Theoretical Issues in Quantum Computing: Graph Isomorphism, PageRank, and Hamiltonian Determination

by

Kenneth Michael Rudinger

A dissertation submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

(Physics)

at the

University of Wisconsin – Madison

2014

Defended on 30 June 2014

Dissertation approved by the following members of the Final Oral Committee:

Robert Joynt · Professor of Physics

Susan Coppersmith · Professor of Physics

Lisa Everett · Professor of Physics

Michael Winokur · Professor of Physics

Eric Bach · Professor of Computer Sciences

Abstract

This thesis explores several theoretical questions pertaining to quantum computing. First we examine several questions regarding multi-particle quantum random walk-based algorithms for the graph isomorphism problem. We find that there exists a non-trivial difference between continuous-time walks of one and two non-interacting particles as compared to non-interacting walks of three or more particles, in that the latter are able to distinguish many strongly regular graphs (SRGs), a class of graphs with many graph pairs that are difficult to distinguish. We demonstrate analytically where this distinguishing power comes from, and we show numerically that three-particle and four-particle non-interacting continuous-time walks can distinguish many pairs of strongly regular graphs. We additionally show that this distinguishing power, while it grows with particle number, is bounded, so that no continuous-time non-interacting walk of fixed particle number can distinguish all strongly regular graphs.

We then investigate the relationship between continuous-time and discrete-time walks, in the context of the graph isomorphism problem. While it has been previously demonstrated numerically that discrete-time walks of non-interacting particles can distinguish some SRGs, we demonstrate where this distinguishing power comes from. We also show that while no continuous-time non-interacting walk of fixed particle number can distinguish SRGs, it remains a possibility that such a discrete-time walk could, leaving open the possibility of a non-trivial difference between discrete-time and continuous-time walks.

The last piece of our work on graph isomorphism examines limitations on certain kinds of continuous-time walk-based algorithms for distinguishing graphs. We show that a very general class of continuous-time walk algorithms, with a broad class of allowable interactions, cannot distinguish all graphs.

We next consider a previously-proposed quantum adiabatic algorithm for computing the PageRank vector, a necessary step in one of Google's search algorithms. It had been previously believed that this algorithm might offer a non-trivial speedup in preparing the PageRank vector. We demonstrate, however, that when this algorithm is tested on graphs

that sufficiently resemble the graph of the World Wide Web, there is no appreciable speedup.

Lastly, we consider the problem of Hamiltonian determination. We show that in the high temperature limit, the classical signal processing technique of compressed sensing may be used to recover the Hamiltonian for a system of qubits, provided that the Hamiltonian does not possess too many interactions, i.e., it is "sparse". This new procedure allows for the determination of the Hamiltonian with a number of measurements that can be significantly smaller than required by standard techniques.

Acknowledgements

It goes almost without saying that research cannot be done in a vacuum. This thesis is no exception. The work presented herein could not have been accomplished without the support and guidance of numerous individuals. If I attempted to cite all such persons here, I suspect that many would still be omitted, so please consider the following list to be necessary, but by no means sufficient.

I first owe a deep debt of gratitude to my advisor, Professor Robert Joynt. I was only able to be as productive as I have been due to his guidance, insight, and patience. His generosity and sense of humor further contributed to my ability to enjoy graduate school as much as I did.

I have also received remarkable assistance from other faculty. Professor Eric Bach, Professor Susan Coppersmith, and Dr. Mark Friesen were, along with Bob, the senior researchers in our quantum algorithms group, which met weekly for several years. Many of the ideas presented in this thesis originated from one or more of them. In addition to long conversations with Bob, I have spent many hours one-on-one with each of them, fine-tuning and refining my ideas and work. Five years can be a long time; I credit Bob and my other collaborators for making that time pass so quickly.

I have also benefitted greatly from collaboration with other graduate students (current and former), whether in formal group meetings or casual whiteboard discussions. Thus I owe thanks to John Gamble, Mark Wellons, Jianjia Fei, Hyungjun Lim, Danny Crow, Teck Seng Koh, and Adam Frees.

I would also like to thank Professor Lisa Everett, who served as an informal mentor over my past five years. Her advice and encouragement have proven to be invaluable.

I should also thank the members of my thesis defense committee: Professors Robert Joynt, Susan Coppersmith, Lisa Everett, Michael Winokur, and Eric Bach. Their efforts allowed me to cross the last stepping stone on my way to my doctorate.

For all of their tireless assistance, I also send thanks to several members of the UW Physics Department Staff: Ann Austin, Keeley Bannon, Dan Bradley, Rita Knox, Aimee

Lefkow, Renee Lefkow, Ian Montgomery, Steve Narf, Jim Reardon and Brett Unks. While all of them are supremely busy, not one has ever told me they lacked the time to offer help, whether to navigate the maze of university regulations, or set up a new server, or discuss the finer points of quantum mechanics, or assist in any of a myriad of other tasks.

Beyond professional associations, I owe many thanks to both friends and family. At Wisconsin, I have been fortunate enough to have many friends, too great in number to enumerate here. Lest I continue indefinitely, I will just allow myself to publicly thank those who I spent much of my recreational time with, whether playing softball, ultimate, board games, or just eating lunch - Felicity Bloom, Zack DeLand, Scott Eilerman, John Gamble, Laura Gladstone, Amanda Kruse, Marty Lichtman, Leon Maurer, Robert Mohr, Will Parker, Andrea Peterson, Walter Pettus, Bethany Reilly, Guilhem Ribeill, Andrew Schechtman-Rook, Josh Weber, Megan Wood, and Mike Wood. Beyond Wisconsin, thanks to Josh Schwartz, Josh Hancox, and Zhao He for long, enduring friendships.

I also want to thank those who, at one point or another, were a roommate of mine here. My idiosyncrasies are legion, so thanks to Martha Malin, Amanda Kruse, and Robert Mohr for putting up with them, and me.

My girlfriend of nearly four years, Becca Goldman, has been an unending source of support and love. Her impact on my time here and beyond is immeasurable.

My family in its entirety has been singularly responsible for my achievements to date. I cannot repay the generosities visited upon me by my family; I can only hope to be as generous to future generations when the opportunities present themselves. In my family, we often joke that "unconditional love" is a valid medium of exchange (e.g. "I will give you unconditional love for that piece of cake."). Joking aside, it is my parents, Nancy and David Rudinger, who taught me through their words and actions what unconditional love truly is. No finite string of words can properly capture my gratitude for that.

It is perhaps unsurprising that of all the people I know, it is my younger sister Rachel who is many ways the most similar to me. Again here I must thank my parents, for deciding that one child would not be enough. I also thank Rachel, not just for her love and support,

but the reassurance that there exist other people with similarly bent perspectives.

I additionally owe much to my aunt Ann Rudinger and uncle Ed Blazek. Not only have they been another constant source of support, but when I moved to the midwest eight years ago, they took it upon themselves to become "surrogate parents", making their house a second home to me. My cousins Jonathan and Danielle have been equally welcoming.

My grandparents also have played a significant positive role in my journey to date. While George Rudinger and Leo Levin passed away within a couple years prior to my arrival at Wisconsin, I consider myself tremendously lucky to have known both of my grandfathers during their lifetimes, and for as long as I did. That Frances Rudinger and Florence Levin continue to be a part of my life makes me luckier still. I only wish that I could have known Ellen Rudinger as well, who by all accounts was a truly remarkable woman, but as I hope these acknowledgements have demonstrated, I already have had, through no fault of my own, tremendous good fortune bestowed upon me.

Lastly, it has been said that physics is a chronic condition that runs in my family. As I now join my grandfather, father, uncle, and cousin as a recipient of an advanced physics degree, I am perhaps inclined to agree with that diagnosis. However, the choice of field of older family physicists should be considered only correlated to my choice, and not directly causal. That is, while I am sure that growing up surrounded by lovers of physics had a profound impact on me, and that I was always supported in my physics studies, I am equally confident that my family would have been no less supportive had I chosen a different path.

I'll conclude these less-than-brief remarks by thanking you, the reader. Perhaps I have known you, and perhaps I have not. Perhaps you are reading this just upon its completion, or perhaps in the distant future (though probably not). Regardless, thanks for taking a moment or two to read these words and my work. I hope my contributions contained in this thesis are helpful to you.

Kenny Rudinger

July 31, 2014

Madison, Wisconsin

For my family - past, present, and future.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

While much progress has been made since Richard Feynman first put forth the idea of a quantum computer in the 1980s, there are clear goals yet to be achieved. In terms of implementation, no universal, full-scale quantum computer has yet been constructed. On the algorithms side, while new quantum algorithms are being developed, the set of such algorithms offering any speedup (and in particular, an exponential speedup) over classical counterparts is relatively small. To these ends, this thesis examines, from a theoretical perspective, issues concerning both advances in algorithms and advances in physical implementation.

From an algorithms perspective, there is a significant desire to develop quantum algorithms that offer substantial speedup over their classical counterparts. To that end, we explore quantum algorithms for two graph-theoretic problems. We examine quantum algorithms for the graph isomorphism problem as well as for calculating the PageRank vector (a quantity used in Google's PageRank internet search algorithm).

From an experimental perspective, one necessary ingredient for full-scale quantum computing is Hamiltonian determination. While traditional quantum algorithms are implemented by manipulating time-dependent Hamiltonians (to effect the application of quantum gates), there is often an architecture-dependent "permanent" Hamiltonian which is always present and beyond the control of the experimentalist. Therefore, we propose and

examine a new method of Hamiltonian determination which takes advantage of a new signal processing technique known as compressed sensing.

1.1 Thesis outline

This thesis is organized in the following manner. The first part of the thesis explores quantum algorithms for graph-theoretic problems. Chapters 2 through 5 cover this first part. The second part of this thesis examines the problem of Hamiltonian determination; this material is presented in Chapter 6.

Chapters 2 through 4 cover quantum algorithms for the graph isomorphism problem. As described in further detail in these chapters, the graph isomorphism problem is the problem of determining whether or not two graphs (that is, networks of vertices and edges) are isomorphic, that is, if one graph can, by moving around its vertices (without breaking or adding any edges), be transformed into the other graph. The graph isomorphism problem is believed to reside in the complexity class NP-Intermediate [1]. As integer factoring is also thought to be in NP-Intermediate, the graph isomorphism problem is thought be a good candidate for a quantum speedup.

The graphs we examine are known as strongly regular graphs. The set of all strongly regular graphs, or SRGs, is partitioned using certain graph properties into collections of graphs known as families. SRGs in the same family have high degree of symmetry and are thus difficult to distinguish classically. Therefore SRGs provide a good candidate dataset for us to test our algorithms on.

In Chapter 2, we examine the power of continuous-time non-interacting multi-particle quantum random walks in distinguishing SRGs. It has been shown that single-particle [2] and non-interacting two-particle walks [3] cannot distinguish SRGs in the same family. We demonstrate in Chapter 2 that this trend does not extend to three or more particles. We first show analytically that non-interacting three-particle walks have the potential to distinguish SRGs, and then proceed to show numerically that three-particle walks can distinguish many (but not all) SRGs. We additionally show that this distinguishing power

increases with the number of particles in the walk; four-particle walks can distinguish more graphs than three-particle walks. However, we also prove that this distinguishing power is bounded in some sense. We show, by a counting argument, that given a quantum walk with any fixed number of non-interacting particles, there will exist SRGs that the walk cannot distinguish. Therefore we conclude that no continuous-time quantum random walk of a fixed number of non-interacting particles can distinguish all graphs.

In Chapter 3, we reexamine two-particle non-interacting walks, but extend our analysis to include discrete-time walks as well as continuous-time walks. While continuous-time walks of two non-interacting particles cannot distinguish same-family SRGs, it has been shown that this result does not hold for discrete-time walks of two non-interacting particles [4]; that is, discrete-time walks of two noninteracting particles can distinguish some (but not all) same-family SRGs. The origin of this difference has heretofore been an open question; in Chapter 3, we show analytically where this difference comes from. We also demonstrate that the proof technique used to derive the above-mentioned limitations of continuous-time walks of non-interacting particles cannot be extended to analogous discrete-time walks. Therefore, it is possible that there exists a non-interacting discrete-time walk with a fixed number of particles that can distinguish all strongly regular graphs.

In Chapter 4, we explore limitations of continuous-time interacting walks. It was demonstrated numerically in Ref. [3] that two-particle continuous-time walks with hard-core interactions could distinguish many SRGs. (Out of the more than 500 million pairs that were tested, not one pair was not distinguished by the two-particle hard-core walk.) These results indicated the possibility that such a walk might have universal distinguishing power, and hence pave the way for a quantum algorithm for graph isomorphism. However, it was subsequently shown in Ref. [5] that a walk with any number of hard-core particles could not distinguish all graphs. We extend these results in Chapter 4 to include arbitrary interaction schemes. We prove that walks with general interactions (when all vertices are treated equally) cannot distinguish all graphs.

In Chapter 5, we turn to a different graph-theoretic problem. We consider the task

of computing the principal eigenvector of the "Google matrix," a computation necessary to implement one of Google's search algorithms. Classically, computing this eigenvector requires a time which scales as $O(n)$, where n is the number of webpages in the World Wide Web. While in the strictest sense such a classical algorithm is "efficient", as an $O(n)$ runtime is polynomial in input size, actually performing this computation is time-intensive, owing to the large size of the web. Therefore any quantum algorithm offering a speedup in computing the principal eigenvector would be of great interest. To that end, Ref. [6] proposed an adiabatic quantum algorithm for computing this eigenvector. Their initial result indicated that their algorithm might be able to prepare a quantum state that encodes the principal eigenvector in a time of $O(\text{polylog } n)$, offering an exponential speedup. In Chapter 5 we demonstrate that this algorithm's runtime depends on features of the web that were not fully explored in Ref. [6]. We additionally show that for networks which more closely resemble the World Wide Web in degree distribution, the proposed quantum algorithm does not provide an exponential speedup.

The last part of this thesis, Chapter 6, deals with questions of quantum computing implementation. In particular, we examine the problem of determining a "fixed" Hamiltonian for a system of qubits, that is, a Hamiltonian which is always present. We find that when the number of interactions present in the Hamiltonian is significantly smaller than the full dimension (i.e. the Hamiltonian is sparse), and the temperature of the system is high enough, both the density matrix and the Hamiltonian itself may be reconstructed using a signal processing technique known as compressed sensing. We show that this procedure offers a speedup over traditional methods of quantum state tomography and Hamiltonian determination.

1.2 Publication list

The work in this thesis is presented in five chapters. The contents of Chapters 2, 3, and 5 have appeared in three separate published works, respectively. The material of Chapter 4 has not been published, and the material of Chapter 6 is at present being prepared for

publication. Additional details are as follows.

Chapter 2 is based on Ref. [7], titled *Noninteracting multiparticle quantum random walks applied to the graph isomorphism problem for strongly regular graphs*, and published in August 2012. This work was completed with John K. Gamble, Mark Wellons, Eric Bach, Mark Friesen, Robert Joynt, and Susan Coppersmith. Support for this work was provided in part by ARO, DOD (W911NF-09-1-0439), NSF (CCR-0635355), and the National Science Foundation Graduate Research Fellowship under Grant No. (DGE-0718123). Additional assistance was provided by Dong Zhou, Dan Bradley, Alessandro Fedrizzi, and Paul Hinrichs, as well as the UW-Madison HEP, Condor and CHTC groups.

Chapter 3 is based on Ref. [8], titled *Comparing algorithms for graph isomorphism using discrete- and continuous-time quantum random walks*, and published in July 2013. This work was completed with John K. Gamble, Eric Bach, Mark Friesen, Robert Joynt, and Susan Coppersmith. Support for this work was provided in part by ARO, DOD (W911NF-09-1-0439), NSF (CCR-0635355). Additional assistance was provided by Jingbo Wang and Adam Frees.

Chapter 4 is based on unpublished work. This work was performed in Spring and Summer of 2012, and was completed with John K. Gamble, Eric Bach, Mark Friesen, Robert Joynt, and Susan Coppersmith. Additional assistance was provided by Jamie Smith.

Chapter 5 is based on Ref. [9], titled *Power law scaling for the adiabatic algorithm for search engine ranking*, and published in September of 2013. This work was completed with Adam Frees, John King Gamble, Eric Bach, Mark Friesen, Robert Joynt, and Susan Coppersmith. Support for this work was provided in part by ARO, DOD (W911NF-09-1-0439), and NSF (CCR-0635355, DMR 0906951, PHY-PIF-1104660). Additional assistance was provided by Silvano Garnerone, Daniel Lidar, and Dan Bradley, as well as the UW-Madison HEP, Condor and CHTC groups.

Chapter 6 is based on unpublished work. This work was performed from Fall of 2013 through Spring of 2014, and was completed with Robert Joynt. Additional assistance was provided by Susan Coppersmith, Eric Bach, Mark Friesen, John K. Gamble, Robin Blume-

Kohout, Adam Frees, Daniel Crow, Amir Kalev, and Charles Baldwin.

Lastly, a note to the reader. Most chapters in this thesis are designed to be comprehensible independent of the other chapters. The two exceptions are Chapters 3 and 4; it is recommended that the reader be familiar with the concepts of Chapter 2 before working through either Chapter 3 or 4 (though Chapter 3 need not be read before Chapter 4).

Chapter 2

Non-interacting multi-particle quantum random walks applied to the graph isomorphism problem for strongly regular graphs

2.1 Introduction

There has long been interest in algorithms that use random walks to solve a variety of mathematical and scientific problems [10, 11, 12, 13, 14]. Typically, the random walks in question have been classical random walks (CRWs). However, there is increasing interest in random walks with quantum walkers. In particular settings, these quantum random walks (QRWs) have been shown to have computational advantages over CRWs [15, 16, 17]. Certain algorithms utilizing QRWs have been proven to have faster runtimes than their best known classical counterparts [18, 19, 20, 21, 22, 23, 24].

Additionally, QRWs have been experimentally demonstrated in a variety of physical settings, such as ion traps [25], atom traps [26], quantum optics [27, 28], and NMR systems [29]. Recent works have experimentally realized QRWs with two walkers, demonstrating the

potential for implementing QRWs with many walkers [30, 31, 32, 33]. Moreover, there are proposed methods for physically implementing non-trivial walks [34], indicating that there may be many QRW algorithms to be developed that would both be physically realizable and computationally powerful.

Often the context for QRWs is one in which the walks occur on graphs. It has been shown that QRWs are universal; any quantum algorithm can be mapped onto a QRW on such a graph [35]. It is also the case that many interesting computational problems are easily expressed in graph theoretic terms [3]. Thus there is considerable interest in further exploring QRWs on graphs, with the hope that we may be able to use such a framework to solve certain problems.

There are also interesting physical phenomena associated with many particles walking on a graph. It is known that QRWs of non-interacting bosons on graphs can give rise to effective statistical interactions [36, 37, 38]. It has even been shown that Bose-Einstein condensation can occur at finite temperature in less than two dimensions if the bosons are placed on a particular kind of graph [38]. Therefore, there is motivation in further exploring the dynamics of multi-particle ensembles on graphs.

This chapter, along with Chapters 3 and 4, addresses the graph isomorphism problem, which is, given two graphs, to determine if they are isomorphic; that is, if one can be transformed into the other by a relabeling of vertices. This problem is of note for several reasons. While many graph pairs may be distinguished by a classical algorithm which runs in a time polynomial in the number of vertices of the graphs, there exist pairs which are computationally difficult to distinguish. Currently, the best classical algorithm for general graphs has a runtime of $O(c^{\sqrt{N}\log N})$, where c is a constant and N is the number of vertices in the two graphs [39]. Graph isomorphism (GI) is believed to be similar to factoring in that both are thought to be NP-Intermediate problems [1]. Additionally, both problems may be approached as hidden subgroup problems, though this approach has had limited success for GI [40]. Due to these similarities, and the known quantum speedup available for factoring [41], there is hope that there similarly exists a quantum speedup for GI.

Strongly regular graphs (SRGs) are a particular class of graphs that are difficult to distinguish classically [39]. (See Section 2.2 for a formal definition.) Shiau *et al.* showed that the single-particle continuous-time QRW fails to distinguish pairs of SRGs with the same family parameters [2]. Gamble *et al.* extended these results, proving that QRWs of two non-interacting particles will always fail to distinguish pairs of non-isomorphic strongly regular graphs with the same family parameters [3]. They also demonstrated numerically the distinguishing power of the two-boson interacting QRW; it successfully distinguished all tested pairs of SRGs [3]. Since the publication of Gamble *et al.*, Smith proved that for any fixed number of bosons p, there exist non-isomorphic graph pairs which the p-boson interacting walk fails to distinguish [5]. These counterexample graphs are not strongly regular; whether or not the two-boson interacting walk successfully distinguishes all non-isomorphic strongly regular graphs is still an open question.

Investigations into discrete-time QRW algorithms for GI have also been made [42, 43, 4]. Berry and Wang numerically showed that a discrete-time non-interacting QRW of two particles could distinguish some SRGs, something its continuous-time counterpart cannot do. However, this distinguishing power is not universal on SRGs, nor is an analytic explanation of the distinguishing power given [4]. The discrete-time algorithm proposed by Emms *et al.* successfully distinguished all tested SRGs [42], but it has been shown to not be universal [5]; it is unknown if it is universal on SRGs. Additionally, for the same number of particles, the discrete-time QRWs require Hilbert spaces larger than the ones required by continuous-time QRWs [4]. In an effort to relate discrete-time and continuous-time QRWs, it has been noted that the coin state of a discrete-time walk may be thought of as a relativistic particle's internal degree of freedom; such a feature is absent from continuous-time QRWs [44]. The relationship between discrete-time and continuous-time quantum random walks in the context of the graph isomorphism problem has been examined as well; we discuss certain aspects of this relationship in Chapter 3. It remains an open question as to whether or not discrete-time walks in general have fundamentally greater distinguishing power than continuous-time walks, or if they are better candidates for a universal GI algorithm.

This chapter extends the results of [3] to address continuous-time multi-particle non-interacting quantum walks on SRGs, with a particular focus on understanding the role of particle number in determining the distinguishing power of the walks. We have several main results. We numerically demonstrate that three-particle non-interacting walks have significant (but not universal) distinguishing power on hard-to-distinguish pairs of SRGs. Additionally, we find that a four-fermion non-interacting walk has even greater (but still not universal) distinguishing power on SRG pairs. We analytically explain where this distinguishing power comes from, and how these multi-particle non-interacting walks are fundamentally different from single-particle and two-particle non-interacting walks. This is done by showing that a particular feature present in the smaller walks which limits their distinguishing power is not present in walks of three or more non-interacting particles. Further, we analytically show that, even though the distinguishing power of non-interacting walks increases with particle number, there is no non-interacting walk with a fixed number of particles that can, with our comparison algorithm, distinguish all strongly regular graphs.

This chapter is organized as follows. Section 2.2 covers the requisite background, including graph theoretic definitions and concepts, a review of strongly regular graphs, and a formal definition of the quantum random walk. In Section 2.3, we first demonstrate analytically how two-particle non-interacting walks are fundamentally different from three-particle non-interacting walks. We then present the numerical results for non-interacting three-particle and four-particle walks on SRGs. In the final part of Section 2.3, we demonstrate that a p-particle non-interacting QRW cannot distinguish all SRGs for any fixed p. We discuss our conclusions in Section 2.4.

Appendix A discusses a fundamental difference between non-interacting walks of two particles and non-interacting walks of more than two particles. Appendix B provides details necessary to show that a non-interacting p-particle walk cannot distinguish all SRGs for a fixed p. In Appendix C, we show that the number of unique evolution operator elements for a p-particle non-interacting walk is super-exponential in p. Lastly, we explain in Appendix D how we ensure numerical stability and determine numerical error in our simulations.

2.2 Background

Basic Graph Definitions

Here we develop the background and definitions necessary to discuss multi-particle QRWs on graphs. This chapter only considers simple, undirected graphs. A graph $G = (V, E)$ is a set of vertices V and edges E. The vertices are a set of labels, usually integers, and the edges are a list of unordered pairs of vertices. If a pair of vertices appears in E, then the vertices are connected by an edge; otherwise there is no edge between the vertices and they are considered disconnected. The terms "adjacent", "neighboring", and "connected" may be used interchangeably to refer to a vertex pair which shares an edge. It is convenient to represent a graph by its adjacency matrix $\mathbf{A}$, defined as:

$$A_{ij} = \begin{cases} 1 & \text{if vertices } i \text{ and } j \text{ are connected.} \\ 0 & \text{if vertices } i \text{ and } j \text{ are disconnected.} \end{cases} \tag{2.1}$$

A graph of N vertices has an $N \times N$ adjacency matrix. For the undirected and simple graphs considered here, $\mathbf{A}$ is symmetric, with zeros on the diagonal.

Two graphs are isomorphic if one graph is transformed into the other by a relabeling of vertices. More formally, given two adjacency matrices $\mathbf{A}$ and $\mathbf{B}$, the graphs represented by $\mathbf{A}$ and $\mathbf{B}$ are isomorphic if and only if a permutation matrix $\mathbf{P}$ exists such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$.

Strongly Regular Graphs

This chapter addresses strongly regular graphs (SRGs), which we examine because they are difficult to distinguish classically, and because of their simple algebraic properties [39, 45]. An SRG is characterized by four parameters, denoted (N, k, λ, μ). N is the number of vertices in the graph, and each vertex is connected to k other vertices (the graph is k-regular, or has degree k). Each pair of neighboring vertices shares λ common neighbors, while each pair of non-adjacent vertices shares μ common neighbors. The set of SRGs sharing the same set of four parameters is referred to as an SRG *family*; correspondingly, the four parameters are often called the family parameters. While some SRG families may

have only one non-isomorphic member, there are many families of SRGs with multiple non-isomorphic graphs. These are the families which are of interest to us.

The adjacency matrix of any SRG has at most three eigenvalues. As these eigenvalues and their multiplicities are functions of the family parameters, the adjacency matrices of SRGs in the same family are always cospectral [45]. This contributes to the difficulty of distinguishing non-isomorphic SRGs.

The adjacency matrix of any SRG satisfies the particularly useful algebraic identity [45]:

$$\mathbf{A}^2 = (k-\mu)\mathbb{1} + \mu\mathbf{J} + (\lambda-\mu)\mathbf{A}, \tag{2.2}$$

where $\mathbb{1}$ is the identity and $\mathbf{J}$ is the matrix of all ones. Because $\mathbf{J}^2 = N\mathbf{J}$, $\mathbf{JA} = \mathbf{AJ} = k\mathbf{A}$, and $\mathbb{1}$ acts trivially on $\mathbb{1}$, $\mathbf{J}$, and $\mathbf{A}$, we see that $\{\mathbb{1}, \mathbf{J}, \mathbf{A}\}$ forms a commutative three-dimensional algebra, so we conclude that for any positive integer n:

$$\mathbf{A}^n = \alpha_n\mathbb{1} + \beta_n\mathbf{J} + \gamma_n\mathbf{A}, \tag{2.3}$$

where α_n, β_n, and γ_n depend only on n and the family parameters.

Defining the quantum random walk

Now we discuss how we form a continuous-time non-interacting quantum random walk on a graph. As in [3], we use the Hubbard model, where each site corresponds to a graph vertex. A particle can move from one vertex to another if the two vertices are connected. Thus, for a graph on N vertices with adjacency matrix $\mathbf{A}$, our non-interacting Hamiltonian is given by

$$\mathbf{H} = -\sum_{i,j}^{N} A_{ij} c_i^\dagger c_j, \tag{2.4}$$

where $c_i^\dagger$ and c_i are the creation and annihilation operators, respectively, for a boson or (spinless) fermion at site i. For bosons, they satisfy the commutation relations $[c_i, c_j^\dagger] = \delta_{ij}$ and $[c_i, c_j] = [c_i^\dagger, c_j^\dagger] = 0$. For fermions, they satisfy the anti-commutation relations $\{c_i, c_j^\dagger\} = \delta_{ij}$ and $\{c_i, c_j\} = \{c_i^\dagger, c_j^\dagger\} = 0$.

For walks of p bosons, we use basis states of the form $|j_1 \dots j_p\rangle_B$, which is the appropriately symmetrized basis state with bosons on vertices j_1 through j_p. These vertices need not

be distinct, since vertices may be multiply occupied. Similarly, for walks of p fermions, we use basis states of the form $|j_1 \dots j_p\rangle_F$, which is the appropriately anti-symmetrized basis state with fermions on vertices j_1 through j_p. These vertices must be distinct, because the Pauli exclusion principle implies that no vertex can be occupied by multiple fermions. We refer to these bases as the particles-on-vertices bases.

