f be a 4-ary signature of the form* (9.1)*. Then* Pl-Holant$(\neq_2 \mid f)$ *is #P-hard unless $f \in \mathscr{P}$, $f \in \mathscr{A}$, or $f \in \widehat{\mathscr{M}}$, in which cases the problem is tractable.*

Proof. Tractability follows from Theorems 2.30 and 9.9. For any f of the form (9.1), note that the support of f is contained in $(x_1 \neq x_2) \wedge (x_3 \neq x_4)$. We have

$$f(x_1,x_2,x_3,x_4) = \widetilde{f}_{\text{In}}(x_1,x_3) \cdot \chi_{x_1 \neq x_2} \cdot \chi_{x_3 \neq x_4},$$

where χ is the 0-1 indicator function. Thus, $\widetilde{f}_{\text{In}} \in \mathscr{P}$ or $\mathscr{A}$ is equivalent to $f \in \mathscr{P}$ or $\mathscr{A}$. In addition, by Lemmas 9.12 and 9.13, $\widetilde{f}_{\text{In}} \in \widehat{\mathscr{M}}$ is equivalent to $f \in \widehat{\mathscr{M}}$. Therefore, if $f \notin \mathscr{P}, \mathscr{A}$ or $\widehat{\mathscr{M}}$, then $\widetilde{f}_{\text{In}} \notin \mathscr{P}, \mathscr{A}$ or $\widehat{\mathscr{M}}$. By Theorem 9.19, Pl-#CSP($\widetilde{f}_{\text{In}}$) is #P-hard, and then by Lemma 9.23, Pl-Holant $(\neq_2 | \, f)$ is #P-hard. □

Remark 9.25. *One may observe that if $f \in \mathscr{M}$, then* Pl-Holant $(\neq_2 | \, f)$ *is also tractable as f and $(=_2)$ are both realized by matchgates. However, Theorem 9.24 already accounted for this case because for signature f of the form (9.1), $f \in \mathscr{M}$ implies $f \in \mathscr{P}$.*

Now, we consider the case that the inner pair is a zero pair and no outer pair is a zero pair. Note that a signature in the form (9.2) has support contained in $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$.

Definition 9.26. *Given a 4-ary signature f with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix}, \tag{9.2}$$

where $(a,x) \neq (0,0)$ and $(b,y) \neq (0,0)$, let $\mathcal{G}_f$ denote the set of all binary signatures g_f of the form

$$M(g_f) = \begin{bmatrix} a^{k_1+\ell_1} y^{k_2+\ell_2} x^{k_3+\ell_3} b^{k_4+\ell_4} & a^{k_2+\ell_4} y^{k_3+\ell_1} x^{k_4+\ell_2} b^{k_1+\ell_3} \\ a^{k_4+\ell_2} y^{k_1+\ell_3} x^{k_2+\ell_4} b^{k_3+\ell_1} & a^{k_3+\ell_3} y^{k_4+\ell_4} x^{k_1+\ell_1} b^{k_2+\ell_2} \end{bmatrix},$$

satisfying $k = \ell$, where $k = \sum_{i=1}^{4} k_i, \ell = \sum_{i=1}^{4} \ell_i$ and $k_1,k_2,k_3,k_4,\ell_1,\ell_2,\ell_3,\ell_4 \in \mathbb{N}$. Let $\mathcal{H}_f$ denote the set of all unary signatures h_f of the form

$$M(h_f) = \begin{bmatrix} a^{m_1} y^{m_2} x^{m_3} b^{m_4} & a^{m_3} y^{m_4} x^{m_1} b^{m_2} \end{bmatrix},$$

where $m_1, m_2, m_3, m_4 \in \mathbb{N}$.

Let $k = k_1 = \ell_1 = \ell = 1$, we get a specific signature $g_{1_f} \in \mathcal{G}_f$, with $M(g_{1_f}) = \left[\begin{smallmatrix} a^2 & by \\ by & x^2 \end{smallmatrix}\right]$. Let $k = k_1 = \ell_3 = \ell = 1$, we get another specific signature $g_{2_f} \in \mathcal{G}_f$, with $M(g_{2_f}) = \left[\begin{smallmatrix} ax & b^2 \\ y^2 & ax \end{smallmatrix}\right]$.

Remark 9.27. *For any $i, j \in \{1, 2, 3, 4\}$, let $k = k_i = \ell_j = \ell = 1$, we can get 16 signatures in $\mathcal{G}_f$ that have similar signature matrices to $M(g_{1_f})$ and $M(g_{2_f})$. For example, Choosing $k = k_3 = \ell_1 = \ell = 1$, we get $g'_{2_f}(x_1, x_2)$ with the signature matrix $M(g'_{2_f}) = \left[\begin{smallmatrix} ax & y^2 \\ b^2 & ax \end{smallmatrix}\right]$. Indeed $g'_{2_f}(x_1, x_2) = g_{2_f}(x_2, x_1)$. In fact, $\mathcal{G}_f$ is the closure by the Hadamard product (entry-wise product) of these 16 basic signature matrices.*

Lemma 9.28. *Let f be a signature of the form (9.2). Then,*

$$\text{Pl-Holant}(\neq_2 |\ f) \leqslant_T \#\text{CSP}(\mathcal{G}_f \cup \mathcal{H}_f), \tag{9.3}$$

If $a^2 = x^2 \neq 0$, $b^2 = y^2 \neq 0$ and $\left(\frac{b}{a}\right)^8 \neq 1$, then

$$\#\text{CSP}(g_{1_f}, g_{2_f}) \leqslant_T \text{Pl-Holant}(\neq_2 |\ f). \tag{9.4}$$

Proof. We divide the proof into two parts: We show the reduction (9.3) in Part I, and the reduction (9.4) in Part II.

Part I: Suppose $\Omega = (G, \pi)$ is a given instance of Pl-Holant$(\neq_2 |\ f)$, where $G = (U, V, E)$ is a plane bipartite graph. Every vertex $v \in V$ has degree 4, and we list its incident four edges in counterclockwise order. Two edges both incident to a vertex $v \in V$ are called adjacent if they are adjacent in this cyclic order, and non-adjacent otherwise. Two edges in G are called 2-*ary edge twins* if they are both incident to a vertex $u \in U$ (of degree 2), and 4-*ary edge twins* if they are non-adjacent but both incident to a vertex $v \in V$ (of degree 4). Both 2-ary edge twins and 4-ary edge twins are called *edge twins*.

Each edge has a unique 2-ary edge twin at its endpoint in U of degree 2 and a unique 4-ary edge twin at its endpoint in V of degree 4. The reflexive and transitive closure of the symmetric binary relation *edge twin* forms a partition of E as an edge disjoint union of *circuits*: $C_1, C_2, \ldots, C_k$. Note that C_i may include repeated vertices called self-intersection vertices, but no repeated edges. We arbitrarily pick an edge e_i of C_i to be the *leader edge* of C_i. Given the leader edge $e_i = (u, v)$

of C_i, with $u \in U$ and $v \in V$, the direction from u to v defines an orientation of the circuit C_i. * For any edge twins $\{e, e'\}$, this orientation defines one edge, say e', as the successor of the other if e' comes right after e in the orientation. When we list the assignments of edges in a circuit, we list successive values of successors, starting with the leader edge.

For any nonzero term in the sum

$$\text{Pl-Holant}_{\Omega} = \sum_{\sigma : E \to \{0,1\}} \prod_{w \in U \cup V} f_w(\sigma \mid_{E_{(w)}}),$$

the assignment of all edges $\sigma : E \to \{0, 1\}$ can be uniquely extended from its restriction on leader edges $\sigma' : \{e_1, e_2, \cdots e_k\} \to \{0, 1\}$. This is because the support of f is contained in $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$. Thus, at each vertex $v \in V$, $f_v(\sigma \mid_{E_{(v)}}) \neq 0$ only if each pair of edge twins in $E_{(v)}$ is assigned value $(0, 1)$ or $(1, 0)$. The same is true for any vertex $u \in U$ of degree 2, which is labeled $(\neq_2)$. Thus, if the leader edge e_i in C_i takes value 0 or 1 respectively, then all edges on C_i must take values $(0, 1, 0, 1, \cdots, 0, 1)$ or $(1, 0, 1, 0, \cdots, 1, 0)$ respectively on successive successor edges, starting with e_i. In particular, all pairs of 4-ary edge twins in C_i take assignment $(0, 1)$ when $e_i = 0$ and $(1, 0)$ when $e_i = 1$ (listing the value of the successor second). Then, we have

$$\text{Pl-Holant}_{\Omega} = \sum_{\sigma' : \{e_1, \cdots, e_k\} \to \{0,1\}} \prod_{v \in V} f_v(\widehat{\sigma'} \mid_{E_{(v)}}),$$

where $\widehat{\sigma'}$ denotes the unique extension of σ'.

For all $1 \leq i < j \leq k$, let $V_{i,j} = C_i \cap C_j$ denote the set of all intersection vertices between C_i and C_j. Denote by $\sigma'_{(e_i,e_j)}$ an assignment $\{e_i, e_j\} \to \{0, 1\}$. Define a binary function $g_{i,j}$ on e_i and e_j as follows: For any $b, b' \in \{0, 1\}$, let

$$g_{i,j}(b, b') = \prod_{v \in V_{i,j}} f_v(\widehat{\sigma'_{(e_i,e_j)}} \mid_{E_{(v)}}),$$

where $\widehat{\sigma'_{(e_i,e_j)}}$ is the unique extension of $\sigma'_{(e_i,e_j)}$ on the union of edge sets of C_i and C_j as described above, and $\sigma'_{(e_i,e_j)}$ is the unique assignment on $\{e_i, e_j\}$ such that $e_i \mapsto b$ and $e_j \mapsto b'$. Since all edges incident to vertices in $V_{i,j}$ are either in C_i or C_j, the assignment values of these edges are

*This default orientation should not be confused with the orientation in the proof of Lemma 9.23.

determined by $\sigma'_{(e_i,e_j)}$. Hence, $g_{i,j}$ is well-defined.

We show that $g_{i,j} \in \mathcal{G}_f$ by induction on the number n of self-intersection vertices in C_i. Note that in this proof, i and j (with $i < j$) are not treated symmetrically.

For each vertex $v \in V_{i,j}$, consider the two pairs of edge twins incident to it. We label the edge twins in C_i by the variables (x_1, x_3) such that x_3 is the successor of x_1 in the orientation of C_i. Hence, for all $v \in V_{i,j}$, these variables (x_1, x_3) take the same assignment $(0, 1)$ when $e_i = 0$ and $(1, 0)$ when $e_i = 1$. Then, label the edge twins in C_j at v by (x_2, x_4) so that the 4 edges at v are ordered (x_1, x_2, x_3, x_4) in counterclockwise order. This choice of (x_2, x_4) is unique given the labeling (x_1, x_3).

As we traverse C_i according to the orientation of C_i, locally there is a notion of the *left side* of C_i. At any vertex $v \in C_i \cap C_j$, if we take the traversal of C_j according to the orientation of C_j, it either *comes into* or *goes out* of the left side of C_i. We call $v \in C_i \cap C_j$ of the former kind "entry-vertices", and the latter kind "exit-vertices" (see Figure 18).

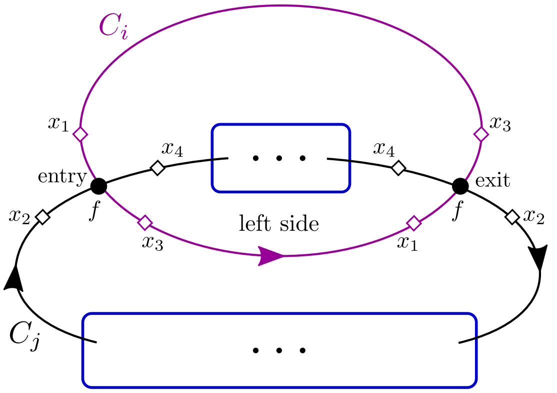


图 18: Intersection vertices between C_i and C_j

At any entry-vertex $v \in V_{i,j}$, the variable x_4 is the successor of x_2, while at any exit-vertex x_2 is the successor of x_4. Therefore, at entry-vertices, variables (x_2, x_4) take assignment $(0, 1)$ when $e_j = 0$ and $(1, 0)$ when $e_j = 1$, while at exit-vertices they take assignment $(1, 0)$ and $(0, 1)$ respectively instead.

Table 7 summarizes the values of f and its rotated copies at intersection vertices $V_{i,j}$. According to the 4 different assignments of (e_i, e_j) as listed in column 1 of the table, column 2 and column 7 (indexed by (x_1, x_2, x_3, x_4)) list the assignments of (x_1, x_2, x_3, x_4) at entry-vertices and exit-vertices

(e_i, e_j)	entry-vertices					exit-vertices				
	(x_1, x_2, x_3, x_4)	f	$f^{\frac{\pi}{2}}$	f^{π}	$f^{\frac{3\pi}{2}}$	(x_1, x_2, x_3, x_4)	f	$f^{\frac{\pi}{2}}$	f^{π}	$f^{\frac{3\pi}{2}}$
$(0,0)$	$(0,0,1,1)$	a	y	x	b	$(0,1,1,0)$	b	a	y	x
$(0,1)$	$(0,1,1,0)$	b	a	y	x	$(0,0,1,1)$	a	y	x	b
$(1,1)$	$(1,1,0,0)$	x	b	a	y	$(1,0,0,1)$	y	x	b	a
$(1,0)$	$(1,0,0,1)$	y	x	b	a	$(1,1,0,0)$	x	b	a	y

表 7: The values of f and its rotated copies at intersection vertices

separately. With respect to this local labeling of (x_1, x_2, x_3, x_4), the signature f has four rotated forms:

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix}, M(f^{\frac{\pi}{2}}) = \begin{bmatrix} 0 & 0 & 0 & y \\ 0 & a & 0 & 0 \\ 0 & 0 & x & 0 \\ b & 0 & 0 & 0 \end{bmatrix}, M(f^{\pi}) = \begin{bmatrix} 0 & 0 & 0 & x \\ 0 & y & 0 & 0 \\ 0 & 0 & b & 0 \\ a & 0 & 0 & 0 \end{bmatrix} \text{ and } M(f^{\frac{3\pi}{2}}) = \begin{bmatrix} 0 & 0 & 0 & b \\ 0 & x & 0 & 0 \\ 0 & 0 & a & 0 \\ y & 0 & 0 & 0 \end{bmatrix}.$$

columns 3, 4, 5, 6 and columns 8, 9, 10, 11 list the corresponding values of the signature f in four forms f, $f^{\frac{\pi}{2}}$, f^{π} and $f^{\frac{3\pi}{2}}$ respectively.

Suppose there are k_1, k_2, k_3 and k_4 many entry-vertices assigned f, $f^{\frac{\pi}{2}}$, f^{π}, and $f^{\frac{3\pi}{2}}$, respectively, and there are ℓ_1, ℓ_2, ℓ_3 and ℓ_4 many exit-vertices assigned $f^{\frac{\pi}{2}}$, f^{π}, $f^{\frac{3\pi}{2}}$ and f, respectively. Then, according to the assignments of (e_i, e_j), the values of $g_{i,j}$ are listed in Table 8, and its signature matrix is given below:

$$M(g_{i,j}) = \begin{bmatrix} a^{k_1+\ell_1} y^{k_2+\ell_2} x^{k_3+\ell_3} b^{k_4+\ell_4} & a^{k_2+\ell_4} y^{k_3+\ell_1} x^{k_4+\ell_2} b^{k_1+\ell_3} \\ a^{k_4+\ell_2} y^{k_1+\ell_3} x^{k_2+\ell_4} b^{k_3+\ell_1} & a^{k_3+\ell_3} y^{k_4+\ell_4} x^{k_1+\ell_1} b^{k_2+\ell_2} \end{bmatrix}.$$

(e_i, e_j)	$g_{i,j}(e_i, e_j) = f^{k_1} (f^{\frac{\pi}{2}})^{k_2} (f^{\pi})^{k_3} (f^{\frac{3\pi}{2}})^{k_4} (f^{\frac{\pi}{2}})^{\ell_1} (f^{\pi})^{\ell_2} (f^{\frac{3\pi}{2}})^{\ell_3} f^{\ell_4}$
$(0,0)$	$a^{k_1} y^{k_2} x^{k_3} b^{k_4} a^{\ell_1} y^{\ell_2} x^{\ell_3} b^{\ell_4}$
$(0,1)$	$b^{k_1} a^{k_2} y^{k_3} x^{k_4} y^{\ell_1} x^{\ell_2} b^{\ell_3} a^{\ell_4}$
$(1,1)$	$x^{k_1} b^{k_2} a^{k_3} y^{k_4} x^{\ell_1} b^{\ell_2} a^{\ell_3} y^{\ell_4}$
$(1,0)$	$y^{k_1} x^{k_2} b^{k_3} a^{k_4} b^{\ell_1} a^{\ell_2} y^{\ell_3} x^{\ell_4}$

表 8: The values of $g_{i,j}$

Our proof that $g_{i,j} \in \mathcal{G}_f$ is based on the assertion that the number of "entry-vertices" and "exit-vertices" are equal, namely $\sum_{i=1}^{4} k_i = \sum_{i=1}^{4} \ell_i$.

- First, consider the base case $n = 0$. That is, C_i is a simple cycle without self-intersection. By the Jordan Curve Theorem, C_i divides the plane into two regions, an interior region and an exterior region. In this case, as we traverse C_i according to the orientation of C_i, the left side of the traversal is always the same region; we call it L_i (which could be either the interior or the exterior region, depending on the choice of the leader edge e_i). If we traverse C_j according to the orientation of C_j, we enter and exit the region L_i an equal number of times. Therefore there is an equal number of "entry-vertices" and "exit-vertices". Hence $\sum_{i=1}^{4} k_i = \sum_{i=1}^{4} \ell_i$. It follows that $g_{i,j} \in \mathcal{G}_f$ by the definition of $\mathcal{G}_f$.

- Inductively, suppose $g_{i,j} \in \mathcal{G}_f$ holds for any circuit C_i with at most n self-intersections. Let C_i have $n + 1$ self-intersections. We decompose C_i into two edge-disjoint circuits, each of which has at most n self-intersections (See Figure 19). Take any self-intersection vertex v^* of C_i. There are two pairs of 4-ary edge twins $\{e, e'\}$ and $\{\overline{e}, \overline{e}'\}$, where e' is the successor of e and $\overline{e}'$ is the successor of $\overline{e}$. Note that e and $\overline{e}$ are oriented toward v^*, and e' and $\overline{e}'$ are oriented away from v^*. By the definition of edge twins, $\{e, \overline{e}\}$ are adjacent, and $\{e', \overline{e}'\}$ are adjacent. We can break C_i into two oriented circuits C_i^1 and C_i^2, by splitting v^* into two vertices, and let e' follow $\overline{e}$ and let $\overline{e}'$ follow e. Let the mapping $\gamma : [0, 1] \to \mathbb{R}^2$, such that $\gamma(0) = \gamma(1/2) = \gamma(1) = v^*$, represent the traversal of C_i. Then we can define two mappings $\gamma^1, \gamma^2 : [0, 1] \to \mathbb{R}^2$, such that $\gamma^1(t) = \gamma(t/2)$ and $\gamma^2(t) = \gamma((t+1)/2)$. Then $\{\gamma^1, \gamma^2\}$ represent $\{C_i^1, C_i^2\}$ respectively. It follows that C_i is the edge disjoint union of C_i^1 and C_i^2 and they both inherit the same orientation from that of C_i. Any vertex in $V_{i,j}$ is distinct from a self intersection point of C_i and thus $V_{i,j}$ is a disjoint union $V_{i,j}^1 \cup V_{i,j}^2$, where $V_{i,j}^1 = C_i^1 \cap C_j$ and $V_{i,j}^2 = C_i^2 \cap C_j$.

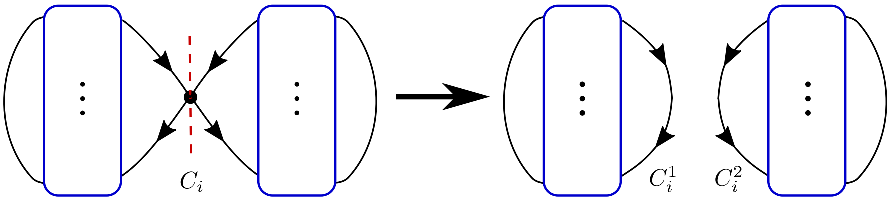


图 19: Decompose C_i into C_i^1 and C_i^2.

Since C_i^1 inherits the orientation from C_i, the orientation on C_i^1 is consistent with the orientation starting by choosing a leader edge on C_i^1. The same is true for the orientation on C_i^2. Thus, by induction, on each $C_i^1 \cap C_j$ and $C_i^2 \cap C_j$ there are an equal number of "entry-vertices" and “exit-vertices”. Hence $\sum_{i=1}^{4} k_i = \sum_{i=1}^{4} \ell_i$, and so $g_{i,j} \in \mathcal{G}_f$, completing the induction.

Let V_i be the set of all self-intersections of C_i. Let $\sigma'_{(e_i)}$ denote the restriction of σ' on $\{e_i\}$. Define a unary function h_i on e_i as follows: For any $b \in \{0, 1\}$, let

$$h_i(b) = \prod_{v \in V_i} f_v(\widehat{\sigma'_{(e_i)}} \mid_{E(v)}),$$

where $\widehat{\sigma'_{(e_i)}}$ is the unique extension of $\sigma'_{(e_i)}$ on the edge set of C_i, and $\sigma'_{(e_i)}$ is the unique assignment on $\{e_i\}$ such that $e_i \mapsto b$. The assignment of those edges incident to vertices in V_i can be uniquely extended from the assignment $\sigma'_{(e_i)}$. Hence, h_i is well-defined. We show that $h_i \in \mathcal{H}_f$.

