A geometric perspective on some arithmetic statistic questions over function fields over finite fields

By

Vlad Matei

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2017

Date of final oral examination: May 10, 2017

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

Jordan S. Ellenberg, John D. MacArthur Professor, Mathematics

Melanie Matchett Wood, Associate Professor, Mathematics

Daniel Erman, Assistant Professor, Mathematics

Tonghai Yang, Professor, Mathematics

Autumn Kent, Associate Professor, Mathematics

This thesis is dedicated to the memory of my grandmother, Leana Litoiu and my grandfather, Gheorghe Litoiu

“Grandparents have silver in their hair and gold in their heart”

Abstract

There are many interesting problems in analytic number theory over the integers or more generally, number fields, but most of them are notoriously difficult to solve and out of reach at the moment. In recent years, people have started investigating the analogous problems over function fields over finite fields and obtained the expected results. This gives us more reason to believe the conjectures over the integers or help us make predictions about what the conjecture should be.

The motivation for the present thesis is one such problem, namely how many integers from 1 to X can be written as a sum of two integers square. Both the result over the integers, in classic work of Landau, and the function field result, done by Lior Bary Soroker, Yotam Smilanski and Adva Wolf in [5] and Ofir Gorodetsky in [21], are well understood.

In this thesis we expand upon the known function field result obtaining a complete description of one of the main theorems in [5]. Moreover, we discover interesting geometric properties that govern this statistic, more precisely a homological stability result. The approach we take is a geometric one, using a twisted Grothendieck Lefschetz, and is inspired by the Church-Ellenberg-Farb paper [9]. We obtain two new statistics, the number of irreducible polynomials and the expected number of roots.

The twisted Grothendieck Lefschetz formula, that will be at the heart of our computations, has been also proven independently in [39] and generalized in [8].

Acknowledgements

First and foremost this thesis would not have been possible without the help and support of my advisor, Jordan S. Ellenberg. He has been a constant source of inspiration and optimism, encouraging me to pursue the problems I've liked, and offering great advice. His passion for mathematics, his way of thought and vision of how things should work have been great models for me, made a better mathematician and I hope that I will be able to be as inspirational to my future students. Thanks Jordan.

I would like to thank also my readers, Melanie Matchett Wood and Daniel Erman for the corrections and suggestions that lead to the improvement of the present manuscript and to Alina Bucur, Chantal David, Lior Bary-Soroker, and Zeév Rudnick for comments and insights into material related to this thesis.

Thirdly I am grateful for the stimulating mathematics discussions that I've had with all the amazing professors I've met here at UW Madison or at various conferences across the US.

The math department has been a wonderful and productive place of research, teaching and fun. I am grateful for all the staff members that helped with various administrative issues.

I would like to thank also my former professors at the University of Cambridge, John Coates, and at the University of Bucharest, Victor Vuletescu, and Gica Alexandru. I am especially indebted to my high school teacher, Chera Ioan, who discovered my talent and passion for mathematics.

I am grateful for my friends here at UW Madison, from conferences and from back

home for all their help and friendship. A special thanks goes to my collaborators, Daniel Hast and Joseph Gunther for their patience and the math we did together. Another special thanks goes to Cosmin Pohoata, Georgescu Flavian and Cezar Lupu.

Many thanks also go to my father and mother, who always encouraged me to pursue my dreams, work hard and supported me in all aspects of life.

Contents

Chapter 1

Introduction

1.1 A brief overview of analytic number theory over $\mathbb{Z}$

Since most of the questions we explore are motivated by questions over $\mathbb{Z}$ we give a brief account on what type of problems are in the general area of analytic number theory over the integers. The center of focus for most analytic number theory over $\mathbb{Z}$ is understanding the behavior of prime numbers. We will only do a brief exposition; a thorough account can be found in the books by Iwaniewic and Kowalski ([28]) and Ivíc([27]).

We know, going back to Euclid, that there are infinitely many prime numbers. The next obvious questions are can we obtain formula for the n-th prime number, how many are there in a interval $[1, X]$, how are they spaced out i.e how small can the distance between two consecutive primes be and how large could it be, how are they distributed and so on.

All these sort of questions have been at the heart of the subject. These questions can be unified by understanding well the behavior of the Riemann zeta function, or more general functions, called L-functions, as we shall see later in the section. This function was introduced by Riemann in 1859 ([38]). More specifically, for $\Re(s) > 1$ consider the series:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

where s is a complex variable. It is easy to see that the series converges for $\Re(s) > 1$ and is absolutely and uniformly convergent in the domain $\Re(s) \geq 1 + \delta$ for every $\delta > 0$. Thus $\zeta(s)$ is holomorphic for $\Re(s) > 1$ and we have the Euler product formula

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

first discovered by Euler in 1737 ([19]).

Using this Euler was able to show the first quantitative estimate

$$\log(\log(x)) = \sum_{p \leq x} \frac{1}{p} + O(1)$$

Riemann moreover introduced the meromorphic continuation of $\zeta(s)$, with a simple pole at $s = 1$ to the whole complex plane. More precisely defining

$$\eta(s) := \frac{s(s-1)}{2} \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

we have the functional equation $\eta(s) = \eta(1 - s)$.

This lead Riemann to conjecture the celebrated Riemann hypothesis

Conjecture 1.1 *The nontrivial zeroes of $\zeta(s)$ all have real part equal to $\frac{1}{2}$.*

A weaker version, namely knowing that the Riemann Zeta has no zeroes on the line $\Re(s) = 1$ gives us

Theorem 1.2 (Prime number theorem) *Let $\pi(x) = \sum_{p \leq X} 1$. Then*

$$\pi(x) \sim \frac{X}{\log(X)}$$

as $X \to \infty$.

The Prime Number Theorem was first conjectured by Legendre and Gauss and for about 100 years it remained open, despite numerous attempts. It was proven in 1896 by J. Hadamard ([25]) and C. J. de la Vallée Poussin ([37]) independently proved the result.

The Riemann hypothesis would imply a stronger asymptotic

$$\pi(x) = \frac{X}{\log(X)} + O(\sqrt{X}\log(X))$$

It turns out that if we want to ask more refined questions about primes, we need to define a more general class of functions which enjoy the same good properties that the Riemman zeta function has. These are the L-functions. We will limit the presentation to just describing Dirichlet L-functions.

Definition 1.3 *A Dirichlet character of modulus* q*, where* $q \in \mathbb{N}$*, is a function* $\chi : \mathbb{Z} \to \mathbb{C}$ *such that*

(i) $\chi(mn) = \chi(m)\chi(n)$*, for all* $m, n \in \mathbb{Z}$

(ii) $\chi(n+q) = \chi(n)$*, for all* $n \in \mathbb{Z}$

(iii) $\chi(1) = 1$*, and*

(iv) $\chi(n) = 0$ *whenever* $(n, q) \neq 1$*, i.e* n *and* q *are not coprime.*

By this definition we have that χ has period q. But this might not be it's smallest period. This motivates the following definition

Definition 1.4 *Let χ be a Dirichlet character modulo q and let $d = q$. The number d is called an induced modulus for χ if*

$$\chi(a) = 1 \textit{ whenever } (a, q) = 1 \textit{ and } a \equiv 1 \pmod{d}$$

In this case we also say that the character induced from modulo d. A character will be called primitive if it is not induced from any modulus $d < q$.

We are ready to define the Dirichlet L-functions.

Definition 1.5 *Let χ be a Dirichlet character modulo q. The Dirichlet L-function corresponding to χ is defined to be*

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

In a similar way to the Riemann zeta the Dirichlet L-function is absolutely convergent for $\Re(s) > 1$. Moreover if we exclude χ_0, the principal character modulo q i.e $\chi(a) = 1$ for every $(a, q) = 1$, we have a holomorphic function for $\Re(s) > 0$. Using the multiplicative property of characters we recover the Euler product formula

$$L(s, \chi) := \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Now restricting to primitive characters we can define a completed L-function by

$$\Lambda(\frac{1}{2} + s, \chi) = \left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{s + \frac{2-\chi(-1)}{2}}{2}\right) L(\frac{1}{2} + s, \chi)$$

This also enjoys a functional equation, namely:

$$\Lambda(\frac{1}{2} + s, \chi) = \frac{\tau(\chi)}{i^{(1-\chi(-1))/2}\sqrt{q}} \Lambda(\frac{1}{2} - s, \overline{\chi})$$

where $\tau(\chi)$ is the Gauss sum, i.e

$$\tau(\chi) := \sum_{j=1}^{q} \chi(j) e(n/q)$$

where $e(x) := \exp(2\pi i x)$.