Following [3] and [5], it is straightforward to show that the elements of the p-boson or p-fermion non-interacting Hamiltonian ($\mathbf{H}_{p,B}$ and $\mathbf{H}_{p,F}$, respectively) are, in their respective particles-on-vertices bases:

$$\begin{aligned} {}_B\langle i_1 \dots i_p|\mathbf{H}_{p,B}|j_1 \dots j_p\rangle_B = \\ -{}_B\langle i_1 \dots i_p|\mathbf{A}^{\oplus p}|j_1 \dots j_p\rangle_B, \end{aligned} \tag{2.5}$$

$$\begin{aligned} {}_F\langle i_1 \dots i_p|\mathbf{H}_{p,F}|j_1 \dots j_p\rangle_F = \\ {}_F\langle i_1 \dots i_p|\mathbf{A}^{\oplus p}|j_1 \dots j_p\rangle_F, \end{aligned} \tag{2.6}$$

where

$$\begin{aligned} \mathbf{A}^{\oplus p} = \underbrace{\mathbf{A} \otimes \mathbb{1} \otimes \mathbb{1} \dots \otimes \mathbb{1}}_{p} \\ + \mathbb{1} \otimes \mathbf{A} \otimes \mathbb{1} \dots \otimes \mathbb{1} + \dots + \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \dots \otimes \mathbf{A}. \end{aligned} \tag{2.7}$$

The evolution operator is defined in the standard manner:

$$\mathbf{U}(t) = e^{-it\mathbf{H}}, \tag{2.8}$$

where $\hbar = 1$ for convenience.

Comparison algorithm

Our method for comparing two graphs in an attempt to determine if they are isomorphic or not is the same as the one used in [3]. Given two graphs with adjacency matrices $\mathbf{A}$ and $\mathbf{B}$, we compute in the particles-on-vertices basis $\mathbf{U_A}(t)$ and $\mathbf{U_B}(t)$, respectively, for the same number and type of particle, as well as the same time t. The absolute value of each element

of $\mathbf{U_A}(t)$ and $\mathbf{U_B}(t)$ are written to lists $\mathbf{X_A}$ and $\mathbf{X_B}$, respectively. Both lists are sorted, and we compute the distance between the lists, Δ:

$$\Delta = \sum_{\nu} |\mathbf{X_A}[\nu] - \mathbf{X_B}[\nu]|. \tag{2.9}$$

We say that $\mathbf{A}$ and $\mathbf{B}$ are distinguished by a particular walk if and only if that walk yields $\Delta \neq 0$; isomorphic graphs and non-isomorphic non-distinguished graphs both yield $\Delta = 0$ [3]. We note that we lose phase information by taking the absolute value of the elements, but it makes our comparison procedure more tractable, and seems to do no harm, see [3]. Lastly, for all simulations presented in this chapter, $t = 1$.

2.3 Quantum random walks on strongly regular graphs

Comparing distinguishing power of two- and three-particle non-interacting walks

In this subsection we show analytically that there is a fundamental difference between two-particle non-interacting walks and three-particle non-interacting walks on strongly regular graphs, because three-particle non-interacting walks are capable of distinguishing SRGs from the same family, unlike two-particle non-interacting walks. To show this difference, we recall the proof used by Gamble *et al.* to demonstrate the inadequacy of two-particle walks [3].

The proof in Gamble *et al.* first shows that the value of every element in the two-particle evolution operators (${}_B\langle ij|\mathbf{U}_{2B}(t)|kl\rangle_B$ or ${}_F\langle ij|\mathbf{U}_{2F}(t)|kl\rangle_F$) must be a function only of the SRG family parameters and the time t. Then it is shown that the multiplicity of each element value in the evolution operator is also a function of SRG family parameters. We begin similarly here for the three-particle walk, and find that while the values of the elements are all functions of the SRG family parameters, the multiplicities of the values are not.

We first address the element values. We refer to each element of each evolution operator (computed in the particles-on-vertices basis) as a *Green's function*, following the nomenclature of Gamble *et al.* [3]. Because the three-particle walk in question is non-interacting, we

know that the evolution operator for the walk factorizes into three single-particle evolution operators:

$$ {}_B\langle ijk|\mathbf{U}_{3B}|lmn\rangle_B = {}_B\langle ijk|{\mathbf{U}_{1P}}^{\otimes 3}|lmn\rangle_B, \tag{2.10} $$

$$ {}_F\langle ijk|\mathbf{U}_{3F}|lmn\rangle_F = {}_F\langle ijk|\overline{\mathbf{U}_{1P}}^{\otimes 3}|lmn\rangle_F, \tag{2.11} $$

where ${\mathbf{U}_{1P}}^{\otimes 3} = \mathbf{U}_{1P} \otimes \mathbf{U}_{1P} \otimes \mathbf{U}_{1P}$; $\mathbf{U}_{1P}$ is the evolution operator for the single-particle walk, that is, $\mathbf{U}_{1P} = e^{i\mathbf{A}t}$ and $\overline{\mathbf{U_{1P}}} = e^{-i\mathbf{A}t}$.

Recalling Eq. (2.3), and expanding $e^{i\mathbf{A}t}$ as a Taylor series in powers of $\mathbf{A}t$, we note that:

$$ \mathbf{U}_{1P} = \alpha\mathbb{1} + \beta\mathbf{J} + \gamma\mathbf{A}, \tag{2.12} $$

where α, β, and γ are functions of the family parameters and the time t. Therefore, we conclude that all possible values of the elements of $\mathbf{U}_{3B}$ and $\mathbf{U}_{3F}$ (the Green's functions) are determined by the family parameters. Thus, the set of all potential values for the Green's functions are the same for any two graphs in the same family. Any distinguishing power of the walks must come from the existence of at least one Green's function with different *multiplicities* for non-isomorphic graphs in the same family.

Gamble *et al.*, prove that the multiplicity of each Green's function for two-particle non-interacting walks is a function of the SRG family parameters. In Appendix A, we show that there exist Green's functions for the three-particle non-interacting walk on SRGs whose multiplicities are *not* functions of the family parameters. This is because the multiplicity of a Green's function in a p-particle walk depends on how many shared neighbors a collection of up to p vertices has. For $p = 2$, strong regularity uniquely determines the number of shared neighbors: λ if the vertices are connected, and μ if they are not. However, for $p \geq 3$, the multiplicity is dependent on the number of shared neighbors among sets of p vertices. Thus the multiplicity is not uniquely determined by strong regularity, so the multiplicity for such a Green's function need not be a function of the family parameters.

The definition of SRGs does not directly constrain the number of neighbors of a set of p vertices with $p \geq 3$. However, this difference from the two-particle case does not guarantee that walks of three or more particles can distinguish non-isomorphic SRGs, only that they

have the potential to do so. Our numerical investigations of the distinguishing power of these walks are presented in Section 2.3.

Numerical results

Table 2.1: Numerical results for the three-particle non-interacting walks on twelve families of SRGs. The first column lists the family parameters for the particular SRG family being examined. The second column lists the number of graphs in the family that we compared. This number is equal to the number of graphs in the family, with the exception of (49,18,7,6), where we only examined a subset of the family. The third column gives the number of comparisons made for each family, which is equal to the number of graphs in that family that we examined choose 2. The fourth and fifth columns list the number of graph pairs which the three-boson and three-fermion walks fail to distinguish, respectively. We see that out of 70 712 graph comparisons, both the boson and fermion walks fail a total of 256 times, corresponding to a success rate of greater than 99.6%

SRG Family (N, k, λ, μ)	Number of Graphs	Comparisons	Boson Failures	Fermion Failures
(16, 6, 2, 2)	2	1	0	0
(16, 9, 4, 6)	2	1	0	0
(25, 12, 5, 6)	15	105	0	0
(26, 10, 3, 4)	10	45	1	1
(28, 12, 6, 4)	4	6	0	0
(29, 14, 6, 7)	41	820	0	0
(35, 18, 9, 9)	227	25651	38	38
(36, 14, 4, 6)	180	16110	89	89
(40, 12, 2, 4)	28	378	8	8
(45, 12, 3, 3)	78	3003	7	7
(49, 18, 7, 6)	147	10731	21	21
(64, 18, 2, 6)	167	13861	92	92

Table 2.2: Numerical results for four-fermion non-interacting walks on 136 graph pairs that are not distinguished by three-particle non-interacting walks. Of the 136 graph pairs tested, only one pair is not successfully distinguished. We therefore see that increasing the number of non-interacting particles beyond three continues to increase the distinguishing power of the non-interacting QRWs.

Family (N, k, λ, μ)	3 Particle Failures	4 Fermion Failures
(26, 10, 3, 4)	1	0
(35, 18, 9, 9)	38	0
(36, 14, 4, 6)	89	1
(40, 12, 2, 4)	8	0

In this subsection, we present our numerical results for three-particle and four-fermion walks on SRGs. To simulate a walk on a graph, we compute the appropriate Hamiltonian

and exponentiate it to compute its corresponding evolution operator, following the algorithm described in Section 2.2. Then, to compare pairs of non-isomorphic graphs from the same family, we compute the list distance Δ, defined in Equation (2.9). We find our error on Δ to be no greater than 10^{-6}, so two non-isomorphic graphs are considered distinguished if and only if $\Delta > 10^{-6}$. Further details of numerical error analysis are provided in Appendix D.

Because the Hamiltonians are very large, we must use a sparse matrix exponentiation routine [46] to make exponentiation computationally tractable. (The largest evolution operators we compute have a dimension of 91 390, and correspond to the four-fermion walks on graphs of 40 vertices.) Additionally, in order to be able perform these exponentiations sufficiently quickly, we parallelize the computations, utilizing the Open Science Grid and the University of Wisconsin-Madison's Center for High Throughput Computing Cluster.

Our numerical results for three-particle walks are presented in Table 2.1. For the 70 712 pairs of SRGs compared, the boson and fermion walks distinguish all but 256 pairs, corresponding to a success rate of greater than 99.6%. Thus we see that both the three-boson and three-fermion walks have significant (but not universal) distinguishing power on SRGs, while the two-particle non-interacting walks fail on *all* pairs of non-isomorphic graphs in the same family [3].

The bosonic and fermionic walks fail to distinguish the same pairs of non-isomorphic graphs that we tested; we have found no graph pair that one kind of particle successfully distinguishes while the other does not. Thus, despite having a state space of smaller dimension (due to Pauli exclusion), the three-fermion walk has the same distinguishing power as the three-boson walk on all tested graph pairs. It remains an open question whether graph pairs exist for which this is not true.

Having identified some graph pairs that three non-interacting particles fail to distinguish, we want to know if non-interacting walks exist that can distinguish these graphs. However, it is computationally expensive (even with speedup provided by parallelization) to simulate four-particle walks. We therefore simulated only fermion walks, and only on

a subset of the three-particle counterexample graph pairs. Our results are summarized in Table 2.2. We simulated four-fermion non-interacting walks on 136 counterexample pairs, finding that all but one pair are distinguished.

Since increasing the number of non-interacting particles in the walk apparently increases the distinguishing power, it is natural to ask "Does there exist a p such that the p-particle non-interacting walk can distinguish all strongly regular graphs?" The next subsection shows that the answer to this question is no.

Limitations of non-interacting walks

In this subsection, we show that pairs of non-isomorphic strongly regular graphs exist that are not distinguished by any p-particle non-interacting quantum walk with fixed p in conjunction with the comparison algorithm described by Equation (2.9). This is because for a fixed p, there exists an N such that the number of strongly regular graphs with N vertices is larger than the maximum number of graphs distinguishable by the p-particle non-interacting walk.

To prove this claim, we define $S(N)$, the number of strongly regular graphs in a particular family with N vertices, and $Z(p, N)$, the number of distinct "graph fingerprints" that the p-boson walk can generate for an SRG family whose graphs have N vertices. By a "graph fingerprint," we mean a sorted list of the absolute value of every element of an evolution operator (Eq. (2.10)). We examine the boson walk here, because its state space is strictly larger than the fermion walk of the same number of particles. Thus the p-boson walk generates more fingerprints than the p-fermion walk (even though we have seen no evidence yet that it distinguishes more graph pairs). Therefore, $Z(p, N)$ bounds from above the maximum number of SRGs with N vertices in a particular family that non-interacting walks of either p fermions or bosons can distinguish.

We now define the ratio $R(p, N)$:

$$R(p, N) = \frac{S(N)}{Z(p, N)}. \tag{2.13}$$

We will show that for any fixed p, R is greater than 1 for large enough N, thus demonstrating that there exist more SRGs than the p-particle walk can distinguish.

It is shown in [47] that there is a mapping between Latin squares of size n and SRGs of size n^2 with family parameters $(n^2, 3(n-1), n, 6)$. The results of [48, 47], imply that when N is large enough, the number of non-isomorphic Latin square SRGs of size N is bounded below by:

$$S(N) \geq \frac{1}{6}(\sqrt{N}!)^{2\sqrt{N}-3} N^{\frac{-N}{2}}. \tag{2.14}$$

As for $Z(p, N)$, we show in Appendix B that for a fixed p, Z satisfies the inequality:

$$Z(p, N) < N^{2X_p(p+1)}, \tag{2.15}$$

where X_p is the number of unique values a Green's function for a p-boson walk can assume. While it can be shown that X_p is super-exponential in p, it does not depend on N. This is because the value of a Green's function for a non-interacting p-particle QRW on an SRG is determined by a configuration of up to $2p$ vertices in that SRG, as discussed in Section 2.3 and Appendix A.

To examine the behavior of R in the limit of large N, we use Stirling's formula:

$$x! = \sqrt{2\pi} e^{-x} x^{x+1/2}(1 + O(x^{-1})). \tag{2.16}$$

This allows us compute a lower-bound for R in the limit of large N:

$$\lim_{N\to\infty} R \geq \frac{1}{6}(2\pi)^{\sqrt{N}-\frac{3}{2}} e^{-2N+3\sqrt{N}} N^{\frac{N}{2}-\sqrt{N}-\frac{3}{4}-2X_p(p+1)}. \tag{2.17}$$

Taking the logarithm of Eq. (2.17) yields:

$$\lim_{N\to\infty} \log R(p, N) \geq \lim_{N\to\infty} \frac{N}{2} \log N + O(N), \tag{2.18}$$

which diverges as $N \to \infty$. Therefore, for a fixed p, R approaches ∞ as N increases, showing that no p-particle non-interacting walk can distinguish all SRGs.

One can let p grow slightly with N and achieve the same result. Indeed, we show in Appendix C that

$$\log_2(X_p) = p^2 + O(p \log p). \tag{2.19}$$

Using this, we find our argument remains valid for $p < C\sqrt{\log_2 N}$, for any $C < 1$.

We can contrast these results to those of Gamble *et al.*. They found that the hard-core two-boson walk distinguished all graph pairs in a dataset of over 500 million pairs of SRGs [3]. This distinguishing power was shown to arise from an underlying algebra that is fundamentally different than that of the noninteracting two-boson or two-fermion walks. As we see no obvious way to extend the proof presented in this section to include hard-core walks, it is an open question as to whether or not the two-boson hard-core walk has universal distinguishing power on SRGs. Even if does not, it is still possible that there exists a fixed $p > 2$ such that the p-boson hard-core walk could distinguish all SRGs. If this is the case, then this would be a marked difference between the non-interacting and hard-core walks.

2.4 Discussion

We have shown how three-particle non-interacting quantum random walks are qualitatively different from two-particle non-interacting quantum random walks; the latter will always fail to distinguish non-isomorphic strongly regular graphs from the same family, whereas the former successfully distinguish many (but not all) non-isomorphic pairs of strongly regular graphs. We have analytically identified a fundamental difference between these two classes of quantum walks. The three-particle walks have potential distinguishing power because the shared connectivity of triples of vertices in SRGs is not governed by the SRG family parameters. We have also demonstrated numerically that three-particle non-interacting walks have significant, but not universal, distinguishing power on SRGs. We observe numerically that bosonic and fermionic walks distinguish the same pairs of non-isomorphic pairs of graphs. Increasing the number of non-interacting fermions to four further increases distinguishing power. However, this distinguishing power is not limitless; we have shown that for any fixed number of non-interacting particles, there exist non-isomorphic pairs of SRGs that cannot be distinguished.

Lastly, we discuss the implications of these results in terms of the computational com-

plexity of the graph isomorphism problem. Not only are there graph pairs on which the three- and four-particle walks fail, but we know that for any fixed particle number, there will be SRGs that such non-interacting walks cannot distinguish. It is still possible that, given any non-isomorphic SRG pair of a fixed size N, there exists a p such that the p-particle non-interacting walk will succeed in distinguishing the graphs. However, the lower bound given at the end of Section 2.3 rules out the possibility of our algorithm providing a classical polynomial-time solution to GI for SRGs.

2.5 Appendices

A. Computing multiplicities of values of matrix elements of the evolution operator for strongly regular graphs

Here we discuss how to compute the multiplicities of values of elements of evolution operators, or Green's functions, for SRGs. We show in this appendix that the multiplicity of a non-interacting three-particle Green's function is in general not a function of SRG family parameters. This result is used in Section 2.3 to demonstrate how two-particle and three-particle non-interacting walks have different distinguishing powers for SRGs.

To compute the multiplicity of each value of the Green's function in a non-interacting three-particle walk, we first note that Eqs. (2.10) through (2.12) imply that the value of a given Green's function depends on the relationships between the vertices in the final state (the bra; $\{i, j, k\}$) and the vertices in the initial state (the ket; $\{p, q, r\}$). For each pair of indices (x, y), with x from the bra ($x \in \{i, j, k\}$), and y from the ket ($y \in \{p, q, r\}$), there are three possible relations. The vertices can be connected ($A_{xy} = 1$), the vertices can be the same ($\delta_{xy} = 1$), or the vertices can be different and disconnected ($A_{xy} = \delta_{xy} = 0$). Therefore, we may think of each Green's function as corresponding to a generalized subgraph of the original graph. We say "generalized subgraph" because the Green's function is unaffected by internal connections within the initial or final state; we adopt the more compact terminology of referring to these generalized subgraphs as "widgets."

To illustrate this point, let us consider the widget shown in Figure 2.1. The solid lines in the widget indicate that the sites are connected in the graph, while the dashed lines indicate that the value of the widget does not depend on whether or not those sites are connected. Thus, two widgets are considered the same whether or not sites that are connected by dashed lines are actually adjacent. To evaluate ${}_B\langle ijk|\mathbf{U}_{3B}|pqr\rangle_B$ for the widget shown in Figure 2.1, we note that all six vertices ($\{i,j,k,l,p,q,r\}$) are distinct. We can then use Eqs. (2.10) and (2.12) to find that ${}_B\langle ijk|\mathbf{U}_{3B}|pqr\rangle_B = 6(\beta+\gamma)^3$, where β and γ, defined in (2.12), are functions of the SRG family parameters. The multiplicity of this particular value for a particular graph is given by the number of times its corresponding widget occurs in the graph.

To compute the multiplicity, M, of $6(\beta+\gamma)^3$ in $\mathbf{U}_{3B}$, we count the number of occurrences of this widget in the graph. To do this, we perform the following combinatorial sum, generalizing the procedure outlined in Appendix B of Gamble *et al.* [3].

$$\begin{aligned} M &= \sum_{i<j<k} \sum_{p<q<r} A_{ip}A_{iq}A_{ir}A_{jp}A_{jq}A_{jr}A_{kp}A_{kq}A_{kr} \\ &= \frac{1}{36} \sum_{ijkpqr} A_{ip}A_{iq}A_{ir}A_{jp}A_{jq}A_{jr}A_{kp}A_{kq}A_{kr} \times \\ &\quad (1-\delta_{ij})(1-\delta_{ik})(1-\delta_{jk})(1-\delta_{pq})(1-\delta_{pr})(1-\delta_{qr}). \end{aligned} \tag{2.20}$$

The analogous sums considered in Gamble *et al.*, which only examines two-particle walks, can be decomposed into sums and traces over powers of the adjacency matrix. Such operations are given by contracting over two occurrences of the same index in the summand. Conveniently, these quantities are expressible in terms of SRG family parameters. Things are not so simple, however, for the three-particle walks. By inspection, we see that Eq. 2.20 contains contractions over three occurrences of the same index. Such contractions correspond to neither matrix multiplication nor computing the trace, and cannot in general be massaged into forms expressible in terms of SRG family parameters, as evidenced by the fact that the three-particle walks have distinguishing power over many pairs of SRGs.

However, the above statement does not give us analytic proof that there exist Green's functions whose multiplicities are not functions of the family parameters; up to this point,

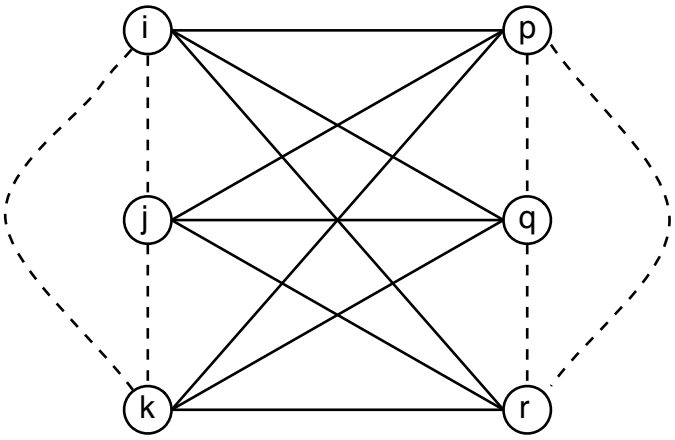

Figure 2.1: Sketch of a generalized subgraph, or "widget," used to calculate the values and degeneracy of a Green's function for a three-particle quantum walk on an SRG. The vertices on the right side correspond to the vertices the particles are on to begin with (the ket $|pqr\rangle_B$ or $|pqr\rangle_F$), and the vertices on the left side correspond to the vertices the particles end up on (the bra ${}_B\langle ijk|$ or ${}_F\langle ijk|$), after application of the evolution operator U. A solid line between vertices x and y indicate that $A_{xy} = 1$. A dashed line between x and y means that the value of A_{xy} does not affect the value of the Green's function. Thus, for bosons, the depicted widget corresponds to the Green's function ${}_B\langle ijk|\mathbf{U}_{3B}|pqr\rangle_B$ when all six vertices are distinct, and when $A_{xy} = 1$ for all $x \in \{i, j, k\}$ and $y \in \{p, q, r\}$. Eqs. (2.10) and (2.12) show that the value of this Green's function, or widget, is ${}_B\langle ijk|\mathbf{U}_{3B}|pqr\rangle_B = 6(\beta + \gamma)^3$.

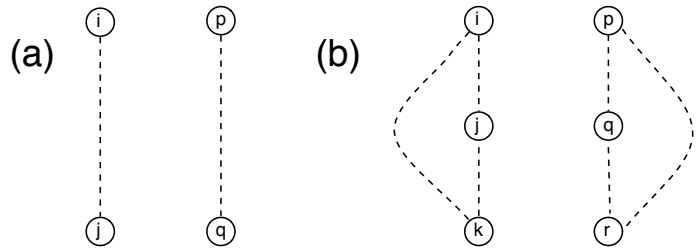

Figure 2.2: Empty widgets for two-particle and three-particle non-interacting walks. In both widgets, all vertices are distinct and no vertex in the initial state is adjacent to any vertex in the final state. The values of the widgets depend only on the family parameters for both (a) and (b), while the degeneracies of these values depend only on family parameters for two particles but not for three. The multiplicity of each widget's respective Green's function for a particular SRG is equal to the number of times that widget appears in the SRG. (a) The empty widget for two particles. The number of times this widget appears in an SRG is a function of the SRG family parameters, as is the case for all two-particle widgets [3]. (b) The empty widget for three particles. The number of times this widget appears in an SRG is *not* a function solely of SRG family parameters. This is demonstrated by the graphs in Figure 2.3. An analytic explanation for this phenomenon is given in the text following Equation (2.21).

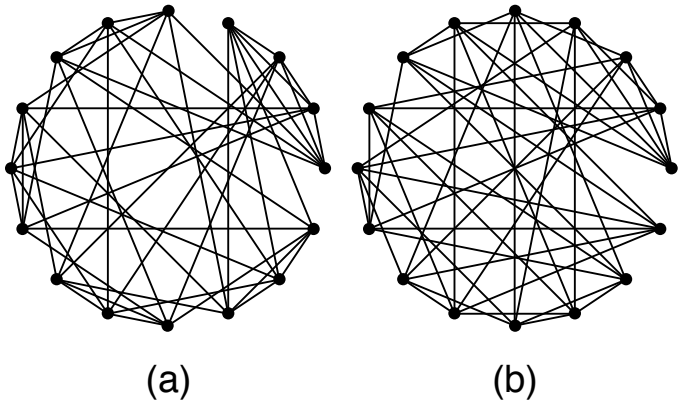

Figure 2.3: The two non-isomorphic graphs of the SRG family (16,6,2,2). The widget of Figure 2.2(b) appears in the graph shown in (a) 608 times, whereas the same widget appears in the graph shown in (b) 512 times. Thus we see that the same three-particle widget can have different multiplicities in graphs of the same family, so the three-particle non-interacting walk can distinguish at least some non-isomorphic graphs from the same SRG family.

we are still relying on the numerical results as proof. Below, we analytically demonstrate that there exist widgets whose multiplicities *cannot* be determined by family parameters. To demonstrate this, we take a step back to the two-particle walk. Consider the widget shown in Figure 2.2(a). We can determine this widget's multiplicity for an arbitrary SRG with family parameters (N, k, λ, μ) by performing the combinatorial sum analogous to Equation (2.20), or equivalently, we can actually count the number of times we can fit this widget on the SRG. To begin, we pick two sites in the graph to serve as sites i and j; these sites may be adjacent or not, as indicated by the dashed line between them in the figure. Now we must count, given our choice of i and j, how many sites we may pick as p and q. If i and j are connected, there are $\binom{N-2k+\lambda}{2}$ choices for p and q, whereas if i and j are disconnected, there are $\binom{N-2-2k+\mu}{2}$ choices for p and q. There are $\frac{Nk}{2}$ choices for connected sites that can serve as i and j, and $\binom{N}{2} - \frac{Nk}{2}$ disconnected sites. Thus, the number of four-vertex empty

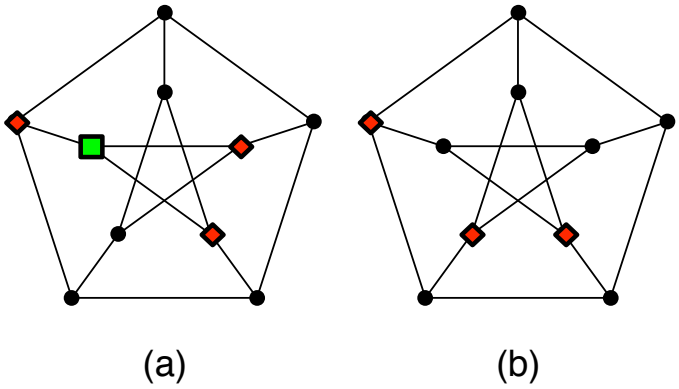

Figure 2.4: Two copies of the Petersen graph, an SRG with parameters $(10, 3, 0, 1)$. In each graph, three mutually non-adjacent vertices are highlighted as red diamonds. In (a), the three vertices share one common neighbor, marked as a green square. In (b), the three vertices share no common neighbors. This demonstrates that the number of neighbors common to a triple of vertices in a strongly regular graph is not strictly a function of the SRG family parameters, thus showing why widget multiplicity is not strictly governed by family parameters when $p \geq 3$.

widgets occurring in a two-particle non-interacting walk is:

$$M_{2,empty} = \frac{Nk}{2}\binom{N-2k+\lambda}{2} + \left(\binom{N}{2} - \frac{Nk}{2}\right)\binom{N-2-2k+\mu}{2}, \tag{2.21}$$

in agreement with the result in Gamble *et al.* for this particular widget [3]. Thus we see that this widget's multiplicity is, as expected, a function of the family parameters. Let's see what happens when we try this same approach for the corresponding widget in the three-particle walks, shown in Figure 2.2(b). Again, we consider the multiplicity of the widget in an arbitrary SRG by counting the number of times we can fit this widget on the graph. Now we pick three sites to serve as i, j, and k. We want to count, given our choice of i, j, and k, the number of sites that can serve as p, q, and r. To do this, we need to know how i, j, and k are connected amongst themselves, just as we did in the previous example. There are four possible non-isomorphic connectivities, as there can be between zero and three

connections amongst these sites. In order to count the multiplicity of this widget, we must consider for each of these four cases how many sites in the graph are mutually disconnected from sites i, j, and k. In the previous example, we could answer the analogous question via the family parameters, as illustrated above. However, this is because the family parameters μ and λ tell us how many common neighbors *pairs* of vertices have. There are no family parameters which encode this information for *triples* of vertices, as strong regularity does not place absolute constraints on shared connectivities for triples of vertices.