For each vertex in V_i, since it is a self-intersection vertex, the two pairs of edge twins incident to it are both in C_i. We still first label each pair of edge twins by a pair of variables (x_1, x_3) obeying the orientation of C_i. That is, x_3 is always the successor of x_1. Now by the definition of 4-ary edge twins, the two edges labeled x_1 are adjacent. Hence at each vertex in V_i, starting from one x_1, the four incident edges are labeled by (x_1, x_1, x_3, x_3) in counterclockwise order. We pick the pair of variables (x_1, x_3) that appear in the second and fourth positions in this listing and change them to (x_2, x_4), so that the four edges are now labeled by (x_1, x_2, x_3, x_4) in counterclockwise order. Clearly, (x_2, x_4) and (x_1, x_3) take the same assignment. That is, at each vertex in V_i, the assignment of (x_1, x_2, x_3, x_4) is $(0, 0, 1, 1)$ when $e_i = 0$, and $(1, 1, 0, 0)$ when $e_i = 1$. Under this labeling, the signature f still has four rotated forms. The values of these four forms are listed in Table 9.

e_i	(x_1, x_2, x_3, x_4)	f	$f^{\frac{\pi}{2}}$	f^{π}	$f^{\frac{3\pi}{2}}$
0	$(0, 0, 1, 1)$	a	y	x	b
1	$(1, 1, 0, 0)$	x	b	a	y

表 9: The values of f and its rotated forms at self-intersection vertices

Suppose on V_i there are m_1, m_2, m_3 and m_4 many vertices assigned f, $f^{\frac{\pi}{2}}$, f^{π} and $f^{\frac{3\pi}{2}}$ respectively. Then, we have

$$M(h_i) = [a^{m_1} y^{m_2} x^{m_3} b^{m_4} \quad a^{m_3} y^{m_4} x^{m_1} b^{m_2}].$$

It follows that $h_i \in \mathcal{H}_f$.

For any vertex $v \in V$, it is either in some $V_{i,j}$ or some V_i. Thus,

$$\begin{aligned}
\text{Pl-Holant}_{\Omega} &= \sum_{\sigma':\{e_1,\cdots,e_k\}\to\{0,1\}} \Bigg(\prod_{\substack{v\in V_{i,j}\\ 1\leqslant i<j\leqslant k}} f_v(\sigma'|E_{(v)})\Bigg)\Bigg(\prod_{\substack{v\in V_i\\ 1\leqslant i\leqslant k}} f_v(\sigma'|E_{(v)})\Bigg)\\
&= \sum_{\sigma':\{e_1,\cdots,e_k\}\to\{0,1\}} \Bigg(\prod_{1\leqslant i<j\leqslant k} g_{i,j}(\sigma'(e_i),\sigma'(e_j))\Bigg)\Bigg(\prod_{1\leqslant i\leqslant k} h_i(\sigma'(e_i))\Bigg),
\end{aligned}$$

where $g_{i,j} \in \mathcal{G}_f$ and $h_i \in \mathcal{H}_f$. Therefore, Pl-Holant$(\neq_2|\ f) \leqslant_T \#CSP(\mathcal{G}_f \cup \mathcal{H}_f)$.

Here, we give an example for the reduction (9.3).

Example. The signature grid $\Omega = (G, \pi)$ for Pl-Holant$\,(\neq_2|\ f)$ in Figure 20 has two circuits C_1 (the Square) and C_2 (the Horizontal Eight) in G. We have chosen (arbitrarily) a leader edge e_i for each circuit C_i. In Figure 20 they are near the top left corner. Given the leader, the direction from its endpoint of degree 2 to the endpoint of degree 4 gives a default orientation of the circuit. Given a nonzero term in the sum Pl-Holant$_\Omega$, as a consequence of the support of f, the assignment of edges in each circuit is uniquely determined by the assignment of its leader. That is, any assignment of the leaders $\sigma' : \{e_1, e_2\} \to \{0, 1\}$ can be uniquely extended to an assignment of all edges $\sigma : E \to \{0, 1\}$ such that on each circuit the values of $0, 1$ alternate.

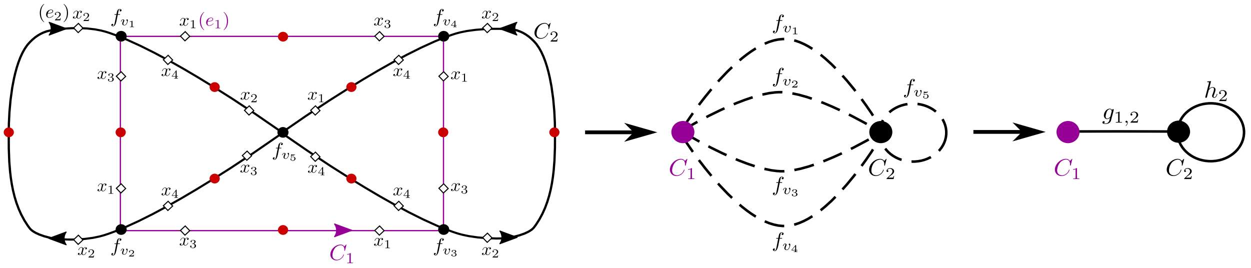


图 20: An example for the reduction (9.3)

Consider the signatures $f_{v_1}, f_{v_2}, f_{v_3}$ and f_{v_4} on the intersection vertices between C_1 and C_2. Assume C_1 does not have self-intersection (as is The Square); otherwise, we will decompose C_1 further and reason inductively. Without self-intersection, C_1 has an interior and exterior region by the Jordan Curve Theorem. For the chosen orientation of C_1, its left side happens to be the interior region. With respect to C_1, the circuit C_2 enters and exits the interior of C_1 alternately. Thus, we can divide the intersection vertices into an equal number of "entry-vertices" and "exit-vertices".

In this example, f_{v_1} and f_{v_4} are on "entry-vertices", while f_{v_2} and f_{v_3} are on "exit-vertices". By analyzing the values of each f when e_1 and e_2 take assignment 0 or 1, we can view each f as a binary constraint on (C_1, C_2). Depending on the 4 different rotation forms of f and whether f is on "entry-vertices" or "exit-vertices", the resulting binary constraint has 8 different forms (See Table 7). By multiplying these constraints, we get the binary constraint $g_{1,2}$. This can be viewed as a binary edge function on the circuits C_1 and C_2. The property of $g_{1,2}$ crucially depends on there are an equal number of "entry-vertices" and "exit-vertices". For any $b, b' \in \{0, 1\}$,

$$g_{1,2}(b, b') = \prod_{1 \leqslant i \leqslant 4} f_{v_i}(\widehat{\sigma'_{(e_1,e_2)}} \mid_{E_{(v_i)}}),$$

where $\widehat{\sigma'_{(e_1,e_2)}}$ uniquely extends to C_1 and C_2 the assignment $\sigma'_{(e_1,e_2)}(e_1) = b$ and $\sigma'_{(e_1,e_2)}(e_2) = b'$.

If the placement of f_{v_1} were to be rotated clockwise $\frac{\pi}{2}$, then f_{v_1} will be changed to $f_{v_1}^{\frac{\pi}{2}}$ in the above formula, where $M_{x_1x_2,x_4x_3}(f_{v_1}^{\frac{\pi}{2}}) = M_{x_2x_3,x_1x_4}(f_{v_1})$.

For the self-intersection vertex f_{v_5}, the notions of "entry-vertex" and "exit-vertex" do not apply. f_{v_5} gives rise to a unary constraint H on e_2. Depending on the 4 different rotation forms of f, H has 4 different forms (see Table 3). For any $b \in \{0, 1\}$,

$$h_2(b) = f_{v_5}(\widehat{\sigma'_{(e_2)}} \mid_{E_{(v_5)}}),$$

where $\widehat{\sigma'_{(e_2)}}$ uniquely extends to C_2 the assignment $\sigma'_{(e_2)}(e_2) = b$.

Therefore, we have

$$\begin{aligned}
\text{Pl-Holant}_\Omega &= \sum_{\sigma: E \to \{0,1\}} \prod_{v \in V(G)} f_v(\sigma \mid_{E_{(v)}}) \\
&= \sum_{\sigma': \{e_1, e_2\} \to \{0,1\}} \left(\prod_{1 \leqslant i \leqslant 4} f_{v_i}(\sigma' | E_{(v_i)}) \right) f_{v_5}(\sigma' | E_{(v_5)}) \\
&= \sum_{\sigma': \{e_1, e_2\} \to \{0,1\}} g_{1,2}(\sigma'(e_1), \sigma'(e_2)) H(\sigma'(e_2)).
\end{aligned}$$

Part II: Suppose I is a given instance of #CSP(g_{1_f}, g_{2_f}). Each constraint g_{1_f} and g_{2_f} is applied on certain pairs of variables. It is possible that they are applied to a single variable, resulting in two unary constraints. We will deal with such constraints later. We first consider the case that every constraint is applied on two distinct variables.

For any pair $i < j$, consider all binary constraints on variables x_i and x_j $(i < j)$. Note that g_{1_f} is symmetric, that is, $g_{1_f}(x_i, x_j) = g_{1_f}(x_j, x_i)$. We assume all the constraints between x_i and x_j are: $s_{i,j}$ many constraints $g_{1_f}(x_i, x_j)$, $t_{i,j}$ many constraints $g_{2_f}(x_i, x_j)$ and $t'_{i,j}$ many constraints $g_{2_f}(x_j, x_i)$. Let $g_{i,j}(x_i, x_j)$ be the function product of these constraints. That is,

$$g_{i,j}(x_i, x_j) = g_{1_f}^{s_{i,j}}(x_i, x_j) g_{2_f}^{t_{i,j}}(x_i, x_j) g_{2_f}^{t'_{i,j}}(x_j, x_i).$$

Then, we have

$$\#\mathrm{CSP}(I) = \sum_{\sigma:\{x_1,\ldots,x_k\}\to\{0,1\}} \prod_{1\leqslant i<j\leqslant n} g_{i,j}(\sigma(x_i), \sigma(x_j)).$$

We prove the reduction (9.4) in two steps. We first reduce #CSP(I) to both instances Ω_i (for $i = 1, 2$) of Pl-Holant $(\neq_2|\ f, \chi_i)$ respectively, where $\chi_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ and $\chi_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$. The instance Ω_i is constructed as follows:

1. Draw a cycle D_1, i.e., a homeomorphic image of S^1, on the plane. For $2 \leqslant j \leqslant k$ successively draw cycles D_j, and for all $1 \leqslant i < j$ let D_j intersect transversally with D_i at least $2(s_{i,j} + t_{i,j} + t'_{i,j})$ many times. This can be done since we can let D_j enter and exit the interiors of D_i successively. A concrete realization is as follows: Place k vertices D_i on a semi-circle in the order of $i = 1, \ldots, k$. For $1 \leqslant i < j \leqslant k$, connect D_i and D_j by a straight line segment L_{ij}. Now thicken each vertex D_i into a small disk, and deform the boundary circle of D_j so that, for every $1 \leqslant i < j$, it reaches across to D_i along the line segment L_{ij}, and intersects the boundary circle of D_i exactly $2(s_{i,j}+t_{i,j}+t'_{i,j})$ many times. (There are also other intersections between these cycles D_i's due to crossing intersections between those line segments. This is why we say "at least" this many intersections in the overall description. We will deal with those extra intersection vertices later.) We can draw these cycles to satisfy the following conditions:

   a. There is no self-intersection for each D_i.

   b. Every intersection point is between exactly two cycles. They intersect transversally. Each intersection creates a vertex of degree 4.

These intersecting cycles define a planar 4-regular graph G', where intersection points are the vertices.

2. Replace each edge of G' by a path of length two. We get a planar bipartite graph $G = (V, E)$. On one side, all vertices have degree 2, and on the other side, all vertices have degree 4. We can still define edge twins as in Part I. Moreover, we still divide the graph into some circuits $C_1, \ldots, C_k$. In fact, C_i is just the cycle D_i after the replacement of each edge by a path of length two.

   Let $V_{i,j} = C_i \cap C_j$ $(i < j)$ be the intersection vertices between C_i and C_j. Clearly, $|V_{i,j}|$ is even and at least $2(s_{i,j} + t_{i,j} + t'_{i,j})$. Since there is no self-intersection, each circuit is a simple cycle. As we did in Part I, we pick an edge e_i as the leader edge of C_i and this gives an orientation of C_i. We can define "entry-vertices" and "exit-vertices" as in Part I. Among $V_{i,j}$, half are entry-vertices and the other half are exit-vertices. (This notion is defined in terms of C_j with respect to C_i; the roles of i and j are not symmetric.) List the edges in C_i according to the orientation of C_i starting with the leader edge e_i. After we place copies of f on each vertex, the support of f, which is contained in $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$, ensures that every 4-ary twins can only take values $(0, 1)$ or $(1, 0)$, since the 4-ary twin edges are non-adjacent. Then all edges in C_i can only take assignment $(0, 1, 0, 1, \cdots, 0, 1)$ when $e_i = 0$ and $(1, 0, 1, 0, \cdots, 1, 0)$ when $e_i = 1$.

3. Label all vertices of degree 2 by $(\neq_2)$. For any vertex in $V_{i,j}$ $(i < j)$, as we showed in Part I, we can label the four edges incident to it by variables (x_1, x_2, x_3, x_4) in a way such that when $\sigma' : (e_i, e_j) \mapsto (b, b') \in \{0, 1\}^2$, we have $(x_1, x_2, x_3, x_4) = (b, b', 1-b, 1-b')$ at any entry-vertex, and $(x_1, x_2, x_3, x_4) = (b, 1-b', 1-b, b')$ at any exit-vertex (See Table 7). Note that f has four rotation forms under this labeling. We have (at least) $s_{i,j} + t_{i,j} + t'_{i,j}$ many entry-vertices and as many exit-vertices. Let $V'_{i,j}$ be the set of these $2(s_{i,j} + t_{i,j} + t'_{i,j})$ vertices. For vertices in $V'_{i,j}$, we label $s_{i,j}$ many entry-vertices by f and $s_{i,j}$ many exit-vertices by $f^{\frac{\pi}{2}}$, $t_{i,j}$ many entry-vertices by f and $t_{i,j}$ many exit-vertices by $f^{\frac{3\pi}{2}}$, and $t'_{i,j}$ many entry-vertices by f^{π} and $t'_{i,j}$ many exit-vertices by $f^{\frac{\pi}{2}}$. Refer to Table 8, this choice amounts to taking

$$k_1 = s_{i,j} + t_{i,j}, \quad k_3 = t'_{i,j}, \quad \text{and,} \quad \ell_1 = s_{i,j} + t'_{i,j}, \quad \ell_3 = t_{i,j},$$

and all other k_i, ℓ_i's equal to 0. Recall that $g_{1_f}(x_1, x_2)$ corresponds to choosing $k_1 = \ell_1 = 1$ and the others all 0, $g_{2_f}(x_1, x_2)$ corresponds to choosing $k_1 = \ell_3 = 1$ and the others all 0, and $g_{2_f}(x_2, x_1)$ corresponds to choosing $k_3 = \ell_1 = 1$ and the others all 0, then we have

$$\prod_{v \in V'_{ij}} f_v(\sigma'_{(e_i,e_j)} \mid_{E(v)}) = g_{1_f}^{s_{i,j}}(e_i, e_j) g_{2_f}^{t_{i,j}}(e_i, e_j) g_{2_f}^{t'_{i,j}}(e_j, e_i) = g_{i,j}(e_i, e_j).$$

For all vertices in $V_{i,j} \backslash V'_{i,j}$, if we label them by an auxiliary signature $\chi_1 = \begin{bmatrix} 0&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&0 \end{bmatrix}$, then, referring to Table 8 (Here $a = x = b = y = 1$), we have

$$\prod_{v \in V_{i,j} \backslash V'_{ij}} \chi_1(\sigma'_{(e_i,e_j)} \mid_{E(v)}) = 1,$$

for all assignments σ' on $\{e_i, e_j\}$. We can also label the vertices in $V_{i,j} \backslash V'_{i,j}$ by an auxiliary signature $\chi_2 = \begin{bmatrix} 0&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \\ -1&0&0&0 \end{bmatrix}$. By our (semi-circle) construction, in $V_{i,j} \backslash V'_{i,j}$, the number of entry-vertices is equal to the number of exit-vertices. We label all entry-vertices by χ_2 and label all exit-vertices by its rotated form $\chi_2^{\frac{\pi}{2}} = \begin{bmatrix} 0&0&0&1 \\ 0&1&0&0 \\ 0&0&-1&0 \\ 1&0&0&0 \end{bmatrix}$. Refer to Table 8 (here $a = b = y = 1, x = -1$, and $k = k_1 = \ell_1 = \ell$, and the crucial equation is $g_{i,j}(1, 1) = x^{k_1+\ell_1} = (-1)^2 = 1$), we have

$$\prod_{v \in V_{i,j} \backslash V'_{ij}} \chi_2(\sigma'_{(e_i,e_j)} \mid_{E(v)}) = 1,$$

for all assignments σ' on $\{e_i, e_j\}$.

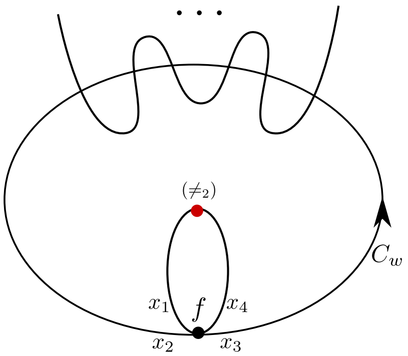


图 21: Creating self-loop locally on cycle C_w

Then, consider the case that g_{1_f} and g_{2_f} are applied to the pair variables (w, w), in which case g_{1_f} and g_{2_f} effectively become unary constraints $[a^2, x^2]$ and $[ax, ax]$ on the variable x_i. The latter is a constant multiple of $[1,1]$ and can be ignored. The unary constraint $[a, x]$, and hence also $[a^2, x^2]$, can be easily realized by f in Pl-Holant($\neq_2|\ f, \chi_i$), by creating a self-loop for the cycle representing the variable w, denoted by C_w (See Figure 21). Note that the self-loop is created locally on the cycle C_w such that it does not affect other cycles. As we did in Part I, we label the four edges incident to a self-intersection vertex by (x_1, x_2, x_3, x_4) such that x_3 is the successor of x_1 and x_4 is the successor of x_2 depending on the default orientation of C_w, and (x_1, x_2, x_3, x_4) are labeled in counterclockwise order. Then, we have $(x_1, x_3) = (x_2, x_4) = (0, 1)$ when $w = 0$ and $(1, 0)$ when $w = 1$. That is, $g_{1f}(0, 0) = a^2 = f^2_{0011}$ and $g_{1f}(1, 1) = x^2 = f^2_{1100}$.

Now, we get an instance Ω_s $(s = 1, 2)$ for each problem Pl-Holant $(\neq_2|\ f, \chi_s)$ respectively. Note that χ_s has the support $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$ as f. As we have showed in Part I, for any nonzero term in the sum Pl-Holant$_{\Omega_s}$, the assignment of all edges $\sigma : E \to \{0, 1\}$ can be uniquely extended from the assignment of all leader edges $\sigma' : \{e_1, e_2, \ldots, e_k\} \to \{0, 1\}$. Therefore, we have

$$\begin{aligned}
\#\mathrm{CSP}(I) &= \sum_{\sigma':\{e_1,\cdots,e_k\}\to\{0,1\}} \prod_{1\leqslant i<j\leqslant n} g_{i,j}(\sigma'(e_i), \sigma'(e_j)) \\
&= \sum_{\sigma':\{e_1,\cdots,e_k\}\to\{0,1\}} \left(\prod_{\substack{v\in V'_{i,j} \\ 1\leqslant i<j\leqslant n}} f_v(\sigma'|_{E_{(v)}}) \right) \left(\prod_{\substack{v\in V_{i,j}\setminus V'_{i,j} \\ 1\leqslant i<j\leqslant n}} \chi_{s_v}(\sigma'|_{E_{(v)}}) \right) \\
&= \text{Pl-Holant}_{\Omega_s}
\end{aligned}$$

for $s = 1, 2$. That is, $\#\mathrm{CSP}(g_{1_f}, g_{2_f}) \leqslant_T$ Pl-Holant $(\neq_2|\ f, \chi_s)$, $(s = 1, 2)$.

From the hypothesis of the reduction (9.4), we have $a = \pm x \neq 0, b = \pm y \neq 0$, and $(b/a)^8 \neq 1$. We show by interpolation

$$\text{Pl-Holant}(\neq_2|\ f, \chi_1) \leqslant_T \text{Pl-Holant}(\neq_2|\ f)$$

when $a = \epsilon x, b = \epsilon y$, and

$$\text{Pl-Holant}(\neq_2|\ f, \chi_2) \leqslant_T \text{Pl-Holant}(\neq_2|\ f)$$

when $a = \epsilon x, b = -\epsilon y$, where $\epsilon = \pm 1$.

- If $a = x$ and $b = y$, since they are all nonzero, and $(\frac{b}{a})^8 \neq 1$, by normalization we may assume $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $b \neq 0$ and $b^8 \neq 1$.