Thus we obtain again an analytic continuation to the whole complex plane, and moreover it is regular everywhere. The zeroes, as before, have to lie in the critical strip and we obtain a generalization of the Riemann hypothesis

Conjecture 1.6 *(Grand Riemann Hypothesis) All non-trivial zeroes of Dirichlet L-functions lie on the critical line.*

In analogy with the proof of the P.N.T the fact that $L(1,\chi) \neq 0$ implies Dirichlet's theorem on arithmetic progressions. More precisely:

Theorem 1.7 *The arithmetic progressions $\{a + nq\}_{n\in\mathbb{Z}}$, where $(a,q) = 1$ contains infinitely many prime numbers.*

We end this section by presenting one more historic result that helps us get quantitative estimates. This is a version of the Wiener Ikehara tauberian theorems which can be found in [36].

Theorem 1.8 *Let $f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ with $a_n \geq 0$ and convergent for $\Re(s) > a > 0$. Assume that in the domain of convergence we can write $f(s) = g(s)(s-a)^{-b} + h(s)$, where g, h are holomorphic functions in the closed halfplane $\Re(s) \geq a$, and morover $g(a) \neq 0$, and $b > 0$. Then*

$$\sum_{1\leq n\leq X} a_n = \frac{g(a)}{a\Gamma(b)} X^a (\log(X))^{b-1} + o(X^a (\log(X))^{b-1})$$

Remark 1.9 *The difficult part in applying the theorem relies on our ability to produce an analytic continuation of f beyond it's domain of convergence, and studying carefully the poles and what residue we obtain at the rightmost pole. In the general case of L-functions we have this analytic continuation.*

This type of estimate has been essential in Manjul's Bhargava asymptotic results on counting number fields by discriminant ([6], [7])

1.2 Analytic Number Theory over Function Fields

A main reference for our presentation is [40]. A great exposition for the geometric exposition of the ideas and results we can obtain can be found in Jordan S. Ellenberg's notes [17]. Let's first fix some notation.

Definition 1.10 $\mathbb{F}_q[T]$ *is the polynomial ring in one variable over* $\mathbb{F}_q$*. The set* $\mathcal{M}_{n,q}$ *will be set of all monic degree* n *polynomials in* $\mathbb{F}_q[T]$.

In turns out that most of the objects that we've described in the previous section have a natural analogue over $\mathbb{F}_q[T]$ as well as being a precise dictionary that lets us take a problem over $\mathbb{Z}$ and construct it's counterpart over $\mathbb{F}_q[T]$.

The first major problem that initiated the study of such analogues was concerning the analogue of the Riemann Zeta function, described in the previous section. Roughly this can be described as a generating function obtained from the counting the number of points on an algebraic variety over a finite field. This problem is known as the Weil conjectures posed in 1949 by Weil. In the case for curves these conjectures were posed earlier by Artin in 1924([2]). The proof of the rationality was done by Dwork in 1960([15]), the functional equation by Grothendieck in 1965([23]) and the analogue Riemann Hypothesis was proved by Deligne in 1974([12]).

This stimulated the investigation of more problems over function fields, and their proofs gave us more reason to believe that their counterparts over $\mathbb{Z}$. A few examples of famous analytic number theory, besides the above, are: number of primes in short intervals ([16]), twin prime conjecture ([4], the analogue of the Goldston Montgomery pair correlation conjecture([30]), proof of an upper bound of the number of extensions of $\mathbb{F}_q[T]$ with given Galois group ([18]), ordered by description which matches the number field predictions of Malle and Bhargava

First let us talk about the dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$. We shall describe just a few entries in this rich dictionary and in chapter 2 more will come to light.

First the positive integers will match the with the set of monic polynomials in $\mathbb{F}_q[T]$. One way to explain this is positive integers are $\mathbb{Z}$ modulo $\{\pm 1\}$- the units; and monic are precisely the analogous thing- $\mathbb{F}_q[T]/(\mathbb{F}_q)^{\times}$.

Secondly prime numbers will correspond to irreducible polynomials.

Counting numbers with certain properties within the box $[X, 2X]$ will correspond to counting polynomials with an analogous property over $\mathcal{M}_n$.

Moreover whenever we have an asymptotic result that involves X and $\log(X)$ we can translate these terms to q^n and n respectively. To see this we note that integers in the box $[X, 2X]$ have roughly size X and the way we should think about size in $\mathbb{Z}$ is the absolute value which is an infinite place. It turns out that over $\mathbb{F}_q[T]$ we still have an infinite place; thinking of our polynomial as a function on $\mathbb{P}^1$ (the projective line) this would be order of vanishing at ∞ which is obviously $-\deg(f)$. Thus the valuation at the infinite place of a polynomials is $q^{\deg(f)}$. Thus we see the first analogy, and note that

$\log(q^n) = n\log(q)$ so ignoring the $\log(q)$ factor we obtain the claim.

Let us now define the zeta function of $\mathbb{F}_q[T]$:

Definition 1.11 *The Riemman zeta of $\mathbb{F}_q[T]$ is*

$$\zeta_{\mathbb{F}_q[T]} = \prod_{f \text{ monic,irreducible}} (1 - q^{-s\deg(f)})^{-1}$$

But as it turns out there is more compact and easy way to write down. Namely, since every monic degree n irreducible polynomial can be factored uniquely into monic irreducible polynomials we have

$$\zeta_{\mathbb{F}_q[T]} = \sum_{n=0}^{\infty} q^n \cdot q^{-ns} = \frac{1}{1 - q^{(1-s)}}$$

We see for example the pole $s = 1$ in analogy with Riemann zeta over $\mathbb{Z}$; but the more striking property is the rationality, alluded in the first paragraph to a more general class of zeta functions which will be defined at the end of this section.

Now let us turn to a few examples and see more explicitly how terms match up. We start first with counting irreducible polynomials in $\mathcal{M}_n$ which should correspond to $\pi(X)$.

Theorem 1.12 *(P.N.T in $\mathbb{F}_q[T]$) Let $\pi_{n,q}$ the number of irreducible polynomials in $\mathcal{M}_n$. Then*

$$\pi_{n,q} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

where μ is the Möbius function.

Remark 1.13 *Using our dictionary we see this corresponds to* $\pi(X) = \frac{X}{\log(X)} + O(\sqrt{X}\log(X))$ *and thus as we can see the Riemann hypothesis is true for function fields.*

The second example, which will be recast in section 1.5, is counting squarefree polynomials in $\mathcal{M}_n$, motivated by counting squarefree integers in $[X, 2X]$.

We again state the two results side by side.

Proposition 1.14 *The number of squarefree integers in* $[X, 2X]$ *is asymptotically equal to*

$$\frac{6}{\pi^2}X + O(\sqrt{X})$$

as $X \to \infty$

Proposition 1.15 *The number of squarefree polynomials in* $\mathcal{M}_n$ *is* $q^n - q^{n-1}$*.*

They might not look the same at a first glance but all the difference is in some cosmetic factors. Namely if we write $q^n - q^{n-1} = q^n(1 - \frac{1}{q}) = \frac{q^n}{\zeta_{\mathbb{F}_q[T]}(2)}$, then we see the matchup of the main terms $X \leftrightarrow q^n$ and $\frac{6}{\pi^2} = \frac{1}{\zeta(2)} \leftrightarrow \frac{1}{\zeta_{\mathbb{F}_q[T]}(2)}$.