We illustrate this point with an example in Figure 2.4. Two copies of the Petersen graph, an SRG with family parameters $(10, 3, 0, 1)$ are depicted. The first copy highlights three mutually non-adjacent vertices; this particular triple of vertices has one common neighbor. The second copy also highlights a triple of mutually non-adjacent vertices, but this triple has *no* shared neighbors. Thus we have demonstrated by example that strong regularity cannot in general uniquely determine the shared connectivity for triples of vertices.

Moreover, we can see that counting the multiplicity of the widget shown in Figure 2.2(b) can be used to distinguish two non-isomorphic graphs from the same SRG family. Figure 2.3 shows the two non-isomorphic graphs in the SRG family (16,6,2,2). The widget in Figure 2.2(b) appears 512 times in the first graph and 608 times in the second graph, thus distinguishing them.

We conclude then that there exist three-particle widgets whose multiplicities *cannot* be functions of family parameters. Thus, the three-particle non-interacting walks are *not* forbidden from distinguishing non-isomorphic SRGs from the same family, unlike the two-particle non-interacting walks.

B. Computing the number of SRG fingerprints

In Section 2.3, it is shown that quantum walks of p non-interacting particles cannot distinguish all non-isomorphic pairs of strongly regular graphs. This is done by showing that $Z(p, N)$, the number of graph fingerprints given by the p-boson walk on an SRG family with N vertices, is less than the number of non-isomorphic strongly regular graphs with N

vertices, in the limit of large N. This subsection presents the calculation of $Z(p, N)$.

To calculate $Z(p, N)$, we note that if there are X_p possible Green's function values for the p-boson walk, and Y elements of the evolution operator U, then computing the number of unique fingerprints is equivalent to computing the number of ways one can put Y indistinguishable balls in X_p labeled bins, so that [49]

$$Z(p, N) = \binom{X_p + Y - 1}{X_p - 1}. \tag{2.22}$$

We recall that X_p is a function of p, but not of N. (We may think of X_p as the number of uniquely-valued widgets that appear in the p-boson walk.) However, Y, the number of elements in the evolution operator, will depend on both p and N, and we henceforth write it as $Y_{p,N}$. The dimension of the evolution operator is computed by determining how many different ways p bosons can be put on N vertices, which this is the same problem as computing the number of ways to put p indistinguishable balls into N labeled bins. The number of elements in the evolution operator is just the square of its dimension, so we find that:

$$Y_{p,N} = \binom{N + p - 1}{p}^2. \tag{2.23}$$

Using Equations (2.22) and (2.23), we now compute an upper bound for $Y_{p,N}$ and Z. It can be shown that $\binom{n+k-1}{k-1} \leq n^k$ when $n \geq 2$ and $k \geq 1$. Thus

$$Y_{p,N} < \binom{N + p}{p}^2 \leq N^{2(p+1)} \tag{2.24}$$

and

$$Z(p, N) \leq (Y_{p,N})^{X_p} < N^{2X_p(p+1)}. \tag{2.25}$$

Therefore, the maximum number of unique graphs the p-boson walk can distinguish is bounded above by $N^{2X_p(p+1)}$. We use this result in Section 2.3 to show that there exist SRGs that a particular p-particle walk cannot distinguish.

C. Bounding the number of widgets in the non-interacting p-particle walk

Here, we show that $\log_2 X_p \sim p^2$, where X_p is the number of distinct widgets for the non-interacting p-boson walk. First, Auluck proved there are $e^{O(p^{2/3})}$ widgets with no edges

[50]. (He counted bipartitions of (p, q), which may be considered to be edgeless widgets when $p = q$.) Since there are at most 2^{p^2} ways to add edges to one of these, we have the upper bound $X_p \leq 2^{p^2+O(p^{2/3})}$. To get a lower bound, it will suffice to consider the widgets with $2p$ distinct indices. The edges in one of these can be specified by a $p \times p$ array of bits, and the widgets isomorphic to it are obtained by permuting rows, permuting columns, or transposing the matrix. Therefore, by Burnside's counting lemma [51], the number of isomorphism classes of widgets of this type is

$$\frac{1}{|F|} \sum_{f \in F} [\ \#\ \text{of arrays fixed by}\ f\ ],$$

where the finite group F is the semidirect product of $S_p \times S_p$ by S_2. (S_p and S_2 are the symmetric groups on p and 2 objects, respectively.) This is lower bounded by the term coming from $f = 1$, which is $2^{p^2}/(2(p!)^2)$, and this is $2^{p^2+O(p \log p)}$ by Stirling's formula. From these two estimates the result of Equation (2.19) follows.

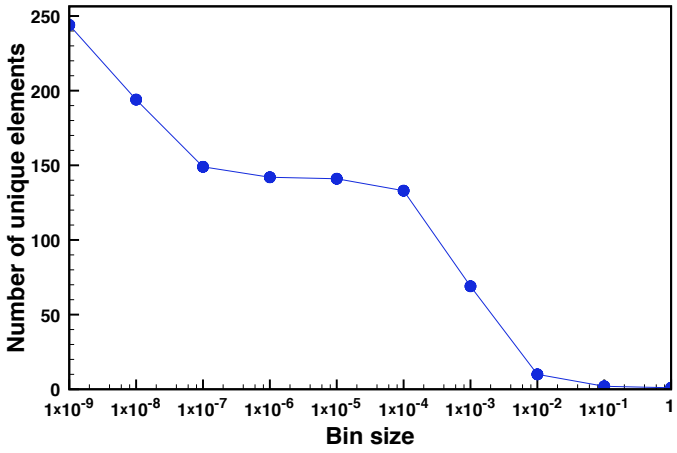

Figure 2.5: The number of numerically distinguished elements in the evolution operator $\mathbf{U}(t)$, defined in Equation (2.8) as a function of the bin size used in grouping the elements. This plot is for the non-interacting three-fermion walk on a graph in the SRG family (16,6,2,2). We see that the actual number of unique elements is about 150, which can be obtained by using a bin size in the range of 10^{-7} to 10^{-4}.

D. Error analysis for numerical computations

When comparing two graphs, we compute Δ, a measure of the distance between the lists of matrix elements of the evolution operators for the two graphs, as defined in Eq. (2.9). Computing Δ requires comparing two lists of numbers that are each exponentially large in particle number p. An evolution operator for a walk of p non-interacting fermions on a graph with N vertices has $\binom{N}{p}^2$ elements, and the boson equivalent has $\binom{N+p-1}{p}^2$ elements. For example, the evolution operator for the non-interacting four-fermion walk on a graph of 35 vertices has over 2.7 billion elements.

The comparison of the lists can be made much more efficient by exploiting the fact that the values in the list are highly degenerate. Instead of comparing the entries in a list, we make histograms of element values and their multiplicities. We then compute Δ by comparing these histograms. When constructing the histograms, it is important to determine the correct bin size. Choosing too large a bin size results in falsely grouping distinct elements together, while choosing too small a bin size results in falsely distinguishing elements. By constructing a series of histograms with different bin sizes for the same evolution operator, we are able to determine a range of bin sizes which are neither too large nor too small. This is illustrated in Figure 2.5, which shows that for the non-interacting three-fermion walk on a graph in $(16, 6, 2, 2)$, an appropriate bin size is between 10^{-7} and 10^{-4}.

Because we compute Δ via numerical simulation, we expect there to be some numerical noise floor. That is, for any two permutations of the same graph, we expect
$\Delta > 0$. It is important to determine how big this quantity, which we denote Δ_{iso}, will be. We only consider two non-isomorphic graphs to be distinguished if they yield a Δ which satisfies $\Delta \gg \Delta_{iso}$.

We numerically compute Δ_{iso} using double precision arithmetic for a variety of random permutations on our graphs, and we find a maximum Δ_{iso} to be approximately 10^{-6}. Thus, only graph pairs which yield a $\Delta > 10^{-6}$ are considered distinguished. We find Δ_{iso} to be relatively insensitive to graph size and particle number.

In practice, we see a gap for Δ between distinguished graph pairs and non-distinguished graph pairs. For distinguished graphs, we find Δ at least two orders of magnitude larger than Δ_{iso} (usually much larger); non-distinguished graph pairs have values of Δ are approximately equal to Δ_{iso} or are even smaller than it.

Chapter 3

Comparing algorithms for graph isomorphism using discrete- and continuous-time quantum random walks

3.1 Introduction

In the previous chapter we examined the use of continuous-time quantum random walks (CTQRWs) to solve the graph isomorphism problem (GI). While the work in Chapter 2 is part of a series of investigations of using CTQRWs for GI [2, 3], others have looked to utilize discrete-time quantum random walks (DTQRWs) for GI algorithms [52, 43]. While these efforts have helped illuminate what kinds of QRW algorithms might be fruitful for GI, an efficient QRW algorithm for GI has yet to be developed. Moreover, it is unknown if DTQRWs or CTQRWs are better candidates for an efficient GI algorithm, or if both classes of walks will ultimately be of equal utility.

This question is explored in a recent paper by Berry and Wang [4]. Their results indicate that discrete-time quantum random walks may have greater ability to distinguish

non-isomorphic strongly regular graphs (a class of graphs which are particularly difficult to distinguish) than continuous-time quantum random walks. This is based on (1) the ability of a specific discrete-time quantum random walk of two noninteracting particles to distinguish strongly regular graphs (SRGs) that are not distinguished by an algorithm based on a continuous-time quantum random walk of two noninteracting particles [3], and (2) the fact that the dimension of the state space of discrete-time walks on graphs is larger than that of continuous-time walks.

In this chapter, we explain why the two-particle noninteracting walks of Berry and Wang are able to distinguish non-isomorphic SRGs. To do this, we show analytically how even single-particle DTQRWs are able to distinguish non-isomorphic SRGs. This demonstrates how two-particle noninteracting DTQRWs can also distinguish SRGs. We then verify numerically that this distinguishing power of single-particle DTQRWs exists.

Additionally, we explore the differences between the comparison algorithm used by Berry and Wang [4] and the one used by Gamble *et al.* [3] (which is the same comparison algorithm used in Chapter 2). Both comparison algorithms rely on the construction of sorted lists of data, or "graph certificates", which are used to compare graphs. To help relate the graph certificates of [3] to those of [4], we introduce a third kind of certificate. This type of certificate features aspects of the certificates of both [3] and [4]. Though all three kinds of certificates are constructed similarly, we find that, when applied to single-particle discrete-time quantum random walks, the graph certificates of [3] have non-trivially less distinguishing power than the other two types of certificates. It remains an open question as to whether or not the graph certificates of [4] have more distinguishing power than the certificates introduced in this chapter. Thus we demonstrate the importance of using the same kind of graph certificates when attempting to compare the distinguishing power of DTQRWs and CTQRWs.

Lastly, we extend a result of Chapter 2, where we showed that there does not exist a CTQRW with a fixed number of noninteracting particles that can distinguish all SRGs when used in conjunction with the comparison algorithm of Gamble *et al.* In this chapter

we show that this argument holds for DTQRWs as well; no DTQRW with a fixed number of noninteracting particles can distinguish all SRGs when the comparison algorithm of Gamble *et al.* is used. We also examine the comparison algorithm of Berry and Wang, as well as an algorithm with similarities to both the algorithms of Berry and Wang as well as Gamble *et al.* We find that no CTQRW of a fixed number of noninteracting particles can distinguish all SRGs when used with these comparison algorithms. It remains an open question as to whether or not this is true for DTQRWs of a fixed number of noninteracting particles.

This chapter is organized as follows: Section 3.2 provides the requisite background regarding graph isomorphism, strongly regular graphs, and quantum random walks. Section 3.3 describes in detail the graph comparison procedures of Gamble *et al.*, and Berry and Wang, as well as a procedure which is "in between" the two. In Section 3.4, we analytically show how the single-particle DTQRW has the potential to distinguish non-isomorphic graphs when used with any of the three comparison algorithms we consider. Section 3.5 provides numerical results for single-particle DTQRWs; we find that all three comparison algorithms numerically distinguish some, but not all, of the tested SRG pairs, and one comparison procedure is not as strong as the other two. In Section 3.6, we show that a DTQRW with a fixed number of noninteracting particles cannot distinguish all SRGs when used with the comparison procedure of Gamble *et al.*; we show the same result holds when the comparison algorithm of Berry and Wang is used with CTQRWs with a fixed number of noninteracting particles. We are unable to extend this result for Berry and Wang's comparison algorithm when used with a DTQRW of a fixed number of noninteracting particles, indicating a potential difference between DTQRWs and CTQRWs. We discuss our results in Section 3.7.

3.2 Background

The graph-theoretic background necessary to discuss quantum random walks on graphs is provided in Section 2.2 of this thesis. The relevant definitions of graphs, adjacency matrices, and strongly regular graphs are provided therein. We note one change in notation compared

to Chapter 2. In keeping with previous work on quantum random walks, a graph's degree is denoted by k in Chapter 2; to be consistent with the notation of Berry and Wang [4], here we denote a graph's degree as d.

Discrete-time and continuous-time quantum random walks of noninteracting particles

Here we discuss how to form quantum random walks on graphs. For the noninteracting continuous-time model used in [3] and Chapter 2, a Hamiltonian is defined for a graph of N vertices with adjacency matrix $\mathbf{A}$:

$$\mathbf{H} = -\sum_{i,j}^{N} A_{ij} c_i^\dagger c_j, \tag{3.1}$$

where $c_i^\dagger$ and c_i are the creation and annihilation operators, respectively, for a boson or (spinless) fermion on site i. This Hamiltonian may be used with any number of particles (either bosons or fermions). Matrix representations of this Hamiltonian for a fixed number of particles are given by Eqs. (2.5) and (2.6). The evolution operator is then defined in the standard fashion:

$$\mathbf{U}_C(t) = e^{-it\mathbf{H}}, \tag{3.2}$$

where we have $\hbar = 1$ for convenience. This is the same as Eq. (2.8), except that we have added the subscript C to explicitly denote that this evolution operator is for a continuous-time walk. In this chapter, discrete-time evolution operators will be denoted with a subscript D.

For discrete-time walks, each particle has an auxiliary coin state, which "points" to where the particle will next move. Thus the single-particle walk has basis states of the form $|ij\rangle$, denoting the particle is on site i, and its coin is on site j, which by definition must be adjacent to i.

The noninteracting walk considered by [4] is based on a single-particle Grover-coined walk. We follow [52] and express the evolution operator in expanded form, allowing the coin index to run over all vertices in the graph, but still requiring the particle be adjacent

to its coin. Thus, for an N-vertex graph with adjacency matrix $\mathbf{A}$, the single-particle discrete-time evolution operator is given by

$$\mathbf{U}_D = \mathbf{S}\mathbf{\Lambda}(\mathbb{1} \otimes \mathbf{C})\mathbf{\Lambda}. \tag{3.3}$$

$\mathbf{\Lambda}|ij\rangle = A_{ij}|ij\rangle$, ensuring that the coin is adjacent to the particle. $\mathbf{S}$ is the swap operator; $\mathbf{S}|ij\rangle = |ji\rangle$. $\mathbf{C}$ is the coin operator. Here it is the Grover coin, which for a d-regular graph is $\mathbf{C} = -\mathbb{1} + \frac{2}{d}\mathbf{J}$. This expanded form of $\mathbf{U}_D$ has the same behavior as in [4]; we have only introduced $N^2 - Nd$ rows of 0, so its dimension is now $N^2 \times N^2$ [52].

To advance the walk a discrete number of time steps t, $\mathbf{U}_D$ is applied t times: $\mathbf{U}_D(t) = (\mathbf{U}_D)^t$. Additionally, the evolution operator for p noninteracting particles is just p tensor copies of $\mathbf{U}_D$: $\mathbf{U}_{D,p} = (\mathbf{U}_D)^{\otimes p}$.

3.3 Comparison Algorithms

Now that we have defined evolution operators for continuous-time and discrete-time walks, we explore how these operators can be used to compare graphs and test for isomorphism. All methods of comparing graphs that we examine are based on, given an evolution operator, generating a list of numbers sorted by size for each of the graphs, and comparing the respective lists. We follow [4] and refer to these sorted lists as graph certificates.

There are multiple graph certificates that can be constructed from a given evolution operator. In this section, we examine three classes of graph certificates. First, we give the definition of the certificate which is used in Chapter 2 and by [3] for CTQRWs. We then describe a certificate which is "between" the aforementioned certificate and the certificate of [4]. Lastly, we define the certificate used by [4] for DTQRWs. All three certificates can be applied to either continuous-time or discrete-time QRWs.

As the certificates are lists, we denote the three different certificate classes as L_0, L_1, and L_2, respectively. To indicate that a specific certificate corresponds to a discrete-time walk, a superscript D is included; a superscript C denotes the certificate corresponds to a continuous-time walk. Additionally, a second superscript is used to indicate that number

of particles in the walk which generates the certificate. For example, $L_2^{D,1}$ would refer to the L_2 graph certificate for a discrete-time walk of a single particle.

We call the graph certificate of [3] and Chapter 2 L_0. It is defined as follows:

$$L_0(\mathbf{A}, t) = \text{sort}\left(\{|U(t)_{mn}| : \forall m, n \in \{1, ..., \dim \mathbf{U}\}\}\right). \tag{3.4}$$

Thus, if the possible values the evolution operator elements can take on (up to different phases) are different for the different graphs, then the graphs will be distinguished. Even if the possible values each element can take on are the same for the different graphs, the graphs will be distinguished if those values have different multiplicities in the two evolution operators. While this algorithm has been used for CTQRWs, it can in principle be used for DTQRWs as well. Additionally, we see from its definition that L_0 is naturally defined for a walk with any number of particles.

It was proven in [2] that $L_0^{C,1}$ certificates could not be used to distinguish non-isomorphic SRGs from the same family, while [3] extended this proof for CTQRWs of two noninteracting particles. However, we showed in Chapter 2 that L_0 for CTQRWs with three or more noninteracting particles could distinguish many (but not all) pairs of non isomorphic SRGs from the same family.

The next graph certificate is designed for DTQRWs, but can be used for CTQRWs. We denote it L_1, which for the single-particle DTQRW is defined as

$$L_1^{D,1}(\mathbf{A}, t) = \text{sort}\left(\left\{\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(t)|kl\rangle|^2 : \forall i, k, l \in \{1 \dots N\}\right\}\right). \tag{3.5}$$

Each element of $L_1^{D,1}$ represents the total probability of a particle being on vertex i after t steps, given an initial state $|kl\rangle$. A natural extension of this method for a two-particle CTQRW is

$$L_1^{C,2}(\mathbf{A}, t) = \text{sort}\left(\left\{\sum_{j=1}^{N} |{}_B\langle ij|\mathbf{U}_{C,2}(t)|kl\rangle_B|^2 : \forall i, k \in \{1 \dots N\}, \forall l \in \{1 \dots k\}\right\}\right), \tag{3.6}$$

where $|ij\rangle_B$ denotes the bosonic (symmetrized) state in which there is a boson on site k and a boson on site l. (This method may be used just as well with fermions, with the basis states

appropriately anti-symmetrized.) The extension of L_1 for more than two continuous-time particles is given in Section 3.6.

The final graph certificate we examine is a variant of this method, and is the one utilized by [4]. This certificate, denoted L_2, is defined for the single-particle DTQRW as follows:

$$L_2^{D,1}(\mathbf{A},T) = \mathrm{sort}\left(\left\{ \sum_{t=1}^{T}\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(t)|kl\rangle|^2 : \forall i,k,l \in \{1\dots N\} \right\}\right). \tag{3.7}$$

This method sums up the probabilities of a particle being at a particular site at different times, given the same initial state. For the two-boson CTQRW, this certificate has the form:

$$L_2^{C,2}(\mathbf{A},T) = \mathrm{sort}\left(\left\{ \sum_{t=1}^{T}\sum_{j=1}^{N} |{}_B\langle ij|\mathbf{U}_{C,2}(t)|kl\rangle_B|^2 : \forall i,k \in \{1\dots N\}, \forall l \in \{1\dots k\} \right\}\right). \tag{3.8}$$

As with L_1, L_2 can be extended to any number of discrete-time or continuous-time walkers.

For a two-particle DTQRW, the size of $L_2^{D,2}$ can be quite large, with as many as N^4d^2 non-zero elements. In [4] the initial states are limited to what Berry and Wang call "bosonic edge states". Given two adjacent vertices k and l, a bosonic edge state, denoted by Berry and Wang as $|\beta^+\rangle$, is defined as

$$|\beta^+\rangle = \frac{1}{\sqrt{2}}(|kllk\rangle + |lkkl\rangle). \tag{3.9}$$

Therefore, their graph certificates (which we denote $\widetilde{L_2}^{D,2}$) have at most $\frac{N^3d}{2}$ nonzero elements, as a d-regular graph with N vertices contains $\frac{Nd}{2}$ edges. The certificate is defined as

$$\begin{aligned}
&\widetilde{L_2}^{D,2}(\mathbf{A},T) = \\
&\mathrm{sort}\Bigg(\Bigg\{ \sum_{t=1}^{T}\sum_{j_1,j_2=1}^{N} |\langle i_1j_1i_2j_2|\mathbf{U}_{D,2}(t)\tfrac{1}{\sqrt{2}}(|kllk\rangle + |lkkl\rangle)|^2 \\
&: \forall i_1,i_2, \in \{1\dots N\}, \forall (k,l) \in E \Bigg\}\Bigg),
\end{aligned} \tag{3.10}$$

where E is the edge set of $\mathbf{A}$. The physical interpretation of the certificate $\widetilde{L_2}^{D,2}$ is identical to that of ${L_2}^{D,2}$ except that each initial state is delocalized across an edge in the graph [4].

3.4 Analytic demonstration of the distinguishing power of DTQRWS on SRGS

Berry and Wang demonstrated numerically that the noninteracting two-particle DTQRW with the $\widetilde{L_2}$ certificate method could distinguish many SRGs. In this section, we show analytically why this is possible. To do so, we first analytically explore the distinguishing power available to single-particle walks using only the L_0 and L_1 graph certificates.

In general, if a particular kind of certificate will always fail to distinguish two non-isomorphic SRGs, it is because all elements of a certificate, as well as their multiplicities, are functions of SRG family parameters. This is how we show, or fail to show, the limitations of each certificate considered in this section.

Single-particle DTQRW with L_0 graph certificate

Here we show analytically that even single-particle DTQRWs have the potential to distinguish SRGs, using only the L_0 graph certificate. To begin our analysis, we compute an arbitrary element of $\mathbf{U}_{D,1}$ for $t = 1$:

$$\langle ij|\mathbf{U}_{D,1}|kl\rangle = A_{ij}A_{kl}\delta_{jk}\left(-\delta_{il} + \frac{2}{d}\right). \tag{3.11}$$

The particle on site k with its coin pointing to site l can move to site i with its coin pointing to site j if and only if $A_{ij} = A_{kl} = \delta_{jk} = 1$. ($A_{ij} = A_{kl} = 1$ is required because both the bra and ket must be legal states; a state must always have its coin point to a site that is adjacent to the location of the particle.) The amplitude of this transition is equal to $\frac{2}{d}$ if $i = l$, and $-1 + \frac{2}{d}$ otherwise. We see that the particle's movement for this single time step is highly restricted, and that all possible evolution operator element values are strictly functions of the family parameters.

Now that we have computed the possible non-zero values for $\langle ij|U|kl\rangle$, we compute the multiplicities of these values. If the multiplicities of one value are different for two SRGs in the same SRG family, then the $L_0^{D,1}$ certificates will distinguish the graphs.

To compute the multiplicities, we follow a procedure developed in [3] and further explored in Chapter 2. We denote by $M(x)$ the multiplicity of the value x in the evolution operator, and we recall that the family parameters for an SRG are denoted (N, d, λ, μ). We find:

$$M\left(\frac{2}{d}\right) = \sum_{ijkl}^{N} A_{ij}A_{kl}\delta_{jk}(1-\delta_{il}), \tag{3.12}$$

$$M\left(-1+\frac{2}{d}\right) = \sum_{ijkl}^{N} A_{ij}A_{kl}\delta_{jk}\delta_{il}. \tag{3.13}$$

Each of these summands is a product of four terms, each of which corresponds to an identity or adjacency relationship that appears in $\langle ij|\mathbf{U}_{D,1}|kl\rangle$. $1-\delta_{il}$ appears in the first summand, because δ_{il} is "turned off" (equals 0) when $\langle ij|\mathbf{U}_{D,1}|kl\rangle = \frac{2}{d}$; δ_{il} appears in the second summand because δ_{il} is "turned on" (equals 1) when $\langle ij|\mathbf{U}_{D,1}|kl\rangle = -1+\frac{2}{d}$.

The sums given in Eqs. (3.12) and (3.13) can be computed straightforwardly because all the index contractions here are reducible to matrix multiplication and traces. Additionally, we use the SRG identity of Eq. (2.2), and find

$$M\left(\frac{2}{d}\right) = N\mu(N-d-1) + N\lambda d, \tag{3.14}$$

$$M\left(-1+\frac{2}{d}\right) = Nd. \tag{3.15}$$

We see that these multiplicities are functions of the family parameters, so the walk has no distinguishing power when $t = 1$.

Next, we consider later times. $\langle ij|\mathbf{U}_{D,1}^{t}|kl\rangle$ for $t = 2$ and $t = 3$ are straightforward to calculate; both the values and degeneracies for these cases are reducible to sums over products of adjacency matrices and traces of adjacency matrices, and therefore can be written as functions of the SRG family parameters. Therefore, $\mathbf{U}_{D,1}^{2}$ and $\mathbf{U}_{D,1}^{3}$ cannot distinguish non-isomorphic SRGs of the same family when used to generate L_0 certificates.

At $t = 4$, all six possible adjacency relations appear (A_{ij}, A_{kl}, A_{jk}, A_{ik}, A_{jl} and A_{il}):

$$\begin{aligned}\langle ij|U^4|kl\rangle = A_{ij}A_{kl}(4d^{-2}(A_{il}-A_{jk}) + 2d^{-1}\times \\ (2\delta_{ik} - A_{il}\delta_{ik} - A_{jk}\delta_{ik} + \delta_{jl} - A_{il}\delta_{jl}) + \delta_{ik}\delta_{jl} - \\ 8d^{-3}((d-\mu)(\delta_{ik}+\delta_{jl}) + (\lambda-\mu)(A_{ik}+A_{jl}) + \\ 2\mu) + 16d^{-4}(\delta_{jk}(d-\mu)(\lambda-\mu) + \\ A_{jk}(d + (\lambda-\mu)^2 - \mu) + (d+\lambda-\mu)\mu)).\end{aligned} \tag{3.16}$$

When all four vertices are connected to each other, $\langle ij|\mathbf{U}^4_{D,1}|kl\rangle = \frac{-16\lambda}{d^3} + \frac{16(d+(\lambda-\mu)^2-\mu+(d+\lambda-\mu)\mu)}{d^4}$. As no other configuration of vertices yields this value for $\langle ij|\mathbf{U}^4_{D,1}|kl\rangle$, this value appears in the operator $\mathbf{U}^4_{D,1}$ M times, where M satisfies

$$M = \sum_{ijkl}^{N} A_{ij}A_{kl}A_{ik}A_{il}A_{jk}A_{jl}. \tag{3.17}$$

Computing the sum in Eq. (3.17) requires contracting over four indices, each of which occurs three times. Such a sum cannot be reduced to be in terms of matrix multiplication and traces. We showed in Chapter 2, in the context of continuous-time noninteracting walks of three particles, that these kinds of sums are functions of the number of shared neighbors belonging to triples of vertices in the graph in question. This number is, in general, different for different triples of vertices in the same SRG, and therefore not a function of the SRG family parameters. Therefore, $\mathbf{U}^4_{D,1}$ has the potential to distinguish non-isomorphic SRGs when used with the L_0 method. In Section 3.5, we numerically show that this method does indeed distinguish some (but not all) non-isomorphic SRGs.