  If b is not a root of unity, by Lemma 9.1, we have Pl-Holant$(\neq_2 | \, f, \chi_1) \leqslant_T$ Pl-Holant$(\neq_2 | \, f)$. Otherwise, b is a root of unity. Construct a gadget $f_{\boxtimes}$ as shown in Figure 22. Given an assignment (x_1, x_2, x_3, x_4) to $f_{\boxtimes}$, and suppose $f_{\boxtimes}(x_1, x_2, x_3, x_4) \neq 0$. Then because of the support of f_{v_1}, f_{v_5} and f_{v_3} we must have $x_1 \neq x_3$. Similarly $x_2 \neq x_4$. Also f_{v_5} receives the same input as $f_{\boxtimes}$. Hence the support of $f_{\boxtimes}$ is contained in $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$, i.e., contained in $\{(0,0,1,1), (1,1,0,0), (0,1,1,0), (1,0,0,1)\}$. In particular, the edges on each Diagonal Line of this gadget can only take assignments $(0,1,0,1,0,1)$ or $(1,0,1,0,1,0)$, otherwise the we get zero. On the other hand, the Square cycle in this gadget is a circuit itself, so that the edges in it can only take two assignments $(0,1,0,1,0,1,0,1)$ or $(1,0,1,0,1,0,1,0)$. We simplify the notation to $(0,1)$ and $(1,0)$ respectively. On $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$, the value of $f_{\boxtimes}$ is the sum over these two terms.

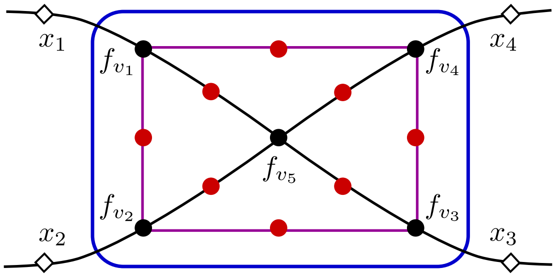


图 22: The Square gadget

  For the signature f, if one pair of its edge twins flips its assignment between $(0,1)$ and $(1,0)$, then the value of f changes from 1 to b, or from b to 1. If both pairs of edge twins flip their assignments, then the value of f does not change. According to this property, we give the Table 10. Here, we place a suitably rotated copy of f at vertices v_i to get f_{v_i} (for $1 \leq i \leq 5$) so that the values of f_{v_i} are all 1 under the assignment $(x_1, x_2, x_3, x_4) = (0,0,1,1)$ and the Square is assigned $= (0,1)$ (row 2 of Table 10). When the assignment of Square flips from $(0,1)$ to $(1,0)$, one pair of edge twins of each vertex except v_5 flips its assignment. So the values of f on these vertices except v_5 change from 1 to b (row 3). When (x_1, x_3) flips its assignment, one pair of edge twins of v_1, v_3 and v_5 flip their assignments. When (x_2, x_4) flips

(x_1, x_2, x_3, x_4)	Square	f_{v_1}	f_{v_2}	f_{v_3}	f_{v_4}	f_{v_5}	$f_{\boxtimes}$
$(0,0,1,1)$	$(0,1)$	1	1	1	1	1	$1+b^4$
	$(1,0)$	b	b	b	b	1	
$(1,1,0,0)$	$(0,1)$	b	b	b	b	1	$1+b^4$
	$(1,0)$	1	1	1	1	1	
$(0,1,1,0)$	$(0,1)$	1	b	1	b	b	$2b^3$
	$(1,0)$	b	1	b	1	b	
$(1,0,0,1)$	$(0,1)$	b	1	b	1	b	$2b^3$
	$(1,0)$	1	b	1	b	b	

表 10: The values of gadget $f_{\boxtimes}$ when $a = x = 1$ and $b = y$

its assignment, one pair of edge twins of v_2, v_4 and v_5 flip their assignments. Using this fact, we get other rows correspondingly.

Hence, $f_{\boxtimes}$ has the signature matrix $M(f_{\boxtimes}) = \begin{bmatrix} 0 & 0 & 0 & 1+b^4 \\ 0 & 2b^3 & 0 & 0 \\ 0 & 0 & 2b^3 & 0 \\ 1+b^4 & 0 & 0 & 0 \end{bmatrix}$. Since $b^8 \neq 1$, we have $1+b^4 \neq 0$, by normalization we can write $M(f_{\boxtimes}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{2b^3}{1+b^4} & 0 & 0 \\ 0 & 0 & \frac{2b^3}{1+b^4} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Since $|b| = 1$ and $b^4 \neq 1$, we have $|1+b^4| < 2$. Then $|\frac{2b^3}{1+b^4}| > |b^3| = 1$, which means $\frac{2b^3}{1+b^4}$ is not a root of unity. By Lemma 9.1, we have Pl-Holant($\neq_2 |\ f, \chi_1$) $\leqslant_T$ Pl-Holant($\neq_2 |\ f, f_{\boxtimes}$). Since $f_{\boxtimes}$ is constructed by f, we have Pl-Holant($\neq_2 |\ f, \chi_1$) $\leqslant_T$ Pl-Holant($\neq_2 |\ f$).

- If $a = -x$ and $b = -y$, then $M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & -b & 0 \\ -a & 0 & 0 & 0 \end{bmatrix}$. Connect the variable x_4 with x_3 of f using ($\neq_2$), and we get a binary signature g', where

$$g' = M_{x_1 x_2, x_4 x_3}(0, 1, 1, 0)^T = (0, b, -b, 0)^T.$$

Since $b \neq 0$, g' can be normalized as $(0, 1, -1, 0)^T$. Modifying $x_1 = 1$ of f by -1 scaling, we get a signature f' with the signature matrix $M(f') = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ a & 0 & 0 & 0 \end{bmatrix}$. As we have proved above, Pl-Holant($\neq_2 |\ f, \chi_1$) $\leqslant_T$ Pl-Holant($\neq_2 |\ f, f'$). Since f' is constructed by f, we have Pl-Holant($\neq_2 |\ f, \chi_1$) $\leqslant_T$ Pl-Holant($\neq_2 |\ f$).

- If $a = -x$, $b = y$ or $a = x$, $b = -y$, by normalization and rotational symmetry, we may assume $M(f) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$, where $b \neq 0$ and $b^8 \neq 1$.

If b is not a root of unity, by Corollary 9.2, we have Pl-Holant$(\neq_2|\ f, \chi_2) \leqslant_T$ Pl-Holant$(\neq_2|\ f)$. Otherwise, b is a root of unity. Construct the gadget $f_{\boxtimes}$ in the same way as shown above. Our discussion on the support of $f_{\boxtimes}$ still holds: It is contained in $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$; on (x_1, x_2, x_3, x_4) with $(x_1 \neq x_3) \wedge (x_2 \neq x_4)$, f_{v_5} receives the same input, and the value of $f_{\boxtimes}$ is the sum over two assignments $(0, 1)$ and $(1, 0)$ for the Square.

For the signature f, if one pair of its edge twins flips its assignment between $(0, 1)$ and $(1, 0)$, then the value of f changes from ± 1 to b, or b to ∓ 1. If two pairs of edge twins both flip their assignments, then the value of f does not change if the value is b, or changes its sign if the value is ± 1. According to this property, we have the following Table 11. Here, we place a suitably rotated copy of f at vertices v_i to get f_{v_i} (for $1 \leq i \leq 5$) so that the values of f_{v_i} are all 1 under the assignment $(x_1, x_2, x_3, x_4) = (0, 0, 1, 1)$ and the Square is assigned $= (0, 1)$ (row 2 of Table 11). When the assignment of Square flips from $(0, 1)$ to $(1, 0)$, one pair of edge twins at each vertex except v_5 flips its assignment. So the values of f at these vertices except v_5 change from 1 to b (row 3). When (x_1, x_3) flips its assignment, one pair of edge twins at v_1, v_3 and v_5 flips their assignments. When (x_2, x_4) flips its assignment, one pair of edge twins at v_2, v_4 and v_5 flips their assignments. Using this fact, we get other rows correspondingly.

(x_1, x_2, x_3, x_4)	Square	f_{v_1}	f_{v_2}	f_{v_3}	f_{v_4}	f_{v_5}	$f_{\boxtimes}$
$(0, 0, 1, 1)$	$(0, 1)$	1	1	1	1	1	$1 + b^4$
	$(1, 0)$	b	b	b	b	1	
$(1, 1, 0, 0)$	$(0, 1)$	b	b	b	b	-1	$-(1 + b^4)$
	$(1, 0)$	-1	-1	-1	-1	-1	
$(0, 1, 1, 0)$	$(0, 1)$	1	b	1	b	b	$2b^3$
	$(1, 0)$	b	-1	b	-1	b	
$(1, 0, 0, 1)$	$(0, 1)$	b	1	b	1	b	$2b^3$
	$(1, 0)$	-1	b	-1	b	b	

表 11: The values of gadget $f_{\boxtimes}$ when $a = -x = 1$ and $b = y$

Hence, $f_{\boxtimes}$ has the signature matrix $\begin{bmatrix} 0 & 0 & 0 & 1+b^4 \\ 0 & 2b^3 & 0 & 0 \\ 0 & 0 & 2b^3 & 0 \\ -(1+b^4) & 0 & 0 & 0 \end{bmatrix}$. Since $|b| = 1$ and $b^8 \neq 1$, we have $b^4 \neq \pm 1$, therefore $0 < |1 + b^4| < 2$, and so $\frac{2b^3}{1+b^4}$ is not a root of unity. By Corollary 9.2, Pl-Holant$(\neq_2|\, f, \chi_2) \leqslant_T$ Pl-Holant$(\neq_2|\, f, f_{\boxtimes})$, and hence Pl-Holant$(\neq_2|\, f, \chi_2) \leqslant_T$ Pl-Holant$(\neq_2|\, f)$.

In summary, we have

$$\begin{tikzcd}
 & \text{Pl-Holant}\,(\neq_2|\, f, \chi_1) \arrow[dr, "{a = \epsilon x, b = \epsilon y\ (\epsilon = \pm 1)}"] & \\
\#\mathrm{CSP}(g_{1_f}, g_{2_f}) \arrow[ur] \arrow[dr] \arrow[r, phantom, "\leqslant_T"] & {} \arrow[r, phantom, "\leqslant_T"] & \text{Pl-Holant}\,(\neq_2|\, f) \\
 & \text{Pl-Holant}\,(\neq_2|\, f, \chi_2) \arrow[ur, "{a = \epsilon x, b = -\epsilon y\ (\epsilon = \pm 1)}"'] &
\end{tikzcd}$$

Therefore, we have $\#\mathrm{CSP}(g_{1_f}, g_{2_f}) \leqslant_T$ Pl-Holant$\,(\neq_2|\, f)$ when $a^2 = x^2 \neq 0$, $b^2 = y^2 \neq 0$ and $(\frac{b}{a})^8 \neq 1$. □

Remark 9.29. *A crucial point in the reduction (9.3) is the fact that the given instance graph G of* Pl-Holant$\,(\neq_2|\, f)$ *is planar so that $\sum_i k_i = \sum_i \ell_i$. Otherwise this does not hold in general; for example the latitudinal and longitudinal closed cycles on a torus intersect at a single point. The equation $\sum_i k_i = \sum_i \ell_i$ is crucial to obtain tractability in the following theorem.*

Theorem 9.30. *Let f be a 4-ary signature of the form (9.2), where $(a, x) \neq (0, 0)$ and $(b, y) \neq (0, 0)$. Then* Pl-Holant$(\neq_2|\, f)$ *is #P-hard unless*

(i) $(ax)^2 = (by)^2$, *or*

(ii) $x = a\mathrm{i}^{\alpha}, b = a\sqrt{\mathrm{i}}^{\beta}, y = a\sqrt{\mathrm{i}}^{\gamma}$, *where $\alpha, \beta, \gamma \in \mathbb{N}$, and $\beta \equiv \gamma \pmod 2$,*

in which cases, the problem is tractable in polynomial time.

Proof of Tractability:

- In case (i), if $ax = by = 0$, then f has support of size at most 2. So we have $f \in \mathscr{P}$, and hence Pl-Holant$(\neq_2|\, f)$ is tractable by Theorem 2.30. Otherwise, $(ax)^2 = (by)^2 \neq 0$. For any signature g in $\mathcal{G}_f$, we have $g_{00} \cdot g_{11} = (ax)^{k_1+\ell_1+k_3+\ell_3}(by)^{k_2+\ell_2+k_4+\ell_4}$ and $g_{01} \cdot g_{10} =$

$(ax)^{k_2+\ell_2+k_4+\ell_4}(by)^{k_1+\ell_1+k_3+\ell_3}$. Since $(k_1+\ell_1+k_3+\ell_3)-(k_2+\ell_2+k_4+\ell_4) \equiv k+\ell \equiv 0 \pmod 2$, we have

$$\frac{g_{00}\cdot g_{11}}{g_{01}\cdot g_{10}} = \left(\frac{ax}{by}\right)^{(k_1+\ell_1+k_3+\ell_3)-(k_2+\ell_2+k_4+\ell_4)} = \left(\frac{(ax)^2}{(by)^2}\right)^{\frac{(k_1+\ell_1+k_3+\ell_3)-(k_2+\ell_2+k_4+\ell_4)}{2}} = 1.$$

That is, $g \in \mathscr{P}$. Since any signature h in $\mathcal{H}_f$ is unary, $h \in \mathscr{P}$. Hence, we have $\mathcal{G}_f \cup \mathcal{H}_f \subseteq \mathscr{P}$. By Theorem 9.19, #CSP$(\mathcal{G}_f \cup \mathcal{H}_f)$ is tractable. By reduction (9.3) of Lemma 9.28, we have Pl-Holant$(\neq_2 \mid f)$ is tractable.

- In case (ii), for any signature $g \in \mathcal{G}_f$ defined in Definition 9.26, $M(g)$ is of the form

$$a^{k+\ell}\begin{bmatrix} \sqrt{\mathfrak{i}}^{\beta(k_4+\ell_4)+\gamma(k_2+\ell_2)+2\alpha(k_3+\ell_3)} & \sqrt{\mathfrak{i}}^{\beta(k_1+\ell_3)+\gamma(k_3+\ell_1)+2\alpha(k_4+\ell_2)} \\ \sqrt{\mathfrak{i}}^{\beta(k_3+\ell_1)+\gamma(k_1+\ell_3)+2\alpha(k_2+\ell_4)} & \sqrt{\mathfrak{i}}^{\beta(k_2+\ell_2)+\gamma(k_4+\ell_4)+2\alpha(k_1+\ell_1)} \end{bmatrix} = a^{k+\ell}\begin{bmatrix} \sqrt{\mathfrak{i}}^{p_{00}} & \sqrt{\mathfrak{i}}^{p_{01}} \\ \sqrt{\mathfrak{i}}^{p_{10}} & \sqrt{\mathfrak{i}}^{p_{11}} \end{bmatrix},$$

where p_{00}, p_{01}, p_{10} and p_{11} denote the integer exponents of $\sqrt{\mathfrak{i}}$ in the respective entries of g. Since $\beta \equiv \gamma \pmod 2$, if they are both even, then $p_{00} \equiv p_{01} \equiv p_{10} \equiv p_{11} \equiv 0 \pmod 2$; if they are both odd, then $p_{00} \equiv p_{11} \equiv k_2+\ell_2+k_4+\ell_4 \equiv k_1+\ell_1+k_3+\ell_3 \equiv p_{01} \equiv p_{10} \pmod 2$. If these exponents are all odd, we can take out a $\sqrt{\mathfrak{i}}$. Hence, g is of the form $a'(\mathfrak{i}^{q_{00}}, \mathfrak{i}^{q_{01}}, \mathfrak{i}^{q_{10}}, \mathfrak{i}^{q_{11}})^T$, where $a' = a^{k+\ell}$ or $a^{k+\ell}\sqrt{\mathfrak{i}}$, and either $q_{ij} = \frac{p_{ij}}{2}$ for all $i, j \in \{0,1\}$ are integers, or $q_{ij} = \frac{p_{ij}-1}{2}$ for all $i, j \in \{0,1\}$ are integers. Thus,

$$q_{00}+q_{01}+q_{10}+q_{11} \equiv (p_{00}+p_{01}+p_{10}+p_{11})/2 \pmod 2.$$

Moreover, since $p_{00}+p_{01}+p_{10}+p_{11} = (k+\ell)(\beta+\gamma+2\alpha) \equiv 0 \pmod 4$, using the assumption that $\beta \equiv \gamma \pmod 2$ and $k \equiv \ell \pmod 2$, we conclude that $q_{00}+q_{01}+q_{10}+q_{11} \equiv 0 \pmod 2$. Therefore, $g \in \mathscr{A}$ by Lemma 2.8.

In this case, for any signature h in $\mathcal{H}_f$, $M(h)$ is of the form

$$a^m \begin{bmatrix} \sqrt{\mathfrak{i}}^{\beta m_4+\gamma m_2+2\alpha m_3} & \sqrt{\mathfrak{i}}^{\beta m_2+\gamma m_4+2\alpha m_1} \end{bmatrix}.$$

Since $\beta \equiv \gamma \pmod 2$, we have $\beta m_4 + \gamma m_2 \equiv \beta m_2 + \gamma m_4 \pmod 2$. Hence, h is of the form $a''[\mathfrak{i}^{q_0}, \mathfrak{i}^{q_1}]$, for some integers q_0, q_1, where $a'' = a^m$ or $a^m\sqrt{\mathfrak{i}}$. That is, $h \in \mathscr{A}$ by Lemma 2.9.

Hence, $\mathcal{G}_f \cup \mathcal{H}_f \subseteq \mathscr{A}$. By Theorem 9.19, #CSP($\mathcal{G}_f \cup \mathcal{H}_f$) is tractable. By reduction (9.3) of Lemma 9.28, we have Pl-Holant($\neq_2|\ f$) is tractable.

Proof of Hardness: We are given that f does not belong to case (i) or case (ii). Note that $M_{x_4x_1,x_3x_2}(f) = \left[\begin{smallmatrix} 0&0&0&b\\ 0&x&0&0\\ 0&0&a&0\\ y&0&0&0 \end{smallmatrix}\right]$ and $M_{x_2x_3,x_1x_4}(f) = \left[\begin{smallmatrix} 0&0&0&y\\ 0&a&0&0\\ 0&0&x&0\\ b&0&0&0 \end{smallmatrix}\right]$. Connect variables x_3, x_2 of a copy of the signature f with variables x_2, x_3 of another copy of signature f both using $(\neq_2)$. We get a signature f_1 with the signature matrix

$$M(f_1) = M_{x_4x_1,x_3x_2}(f) N_2 M_{x_2x_3,x_1x_4}(f) = \begin{bmatrix} 0&0&0&by\\ 0&0&x^2&0\\ 0&a^2&0&0\\ by&0&0&0 \end{bmatrix}.$$

Similarly, connect x_3, x_2 of a copy of signature f with x_4, x_1 of another copy of signature f both using $(\neq_2)$. We get a signature f_2 with the signature matrix

$$M(f_2) = M_{x_4x_1,x_3x_2}(f) N_2 M_{x_4x_1,x_3x_2}(f) = \begin{bmatrix} 0&0&0&b^2\\ 0&0&ax&0\\ 0&ax&0&0\\ y^2&0&0&0 \end{bmatrix}.$$

Notice that $M(f_1^{\frac{\pi}{2}}) = \left[\begin{smallmatrix} 0&0&0&0\\ 0&by&a^2&0\\ 0&x^2&by&0\\ 0&0&0&0 \end{smallmatrix}\right]$, $M(f_2^{\frac{\pi}{2}}) = \left[\begin{smallmatrix} 0&0&0&0\\ 0&b^2&ax&0\\ 0&ax&y^2&0\\ 0&0&0&0 \end{smallmatrix}\right]$, $M(g_{1_f}) = \left[\begin{smallmatrix} a^2&by\\ by&x^2 \end{smallmatrix}\right]$ and $M(g_{2_f}) = \left[\begin{smallmatrix} ax&b^2\\ y^2&ax \end{smallmatrix}\right]$. Recall that $M\left(\widetilde{f_i^{\frac{\pi}{2}}}_{\text{In}}\right) = M_{\text{In}}(f_i^{\frac{\pi}{2}}) \left[\begin{smallmatrix} 0&1\\ 1&0 \end{smallmatrix}\right]$. We have $g_{i_f} = \widetilde{f_i^{\frac{\pi}{2}}}_{\text{In}}$. That is, $f_i(x_1, x_2, x_3, x_4) = g_{i_f}(x_2, x_4) \cdot \chi_{x_1 \neq x_4} \cdot \chi_{x_2 \neq x_3}$. Now, we analyze g_{1_f} and g_{2_f}.

- If $\{g_{1_f}, g_{2_f}\} \subseteq \mathscr{P}$, then either $(ax)^2 = (by)^2$ if either signature is degenerate, or g_{1_f} and g_{2_f} are each generalized Equality or generalized Disequality respectively. In the latter case, since $(a, x) \neq (0, 0)$ and $(b, y) \neq (0, 0)$, it forces that $ax = by = 0$. So we still have $(ax)^2 = (by)^2$. That is, $\{a, b, x, y\}$ belongs to case (i). A contradiction.

- If $\{g_{1_f}, g_{2_f}\} \subseteq \mathscr{A}$, there are two subcases. Note that the support of a function in $\mathscr{A}$ has size a power of 2.

- If both g_{1_f} and g_{2_f} have support of size at most 2, then we have $ax = by = 0$ due to $(a, x) \neq (0, 0)$ and $(b, y) \neq (0, 0)$. This belongs to case (i). A contradiction.