Finally, let us remark on another important aspect. In analytic number theory over $\mathbb{Z}$ we are interested in the behavior of our count as $X \to \infty$. Over function fields, we have more degrees of freedom. Namely we can work in the regime $q \to \infty$, the large field limit, or $n \to \infty$ limit, the large degree limit. Ideally we would want to study our problem in the situation n, q are both fixed, but that turns out to be too hard. Also the strongest analytic result would be in the limit $q^n \to \infty$ and this would correspond to an uniformity result across a family of number fields of the analogous $\mathbb{Z}$ problem.

In general most of the results that we have been obtained from analogous problems over $\mathbb{Z}$ are solved in the $q \to \infty$ regime; the $n \to \infty$ regime, in most cases, is out of reach with the current methods.

1.3 Weil Conjectures and Dirichlet L-functions

We begin explaining in this section and in the further ones why it is easier solve the analytic number theory problems over function fields. One of the major breakthroughs was the proof of the Generalized Riemann Hypothesis. As mentioned in the previous section this is a part of a series of conjectures, the Weil Conjectures. These were formulated by André Weil in his paper [43].

Definition 1.16 *Let X_0 be a nonsingular projective variety over $\mathbb{F}_q$. For each m, we denote with N_m the number of points of X_0 that are in $\mathbb{F}_{q^m}$ and we define the zeta function of X_0 to be*

$$Z(X_0, t) = \exp\left(\sum_{m\geq 1} N_m \frac{t^m}{m}\right)$$

where by exp *we mean the formal power series* $\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$.

Theorem 1.17 *(Weil Conjectures) The zeta function of a nonsingular, d-dimensional projective variety X_0 has the following properties*

(i) $Z(\frac{1}{q^d t}) = \pm q^{d\chi/2} \cdot \chi \cdot Z(t)$, where χ is the Euler-Poincaré characteristic of X

(ii) $Z(t) = \frac{P_1(t) \cdot P_3(t) \dots P_{2d-1}(t)}{P_0(t) \cdot P_2(t) \dots P_{2d}(t)}$, with $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$ and all these terms are polynomial in t.

(iii) $P_r(t) = \prod_{i=1}^{b_r}(1 - \alpha_{i,r} t)$ where $\alpha_{i,r}$ are algebraic integers of absolute value $q^{r/2}$.

Remark 1.18 *Part (i) can be seen as the functional equation, the second part would be the rationality, and the third is the analogue of the Generalized Riemann Hypothesis.*

Remark 1.19 *The numbers b_r will have meaning as Betti numbers of X once we will talk about étale cohomology in the next section. Then the usual formula for the Euler-Poincaré characteristic of X from singular cohomology over $\mathbb{C}$, $\chi = \sum_r (-1)^r b_r$, will make sense also.*

Remark 1.20 *We can unify the Riemann zeta over $\mathbb{Z}$ and the zeta function of a projective variety, by considering schemes. Namely let X be a scheme of finite type over Spec($\mathbb{Z}$). The zeta function of Z is*

$$\zeta_X(s) = \prod_{y \ closed} \frac{1}{1 - N(y)^{-s}}$$

where by $N(y)$ we mean the size of the residue field. This product converges and defines a holomorphic function for $\Re(s) > \dim(Y)$.

For $Y =$ Spec($\mathbb{Z}$) we recover the Riemann zeta and a projective variety can be regarded as a scheme of finite type over Spec($\mathbb{Z}$) by the short exact sequence

$$X_0 \to Spec(\mathbb{F}_q) \to Spec(\mathbb{Z})$$

Let us talk next about the Dirichlet L-functions over function fields and the implication of the Weil conjectures for them.

Definition 1.21 *Let $Q(T) \in \mathbb{F}_q[T]$ be a polynomial of positive degree. A Dirichlet character modulo Q is a homomorphism*

$$\chi : (\mathbb{F}_q[T]/Q)^\times \to \mathbb{C}^\times$$

A character χ is "even" if $\chi(aP) = \chi(P)$ for every $a \in \mathbb{F}_q^\times$. We also χ primitive if it not again induced from a smaller divisor Q' of Q, in complete analogy with the $\mathbb{Z}$ definition.

Definition 1.22 *The L-function of χ is*

$$L(u,\chi) = \sum_{\substack{f \ monic \\ (f,Q)=1}} \chi(f)u^{\deg(f)} = \prod_{\substack{g \ irreducible, monic \\ g \nmid Q}} (1 - \chi(g)u^{\deg(g)})^{-1}$$

and this product is absolutely convergent for $|u| < \frac{1}{q}$.

The connection between the L-function and the Weil conjectures is that every Q with degree ≥ 2, and every nonprincipal character χ gives rise to a curve C over $\mathbb{F}_q$ and as a consequence $L(u,\chi)$ will be a polynomial in u of degree at most $\deg(Q) - 1$.

Using further the Weil conjectures and the fact for even characters we have a trivial zero at $u = 1$ we can write

$$L(u,\chi) = (1-u)\det(1 - uq^{1/2}\Theta_\chi)$$

where the matrix Θ_χ in $U(\deg(Q) - 2$ is unitary, and uniquely defined up to conjugacy.

Definition 1.23 *The matrix Θ_χ is called the unitarized Frobenius.*

We can define a similar unitarized Frobenius for χ odd, except it lives in $U(\deg(Q) - 1)$ since we don't have the $u - 1$ in the expression of $L(u,\chi)$.

We are ready to describe a deep theorem of Katz that tell us how the unitarized Frobenius varies in the unitary group.

Theorem 1.24 *The unitarized Frobenius Θ_χ, where χ ranges over all primitive even characters mod T^{n+2} become equidistributed in the projectivized unitary group, $PU(n)$ as $q \to \infty$.*

Remark 1.25 *As a consequence we have that for nice function F on $U(n)$, which is invariant under the unit circle ($F(\omega U) = F(U)$ for $|\omega| = 1$) ,*

$$\lim_{q\to\infty} \frac{1}{q^{n+1}} \sum_{\substack{\chi \ mod \ T^{n+2} \\ even, \ primitive}} F(\Theta_\chi) = \int_{PU(n)} F(U) \, dU$$

This is the main technical ingredient in a wealth of recent results of Zeev Rudnick, J.P Keating, Brad Rodgers, Edva Roditty-Gherson ([31],[30], [29])on arithmetical statistical questions in function fields over finite fields. A good survey on these results and more is [41].

With this last theorem we end the discussion about the main analytical tools needed to answer arithmetical statistics questions over function fields over finite fields.

1.4 Where is the geometry?

We will turn our attention now to the geometry that underlies some of these questions. We have already seen already two deep geometric results, the Weil conjectures and Katz equidistribution theorem.

Both their proofs rely on the étale cohomology and l-adic sheaf theory, introduced by Alexander Grothendieck. The basis for this subjects are the SGA books ([24], [14],

[22]). The standard references we will use are James Milne's book and his lecture notes ([35], [34]). We will not try to describe this beautiful theory thoroughly, but mostly we will try to give the reader a user guide how it is applied in various contexts and what kind of properties does étale cohomology have.

We start first with the ideas that lead to the development of this subject. Let's first describe the properties of a Weil cohomology theory, which shares the properties of singular cohomology for varieties defined over the complex numbers.

Definition 1.26 *A Weil cohomology theory is a contravariant functor $H^i(-,K)$ from non-singular complete irreducible varieties over an algebraically closed field k to finite dimensional vector spaces over a characteristic zero fields, called K, satisfying the following:*

(i)(Dimension) $H^i(X) = 0$ for $i < 0$ or $i > 2n$, where $n = \dim(X)$;

(ii) $H^{2n}(X)$ is isomorphic to K- the orientation map;

(iii) (Poincaré Duality) There is a non-degenerate pairing $H^i(X) \times H^{2n-i}(X) \rightarrow H^{2n}(X) \cong K$

(iv)(Künneth isomorphism) $H^*(X) \otimes H^*(Y) \rightarrow H^*(X \times Y)$ is an isomorphism.

(v) (Cycle Map) There is a cycle map $\gamma_X : Z^j(X) \rightarrow H^{2j}(X)$, where $Z^j(X)$ is the algebraic group of codimension j cycles, satisfying compatibility relations to the functoriality of H, the Küneth isomorphism and such that for a X being a point, the cycle map is the inclusion $Z \hookrightarrow K$.