In contrast, in Refs. [2, 3] it is proved that single-particle and noninteracting two-particle CTQRWs with the L_0 graph certificate method cannot distinguish any non-isomorphic SRG pair from the same family. Several key differences between DTQRWs and CTQRWs become apparent. First, an element of the single-particle continuous-time walk evolution operator is indexed by up to 2 vertices (as the particle is on 1 vertex in an initial state, 1 vertex in the final state, and the sets of final and initial vertices need not overlap). However, an element of the corresponding single-particle discrete-time walk evolution operator is indexed

by up to 4 vertices, because each particle corresponds to a vertex, as does each particle's coin. Additionally, in the continuous-time walk, the value of an evolution operator element does not depend on whether or not two vertices which are both in the final or initial state are adjacent. Therefore, such adjacency relations are not considered when performing the appropriate multiplicity sum. However, because a particle must always be adjacent to its coin, the adjacency relation between a particle and its coin is always included in the discrete-time sum used to compute element multiplicity. The presence of these additional adjacency relations gives the single-particle DTQRW with the L_0 comparison protocol the potential to distinguish non-isomorphic SRGs.

Single-particle DTQRW with L_1 graph certificate

Here we show that the L_1 method, when used with the single-particle DTQRW, also has the potential to distinguish non-isomorphic SRGs from the same family. To start, we compute an element of $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}|kl\rangle|^2$ for $t = 1$.

$$\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}|kl\rangle|^2 = A_{ik}A_{kl}\left(\delta_{il}\left(1 - \tfrac{4}{d}\right) + \tfrac{4}{d^2}\right) \tag{3.18}$$

Possible non-zero values for $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}|kl\rangle|^2$ are $\frac{4}{d^2}$ and $1 - \frac{4}{d} + \frac{4}{d^2}$, which are both functions of the family parameters. We may compute their multiplicities, and find that they are also functions of the family parameters. Thus, $L_1^{D,1}(t = 1)$ graph certificates cannot distinguish non-isomorphic SRGs from the same family.

Similarly, it may be shown that at $t = 2$ for the single-particle DTQRW, all elements of L_1 are functions of the family parameters, as well as their multiplicities. Therefore, $L_1^{D,1}(t = 2)$ certificates also cannot distinguish non-isomorphic SRGs from the same family.

However, at $t = 3$, the values of the elements of L_1 for the single-particle DTQRW at $t = 3$ are *not* functions of the family parameters. The Appendix provides the value of $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(3)|kl\rangle|^2$, which has the form:

$$\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(3)|kl\rangle|^2 = g(i,k,l) + h(i,k,l)\sum_{j=1}^{N} A_{ij}A_{jl}A_{jk}, \tag{3.19}$$

where $g(i,k,l)$ and $h(i,k,l)$ are functions of the family parameters. However, $\sum_{j=1}^{N} A_{ij}A_{jl}A_{jk}$ is not a function strictly of family parameters, for the same reason that Eq. (3.17) is not. Thus we do not even need to examine the multiplicities of different values of $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(3)|kl\rangle|^2$, as this sum takes on values that are not functions of the SRG family parameters. Therefore, the single-particle L_1 method at $t = 3$ can potentially distinguish non-isomorphic SRGs from the same family. In Section 3.5, we numerically show that this method can distinguish some non-isomorphic graph pairs from the same SRG family.

However, this is not true for two-particle noninteracting CTQRWs. Using the methods of [3] and Chapter 2, it can be shown that, when the appropriately symmetrized or anti-symmetrized states are used with the continuous-time evolution operator, all possible values and corresponding multiplicities of $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{C,2}(t)|kl\rangle|^2$ are functions of the family parameters and the time t. Thus, we see that the single-particle DTQRW L_1 method is strictly stronger than the two-particle noninteracting CTQRW L_1 method for distinguishing SRGs.

Single-particle DTQRW with L_2 graph certificate

Now we examine $L_2^{D,1}(T)$ analytically for varying values of T. Recall that elements of $L_2^{D,1}(T)$ are sums of elements from $L_1^{D,1}(t)$ with t running from 1 to T. By inspection of Eqs. (3.5) and (3.7), we see that for a final time of $T = 1$, L_2 is the same as $L_1(t = 1)$, and will have no distinguishing power. Similarly, for $T = 2$, each element of L_2 will be a sum of a term from $L_1(t = 1)$ and $L_1(t = 2)$. As the value and multiplicity of each of those terms is strictly a function of SRG family parameters, the corresponding values and multiplicities of each element of $L_2(T = 2)$ will be a function of SRG family parameters. Thus $L_2^{D,1}(T = 2)$ certificates cannot distinguish non-isomorphic SRGs from the same family.

However, we know that $L_1^{D,1}(t = 3)$ certificates have the potential to distinguish SRGs. Thus, $L_2^{D,1}(T = 3)$ certificates also have the potential to distinguish SRGs from the same family, as the elements of a $L_2^{D,1}(T = 3)$ certificate are sums of terms which include elements of a $L_1^{D,1}(t = 3)$ certificate, which we have shown to not be functions of family parameters.

Two-particle noninteracting CTQRWs with the L_2 method may be similarly analyzed. Because the L_1 method fails to distinguish SRGs with noninteracting two-particle CTQRWs for all values of t, these walks with the L_2 method will also be unable to distinguish SRGs. Thus we analytically see that for all three comparison methods contemplated, the single-particle DTQRW has the potential to distinguish non-isomorphic SRGs from the same family, while two-particle noninteracting CTQRWs cannot.

3.5 Numerical Results

			Number of Undistinguished Pairs						
SRG Family (N,d,λ,μ)	Number of Graphs	Comparisons	$L_0^{D,1}$ (t=4)	$L_0^{D,1}$ (t=2N)	$L_1^{D,1}$ (t=3)	$L_1^{D,1}$ (t=4)	$L_2^{D,1}$ (T=3)	$L_2^{D,1}$ (T=4)	$L_2^{D,1}$ (T=2N)
(16,6,2,2)	2	1	1	1	1	1	1	1	1
(25,12,5,6)	15	105	11	11	0	0	0	0	0
(26,10,3,4)	10	45	3	3	1	1	1	1	1

Table 3.1: Numerical results for graph isomorphism testing using single-particle DTQRWs with varying comparison algorithms with various times. The different graph certificates ($L_0^{D,1}$, $L_1^{D,1}$, and $L_2^{D,1}$) are defined in Eqs. (3.4), (3.5), and (3.7). We note that all three algorithms have significant, but not universal, distinguishing power on SRGs. Additionally, this distinguishing power saturates at the minimum time at which each algorithm can potentially distinguish SRGs. Lastly, we see that $L_1^{D,1}$ and $L_2^{D,1}$ are more powerful than $L_0^{D,1}$, but $L_2^{D,1}$ is possibly no more powerful than $L_1^{D,1}$.

We now test the three comparison methods with the single-particle DTQRW on three families of SRGs. For the DTQRWs, all three algorithms are tested at the minimum time they can potentially distinguish SRGs ($t = 4$ for $L_0^{D,1}$, $t = 3$ for $L_1^{D,1}$, and $T = 3$ for $L_2^{D,1}$). We additionally test $L_0^{D,1}$ at $t = 2N$, $L_1^{D,1}$ at $t = 4$, and $L_2^{D,1}$ at $T = 4$ and $T = 2N$. ($T = 2N$ is the total time used by Berry and Wang for their tests [4].) Our results are given in Table 3.1.

Each algorithm distinguishes some, but not all, non-isomorphic SRGs from the same family. Also, no single-particle DTQRW algorithm that we test is able to distinguish the pair of SRGs in $(16, 6, 2, 2)$, which is in contrast to the results of Berry and Wang, who successfully distinguished these graphs using the two-particle DTQRW with $\widetilde{L_2}^{D,2}$ certificates. Additionally, the various algorithms we test have significant distinguishing power on the

other two SRG families we examine. We note that the distinguishing power for each algorithm saturates at the minimum time required to allow for potentially distinguishing SRGs. This could be because SRGs are distance-regular with diameter 2, so allowing the particles to walk for longer does not actually result in capturing more of the graph structure.

The distinguishing power seems to saturate with $L_1^{D,1}(t = 3)$, for higher times, either with $L_1^{D,1}$ or $L_2^{D,1}$, no further distinguishing power is obtained. For $(25, 12, 5, 6)$, $L_1^{D,1}(t = 3)$ distinguishes all possible graph pairs. For $(26, 10, 3, 4)$, there is one graph pair that cannot be distinguished by $L_1^{D,1}(t = 3)$, $L_1^{D,1}(t = 4)$, or $L_2^{D,1}$ with any time we test. Therefore, it is possible that $L_2^{D,1}$ offers no more distinguishing power than $L_1^{D,1}$. More generally, it is possible that $L_2^{D,p}$ yields no more distinguishing power than $L_1^{D,p}$. Additionally, it is possible that there exists a certain time (and perhaps relatively small time) beyond which no additional distinguishing power is obtained. As the complexity of computing $L_1^{D,p}$ and $L_2^{D,p}$ increase with the number time steps used, it could useful to know if there is no additional information to be gained by increasing the number of time steps.

3.6 Asymptotic limits for DTQRWS and CTQRWS

We have shown how, by all three comparison algorithms considered, the single-particle DTQRW has more distinguishing power on SRGs than noninteracting two-particle CTQRWs (which cannot distinguish any non-isomorphic pair of SRGs from the same family). However, as the distinguishing power of the single-particle DTQRW is not universal on SRGs, we can contemplate how to increase this distinguishing power. One obvious method is to add additional particles to the walk. Indeed, with a two-particle noninteracting DTQRW, Berry and Wang distinguished SRG pairs that are not distinguished by $L_2^{D,1}$ certificates for $T = 3, 4$ and $2N$ [4]. Thus it is interesting to characterize the asymptotic distinguishing power of many-body QRWs. In this section, we show that no CTQRW of a fixed number of noninteracting particles can distinguish all SRGs when used with either L_0, L_1, or L_2 certificates. We also show this result holds for DTQRWs of any fixed number of noninteracting particles when used to generate L_0 certificates; we are unable to extend this result

for such walks with L_1 and L_2 certificates.

Asymptotic behavior for L_0

It was demonstrated in Chapter 2 that increasing the number of noninteracting particles in a CTQRW could significantly increase distinguishing power of the walk when used with the L_0 method. However, it was also shown there that no CTQRW with a fixed number of noninteracting particles could distinguish all SRGs. This was done by showing that, as graph size increases, the number of unique SRGs with the same family parameters is super-exponentially large in graph size [47, 48], while for a fixed particle number p, the number of unique graphs that the p-particle CTQRW can distinguish with the L_0 method is polynomial in graph size.

We show here that this limitation of L_0 certificates applies to DTQRWs as well. Let us consider the p-particle noninteracting DTQRW, and let us denote by X_p the maximum number of unique values that $\langle i_1, j_i \dots i_p, j_p | \mathbf{U}_{D,p}^t | k_1, l_1 \dots k_p, l_p \rangle$ can take on. X_p is *not* a function of the size of the graph; the value of a DTQRW evolution operator element for an SRG is determined only by the configuration of up to $4p$ vertices in that SRG. (For further details, see Chapter 2, Appendix C.)

Additionally, the number of elements in $\mathbf{U}_{D,p}$ is N^{4p}, where N is the number of vertices in the graph. Thus, for an SRG family with graphs of N vertices, the L_0 method generates certificates of length N^{4p}, where each element in the certificate can take on a maximum number of X_p different values. Thus, given an SRG family with graph size N, the maximum number of unique L_0 graph certificates the noninteracting p-particle DTQRW can generate is equivalent to the number of ways one can put N^{4p} indistinguishable balls into X_p distinguishable bins, or $\binom{X_p + N^{4p} - 1}{X_p - 1}$ [49].

As X_p is constant in N, this quantity is polynomial in N. Thus, just like noninteracting CTQRWs with fixed particle number, DTQRWs with fixed particle number cannot distinguish all SRGs with the L_0 graph certificate method. Thus, the L_0 method for noninteracting p-particle walks *cannot* yield a universal GI algorithm for SRGs, whether or not

the walks are continuous-time or discrete-time.

Asymptotic behavior for L_1 and L_2

For discrete-time walks, the L_1 graph certificate does not necessarily have the same limitations as L_0. This is because the values of the elements of discrete-time L_1 certificates are *not* functions of SRG family parameters, as demonstrated by Eq. (3.19). Given a fixed number of discrete-time walkers, the number of unique values that the sum $\sum_{j_1 \ldots j_p=1}^{N} |\langle i_1 j_1 \ldots i_p j_p | \mathbf{U}_{D,p}^{t} | k_1 l_1 \ldots k_p l_p \rangle|^2$ can take on is not a function only of particle number. In principle, this quantity may be a function of the graph size, in which case the number of unique L_1 graph certificates for a fixed particle number and SRG family may be super-exponential in graph size. Thus, the number of unique SRGs in a family with graph size N is *not* guaranteed to be larger than the number of unique discrete-time L_1 graph certificates that can be generated for walks of p noninteracting particles on graphs of N vertices. Thus, the proof of the limitations of the L_0 method fails to translate to the L_1 method for DTQRWs. Whether there exists such a limitation is therefore still an open question.

Because DTQRW L_2 graph certificates are also affected by sums of the form shown in Eq. (3.19), we conclude that, for DTQRWs, the proof of the limitations of L_0 cannot be applied to L_2, just as it cannot be applied to L_1. Therefore, for DTQRWs with L_0 and L_1 graph certificates, it is possible that there exists a fixed p such that the p-particle noninteracting walk can distinguish all SRGs.

We will now show that, using the same method of proof from the previous subsection, no CTQRW of a fixed number of noninteracting particles can distinguish all SRGs, when used in conjunction either the L_1 or L_2 graph certificates. We will only examine bosonic walks; the results for fermionic walks can be proved in the same manner.

We begin by stating the definition of L_1 for p-boson CTQRWs. There are multiple ways in which we can extend L_1 for more than two particles in a CTQRW, as we can choose the number of particles in the final state whose probability distribution we wish to measure.

For simplicity, here we sum over one particle. However, our proof holds if we sum over more than one particle as well.

We examine the certificate $L_1^{C,p}(t)$:

$$L_1^{C,p}(t) = \text{sort}\{\sum_{i_1}^{N} |{}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B|^2 : \\ 1 \leq i_2 \leq i_3 \dots \leq i_p \leq N, 1 \leq j_1 \leq j_2 \dots \leq j_p \leq N\}. \tag{3.20}$$

It has been shown [3] that for SRGs, elements of the noninteracting p-boson CTQRW evolution operator have the following simple form:

$$ {}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B = \\ {}_B\langle i_1 \dots i_p|(\alpha\mathbb{1} + \beta\mathbf{J} + \gamma\mathbf{A})^{\otimes p}|j_1 \dots j_p\rangle_B \tag{3.21}$$

where α, β, and γ are all functions of the family parameters and the time t. (The fermionic walks have the same form, except the states are anti-symmetrized, and α, β, and γ are replaced by their respective complex conjugates.)

Therefore, ${}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B$ is a function of family parameters, t, and the binary relationships A_{xy} and δ_{xy} for $x \in \{i_1 \dots i_p\}$ and $y \in \{j_1 \dots j_p\}$. Moreover, this quantity is a sum of terms where each term is a product of up to p binary relationships and various powers of α, β, γ. Each term does not contain any more than one instance of any one of the $2p$ indices.

Hence $|{}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B|^2$ contains no term which includes more than two instances of the same index. Thus, $\sum_{i_1}^{N} |{}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B|^2$ is only a function of family parameters and the binary relationships A_{xy} and δ_{xy} for $x \in \{i_2 \dots i_p\}$ and $y \in \{j_1 \dots j_p\}$. For this quantity to *not* be a function of family parameters, the index i_1 would have to appear three times in a single term in $|{}_B\langle i_1 \dots i_p|\mathbf{U}_{C,p}(t)|j_1 \dots j_p\rangle_B|^2$, as explained in Chapter 2.

The value of each unique element in $L_1^{C,p}(t)$ is determined by relationships between the $2p-1$ indices $\{i_2 \dots i_p, j_1 \dots j_p\}$. Following Appendix B in Chapter 2, it can be shown

that the number of unique elements $L_1^{C,p}(t)$ can contain is bounded above by $2^{p^2+O(p\log p)}$. Additionally, the length of $L_1^{C,p}(t)$ is $\binom{N+p-1}{p}\binom{N+p-2}{p-1}$. Following the same argument from the end of the previous subsection and from Section 3 of Chapter 2, the number of unique graph certificates this process can generate for a fixed particle number p is polynomial in graph size N. Thus a CTQRW used with the L_1 method and a fixed number of noninteracting particles cannot be universal for SRGs, as there will exist more SRGs than unique $L_1^{C,p}(t)$ certificates.

This analysis extends to $L_2^{C,p}(T)$. The possible values elements of $L_2^{C,p}(T)$ will in general be different from the possible values of $L_1^{C,p}(t)$. However, the number of possible values elements of $L_2^{C,p}(T)$ can take on will still be bounded above by $2^{p^2+O(p\log p)}$. Additionally, the lengths of the $L_2^{C,p}(T)$ and $L_1^{C,p}(t)$ certificates are the same. Thus the number of SRGs of size N in a single family that $L_2^{C,p}(T)$ certificates can distinguish will be polynomial in N. We conclude that computing $L_2^{C,p}(T)$ certificates for a fixed number p of noninteracting particles cannot distinguish all SRGs.

3.7 Summary

We have shown how single-particle discrete-time quantum random walks can distinguish many non-isomorphic strongly regular graphs. These results are proven with techniques used to analyze the distinguishing power of noninteracting continuous-time quantum random walks [2, 3]. These results regarding single-particle DTQRWs in turn explain the results of Berry and Wang [4], who numerically found that two-particle discrete-time walks could distinguish many strongly regular graphs.

Additionally, we have examined a proposal of [4], that DTQRWs have more distinguishing power than CTQRWs. To evaluate this proposal, we have found that it is important to consider not just the kind of QRW in question, but the method in which the graph certificate is constructed. We have considered three related graph certificate construction methods, which we have dubbed L_0, L_1, and L_2.

We have found that single-particle DTQRWs used with the L_0 method can distinguish

many SRGs, in contrast to single-particle and noninteracting two-particle CTQRWs, which, when used with the L_0 method, cannot distinguish any SRGs from the same family, as proven in [2, 3]. However, we have also extended the results of Chapter 2, where we showed that there does not exist a fixed particle number p such that a noninteracting p-particle CTQRW with the L_0 can distinguish all SRGs. Here we have shown this limitation to hold true for noninteracting p-particle DTQRWs as well.

Lastly, we have shown that this limitation holds for CTQRWs when the L_1 and L_2 certificate methods are considered. There does not exist a fixed number p such that a non-interacting p-particle CTQRW with either L_1 or L_2 certificates can distinguish all SRGs. However, it remains an open question as to whether or not these limitations of L_1 and L_2 apply to DTQRWs. Thus it is possible that there exists a noninteracting p-particle DTQRW such that L_1 or L_2 certificates can distinguish all SRGs. This would demonstrate a nontrivial difference in distinguishing power between continuous-time and discrete-time noninteracting walks.

3.8 Appendix

Eq. (3.19) in Section 3.4 demonstrates that $L_1^{D,1}$ certificates can distinguish non-isomorphic SRGs of the same family. To show that Eq. (3.19) is of the correct form and cannot be a function of family parameters, we provide here the value of $\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(3)|kl\rangle|^2$:

$$\begin{aligned}
&\sum_{j=1}^{N} |\langle ij|\mathbf{U}_{D,1}(3)|kl\rangle|^2 = \\
&\sum_{j=1}^{N} A_{ij}A_{kl}((A_{ik}+A_{jl})\times \\
&\left(\tfrac{-16}{d^4}(A_{ik}+A_{jl}) - \tfrac{16}{d^3}\delta_{il} + \tfrac{8}{d^2}\delta_{il}\delta_{jk} - \tfrac{64}{d^5}A_{jk}^2\right) + \\
&\delta_{il}\left(\tfrac{4}{d^2} - \tfrac{4}{d}\delta_{jk} + \tfrac{32}{d^4}A_{jk}^2 + \delta_{jk}\left(1 - \tfrac{16}{d^3}A_{jk}^2\right)\right) + \tfrac{64}{d^5}\left(A_{jk}^2\right)^2)
\end{aligned} \tag{3.22}$$

We recall the SRG identity of Eq. (2.2), and see that $A_{jk}^2 = (d-\mu)\delta_{jk} + \mu + (\lambda-\mu)A_{jk}$. Thus by inspection of Eq. (3.22), we see that

$\sum_{j=1}^{N} |\langle ij|\mathbf{U}(3)|kl\rangle|^2$ contains a term proportional to $A_{kl}\sum_{j=1}^{N} A_{ij}A_{jl}A_{jk}$, corroborating Eq. (3.19). Therefore, no element of $L_1^{D,1}$ can be a function only of SRG family parameters, as explained in Section 3.4.

Chapter 4

Limitations of Quantum Random Walks for Graph Isomorphism

4.1 Introduction

The previous two chapters examined algorithms for the graph isomorphism problem which were based on multi-particle quantum random walks of non-interacting particles. In this chapter, we turn towards examining GI algorithms based on walks of *interacting* particles. Note that here, unlike the last chapter, we restrict ourselves to considering only continuous-time quantum random walks. Additionally, we only consider the L_0 comparison method.[1]

Gamble *et al.* [3] proved analytically that two-particle non-interacting walks could not distinguish non-isomorphic same-family strongly regular graphs. However, they also showed that walks of two interacting particles (in particular, walks of two hard-core bosons) could distinguish at least some same-family SRGs. As such interacting walks lacked the relatively simple algebraic structure of non-interacting walks, the demonstration of an interacting walk's ability to distinguish SRGs relied on numerical evidence alone. Simulating such walks, Gamble *et al.* distinguished over 500 million pairs of SRGs. As every tested pair was

[1] See Eq. (3.7) for formal definition of L_0. Additionally, although we do not consider L_1 or L_2 methods (Eqs. (3.9) and (3.11), respectively) in this chapter, we currently have no evidence that the L_1 or L_2 methods yield any greater distinguishing power for continuous-time walks.

in fact distinguished by the two-boson hard-core walk, these findings raised two interesting questions:

1. Could the two-boson hard-core walk distinguish all pairs of non-isomorphic SRGs?

2. Could the two-boson hard-core walk distinguish all pairs of non-isomorphic graphs?

As of this writing, the first question is still open. However, the second question has been answered with a firm, if disappointing, "no".

Shortly after the publication of Gamble *et al.*, Jamie Smith proved that indeed *no* quantum walk of any number of hard-core particles could distinguish arbitrary graphs [5]. This proof relied heavily on the usage of what are called cellular algebras, as will be explained in the next section.

This chapter extends the work of Jamie Smith, as we demonstrate that not only will hard-core walks not distinguish all graph pairs, but even very general kinds of interacting walks will fail to distinguish all graphs. The chapter is organized as follows: We first provide basic definitions, including those of the cellular algebra and its relevant properties. Next we provide a framework for how our proofs will proceed. We then examine a series of walks where the nature of the interactions are restricted to be two-body interactions. We demonstrate that the most general walks with only two-body interactions cannot distinguish all graphs. Then we examine walks where the interactions are not restricted to be two-body. After working through smaller examples, we conclude with the most general case, namely a walk with both an arbitrary numbers of particles and an arbitrary number of bodies in the interaction, provided that the interactions only depend on "local" graph properties (that is, the Hamiltonian does not have any global graph properties programmed into it).[2] This demonstrates that no locally-interacting walk with any number of particles can, in conjunction with the comparison algorithm L_0, distinguish all graphs.

[2]If this restriction were not present, we could "cheat" in the sense that we could preprocess a graph's adjacency matrix in order to encode a global property (such as the isomorphism class) of the graph into the Hamiltonian. This would make distinguishing graphs trivial, but the preprocessing cost would be exponential (as one would have to classically determine a graph's isomorphism class).

4.2 Cellular algebras

Basic definitions

The main results of Jamie Smith's work, as well as this chapter, rely heavily on structures known as *cellular algebras*. Therefore, we will begin with its definition. Consider a finite set V and a set of $|V| \times |V|$ matrices $\mathcal{R} = \{R_1, \ldots, R_s\}$ such that each matrix in $\mathcal{R}$ is a 0-1 matrix and $\mathcal{R}$ partitions $V \times V$. We call each matrix in $\mathcal{R}$ a *binary relation* as for any $R_i \in \mathcal{R}$, each ordered pair $(j,k) \in V \times V$ is either "in" R_i ($\langle j|R_i|k\rangle = 1$) or it is "not in" R_i ($\langle j|R_i|k\rangle = 0$).

We say that the pair $W = (V, \mathcal{R})$ is a cellular algebra if the following hold:

1. There exists a subset $\mathcal{R}_0$ of $\mathcal{R}$ such that $\sum_{R_i \in \mathcal{R}_0} R_i = I$, where I is the $|V| \times |V|$ identity matrix.

2. $R_i \in \mathcal{R}$ if and only if $R_i^T \in \mathcal{R}$.

3. For all $R_i, R_j \in \mathcal{R}$, $R_i R_j = \sum_{k=1}^{s} c_{ij}^k R_k$.

The numbers c_{ij}^k are referred to as the *intersection numbers* or the *structure constants* of W. Given the definition of a cellular algebra, there are two additional corollaries that we now state:

1. $\sum_{R_i \in \mathcal{R}} R_i = J$, where J is the $|V| \times |V|$ matrix of all ones.

2. For each $M \in W$, $M = \sum_{i=1}^{s} \beta_i R_i$, where each β_i depends on M.

The first corollary is equivalent to the statement that $\mathcal{R}$ partitions $V \times V$. The second corollary arises because W is an algebra, and $\mathcal{R}$ forms its basis.

Next, we define the set $\mathcal{R}^*$, which is the set of all sums of elements of $\mathcal{R}$. As $\mathcal{R}^*$ permits sums, but not arbitrary linear combinations, of elements of $\mathcal{R}$, $\mathcal{R}^*$ is also a set of 0-1 matrices. Additionally, we see that by definition, $\mathcal{R}^* \subset W$.

Lastly, we may consider a graph G with adjacency matrix A. $[A]$ denotes the cellular algebra which contains A and whose set of binary relations is as small as possible [5]. More generally, $[M_1, \ldots, M_n]$ denotes the cellular algebra of smallest basis size which contains the set of matrices $\{M_1, \ldots, M_n\}$. Additionally, as the binary relations of $[A]$ partition $V \times V$ into at least sets of vertices, edges, and non-edges, if $[A] = (V, \mathcal{R})$, then $A \in \mathcal{R}^*$ [53].

p-extensions

We now consider tensor products of cellular algebras. If $W = (V, \mathcal{R})$, then its p-fold tensor product is $W^{\otimes p} = (V^p, \mathcal{R}^{\otimes p})$ [54]. Throughout the literature, $W^{\otimes p}$ is often referred to as W^p.

We additionally consider the "diagonal identity" operator $I_{\Delta p}$, so-called because it acts as the identity on the diagonal of V^p. It is formally defined as

$$I_{\Delta p} = \sum_{i=1}^{|V|} |i\rangle^{\otimes p} \langle i|^{\otimes p}. \tag{4.1}$$

(Equivalently, $I_{\Delta p}$ acts as the identity on all vectors associated with elements of V^p (p-tuples) that are of the form $(i, i, \ldots, i, i)$.)

With $I_{\Delta p}$ and $W^{\otimes p}$ now defined, we may now define the p-extension of W, denoted $\widehat{W^p}$:

$$\widehat{W^p} := [W^{\otimes p}, I_{\Delta p}]. \tag{4.2}$$

Weak isomorphisms

Now we introduce the notion of a *weak isomorphism*. We say that two cellular algebras $W = (V, \mathcal{R})$ and $W' = (V', \mathcal{R}')$ are weakly isomorphic if there exists a bijection $\varphi : W \to W'$ such that when the domain is restricted to $\mathcal{R}$, $\varphi : \mathcal{R} \to \mathcal{R}'$ [5], that is, φ is also a bijection between $\mathcal{R}$ and $\mathcal{R}'$. (For compactness of notation, the element of $\mathcal{R}'$ that φ maps R_i to is denoted as $R_{\varphi(i)}$, i.e., $\varphi(R_i) = R_{\varphi(i)}$.)

If these conditions hold, we call φ a *weak isomorphism*. Additionally, we note that a weak isomorphism φ acts as a similarity transformation; for all $M \in W$, $\varphi(M) = \varphi^{-1} M \varphi$.