- Otherwise, at least one of g_{1_f} or g_{2_f} has support of size 4. Then $abxy \neq 0$ and therefore both g_{1_f} and g_{2_f} have support of size 4. Let $x' = \frac{x}{a}, b' = \frac{b}{a}$ and $y' = \frac{y}{a}$. By normalization, we have
$$M(g_{1_f}) = a^2 \begin{bmatrix} 1 & b'y' \\ b'y' & x'^2 \end{bmatrix}.$$
Since $g_{1_f} \in \mathscr{A}$, by Lemma 2.8, x'^2 and $b'y'$ are both powers of $\mathfrak{i}$, and the sum of all exponents is even. It forces that $x'^2 = \mathfrak{i}^{2\alpha}$ for some $\alpha \in \mathbb{N}$. Then, we can choose α such $x' = \mathfrak{i}^{\alpha}$. Also, we have
$$M(g_{2_f}) = a^2 \begin{bmatrix} x' & b'^2 \\ y'^2 & x' \end{bmatrix}.$$
Since $g_{2_f} \in \mathscr{A}$ and x' is already a power of $\mathfrak{i}$, y'^2 and b'^2 are both powers of $\mathfrak{i}$. That is, $b' = \sqrt{\mathfrak{i}}^{\beta}$ and $y' = \sqrt{\mathfrak{i}}^{\gamma}$. Also, since $g_{1_f} \in \mathscr{A}$, $b'y' = \sqrt{\mathfrak{i}}^{\beta+\gamma}$ is a power of $\mathfrak{i}$, which means $\beta \equiv \gamma \pmod 2$. That is, $\{a, b, x, y\}$ belongs to case (ii). A contradiction.

- If $\{g_{1_f}, g_{2_f}\} \subseteq \widehat{\mathscr{M}}$, then by Lemma 9.12, we have both $a^2 = \epsilon x^2, by = \epsilon by$ and $ax = \epsilon' ax, y^2 = \epsilon' b^2$, for some $\epsilon, \epsilon' \in \{1, -1\}$. If $\epsilon = -1$ then $by = 0$, and then by the second set of equations $b = y = 0$, contrary to assumption that $(b, y) \neq (0, 0)$. So $\epsilon = 1$. Similarly $\epsilon' = 1$. Hence
$$a^2 = x^2 \qquad b^2 = y^2, \tag{9.5}$$
and it also follows that all 4 entries are nonzero.

Therefore, if $\{a, b, x, y\}$ does not satisfy (9.5) then $\{g_{1_f}, g_{2_f}\} \nsubseteq \mathscr{P}, \mathscr{A}$ or $\widehat{\mathscr{M}}$. By Theorem 9.19, Pl-#CSP(g_{1_f}, g_{2_f}) is #P-hard. Then by Lemma 9.23, Pl-Holant$(\neq_2 |\ f_1^{\frac{\pi}{2}}, f_2^{\frac{\pi}{2}})$ is #P-hard, and hence Pl-Holant$(\neq_2 |\ f)$ is #P-hard.

Otherwise, the 4 nonzero entries $\{a, b, x, y\}$ satisfy (9.5). If $(\frac{b}{a})^8 = 1$, i.e., $b = a\sqrt{\mathfrak{i}}^{\beta}$ for some $\gamma \in \mathbb{N}$, then $x = \pm a = a\mathfrak{i}^{\alpha}$, and $y = \pm b = a\sqrt{\mathfrak{i}}^{\beta+4\delta}$ for some $\alpha, \delta \in \mathbb{N}$. It follows that $\{a, b, x, y\}$ satisfies (ii), a contradiction.

So $(\frac{b}{a})^8 \neq 1$, and we can apply reduction (9.4) of Lemma 9.28. By the reduction (9.4), we have

$\#\mathrm{CSP}(g_{1_f}, g_{2_f}) \leqslant_T \text{Pl-Holant}(\neq_2|\, f)$. Moreover, since $\{a, b, x, y\}$ does not belong to case (i) or case (ii), we have $\{g_{1_f}, g_{2_f}\} \nsubseteq \mathscr{P}$ or $\mathscr{A}$. By Theorem 9.19, $\#\mathrm{CSP}(g_{1_f}, g_{2_f})$ is #P-hard. Therefore, we have $\text{Pl-Holant}(\neq_2|\, f)$ is #P-hard. □

Corollary 9.31. *Let f be a 4-ary signature of the form (9.2), where $(a, x) \neq (0, 0)$ and $(b, y) \neq (0, 0)$. If $|ax| \neq |by|$ then $\text{Pl-Holant}(\neq_2|\, f)$ is #P-hard.*

9.5 Case III: $\mathsf{N} = 2$ with No Zero Pair or $\mathsf{N} = 1$ with Zero in an Outer Pair

If there are exactly two zeros $\mathsf{N} = 2$ with no zero pair, then the two zeros are in different pairs, at least one of them must be in an outer pair. So in Case III there is a zero in an outer pair regardless $\mathsf{N} = 1$ or $\mathsf{N} = 2$. By rotational symmetry, we may assume $a = 0$, and we prove this case in Theorem 9.33. We first give the following lemma.

Lemma 9.32. *Let f be a 4-ary signature with the signature matrix $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $\det M_{\mathrm{In}}(f) = by - cz \neq 0$. Let g be a 4-ary signature with the signature matrix $M(g) = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. Then for any signature set $\mathcal{F}$ containing f, we have*

$$\text{Pl-Holant}(\neq_2|\, \mathcal{F} \cup \{g\}) \leqslant_T \text{Pl-Holant}(\neq_2|\, \mathcal{F}).$$

Proof. We construct a series of gadgets f_s by a chain of s copies of f linked by double Disequality N. f_s has the signature matrix

$$M(f_s) = M(f)(N_2 M(f))^{s-1} = N(N_2 M(f))^s = N \begin{bmatrix} 0 & \mathbf{0} & 0 \\ \mathbf{0} & \begin{bmatrix} z & y \\ b & c \end{bmatrix}^s & \mathbf{0} \\ 0 & \mathbf{0} & 0 \end{bmatrix}.$$

The inner matrix of $N_2 M(f)$ is $N_{\mathrm{In}} M_{\mathrm{In}}(f) = \left[\begin{smallmatrix} z & y \\ b & c \end{smallmatrix}\right]$. Suppose its spectral decomposition is $Q^{-1} \Lambda Q$, where $\Lambda = \left[\begin{smallmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{smallmatrix}\right]$ is the Jordan Canonical Form. Note that $\lambda_1 \lambda_2 = \det \Lambda = \det(N_{\mathrm{In}} M_{\mathrm{In}}(f)) \neq 0$.

We have $M(f_s) = NP^{-1}\Lambda_s P$, where

$$P = \begin{bmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & Q & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{bmatrix} \quad \text{and} \quad \Lambda_s = \begin{bmatrix} 0 & \mathbf{0} & 0 \\ \mathbf{0} & \begin{bmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{bmatrix}^s & \mathbf{0} \\ 0 & \mathbf{0} & 0 \end{bmatrix}.$$

1. Suppose $\mu = 0$, and $\frac{\lambda_2}{\lambda_1}$ is a root of unity, with $(\frac{\lambda_2}{\lambda_1})^n = 1$. Then $\Lambda_n = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & \lambda_1^n & 0 & 0 \\ 0 & 0 & \lambda_2^n & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & \lambda_1^n & 0 & 0 \\ 0 & 0 & \lambda_1^n & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$, and $M(f_n) = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1^n & 0 \\ 0 & \lambda_1^n & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right] = \lambda_1^n \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. After normalization, we can realize the signature g.

2. Suppose $\mu = 0$, and $\frac{\lambda_2}{\lambda_1}$ is not a root of unity. The matrix $\Lambda_s = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & \lambda_1^s & 0 & 0 \\ 0 & 0 & \lambda_2^s & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$ has a good form for interpolation. Suppose g appears m times in an instance Ω of Pl-Holant($\neq_2|\ \mathcal{F} \cup \{g\}$). Replace each appearance of g by a copy of the gadget f_s to get an instance Ω_s of Pl-Holant($\neq_2|\ \mathcal{F} \cup \{f_s\}$), which is also an instance of Pl-Holant($\neq_2|\ \mathcal{F}$). We can treat each of the m appearances of f_s as a new gadget composed of four functions in sequence N, P^{-1}, Λ_s and P, and denote this new instance by Ω'_s. We divide Ω'_s into two parts. One part consists of m signatures $\Lambda_s^{\otimes m}$. Here $\Lambda_s^{\otimes m}$ is expressed as a column vector. The other part is the rest of Ω'_s and its signature is represented by A which is a tensor expressed as a row vector. Then the Holant value of Ω'_s is the dot product $\langle A, \Lambda_s^{\otimes m}\rangle$, which is a summation over $4m$ bits. That is, the value of the $4m$ edges connecting the two parts. We can stratify all $0, 1$ assignments of these $4m$ bits having a nonzero evaluation of a term in Pl-Holant$_{\Omega'_s}$ into the following categories:

   - There are i many copies of Λ_s receiving inputs 0110;
   - There are j many copies of Λ_s receiving inputs 1001;

   where $i + j = m$.

   For any assignment in the category with parameter (i, j), the evaluation of $\Lambda_s^{\otimes m}$ is clearly $\lambda_1^{si}\lambda_2^{sj} = \lambda_1^{sm}\left(\frac{\lambda_2}{\lambda_1}\right)^{sj}$. Let a_{ij} be the summation of values of the part A over all assignments in the category (i, j). Note that a_{ij} is independent from the value of s since we view the gadget

Λ_s as a block. Since $i+j=m$, we can denote a_{ij} by a_j. Then we rewrite the dot product summation and get

$$\text{Pl-Holant}_{\Omega_s} = \text{Pl-Holant}_{\Omega'_s} = \langle A, \Lambda_s^{\otimes m} \rangle = \lambda_1^{sm} \sum_{0 \leqslant j \leqslant m} a_j \left(\frac{\lambda_2}{\lambda_1}\right)^{sj}.$$

Note that $M(g) = NP^{-1}(N_2M(g))P$, where $N_2M(g) = \left[\begin{smallmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&0 \end{smallmatrix}\right]$. Similarly, divide Ω into two parts. Under this stratification, we have

$$\text{Pl-Holant}_{\Omega} = \langle A, (N_2M(g))^{\otimes m} \rangle = \sum_{0 \leqslant j \leqslant m} a_j.$$

Since $\frac{\lambda_2}{\lambda_1}$ is not a root of unity, the Vandermonde coefficient matrix

$$\begin{bmatrix} \rho^0 & \rho^1 & \cdots & \rho^m \\ \rho^0 & \rho^2 & \cdots & \rho^{2m} \\ \vdots & \vdots & \vdots & \vdots \\ \rho^0 & \rho^{m+1} & \cdots & \rho^{(m+1)m} \end{bmatrix},$$

has full rank, where $\rho = \frac{\lambda_2}{\lambda_1}$. Hence, by oracle querying the values of Pl-Holant$_{\Omega_s}$, we can solve for a_j, and thus obtain the value of Pl-Holant$_\Omega$ in polynomial time.

3. Suppose $\mu = 1$, and $\lambda_1 = \lambda_2$ denoted by λ. Then $\Lambda_s = \left[\begin{smallmatrix} 0&0&0&0\\ 0&\lambda^s&s\lambda^{s-1}&0\\ 0&0&\lambda^s&0\\ 0&0&0&0 \end{smallmatrix}\right]$. We use this form to give a polynomial interpolation. As in the case above, we can stratify the assignments of $\Lambda_s^{\otimes m}$ of these $4m$ bits having a nonzero evaluation of a term in Pl-Holant$_{\Omega'_s}$ into the following categories:

   - There are i many copies of Λ_s receiving inputs 0110 or 1001;
   - There are j many copies of Λ_s receiving inputs 0101;

   where $i+j=m$.

   For any assignment in the category with parameter (i,j), the evaluation of $\Lambda_s^{\otimes m}$ is clearly $\lambda^{si}(s\lambda^{s-1})^j = \lambda^{sm}(\frac{s}{\lambda})^j$. Let a_{ij} be the summation of values of the part A over all assignments in the category (i,j). a_{ij} is independent from s. Since $i+j=m$, we can denote a_{ij} by a_j.

Then, we rewrite the dot product summation and get

$$\text{Pl-Holant}_{\Omega_s} = \text{Pl-Holant}_{\Omega_s'} = \langle A, \Lambda_s^{\otimes m} \rangle = \lambda^{sm} \sum_{0 \leqslant j \leqslant m} a_j \left(\frac{s}{\lambda} \right)^j,$$

for $s \geq 1$. We consider this as a linear system for $1 \leq s \leq m+1$. Similarly, divide Ω into two parts. Under this stratification, we have

$$\text{Pl-Holant}_{\Omega} = \langle A, (N_2 M(g))^{\otimes m} \rangle = a_0.$$

The Vandermonde coefficient matrix

$$\begin{bmatrix} \rho_1^0 & \rho_1^1 & \cdots & \rho_1^m \\ \rho_2^0 & \rho_2^1 & \cdots & \rho_2^m \\ \vdots & \vdots & \vdots & \vdots \\ \rho_{m+1}^0 & \rho_{m+1}^1 & \cdots & \rho_m \end{bmatrix},$$

has full rank, where $\rho_s = s/\lambda$ are all distinct. Hence, we can solve a_0 in polynomial time and it is the value of $\text{Pl-Holant}_{\Omega}$.

Therefore, we have Pl-Holant($\neq_2 \mid \mathcal{F} \cup \{g\}) \leqslant_T$ Pl-Holant($\neq_2 \mid \mathcal{F}$). □

Theorem 9.33 gives a classification for Case III.

Theorem 9.33. *Let f be a 4-ary signature with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix},$$

where $x \neq 0$ and there is at most one number in $\{b, c, y, z\}$ that is 0. Then Pl-Holant($\neq_2 \mid f$) *is #P-hard unless $f \in \mathscr{M}$, in which case the problem is tractable.*

Proof. Tractability follows from Theorem 9.9.

Suppose $f \notin \mathscr{M}$. By Lemma 9.7, $\det M_{\text{In}}(f) \neq \det M_{\text{Out}}(f) = 0$, that is $\det \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right] = by - cz \neq 0$. Note that $M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$, $M_{x_3x_4,x_2x_1}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & x \\ 0 & y & c & 0 \\ 0 & z & b & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$, and $M_{x_2x_3,x_1x_4}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & y \\ 0 & 0 & z & 0 \\ 0 & c & x & 0 \\ b & 0 & 0 & 0 \end{smallmatrix}\right]$.

Connect variables x_4, x_3 of a copy of signature f with variables x_3, x_4 of another copy of signature f both using $(\neq_2)$. We get a signature f_1 with the signature matrix

$$M(f_1) = M_{x_1x_2,x_4x_3}(f)N_2M_{x_3x_4,x_2x_1}(f) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & b_1 & c_1 & 0 \\ 0 & z_1 & y_1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

where $\left[\begin{smallmatrix} b_1 & c_1 \\ z_1 & y_1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} z & b \\ y & c \end{smallmatrix}\right]$. This f_1 has the form in Lemma 9.32. Here, $\det \left[\begin{smallmatrix} b_1 & c_1 \\ z_1 & y_1 \end{smallmatrix}\right] = -(by - cz)^2 \neq 0$. By Lemma 9.32, we have

$$\text{Pl-Holant}(\neq_2 \mid f, g) \leqslant_T \text{Pl-Holant}(\neq_2 \mid f, f_1),$$

where g has the signature matrix $M(g) = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$.

- If $bcyz \neq 0$, connect variables x_1, x_4 of signature f with variables x_1, x_2 of signature g both using $(\neq_2)$. We get a signature f_2 with the signature matrix

  $$M(f_2) = M_{x_2x_3,x_1x_4}(f)N_2M_{x_1x_2,x_4x_3}(g) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & c & x & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

- Otherwise, connect variables x_4, x_3 of signature f with variables x_1, x_2 of signature g both using $(\neq_2)$. We get a signature f_2 with the signature matrix

  $$M(f_2) = M_{x_1x_2,x_4x_3}(f)N_2M_{x_1x_2,x_4x_3}(g) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

  and there is exactly one entry in $\{b, c, y, z\}$ that is zero.

In both cases, the support of f_2 has size 3, which means $f_2 \notin \mathscr{P}, \mathscr{A}$ or $\widehat{\mathscr{M}}$. By Theorem 9.24, Pl-Holant($\neq_2$| f_2) is #P-hard. Since

$$\text{Pl-Holant}(\neq_2|\, f_2) \leqslant_T \text{Pl-Holant}(\neq_2|\, f, g) \leqslant_T \text{Pl-Holant}(\neq_2|\, f, f_1) \leqslant_T \text{Pl-Holant}(\neq_2|\, f),$$

we have Pl-Holant($\neq_2$| f) is #P-hard. □

9.6 Case IV: $\mathsf{N} = 1$ with Zero in the Inner Pair or $\mathsf{N} = 0$

By rotational symmetry, *if* there is one zero in the inner pair, we may assume it is $c = 0$, and $abxyz \neq 0$. We first consider the case that $x = \epsilon a, y = \epsilon b$ and $z = \epsilon c$, where $\epsilon = \pm 1$.

Lemma 9.34. *Let f be a 4-ary signature with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & \epsilon c & \epsilon b & 0 \\ \epsilon a & 0 & 0 & 0 \end{bmatrix}, \qquad \textit{where } \epsilon = \pm 1 \textit{ and } abc \neq 0.$$

Then Pl-Holant($\neq_2$| f) *is #P-hard if $f \notin \mathscr{M}$.*

Proof. If $\epsilon = -1$ we first transform the case to $\epsilon = 1$ as follows. Connecting the variable x_4 with x_3 of f using ($\neq_2$) we get a binary signature g_1, where

$$g_1 = M_{x_1x_2,x_4x_3}(f)(0, 1, 1, 0)^T = (0, b + c, -(b + c), 0)^T.$$

Also connecting the variable x_1 with x_2 of f using ($\neq_2$) we get a binary signature g_2, where

$$g_2 = ((0, 1, 1, 0)M_{x_1x_2,x_4x_3}(f))^T = (0, b - c, -(b - c), 0)^T.$$

Since $bc \neq 0$, $b + c$ and $b - c$ cannot be both zero. Without loss of generality, suppose $b + c \neq 0$. By normalization, we have $g_1 = (0, 1, -1, 0)^T$. Then, modifying $x_1 = 1$ of f with -1 scaling we get a signature with the signature matrix $\left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & c & b & 0 \\ a & 0 & 0 & 0 \end{smallmatrix}\right]$. Therefore, it suffices to show #P-hardness for the case $\epsilon = 1$.

Since $f \notin \mathscr{M}$, by Lemma 9.7, $c^2 - b^2 \neq a^2$. We prove #P-hardness in the following three Cases depending on the values of a, b and c.

Case 1: Either $c^2 - b^2 \neq 0$ and $|c+b| \neq |c-b|$, or $c^2 - a^2 \neq 0$ and $|c+a| \neq |c-a|$. By rotational symmetry, we may assume $c^2 - b^2 \neq 0$ and $|c+b| \neq |c-b|$. We may normalize $a = 1$ and assume $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & b & c & 0 \\ 0 & c & b & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $c^2 - b^2 \neq 0$ or 1.

We construct a series of gadgets f_s by a chain of s copies of f linked by double Disequality N. f_s has the signature matrix

$$M(f_s) = M(f)(N_2 M(f))^{s-1} = N(N_2 M(f))^s = N \begin{bmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \begin{bmatrix} c & b \\ b & c \end{bmatrix}^s & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{bmatrix}.$$

We diagonalize $\left[\begin{smallmatrix} c & b \\ b & c \end{smallmatrix}\right]^s$ using $H = \frac{1}{\sqrt{2}} \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ (note that $H^{-1} = H$), and get $M(f_s) = N P \Lambda_s P$, where

$$P = \begin{bmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & H & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{bmatrix}, \quad \text{and} \quad \Lambda_s = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & (c+b)^s & 0 & 0 \\ 0 & 0 & (c-b)^s & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The signature matrix Λ_s has a good form for polynomial interpolation. In the following, we will reduce Pl-Holant($\neq_2|\ \hat{f}$) to Pl-Holant($\neq_2|\ f$), for suitably chosen $M(\hat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & \hat{b} & \hat{c} & 0 \\ 0 & \hat{c} & \hat{b} & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$, and use that to prove that Pl-Holant($\neq_2|\ f$) is #P-hard.

Suppose $\hat{f}$ appears m times in an instance $\hat{\Omega}$ of Pl-Holant($\neq_2|\ \hat{f}$). We replace each appearance of $\hat{f}$ by a copy of the gadget f_s to get an instance Ω_s of Pl-Holant($\neq_2|\ f$). We can treat each of the m appearances of f_s as a new gadget composed of four functions in sequence N, P, Λ_s and P, and denote this new instance by Ω'_s. We divide Ω'_s into two parts. One part consists of m occurrences of Λ_s, which is $\Lambda_s^{\otimes m}$, and is written as a column vector of dimension 2^{4m}. The other part is the rest of Ω'_s and its signature is expressed by a tensor A, written as a row vector of dimension 2^{4m}. Then the Holant value of Ω'_s is the dot product $\langle A, \Lambda_s^{\otimes m} \rangle$, which is a summation over $4m$ bits, i.e., the values of the $4m$ edges connecting the two parts. We can stratify all $0, 1$ assignments of these

$4m$ bits having a nonzero evaluation of a term in Pl-Holant$_{\Omega'_s}$ into the following categories:

- There are i many copies of Λ_s receiving inputs 0000 or 1111;
- There are j many copies of Λ_s receiving inputs 0110;
- There are k many copies of Λ_s receiving inputs 1001;

where $i + j + k = m$.