(vi) (Weak Lefschetz axiom) For any smooth hyperplane section $j : W \subset X$ ($W = X \cap \mathcal{H}$, where $\mathcal{H}$ is some hyperplane in the ambient projective space) the maps $j_* : H^j(X) \rightarrow H^j(W)$ are isomorphism for $j \leq \dim(X) - 2$ and monomorphism for $j =$

$\dim(X) - 1$.

(vii) (Hard Leschetz axiom) Like above let W be a hyperplane section and $w = \gamma_x(W) \in H^2(X)$ be it's image under the cycle map. The Lefschetz operator $L : H^j(X) \to H^{j+2}(X)$ which maps $x \to x \cdot w$ (this operation is in the algebra H^*). Then $L^i \to H^{n-i}(X) \to H^{n+i}(X)$ is an isomorphism for $1 \leq i \leq \dim(X)$.

There are four different cohomology theories that satisfy these properties: singular cohomology, de Rham Cohomology,étale cohomology or l-adic cohomology for varieties over fields of characteristic not equal to l, crystalline cohomology.

While these properties are classical and well understood for singular and de Rham cohomology, all of them are deep theorems for the situation of étale cohomology.

Grothendieck defined the l-adic cohomology as

$$H(X, \mathbb{Q}_l) = \lim_{\leftarrow} H_{\acute{e}t}(X, \mathbb{Z}/l^n\mathbb{Z}) \otimes \mathbb{Q}_l$$

for X a projective variety over k, and l coprime to the characteristic of k.

Of course the difficult part is constructing $H_{\acute{e}t}(X, \mathbb{Z}/l^n\mathbb{Z})$, and the starting point is that they agree with the singular cohomology over $\mathbb{C}$ with coefficients in torsion sheaves. The bulk of the work is constructing the étale topology, and the beautiful idea of Grothendieck was to replace the idea of an open covering of the space (as we usually have in the complex topology), with étale covers of the space.

The insight was of course given by the complex topology; every space has covers which are classified by the fundamental group, and in a similar way a space has étale covers which are classified by the étale fundamental group.

Definition 1.27 *An $\mathbb{Z}_l$ is as a pro object $\ldots \to K_2 \to K_1$ in the category of sheaves on* *the étale site $X_{ét}$ where*

(i) Each K_i is a $\mathbb{Z}/l^i$ module;

(ii) Each K_i is constructible, i.e the stalks are finite and there is a partition of X into locally closed sets $\{S_j\}$ such that $K_i|_{S_j}$ is locally constant.

(iii) The structure maps $K_i \otimes \mathbb{Z}/l^{i-1} \to K_{i_1}$ are isomorphism

Remark 1.28 *We can pretend we are working with $\lim\limits_{\leftarrow} K_i$, although the homological algebra involved in arguing that the construction works is far from trivial. These subtleties can be ignored in general.*

If each K_i is locally constant, then we call the sheaf *lisse*. A typical example is the Tate sheaf:

$$\mathbb{Z}_l(1)_X = (\mathbb{Z}/l^n\mathbb{Z}(1))_X$$

with transition maps $x \to x^l : \mu_{l^{n+1}} \to \mu_{l^n}$, is *lisse* and locally free of rank one. We can consider it's tensor powers $\mathbb{Z}_l(i) := \mathbb{Z}_l(1)^{\otimes i}$.

Another important point is that if X is connected and x is a geometric point, the fiber functor $F \to F_x$ gives an equivalence between the category of *lisse* $\mathbb{Z}_l$ sheaves on X and continuous representations of the fundamental group $\pi_1(X, x)$ (in the sense of SGA 1 V 7) in $\mathbb{Z}_l$ modules of finite type.

We start describing the main theorems, that shall be useful in our computations. First we introduce the notion of Frobenius.

Let's first describe the situation for $\mathbb{A}^1_{\mathbb{F}_q} = \operatorname{Spec} \mathbb{F}[x]$ the affine line over $\mathbb{F}_q$. There are four different operators that we could call Frobenius:

(i) The absolute Frobenius Frob_X, $\displaystyle\sum_i a_i x^i \to \Big(\sum a_i x^i\Big)^q$;

(iii) The relative Frobenius $\mathrm{Frob}_{X/\mathbb{F}_q}$, $\quad \sum_i a_i x^i \to \sum a_i (x^i)^q$;

(iii) The arithmetic Frobenius ϕ, $\quad \sum_i a_i x^i \to \sum a_i^q x^i$;

(iv) The geometric Frobenius, which is the inverse of ϕ, $\quad \phi^{-1}$.

These can be defined in general for schemes X of finite type over a finite field $\mathbb{F}_q$. We have the obvious relation $\mathrm{Frob}_X = \mathrm{Fr}_{X/\mathbb{F}_q} \circ \phi$. Since obviously these operators act on X they will induce also an action on the étale cohomology groups which is a linear operator.

In the second paper of Deligne on the Weil conjectures ([13]) it is proven that Frob_X acts trivially on the étale cohomology groups. Thus the interesting action is of the relative Frobenius or equivalently ϕ^{-1}, the geometric Frobenius. This is what will call in general Frob_q for the rest of remaining sections and chapters.

The basic result in the Weil II paper is the following:

Theorem 1.29 *Suppose that X is a variety. Then the eigenvalues of Frob_q on $H^i_c(X_{\acute{e}t}, \mathbb{Q}_l)$ are algebraic numbers all of whose absolute values (after fixing an embedding $\mathbb{Q}_l \hookrightarrow \mathbb{C}$)) have absolute value $q^{w/2}$ with $0 \leq w \leq i$; all of the eigenvalues satisfy $w = i$ if X is proper and smooth.*

We turn our attention to another two important results in étale cohomology that will be fundamental in our counts. The first is the Grothendieck Lefschetz formula.

Theorem 1.30 *For any smooth projective variety X over $\mathbb{F}_q$ we have*

$$X(\mathbb{F}_q) = \sum_{i \geq 0} \mathrm{tr}(\mathrm{Frob}_q : H^i_{\acute{e}t}(X; \mathbb{Q}_l))$$

Remark 1.31 *This formula is inspired by the Lefschetz fixed point theorem for singular homology:*

Let X be a closed smooth manifold and let $f : X \to X$ be a smooth map with all fixed points nondegenerate. Then

$$L(f) = \sum_i (-1)^i Tr(f_\star : H_i(X;\mathbb{Q}) \to H_i(X;\mathbb{Q})$$

where $L(f)$ is the Lefschetz number which counts fixed points with some signed multiplicity.

Remark 1.32 *We can also deal with non-projective varieties; these would be in singular cohomology terms, non-compact. The fix in the singular cohomology is to use compactly supported cohomology and in a similar way there exist compactly supported étale cohomology groups. When X is smooth we can further use Poincaré duality to obtain:*

$$X(\mathbb{F}_q) = q^{\dim(X)} \sum_{i \geq 0} \mathrm{tr}(\mathrm{Frob}_q : H^i_{\acute{e}t}(X;\mathbb{Q}_l)^\vee)$$

Of course an important point to make is that using the formula is not going to be helpful, unless we get a good understanding of two things: the étale cohomology groups and the action of Frobenius. We have already presented the most important result on the action of Frobenius, namely Deligne's result, but even in the easy case when our variety is proper and smooth we don't know what roots of unity we have in the eigenvalues of the Frobenius.

For actually understanding the étale cohomology groups we have the following result of Artin that allows us to recover the dimension of these groups by comparing them to singular cohomology over $\mathbb{C}$. Namely if we take a variety defined over $\mathbb{Z}$ or $\mathbb{Z}_p$ we can reduce it modulo p and obtain a variety over a finite field; or we can change scalars from $\mathbb{Z}$ to $\mathbb{C}$ and obtain a manifold. Thus we have

Theorem 1.33 *(Artin comparison theorem) Let X be a smooth variety. Then there is a map*

$$c_X : H^i_{\acute{e}t}(X(\mathbb{F}_q); \mathbb{Q}_l) \to H^i(X(\mathbb{C}); \mathbb{Q}_l)$$

which is an isomorphism of vector spaces.