We can extend the notion of weak isomorphism to p-extensions of cellular algebras. Consider two cellular algebras W and W'. Suppose there exists a weak isomorphism $\widehat{\varphi}$: $\widehat{W^p} \to \widehat{W'^p}$. We then say that a weak isomorphism φ which maps W to W' is a *p-equivalence* if the following two constraints on $\widehat{\varphi}$ hold:

1. For all M_i in W, $\widehat{\varphi}(M_1 \otimes \ldots \otimes M_p) = \varphi(M_1) \otimes \ldots \otimes \varphi(M_p)$.

2. $\widehat{\varphi}(I_{\Delta_p}) = I_{\Delta'_p}$. ($I_{\Delta'_p}$ acts as the identity on the diagonal of V'^p.)

Recalling the tensor product identities $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ and $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$, we see that the first constraint implies that $\widehat{\varphi} = \varphi^{\otimes p}$.

Now, consider two adjacency matrices A and A' with cellular algebras $W = [A]$ and $W' = [A']$, respectively. If there exists a weak isomorphism φ which maps W to W' such that $\varphi(A) = A'$, *and* φ is a p-equivalence between W and W', then we say that A and A' are *p-equivalent* graphs. It is known result that for all positive integers p, there exist non-isomorphic p-equivalent graphs [54]. Therefore, to show that a proposed graph isomorphism algorithm is *not* universal, it suffices to show that it cannot distinguish non-isomorphic p-equivalent graphs for some p, as such graph pairs are known to exist.

Cylindric relations

The last definition we introduce, before getting to our proofs, is that of the cylindric relation. Consider a cellular algebra $W = (V, \mathcal{R})$, a positive integer p, and a multi-set $S := \{S_{ij} : 1 \leq i, j \leq p\} \subset \mathcal{R}^*$. (That is, each $S_{ij} \in \mathcal{R}^*$, and each S_{ij} need not be distinct, so $|S| \leq p^2$.) We can then define a cylindric relation on S, denoted Cyl_S. $Cyl_S : \mathbb{C}^{|V|} \to \mathbb{C}^{|V|}$, and has the following element-wise definition:

$$\langle x_1, \ldots, x_p | Cyl_S | y_1, \ldots, y_p \rangle = \prod_{i,j=1}^{p} \langle x_i | S_{ij} | y_j \rangle \tag{4.3}$$

A cylindric relation may be thought of as an extension to the previously-mentioned binary relations. Cyl_S "relates" $\{x_1, \ldots, x_p\}$ to $\{y_1, \ldots, y_p\}$ if and only if $S_{ij}(x_i, y_j) = 1$ for all i and j [53]. Additionally, it can be shown [55] that:

$$Cyl_S \in \widehat{W^p}. \tag{4.4}$$

Lastly, let us consider a p-extension $\widehat{\varphi}$. It has been proven [55] that

$$\widehat{\varphi}(Cyl_S) = Cyl_{\varphi(S)} \tag{4.5}$$

where $\varphi(S) = \{\varphi(S_{ij}) : 1 \leq i, j \leq p\}$.

With all the above definitions and properties in mind, we are ready to begin discussing our proofs.

4.3 Proof outline

Each proof provided follows the same procedure. Consider any particular interaction scheme for any particular walk (e.g. three-particle walk with nearest neighbor interactions).

Any given interaction scheme on a graph A has associated interaction Hamiltonian H. To demonstrate that that particular interaction scheme cannot distinguish all graphs, To show that a given kind of walk cannot distinguish all graphs, it is sufficient that there exist a pair of non-isomorphic graphs A and A' which reside in cellular algebras $W = (V, \mathcal{R})$ and $W' = (V', \mathcal{R}')$, respectively, for which the following hold:

1. There exists a weak isomorphism $\varphi : W \to W'$ such that $\varphi(A) = A'$.
2. $H \in \widehat{W}^p$ and $H' \in \widehat{W'}^p$, where H and H' denote the interaction Hamiltonians for A and A', respectively.
3. φ has a p-extension $\widehat{\varphi}$ such that $\widehat{\varphi}(H) = H'$.

It was proved in [5] that if the above conditions hold, our comparison technique (computing the list-distance between the norm-sorted lists of evolution operators) could not distinguish all graphs, as non-isomorphic p-equivalent graphs would not be distinguished. (Given the results of [54], it is known that there exist non-isomorphic p-equivalent graphs for all positive integers p.)

For a walk with p particles, we will consider adjacency matrices A and A' which correspond to two non-isomorphic graph which are p-equivalent. Therefore, the first requirement

has been satisfied, as we know there exists a φ such that $\varphi(A) = A'$. We must then show that, for the interaction in question, each graph's Hamiltonian resides its cellular algebra's p-extension, and that $\widehat{\varphi}$ maps the "unprimed" Hamiltonian to the "primed" one.

We now are ready to present our proofs.

4.4 2-body interaction proofs

In this section, we consider a variety of interaction schemes with varying numbers of particles, but all interactions considered are 2-body interactions.

2 particles; nearest neighbors

In this subsection, we show that the two-particle walk with a nearest-neighbor interaction fails to distinguish all graphs. We begin with the definition of H_1^2, which is given in terms of a graph with adjacency matrix A:

$$\langle x_1 x_2 | H_1^2 | y_1 y_2 \rangle = V_1 \delta_{x_1 y_1} \delta_{x_2 y_2} A_{x_1 x_2}, \tag{4.6}$$

where V_1 is the strength of the nearest-neighbor interaction. (Throughout this chapter, we will denote the strength of an interaction of length d by V_d.) We consider two non-isomorphic graphs 2-equivalent graphs with adjacency matrices A and A' that reside in cellular algebras $W = (V, \mathcal{R})$ and $W' = (V', \mathcal{R}')$, respectively.

To show that H_1^2 resides in $\widehat{W^p}$, we express H_1^2 in terms of a cylindric relation:

$$H_1^2 = V_1 Cyl_S, \tag{4.7}$$

where

$$S = \{S_{ij} : 1 \leq i, j \leq 2\}, \tag{4.8}$$

$$S_{ij} = \begin{cases} I & i = j \\ A & i < j \\ J & \text{otherwise} \end{cases}. \tag{4.9}$$

We check our new definition for H_1^2 and find

$$\langle x_1x_2|H_1^2|y_1y_2\rangle = V_1\prod_{i,j=1}^{2} S_{i,j}(x_i,y_j) = V_1S_{1,1}(x_1,y_1)S_{1,2}(x_1,y_2)S_{2,1}(x_2,y_1)S_{2,2}(x_2,y_2) = V_1\delta_{x_1y_1}A_{x_1y_2}J_{x_2y_1}\delta_{x_2y_2} = V_1\delta_{x_1y_1}\delta_{x_2y_2}A_{x_1x_2}, \tag{4.10}$$

which confirms that (4.7) is a valid definition for H_1^2, and that $H_1^2 \in \widehat{W^p}$.

Now we must see how $\widehat{\varphi}$ acts on H_1^2:

$$\widehat{\varphi}(H_1^2) = V_1Cyl_{\varphi(S)} \tag{4.11}$$

We know that $\varphi(S) = \{\varphi(S_{ij}) : 1 \le i,j \le 2\} = \{\varphi(S_{ij}) : 1 \le i,j \le 2\}$. We know $\varphi(A) = A'$, $\varphi(I) = I$, and $\varphi(J) = J$, thus:

$$\varphi(S_{ij}) = \begin{cases} I & i = j \\ A' & i < j \\ J & \text{otherwise} \end{cases}. \tag{4.12}$$

By inspection, we conclude:

$$\langle x_1x_2|\widehat{\varphi}(H_1^2)|y_1y_2\rangle = V_1\delta_{x_1y_1}\delta_{x_2y_2}A'_{x_1x_2} = \langle x_1x_2|H_1^{2\prime}|y_1y_2\rangle, \tag{4.13}$$

or more simply, $\widehat{\varphi}(H_1^2) = H_1^{2\prime}$. Thus, we have shown that 2-equivalent graphs will not be distinguished by the two-particle nearest-neighbor interaction.

p particles, nearest neighbors

Now we show that p-particle walk with an interaction between nearest neighbors cannot distinguish all graphs. H_1^p is defined on a graph with adjacency matrix A as follows:

$$\langle x_1,\ldots,x_p|H_1^p|y_1,\ldots,y_p\rangle = V_1\delta_{x_1,y_1}\delta_{x_2,y_2}\ldots\delta_{x_p,y_p}(A_{x_1,x_2}+A_{x_1,x_3}+\ldots+A_{x_{p-1},x_p}). \tag{4.14}$$

We note that Equation (4.14) has p δ's, along with a sum of $\binom{p}{2}$ elements of A.

To show $H_1^p \in \widehat{W}^p$, we will first define a set α such that each element $\alpha_i \in \alpha$ is a label for one of the $\binom{p}{2}$ possible pairs of particles in $\{x_1, \ldots, x_p\}$. α is defined as follows:

$$\begin{aligned} \alpha_1 &= (1,2) \\ \alpha_2 &= (1,3) \\ &\vdots \\ \alpha_p &= (1,p-1) \\ \alpha_{p+1} &= (2,3) \\ &\vdots \\ \alpha_{\binom{p}{2}} &= (p-1,p) \end{aligned} \tag{4.15}$$

We now define a cylindric relation Cyl_{S^l}:

$$S^l = \{S^l_{i,j} : 1 \leq i,j \leq p\}, \tag{4.16}$$

where we define $S^l_{i,j}$ as

$$S^l_{ij} = \begin{cases} I & i = j \\ A & (i,j) = \alpha_l \cdot \\ J & \text{otherwise} \end{cases} \tag{4.17}$$

We may now define H_1^p in terms of the cylindric relations Cyl_{S^l}:

$$H_1^p = V_1 \sum_{l=1}^{\binom{p}{2}} Cyl_{S^l}. \tag{4.18}$$

Inspection of Equations (4.15) through (4.18) confirms that our definition of H_1^p in terms of cylindric relations indeed reproduces (4.14). Thus we conclude that $H_1^p \in \widehat{W}^p$.

Now we examine the action of $\widehat{\varphi}$ on H_1^p:

$$\widehat{\varphi}(H_1^p) = V_1 \sum_{l=1}^{\binom{p}{2}} Cyl_{\varphi(S^l)}. \tag{4.19}$$

$Cyl_{\varphi(S^l)} = \{\varphi(S^l_{ij}) : 1 \leq i, j \leq p\}$, so we examine $\varphi(S^l_{ij})$:

$$\varphi(S^l_{ij}) = \begin{cases} I & i = j \\ A & (i,j) = \alpha_l \\ J & \text{otherwise} \end{cases} \tag{4.20}$$

Therefore, we conclude that $\widehat{\varphi}(H_1^p) = H_1^{p\prime}$, so the p-particle walk with a nearest-neighbor interaction cannot distinguish non-isomorphic p-equivalent graphs.

2 particles; d-range interactions

Here we show that the two-particle walk with an interaction for each path of length d between the two particles cannot distinguish all graph pairs. The interaction in question has the following form:

$$\langle x_1 x_2 | H_d^2 | y_1 y_2 \rangle = V_d \delta_{x_1 y_1} \delta_{x_2 y_2} A^d_{x_1 x_2} \tag{4.21}$$

Our previous approach will not work without some modification. That is, we cannot simply define H_d^2 in terms of a cylindric relation similar to the one defined in Equation (4.9), where the only change is that $S_{ij} = A^d$ when $i < j$. This is because $A^d \notin \mathcal{R}^*$, which we know because every element of $\mathcal{R}^*$ is a 0-1 matrix, and A^d is not in general a $0-1$ matrix.

However, not all is lost. We recall the second corollary of our cellular algebra definition, and note for any matrix $A \in W$

$$A^2 = \sum_{i,j=1}^{s} \beta_i \beta_j R_i R_j. \tag{4.22}$$

We additionally recall the third cellular algebra axiom, and we discover

$$A^2 = \sum_{i,j,k=1}^{s} \beta_i \beta_j c^k_{ij} R_k. \tag{4.23}$$

We may generalize this result to express A^d as a linear combination of binary relations:

$$A^d = \sum_{i_1 \ldots i_d = 1}^{s} \beta_{i_1} \ldots \beta_{i_d} R_{i_1} \ldots R_{i_d} = \sum_{i_1 \ldots i_d, j_1 = 1}^{s} \beta_{i_1} \ldots \beta_{i_d} c^{j_1}_{i_1 i_2} R_{j_1} R_{i_3} \ldots R_{i_d} =$$
$$\sum_{i_1 \ldots i_d, j_1 \ldots j_{d-1} = 1}^{s} \beta_{i_1} \ldots \beta_{i_d} c^{j_1}_{i_1 i_2} c^{j_2}_{j_1 i_3} c^{j_3}_{j_2 i_4} \ldots c^{j_{d-1}}_{j_{d-2} i_d} R_{j_{d-1}}. \tag{4.24}$$

To simplify notation, we use the vectors $\mathbf{i}$ and $\mathbf{j}$ to denote the sets of indices $\{i_1 \dots i_d\}$ and $\{j_1 \dots j_{d-1}\}$. Furthermore, we introduce a coefficient with $2d-1$ indices equal to the coefficient of $R_{j_{d-1}}$. We denote this quantity $Z_{\mathbf{ij}}$, simplifying Equation (4.24):

$$A^d = \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} R_{j_{d-1}}. \tag{4.25}$$

Now we may express Equation (4.21) in terms of linear combinations of cylindric relations:

$$H_d^2 = V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} Cyl_{T_{j_{d-1}}}, \tag{4.26}$$

where $Cyl_{T_{j_{d-1}}} = \{S_{m,n}^{j_{d-1}} : 1 \le m,n \le 2\}$ and

$$S_{m,n}^{j_{d-1}} = \begin{cases} I & m = n \\ R_{j_{d-1}} & m < n \\ J & \text{otherwise} \end{cases}. \tag{4.27}$$

We explicitly confirm this correctly yields H_d^2:

$$\langle x_1 x_2 | H_d^2 | y_1 y_2 \rangle = V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} \prod_{m,n=1}^{2} S_{m,n}^{j_{d-1}}(x_m, y_n) =$$

$$V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} S_{1,1}^{j_{d-1}}(x_1,y_1) S_{1,2}^{j_{d-1}}(x_1,y_2) S_{2,1}^{j_{d-1}}(x_2,y_1) S_{2,2}^{j_{d-1}}(x_2,y_2) =$$

$$V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} \delta_{x_1 y_1} R_{j_{d-1}}(x_1,y_2) \cdot 1 \cdot \delta_{x_2 y_2} = V_d \delta_{x_1 y_1} \delta_{x_2 y_2} \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} R_{j_{d-1}}(x_1,y_2). \tag{4.28}$$

Along with Equation (4.25), this confirms that Equation (4.26) provides the correct definition of H_d^2. By extension, we also see that because H_d^2 is a linear combination of cylindric relations, $H_d^2 \in \widehat{W}^2$.

Now we must show that $\widehat{\varphi}(H_d^2) = H_d^{2\prime}$. We note that

$$\widehat{\varphi}(H_d^2) = V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} Z_{\mathbf{ij}} Cyl_{\varphi(T_{j_{d-1}})}. \tag{4.29}$$

The elements of $\varphi(T_{j_{d-1}})$ are $\varphi(S_{m,n}^{j_{d-1}})$, which are defined as

$$\varphi(S_{m,n}^{j_{d-1}}) = \begin{cases} I & m = n \\ R_{\varphi(j_{d-1})} & m < n \\ J & \text{otherwise} \end{cases} . \tag{4.30}$$

Therefore, if we can show that $Z_{\mathbf{ij}} = Z_{\varphi(\mathbf{i})\varphi(\mathbf{j})}$, we will have shown that $\varphi(H_d^2) = H_d^{2\prime}$. This is equivalent to proving:

$$c_{ij}^k = c_{\varphi(i)\varphi(j)}^{\varphi(k)} \tag{4.31}$$

and

$$\beta_i = \beta_{\varphi(i)} \tag{4.32}$$

for all $\{i, j, k\} \in \{1 \dots s\}$.

To prove Equation (4.31), we consider the action of φ on $R_i R_j$:

$$\varphi(R_i R_j) = \varphi\left(\sum_{k=1}^{s} c_{ij}^k R_k\right) = \sum_{k=1}^{s} c_{ij}^k \varphi(R_k) = \sum_{k=1}^{s} c_{ij}^k R_{\varphi(k)}. \tag{4.33}$$

However, we also know that

$$\varphi(R_i R_j) = \varphi(R_i)\varphi(R_j) = R_{\varphi(i)} R_{\varphi(j)} = \sum_{k=1}^{s} c_{\varphi(i)\varphi(j)}^{\varphi(k)} R_{\varphi(k)}. \tag{4.34}$$

Therefore, as each R_i is a 0-1 matrix, and every element of $\mathcal{R}^*$ is also a 0-1 matrix, $c_{ij}^k = c_{\varphi(i)\varphi(j)}^{\varphi(k)}$. We similarly prove Equation (4.32) by considering the action of φ on A:

$$\varphi(A) = \varphi\left(\sum_{i=1}^{s} \beta_i R_i\right) = \sum_{i=1}^{s} \beta_i R_{\varphi(i)}. \tag{4.35}$$

It is also true that

$$\varphi(A) = A' = \sum_{i=1}^{k} \beta_{\varphi(i)} R_{\varphi(i)}. \tag{4.36}$$

By the same reasoning as above, we see that $\beta_i = \beta_{\varphi(i)}$.

Thus, we have shown that $\varphi(H_d^2) = H_d^{2\prime}$, so the two-particle walk with interactions of arbitrary range cannot distinguish p-equivalent graphs.

p particles; d-range interactions

Now we prove our most general result for walks with two-body interactions, that a walk with an arbitrary number of particles and arbitrary interaction range cannot distinguish all graphs. We begin with the definition of H_d^p:

$$\langle x_1 \dots x_p | H_d^p | y_1 \dots y_p \rangle = V_d \delta_{x_1 y_1} \delta_{x_2 y_2} \dots \delta_{x_p y_p} (A^d_{x_1 x_2} + A^d_{x_1 x_3} + \dots + A^d_{x_{p-1} x_p}). \tag{4.37}$$

Drawing on our previous proofs, we will now construct H_d^p as a linear combination of cylindric relations. We introduce the cylindric relation $Cyl_{T_{j_{d-1},l}}$, whose elements are $S_{m,n}^{j_{d-1},l}$, defined as:

$$S_{m,n}^{j_{d-1},l} = \begin{cases} I & m = n \\ R_{j_{d-1}} & (m,n) = \alpha_l \\ J & \text{otherwise.} \end{cases} \tag{4.38}$$

Now we are ready to express H_d^p as a linear combination of cylindric relations:

$$H_p^d = V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} \sum_{l=1}^{\binom{p}{2}} Z_{\mathbf{ij}} Cyl_{T_{j_{d-1},l}}. \tag{4.39}$$

By inspection, we can see that Equation (4.39) correctly reproduces Equation (4.37). Thus, we see that $H_d^p \in \widehat{W}^p$.

Next, we check the action of $\widehat{\varphi}$ on H_d^p:

$$\widehat{\varphi}(H_d^p) = V_d \sum_{\mathbf{i},\mathbf{j}=1}^{s} \sum_{l=1}^{\binom{p}{2}} Z_{\mathbf{ij}} Cyl_{\varphi(T_{j_{d-1},l})}. \tag{4.40}$$

The elements of $\varphi(T_{j_{d-1},l})$ are given by

$$\varphi(S_{m,n}^{j_{d-1},l}) = \begin{cases} I & m = n \\ R_{\varphi(j_{d-1})} & (m,n) = \alpha_l \\ J & \text{otherwise.} \end{cases} \tag{4.41}$$

As we already know that $Z_{\varphi(\mathbf{i})\varphi(\mathbf{j})} = Z_{\mathbf{ij}}$, we see that $\widehat{\varphi}(H_d^p) = H_d^{p\prime}$. Therefore, any quantum random walk with an arbitrary number of particles cannot distinguish non-isomorphic p-equivalent graphs, and therefore cannot be a universal graph isomorphism algorithm.

Fermions and bosons

Thus far, all of our proofs have relied on using distinguishable particle bases. However, we know that the actual systems of interest will contain indistinguishable particles. Here we show that our results for distinguishable particles hold for indistinguishable particles as well (both bosons and fermions). To show this, it is sufficient to show that $\langle x_1 \dots x_p | H_d^p | y_1 \dots y_p \rangle = {}_B\langle x_1 \dots x_p | H_d^p | y_1 \dots y_p \rangle_B$, where the B subscript denotes the state is bosonic and symmetrized accordingly.

We note that H_d^p is diagonal, so it $\langle x_1 \dots x_p | H_d^p | y_1 \dots y_p \rangle \neq 0$ only when the ordered p-tuples $(x_1, \dots x_p)$ and $(y_1 \dots y_p)$ are equal. Thus, we only need to show

$$\langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle = {}_B\langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle_B. \tag{4.42}$$

We additionally note that H_d^p is symmetric under particle interchange, which is to say

$$\langle x_{\pi(1)} \dots x_{\pi(p)} | H_d^p | x_{\pi(1)} \dots x_{\pi(p)} \rangle = \langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle, \tag{4.43}$$

for any permutation $\pi \in S_p$, where S_p is the symmetric group on p objects.

From the definition of symmetrization, we find

$${}_B\langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle_B = \frac{n_1! \dots n_p!}{p!} \sum_{\pi \in \widetilde{S}_p} \langle x_{\pi(1)} \dots x_{\pi(p)} | H_d^p | x_{\pi(1)} \dots x_{\pi(p)} \rangle, \tag{4.44}$$

where n_i denotes the multiplicity of the i^{th} state, and $\widetilde{S}_p$ denotes the subset of S_p that generates unique permutations of $\{x_1 \dots x_p\}$. We know that $|\widetilde{S}_p| = \frac{p!}{n_1! \dots n_p!}$, and the value of each element in the above sum is identical, due to Equation (4.43). Therefore, we conclude

$${}_B\langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle_B = \frac{n_1! \dots n_p!}{p!} \frac{p!}{n_1! \dots n_p!} \langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle = \langle x_1 \dots x_p | H_d^p | x_1 \dots x_p \rangle, \tag{4.45}$$

thus proving Equation (4.42).

The proof for fermions is identical, with the further restriction that $n_i = 1$ for all i, due to the Pauli Exclusion Principle. Therefore, we have shown that our results are general for p-fermion and p-boson interactions.

4.5 Multi-body interactions

Now that we have shown that no two-body interaction scheme can distinguish all graphs, we will consider more general multi-body interactions. We will ultimately provide a proof that no p-body interaction scheme can distinguish p-equivalent graphs, but we will begin with more restrictive cases as examples.

Triangle-interaction

Here we consider a three-body "triangle interaction"- an interaction energy is associated with three particles all adjacent to each other. We consider the case where $p = 3$. We do not explicitly consider the case where $p \geq 3$, as the results in the next subsection include such cases.

An element of the Hamiltonian for this particular interaction is

$$\langle x_1x_2x_3|H^3_\Delta|y_1y_2y_3\rangle = V_\Delta\delta_{x_1y_1}\delta_{x_2y_2}\delta_{x_3y_3}A_{x_1x_2}A_{x_1x_3}A_{x_2,x_3}, \tag{4.46}$$

where V_Δ is the strength of the triangle interaction. Now we introduce the cylindric relation Cyl_{T_Δ}, where $T_\Delta = \{S_{ij} : 1 \leq i, j \leq 3\}$ and

$$S_{ij} = \begin{cases} I & i = j \\ A & i < j \\ J & \text{otherwise} \end{cases}. \tag{4.47}$$

Then we may define our Hamiltonian as

$$H^3_\Delta = V_\Delta Cyl_{T_\Delta}. \tag{4.48}$$

By this definition, we find any element of H^3_Δ to be:

$$\langle x_1x_2x_3|H^3_\Delta|y_1y_2y_3\rangle = V_\Delta \prod_{i,j=1}^{3} S_{ij}(x_i, y_j) = V_\Delta\delta_{x_1y_1}\delta_{x_2y_2}\delta_{x_3y_3}A_{x_1x_2}A_{x_1x_3}, \tag{4.49}$$

confirming that Equation (4.48) provides the correct definition of H^3_Δ. Now we examine the action of $\widehat{\varphi}$ on H^3_Δ:

$$\widehat{\varphi}(H^3_\Delta) = V_\Delta Cyl_{\varphi(T_\Delta)}, \tag{4.50}$$

where the elements of $Cyl_{\varphi(T_\Delta)}$ are $\varphi(S_{ij})$:

$$\varphi(S_{ij}) = \begin{cases} I & i = j \\ A' & i < j \\ J & \text{otherwise} \end{cases} . \tag{4.51}$$

Thus, we see that $\widehat{\varphi}(H^3_\Delta) = H^{3\,\prime}_\Delta$, completing the proof.

Arbitrary hard-core + nearest-neighbor q-body interaction; q-particle walk

We now consider a q-particle walk with a q-body interaction scheme in which an interaction is present if the q particle arrangement matches a specified configuration of $\binom{q}{2}$ pairs of particles, where the relationship between each pair of particles is chosen from the set $C = \{I, A, J-I-A, J-I, J-A, J\}$[3]. An arbitrary interaction of this form corresponds to an array of matrices which we denote θ:

$$\theta = \begin{pmatrix} I & \theta_{1,2} & \cdots & \cdots & \theta_{1,q} \\ J & I & \theta_{2,3} & \cdots & \theta_{2,q} \\ \vdots & & \ddots & & \vdots \\ J & & & I & \theta_{q-1,q} \\ J & \cdots & \cdots & J & I \end{pmatrix} \tag{4.52}$$

Each element of θ is an element of the set C, and we see that $\theta_{ij} = I$ if $i = j$, and $\theta_{ij} = J$ if $i < j$. Then an element of a q-particle walk whose Hamiltonian implements this interaction is:

$$\langle x_1 \dots x_q | H^q_\theta | y_1 \dots y_p \rangle = V_\theta \sum_{\pi \in \widetilde{S}^\theta_q} \prod_{i,j=1}^{q} \theta_{\pi(i),\pi(j)}(x_i, y_j) \tag{4.53}$$

$\widetilde{S}^\theta_q$ is the subset of the symmetric group on q objects whose elements each produce a unique labeled configuration of q particles.[4] We must sum over all relevant particle permutations

[3] These relationships correspond, respectively, to the particles being on the same vertex, adjacent vertices, different and non-adjacent vertices, different vertices, non-adjacent (but possibly same) vertices, or any two vertices.

[4] For example, if we consider a three-body interaction which triggers when particles 1 and 2 are adjacent, and particle 3 is non-adjacent to both 1 and 2, then this interaction must also trigger when particles 2 and

to ensure that our Hamiltonian is symmetric under particle interchange. It should be noted that in general determining the elements of $\widetilde{S}_q^\theta$ is non-trivial. However, for our proof to be successful, we do not need to be able to construct the Hamiltonian efficiently. We simply need to show that the Hamiltonians for two q-equivalent graphs are related by of the q-equivalence's q-extension.

We now introduce the cylindric relation $Cyl_{T_\theta^\pi}$, where $T_\theta^\pi = \{S_{i,j}^{\theta,\pi} : 1 \leq i,j \leq q\}$, and

$$S_{i,j}^{\theta,\pi} = \theta_{\pi(i),\pi(j)}. \tag{4.54}$$

We then define the Hamiltonian in terms of this cylindric relation as

$$H_\theta^q = V_\theta \sum_{\pi \in \widetilde{S}_q^\theta} Cyl_{T_\theta^\pi}. \tag{4.55}$$

By inspection, we see that this reproduces Equation (4.53). To see that $\widehat{\varphi}(H_\theta^q) = H_\theta^{q'}$, we note that

$$\widehat{\varphi}(H_\theta^q) = V_\theta \sum_{\pi \in \widetilde{S}_q^\theta} Cyl_{\varphi(T_\theta^\pi)}, \tag{4.56}$$

and that the elements of $\varphi(T_\theta^\pi)$ are

$$\varphi(S_{i,j}^{\theta,\pi}) = \varphi(\theta_{\pi(i),\pi(j)}) = \theta'_{\pi(i),\pi(j)}. \tag{4.57}$$

We know that Equation (4.57) holds because for each $\theta_{i,j} \in C$, there is a corresponding $\theta'_{i,j} \in C'$, where $C' = \{I, A', J - I - A', J - I, J - A', J\}$. Thus, $\widehat{\varphi}(H_\theta^q) = H_\theta^{q'}$, so q-particle walks with arbitrary nearest-neighbor and hard-core q-body interactions cannot distinguish q-equivalent graphs.