For any assignment in the category with parameter (i, j, k), the evaluation of $\Lambda_s^{\otimes m}$ is clearly $(c+b)^{sj}(c-b)^{sk}$. Let a_{ijk} be the summation of values of the part A over all assignments in the category (i, j, k). Note that a_{ijk} is independent of the value of s. Since $i + j + k = m$, we can denote a_{ijk} by a_{jk}. Then we rewrite the dot product summation and get

$$\text{Pl-Holant}_{\Omega_s} = \text{Pl-Holant}_{\Omega'_s} = \langle A, \Lambda_s^{\otimes m}\rangle = \sum_{0 \leqslant j+k \leqslant m} a_{jk}(c+b)^{sj}(c-b)^{sk}.$$

Under this stratification, correspondingly we can define $\hat{\Omega}'$ and $\hat{\Lambda}$ from $\hat{\Omega}$. Then we have

$$\text{Pl-Holant}_{\hat{\Omega}} = \text{Pl-Holant}_{\hat{\Omega}'} = \langle A, \hat{\Lambda}^{\otimes m}\rangle = \sum_{0 \leqslant j+k \leqslant m} a_{jk}(\hat{c}+\hat{b})^{j}(\hat{c}-\hat{b})^{k},$$

where the same set of values a_{jk} appear. Let $\phi = \hat{c} + \hat{b}$ and $\psi = \hat{c} - \hat{b}$. If we can obtain the value of $p(\phi, \psi) = \sum\limits_{0 \leqslant j+k \leqslant m} a_{jk}\phi^j\psi^k$ from oracle queries to Pl-Holant$_{\Omega_s}$ (for $s \geq 1$) in polynomial time, then we will have proved

$$\text{Pl-Holant}(\neq_2 | \hat{f}) \leqslant_T \text{Pl-Holant}(\neq_2 | f).$$

Let $\alpha = c + b$ and $\beta = c - b$. Since $c^2 - b^2 \neq 0$ or 1, we have $\alpha \neq 0$, $\beta \neq 0$ and $\alpha\beta \neq 1$. Also, by assumption $|c + b| \neq |c - b|$, we have $|\alpha| \neq |\beta|$. Define $L = \{(j, k) \in \mathbb{Z}^2 \mid \alpha^j\beta^k = 1\}$. This is a sublattice of $\mathbb{Z}^2$. Every lattice has a basis. There are 3 cases depending on the rank of L.

- $L = \{(0, 0)\}$. All $\alpha^j\beta^k$ are distinct. It is an interpolation reduction in full power. That is, we can interpolate $p(\phi, \psi)$ for any ϕ and ψ in polynomial time. Let $\phi = 4$ and $\psi = 0$, that is $\hat{b} = 2$ and $\hat{c} = 2$, and hence $M(\hat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. That is, $\hat{f}$ is non-singular redundant. By Theorem 9.16, Pl-Holant$(\neq_2 | \hat{f})$ is #P-hard, and hence Pl-Holant$(\neq_2 | f)$ is #P-hard.

- L contains two independent vectors (j_1, k_1) and (j_2, k_2) over $\mathbb{Q}$. Then the nonzero vectors $j_2(j_1, k_1) - j_1(j_2, k_2) = (0, j_2k_1 - j_1k_2)$ and $k_2(j_1, k_1) - k_1(j_2, k_2) = (k_2j_1 - k_1j_2, 0)$ are in L. Hence, both α and β are roots of unity. This implies that $|\alpha| = |\beta| = 1$, a contradiction.

- $L = \{(ns, nt) \mid n \in \mathbb{Z}\}$, where $s, t \in \mathbb{Z}$ and $(s, t) \neq (0, 0)$. Without loss of generality, we may assume $t \geqslant 0$, and $s > 0$ when $t = 0$. Also, we have $s + t \neq 0$, otherwise $|\alpha| = |\beta|$, a contradiction. By Lemma 9.6, for any numbers ϕ and ψ satisfying $\phi^s\psi^t = 1$, we can obtain $p(\phi, \psi)$ in polynomial time. Since $\phi = \hat{c} + \hat{b}$ and $\psi = \hat{c} - \hat{b}$, we have $\hat{b} = \frac{\phi-\psi}{2}$ and $\hat{c} = \frac{\phi+\psi}{2}$. That is $M(\hat{f}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{\phi-\psi}{2} & \frac{\phi+\psi}{2} & 0 \\ 0 & \frac{\phi+\psi}{2} & \frac{\phi-\psi}{2} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. There are three cases depending on the values of s and t.

  - $s \geqslant 0$ and $s + t \geqslant 2$. Consider the function $q(x) = (2 - x)^s x^t - 1$. Since $s \geqslant 0$ and $t \geqslant 0$, $q(x)$ is a polynomial. Clearly, 1 is a root and 0 is not a root. If $q(x)$ has no other roots, then for some constant $\lambda \neq 0$,

    $$q(x) = \lambda(x - 1)^{s+t} = (-1)^{s+t}\lambda((2 - x) - 1)^{s+t}.$$

    (In fact by comparing leading coefficients, $\lambda = (-1)^s$.) Notice that $x^t | q(x) + 1$, while $x^t \nmid \lambda(x - 1)^{s+t} + 1$ for $t \geqslant 2$. Also, notice that $(2 - x)^s | q(x) + 1$, while $(2 - x)^s \nmid (-1)^{s+t}\lambda((2-x)-1)^{s+t}$ for $s \geqslant 2$. Hence, $t = s = 1$, which means $\alpha\beta = 1$. Contradiction. Therefore, $q(x)$ has a root x_0, with $x_0 \neq 1$ or 0. Let $\psi = x_0$ and $\phi = 2 - x_0$. Then $\phi^s\psi^t = 1$ and $M(\hat{f}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1-x_0 & 1 & 0 \\ 0 & 1 & 1-x_0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Note that $M_{x_2x_3,x_1x_4}(\hat{f}) = \begin{bmatrix} 0 & 0 & 0 & 1-x_0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1-x_0 & 0 & 0 & 0 \end{bmatrix}$. Since $1 - x_0 \neq 0$, $\hat{f}$ is non-singular redundant. By Theorem 9.16, Pl-Holant$(\neq_2 | \hat{f})$ is #P-hard and hence Pl-Holant $(\neq_2 | f)$ is #P-hard.

  - $s < 0$ and $t > 0$. (Note that $s < 0$ implies $t > 0$.) Consider the function $q(x) = x^t - (2 - x)^{-s}$. Since $t > 0$ and $-s > 0$, it is a polynomial. Clearly, 1 is a root, but neither 0 nor 2 is a root. Since $t + s \neq 0$, the highest order term of $q(x)$ is either x^t or $-(-x)^{-s}$, which means the coefficient of the highest order term is ± 1. While the constant term of $q(x)$ is $-2^{-s} \neq \pm 1$. Hence, $q(x)$ cannot be of the form $\lambda(x - 1)^{\max(t,-s)}$ for some constant $\lambda \neq 0$. Moreover, since $t + s \neq 0$, $\max(t, -s) \geqslant 2$, which means $q(x)$ has a root x_0, where $x_0 \neq 0, 1, 2$. Dividing by the nonzero term $(2 - x_0)^{-s}$ we have

$(2-x_0)^s x_0^t = 1$. Now we let $\psi = x_0$ and $\phi = 2-x_0$, and we have Pl-Holant $(\neq_2|\, f)$ is #P-hard by the same proof as above.

- $s \geqslant 0$ and $s+t=1$. In this case, we have $(s,t)=(0,1)$ or $(1,0)$ since $t \geqslant 0$.
  - $(s,t)=(1,0)$. Let $\phi = 1$ and $\psi = \frac{1}{2}$. Then we have $\phi^1\psi^0 = 1$ and $M(\hat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{1}{4} & \frac{3}{4} & 0 \\ 0 & \frac{3}{4} & \frac{1}{4} & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Let $M(f') = 4M_{x_2x_3,x_1x_4}(\hat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 4 & 3 & 0 \\ 0 & 3 & 4 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Clearly, Pl-Holant$(\neq_2|\, f') \leqslant_T$ Pl-Holant $(\neq_2|\, f)$. For $M(f')$, correspondingly we define $\alpha' = 3+4 = 7$ and $\beta' = 3-4 = -1$. Obviously, $\alpha' \neq 0$, $\beta' \neq 0$, $\alpha'\beta' \neq 1$, and $|\alpha'| \neq |\beta'|$. Let $L' = \{(j,k) \in \mathbb{Z}^2 \mid \alpha'^j\beta'^k = 1\}$. Then we have $L' = \{(ns', nt') \mid n \in \mathbb{Z}\}$, where $s' = 0$ and $t' = 2$. Therefore, $s' \geqslant 0$ and $s'+t' \geqslant 2$. As we have showed above, we have Pl-Holant $(\neq_2|\, f')$ is #P-hard, and hence Pl-Holant $(\neq_2|\, f)$ is #P-hard.
  - $(s,t)=(0,1)$. Let $\phi = 3$ and $\psi = 1$. Then we have $\phi^0\psi^1 = 1$ and $M(\hat{f}) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. By Theorem 9.17, Pl-Holant$(\neq_2|\, \hat{f})$ is #P-hard, and hence Pl-Holant $(\neq_2|\, f)$ is #P-hard.

Case 2: If $c^2-b^2 \neq 0$ and $|c+b| = |c-b|$, or $c^2-a^2 \neq 0$ and $|c+a| = |c-a|$. By rotational symmetry, we may assume $c^2-b^2 \neq 0$ and $|c+b| = |c-b|$. Normalizing f by assuming $c=1$, we have $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & 1 & 0 \\ 0 & 1 & b & 0 \\ a & 0 & 0 & 0 \end{smallmatrix}\right]$, where $1^2-b^2 \neq 0$ and $1^2-b^2 \neq a^2$ due to $f \notin \mathscr{M}$. Since $|1+b| = |1-b|$, b is a pure imaginary number (as $b \neq 0$).

Connect variables x_4, x_3 of a copy of signature f with variables x_1, x_2 of another copy of signature f both using $(\neq_2)$. We get a signature f_1 with the signature matrix

$$M(f_1) = M_{x_1x_2,x_4x_3}(f)N_2M_{x_1x_2,x_4x_3}(f) = \begin{bmatrix} 0 & 0 & 0 & a^2 \\ 0 & 2b & b^2+1 & 0 \\ 0 & b^2+1 & 2b & 0 \\ a^2 & 0 & 0 & 0 \end{bmatrix}.$$

a. If $c^2-a^2=0$, that is $a^2=1$, and then $M(f_1) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 2b & b^2+1 & 0 \\ 0 & b^2+1 & 2b & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Since $b^2 < 0$, we have $(b^2+1)^2-(2b)^2 = (b^2-1)^2 > 1 = (a^2)^2$, which means $f_1 \notin \mathscr{M}$.

- If $b^2 = -1$, then $M(f_1) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \pm 2\mathrm{i} & 0 & 0 \\ 0 & 0 & \pm 2\mathrm{i} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. By Corollary 9.31, Pl-Holant($\neq_2|\ f_1$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.
- If $b^2 = -2$, then $M(f_1) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \pm 2\sqrt{2}\mathrm{i} & -1 & 0 \\ 0 & -1 & \pm 2\sqrt{2}\mathrm{i} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Connect two copies of f_1, and we have a signature f_2 with the signature matrix

  $$M(f_2) = M_{x_1x_2,x_4x_3}(f_1)N_2M_{x_1x_2,x_4x_3}(f_1) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \mp 4\sqrt{2}\mathrm{i} & -7 & 0 \\ 0 & -7 & \mp 4\sqrt{2}\mathrm{i} & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

  It is easy to check that $f_2 \notin \mathscr{M}$, by Lemma 9.7. Then, f_2 belongs to Case 1. Therefore, Pl-Holant($\neq_2|\ f_2$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.
- If $b^2 \neq -1$ or -2, then $b^2+1 \neq \pm 1$ due to $b \neq 0$, hence $1^2 - (b^2+1)^2 \neq 0$. Also, since b^2+1 is a real number and $b^2+1 \neq 0$, we have $|(b^2+1)+1| \neq |(b^2+1)-1|$. Then f_1, which is not in $\mathscr{M}$ as shown above, has a signature matrix of the form $\begin{bmatrix} 0 & 0 & 0 & a_1 \\ 0 & b_1 & c_1 & 0 \\ 0 & c_1 & b_1 & 0 \\ a_1 & 0 & 0 & 0 \end{bmatrix}$, where $a_1 = a^2 = 1$, $b_1 = 2b$, and $c_1 = b^2+1$, and $a_1b_1c_1 \neq 0$, $c_1^2 - a_1^2 \neq 0$ and $|c_1+a_1| \neq |c_1-a_1|$. That is, f_1 belongs to Case 1. Therefore, Pl-Holant($\neq_2|\ f_1$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.

b. If $c^2 - a^2 \neq 0$ and $|c+a| = |c-a|$, i.e., $|1+a| = |1-a|$, then $a \neq 0$ is also a pure imaginary number. Connect variables x_1, x_4 of a copy of signature f with variables x_2, x_3 of another copy of signature f. We get a signature f_3 with the signature matrix

$$M(f_3) = M_{x_2x_3,x_1x_4}(f)N_2M_{x_2x_3,x_1x_4}(f) = \begin{bmatrix} 0 & 0 & 0 & b^2 \\ 0 & 2a & a^2+1 & 0 \\ 0 & a^2+1 & 2a & 0 \\ b^2 & 0 & 0 & 0 \end{bmatrix}.$$

Note that $f_3 \in \mathscr{M}$ implies $(a^2-1)^2 = (b^2)^2$. Since $f \notin \mathscr{M}$, $1 - a^2 \neq b^2$. Hence, $f_3 \in \mathscr{M}$ implies $a^2 - 1 = b^2$. Similarly, $f_1 \in \mathscr{M}$ implies $b^2 - 1 = a^2$. Clearly, f_1 and f_3 cannot both be in $\mathscr{M}$. Without loss of generality, we may assume $f_3 \notin \mathscr{M}$.

- If $a^2 \neq -1$, then there are two subcases.
  - $(a^2+1)^2-(b^2)^2=0$. Since a is a pure imaginary number, $|a^2+1+2a|=|a+1|^2=|a-1|^2=|a^2+1-2a|$. Then f_3 has the signature matrix of the form $\begin{bmatrix} 0 & 0 & 0 & a_3 \\ 0 & b_3 & c_3 & 0 \\ 0 & c_3 & b_3 & 0 \\ a_3 & 0 & 0 & 0 \end{bmatrix}$, where $a_3b_3c_3 \neq 0$, $c_3^2-b_3^2=(a^2-1)^2 \neq 0$ since a is pure imaginary, $|c_3+b_3|=|c_3-b_3|$ and $c_3^2-a_3^2=0$. That is, f_3 belongs to Case 2.a. Therefore, Pl-Holant($\neq_2|\ f_3$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.
  - $(a^2+1)^2-(b^2)^2 \neq 0$. Since a^2+1 and b^2 are both nonzero real numbers due to a and b are both pure imaginary numbers, we have $|a^2+1+b^2| \neq |a^2+1-b^2|$. Then f_3 has the signature matrix of the form $\begin{bmatrix} 0 & 0 & 0 & a_3 \\ 0 & b_3 & c_3 & 0 \\ 0 & c_3 & b_3 & 0 \\ a_3 & 0 & 0 & 0 \end{bmatrix}$, where $a_3b_3c_3 \neq 0$, $c_3^2-a_3^2 \neq 0$ and $|c_3+a_3| \neq |c_3-a_3|$. That is, f_3 belongs to Case 1. Therefore, Pl-Holant($\neq_2|\ f_3$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.
- If $a^2=-1$ and $b^2 \neq -2$, then $M(f_3)=\begin{bmatrix} 0 & 0 & 0 & b^2 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2a & 0 \\ b^2 & 0 & 0 & 0 \end{bmatrix}$, where $|2a|=2 \neq |b^2|$. By Corollary 9.31, Pl-Holant($\neq_2|\ f_3$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.
- If $a^2=-1$ and $b^2=-2$, then $M(f_1)=\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & \pm 2\sqrt{2}\mathrm{i} & -1 & 0 \\ 0 & -1 & \pm 2\sqrt{2}\mathrm{i} & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$. Note that $M_{x_2x_3,x_1x_4}(f_1)=\begin{bmatrix} 0 & 0 & 0 & \pm 2\sqrt{2}\mathrm{i} \\ 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ \pm 2\sqrt{2}\mathrm{i} & 0 & 0 & 0 \end{bmatrix}$, which means f_1 is non-singular redundant. Therefore, we have Pl-Holant($\neq_2|\ f_1$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.

c. If $c^2-a^2 \neq 0$ and $|c+a| \neq |c-a|$. This is Case 1. Done.

Case 3: $c^2-b^2=0$ and $c^2-a^2=0$. If $c=b$ or $c=a$, then f is non-singular redundant, and hence Pl-Holant($\neq_2|\ f$) is #P-hard. Otherwise, $a=b=-c$. By normalization, we have $M(f)=\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$, and then $M(f_1)=\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & -2 & 2 & 0 \\ 0 & 2 & -2 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Notice that $2^2-1^2 \neq 0$ and $|2+1| \neq |2-1|$. That is, f_1 belongs to Case 1. Therefore, Pl-Holant($\neq_2|\ f_1$) is #P-hard, and hence Pl-Holant($\neq_2|\ f$) is #P-hard.

Case 1 to Case 3 cover all cases for (a,b,c): Suppose (a,b,c) does not satisfy Case 3. Then either $c^2-b^2 \neq 0$ or $c^2-a^2 \neq 0$. If $c^2-b^2 \neq 0$, then either $|c+b| \neq |c-b|$ (Case 1) or $|c+b|=|c-b|$ (Case 2). Similarly if $c^2-a^2 \neq 0$ it is either Case 1 or Case 2. This completes the proof of the lemma. □

Lemma 9.35. *Let f be a 4-ary signature with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix}, \quad \textit{where} \quad abcxyz \neq 0.$$

If $by - cz = 0$ or $ax - cz = 0$, then Pl-Holant$(\neq_2|\ f)$ *is #P-hard.*

Proof. By rotational symmetry, we assume $by - cz = 0$. By normalization, we assume $b = 1$, and then $y = cz$. That is, $M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & 1 & c & 0 \\ 0 & z & cz & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$.

- If $1 + c \neq 0$. Connecting the variables x_4 with x_3 of f using $(\neq_2)$ we get a binary signature g_1, where

  $$g_1 = M_{x_1x_2,x_4x_3}(f)(0,1,1,0)^T = (0, 1 + c, (1 + c)z, 0)^T.$$

  Note that $g_1(x_1, x_2)$ can be normalized as $(0, z^{-1}, 1, 0)^T$. That is $g(x_2, x_1) = (0, 1, z^{-1}, 0)^T$. Modifying $x_1 = 1$ of f with z^{-1} scaling we get a signature f_1 with the signature matrix $\left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & 1 & c & 0 \\ 0 & 1 & c & 0 \\ x/z & 0 & 0 & 0 \end{smallmatrix}\right]$. Connecting the variable x_1 with x_2 of f_1 using $(\neq_2)$ we get a binary signature g_2, where

  $$g_2 = ((0, 1, 1, 0)M_{x_1x_2,x_4x_3}(f))^T = (0, 2, 2c, 0)^T,$$

  and $g_2(x_1, x_2)$ can be normalized to $g_2(x_2, x_1) = (0, 1, c^{-1}, 0)^T$. Modifying $x_4 = 1$ of f_1 with c^{-1} scaling we get a signature f_2 with the signature matrix $\left[\begin{smallmatrix} 0 & 0 & 0 & a/c \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ x/z & 0 & 0 & 0 \end{smallmatrix}\right]$. It is non-singular redundant. By Lemma 9.16, we have Pl-Holant$(\neq_2|\ f_2)$ is #P-hard, and hence Pl-Holant$(\neq_2|\ f)$ is #P-hard.

- If $1 + z \neq 0$, then connecting the variable x_1 with x_2 of f using $(\neq_2)$ we get a binary signature g'_1, where

  $$g'_1 = ((0, 1, 1, 0)M_{x_1x_2,x_4x_3})^T = (0, 1 + z, (1 + z)c, 0)^T.$$

  $g'_1(x_1, x_2)$ can be normalized to $(0, c^{-1}, 1, 0)^T$. By the same analysis as in the case $1 + c \neq 0$, we have Pl-Holant$(\neq_2|\ f)$ is #P-hard.

- Otherwise, $1 + c = 0$ and $1 + z = 0$, that is $c = z = -1$. Then $M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ x & 0 & 0 & 0 \end{smallmatrix}\right]$, and $M_{x_3x_4,x_2x_1}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & x \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ a & 0 & 0 & 0 \end{smallmatrix}\right]$. Connecting variables x_4, x_3 of a copy of signature f with variables x_3, x_4 of another copy of signature f, we get a signature f_3 with the signature matrix

$$M(f_3) = M_{x_1x_2,x_4x_3}(f)N_2M_{x_3x_4,x_2x_1}(f) = \begin{bmatrix} 0 & 0 & 0 & ax \\ 0 & -2 & 2 & 0 \\ 0 & 2 & -2 & 0 \\ ax & 0 & 0 & 0 \end{bmatrix},$$

Clearly, $ax \neq 0$ and so $f_3 \notin \mathscr{M}$ by Lemma 9.7. By Lemma 9.34, Pl-Holant $(\neq_2 |\, f_3)$ is #P-hard and hence Pl-Holant $(\neq_2 |\, f)$ is #P-hard. □

In the following Lemmas 9.36, 9.37, 9.40 and Corollaries 9.39, 9.41, let f be a 4-ary signature with the signature matrix

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix}, \tag{9.6}$$

where $abxyz \neq 0$, $\det \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right] = by - cz \neq 0$ and $\det \left[\begin{smallmatrix} a & z \\ c & x \end{smallmatrix}\right] = ax - cz \neq 0$. Moreover $f \notin \mathscr{M}$, that is $cz - by \neq ax$. These lemmas handle "generic" cases of this section and will culminate in Theorem 9.42, which is a classification for Case IV. It is here we will use Möbius transformations to handle interpolations where it is particularly difficult to get desired signatures of "infinite order".