Remark 1.34 *The Artin comparison theorem and the* Frob_q *action would justify saying that étale cohomology sits in the middle between Galois cohomology and singular cohomology; this in analogy to Weil's perspective that function fields $\mathbb{F}_q[T]$ sit in the middle between classical number theory and the Riemmanian theory of algebraic functions over $\mathbb{C}[T]$.*

Remark 1.35 *As a consequence from all the theorems presented above we have that for X smooth, proper and irreducible*

$$\lim_{q\to\infty} \frac{X(\mathbb{F}_q)}{q^{\dim(X)}} = 1$$

1.5 The Church-Ellenberg-Farb approach to polynomial statistics

After discussing all the preliminaries we have come to the main motivation for this thesis, namely the paper [9].

The motto of the paper is that for any "good" counting statistic we want over $\mathbb{F}_q[T]$, we just need to understand the cohomology of a fixed space with coefficients in some sheaf. Good will mean loosely that for a statistic over $\mathcal{M}_{n,q}$ we can encode the action of Frobenius as a certain class function of S_n and then all we are left to do to obtain a count is compute some inner products coming from representation theory.

The caveat for this approach is that we will deal only with squarefree polynomials. This is a mild obstruction in most cases, since we can factor each polynomial uniquely as A^2B where B is squarefree, so we can recover a general result by means of a recurrence relation.

We begin by defining the spaces we will use.

Definition 1.36 *For a space X we can define* $\mathrm{PConf}^n(X) = \{(x_1, \ldots, x_n) | x_i \neq x_j\}$*, the space of ordered tuples of n points of X and* $\mathrm{Conf}^n(X) = \mathrm{PConf}^n(X)/S_n$*, the space of unordered tuples of n points on X.*

Remark 1.37 *For X a topological space we have that* $\mathrm{PConf}^n(X)/S_n$ *is also a topological space since the action of S_n on* $\mathrm{PConf}^n(X)$ *is free.*

Definition 1.38 *A hyperplane arrangement is $\displaystyle\bigcup_{i=1}^{m} H_i$ where $H_i \subset \mathbb{A}^n$. A hyperplane complement is $\mathbb{A}^n - \displaystyle\bigcup_{i=1}^{m} H_i$.*

Remark 1.39 *For the general purpose of this thesis we are only interested in hyperplane arrangements that are stable under some symmetry group, like S_n or more generally $C^n \rtimes S_n$ where C is a finite cyclic group. For example, the space* $\mathrm{PConf}^n(\mathbb{C})$ *is a hyperplane complement stable under the S_n action; we can say that is generated by the hyperplane $x_1 = x_2$ and the S_n action component wise.*

The next layer to uncover is finding a good system of coefficients for our statistic.

First let's describe the situation over the complex numbers so we are looking at $\mathrm{Conf}^n(\mathbb{C})$. This space is in natural bijection with the set of squarefree polynomials with complex coefficients namely:

$$(z_1, \ldots, z_n) \to (T - z_1) \ldots (T - z_n)$$

Now we also have a map backwards from a squarefree polynomial $f \in \mathbb{C}[T]$ to its set of roots $R(f)$.

Definition 1.40 *Let $X_1, ..., X_n$ be the standard characters of S_n, i.e $X_i(\sigma)$ is equal to the number of i-cycles in σ.*

Definition 1.41 *Let V the vector bundle*

$$V = \{(f(T) \in \mathrm{Conf}^n(\mathbb{C}), h : R(f) \to \mathbb{Q})\}$$

Picking different h's will give trivializations of our vector bundle and thus we get a system of coefficients. Our choice of h's will depend on the counting statistic over $\mathbb{F}_q[T]$ so let's describe the process.

If we have a squarefree polynomial in $\mathcal{M}_n$ and we look at it's roots in $\overline{\mathbb{F}}_q$ then Frob_q will induce a permutation on the roots. This preserves the irreducible factors, and thus will preserve the cycle structure as a permutation. Thus we can regard Frob_q as a class function.

For our counting statistic will be interested in taking h to be equal to this class function. In particular, when h is a polynomial in the characters $X_1, .., X_n$ with $\mathbb{Q}$

coefficients we can reconstruct by means of representation theory the local systems corresponding to our statistic since h would be trace of this S_n representation.

As an example if $h = X_1$ we are looking at fixed points and we want to know what representation has trace equal to X_1. This is the standard representation $\mathbb{Q}^n$.

From the topological perspective, if we look at stalk V_f we have that for any loop γ in $\mathrm{Conf}^n(\mathbb{C})$ we obtain a permutation σ_f on $R(f)$ by identifying around the loop the roots of f_t with the roots of f, using continuity. Thus we just have to ensure that $\operatorname{tr}\gamma_\star$ is the prescribed polynomial in the X_i characters where $\gamma_\star : V_f \to V_f$ is the S_n representation we obtain.

Using this perspective we can do the same construction for étale sheaves; namely we can construct everything stalkwise by prescribing the permutation action induced by Frob_q. Thus similar to $\mathrm{Conf}^n(\mathbb{C})$ we can find a sheaf for $\mathrm{Conf}^n(\mathbb{F}_q)$ that encodes our polynomial statistic.

The last layer before we state the main counting result, is the Frob_q action on étale cohomology. We have the following general result of Kim([32]) over any base field (see also Lehrer([33]).

Theorem 1.42 *Let k be a field, and fix l a prime different from the characteristic of k. Give a finite set of hyperplanes $H_1, \ldots, H_m$ in $\mathbb{A}^n$ defined over k, let $\mathcal{A}$ the complement: $\mathcal{A} = \mathbb{A}^n - \bigcup_{i=1}^m H_i$. Then:*

(i) $H^1_{ét}(\mathcal{A}; \mathbb{Q}_l)$ is spanned by the images of the m maps:

$$H^1_{ét}(\mathbb{A}^n - H_j; \mathbb{Q}_l) \to H^1_{ét}(\mathcal{A}; \mathbb{Q}_l)$$

induced by the inclusion of $\mathcal{A}$ into $\mathbb{A}^n - H_j$ for $j = 1, \ldots, m$.

(ii) $H^i_{\acute{e}t}(\mathcal{A};\mathbb{Q}_l)$ *is generated by* $H^1_{\acute{e}t}(\mathcal{A};\mathbb{Q}_l)$ *under cup product.*

We also need a definition.

Definition 1.43 *For* χ *a class function on* S_n *and* f *a squarefree polynomial in* $\mathcal{M}_n$*, we define* $\chi(f) = \chi(\sigma_f)$ *where* σ_f *is the permutation induced by action of the* Frob_q *on the roots of* f*.*

Remark 1.44 *This* σ_f *is not unique since there is no canonical labelling of the roots but it's cycle structure is since it corresponds to irreducible factors of* f*.*

The main counting result in [9] is

Theorem 1.45 *Let* $\mathcal{A}$ *be a hyperplane complement stable under the* S_n *action, that contains the diagonal* $(x_i \neq x_j)$ *and* $\mathcal{B} = \mathcal{A}/S_n$ *. Then we have that for any class function* χ *on* S_n *we have*

$$\sum_{f(T)\in\mathcal{B}(\mathbb{F}_q)} \chi(f) = \sum_i (-1) q^{n-i} \langle \chi, H^i(\mathcal{A}) \rangle$$

Remark 1.46 *Here we think of* H^i *as a representation of* S_n *and inner product makes sense as class functions of* S_n*. We could either think in the étale setting or the singular cohomology setting about* H^i*.*

Going back to our favorite example, counting squarefree polynomials which is the same counting points in $\mathrm{Conf}^n(\mathbb{F}_q)$ we get that the formula gives us

$$\mathrm{Conf}^n(\mathbb{F}_q) = \sum_i (-1) q^{n-i} H^i(\mathrm{Conf}^n(\mathbb{C});\mathbb{Q}_l)$$

Arnold's result ([1]) tells us that $H^i(\mathrm{Conf}^n(\mathbb{C});\mathbb{Q}_l) = \mathbb{Q}_l$ for $i = 0, 1$ and it vanishes otherwise; this is true for any $n \geq 2$.