---

3 are adjacent and 1 is not, and also when particles 1 and 3 are adjacent and 2 is not. The symmetric group on three objects has six elements, but we only need to consider three of those six permutations in this example case.

Additionally, we note that two permutations π_α and π_β are equivalent, that is, they do not produce unique configurations of q particles from the configuration θ, if and only if for all $i,j \in [q]$, $(\pi_\alpha^\dagger \theta \pi_\alpha)_{ij} = (\pi_\beta^\dagger \theta \pi_\beta)_{ij}$ or $(\pi_\alpha^\dagger \theta \pi_\alpha)_{ij} = (\pi_\beta^\dagger \theta \pi_\beta)_{ji}$. We allow for the second case because each element of the lower triangle of θ is defined to be J, but permutations of θ need not preserve this property.

Arbitrary hard-core + nearest-neighbor q-body interaction; p-particle walk

We now consider the case where as before, except that the interaction being considered is only a q-body interaction, while there are p ($p > q$) particles in the walk. To show that walks of this kind cannot distinguish p-equivalent graphs, we consider a q-body interaction expressed as an array θ, taking the form presented in Equation (4.52). We can then write down a p-body interaction scheme, denoted Θ, which incorporates the q-body interaction scheme θ, but does not add any additional interactions:

$$\Theta_{i,j} = \begin{cases} \theta_{i,j} & i,j \leq q \\ I & i = j \\ J & \text{otherwise} \end{cases} \tag{4.58}$$

We now retrace the steps of the previous subsection identically, except that particle indices run from 1 to p, and all permutations considered are in a subset of S_p instead of S_q. Thus, the argument from the previous subsection generalizes, so we may state that any p-particle walk with an arbitrary hard-core and nearest-neighbor q-body interaction cannot distinguish p-equivalent graphs.

Arbitrary p-body interactions

Lastly, we address the most general case- a p-particle walk with arbitrary p-body interactions.[5] As before, we can express any p-body interaction as a product of $\binom{p}{2}$ two-body interactions. However, now each two-body interaction θ_{ij} may represent a longer-range interaction. If we consider a graph's cellular algebra $[A] = (V, \mathcal{R})$, then the most general class of "local" interactions which is invariant under vertex permutation is one in which

[5] In the previous section, we showed that q-body interactions in a p-particle walk may be expressed as p-body interactions. The same is true here, so the most general walk is a p-particle walk with a p-body interaction.

each $\theta_{ij} \in [A]$.[6] Therefore, we may state that for any 2-body interaction θ_{ij}:

$$\theta_{ij} = \sum_{m=1}^{|\mathcal{R}|} \beta_m^{ij} R_m, \tag{4.59}$$

where each R_m is an element of $\mathcal{R}$ and β_m^{ij} is its the corresponding coefficient. We can express the array of 2-body interactions in terms of Equation (4.59):

$$\theta = \begin{pmatrix} I & \theta_{1,2} & \cdots & \cdots & \theta_{1,p} \\ J & I & \theta_{2,3} & \cdots & \theta_{2,p} \\ \vdots & & \ddots & & \vdots \\ J & & & I & \theta_{p-1,p} \\ J & \cdots & \cdots & J & I \end{pmatrix} = \begin{pmatrix} I & \sum_{m_1} \beta_{m_1}^{1,2} R_{m_1} & \cdots & \cdots & \sum_{m_{p-1}} \beta_{m_{p-1}}^{1,p} R_{m_{p-1}} \\ J & I & \sum_{m_p} \beta_{m_p}^{2,3} R_{m_p} & \cdots & \sum_{m_{2p-3}} \beta_{m_{2p-3}}^{2,p} R_{m_{2p-3}} \\ \vdots & & \ddots & & \vdots \\ J & & & I & \sum_{m_{\binom{p}{2}}} \beta_{m_{\binom{p}{2}}}^{p-1,p} R_{m_{\binom{p}{2}}} \\ J & \cdots & \cdots & J & I \end{pmatrix} \tag{4.60}$$

We introduce the following notation to simplify further discussion: $\mathbf{m} := (m_1, \ldots, m_{\binom{p}{2}})$, and $\Gamma_{\mathbf{m}} := \beta_{m_1}^{1,2} \cdot \ldots \cdot \beta_{m_p}^{p-1,p}$. Then, with appropriate symmetrization taken into account, we find that an element of the Hamiltonian is

$$\langle x_1 \ldots x_p | H_\theta^p | y_1 \ldots y_p \rangle = V_\theta \delta_{x_1 y_1} \ldots \delta_{x_p y_p} \sum_{\mathbf{m}} \sum_{\pi \in \widetilde{S}_p^\theta} \Gamma_{\mathbf{m}} R_{m_1}(x_{\pi(1)}, x_{\pi(2)}) \cdot \ldots \cdot R_{m_{\binom{p}{2}}}(x_{\pi(p-1)}, x_{\pi(p)}) \tag{4.61}$$

We introduce the following cylindric relation $Cyl_{T^{\mathbf{m},\pi}}$, where $T^{\mathbf{m},\pi} = \{S_{i,j}^{\mathbf{m},\pi} : 1 \leq i, j \leq p\}$, and

$$S_{i,j}^{\mathbf{m},\pi} = \begin{cases} I & i = j \\ R_{m_1} & (\pi(i), \pi(j)) = (1, 2) \\ \vdots & \\ R_{m_{\binom{q}{2}}} & (\pi(i), \pi(j)) = (q-1, q) \\ J & \text{otherwise} \end{cases}. \tag{4.62}$$

[6] By "local" we do not mean "adjacent"; rather, we mean an interaction which does not need to know about any global properties of the graph. Equivalently, each two-body interaction only knows, at most, about the number of paths of a fixed length between two vertices. This can be formally achieved by requiring each θ_{ij} to be a two-body interaction which is a polynomial in linear combinations of I, J, and A. This restriction is required for reasons outlined in the second footnote of the chapter.

Then we may define our Hamiltonian as

$$H_\theta^p = \sum_{\mathbf{m}} \sum_{\pi \in \widetilde{S}_\theta^p} \Gamma_{\mathbf{m}} Cyl_{T^{\mathbf{m},\pi}}. \tag{4.63}$$

This reproduces Equation (4.61), so we see that this Hamiltonian can be expressed in terms of cylindric relations. Lastly, we check the action of $\widehat{\varphi}$ on H_θ^p:

$$\widehat{\varphi}(H_\theta^p) = \sum_{\mathbf{m}} \sum_{\pi \in \widetilde{S}_\theta^p} \Gamma_{\mathbf{m}} Cyl_{\widehat{\varphi}(T^{\mathbf{m},\pi})}. \tag{4.64}$$

By definition, $Cyl_{\widehat{\varphi}(T^{\mathbf{m},\pi})} = \{\varphi(S_{i,j}^{\mathbf{m},\pi}) : 1 \leq i,j \leq p\}$, and we find that

$$\varphi(S_{i,j}^{\mathbf{m},\pi}) = \begin{cases} I & i = j \\ {R_{m_1}}' & (\pi(i),\pi(j)) = (1,2) \\ \vdots & \\ {R_{m_{\binom{q}{2}}}}' & (\pi(i),\pi(j)) = (q-1,q) \\ J & \text{otherwise} \end{cases}. \tag{4.65}$$

Because ${\Gamma_{\mathbf{m}}}' = \Gamma_{\varphi(\mathbf{m})} = \Gamma_{\mathbf{m}}$ (by the same reasoning that $Z_{\mathbf{ij}} = Z_{\varphi(\mathbf{i})\varphi(\mathbf{j})}$, as shown in Subsection 4.4), we see that $\widehat{\varphi}(H_\theta^p) = H_\theta^{p\prime}$. Thus we have completed our final proof, and have demonstrated that any arbitrary p-particle walk with a p-body local interaction cannot distinguish p-equivalent graphs, when used with the L_0 comparison method.

Chapter 5

Power law scaling for the adiabatic algorithm for search engine ranking

5.1 Introduction

Quantum algorithms, which run on quantum computers, are known to be able to outperform classical algorithms for certain computational problems [41, 56]. Thus, finding a new algorithm that exhibits a quantum speedup, in particular an exponential speedup, is of great interest [57]. An extremely important problem in computer science is calculating ranking for search engine results. PageRank, first proposed by Brin and Page [58] underlies the success of the Google search engine [59]. In this algorithm, websites are represented as nodes on a network graph, connected by directed edges that represent links. The matrix of network connections is constructed, and the PageRank vector is its principal eigenvector. Currently, computing the PageRank vector requires a time $O(n)$, where n is the number of websites in the network considered (e.g. the World Wide Web) [6]. Obtaining a quantum algorithm for PageRank that runs exponentially faster than the classical algorithm would be of great interest.

Recently, Garnerone, Zanardi, and Lidar (GZL) proposed an adiabatic quantum algorithm [60] to prepare the PageRank vector for a given network [6]. Remarkably, GZL present

evidence that this algorithm can prepare the PageRank vector in time $O\left[\text{polylog}(n)\right]$, exponentially faster than classical algorithms for certain networks. This runtime is due to the apparent logarithmic scaling of the gap between the two smallest eigenvalues of the Hamiltonian used in the algorithm (the energy gap). This scaling emerged on graphs constructed using adapted versions of two established methods of network construction: the preferential attachment model [61] and the copying model [62]. Both of these models yield graphs that are similar to the connectivity of the World Wide Web in that they are sparse (the total number of edges scales at most proportionally to the number of nodes) and scale-free (the probability of finding a node with a specified in- or out-degree scales as a power law in those degrees). These features lead to networks that exhibit large-scale structure similar to that of the internet, such as being small-world [63] and loosely hierarchical [64]. GZL studied sets of networks that exhibited both logarithmic scaling and polynomial scaling of the gap in the system size. However, they did not demonstrate that the networks with the favorable logarithmic gap scaling are scale-free over the region studied numerically.

Here, we study the scaling of the GZL algorithm for graphs with degree distributions consistent with the internet. A realistic network model of the World Wide Web must be scale-free in both the in- and the out-degree [65, 66]. We consider a broad variety of scale-free networks constructed by different methods. Choosing three well-known models for constructing random, scale-free networks, we control for both the mean degree and the exponent of the power-law governing the degree distribution. We find that graphs with the same degree distribution can have different energy gap and run-time behaviors. Finally, we focus on degree distributions described by power laws consistent with those measured for the Web, both for the in-degree and the out-degree. We find that the relevant energy gap scales as a power of the system size, rather than logarithmically. These results demonstrate that for Web-like graphs, the GZL adiabatic algorithm does not yield an exponential quantum speedup for preparing the PageRank vector compared to current classical algorithms.

5.2 Network growth models

We generate samples of graphs with prescribed degree distributions using three different network growth models. GZL [6] use modified versions of two network construction algorithms: the preferential attachment model [61] and the copying model [62]. In addition to these two models, here we include also the more complex α-preferential attachment model described by Bollobás *et al.* [65, 67]. All three models grow random networks using probabilistic rules at discrete construction steps, which are detailed in Fig. 5.1.

All three of these models produce sparse, scale-free directed networks, in which the probability of the in-degree (the number of incoming edges) and out-degree (the number of outgoing edges) of node i being equal to k are each proportional to a power law:

$$P(d_{in}(i) = k) \sim k^{-\gamma_{in}} \tag{5.1}$$

$$P(d_{out}(i) = k) \sim k^{-\gamma_{out}}, \tag{5.2}$$

where $d_{in}(i)$ and $d_{out}(i)$ are the in- and out-degrees of node i, respectively, and the exponents γ_{in} and γ_{out} are typically between 2 and 4 [61]. The GZL versions [6] of the preferential attachment and copying models [61, 68] produce networks that are scale-free in the limit of large graph size. However, due to the addition procedure described below, the networks are not necessarily scale-free for the sizes of graphs studied numerically here and in Ref. [6]. To achieve networks that are scale-free in the out-degree, GZL suggest to construct two networks, X and Y, independently. X and Y are each generated as in Fig. 5.1, except that for Y the direction of the edges added is reversed. The networks can then be added together, and the weights and loops discarded [6, 69]. The resulting composite network is scale-free in both in-degree and out-degree, provided X and Y have the same number of edges per node. (See Section 5.5 for details.) In contrast to Ref. [6], the graphs studied here are all constrained in this way. However, the graphs exhibiting logarithmic scaling in [6] are not so constrained [69], and so they do not exhibit truly scale-free degree distributions over the numerically studied region. On the other hand, the α-preferential attachment model (considered here but not in [6]) constructs a network which is scale-free in both in- and

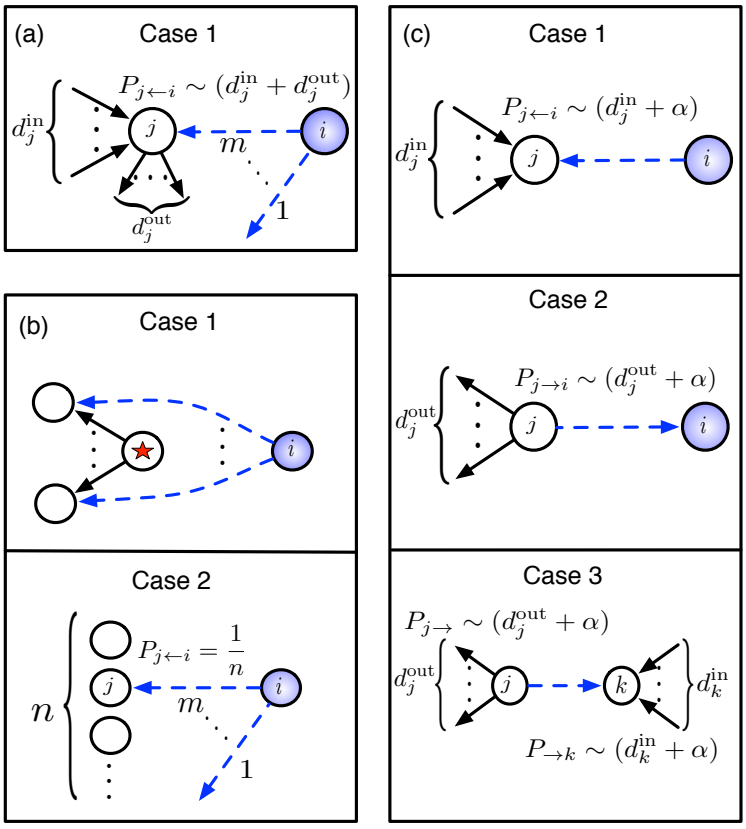

Figure 5.1: Illustrations of the three network generation models used. (a): GZL [6] preferential attachment, (b): GZL copying, and (c): α-preferential attachment [65, 67]. In all three models, a network is constructed by adding vertices and edges sequentially. (a): At each time step a new vertex i is added with m outgoing edges. The probability that one of these edges connects to a node j is proportional to the total degree of j. (b): At each time step there are two possible actions. With probability $(1-p)$, the new vertex points to all of the same vertices as the "star vertex," which is a pre-existing vertex chosen uniformly at random at each time step. With probability p, m outgoing edges are added to the new vertex, each pointing to vertices chosen uniformly at random. (c): There are three possible actions at each time step. With probability p_1, a new vertex is added with a single outgoing edge, pointing to a node j with probability proportional to the in-degree of j plus a parameter α. With probability p_2, a new vertex is added with a single incoming edge, pointing from a node j with probability proportional to the out-degree of j plus α. With probability $(1-p_1-p_2)$, no vertex, only an edge, is added. Its ending and starting points are determined as in cases 1 and 2, respectively. In all panels, the newly-added edges are indicated by dashed lines.

out-degrees without requiring an additional combination step. As with the GZL preferential attachment model, all weights and loops are removed from the final α-preferential attachment network.

The exponents γ_{in} (Eq. 5.1) and γ_{out} (Eq. 5.2) of the degree distribution are model-dependent. In the GZL preferential attachment model the number of edges added at each construction step controls the sparsity, and it is always the case that $\gamma_{in} = \gamma_{out} = 3$ [61]. Both the GZL copying model and α-preferential attachment allow for independently tunable exponents and mean degree. (See Section 5.5 for details.) This flexibility enables us to create three ensembles of model networks that have nearly identical degree distributions for $\gamma_{in} = \gamma_{out} = 3$. Further, the last two models can be set with the exponents estimated for the World Wide Web [62, 65], namely $\gamma_{in} = 2.1$ and $\gamma_{out} = 2.72$ [66].

5.3 Algorithm description

The Google matrix is constructed by taking as input an unweighted, simple network with n nodes [58], and representing it as an adjacency matrix A, where $A(i, j) = 1$ if a directed edge points from node i to node j, and 0 otherwise. From this, one defines the matrix P:

$$P(i,j) = \begin{cases} 1/d_{out}(i) & \text{if } A(i,j) = 1 \quad (5.3a) \\ 1/n & \text{if } \forall j, A(i,j) = 0 \quad (5.3b) \\ 0 & \text{otherwise} \quad (5.3c) \end{cases}$$

The matrix P is stochastic because $\sum_j P(i, j) = 1$ for all i. P can be thought of as a random walk (i.e. a web-surfer), where the walker follows the network with equal likelihood of traversing all allowed links. If the walker ever reaches a dangling node (a node with $d_{out} = 0$), Eq. 5.3b implies that it can randomly hop to any vertex with equal probability. To prevent the walker from becoming trapped in an isolated portion of the network (a sink), the probability $(1 - \alpha_g)$ of moving to a node uniformly at random (including the possibility of staying still) is included, where $0 < \alpha_g < 1$; Google uses $\alpha_g = 0.85$, which we also use here [6]. The Google matrix G is defined as the transpose of this resulting transition matrix:

$$G = \alpha_g P^T + (1 - \alpha_g) J, \tag{5.4}$$

where J is the matrix of all ones. The PageRank vector $\vec{p}$ is the unique eigenvector associated with the largest eigenvalue of G, which is 1. The runtime of the best classical algorithm, which calculates the PageRank vector via power iteration, is $O(n)$ [58, 6].

To formulate an adiabatic quantum algorithm, GZL construct the Hamiltonian $h(G)$:

$$h(G) = (\mathbb{1} - G)^\dagger (\mathbb{1} - G), \tag{5.5}$$

which is Hermitian, even though G is not. ($\mathbb{1}$ is the identity matrix.) The ground state of this Hamiltonian is the normalized PageRank vector. The adiabatic algorithm is completely defined by the interpolation Hamiltonian $H(s) = sh(G) + (1-s)h(G_c)$, where $s \in [0, 1]$, and G_c is the Google matrix for the complfete network (including loops), whose ground state is a uniform superposition. The adiabatic theorem guarantees that if we initialize our system in the ground state of $h(G_c)$ and change s from 0 to 1 sufficiently slowly, the system remains in the ground state [60]. Since the PageRank vector is the ground state of $H(1) = h(G)$, the PageRank vector is obtained when $s = 1$. The required slowness is also determined by the adiabatic theorem: as long as $s(t)$ is a smooth function of the time t with $0 \leq t \leq T$, the runtime $T \sim \delta^{-b}$, where b is $O(1)$ and δ is the energy gap between the ground and first excited state of $H(s)$, minimized over s [60]. Thus, an exponential speedup over the classical case is possible if δ^{-1} is $O[\log(n)]$, since then T is $O[\text{polylog}(n)]$.

5.4 Numerical results

To study the scaling of the minimum energy gap δ with the network size n, we compute δ for the GZL Hamiltonian $H(s)$, averaging the results over many network realizations (typically 1000). Specifically, we calculate the minimum value of δ over $s \in [0, 1]$ using the Nelder-Mead method [70], where each objective function call calculates directly the eigenvalue spectrum of $H(s)$. We find that for most, but not all, network choices the minimum gap occurs when $s = 1$. Since $H(s)$ is a dense matrix, this process is computationally intensive.

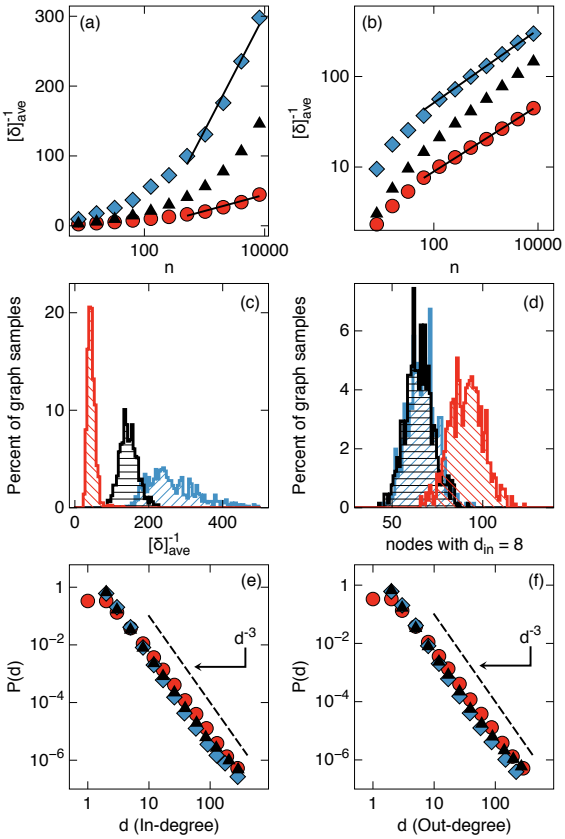

Figure 5.2: Comparison of the scaling of the inverse energy gap δ^{-1} for the GZL [6] preferential attachment model (triangles, horizontal hatching), GZL copying model (diamonds, upward-sloping hatching), and α-preferential attachment model [65] (circles, downward-sloping hatching), shown on (a): Semilog and (b): Log-Log scales, demonstrating that δ^{-1} is not proportional to $\log(n)$ for these models. Results are averaged over 1000 random instances for $n < 8192$, and over 500 random instances at $n = 8192$. The fitting lines showed in (a) are $72.2 \cdot \ln(n) - 363$ for the copying model and $10.1 \cdot \ln(n) - 48.8$ for the α-preferential attachment model. In (b), the fits shown are $8.0 \cdot n^{0.4}$ for the copying model and $1.7 \cdot n^{0.4}$ for the α-preferential attachment model. If we fit the data instead to a power of a logarithm (not shown), we obtain $0.56 \cdot \ln^{2.9}(n)$ for the copying model and $0.18 \cdot \ln^{2.5}(n)$ for the α-preferential attachment model. (c): Histogram of the inverse energy gaps for the data shown in panels (a)-(b) at $n = 8192$. (d): Histogram showing the distribution of number of vertices with in-degree $d_{in} = 8$ for $n = 8192$. (e)-(f): Degree-distributions of the three models, demonstrating scale-free behavior and indicating that $\gamma_{\text{in}} = \gamma_{\text{out}} = 3$. Adaptive binning was used, as described in Section 5.5. In all cases, both the mean in- and out-degree of each graph are 2 edges per node. These results demonstrate that δ^{-1} differs significantly for the different graph construction methods, while the degree distributions are very similar.

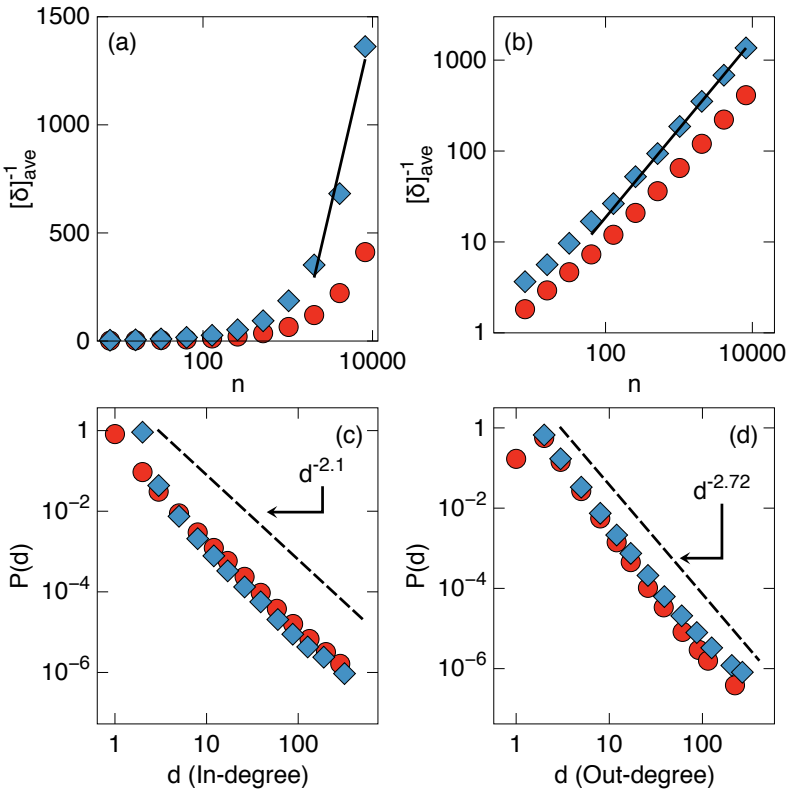

Figure 5.3: Inverse energy gap scaling for GZL [6] copying model (diamonds), and α-preferential attachment model [65] (circles) of WWW-like networks, shown on (a): Semilog and (b): Log-Log scales. Results are averaged over 1000 random instances for $n < 8192$, and over 500 random instances at $n = 8192$. In (a), the line fit shown is $730 \cdot \ln(n) - 5300$, while in (b) the line fit is $0.2 \cdot n^{0.97}$. If we fit the data to a power of a logarithm (not shown), for the copying model we obtain $3 \times 10^{-5} \cdot \ln^{8.0}(n)$. Because of the large power of the logarithm required for the polylogarithmic fit, the power-law dependence on n appears more natural and plausible. (c)-(d): Degree-distributions of the two models, histogrammed using adaptive binning (see Section 5.5.), indicating that $\gamma_{\text{in}} = 2.1$ and $\gamma_{\text{out}} = 2.72$, corresponding to the estimates for the degree distribution of the World Wide Web [66]. In all cases, the mean in- and out-degree of each network were each 2 edges per node.

We use the University of Wisconsin-Madison Center for High Throughput Computing and Open Science Grid to perform the simulations.

To assess whether the inverse energy gap δ^{-1} scales logarithmically or as a power-law in n, we plot in Fig. 5.2 δ^{-1} versus the network size on both log-linear and log-log scales, with data for the GZL preferential attachment, GZL copying, and α-preferential attachment models. The model parameters are tuned (see Section 5.5) so that all three

have $\gamma_{in} = \gamma_{out} = 3$ and have an average of 2 in- and 2 out-edges per node. Despite having nearly identical degree distributions (shown in Figs. 5.2(e) and 5.2(f)), the scaling of δ^{-1} depends significantly on the method used to construct the graphs when viewed in Fig. 5.2(a). In Fig. 5.2(c), we show the distribution corresponding to the final data points in Fig. 5.2(a), where we see that the distributions are well-separated and hence the construction models give different values of δ^{-1}. By contrast, the degree distributions are difficult to distinguish, as shown in Fig. 5.2(d). Finally, we conclude that for all three models, the data are more consistent with δ^{-1} scaling as a power law or a high-order polylogarithm, rather than a logarithm, as consistent with the data presented by GZL in the supplemental information of Ref. [6].

We next perform a similar analysis for degree distributions more closely related to the network of primary interest, the World Wide Web, for which a realistic set of degree parameters is given by $\gamma_{in} = 2.1$ and $\gamma_{out} = 2.72$ [66]. As mentioned above, the preferential attachment model cannot be tuned to obtain degree parameters other than 3. However, the other two network models can be adjusted to match these values [62, 65]. More details on this are discussed in Section 5.5. As before, we set the mean degree to be 2 in- and 2 out-edges per node.

Fig. 5.3 presents the results of these simulations, clearly indicating that δ^{-1} scales at least as a power of n. In particular, we note that the prefactor of the logarithmic fit is over 700 and the power of the logarithm in the polylogarithmic fit is 8, while the power law fit exponent is close to one. The results do not change substantially when the mean degree is varied and the degree distributions exponents are fixed. These data indicate that for graphs with degree distributions similar to those measured for the World Wide Web, the GZL adiabatic algorithm for PageRank vector preparation is unlikely to provide an exponential speedup over the classical case.

5.5 Discussion

We have investigated the recently proposed adiabatic quantum algorithm for preparing the PageRank vector using an adiabatic quantum algorithm [6]. We find that the eigenvalue gap that determines the algorithm runtime depends on the method of construction of the network, even when the feature believed to be critical for large-scale network structure, the degree distribution, is held fixed. The exponent governing the variation of the gap with graph size does not vary significantly with the method of construction only if power-law scaling of the gap with size is assumed. For networks that are scale-free in their in- and out-degree distributions, and particularly when the degree distributions similar to those measured for the World Wide Web, our numerical results indicate strongly that the GZL adiabatic algorithm for PageRank vector preparation does not offer an exponential speedup over current classical algorithms.