Lemma 9.36. *Let $g = (0, 1, t, 0)^T$ be a binary signature, where $t \neq 0$ is not a root of unity. Then* Pl-Holant$(\neq_2 |\, f, g)$ *is #P-hard.*

Proof. Let $\mathcal{B} = \{g_1, g_2, g_3\}$ be a set of three binary signatures $g_i = (0, 1, t_i, 0)^T$, for some $t_i \in \mathbb{C}$. By Lemma 9.3, we have Pl-Holant $(\neq_2 |\, \{f\} \cup \mathcal{B}) \leqslant$ Pl-Holant $(\neq_2 |\, f, g)$. We will show that Pl-Holant $(\neq_2 |\, \{f\} \cup \mathcal{B})$ is #P-hard and it follows that Pl-Holant $(\neq_2 |\, f, g)$ is #P-hard.

Modifying $x_1 = 1$ of f with t_i $(i = 1, 2)$ scaling separately, we get two signatures f_{t_i} with the signature matrices $M(f_{t_i}) = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & t_iz & t_iy & 0 \\ t_ix & 0 & 0 & 0 \end{smallmatrix}\right]$. Note that

$$\det M_{\text{In}}(f_{t_i}) = t_i \det M_{\text{In}}(f) \quad \text{and} \quad \det M_{\text{Out}}(f_{t_i}) = t_i \det M_{\text{Out}}(f).$$

Connecting variables x_4, x_3 of f with variables x_1, x_2 of f_{t_1} both using $(\neq_2)$, we get a signature f_1

with the signature matrix

$$M(f_1) = \begin{bmatrix} 0 & 0 & 0 & a_1 \\ 0 & b_1 & c_1 & 0 \\ 0 & z_1 & y_1 & 0 \\ x_1 & 0 & 0 & 0 \end{bmatrix} = M(f)N_2M(f_{t_1}) = \begin{bmatrix} 0 & 0 & 0 & a^2 \\ 0 & t_1bz + bc & t_1by + c^2 & 0 \\ 0 & t_1z^2 + yb & t_1yz + yc & 0 \\ t_1x^2 & 0 & 0 & 0 \end{bmatrix}.$$

We first show that there is a $t_1 \neq 0$ such that $b_1y_1c_1z_1 \neq 0$ and $(b_1z)(y_1c) - (c_1b)(z_1y) \neq 0$. Consider the quadratic polynomial

$$p(t) = (tbz + bc)(tyz + yc)cz - (tby + c^2)(tz^2 + yb)by.$$

We have $p(t_1) = (b_1z)(y_1c) - (c_1b)(z_1y)$. Notice that the coefficient of the quadratic term in $p(t)$ is $byz^2(cz - by)$. It is not equal to zero since $byz^2 \neq 0$ and $cz - by \neq 0$. That is, $p(t)$ has degree 2, and hence it has at most two roots. Also we have the following three implications by the definitions of b_1, y_1, c_1, z_1: $b_1y_1 = 0 \Longrightarrow t_1 = -\frac{c}{z}$, $c_1 = 0 \Longrightarrow t_1 = -\frac{c^2}{by}$, and $z_1 = 0 \Longrightarrow t_1 = -\frac{yb}{z^2}$. Therefore we can choose such a t_1 that does not take these values $0, -\frac{c}{z}, -\frac{c^2}{by}$ and $-\frac{yb}{z^2}$, and t_1 is not a root of $p(t)$. Then, we have $t_1 \neq 0$, $b_1y_1c_1z_1 \neq 0$ and $(b_1z)(y_1c) - (c_1b)(z_1y) \neq 0$.

Connecting variables x_4, x_3 of f_1 with variables x_1, x_2 of f_{t_2} both using $(\neq_2)$, we get a signature f_2 with the signature matrix

$$M(f_2) = \begin{bmatrix} 0 & 0 & 0 & a_2 \\ 0 & b_2 & c_2 & 0 \\ 0 & z_2 & y_2 & 0 \\ x_2 & 0 & 0 & 0 \end{bmatrix} = M(f_1)N_2M(f_{t_2}) = \begin{bmatrix} 0 & 0 & 0 & a_1a \\ 0 & t_2b_1z + c_1b & t_2b_1y + c_1c & 0 \\ 0 & t_2z_1z + y_1b & t_2z_1y + y_1c & 0 \\ t_2x_1x & 0 & 0 & 0 \end{bmatrix}.$$

Since $b_1z \neq 0$ and $c_1b \neq 0$, we can let $t_2 = -\frac{c_1b}{b_1z}$ and $t_2 \neq 0$. Then $b_2 = t_2b_1z + c_1b = 0$. Since

$(b_1 z)(y_1 c) - (c_1 b)(z_1 y) \neq 0$, we have $y_2 = t_2 z_1 y + y_1 c \neq 0$. Notice that

$$\begin{aligned}
\det M_{\text{In}}(f_2) &= \det M_{\text{In}}(f_1) \cdot (-1) \cdot \det M_{\text{In}}(f_{t_2}) \\
&= \det M_{\text{In}}(f) \cdot (-1) \cdot \det M_{\text{In}}(f_{t_1}) \cdot (-1) \cdot \det M_{\text{In}}(f_{t_2}) \\
&= t_1 t_2 \det M_{\text{In}}(f)^3 \\
&\neq 0.
\end{aligned}$$

We have $\det M_{\text{In}}(f_2) = b_2 y_2 - c_2 z_2 = -c_2 z_2 \neq 0$. Similarly, we have $\det M_{\text{Out}}(f_2) = -a_2 x_2 = t_1 t_2 \det M_{\text{Out}}(f)^3 \neq 0$. Therefore, $M(f_2)$ is of the form $\left[\begin{smallmatrix} 0 & 0 & 0 & a_2 \\ 0 & 0 & c_2 & 0 \\ 0 & z_2 & y_2 & 0 \\ x_2 & 0 & 0 & 0 \end{smallmatrix}\right]$, where $a_2 x_2 y_2 c_2 z_2 \neq 0$. That is, f_2 is a signature in Case III. If $f_2 \notin \mathscr{M}$, then Pl-Holant $(\neq_2 | \, f_2)$ is #P-hard by Theorem 9.33, and hence Pl-Holant $(\neq_2 | \, \{f\} \cup \mathcal{B})$ is #P-hard.

Otherwise, $f_2 \in \mathscr{M}$, which means $\dfrac{\det M_{\text{In}}(f_2)}{\det M_{\text{Out}}(f_2)} = 1$. Thus $\dfrac{\det M_{\text{In}}(f)^3}{\det M_{\text{Out}}(f)^3} = 1$. Since $f \notin \mathscr{M}$, $\dfrac{\det M_{\text{In}}(f)}{\det M_{\text{Out}}(f)} \neq 1$, and hence $\dfrac{\det M_{\text{In}}(f)^7}{\det M_{\text{Out}}(f)^7} \neq 1$. Similar to the construction of f_1, we construct f_3. First, modify $x_1 = 1$ of f_1 with t_3 scaling. We get a signature f_{1t_3} with the signature matrix $M(f_{1t_3}) = \left[\begin{smallmatrix} 0 & 0 & 0 & a_1 \\ 0 & b_1 & c_1 & 0 \\ 0 & t_3 z_1 & t_3 y_1 & 0 \\ t_3 x_1 & 0 & 0 & 0 \end{smallmatrix}\right]$. Note that $\det M_{\text{In}}(f_{1t_3}) = t_3 \det M_{\text{In}}(f_1)$ and $\det M_{\text{Out}}(f_{1t_3}) = t_3 \det M_{\text{Out}}(f_1)$. Then connect variables x_4, x_3 of f_1 with variables x_1, x_2 of f_{1t_3} both using $(\neq_2)$. We get a signature f_3 with the signature matrix

$$M(f_3) = \begin{bmatrix} 0 & 0 & 0 & a_3 \\ 0 & b_3 & c_3 & 0 \\ 0 & z_3 & y_3 & 0 \\ x_3 & 0 & 0 & 0 \end{bmatrix} = M(f_1) N_2 M(f_{1t_3}) = \begin{bmatrix} 0 & 0 & 0 & a^2 \\ 0 & t_3 b_1 z_1 + b_1 c_1 & t_3 b_1 y_1 + c_1^2 & 0 \\ 0 & t_3 z_1^2 + y_1 b_1 & t_3 y_1 z_1 + y_1 c_1 & 0 \\ t_3 x_1^2 & 0 & 0 & 0 \end{bmatrix}.$$

Since $c_1 \neq 0$ and $z_1 \neq 0$, we can define $t_3 = -\frac{c_1}{z_1}$ and $t_3 \neq 0$. Then $b_3 = b_1(t_3 z_1 + c_1) = 0$ and

$y_3 = y_1(t_3 z_1 + c_1) = 0$. Notice that

$$\begin{aligned}
\det M_{\text{In}}(f_3) &= \det M_{\text{In}}(f_1) \cdot (-1) \cdot \det M_{\text{In}}(f_{1t_3}) \\
&= -\det M_{\text{In}}(f_1) \cdot t_3 \det M_{\text{In}}(f_1) \\
&= -t_3 \left[\det M_{\text{In}}(f) \cdot (-1) \cdot \det M_{\text{In}}(f_{t_1})\right]^2 \\
&= -t_3 t_1^2 \det M_{\text{In}}(f)^4 \\
&\neq 0
\end{aligned}$$

We have $\det M_{\text{In}}(f_3) = -c_3 z_3 \neq 0$ and similarly, $\det M_{\text{Out}}(f_3) = -a_3 x_3 = -t_3 t_1^2 \det M_{\text{Out}}(f)^4 \neq 0$. That is, $M(f_3)$ is of the form $\left[\begin{smallmatrix} 0 & 0 & 0 & a_3 \\ 0 & 0 & c_3 & 0 \\ 0 & z_3 & 0 & 0 \\ x_3 & 0 & 0 & 0 \end{smallmatrix}\right]$ where $a_3 x_3 c_3 z_3 \neq 0$.

Connect variables x_4, x_3 of f_2 with variables x_1, x_2 of f_3 both using $(\neq_2)$. We get a signature f_4 with the signature matrix

$$M(f_4) = \begin{bmatrix} 0 & 0 & 0 & a_4 \\ 0 & b_4 & c_4 & 0 \\ 0 & z_4 & y_4 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} = M(f_2) N_2 M(f_3) = \begin{bmatrix} 0 & 0 & 0 & a_2 a_3 \\ 0 & 0 & c_2 c_3 & 0 \\ 0 & z_2 z_3 & y_2 c_3 & 0 \\ x_2 x_3 & 0 & 0 & 0 \end{bmatrix}.$$

Clearly, f_4 is a signature in Case III. Also, notice that

$$\begin{aligned}
\det M_{\text{In}}(f_4) &= \det M_{\text{In}}(f_2) \cdot (-1) \cdot \det M_{\text{In}}(f_3) \\
&= t_1 t_2 \det M_{\text{In}}(f)^3 \cdot t_3 t_1^2 \det M_{\text{In}}(f)^4 \\
&= t_3 t_2 t_1^3 \det M_{\text{In}}(f)^7.
\end{aligned}$$

and

$$\det M_{\text{Out}}(f_4) = t_3 t_2 t_1^3 \det M_{\text{Out}}(f)^7.$$

We have

$$\frac{\det M_{\text{In}}(f_4)}{\det M_{\text{Out}}(f_4)} = \frac{\det M_{\text{In}}(f)^7}{\det M_{\text{Out}}(f)^7} \neq 1,$$

which means $f_4 \notin \mathscr{M}$. By Theorem 9.33, Pl-Holant $(\neq_2 |\ f_4)$ is #P-hard, and hence Pl-Holant $(\neq_2 |\ \{f\} \cup \mathcal{B})$ is #P-hard. □

Lemma 9.37. *Let $g = (0, 1, t, 0)^T$ be a binary signature where t is an n-th primitive root of unity, and $n \geq 5$. Then* Pl-Holant$(\neq_2 |\ f, g)$ *is #P-hard.*

Proof. Note that $M_{x_1,x_2}(g) = \left[\begin{smallmatrix} 0 & 1 \\ t & 0 \end{smallmatrix}\right]$. Connect the variable x_2 of a copy of signature g with the variable x_1 of another copy of signature g using $(\neq_2)$. We get a signature g_2 with the signature matrix

$$M_{x_1,x_2}(g_2) = \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ t^2 & 0 \end{bmatrix}.$$

That is, $g_2 = (0, 1, t^2, 0)^T$. Similarly, we can construct $g_i = (0, 1, t^i, 0)^T$ for $1 \leqslant i \leqslant 5$. Here, g_1 denotes g. Since the order $n \geqslant 5$, g_i are distinct $(1 \leq i \leq 5)$.

Connect variables x_4, x_3 of signature f with variables x_1, x_2 of g_i for $1 \leqslant i \leqslant 5$ respectively. We get binary signatures h_i, where

$$h_i = M_{x_1x_2,x_4x_3}(f) g_i = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \\ t^i \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ b + ct^i \\ z + yt^i \\ 0 \end{pmatrix}.$$

Let $\varphi(\mathfrak{z}) = \dfrac{z + y\mathfrak{z}}{b + c\mathfrak{z}}$. Since $\det \left[\begin{smallmatrix} b & c \\ z & y \end{smallmatrix}\right] = by - cz \neq 0$, $\varphi(\mathfrak{z})$ is a Möbius transformation of the extended complex plane $\widehat{\mathbb{C}}$. We rewrite h_i in the form of $(b + ct^i)(0, 1, \varphi(t^i), 0)^T$, with the understanding that if $b + ct^i = 0$, then $\varphi(t^i) = \infty$, and we define $(b + ct^i)(0, 1, \varphi(t^i), 0)^T$ to be $(0, 1, z + yt^i, 0)^T$. If there is a t^i such that $\varphi(t^i)$ is not a root of unity, and $\varphi(t^i) \neq 0$ and $\varphi(t^i) \neq \infty$, by Lemma 9.36, we have Pl-Holant$\,(\neq_2 |\ f, h_i)$ is #P-hard, and hence Pl-Holant$\,(\neq_2 |\ f, g_1)$ is #P-hard. Otherwise, $\varphi(t^i)$ is 0, ∞ or a root of unity for $1 \leqslant i \leqslant 5$. Since $\varphi(\mathfrak{z})$ is a bijection of $\widehat{\mathbb{C}}$, there is at most one t^i such that $\varphi(t^i) = 0$ and at most one t^i such that $\varphi(t^i) = \infty$. That means, there are at least three t^i such that $|\varphi(t^i)| = 1$. Since a Möbius transformation is determined by any 3 distinct points, mapping 3 distinct points from S^1 to S^1 implies that this $\varphi(\mathfrak{z})$ maps S^1 homeomorphically onto S^1 (so in fact there is no t^i such that $\varphi(t^i) = 0$ or ∞). Such a Möbius transformation has a special form: $\mathcal{M}(\alpha, e^{\mathrm{i}\theta}) = e^{\mathrm{i}\theta} \dfrac{(\mathfrak{z} + \alpha)}{1 + \bar{\alpha}\mathfrak{z}}$, where $|\alpha| \neq 1$. (It cannot be of the form $e^{\mathrm{i}\theta}/\mathfrak{z}$, since $b \neq 0$.)

By normalization in signature f, we may assume $b = 1$. Compare the coefficients, we have $c = \bar{\alpha}$, $y = e^{\mathrm{i}\theta}$ and $z = \alpha e^{\mathrm{i}\theta}$. Here $\alpha \neq 0$ due to $z \neq 0$. Also, since $M_{x_2x_3,x_1x_4}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & y \\ 0 & a & z & 0 \\ 0 & c & x & 0 \\ b & 0 & 0 & 0 \end{smallmatrix}\right]$ and

$\det\left[\begin{smallmatrix} a & z \\ c & x \end{smallmatrix}\right] = ax - cz \neq 0$, we have another Möbius transformation $\psi(\mathfrak{z}) = \dfrac{c + x\mathfrak{z}}{a + z\mathfrak{z}}$. Plug in $c = \bar{\alpha}$ and $z = \alpha e^{\mathrm{i}\theta}$, we have

$$\psi(\mathfrak{z}) = \frac{\bar{\alpha} + x\mathfrak{z}}{a + \alpha e^{\mathrm{i}\theta}\mathfrak{z}} = \frac{\frac{\bar{\alpha}}{a} + \frac{x}{a}\mathfrak{z}}{1 + \frac{\alpha e^{\mathrm{i}\theta}}{a}\mathfrak{z}}.$$

By the same proof for $\varphi(\mathfrak{z})$, we get Pl-Holant $(\neq_2 |\, f, g)$ is #P-hard, unless $\psi(\mathfrak{z})$ also maps S^1 to S^1. Hence, we can assume $\psi(\mathfrak{z})$ has the form $\mathcal{M}(\beta, e^{\mathrm{i}\theta'}) = e^{\mathrm{i}\theta'}\dfrac{(\mathfrak{z} + \beta)}{1 + \bar{\beta}\mathfrak{z}}$, where $|\beta| \neq 1$. (It is clearly not of the form $e^{\mathrm{i}\theta'}/\mathfrak{z}$.) Compare the coefficients, we have

$$\begin{cases} \alpha e^{\mathrm{i}\theta}/a = \bar{\beta} \\ \quad \bar{\alpha}/a = e^{\mathrm{i}\theta'}\beta \\ \quad x/a \ = e^{\mathrm{i}\theta'} \end{cases}.$$

Solving these equations, we get $a = e^{\mathrm{i}\theta}\alpha/\bar{\beta}$ and $x = \bar{\alpha}/\beta$. Let $\gamma = \alpha/\bar{\beta}$, and we have $a = \gamma e^{\mathrm{i}\theta}$ and $x = \bar{\gamma}$, where $|\gamma| \neq |\alpha|$ since $|\beta| \neq 1$ and $\gamma \neq 0$ since $x \neq 0$. Then, we have signature matrices $M_{x_1x_2,x_4x_3}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & \gamma e^{\mathrm{i}\theta} \\ 0 & 1 & \bar{\alpha} & 0 \\ 0 & \alpha e^{\mathrm{i}\theta} & e^{\mathrm{i}\theta} & 0 \\ \bar{\gamma} & 0 & 0 & 0 \end{smallmatrix}\right]$, $M_{x_2x_3,x_1x_4}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & e^{\mathrm{i}\theta} \\ 0 & \gamma e^{\mathrm{i}\theta} & \alpha e^{\mathrm{i}\theta} & 0 \\ 0 & \bar{\alpha} & \bar{\gamma} & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right]$, $M_{x_3x_4,x_2x_1}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & \bar{\gamma} \\ 0 & e^{\mathrm{i}\theta} & \bar{\alpha} & 0 \\ 0 & \alpha e^{\mathrm{i}\theta} & 1 & 0 \\ \gamma e^{\mathrm{i}\theta} & 0 & 0 & 0 \end{smallmatrix}\right]$ and $M_{x_4x_1,x_3x_2}(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & \bar{\gamma} & \alpha e^{\mathrm{i}\theta} & 0 \\ 0 & \bar{\alpha} & \gamma e^{\mathrm{i}\theta} & 0 \\ e^{\mathrm{i}\theta} & 0 & 0 & 0 \end{smallmatrix}\right]$. Connect variables x_4, x_3 of a copy of signature f with variables x_3, x_4 of another copy of signature f using $(\neq_2)$. We get a signature f_1 with the signature matrix

$$M(f_1) = M_{x_1x_2,x_4x_3}(f)N_2M_{x_3x_4,x_2x_1}(f) = \begin{bmatrix} 0 & 0 & 0 & \gamma\bar{\gamma}e^{\mathrm{i}\theta} \\ 0 & (\alpha + \bar{\alpha})e^{\mathrm{i}\theta} & 1 + \bar{\alpha}^2 & 0 \\ 0 & (1 + \alpha^2)e^{\mathrm{i}2\theta} & (\alpha + \bar{\alpha})e^{\mathrm{i}\theta} & 0 \\ \gamma\bar{\gamma}e^{\mathrm{i}\theta} & 0 & 0 & 0 \end{bmatrix}.$$

- If $\alpha + \bar{\alpha} \neq 0$, normalizing $M_{x_1x_2,x_4x_3}(f_1)$ by dividing by $(\alpha + \bar{\alpha})e^{\mathrm{i}\theta}$, we have

$$M(f_1) = \begin{bmatrix} 0 & 0 & 0 & \dfrac{\gamma\bar{\gamma}}{(\alpha + \bar{\alpha})} \\ 0 & 1 & \dfrac{(1 + \bar{\alpha}^2)e^{-\mathrm{i}\theta}}{(\alpha + \bar{\alpha})} & 0 \\ 0 & \dfrac{(1 + \alpha^2)e^{\mathrm{i}\theta}}{(\alpha + \bar{\alpha})} & 1 & 0 \\ \dfrac{\gamma\bar{\gamma}}{(\alpha + \bar{\alpha})} & 0 & 0 & 0 \end{bmatrix}.$$

Note that $\dfrac{(1+\alpha^2)e^{\mathrm{i}\theta}}{(\alpha+\bar{\alpha})}$ and $\dfrac{(1+\bar{\alpha}^2)e^{-\mathrm{i}\theta}}{(\alpha+\bar{\alpha})}$ are conjugates. Let $\delta = \dfrac{(1+\alpha^2)e^{\mathrm{i}\theta}}{(\alpha+\bar{\alpha})}$, and then $\bar{\delta} = \dfrac{(1+\bar{\alpha}^2)e^{-\mathrm{i}\theta}}{(\alpha+\bar{\alpha})}$. We have $|\delta|^2 = \delta\bar{\delta} = \dfrac{(1+\alpha^2)(1+\bar{\alpha}^2)}{(\alpha+\bar{\alpha})^2} \neq 1$ due to $\det M_{\mathrm{In}}(f_1) \neq 0$, and $\delta \neq 0$ due to $|\alpha| \neq 1$. Consider the inner matrix of $M(f_1)$, we have $M_{\mathrm{In}}(f_1) = \left[\begin{smallmatrix} 1 & \bar{\delta} \\ \delta & 1 \end{smallmatrix}\right]$. Notice that the two eigenvalues of $M_{\mathrm{In}}(f_1)$ are $1+|\delta|$ and $1-|\delta|$, and obviously $\left|\frac{1-|\delta|}{1+|\delta|}\right| \neq 1$, which means there is no integer $n > 0$ and complex number C such that $M^n_{\mathrm{In}}(f_1) = CI$. Note that $\varphi_1(\mathfrak{z}) = \dfrac{\delta+\mathfrak{z}}{1+\bar{\delta}\mathfrak{z}}$ is a Möbius transformation of the form $\mathcal{M}(\delta, 1)$ mapping S^1 to S^1.