This example gives insight into some extra geometrical information that we get from our count. Namely the spaces $H^i(\mathrm{Conf}^n)$ exhibit homological stability. Let's define this more precisely.

Definition 1.47 *A sequence of space $X_1 \subset X_2 \subset \ldots X_n \subset \ldots$ is said to be homologically stable if for any i, the cohomology groups $H^i(X_n;\mathbb{C})$ stabilize, i.e $H^i(X_n) = H^i(X_{n+1})$, for $n >> i$.*

In this sense the authors define a special class of hyperplane arrangements that have the property that $\langle \chi, H^i(\mathcal{A}) \rangle$ stabilize as $n >> i$. This allows us to take the $n\infty$ limit in the above theorem.

Also this notion give a new interpretation of the tauberian theorem. Namely the quantity $\frac{1}{q^n} \sum_{f(T) \in \mathcal{B}_(\mathbb{F}_q)} \chi(f)$ by the tauberian theorem would compute exactly the residue of the L-function associated to our counting problem. What we obtain is that this residue can be recovered purely from the geometric side and the computation of the inner products.

Let's make the necessary definitions. FI is the category introduced in , and the objects are finite sets and the morphisms are inclusions. An FI-module is a functor from this category to the category of module over a ring A, and we shall call this an FI-module over A.

Now let us consider a ring R and let $L = \{L_1, \ldots, L_m\}$ be a finite set of nontrivial linear forms over R in the variables $x_1, \ldots, x_d$-these will be the equations of our hyperplanes. We also impose that $x_1 - x_2$ is contained in L. For each n, L_i and any finite injection

$f : \{1, \ldots, d\} \to \{1, \ldots, n\}$ we can define L_i^f by $L_i^f(x_1, \ldots, x_n) = L^i(x_{f(1)}, \ldots, x_{f(d)})$.

Thus we obtain the complement of hyperplane arrangement

$$\mathcal{A}(L)_n = \mathbb{A}_R^n - \bigcup_{f,i} H_i^f$$

where H_i^f are the hyperplanes where $L_i^f = 0$.

This class of hyperplane complements is denominated by FI-CHA. As the reader can see it is a restricted class of hyperplane arrangements; we could roughly say it involves only a fixed number of variables in each hyperplane equation plus some S_n symmetry. We also note that $\mathcal{A}(L)_n$ carries a natural S_n action by using the permutation action on the coordinates of $\mathbb{A}_R^n$.

Moreover we have that $H^i_{\acute{e}t}(\mathcal{A}(L)_n; \mathbb{Q}_l)$ fit together into an FI-module over $\mathbb{Q}_l$. The authors in [9], prove strong results about the finite generation of FI-modules and this will give the desired stabilization results on the inner products with characters of S_n.

1.6 Overview of thesis

This thesis is devoted to study some statistical problems centered around polynomials in $\mathcal{M}_n$ that can be written as $|A^2 - TB^2|$ where A, B are in $\mathbb{F}_q[T]$ monic. This was first studied by lior by using an L-function approach. The results obtained where in two different regimes $q \to \infty$ and $n \to \infty$; but there was no $q^n \to \infty$ because of the dependencies in the error terms. This obstacle was removed by Ofir Goredetsky in, using a generating functions technique.

We study more carefully the $n \to \infty$ result and make it work in the $q^n \to \infty$ regime using a twisted Grothendieck Lefschetz trace formula similar to the one in section 1.5, for the group $G_n = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$. This formula was also proven independently in recent work by Jennifer C.H Wilson and Rita Jimeneze Rolland in [39] , and a more general formula was proven by Kevin Casto in [8] for $G = C^n \rtimes S_n$ where C is a finite cyclic group.

The characteristic function that governs this statistic is a class function on G_n, but it will not be given by a character polynomial; this in contrast to the papers that obtain general results for polynomials in the characters $X_1, \ldots, X_n$.

Moreover a new type of homological stability arises that is not present in the character polynomial situation, since our class function depends on all the cycles in the decomposition. Thus there should be a richer picture of stability.

We also obtain the number of irreducible polynomials and the expected number of roots of a squarefree polynomial that can be written in this way.

Chapter 2

A geometric perspective on Landau's problem over function fields

2.1 Introduction

The present paper is motivated by the results obtained in [5] in which the authors state and prove a function field analogue of Landau's theorem about sums of two squares.

Definition 2.1 *Let q be an odd prime power. For a polynomials $f \in \mathcal{M}_{n,q}$ we define the characteristic function:*

$$b_q(f) = \begin{cases} 1, & \textit{if } f(T) = A^2 + TB^2 \quad \textit{for} \quad A, B \in \mathbb{F}_q[T] \\ 0, & \textit{otherwise.} \end{cases}$$

and the counting function $B_q(n) = \sum_{f \in \mathcal{M}_{n,q}} b_q(f)$

The following two theorems about the asymptotic of $B_q(n)$ are obtained by Lior Bary-Soroker, Yotam Smilansky and Adva Wolf in [5]

Theorem 2.2 (SSW)

$$B_q(n) = \frac{1}{4^n}\binom{2n}{n}q^n + \left(\frac{1}{2\cdot 4^{n-1}}\binom{2(n-1)}{(n-1)} + \frac{1}{4^{n-1}}\binom{2(n-2)}{(n-2)}\right)q^{n-1} + \mathcal{O}_n(q^{n-2}), \quad q\to\infty$$

Theorem 2.3 (SSW)

$$B_q(n) = \frac{K_q}{\sqrt{\pi}}\cdot\frac{q^n}{\sqrt{n}} + \mathcal{O}_q\left(\frac{q^n}{n^{3/2}}\right), \quad n\to\infty$$

where

$$K_q = (1-q^{-1})^{-\frac{1}{2}}\prod_{\left(\frac{P}{T}\right)=-1}(1-|P|^{-2})^{-\frac{1}{2}}$$

Here $\left(\frac{P}{T}\right)$ *is the Legendre symbol.*

Recently in [21] the dependency on q in the error term in this second theorem was removed by using a generating functions technique.

What we shall prove is an expansion on the first theorem above, namely

Theorem 2.4 *For every* $n\geq 2$ *we can write* $B_q(n) = \sum_{k=0}^{n} b_{k,n}q^{n-k}$ *such that*

a) $b_{k,n} = \sum_{j=k}^{2k}\delta_{k,j,n}\frac{\binom{2(n-j)}{n-j}}{4^{n-j}}$;

b) We have that $\delta_{k,j,n} = \delta_{k,j,n+1}$ *for* $n\geq 2k$ *and*

$$|\delta_{k,j,n}|\leq C(1.1)^k$$

for some absolute constant C.

Next let us make some remarks connecting the theorem we stated with previous results.

Remarks • Part a) of our theorem is a generalization and gives a complete description of the statement of the first theorem stated above.

• In the course of the proof of the theorem we shall give a geometric interpretation to the binomial coefficients appearing in the expansion

• The stabilization of the coefficients $\delta_{p,j,n}$ as n gets large with respect to p is explained by the stabilization of the multiplicity of a character paired against the cohomology of a certain space and thus can be viewed thus a homological stabilization result

• Our result is in direct connection with Remark 4.1 in [21], namely

$$B_q(n) = \sum_{i=0}^{2d-2} q^{n-i} \binom{n-i-\frac{1}{2}}{n-i} [x^i] \exp\left(\sum_{j\geq 1} \frac{e_j x^j}{j}\right) + O_n(q^{n-d})$$

where $[x^i]$ represents the coefficient of x^i in the taylor series expansion of the exponential and $e_n = \frac{1}{2} + \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i}-1}{2}$ where for a given natural number x, $v_2(x)$ is the valuation of 2 in x.

As the reader can notice it would require some combinatorial manipulations to obtain the same form as the result in theorem 1 since every exponential also involves q.