5.6 Appendices

A. Parameters of Web Graph Models

In implementing the models used in chapter 5, the relationship between the parameters of the network generation algorithms and the generated networks themselves is not always obvious, so in the following section we explain it in detail.

B. GZL Preferential Attachment

The method of graph construction in the GZL Preferential Attachment Model [6] consists of two phases, each with its own parameter. First, a graph X (with adjacency matrix A_X) is created by adding a new vertex at each time step, where each vertex is created with m_X out-going edges. Next, a second graph Y (with adjacency matrix A_Y) is created in the same fashion, only with each new vertex having m_Y in-coming edges. A_X and A_Y are then added together, with loops and weights discarded, forming the adjacency matrix of the desired network. m_X and m_Y are the two parameters to consider in this algorithm.

In order for a graph to be scale-free, $\Pr(d_{in} = k)$ and $\Pr(d_{out} = k)$, the probabilities that the in-degree d_{in} and the out-degree d_{out} of a random node have the value k, must satisfy

$$\Pr(d_{in} = k) \sim k^{-\gamma_{in}}, \tag{5.6}$$
$$\Pr(d_{out} = k) \sim k^{-\gamma_{out}},$$

where γ_{in} and γ_{out} are positive real numbers, and it is understood that $\Pr(d_{in} = k) = 0$ when $k < m_X$ and $\Pr(d_{out} = k) = 0$ when $k < m_Y$. To compute γ_{in} and γ_{out}, one starts from the undirected version from Ref. [71]. This result is then combined with a constant offset, since each vertex of X has m_x outgoing edges and each vertex of Y has m_Y incoming edges. The resulting composite probability distributions follow

$$\Pr(d_{in} = k) \sim (k + m_X - m_Y)^{-3}, \tag{5.7}$$
$$\Pr(d_{out} = k) \sim (k - m_X + m_Y)^{-3}.$$

Thus, for sufficiently large k, these distributions are scale-free. However, for a large range of intermediate k, we expect substantial deviation from the power law dependence of Eq. (5.6). According to GZL [69], the parameters used to generate Fig. 2 in their paper [6], which provides the main evidence for logarithmic scaling of the gap, follow $m_Y \gg m_X$. In Fig. 5.4, we show the degree distributions for such a network, where we set $m_X = 1$ and $m_Y = 15$. There, we see that the degree distributions are well-described by Eq. (5.7), and that the addition process does indeed distort the degree distributions. By requiring $m_X = m_Y$, as we have done in this paper (and GZL did for a portion of their supplemental material [6]), $\gamma_{in} = \gamma_{out} = 3$ for all k, meaning that the in-degrees and out-degrees both follow the desired power law behavior.

The asymptotic (large number of nodes) value of average edges per node for the composite graph is also determined by the parameters m_X and m_Y. Because m_X is the number of out-going edges per vertex in graph X, it is also the average number of edges per vertex in X. The same logic holds for m_Y and graph Y. Thus, when constructing the composite graph, the asymptotic average edges per node would be simply $m_X + m_Y$. Although loops

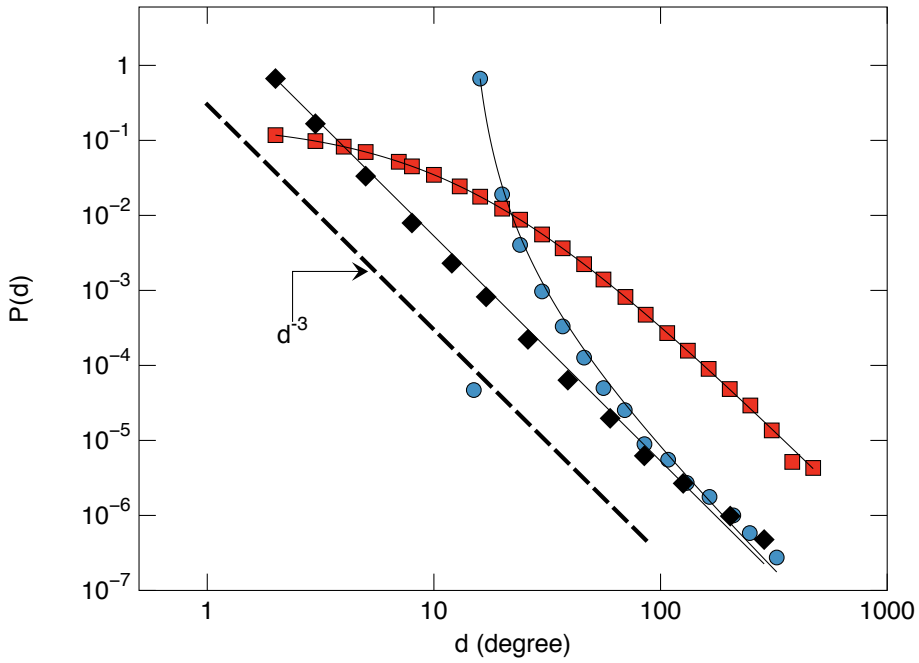

Figure 5.4: Degree distributions for the GZL preferential attachment model with $m_X = 1$ and $m_Y = 15$, taken at graph size $n = 8196$ and averaged over approximately 1000 random graph realizations. Both the in-degree (blue circles) and out-degree (red squares) distributions are shown. For reference, the in-degree distribution for $m_X = 1$ and $m_Y = 1$ (duplicated from Fig. 5.2 of the main text is shown (black diamonds). The dashed line is the expected power law scaling of d^{-3}, which is applicable for large d. As predicted by Eq. (5.7), shown as fitting curves, the $m_X = 1$ and $m_Y = 15$ distributions exhibit non-scale-free behavior over a wide region of d.

are then eliminated from the composite graph, the expected number of loops is much less than n in the large-n case, so this has little effect on the average edges per node. To produce a graph with $\gamma_{in} = \gamma_{out} = 3$ and average in- and out-edges per node of 2 (as in Fig. 2 of the main text), we use this model with $m_X = m_Y = 1$.

C. GZL Copying Model

The parameters of the GZL Copying Model [6] are similar to the GZL Preferential Attachment, as they both involve the adding of two graphs to form a composite graph. We again have the parameters m_X and m_Y, which again indicate the number of out-going edges per node in one component graph and the number of in-coming edges per node in the other.

This model has two new parameters, p_X and p_Y, which are the probabilities of a new node connecting to nodes chosen uniformly at random at a given time step during the construction of X and Y, respectively. We follow Ref. [68] and add a constant offset (just as in the preferential attachment case). Doing so, we again obtain the result that the graphs are scale-free only for $m_X = m_Y$. Assuming this constraint, the composite graph follows

$$\gamma_{in} = \frac{2 - p_X}{1 - p_X}, \tag{5.8}$$

$$\gamma_{out} = \frac{2 - p_Y}{1 - p_Y}. \tag{5.9}$$

For the data in Fig. 2 of the main text, we used the parameters $p_X = p_Y = 0.5$ and $m_X = m_Y = 1$. In Fig. 3 of the main text, we used $p_X = 1/11$ and $p_Y = 35/86$ and $m_X = m_Y = 1$.

D. α-Preferential Attachment

Just as in the GZL Copying Model, there are multiple possible actions at each time step in the α-Preferential Attachment Model [65], and each of these steps has an associated probability. p_1 is the probability of adding a new vertex with a single out-going edge, p_2 is the probability of adding a new vertex with a single in-coming edge, and $1 - p_1 - p_2$ is the probability of an edge being added to the existing network without the addition of a new vertex. α, the third parameter, measures how far the generated network deviates from the GZL preferential attachment model.

As laid out in Ref. [65], the relationship between these 3 parameters and the exponents is

$$\gamma_{in} = \frac{2 + (p_1 + p_2)\alpha - p_2}{1 - p_2}, \tag{5.10}$$

$$\gamma_{out} = \frac{2 + (p_1 + p_2)\alpha - p_1}{1 - p_1}. \tag{5.11}$$

The connection between these parameters and the average number of directed edges per node in the graph is clear when one considers that the probability that a new node will be added at a given time step is $p_1 + p_2$, and a new edge is added at each step.

Using these constraints, we can find appropriate values for the parameters for both Fig. 2 and Fig. 3 of the main text. In Fig. 2, we used $p_1 = p_2 = 0.25$, and $\alpha = 1$, and in Fig. 3, we used $p_1 = 0.415$, $p_2 = 0.0851$, and $\alpha = 0.0128$. These choices in parameters keep γ_{in} and γ_{out} fixed at our desired values, while simultaneously keeping the graph at an average of 2 in- and 2 out-edges per node.

E. Initial Conditions

For each of these models, it is necessary to specify an initial graph to seed the network growth. In our simulations we used a complete graph (including loops) with $m+1$ vertices, where m is the number of edges added per vertex (in the α-Preferential Attachment Model, we used $m = 1$).

F. Adaptive Binning

In the plots of the degree distributions (Figs. 2(e)-(f), Figs. 3(c)-(d), and Fig. 5.4), numerical noise caused by few high-degree vertices leads to data which are difficult to interpret. In order to combat this, we use adaptive binning, which functions as follows. First, some sampling threshold s_t is set, which we take to be 200 in our analysis. If a given data point, corresponding to a degree, contains at least s_t samples, then it is included. If the data point instead has fewer than s_t samples, it is combined with nearby points until the aggregated samples total at least s_t. The weighted average degree and probability are then recorded.

Chapter 6

Compressed sensing for Hamiltonian reconstruction

6.1 Introduction

In quantum physics, the standard method for understanding a large system has long been to make an approximate model Hamiltonian that captures the essential physics of the material in question. More recently, this situation is often turned on its head - a quantum system of n qubits is constructed and we need to find its Hamiltonian from experimental data. To do quantum information processing of any kind, accurate control of the Hamiltonian is always a prerequisite. One needs to be able to apply external control that involves the engineering of a time-dependent Hamiltonian, but it is usually also the case that there are "always-on" terms, generally time-independent or nearly so, in the Hamiltonian that need to be determined at a precise quantitative level. This is a particularly pressing issue for a quantum memory, or in systems that are specifically constructed in order to simulate many-body Hamiltonians . For electron spin qubits in semiconductor quantum dots [72], for example, the single-qubit energy-level splittings are subject to unknown random hyperfine fields, and there are two-qubit interactions due to the dipole-dipole interactions. We will also investigate the challenging case of multi-qubit interactions. In this chapter we propose

an efficient way to determine these "always-on" terms.

For $n = 1$ and $n = 2$, considerable work has been done, since these cases are relevant to the performance of gates [73, 74, 75]. Process tomography is the usual tool for problems with $n > 2$, but standard methods [76, 77] require a number of measurements that scales exponentially with n. Other methods that pertain particularly to spin systems require only a small number of measurements, but they appear to involve full simulation of the system, a task that again scales exponentially [78, 79, 80, 81]. Several authors have investigated the use of techniques from compressed sensing [82] which would give an efficient solution to this problem when the process matrix χ is $s-$sparse (has only s nonzero elements) in some basis [83, 84]. The number of measurements needed to determine χ is then $O(sn)$. However, this scheme requires prior knowledge of the basis in which χ is sparse. Thus it is useful for verifying quantum gates, but cannot be used to determine entirely unknown processes (or Hamiltonians), which is the case we are considering.

As pointed out in Ref. [85], it makes sense to take advantage of the fact that, to a very good approximation, almost all qubit Hamiltonians H have only one- and two-qubit interactions, so that the number of parameters to be determined scales only as n^2. These authors suggest a sequence of randomly chosen measurements on randomly prepared states. If the time interval t between preparation and measurement is short enough: $||H||\ t << 1$, then the density matrix is simply related to H. Here $||H||$ is the operator norm (largest eigenvalue) of H. Compressed-sensing techniques can then come into play and the number of measurements required to determine H is $O(n^3)$. However, $||H||$ grows with the size of the system, which limits the usefulness of this scheme.

6.2 Method

Here we propose a different approach for the experimental determination of H. The most general Hamiltonian for an array of N qubits is:

$$H = -\eta \sum_{a=1}^{4^n-1} J_a \lambda_a \tag{6.1}$$

where a is an N-digit base-4 number $a = a_1 a_2 ... a_N$ and the λ_a are tensor products of Pauli matrices: $\lambda_a = \sigma_{a_1} \otimes \sigma_{a_2} \otimes ... \otimes \sigma_{a_N}$. $\sigma_{1,2,3} = \sigma_{x,y,z}$ and σ_0 is the identity matrix. For notational convenience we have defined the energy scale η and set it by the condition that the dimensionless variables J_a satisfy $|J_a| \leq 1$. We will assume that only s of the $4^n - 1$ possible J_a are zero and $s << 1$. The system is placed in a bath and comes to thermal equilibrium. The density matrix is $\rho = \exp(-\beta H)/Q$, where Q is the partition function: $Q = \mathrm{Tr} \exp(-\beta H)$ and $\beta = 1/k_B T$. If $T = 0$, ρ reduces to $\rho = |0\rangle \langle 0|$ where $|0\rangle$ is the ground state so that the density matrix has rank 1. We will work in the opposite limit: $\eta\beta << 1$. $\rho \sim I - \beta H + \beta^2 H^2/2 + ...$ and in this limit we may truncate the expansion. In general there are a macroscopic number of energy eigenstates that enter ρ and ρ represents a high rank state. It is important to note that the application of compressed sensing proposed here is opposite to others in the literature that primarily focus on the determination of states of low rank [86, 87]. In fact the density matrix is technically of *full* rank at any finite temperature and the naive (but inefficient) procedure to determine the J_a would be to measure the observables λ_a. For $\eta\beta << 1$ this gives $\eta J_a = -2^{-n} \mathrm{Tr}(\lambda_a H) \approx \beta^{-1} \mathrm{Tr}(\lambda_a \rho)$. However, most of the diagonal matrix elements are exponentially small, and we will use this fact to reduce the number of measurements that need to be made.

The measurement and processing protocol is as follows. After the system reaches equilibrium, its state is given by $\rho = 2^{-n} I + 2^{-n} \sum_{a=1}^{4^n-1} v_a \lambda_a$, where $\vec{v}$ is the equilibrium polarization vector of the system. We then subject the system to a random unitary transformation U so that the new state of the system is $\rho' = U \rho U^{-1}$. The procedure for generating random U's that are efficiently implementable with a small gate set is a modification of one proposed for quantum data hiding by DiVincenzo, Leung, and Terhal [88], using work by Harrow and Low on random quantum circuits [89]. The U's are not selected uniformly from the Haar distribution but they appear to provide usable compression matrices. (Details for generating each U are provided in Appendix A.)

The new polarization vector $\vec{v}'$ is linearly related to the previous one: $v'_a = \sum_{b=1}^{4^n-1} C_{ab} v_b$ with $C_{ab} = 2^{-n}\ \mathrm{Tr}\left(\lambda_a U \lambda_b U^{-1}\right)$. C is an orthogonal matrix and $\vec{v}$ is a long but approximately sparse vector, the "signal vector". We now measure M of the observables λ obtaining the results $\{y_k\}_{k=1}^{M}$ with the y_k satisfying $-1 \leq y_k \leq 1$. We will discuss the magnitude of M and the choice of the λ's below. $\vec{y}$ is our "measurement vector", a subset of the elements of $\vec{v}$. We now have

$$y_k = \sum_b C^{(M)}_{kb} v_b, \tag{6.2}$$

where $C^{(M)}$ consists of M rows of C, the choice of rows corresponding to the measurements taken. $C^{(M)}$ is an $M \times (4^n - 1)$ matrix, the "compression matrix". The next step is to estimate the polarization vector by minimizing the L_1 norm of all possible polarization vectors that are consistent with the measurement results:

$$\vec{v}_{est} = \arg\min_{\vec{w}} ||\vec{w}||_1\,, \text{ subject to } \sum_b C^{(M)}_{kb} w_b = y_k. \tag{6.3}$$

The L_1 norm of a vector $\vec{w}$ is defined as $||\vec{w}||_1 = \sum_{i=1}^{d} |w_i|$. This is a convex optimization problem that can be solved efficiently. For our purposes it is important to note that this compressed sensing protocol is stable with respect deviations from exact sparsity in the signal vector, so that, as we shall see below, the protocol works at moderate temperatures. Also, it can be shown that If $C^{(M)}$ is formed by choosing rows at random from C, then $C^{(M)}$ satisfies a certain restricted isometry condition which guarantees that that if $M > A\ n\ \ln^3 s$ we can recover $\vec{v}$ with high probability, Here A is a constant. [90].

Once a good estimate of the polarization vector is available, we can estimate the Hamiltonian:

$$H_{est} = \beta^{-1}(2^{-n}\mathrm{Tr}\,(\ln \rho_{est})\ \ I - \ln \rho_{est}). \tag{6.4}$$

6.3 Results

We now turn to numerical studies of the protocol for 3, 4 and 5 qubits, for which a takes on $N = 63$, $N = 255$, and $N = 1023$ values, respectively. We input a random Hamiltonian,

compute the equilibrium density matrix ρ, and perform M measurements, i.e., characterize ρ by the numbers $\mathrm{Tr}(\lambda_i \rho)\,,\ i = 1, 2, ..., M$. (This is our definition of a measurement.) While measurements are chosen at random, they are ordered by weight, that is all measurements of weight one (i.e., single-qubit measurements) are performed before all measurements of weight two (i.e., two-qubit measurements), and so on. (See Appendix B for further explanation.)

The simplest case is the determination of the J_a when we are given that only s of them are nonzero. We do not have firm guarantees of success at finite temperature, since the density matrix is not s-sparse. So the first task is to determine how high the temperature needs to be to ensure success. The temperature is quantified by the dimensionless ratio $\eta\beta$. Success is measured by the distance of H_{est}, the Hamiltonian estimated from Eq. 6.4, from the actual Hamiltonian H, the metric chosen as the one corresponding to the Frobenius norm: if $(||H_{est} - H||_F)/\eta <$ threshold, the procedure is judged to have succeeded.

Fig. 1 shows the quality of the reconstruction of H as a function of the parameters M/N, which is the number of measurements divided by the signal length, and the sparsity ratio s/N. There are 3 qubits and each pixel in the plots is the result of 100 trials. Note first that the lower right corner is a region where the number of nonzero entries in J_a is greater than the number of measurements: reconstruction is impossible there. As we move away from the diagonal, the success probability increases. As is generally observed in cases where compressed sensing works, the boundary between success and failure (Tanner-Donoho phase transition) is sharp. High temperature is favorable for reconstruction, but even at quite moderate temperatures there is a very substantial region of parameter space where the determination of H succeeds. The red region in both panels is where H is successfully reconstructed, due to the density matrix is approximately sparse in that region.

These computations show that compressed sensing can work in principle, and gives strong evidence that the number of measurements needed is proportional to n, the number of qubits, rather than N, the number of possible couplings, when the Hamiltonian is sparse. However, equipped with the knowledge that H is sparse, quantum state tomography can

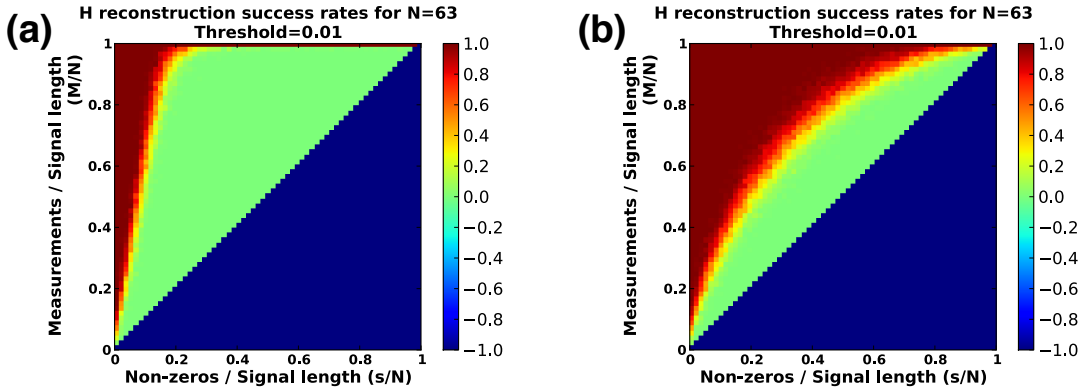

Figure 6.1: Quality of Hamiltonian determination for random couplings as a function of temperature. In (a) and (b) the inverse dimensionless temperature is given by $\eta\beta = 10^{-4}$ and $\eta\beta = 10^{-1}$ respectively. Red indicates a high success rate, green indicates failure, and a negative success rate (blue) means that reconstruction is impossible. Each pixel is an average of 100 trials.

also be carried out with a reduced number of meaurements. We next examine the question of how much advantage is actually gained in practice over the straightforward method of standard tomography, stopping when H has been determined. Fig. 2 gives this comparison for $n = 3$ [Fig. 2(a)], $n = 4$ [Fig. 2(b)], and $n = 5$ [Fig. 2(c)], with small values of s, and for a moderate temperature of $\eta\beta = 10^{-1}$. The number of trials per data point is 100. The sampled M's have a spacing of 1 for $n = 3$ and $n = 4$, starting at a value of $M = 2$; due to computational constraints, every tenth value of M is used for $n = 5$, starting at a value of $M = 11$. The median value of the normalized quality $(||H_{est} - H||_F)/\,||H||_F$ of the estimate is plotted as a function of M, so that low values correspond to accurate estimates. When the curve drops off sharply, the "phase transition" from failure to success has occurred. Thus for example, in Fig. 2(a), the compressed sensing (CS) protocol for $n = 3$ and $s = 1$ succeeds at $M = 5$. It is seen that compressed sensing gives a large saving in the number of measurements for all cases considered, ranging (roughly) from a factor of 4 to 7 for $n = 3$, from 6 to 12 for $n = 4$, and from 12 to as high as 50 for $n = 5$. This is good evidence that the advantage of the compressed sensing protocol increases with n, as we would expect from the scaling arguments above.

In most cases of actual physical interest, we not only have some knowledge of the

sparsity of H, we also have some knowledge of where the nonzeros lie. For example, for spin qubits, 1- and 2-body interactions are likely to be much greater in magnitude than 3- and higher-body interactions. We then find $s = O\left(n^2\right)$. Locality may also reduce the sparsity; for sufficiently short-range interactions $s = O\left(n\right)$. This is a very different situation than we have considered so far, where the nonzero J_a were taken at random. Of course exponential speedups in M are now out of the question. The question is whether we can still get speedups that may be useful in real situations - even constant speedups can be important. So we perform the same numerical experiment as in Fig. 2, but now the nonzero J_a are restricted to those corresponding to λ_a that are 1- and 2-qubit operators, *i.e.*, a has at most 2 nonzero digits. The results are shown in Fig. 3. The number of trials and all other parameters are the same as in Fig. 2. In the "no CS" (standard tomography) protocol, measurements of 1- and 2-body operators are made first, which now improves the performance of the "no CS" procedure, but not enough to overcome the advantage of the CS protocol.[1]

The ratio of the number of measurements required is about a factor of 2 to 4 for $n = 3$, about a factor of 3 to 6 for $n = 4$, and about a factor of 6 to 8 for $n = 5$. Thus the speedup is less when the knowledge of the locations of the nonzeros is increased, but it is still quite substantial. More importantly, it appears that the speedup still increases with the number of qubits.

6.4 Conclusion

Previous improvements in efficiency of quantum state tomography have shown the usefulness of compressed sensing techniques by focusing on the reconstruction of states of low rank. This work, by contrast, uses this technique to reconstruct states of high rank. This is not

[1] The actual "no CS" protocol for reconstructing ρ is as follows. For an estimate of ρ in which M Pauli measurements are allowed, the M expectation values are input as the appropriate v_i's; the remaining v_i's are set to zero. While this estimation procedure could theoretically produce a non-physical ρ_{est} with negative eigenvalues, in practice this is not a concern as any state we are estimating has a polarization vector with a small L_2 norm , while a non-physical density matrix with one or more negative eigenvalues has a polarization vector with a large L_2 norm.

of great interest, for example, for validation of gate quality, but it can be used to determine the parameters in a many-body Hamiltonian.

Compressed sensing is only of value for systems in which measurements are expensive but signal processing and computational post-processing is cheap. This is true in all applications, even in the classical context, but the tradeoffs are vary from case to case. In our protocol, it is assumed that gate operations are cheap but measurements are expensive or destructive. Otherwise, straightforward tomography will be better. The competition between the two is greatly affected by how much advance knowledge we have about the system. It is when we do not have a very good idea in advance about the shape of the Hamiltonian that our method is useful.

6.5 Appendices

A. Generation of U

To choose a random unitary map that is efficiently implementable with a small gate set, we use the following procedure, inspired by a technique for quantum data hiding proposed by DiVincenzo, Leung, and Terhal [88], along with work by Harrow and Low on random quantum circuits [89].

For an n-qubit system, we consider the following set $\mathcal{G}$ of quantum gates

$$\mathcal{G} = \{H_p, P_q, P_r^\dagger, R_s\left(\tfrac{\pi}{8}\right), CNOT_{tu}\}, \tag{6.5}$$

where H is the Hadamard gate, P is the phase gate, $R\left(\frac{\pi}{8}\right)$ is the $\frac{\pi}{8}$ gate, and $CNOT$ is the controlled-not gate. The subscripts label the qubit (or qubits) that each gate is acting on, that is, $\mathcal{G}$ contains all single-qubit copies of $\{H, P, P^\dagger, R\left(\frac{\pi}{8}\right)\}$ and all two-qubit copies of $CNOT$.

To form the unitary map U, we simply select (with replacement) n^8 elements of $\mathcal{G}$ uniformly at random. Letting g_i denote the i^{th} selection from $\mathcal{G}$, we define U to be given by

$$U = \prod_{i=1}^{n^8} g_i. \tag{6.6}$$

Note that this gives us a random unitary operation on n qubits which, while not selected uniformly from the Haar distribution, is sufficiently random as to successfully generate a compression matrix which can be used for compressed sensing. Additionally, we note that it is an open question as to whether or not a smaller set of gates and/or a shorter gate sequence could yield equally successful results.

B. Weight-ordering of measurements

It may be of some benefit to the experimentalist for whom lower weight measurements are easier to perform to be able to prioritize low-weight measurements over high-weight measurements.

Therefore, we show here that the order the measurements are chosen in should not affect the accuracy of the Hamiltonian or the density matrix reconstructions, allowing for the measurements to be chosen according to weight. (That is to say, all single-qubit measurements may performed before any two-qubit measurement, which in turn may precede all three-qubit measurements, and so on.) This ordering by weight is justified in the following manner.

We note that if the k^{th} Pauli measured is λ_k, then the k^{th} element of our measurement vector $\vec{y}$ is given as

$$y_k = \mathrm{Tr}\left(\lambda_k U^\dagger \rho U\right), \tag{6.7}$$

where ρ is the initial density matrix and U is the random unitary map. However, due to the cyclic property of the trace, we may re-express Eq. (6.7) as

$$y_k = \mathrm{Tr}\left(\left(U\lambda_k U^\dagger\right)\rho\right). \tag{6.8}$$

That is, we may consider our k^{th} measurement to correspond to measuring the expectation value a Pauli subjected to a random unitary transformation with respect to the fixed and original density matrix. Therefore, as U effectively randomizes each λ_k, choosing them in

order of their weights should not affect the reconstruction algorithm. (Indeed, we have performed numerical tests which demonstrate this.)