Connect variables x_4, x_3 of signature f_1 with variables x_1, x_2 of signatures g_i. We get binary signatures $g_{(i,\varphi_1)}$, where

$$g_{(i,\varphi_1)} = M_{x_1x_2,x_4x_3}(f_1)g_i = \begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 1 & \bar{\delta} & 0 \\ 0 & \delta & 1 & 0 \\ * & 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \\ t^i \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1+\bar{\delta}t^i \\ \delta + t^i \\ 0 \end{pmatrix} = (1+\bar{\delta}t^i) \begin{pmatrix} 0 \\ 1 \\ \varphi_1(t^i) \\ 0 \end{pmatrix}.$$

Since φ_1 is a Möbius transformation mapping S^1 to S^1 and $|t^i| = 1$, we have $|\varphi_1(t^i)| = 1$, which means $1+\bar{\delta}t^i \neq 0$. Hence, $g_{(i,\varphi_1)}$ can be normalized as $(0, 1, \varphi_1(t^i), 1)^T$. Successively construct binary signatures $g_{(i,\varphi_1^n)}$ by connecting f_1 with $g_{(i,\varphi_1^{n-1})}$. We have

$$g_{(i,\varphi_1^n)} = M(f_1)g_{(i,\varphi_1^{n-1})} = M^n(f_1)g_i = C_{(i,n)}(0, 1, \varphi_1^n(t^i), 0)^T,$$

where $C_{(i,n)} = \prod\limits_{0\leqslant k\leqslant n-1} \left(1+\bar{\delta}\varphi_1^k(t^i)\right)$. We know $C_{(i,n)} \neq 0$, because for any k, $1+\bar{\delta}\varphi_1^{k-1}(t^i) \neq 0$ due to $|\varphi_1^k(t^i)| = \dfrac{|\delta+\varphi_1^{k-1}(t^i)|}{|1+\bar{\delta}\varphi_1^{k-1}(t^i)|} = 1$. Hence, $g_{(i,\varphi_1^n)}$ can be normalized as $(0, 1, \varphi_1^n(t^i), 0)^T$. Notice that the nonzero entries $(1, \varphi_1^n(t^i))^T$ of $g_{(i,\varphi_1^n)}$ are completely decided by the inner matrix $M_{\mathrm{In}}(f_1)$. That is

$$M^n_{\mathrm{In}}(f_1) \begin{pmatrix} 1 \\ t^i \end{pmatrix} = C_{(i,n)} \begin{pmatrix} 1 \\ \varphi_1^n(t^i) \end{pmatrix}.$$

If for each $i \in \{1, 2, 3\}$, there is some $n_i \geqslant 1$ such that $(1, \varphi_1^{n_i}(t^i))^T = (1, t^i)^T$, then $\varphi_1^{n_0}(t^i) = t^i$, where $n_0 = n_1n_2n_3$ for $1 \leqslant i \leqslant 3$, i.e., the Möbius transformation $\varphi_1^{n_0}$ fixes three distinct complex numbers t, t^2, t^3. So the Möbius transformation is the identity map, i.e., $\varphi_1^{n_0}(\mathfrak{z}) = \mathfrak{z}$

for all $\mathfrak{z} \in \mathbb{C}$. This implies that $M_{\text{In}}^{n_0}(f_1) = C\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ for some constant $C \neq 0$. This contradicts the fact that the ratio of the eigenvalues of M_{In} is not a root of unity. Therefore, there is an i such that $(1, \varphi_1^n(t^i))^T$ are all distinct for $n \in \mathbb{N}$. Then, we can realize polynomially many distinct binary signatures of the form $(0, 1, \varphi_1^n(t^i), 1)^T$. By Lemma 9.5, we have Pl-Holant$(\neq_2 \mid f, g)$ is #P-hard.

- Otherwise $\alpha + \bar{\alpha} = 0$, which means α is a pure imaginary number. We already have $\alpha \neq 0$ due to $z \neq 0$. Also $|\alpha| \neq 1$ from the form of $\mathcal{M}(\alpha, e^{\mathfrak{i}\theta})$. Let $\alpha = r\mathfrak{i}$, where $r \in \mathbb{R}$ and $|r| \neq 0$ or 1. Connect variables x_1, x_4 of a copy of signature f with variables x_4, x_1 of another copy of signature f, we get a signature f_2 with the signature matrix

$$\begin{aligned}
M(f_2) &= M_{x_2x_3,x_1x_4}(f) N_2 M_{x_4x_1,x_3x_2}(f)\\
&= \begin{bmatrix} 0 & 0 & 0 & e^{\mathfrak{i}\theta}\\ 0 & \gamma e^{\mathfrak{i}\theta} & r\mathfrak{i}e^{\mathfrak{i}\theta} & 0\\ 0 & -r\mathfrak{i} & \bar{\gamma} & 0\\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1\\ 0 & \bar{\gamma} & r\mathfrak{i}e^{\mathfrak{i}\theta} & 0\\ 0 & -r\mathfrak{i} & \gamma e^{\mathfrak{i}\theta} & 0\\ e^{\mathfrak{i}\theta} & 0 & 0 & 0 \end{bmatrix}\\
&= \begin{bmatrix} 0 & 0 & 0 & e^{\mathfrak{i}\theta}\\ 0 & (-\gamma+\bar{\gamma})r\mathfrak{i}e^{\mathfrak{i}\theta} & (\gamma^2 - r^2)e^{\mathfrak{i}2\theta} & 0\\ 0 & \bar{\gamma}^2 - r^2 & (-\gamma+\bar{\gamma})r\mathfrak{i}e^{\mathfrak{i}\theta} & 0\\ e^{\mathfrak{i}\theta} & 0 & 0 & 0 \end{bmatrix}.
\end{aligned}$$

  - If $-\gamma + \bar{\gamma} \neq 0$, normalizing $M(f_2)$ by dividing the quantity $(-\gamma + \bar{\gamma})r\mathfrak{i}e^{\mathfrak{i}\theta}$, we have

$$M_{\text{In}}(f_2) = \begin{bmatrix} 1 & \dfrac{(\gamma^2 - r^2)e^{\mathfrak{i}\theta}}{(-\gamma+\bar{\gamma})r\mathfrak{i}}\\ \dfrac{(\bar{\gamma}^2 - r^2)e^{-\mathfrak{i}\theta}}{(-\gamma+\bar{\gamma})r\mathfrak{i}} & 1 \end{bmatrix}.$$

    Note that $\dfrac{(\gamma^2 - r^2)e^{\mathfrak{i}\theta}}{(-\gamma+\bar{\gamma})r\mathfrak{i}}$ and $\dfrac{(\bar{\gamma}^2 - r^2)e^{-\mathfrak{i}\theta}}{(-\gamma+\bar{\gamma})r\mathfrak{i}}$ are conjugates. Let $\zeta = \dfrac{(\bar{\gamma}^2 - r^2)e^{-\mathfrak{i}\theta}}{(-\gamma+\bar{\gamma})r\mathfrak{i}}$, and then $|\zeta| \neq 1$ due to $\det M_{\text{In}}(f_2) \neq 0$, and $\zeta \neq 0$ due to $|\gamma| \neq |\alpha| = |r|$ (as $|\beta| \neq 1$). With the same analysis as for $M_{\text{In}}(f_1)$ in the case $\alpha + \bar{\alpha} \neq 0$, the ratio of the two eigenvalues of $M_{\text{In}}(f_2) = \left[\begin{smallmatrix}1 & \bar{\zeta}\\ \zeta & 1\end{smallmatrix}\right]$ is also not equal to 1, which means there is no integer

n and complex number C such that $M^n_{\text{In}}(f_2) = CI$. Notice that $\varphi_2(\mathfrak{z}') = \dfrac{\zeta + \mathfrak{z}'}{1 + \bar{\zeta}\mathfrak{z}'}$ is also a Möbius transformation of the form $\mathcal{M}(\zeta, 1)$ mapping S^1 to S^1. Similarly, we can realize polynomially many distinct binary signatures, and hence Pl-Holant($\neq_2$| f, g) is #P-hard.

– Otherwise, $-\gamma + \bar{\gamma} = 0$, which means γ is a real number. We have $\gamma \in \mathbb{R}$, $|\gamma| \neq 0$ or $|r|$. Connect variables x_4, x_3 of a copy of signature f with variables x_1, x_2 of another copy of signature f, we get a signature f' with the signature matrix

$$\begin{aligned} M(f') &= M_{x_1x_2,x_4x_3}(f) N_2 M_{x_1x_2,x_4x_3}(f) \\ &= \begin{bmatrix} 0 & 0 & 0 & \gamma e^{\mathrm{i}\theta} \\ 0 & 1 & -r\mathrm{i} & 0 \\ 0 & r\mathrm{i}e^{\mathrm{i}\theta} & e^{\mathrm{i}\theta} & 0 \\ \gamma & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & \gamma e^{\mathrm{i}\theta} \\ 0 & 1 & -r\mathrm{i} & 0 \\ 0 & r\mathrm{i}e^{\mathrm{i}\theta} & e^{\mathrm{i}\theta} & 0 \\ \gamma & 0 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & \gamma^2 e^{\mathrm{i}2\theta} \\ 0 & (e^{\mathrm{i}\theta} - 1)r\mathrm{i} & e^{\mathrm{i}\theta} - r^2 & 0 \\ 0 & e^{\mathrm{i}\theta} - e^{\mathrm{i}2\theta}r^2 & (e^{\mathrm{i}2\theta} - e^{\mathrm{i}\theta})r\mathrm{i} & 0 \\ \gamma^2 & 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

∗ If $e^{\mathrm{i}\theta} = 1$, then $M(f) = \left[\begin{smallmatrix} 0 & 0 & 0 & \gamma \\ 0 & 1 & \bar{\alpha} & 0 \\ 0 & \alpha & 1 & 0 \\ \bar{\gamma} & 0 & 0 & 0 \end{smallmatrix}\right]$, and $M_{\text{In}}(f) = \left[\begin{smallmatrix} 1 & \bar{\alpha} \\ \alpha & 1 \end{smallmatrix}\right]$. Since $|\alpha| \neq 1$, same as the analysis of $M_{\text{In}}(f_1)$, we can realize polynomially many binary signatures, and hence Pl-Holant($\neq_2$| f, g) is #P-hard.

∗ Otherwise $e^{\mathrm{i}\theta} \neq 1$, normalizing $M(f')$ by dividing by $(e^{\mathrm{i}\theta} - 1)r\mathrm{i}$, we have

$$M(f') = \begin{bmatrix} 0 & 0 & 0 & \dfrac{\gamma^2 e^{\mathrm{i}\theta}}{(e^{\mathrm{i}\theta} - 1)r\mathrm{i}} \cdot e^{\mathrm{i}\theta} \\ 0 & 1 & \dfrac{e^{\mathrm{i}\theta} - r^2}{(e^{\mathrm{i}\theta} - 1)r\mathrm{i}} & 0 \\ 0 & \dfrac{1 - e^{\mathrm{i}\theta}r^2}{(e^{\mathrm{i}\theta} - 1)r\mathrm{i}} \cdot e^{\mathrm{i}\theta} & e^{\mathrm{i}\theta} & 0 \\ \dfrac{\gamma^2}{(e^{\mathrm{i}\theta} - 1)r\mathrm{i}} & 0 & 0 & 0 \end{bmatrix}.$$

Note that $\dfrac{1-e^{\mathrm{i}\theta}r^2}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$ and $\dfrac{e^{\mathrm{i}\theta}-r^2}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$ are conjugates, and $\dfrac{\gamma^2 e^{\mathrm{i}\theta}}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$ and $\dfrac{\gamma^2}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$ are conjugates. Let $\alpha' = \dfrac{1-e^{\mathrm{i}\theta}r^2}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$ and $\gamma' = \dfrac{\gamma^2 e^{\mathrm{i}\theta}}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}}$. Then

$$M(f') = \begin{bmatrix} 0 & 0 & 0 & \gamma' e^{\mathrm{i}\theta} \\ 0 & 1 & \bar{\alpha}' & 0 \\ 0 & \alpha' e^{\mathrm{i}\theta} & e^{\mathrm{i}\theta} & 0 \\ \bar{\gamma}' & 0 & 0 & 0 \end{bmatrix}.$$

Notice that $M(f')$ and $M(f)$ have the same form. Similar to the construction of f_2, we can construct a signature f_2' using f' instead of f. Since $-\gamma' + \bar{\gamma}' = -\dfrac{\gamma^2 e^{\mathrm{i}\theta}}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}} + \dfrac{\gamma^2}{(e^{\mathrm{i}\theta}-1)r\mathrm{i}} = -\dfrac{\gamma^2}{r\mathrm{i}} \neq 0$, by the analysis of f_2, we can still realize polynomially many binary signatures and hence Pl-Holant($\neq_2$| f, g) is #P-hard. □

Remark 9.38. *The order $n \geqslant 5$ promises that there are at least three points mapped to points on S^1, since at most one point can be mapped to 0 and at most one can be mapped to ∞. When the order n is 3 or 4, if no point is mapped to 0 or ∞, then there are still at least three points mapped to points on S^1. So, we have the following corollary.*

Corollary 9.39. *Let $g = (0, 1, t, 0)^T$ be a binary signature where t is an n-th primitive root of unity, and $n = 3$ or 4. Let g_m denote $(0, 1, t^m, 0)^T$. For any cyclic permutation (i, j, k, ℓ) of $(1, 2, 3, 4)$, if there is no g_m such that $M_{x_i x_j, x_\ell x_k}(f) g_m = d_1(0, 1, 0, 0)^T$ or $d_2(0, 0, 1, 0)^T$, where $d_1, d_2 \in \mathbb{C}$, then* Pl-Holant($\neq_2$| f, g) *is #P-hard.*

We normalize f by setting $b = 1$ in Lemma 9.6.

Lemma 9.40. *Let $g = (0, 1, 0, 0)^T$ be a binary signature. Then* Pl-Holant($\neq_2$| f, g) *is #P-hard.*

Proof. Connecting variables x_4, x_3 of the signature f with variables x_2 and x_1 of g both using $(\neq_2)$ we get a binary signature g_1, where

$$g_1 = M_{x_1 x_2, x_4 x_3}(f)(0, 1, 0, 0)^T = (0, 1, z, 0)^T.$$

$g_1(x_1, x_2)$ can be normalized to $(0, z^{-1}, 1, 0)^T$ since $z \neq 0$. So we have $g_1(x_2, x_1) = (0, 1, z^{-1}, 0)$.

Then, modifying $x_1 = 1$ of f with z^{-1} scaling, we get a signature f_1 with the signature matrix $M(f_1) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & 1 & c & 0 \\ 0 & 1 & y/z & 0 \\ x/z & 0 & 0 & 0 \end{bmatrix}$. We denote it by $\begin{bmatrix} 0 & 0 & 0 & a \\ 0 & 1 & c & 0 \\ 0 & 1 & y_1 & 0 \\ x_1 & 0 & 0 & 0 \end{bmatrix}$, where $x_1 y_1 \neq 0$.

- If $c = 0$, connecting variables x_4, x_3 of f_1 with variables x_1, x_2 of g both using $(\neq_2)$ we get a binary signature h_1, where

  $$h_1 = M_{x_1x_2,x_4x_3}(f_1)(0,0,1,0)^T = (0,1,y_1,0)^T.$$

  Also, connecting the variable x_4 with x_3 of f_1 using $(\neq_2)$ we get a binary signature H, where

  $$H = M_{x_1x_2,x_4x_3}(f_1)(0,1,1,0)^T = (0,2,y_1,0)^T.$$

  H can be normalized to $(0,1,\frac{y_1}{2},0)^T$. Clearly, $|y_1| \neq |\frac{y_1}{2}|$, so they cannot both be roots of unity. By Lemma 9.36, Pl-Holant $(\neq_2|\, f, h_1, H)$ is #P-hard, and we conclude that Pl-Holant $(\neq_2|\, f, g)$ is #P-hard.

- Otherwise $c \neq 0$. Connecting variables x_2, x_1 of g with variables x_1, x_2 of f both using $(\neq_2)$ we get a binary signature g_2, where

  $$g_2 = ((0,1,0,0)M_{x_1x_2,x_4x_3}(f_1))^T = (0,1,c,0)^T.$$

  which can be normalized to $g_2(x_2,x_1) = (0,1,c^{-1},0)^T$. Then, modifying $x_4 = 1$ of f_1 with c^{-1} scaling, we get a signature f_2 with the signature matrix $M(f_2) = \begin{bmatrix} 0 & 0 & 0 & \frac{a}{c} \\ 0 & 1 & 1 & 0 \\ 0 & 1 & \frac{y}{zc} & 0 \\ \frac{x}{z} & 0 & 0 & 0 \end{bmatrix}$ which we denote by $\begin{bmatrix} 0 & 0 & 0 & a_2 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & y_2 & 0 \\ x_2 & 0 & 0 & 0 \end{bmatrix}$, where $a_2x_2y_2 \neq 0$. Notice that $M_{x_2x_3,x_1x_4}(f_2) = \begin{bmatrix} 0 & 0 & 0 & y_2 \\ 0 & a_2 & 1 & 0 \\ 0 & 1 & x_2 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Connect variables x_1, x_4 of signature f_2 with variables x_2, x_1 of g both using $(\neq_2)$. We get a binary signature h_3, where

  $$h_3 = M_{x_2x_3,x_1x_4}(f_2)(0,1,0,0)^T = (0,a_2,1,0)^T.$$

  h_3 can be normalized as $(0,1,\frac{1}{a_2},0)^T$. Also connect variables x_1, x_4 of signature f_2 with variables x_1, x_2 of g both using $(\neq_2)$. We get a binary signature h_4, where

$$h_4 = M_{x_2x_3,x_1x_4}(f_2)(0,0,1,0)^T = (0,1,x_2,0)^T.$$

If $|a_2| \neq 1$ or $|x_2| \neq 1$, then a_2 or x_2 is not a root of unity. By Lemma 9.36, Pl-Holant $(\neq_2|\ f, h_3, h_4)$ is #P-hard, and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard. Otherwise, $|a_2| = |x_2| = 1$. Same as the construction of h_1 and H, construct binary signatures h'_1 and h'_2 using f_2 instead of f_1. We get

$$h'_1 = M_{x_1x_2,x_4x_3}(f_2)(0,0,1,0)^T = (0,1,y_2,0)^T,$$

and

$$h'_2 = M_{x_1x_2,x_4x_3}(f_2)(0,1,1,0)^T = (0,2,1+y_2,0)^T.$$

Note that h'_2 can be normalized as $(0,1,\frac{1+y_2}{2},0)^T$.

- If y_2 is not a root of unity, then by Lemma 9.36, Pl-Holant $(\neq_2|\ f, h'_1)$ is #P-hard, and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard.
- If y_2 is an n-th primitive root of unity and $n \geqslant 5$, then by Lemma 9.37, Pl-Holant $(\neq_2|\ f, h'_1)$ is #P-hard, and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard.
- If $y_2 = \frac{-1\pm\sqrt{3}\mathfrak{i}}{2}$ or $\pm\mathfrak{i}$, then $0 < |\frac{1+y_2}{2}| < 1$, which means it is not zero neither a root of unity. By Lemma 9.36, Pl-Holant $(\neq_2|\ f, h'_2)$ is #P-hard, and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard.
- If $y_2 = 1$, then f_2 is non-singular redundant and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard.
- If $y_2 = -1$. Connect two copies of f_2, we get a signature f_3 with the signature matrix

$$M(f_3) = M_{x_1x_2,x_4x_3}(f_2)N_2M_{x_1x_2,x_4x_3}(f_2) = \begin{bmatrix} 0 & 0 & 0 & a_2^2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ x_2^2 & 0 & 0 & 0 \end{bmatrix}.$$

  Since $|a_2| = |x_2| = 1$, $|a_2^2x_2^2| = 1 \neq 4$. Therefore, applying Corollary 9.31 to $\{a_2^2, 2, x_2^2, -2\}$, we get Pl-Holant $(\neq_2|\ f_3)$ is #P-hard, and hence Pl-Holant $(\neq_2|\ f, g)$ is #P-hard. □

Combining Lemma 9.37, Corollary 9.39 and Lemma 9.40, we have the following corollary.