• Another interesting connection between our theorem 1 and all the other results that can be explored further would be to make use of the following binomial expansion from Yudell L. Luke's book ([45])

$$\binom{x}{n} = \frac{(-1)^n \cdot n^{-(x+1)}}{\Gamma(-x)} \sum_{k=0}^{\infty} \frac{(x+1)_k B_k^{(-x)}}{k! n^k}$$

Here we denote with $\Gamma(y)$ the usual gamma function, $(y)_k$ is the lower factorial and $B_k^{(-x)}$ are generalized Bernoulli numbers. If we set $x = -\frac{1}{2}$ then we obtain that

$$\binom{2n}{n} = \frac{4^n}{\sqrt{\pi n}}\left(1 + \frac{c_1}{n} + \frac{c_2}{n^2} + \ldots + \frac{c_r}{n^r} + \mathcal{O}\left(\frac{1}{n^{r+1}}\right)\right)$$

where $c_1, \ldots, c_r$ which can be computed from the above expansion of the binomial.

The difficulty relies on the fact that we need to obtain an asymptotic expansion of sums of central binomial coefficients with exponentially decaying coefficients, i.e $\sum_{i=0}^{k} a_i \binom{2(n-i)}{n-i}$, where k might also have growth with respect to n.

This theorem will be a consequence of theorem 2, but before stating it properly we need to make some definitions.

Definition 2.5 *Let q an odd prime power. For a polynomials $f \in \mathcal{M}_{n,q}$ we define the characteristic function:*

$$s_q(f) = \begin{cases} 1, & \textit{if } f(T) = A^2 - TB^2 \quad \textit{for} \;\; A, B \in \mathbb{F}_q[T] \\ 0, & \qquad\qquad \textit{otherwise.} \end{cases}$$

Let $\mathcal{S}_{n,q} \subset \mathcal{M}_{n,q}$ be the set of monic square free polynomials.

Definition 2.6 *Define the counting functions $S_q(n) = \sum_{f \in \mathcal{S}_{n,q}} s_q(f)$ and $S_q^o(n) = \sum_{f \in \mathcal{S}_{n,q}, f(0) \neq 0} s_q(f)$.*

Equivalently we could say that $s_q(f) = 1$ if f is a norm in the function field extension $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$. Also note the obvious relation

$$S_q(n) = S_q^o(n) + S_q^o(n-1)$$

since any monic squarefree either is non zero at zero or vanishes with order 1, namely f/T would be monic squarefree polynomial of degree $n-1$ and nonvanishing at zero.

Our next theorem will concern finding an asymptotic for $S_q^o(n)$ as $q^n \to \infty$. We thus have the following

Theorem 2.7 *For every $n \geq 2$ we can write $S_q^o(n) = \sum_{i=0}^{n} (-1)^i c_{i,n} q^{n-i}$. Moreover*

a) $c_{i,n} = \sum_{j=0}^{i} \Gamma_{i,j,n} \frac{\binom{2(n-j-i)}{n-j-i}}{4^{n-j-i}}$ where $\Gamma_{i,j,n}$ are rational numbers.

b) $\Gamma_{i,j,n} = \Gamma_{i,j,n+1}$ for $n \geq 2i$ and we have the following bound

$$|\Gamma_{i,j,n}| \leq B \cdot (1.1)^j$$

for some absolute constant B.

2.2 Preliminaries

For a squarefree polynomial $f \in \mathcal{M}_{n,q}$ with $f(0) \neq 0$ let the unordered n tuple of it's roots be $\{z_1, \ldots, z_n\}$ where $z_i \neq z_j$ and $z_i \neq 0$. Since F_q fixed the coefficients of the polynomial this induces a permutation on the roots of f. For each z_i pick an $x_i \in \overline{\mathbb{F}}_q$ such that $x_i^2 = z_i$. It follows that Frob_q induces a signed permutation on these representatives. Call R_n the space of all tuples $\{x_1, \ldots, x_n\}$ and we shall also denote with G_n the signed permutation group.

Now we can restate $b_q(f) = 1$ if the two roots of $x^2 = z_i$ lie in different orbits of the Frob_q action on the space R_n, thought as the space of points on the tuples $(x_i, -x_i)$ where these are the roots of $x^2 = z_i$.

Definition 2.8 *Let L_n be the subset of G_n, consisting of all signed permutation π such that x_i and $-x_i$ lie in different orbits under π.*

It is now time to relate the geometry of the space of roots and our counting problem. Note the fact that $z_i \neq z_j$ imposes that $x_i \neq \pm x_j$.

I claim that now we can identify R_n as a hyperplane complement in affine n space,

$R_n = \{(\alpha_1, \ldots, \alpha_n) | \alpha_i \neq \pm\alpha_j, \alpha_i \neq 0\}$.This is because for each $f \in \mathcal{M}_{n,q}$ considering the tuple $\{x_1, \ldots, x_n\}$ we can see this is a point of R_n over $\overline{\mathbb{F}}_q$. The representation theory and homological stability properties of this hyperplane arrangement are well understood; the interested reader can look at [44].

Definition 2.9 *Let χ_n be the characteristic function of L_n as a subset of G_n.*

We shall prove a theorem which relates the geometry of our space and the counting problem, which is the same spirit as theorem 3.7 in [9]. The main difference is to state and prove an analogous result for G_n Galois covers instead of S_n covers.

To make it more explicit, if we consider a class function $\chi : G_n \to \mathbb{Q}$ then we can define its action on a squarefree polynomial f in the following way: set $R(f) = \{z_1, z_2, \ldots, z_n\}$ to be sets of roots and we have an induced action of Frob_q on the set of squareroots of these, namely $\{x_1, x_2, \ldots, x_n\}$ as above and this will give us a signed permutation σ_f. We define $\chi(f) = \chi(\sigma_f)$ and we need to argue this is well defined. By forgetting the signs on the signed permutation, we recover the action of Frob_q on $R(f)$ and this has invariant cycle structure since cycles correspond to irreducible factors of f. Since conjugation preserves the cycle structure we are done.

Theorem 2.10 *Let $\mathcal{G}_q(n) = \sum_{f \in \mathcal{S}_{n,q}, f(0) \neq 0} \chi(f)$. Then*

$$\mathcal{G}_q(n) = \sum_i (-1)^i q^{n-i} \langle \chi, H^i_{\acute{e}t}(R_n; \mathbb{Q}_l) \rangle_{G_n}$$

Here $\langle \cdot, \cdot \rangle$ denotes the standard product of class functions and the subscript G_n denote the groups where the respective class functions live.

As a corollary for our problem

Corollary Applying the above theorem to our special case we have

$$S_q^0(n) = \sum_i (-1)^i q^{n-i} \langle \chi_n, H^i_{ét}(R_n; \mathbb{Q}_l) \rangle_{G_n}$$

2.3 Proof of Theorem 2.10

This is the main technical machinery to setup and prove for our problem. Let $\mathbf{Conf}_n^0$ be the affine complement $U_n = \{(z_1, z_2, \ldots, z_n) | z_i \neq z_j, z_i \neq 0\}$ modulo S_n. First let us argue that R_n is a étale Galois cover of $\mathbf{Conf}_n^0$ with Galois group G_n.

Let P_n be the set of monic degree n polynomials which are split in the extension $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$ and which do not vanish at 0. Consider the map

$$\pi : \mathbb{A}^n \to P_n$$

defined by

$$\pi : (x_1, x_2, \ldots, x_n) \to f(T) = (T - x_1^2)(T - x_2^2) \ldots (T - x_n^2)$$

The map is well defined using again theorem 2.5 in [5]. Note that the map is invariant under the G_n action on the points $(x_1, x_2, \ldots, x_n)$ thus it factors through the scheme theoretic quotient $\mathbb{A}^n/G_n$. We prove moreover that actually the map

$\pi : \mathbb{A}^n/G_n \to P_n$ is an isomorphism. The G_n invariant functions on $\mathbb{A}^n$ form a ring, namely $\mathbb{Z}[x_1, x_2, \ldots, x_n]^{G_n}$. First note that if such a function is invariant to switching signs on the x_i's then it has to be a polynomial in x_i^2's. Thus $\mathbb{Z}[x_1, x_2, \dots, x_n]^{G_n} = \mathbb{Z}[x_1^2, x_2^2, \dots, x_n^2]^{S_n}$. As a function of x_i, the coefficient a_i in f is ± the ith symmetric polynomial $e_i(x_1^2, x_2^2, \dots, x_n^2)$. The fundamental theorem of symmetric polynomials states

$$\mathbb{Z}[x_1^2, x_2^2, \dots, x_n^2]^{S_n} = \mathbb{Z}[e_1, \dots, e_n] = \mathbb{Z}[a_1, a_2, \dots, a_n]$$

thus giving the desired isomorphism.