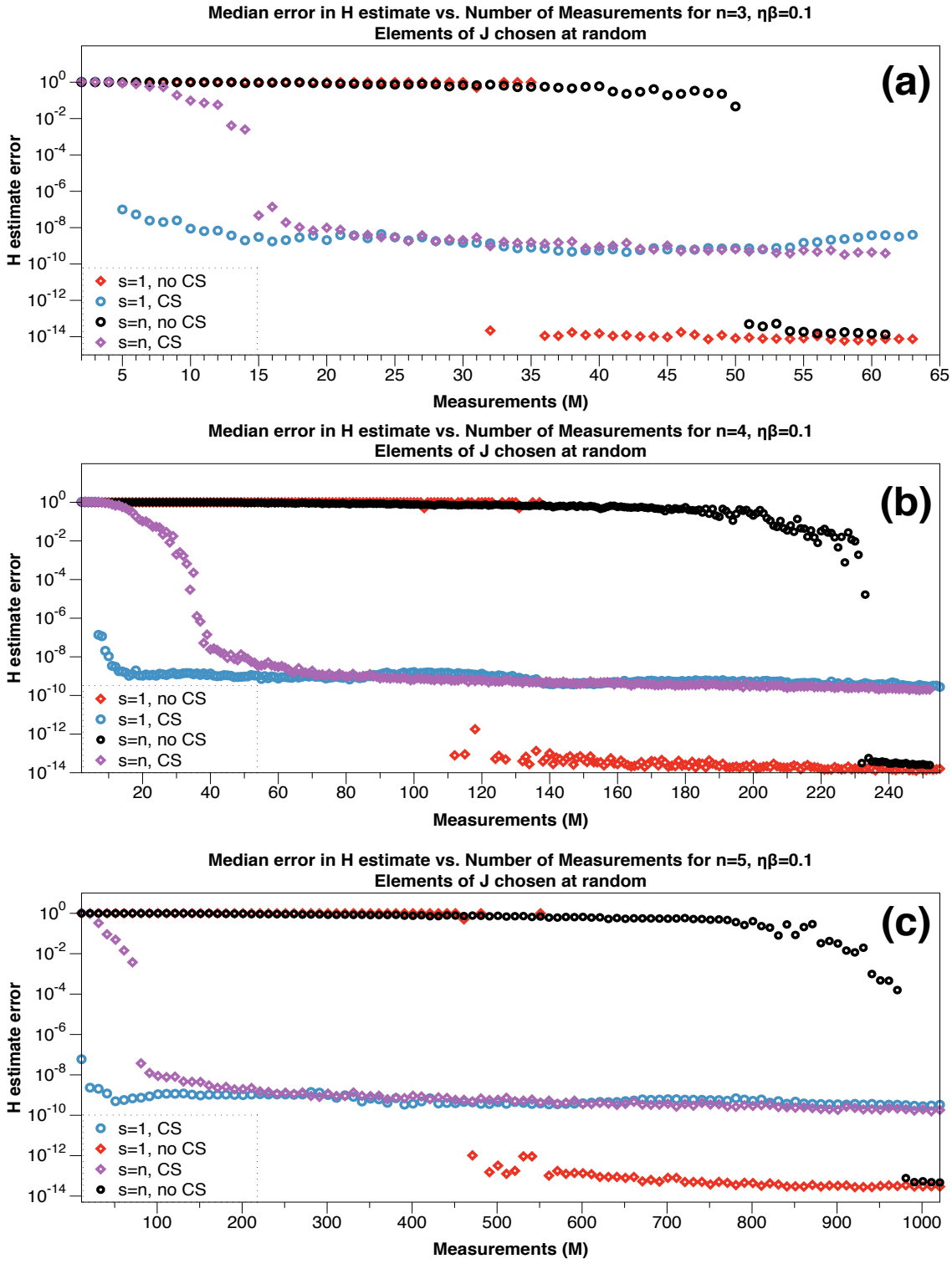

Figure 6.2: Quality of Hamiltonian determination for random couplings as a function of number of qubits. (a), (b), and (c) give the quality of Hamiltonian determination for $n = 3$, 4 and 5 qubits, respectively, as a function of the number of measurements made, with compressed sensing (CS) and without (no CS). In each case, the CS protocol gives a substantial speedup. The speedup increases as the number of qubits increases. Each data point is the median value of 100 trials.

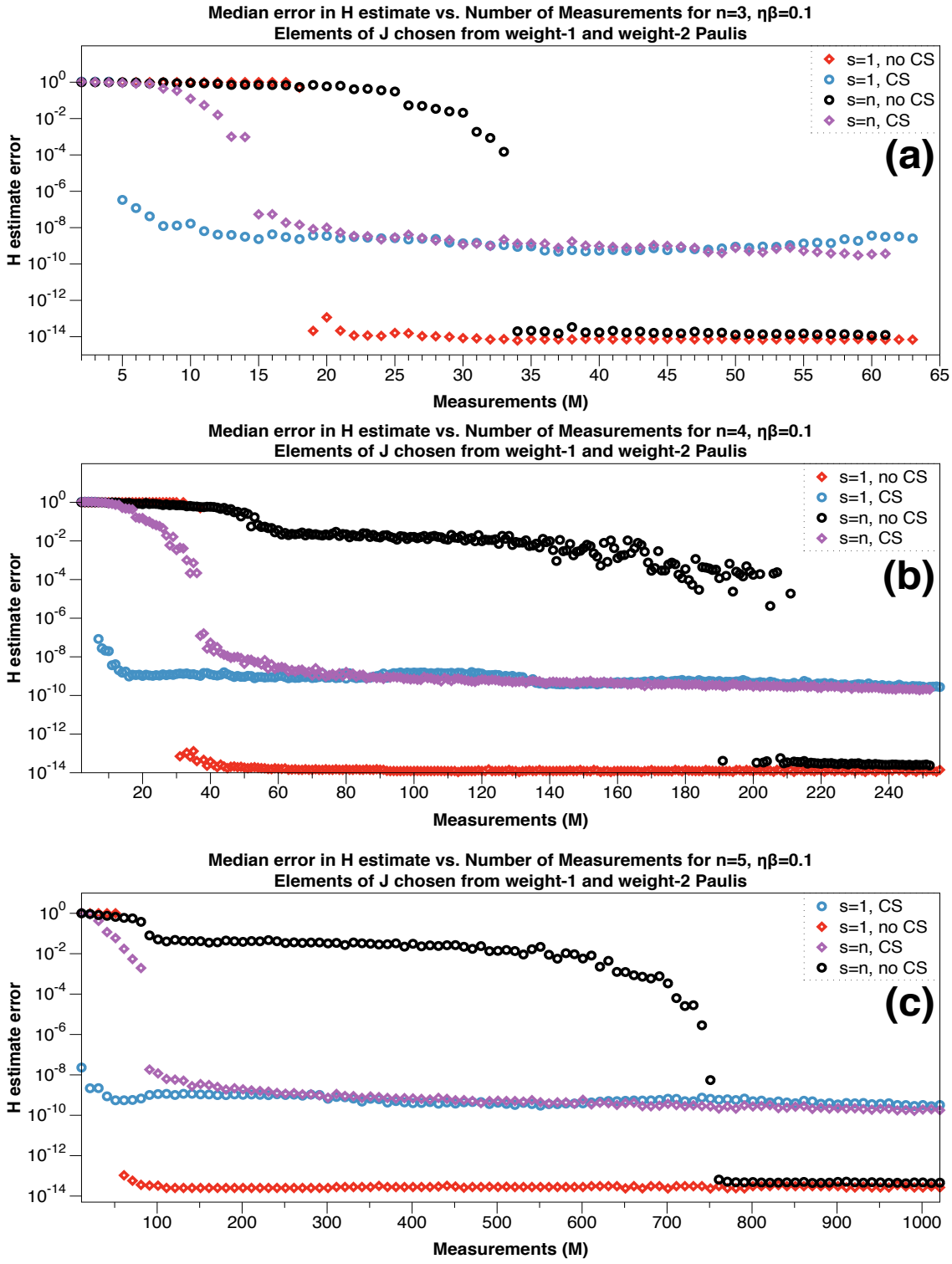

Figure 6.3: Quality of Hamiltonian determination for 1- and 2-qubit couplings as a function of number of qubits. (a), (b), and (c) give the quality of Hamiltonian determination for $n = 3$, 4, and 5 qubits, respectively, as a function of the number of measurements made, with compressed sensing (CS) and without (no CS). In each case, the CS protocol gives a substantial speedup, though not quite as big as for random couplings. The speedup increases as the number of qubits increases. Each data point is the median value of 100 trials.

Chapter 7

Conclusion

Over the course of this thesis, we have covered several different topics and presented several new and interesting results. We have demonstrated new insights regarding quantum random walk-based algorithms for graph isomorphism. In particular, we've shown numerically and analytically why continuous-time walks of three or more non-interacting particles are fundamentally different from such walks of one or two particles. We've additionally shown that even though such walks of three or more particles can distinguish many strongly regular graphs, no such walk of a fixed number of particles can distinguish all strongly regular graphs. Furthermore, we have explicitly shown where fundamental differences between discrete-time and continuous-time walks of non-interacting particles arise from, in terms of ability to distinguish strongly regular graphs. Our graph isomorphism work is rounded out by new results that demonstrate that a broad class of continuous-time interacting quantum random walk algorithms cannot be suitable as general graph isomorphism algorithm candidates.

We have also looked at the previously-proposed adiabatic quantum algorithm, dubbed GZL [6], for determining the PageRank vector as part of one of Google's search algorithms. While there had been hope that the GZL algorithm could offer a significant speedup, we have demonstrated this not to be the case. Specifically, we have shown that while different methods of generating random graphs can each yield graphs whose degree distributions

follow a power law, the eigenvalue gap scaling (and hence the algorithm's runtime) vary dramatically as a function of graph generation method. When graphs which resemble the graph of World Wide Web are considered, we have shown that the GZL algorithm does not offer an exponential speedup.

We have concluded this work with an exploration of how to optimize the determination of a qubit Hamiltonian. We have shown that, in the high-temperature limit, compressed sensing can be used to deduce a Hamiltonian, provided that the Hamiltonian contain a relatively small number of interactions. Thus we have demonstrated how, in certain circumstances, Hamiltonian determination may be achieved with fewer measurements than are demanded by techniques which employ full quantum state tomography.

While we detail all of the above advances in this thesis, it is only natural that there still remain both many open questions to be answered and future work to be done.

For graph isomorphism algorithms, our work immediately points to several potential avenues of further research. While we know that continuous-time walks of two hard-core particles cannot distinguish all graphs, it is still possible that they distinguish all strongly regular graphs. Failing that, it is still possible that there exists a continuous-time walk of a fixed number of interacting particles (with hard-core interactions or more general ones) which can distinguish all strongly regular graphs. Such an algorithm would be of significant interest, as it would be a polynomial time quantum algorithm for distinguishing SRGs, giving an exponential speedup over the best current classical algorithms.

Similar comments could be made regarding discrete-time walks. While we've shown that no fixed-number non-interacting continuous-time walk can distinguish all SRGs, we have been unable to extend this analysis for analogous discrete-time walks. This is to say nothing of further investigating the distinguishing power of interacting discrete-time walks; while Berry and Wang performed numerical investigations of such walks [4], there remains much analytic work to be done to fully understand the power of these walks.

Finally, with regards to graph isomorphism, further work may performed in developing new comparison algorithms. Our comparison algorithms have been restricted in that they

both require computing evolution operators in their entirety, and they are restricted in only allowing for "local" interactions to appear in the Hamiltonian. This then leaves open two possible areas of research. First, it is possible that there exist better algorithms which use efficiently computable observables as their graph certificates. Second, it is possible that "non-local" interactions, that is, those which take advantage of global properties of the graph, could be used to generate walks which could distinguish all graphs. (Such global properties would still have to be efficiently computable, lest we cheat by considering interactions that program the isomorphism class of the graph into the Hamiltonian.)

As for a quantum algorithm for calculating the PageRank vector, there remains much in terms of research potential. While we have shown that the algorithm proposed by Garnerone *et al.* does not offer an exponential speedup, this by no means proves that one does not exist. It is entirely possible that a different quantum algorithm, adiabatic or otherwise, will provide such a speedup. Indeed, such an algorithm could even potentially be very similar to the GZL algorithm, with small, but important, differences. Whether or not any of these conjectures turns out to be true remains to be seen.

Lastly, turning to Hamiltonian determination and compressed sensing, it is clear that there exists more work to do. Further robustness testing of our procedure can be performed, examining, in particular, sensitivity to noisy measurements. Additional optimization may be pursued as well; while we currently require, for a system of n qubits, n^8 gate operations to form our random unitary map, is possible that we can significantly improve upon the length of this gate sequence, making matters easier for the experimentalist. Finally, and perhaps most importantly, while we have demonstrated through numerical simulation that determining a sparse Hamiltonian is possible via compressed sensing at high temperature, this scheme has yet to be experimentally implemented. There exist several different architectures (such as silicon-based spin qubits) that appear to be well-suited for experimentally testing our procedure; it is our hope that in the near future such experimental tests are performed. Ultimately, as is the case with much of theoretical physics, the utility of this work will largely rest upon its ability to impact experimental work. In this particular case,

the hope is that this will work will, either directly or indirectly, assist in the creation and manipulation of working quantum computers.

Bibliography

[1] U. Schöning, "Graph isomorphism is in the low hierarchy.," *J. Comp. Syst. Sci.*, vol. 37, pp. 312–323, Jan 1988.

[2] S. Shiau, R. Joynt, and S. Coppersmith, "Physically-motivated dynamical algorithms for the graph isomorphism problem," *Quantum Inf. Comput.*, vol. 5, pp. 492–506, Jan 2005.

[3] J. K. Gamble, M. Friesen, D. Zhou, R. Joynt, and S. N. Coppersmith, "Two-particle quantum walks applied to the graph isomorphism problem," *Phys. Rev. A*, vol. 81, p. 052313, May 2010.

[4] S. D. Berry and J. B. Wang, "Two-particle quantum walks: Entanglement and graph isomorphism testing," *Phys. Rev. A*, vol. 83, p. 042317, Apr 2011.

[5] J. Smith, "arxiv:1004.0206v1," April 2010.

[6] S. Garnerone, P. Zanardi, and D. A. Lidar, "Adiabatic quantum algorithm for search engine ranking," *Phys. Rev. Lett.*, vol. 108, p. 230506, Jun 2012.

[7] K. Rudinger, J. K. Gamble, M. Wellons, E. Bach, M. Friesen, R. Joynt, and S. N. Coppersmith, "Noninteracting multiparticle quantum random walks applied to the graph isomorphism problem for strongly regular graphs," *Phys. Rev. A*, vol. 86, p. 022334, Aug 2012.

[8] K. Rudinger, J. K. Gamble, M. Wellons, E. Bach, M. Friesen, R. Joynt, and S. N. Coppersmith, "Comparing algorithms for graph isomorphism using discrete- and continuous-time quantum random walks," *J. Comput. Theor. Nanos.*, vol. 7, no. 7, 2013.

[9] A. Frees, J. K. Gamble, K. Rudinger, E. Bach, M. Friesen, R. Joynt, and S. N. Coppersmith, "Power law scaling for the adiabatic algorithm for search engine ranking," 2012.

[10] R. Motwani and P. Raghavan, "Randomized algorithms," *ACM Comput. Surv.*, vol. 28, no. 1, pp. 33–37, 1996.

[11] R. Aleliunas, R. M. Karp, R. J. Lipton, L. Lovasz, and C. Rackoff, "Random walks, universal traversal sequences, and the complexity of maze problems," in *SFCS '79: Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, (Washington, DC, USA), pp. 218–223, IEEE Computer Society, 1979.

[12] Z. Trautt, M. Upmanyu, and A. Karma, "Interface mobility from interface random walk," *Science*, vol. 314, p. 632, Oct 2006.

[13] R. Sessions, M. Oram, and M. Szczelkun, "Random walk models for dna synapsis by resolvase," *J. Mol. Biol.*, vol. 270, pp. 413–425, Jan 1997.

[14] L. Kilian and M. P. Taylor, "Why is it so difficult to beat the random walk forecast of exchange rates?," *J. Int. Econ.*, vol. 60, no. 1, pp. 85 – 107, 2003.

[15] Y. Aharonov, L. Davidovich, and N. Zagury, "Quantum random walks," *Phys. Rev. A*, vol. 48, pp. 1687–1690, Aug 1993.

[16] E. Bach, S. Coppersmith, M. P. Goldschen, R. Joynt, and J. Watrous, "One-dimensional quantum walks with absorbing boundaries," *Journal of Computer and System Sciences*, vol. 69, no. 4, pp. 562 – 592, 2004.

[17] D. Solenov and L. Fedichkin, "Continuous-time quantum walks on a cycle graph," *Phys. Rev. A*, vol. 73, p. 012313, Jan 2006.

[18] A. Childs, E. Farhi, and S. Gutmann, "An example of the difference between quantum and classical random walks," *Quantum Inf. Process.*, Jan 2002.

[19] N. Shenvi, J. Kempe, and K. B. Whaley, "Quantum random-walk search algorithm," *Phys. Rev. A*, vol. 67, p. 052307, May 2003.

[20] A. Ambainis, "Quantum walks and their algorithmic applications," *International Journal of Quantum Information*, vol. 1, pp. 507–518, 2003.

[21] A. Ambainis, "Quantum walk algorithm for element distinctness," *Foundations of Computer Science, Annual IEEE Symposium on*, vol. 0, pp. 22–31, 2004.

[22] F. Magniez, A. Nayak, J. Roland, and M. Santha, "Search via quantum walk," in *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, (New York, NY, USA), pp. 575–584, ACM, 2007.

[23] V. Potoček, A. Gábris, T. Kiss, and I. Jex, "Optimized quantum random-walk search algorithms on the hypercube," *Phys. Rev. A*, vol. 79, p. 012325, Jan 2009.

[24] D. Reitzner, M. Hillery, E. Feldman, and V. Bužek, "Quantum searches on highly symmetric graphs," *Phys. Rev. A*, vol. 79, p. 012323, Jan 2009.

[25] H. Schmitz, R. Matjeschk, C. Schneider, J. Glueckert, M. Enderlein, T. Huber, and T. Schaetz, "Quantum walk of a trapped ion in phase space," *Phys. Rev. Lett.*, vol. 103, p. 090504, Aug 2009.

[26] M. Karski, L. Förster, J.-M. Choi, A. Steffen, W. Alt, D. Meschede, and A. Widera, "Quantum walk in position space with single optically trapped atoms," *Science*, vol. 325, no. 5937, pp. 174–177, 2009.

[27] A. Schreiber, K. N. Cassemiro, V. Potoček, A. Gábris, P. J. Mosley, E. Andersson, I. Jex, and C. Silberhorn, "Photons walking the line: A quantum walk with adjustable coin operations," *Phys. Rev. Lett.*, vol. 104, p. 050502, Feb 2010.

[28] M. A. Broome, A. Fedrizzi, B. P. Lanyon, I. Kassal, A. Aspuru-Guzik, and A. G. White, "Discrete single-photon quantum walks with tunable decoherence," *Phys. Rev. Lett.*, vol. 104, p. 153602, Apr 2010.

[29] C. A. Ryan, M. Laforest, J. C. Boileau, and R. Laflamme, "Experimental implementation of a discrete-time quantum random walk on an nmr quantum-information processor," *Phys. Rev. A*, vol. 72, p. 062317, Dec 2005.

[30] F. Zähringer, G. Kirchmair, R. Gerritsma, E. Solano, R. Blatt, and C. F. Roos, "Realization of a quantum walk with one and two trapped ions," *Phys. Rev. Lett.*, vol. 104, p. 100503, Mar 2010.

[31] J. O. Owens, M. A. Broome, D. N. Biggerstaff, M. E. Goggin, A. Fedrizzi, T. Linjordet, M. Ams, G. D. Marshall, J. Twamley, M. J. Withford, and A. G. White, "Two-photon quantum walks in an elliptical direct-write waveguide array," *New Journal of Physics*, vol. 13, no. 7, p. 075003, 2011.

[32] A. Peruzzo, M. Lobino, J. C. F. Matthews, N. Matsuda, A. Politi, K. Poulios, X.-Q. Zhou, Y. Lahini, N. Ismail, K. Wörhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson, and J. L. OBrien, "Quantum walks of correlated photons," *Science*, vol. 329, no. 5998, pp. 1500–1503, 2010.

[33] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame, "Two-particle bosonic-fermionic quantum walk via integrated photonics," *Phys. Rev. Lett.*, vol. 108, p. 010502, Jan 2012.

[34] K. Manouchehri and J. B. Wang, "Quantum random walks without walking," *Phys. Rev. A*, vol. 80, p. 060304, Dec 2009.

[35] A. M. Childs, "Universal computation by quantum walk," *Phys. Rev. Lett.*, vol. 102, p. 180501, May 2009.

[36] R. Burioni, D. Cassi, I. Meccoli, M. Rasetti, S. Regina, P. Sodano, and A. Vezzani, "Bose-einstein condensation in inhomogeneous josephson arrays," *Europhys. Lett.*, vol. 52, p. 251, Nov 2000.

[37] P. Buonsante, R. Burioni, D. Cassi, and A. Vezzani, "Bose-einstein condensation on inhomogeneous networks: Mesoscopic aspects versus thermodynamic limit," *Phys. Rev. B*, vol. 66, p. 094207, Sep 2002.

[38] F. P. Mancini, P. Sodano, and A. Trombettoni, "Bec in a star-comb graph," *AIP Conference Proceedings*, vol. 918, p. 302, 2007.

[39] D. A. Spielman, "Faster isomorphism testing of strongly regular graphs," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, (New York, NY, USA), pp. 576–584, ACM, 1996.

[40] C. Moore, A. Russell, and P. Sniady, "On the impossibility of a quantum sieve algorithm for graph isomorphism," in *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, (New York, NY, USA), pp. 536–545, ACM, 2007.

[41] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *SFCS '94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, (Washington, DC, USA), pp. 124–134, IEEE Computer Society, 1994.

[42] D. Emms, S. Severini, R. Wilson, and E. Hancock, "Coined quantum walks lift the cospectrality of graphs and trees," *Pattern Recogon.*, Jan 2009.

[43] C. Godsil and K. Guo, "Quantum walks on regular graphs and eigenvalues," *The Electronic Journal of Combinatorics*, vol. 18, no. 1, 2011.

[44] F. W. Strauch, "Connecting the discrete- and continuous-time quantum walks," *Phys. Rev. A*, vol. 74, p. 030301, Sep 2006.

[45] C. Godsil and G. Royle, *Algebraic Graph Theory*. Springer, 2001.

[46] R. B. Sidje, "Expokit. A software package for computing matrix exponentials," *ACM Trans. Math. Softw.*, vol. 24, no. 1, pp. 130–156, 1998.

[47] D. S. Stones, "The many formulae for the number of latin rectangles," *Electr. J. Comb.*, vol. 17, 2010.

[48] B. McKay and I. Wanless, "On the number of latin squares," *Annals of Combinatorics*, vol. 9, pp. 335–344, 2005. 10.1007/s00026-005-0261-7.

[49] A. Tucker, *Applied Combinatorics*. John Wiley & Sons, 4 ed., 2004.

[50] F. C. Auluck, "On partitions of bipartite numbers," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 49, no. 1, p. 72, 1953.

[51] C. L. Liu, *Introduction to Combinatorial Mathematics*. McGraw-Hill, 1968.

[52] D. Emms, S. Severini, R. C. Wilson, and E. R. Hancock, "Coined quantum walks lift the cospectrality of graphs and trees," *Pattern Recogn.*, vol. 42, September 2009.

[53] J. Garnerone private communication, 2012.

[54] A. Barghi and I. Ponomarenko, "Non-isomorphic graphs with cospectral symmetric powers," *Electr. J. Comb.*, vol. 16, Sept 2009.

[55] S. Evdokimov, M. Karpinski, and I. Ponomarenko, "On a new high dimensional weisfeiler-lehman algorithm," *Journal of Algebraic Combinatorics*, vol. 10, pp. 29–45, 1999. 10.1023/A:1018672019177.

[56] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, (New York, NY, USA), pp. 212–219, ACM, 1996.

[57] D. Bacon and W. van Dam, "Recent progress in quantum algorithms," *Commun. ACM*, vol. 53, pp. 84–93, Feb. 2010.

[58] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," *Computer Networks and ISDN Systems*, vol. 30, no. 1-7, pp. 107 – 117, 1998.

[59] P. Berkhin, "A survey on pagerank computing," *Internet Math*, vol. 2, no. 1, pp. 73–120, 2005.

[60] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," *arXiv:quant-ph/0001106v1*, 2000.

[61] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[62] B. Bollobás, O. Riordan, J. Spencer, and G. Tusnády, "The degree sequence of a scale-free random graph process," *Random Structures and Algorithms*, vol. 18, no. 3, pp. 279–290, 2001.

[63] R. Cohen and S. Havlin, "Scale-free networks are ultrasmall," *Phys. Rev. Lett.*, vol. 90, p. 058701, Feb 2003.

[64] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger, "Network topology generators: degree-based vs. structural," in *SIGCOMM '02: Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*, (New York, NY, USA), pp. 147–159, ACM, 2002.

[65] B. Bollobás, C. Borgs, J. Chayes, and O. Riordan, "Directed scale-free graphs," in *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, SODA '03, (Philadelphia, PA, USA), pp. 132–139, Society for Industrial and Applied Mathematics, 2003.

[66] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener, "Graph structure in the web," *Comput. Netw.*, vol. 33, pp. 309–320, June 2000.

[67] F. Chung and L. Lu, *Complex Graphs and Networks (Cbms Regional Conference Series in Mathematics)*. No. 107, Boston, MA, USA: American Mathematical Society, 2006.

[68] J. M. Kleinberg, R. Kumar, P. Raghavan, S. Rajagopalan, and A. S. Tomkins, "The web as a graph: measurements, models, and methods," in *Proceedings of the 5th annual international conference on Computing and combinatorics*, COCOON'99, (Berlin, Heidelberg), pp. 1–17, Springer-Verlag, 1999.

[69] S. Garnerone private communication, 2012.

[70] J. Nelder and R. Mead, "A simplex method for function minimization," *Computer Journal*, vol. 7, pp. 308–313, 1965.

[71] A. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Physica A*, vol. 272, pp. 173–187, 1999.

[72] D. P. DiVincenzo and D. Loss, "Quantum information is physical," *Superlatt Microstruct*, vol. 23, no. 3-4, pp. 419 – 432, 1998.

[73] J. H. Cole, S. G. Schirmer, A. D. Greentree, C. J. Wellard, D. K. L. Oi, and L. C. L. Hollenberg, "Identifying an experimental two-state hamiltonian to arbitrary accuracy," *Phys. Rev. A*, vol. 71, p. 062312, Jun 2005.

[74] S. J. Devitt, J. H. Cole, and L. C. L. Hollenberg, "Scheme for direct measurement of a general two-qubit hamiltonian," *Phys. Rev. A*, vol. 73, p. 052317, May 2006.

[75] S. G. Schirmer and D. K. L. Oi, "Two-qubit hamiltonian tomography by bayesian analysis of noisy data," *Phys. Rev. A*, vol. 80, p. 022333, Aug 2009.

[76] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

[77] I. L. Chuang and M. A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box," *Journal of Modern Optics*, vol. 44, pp. 2455–2467, Nov. 1997.

[78] D. Burgarth, K. Maruyama, and F. Nori, "Coupling strength estimation for spin chains despite restricted access," *Phys. Rev. A*, vol. 79, p. 020305, Feb 2009.

[79] D. Burgarth and K. Maruyama, "Indirect hamiltonian identification through a small gateway," *New. J. Phys.*, vol. 11, no. 10, p. 103019.

[80] D. Burgarth, K. Maruyama, and F. Nori, "Indirect quantum tomography of quadratic hamiltonians," *New. J. Phys.*, vol. 13, no. 1, p. 013019.

[81] C. Di Franco, M. Paternostro, and M. S. Kim, "Hamiltonian tomography in an access-limited setting without state initialization," *Phys. Rev. Lett.*, vol. 102, p. 187203, May 2009.

[82] E. Candès and M. Wakin, "An introduction to compressive sampling," *Signal Processing Magazine, IEEE*, vol. 25, pp. 21–30, March 2008.

[83] A. Shabani, R. L. Kosut, M. Mohseni, H. Rabitz, M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, "Efficient measurement of quantum dynamics via compressive sensing," *Phys. Rev. Lett.*, vol. 106, p. 100401, Mar 2011.

[84] C. Baldwin, A. Kalev, and I. Deutsch, "arxiv:1404.2877v2," April 2014.

[85] A. Shabani, M. Mohseni, S. Lloyd, R. L. Kosut, and H. Rabitz, "Estimation of many-body quantum hamiltonians via compressive sensing," *Phys. Rev. A*, vol. 84, p. 012107, Jul 2011.

[86] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Phys. Rev. Lett.*, vol. 105, p. 150401, Oct 2010.

[87] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, "Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators," *New Journal of Physics*, vol. 14, no. 9, p. 095022, 2012.

[88] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, "arxiv:quant-ph/0103098v1," Mar 2001.

[89] A. W. Harrow and R. A. Low, "arxiv:0802.1919v3," Oct 2009.

[90] R. Vershynin, "arxiv:1011.3027v7," April 2010.