Corollary 9.41. *Let $g = (0,1,t,0)^T$ be a binary signature where t is an n-th primitive root of unity, and $n \geqslant 3$. Then* Pl-Holant$(\neq_2|\, f, g)$ *is #P-hard.*

Now, we are able to prove the following theorem for Case IV.

Theorem 9.42. *Let f be a 4-ary signature with the signature matrix*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & z & y & 0 \\ x & 0 & 0 & 0 \end{bmatrix},$$

where $abxyz \neq 0$. Pl-Holant$(\neq_2|\, f)$ *is #P-hard unless $f \in \mathscr{M}$, in which case,* Pl-Holant$(\neq_2|\, f)$ *is tractable.*

Proof. Tractability follows by 9.9.

Now suppose $f \notin \mathscr{M}$. Connect the variable x_4 with x_3 of f using $(\neq_2)$, and we get a binary signature g_1, where

$$g_1 = M_{x_1x_2,x_4x_3}(0,1,1,0)^T = (0, b+c, z+y, 0)^T.$$

Connect the variable x_1 with x_2 of f using $(\neq_2)$, and we get a binary signature g_2, where

$$g_2 = ((0,1,1,0)M_{x_1x_2,x_4x_3})^T = (0, b+z, c+y, 0)^T.$$

- If one of g_1 and g_2 is of the form $(0,0,0,0)^T$, then $by = (-c)(-z) = cz$. That is $by - cz = 0$. Here $c \neq 0$ due to $by \neq 0$. By Lemma 9.35, Pl-Holant$(\neq_2|\, f)$ is #P-hard.

- If one of g_1 and g_2 can be normalized as $(0,1,0,0)$ or $(0,0,1,0)$. By Lemma 9.40, Pl-Holant$(\neq_2|\, f)$ is #P-hard.

- If one of g_1 and g_2 can be normalized as $(0,1,t,0)^T$, where $t \neq 0$ is not a root of unity, then by Lemma 9.36, Pl-Holant$(\neq_2|\, f)$ is #P-hard.

- If one of g_1 and g_2 can be normalized as $(0,1,t,0)^T$, where t is an n-th primitive root of unity and $n \geqslant 3$, then by Corollary 9.41, Pl-Holant$(\neq_2|\, f)$ is #P-hard.

- Otherwise, g_1 and g_2 do not belong to those cases above, which means both g_1 and g_2 both can be normalized as $(0, 1, \epsilon_1, 0)$ and $(0, 1, \epsilon_2, 0)$, where $\epsilon_1 = \pm 1$ and $\epsilon_2 = \pm 1$. That is, $b + c = \epsilon_1(z + y) \neq 0$ and $b + z = \epsilon_2(c + y) \neq 0$.
  - If $b+c = z+y$ and $b+z = c+y$, then $b = y$ and $c = z$. This case will be proved below.
  - If $b + c = -(z + y)$ and $b + z = c + y$, then $b + z = c + y = 0$, so $g_2 = (0, 0, 0, 0)^T$, a contradiction.
  - If $b + c = z + y$ and $b + z = -(c + y)$, then $b + c = z + y = 0$, so $g_1 = (0, 0, 0, 0)^T$, a contradiction.
  - If $b + c = -(z + y)$ and $b + z = -(c + y)$, we get $b + c + y + z = 0$. But $b + c \neq 0$, otherwise $g_1 = (0, 0, 0, 0)^T$, a contradiction. So we can normalize g_1 to $(0, 1, -1, 0)^T$. Modify $x_1 = 1$ of f with -1 scaling, and we get a signature f' with the signature matrix $M(f') = \left[\begin{smallmatrix} 0 & 0 & 0 & a \\ 0 & b & c & 0 \\ 0 & -z & -y & 0 \\ -x & 0 & 0 & 0 \end{smallmatrix}\right]$. Connect the variable x_1 with x_2 of f' using $(\neq_2)$, and we get a binary signature $g' = (0, b - z, c - y, 0)^T$. Same as the analysis of g_1 and g_2 above, we have Pl-Holant$(\neq_2 |\ f')$ is #P-hard unless g' can be normalized as $(0, 1, \epsilon_3, 0)$, where $\epsilon_3 = \pm 1$. That is, $b - z = \epsilon_3(c - y) \neq 0$, $\epsilon_3 = \pm 1$.
    - If $b - z = c - y$, combined with $b + c = -(z + y)$, we have $b = -y$ and $c = -z$. This case will be proved below.
    - If $b - z = -(c - y)$, combined with $b + c = -(z + y)$, we have $b + c = z + y = 0$, and so $g_1 = (0, 0, 0, 0)^T$, a contradiction.

    Therefore, Pl-Holant$(\neq_2 |\ f')$ is #P-hard and hence Pl-Holant$(\neq_2 |\ f)$ is #P-hard.

To summarize, except for the cases $b = \epsilon y$ and $c = \epsilon z$, where $\epsilon = \pm 1$, we have proved that Pl-Holant$(\neq_2 |\ f)$ is #P-hard. We can connect the variable x_2 with x_3 of f using $(\neq_2)$, and get a binary signature $g_3 = (0, a + c, z + x, 0)^T$. Connect the variable x_1 with x_4 of f using $(\neq_2)$, and we get a binary signature $g_4 = (0, a + z, c + x, 0)^T$. Same as the analysis of g_1 and g_2, we have Pl-Holant$(\neq_2 |\ f)$ is #P-hard unless $a = \epsilon' x$ and $c = \epsilon' z$, where $\epsilon' = \pm 1$. By both $c = \epsilon z$ and $c = \epsilon' z$ and $z \neq 0$ we get $\epsilon = \epsilon'$. Therefore, Pl-Holant$(\neq_2 |\ f)$ is #P-hard unless $a = \epsilon x$, $b = \epsilon y$ and $c = \epsilon z$, where $\epsilon = \pm 1$. In this case, since $z \neq 0$, we have $abc \neq 0$. By Lemma 9.34, Pl-Holant$(\neq_2 |\ f)$ is #P-hard, since we have assumed $f \notin \mathscr{M}$. □

9.7 Proof of the Trichotomy Theorem

Now we are ready to prove the main theorem, Theorem 9.21.

Proof of Tractability:

- If f satisfies condition 1 or 2, then by Theorem 9.20, Holant$(\neq_2 | \, f)$ is tractable without the planarity restriction. Obviously, Pl-Holant$(\neq_2 | \, f)$ is tractable.
- If f satisfies condition 3, then by Theorem 9.9, Pl-Holant$(\neq_2 | \, f)$ is tractable.
- If f satisfies condition 4, then by Theorem 9.30, Pl-Holant$(\neq_2 | \, f)$ is tractable.

Proof of Hardness:

Since f does not satisfy condition 2, f does not belong to Case I. Therefore it belongs to Cases II, III, or IV.

- Suppose f belongs to Case II.
  - If an outer pair is a zero pair, since f does not satisfy condition 1 or condition 3, then by Theorem 9.24, Pl-Holant$(\neq_2 | \, f)$ is #P-hard.
  - If the inner pair is a zero pair and no outer pair is zero, since f does not satisfy condition 4, then by Theorem 9.30, Pl-Holant$(\neq_2 | \, f)$ is #P-hard.
- Suppose f belongs to Case III. Since f does not satisfy condition 3, then by Theorem 9.33, Pl-Holant$(\neq_2 | \, f)$ is #P-hard.
- Suppose f belongs to Case IV. Since f does not satisfy condition 3, then by Theorem 9.42, Pl-Holant$(\neq_2 | \, f)$ is #P-hard. □

Chapter 10

Conclusion and Outlook

In this dissertation, we proved a complexity dichotomy for real-valued Holant problems with arbitrary asymmetric signatures and a complexity trichotomy for planar six vertex models with arbitrary complex values. The ultimate goal is definitely a complete complexity classification for all complex-valued Holant problems.

One natural question is whether the tractability condition (T) in the real Holant dichotomy covers all tractable cases for complex-valued Holant problems without considering the planar restriction. The answer is *no*. It is already known that there is a family of complex-valued signatures, called vanishing signatures, that define tractable Holant problems [28]. For these signatures, it is crucially the possibility to take complex values that makes them tractable. In fact, the evaluation of problems defined by vanishing signatures is always zero, for the sake of which these signatures are named after "vanishing".

The complexity dichotomy for six-vertex models without considering the planar restriction also captures a tractable case beyond the tractability condition (T). Based on this result, our on-going work suggests that there is potentially a more general family of new tractable signatures. This family may complete the picture for the complexity classification of complex-valued Holant problems over general graphs. It seems to be more convenient to carve out this new tractable family in the framework of Holant($\neq_2 | \mathcal{F}$) without assuming ARS on $\mathcal{F}$. As a special case of Holant($\neq_2 | \mathcal{F}$), a complexity classification of #EO problems without assuming ARS will serve as a building block.

Taking account of the planar restriction, a very interesting question is whether there are more planar tractable cases beyond the reach of the FKT algorithm. We believe the answer is *yes*. The new tractable case for planar six-vertex models obtained by the non-local reduction to #CSP can be generalized to planar #EO problems with signatures of higher arity. In this sense, a complexity classification of planar #EO problems may extend the non-local reduction technique to a universal algorithm for planar tractable Holant problems.

However, a much more challenging question is whether there are other planar tractable cases beyond both the FKT algorithm and the non-local reduction technique. If the answer is yes, then we suspect that such cases may be revealed by exploring planar eight-vertex models. Overall, there is still a long way to go to achieve a complete complexity classification for Holant problems with asymmetric signatures over planar graphs.

Bibliography

[1] D. Aharonov, I. Arad, E. Eban, and Z. Landau. Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane. *arXiv preprint quant-ph/0702008*, 2007.

[2] L. Ahlfors. *Complex analysis: an introduction to the theory of analytic functions of one complex variable*. McGraw-Hill, 1979.

[3] M. Backens. A new Holant dichotomy inspired by quantum computation. In *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming*, pages 16:1–16:14, 2017.

[4] M. Backens. A complete dichotomy for complex-valued Holant^c. In *Proceedings of the 45th International Colloquium on Automata, Languages, and Programming*, pages 12:1–12:14, 2018.

[5] F. Barahona. On the computational complexity of Ising spin glass models. *Journal of Physics A: Mathematical and General*, 15(10):3241, 1982.

[6] R. J. Baxter. Eight-vertex model in lattice statistics. *Physical Review Letters*, 26(14):832, 1971.

[7] R. J. Baxter. The six and eight-vertex models revisited. *Journal of statistical physics*, 116(1-4):43–66, 2004.

[8] R. J. Baxter. *Exactly solved models in statistical mechanics*. Elsevier, 2016.

[9] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[10] D. M. Bressoud. *Proofs and confirmations: the story of the alternating-sign matrix conjecture*. Cambridge University Press, 1999.

[11] A. Bulatov. The complexity of the counting constraint satisfaction problem. *Journal of the ACM (JACM)*, 60(5):1–41, 2013.

[12] A. Bulatov, M. Dyer, L. A. Goldberg, M. Jalsenius, M. Jerrum, and D. Richerby. The complexity of weighted and unweighted #CSP. *Journal of Computer and System Sciences*, 78(2):681–688, 2012.

[13] A. Bulatov and M. Grohe. The complexity of partition functions. *Theoretical Computer Science*, 348(2-3):148–186, 2005.

[14] J.-Y. Cai and X. Chen. *Complexity Dichotomies for Counting Problems: Volume 1, Boolean Domain*. Cambridge University Press, 2017.

[15] J.-Y. Cai and X. Chen. Complexity of counting CSP with complex weights. *Journal of the ACM (JACM)*, 64(3):1–39, 2017.

[16] J.-Y. Cai, X. Chen, and P. Lu. Graph homomorphisms with complex values: A dichotomy theorem. *SIAM Journal on Computing*, 42(3):924–1029, 2013.

[17] J.-Y. Cai, X. Chen, and P. Lu. Nonnegative weighted #CSP: An effective complexity dichotomy. *SIAM Journal on Computing*, 45(6):2177–2198, 2016.

[18] J.-Y. Cai and V. Choudhary. Some results on matchgates and holographic algorithms. In *International Colloquium on Automata, Languages, and Programming*, pages 703–714. Springer, 2006.

[19] J.-Y. Cai and Z. Fu. Complexity classification of the eight-vertex model. *arXiv preprint arXiv:1702.07938*, 2017.

[20] J.-Y. Cai and Z. Fu. Holographic algorithm with matchgates is universal for planar #CSP over Boolean domain. *SIAM Journal on Computing*, special issue of STOC 17:50–151, 2019.

[21] J.-Y. Cai, Z. Fu, H. Guo, and T. Williams. A Holant dichotomy: is the FKT algorithm universal? In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 1259–1276. IEEE, 2015.

[22] J.-Y. Cai, Z. Fu, and S. Shao. New planar P-time computable six-vertex models and a complete complexity classification. *arXiv preprint arXiv:1704.01657 (to appear in SODA 2021)*, 2017.

[23] J.-Y. Cai, Z. Fu, and S. Shao. Beyond #CSP: A dichotomy for counting weighted Eulerian orientations with ARS. *Information and Computation*, *https://doi.org/10.1016/j.ic.2020.104589*, 2020.

[24] J.-Y. Cai, Z. Fu, and S. Shao. From Holant to quantum entanglement and back. In *Proceedings of the 47th International Colloquium on Automata, Languages, and Programming*, pages 22:1–22:16, 2020.

[25] J.-Y. Cai, Z. Fu, and M. Xia. Complexity classification of the six-vertex model. *Information and Computation*, 259:130–141, 2018.

[26] J.-Y. Cai and A. Gorenstein. Matchgates revisited. *arXiv preprint arXiv:1303.6729*, 2013.

[27] J.-Y. Cai and A. Govorov. Perfect matchings, rank of connection tensors and graph homomorphisms. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 476–495. SIAM, 2019.

[28] J.-Y. Cai, H. Guo, and T. Williams. A complete dichotomy rises from the capture of vanishing signatures. *SIAM Journal on Computing*, 45(5):1671–1728, 2016.

[29] J.-Y. Cai, P. Lu, and M. Xia. Holographic algorithms with matchgates capture precisely tractable planar #CSP. In *Proceedings of the 51st IEEE Annual Symposium on Foundations of Computer Science*, pages 427–436. IEEE, 2010.

[30] J.-Y. Cai, P. Lu, and M. Xia. Dichotomy for Holant* problems of Boolean domain. In *Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms*, pages 1714–1728. SIAM, 2011.

[31] J.-Y. Cai, P. Lu, and M. Xia. The complexity of complex weighted Boolean #CSP. *Journal of Computer and System Sciences*, 80(1):217–236, 2014.

[32] J.-Y. Cai, P. Lu, and M. Xia. Dichotomy for real Holant^c problems. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1802–1821. SIAM, 2018.

[33] N. Creignou and M. Hermann. Complexity of generalized satisfiability counting problems. *Information and computation*, 125(1):1–12, 1996.

[34] J. Draisma, D. C. Gijswijt, L. Lovász, G. Regts, and A. Schrijver. Characterizing partition functions of the vertex model. *Journal of Algebra*, 350(1):197–206, 2012.

[35] M. Dyer, L. A. Goldberg, and M. Jerrum. The complexity of weighted Boolean #CSP. *SIAM Journal on Computing*, 38(5):1970–1986, 2009.

[36] M. Dyer, L. A. Goldberg, and M. Paterson. On counting homomorphisms to directed acyclic graphs. In *International Colloquium on Automata, Languages, and Programming*, pages 38–49. Springer, 2006.

[37] M. Dyer and C. Greenhill. The complexity of counting graph homomorphisms. *Random Structures & Algorithms*, 17(3-4):260–289, 2000.

[38] M. Dyer and D. Richerby. An effective dichotomy for the counting constraint satisfaction problem. *SIAM Journal on Computing*, 42(3):1245–1274, 2013.

[39] C. Fan and F. Y. Wu. Ising model with second-neighbor interaction. I. some exact results and an approximate solution. *Physical Review*, 179(2):560, 1969.

[40] C. Fan and F. Y. Wu. General lattice model of phase transitions. *Physical Review B*, 2(3):723, 1970.

[41] M. Freedman, L. Lovász, and A. Schrijver. Reflection positivity, rank connectivity, and homomorphism of graphs. *Journal of the American Mathematical Society*, 20(1):37–51, 2007.

[42] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley. A complexity dichotomy for partition functions with mixed signs. *SIAM Journal on Computing*, 39(7):3336–3402, 2010.

[43] L. A. Goldberg, M. Jerrum, and M. Paterson. The computational complexity of two-state spin systems. *Random Structures & Algorithms*, 23(2):133–154, 2003.

[44] C. Gómez, M. Ruiz-Altaba, and G. Sierra. *Quantum groups in two-dimensional physics*. Cambridge University Press, 2005.

[45] S. Huang and P. Lu. A dichotomy for real weighted Holant problems. *Computational Complexity*, 25(1):255–304, 2016.

[46] E. Ising. Beitrag zur theorie des ferromagnetismus. *Zeitschrift für Physik*, 31(1):253–258, 1925.

[47] M. Jerrum and A. Sinclair. Polynomial-time approximation algorithms for the Ising model. *SIAM Journal on Computing*, 22(5):1087–1116, 1993.

[48] P. W. Kasteleyn. Graph theory and crystal physics. *Graph theory and theoretical physics*, pages 43–110, 1967.

[49] P. W. Kasteleyn. The statistics of dimers on a lattice. In *Classic Papers in Combinatorics*, pages 281–298. Springer, 2009.

[50] V. E. Korepin. Calculation of norms of Bethe wave functions. *Communications in Mathematical Physics*, 86(3):391–418, 1982.

[51] G. Kuperberg. Another proof of the alternative-sign matrix conjecture. *International Mathematics Research Notices*, 1996(3):139–150, 1996.

[52] R. E. Ladner. On the structure of polynomial time reducibility. *Journal of the ACM (JACM)*, 22(1):155–171, 1975.

[53] M. Las Vergnas. On the evaluation at (3, 3) of the Tutte polynomial of a graph. *Journal of Combinatorial Theory, Series B*, 45(3):367–372, 1988.

[54] T.-D. Lee and C.-N. Yang. Statistical theory of equations of state and phase transitions. ii. Lattice gas and Ising model. *Physical Review*, 87(3):410, 1952.

[55] L. Li, P. Lu, and Y. Yin. Correlation decay up to uniqueness in spin systems. In *Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms*, pages 67–84. SIAM, 2013.

[56] E. H. Lieb. Residual entropy of square ice. *Physical Review*, 162(1):162, 1967.

[57] J. Lin and H. Wang. The complexity of Boolean Holant problems with nonnegative weights. *SIAM Journal on Computing*, 47(3):798–828, 2018.

[58] M. Mihail and P. Winkler. On the number of Eulerian orientations of a graph. *Algorithmica*, 16(4-5):402–414, 1996.

[59] W. H. Mills, D. P. Robbins, and H. Rumsey Jr. Alternating sign matrices and descending plane partitions. *Journal of Combinatorial Theory, Series A*, 34(3):340–359, 1983.

[60] L. Onsager. Crystal statistics. i. a two-dimensional model with an order-disorder transition. *Physical Review*, 65(3-4):117, 1944.

[61] L. Pauling. The structure and entropy of ice and of other crystals with some randomness of atomic arrangement. *Journal of the American Chemical Society*, 57(12):2680–2684, 1935.

[62] F. Rys. Über ein zweidimensionales klassisches Konfigurationsmodell. *Helvetica Physica Acta*, 36(5):537–559, 1963.

[63] A. Schrijver. Characterizing partition functions of the spin model by rank growth. *Indagationes Mathematicae*, 24(4):1018–1023, 2013.

[64] S. Shao and J.-Y. Cai. A dichotomy for real Boolean Holant problems. *arXiv preprint arXiv:2005.07906, (to appear in FOCS 2020)*, 2020.

[65] J. C. Slater. Theory of the transition in KH_2PO_4. *The Journal of Chemical Physics*, 9(1):16–33, 1941.

[66] H. N. V. Temperley and M. E. Fisher. Dimer problem in statistical mechanics-an exact result. *Philosophical Magazine*, 6(68):1061–1063, 1961.

[67] L. G. Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[68] L. G. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

[69] L. G. Valiant. Expressiveness of matchgates. *Theoretical Computer Science*, 289(1):457–471, 2002.

[70] L. G. Valiant. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal on Computing*, 31(4):1229–1254, 2002.

[71] L. G. Valiant. Accidental algorthims. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 06)*, pages 509–517. IEEE, 2006.

[72] L. G. Valiant. Holographic algorithms. *SIAM Journal on Computing*, 37(5):1565–1594, 2008.

[73] C. N. Yang. The spontaneous magnetization of a two-dimensional ising model. *Physical Review*, 85(5):808, 1952.

[74] C.-N. Yang and T.-D. Lee. Statistical theory of equations of state and phase transitions. i. theory of condensation. *Physical Review*, 87(3):404, 1952.

[75] D. Zeilberger. Proof of the alternating sign matrix conjecture. *The Electronic Journal of Combinatorics*, 3(2):R13, 1996.