Under this map we can look thus at the preimage of $\mathbf{Conf}_n^0$ and since this space can be identified with monic squarefree degree n polynomials which do not vanish at zero, it can be easily seen that this preimage is R_n. Since we can define R_n in $\mathbb{A}^n$ as nonvanishing of integral polynomials, R_n is a smooth n dimensional scheme over $\mathbb{Z}$.

Since G_n acts freely on R_n by definition, restricting π to a map $R_n \to \mathbf{Conf}_n^0$ gives an étale Galois cover with Galois group G_n.

Now moving further note the fact that the Galois cover $R_n \to \mathbf{Conf}_n^0$ gives a natural correspondence between finite-dimensional representations of G_n and finite-dimensional local systems (locally constant sheaves) on $\mathbf{Conf}_n^0$ that become trivial when restricted to R_n. Given V a representation of G_n, let the χ_V be the associated character to it and let $\mathcal{V}$ be the corresponding local system on $\mathbf{Conf}_n^0$. Initially this construction is done over $\mathbb{C}$ but since since every irreducible representation of G_n can be defined over $\mathbb{Z}$ (see [20],[10]), the local system $\mathcal{V}$ determines an l-adic sheaf and we shall not make a distinction between the two objects.

If $f(T) \in \mathbf{Conf}_n^0$ and is a fixed point for the action of Frob_q on $\mathbf{Conf}_n^0(\overline{\mathbb{F}}_q)$ then Frob_q acts on the stalk $\mathcal{V}_f$ over f. To give a concrete description, the roots of $f(T)$ are permuted by the action of Frobenius on $\overline{\mathbb{F}}_q$, and moreover this induces a signed permutation on the squareroots of the roots of the polynomial f, σ_f which is defined up to conjugacy. The stalk $\mathcal{V}_f$ is isomorphic to V, and by choosing an appropriate basis the automorphism Frob_q acts according to σ_f. Thus we can conclude

$$\mathrm{tr}(\mathrm{Frob}_q : \mathcal{V}_f) = \chi_V(\sigma_f) \quad (1)$$

The next ingredient we need is a version of the Grothendieck-Lefschetz trace formula with twisted coefficients. Namely for an appropiate system of coefficients $\mathcal{F}$ on a smooth projective variety X defined over $\mathbb{F}_q$ (more precisely terminology is a l-adic sheaf), we have :

$$\sum_{x \in X(\mathbb{F}_q)} \mathrm{tr}(\mathrm{Frob}_q \,|\mathcal{F}_x) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q : H^i_{\acute{e}t}(X; \mathcal{F}))$$

This also holds for non-projective X, but we need to correct it by either using compactly supported cohomology or via Poincaré duality.

If we apply to our case using compactly supported cohomology we have that

$$\sum_{f \in \mathbf{Conf}^0_n(\mathbb{F}_q)} \mathrm{tr}(\mathrm{Frob}_q \,|\mathcal{V}_f) = q^n \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q : H^i_c(\mathbf{Conf}^0_n; \mathcal{V})) \quad (2)$$

Notice that the left hand side is exactly the statistical count on polynomials we need using (1). The only thing left to unravel is the right hand side of the equality.

First let us make some remarks about the setup. If V is a G_n representation, we denote by $\langle \chi, V \rangle$ the standard inner product of χ with the character of V; we can name this the multiplicity of χ in V, since this is true when χ is irreducible, by Schur's lemma. Also note that for any class function on G_n we can decompose it into a sum of irreducible characters and since both sides in (2) are linear in χ, it follows that we can reduce to the case of an irreducible character χ of G_n.

Let $\tilde{\mathcal{V}}$ denote the pullback of $\mathcal{V}$ to R_n. Transfer gives us the isomorphism $H_c^i(\mathbf{Conf}_n^0; \mathcal{V}) \approx (H_c^i(R_n; \tilde{\mathcal{V}}))^{G_n}$. Now we know that $\tilde{\mathcal{V}}$ is trivial on R_n, so we have

$$H_c^i(R_n; \tilde{\mathcal{V}}) \approx H_c^i(R_n; \mathbb{Q}_l) \otimes V$$

as G_n representations. Putting it together

$$H_c^i(\mathbf{Conf}_n^0; \mathcal{V}) \approx (H_c^i(R_n; \mathbb{Q}_l) \otimes V)^{G_n} \approx H_c^i(R_n; \mathbb{Q}_l) \otimes_{\mathbb{Q}[G_n]} V$$

Now this gives the immediate consequence that $\dim(H_c^i(\mathbf{Conf}_n^0; \mathcal{V})) = \dim(H_c^i(R_n; \mathbb{Q}_l) \otimes_{\mathbb{Q}[G_n]} V)$.

Since V is self-dual as an S_n representation, $H_c^i(R_n; \mathbb{Q}_l) \otimes_{\mathbb{Q}[G_n]} V$ is isomorphic to $\mathrm{Hom}_{\mathbb{Q}[G_n]}(V; H_c^i(R_n; \mathbb{Q}_l))$, whose dimension is computed using the inner product $\langle \chi, H_c^i(R_n; \mathbb{Q}_l) \rangle$.

Since R_n is smooth of dimension n, applying Poincaré duality gives

$$H_c^{2n-i}(R_n; \mathbb{Q}_l) \approx \mathrm{Hom}(H_{\text{ét}}^i(R_n; \mathbb{Q}_l); \mathbb{Q}_l(-n).$$

Since the action of G_n on $\mathbb{Q}_l(-n)$ is trivial (this is the constant sheaf), we have that $\langle \chi, H_c^{2n-i}(R_n; \mathbb{Q}_l) \rangle = \langle \chi, H_{\text{ét}}^i(R_n; \mathbb{Q}_l) \rangle$. The last layer to uncover is the action on Frob_q.

Theorem 1.42 from section 1.5 of chaper 1 will give that the action of Frob_q on $H_{\text{ét}}^i(R_n; \mathbb{Q}_l)$ is scalar multiplication by q^i. The action of Frob_q on $\mathbb{Q}_l(-n)$ is scalar multiplication by q^n so the action of Frob_q on $H_c^{2n-i}(\mathbf{Conf}_n^0; V))$ is scalar multiplication by q^{n-i}.

Putting it all together we obtain that

$$\mathrm{tr}(\mathrm{Frob}_q : H_c^{2n-i}(\mathbf{Conf}_n^0; \mathcal{V}))) = q^{n-i} \langle \chi, H^i_{\text{ét}}(R_n; \mathbb{Q}_l) \rangle$$

2.4 Computation of the inner products

To finish to proof of Theorem 2, note that according to Theorem 4 we just need to understand the inner product $\langle \chi_n, H^i_{\acute{e}t}(R_n; \mathbb{Q}_l) \rangle_{G_n}$

Note that we can use instead of the etale cohomology singular cohomology over $\mathbb{C}$, since for hyperplane arrangements, the cohomology depends only on the lattice of intersection of the hyperplane arrangement.

To proceed to actual computations we shall need the following result in [26] which gives a description of $H^i(R_n; \mathbb{C})$ as a G_n representation.

Theorem 2.11 (Henderson) *As a representation of G_n, $H^p(R_n; \mathbb{C})$ is equal to $\bigoplus_{0 \le l \le p} A^l(R_n)$ where $\varepsilon_n \otimes A^l(R_n)$ is isomorphic to the following direct sum:*

$$\bigoplus_{\substack{\lambda^1, \lambda^2 \\ |\lambda^1| + |\lambda^2| = n \\ l(\lambda^1) = n-p \\ l(\lambda^2) = l}} \mathrm{Ind}^{G_n}_{\substack{(((\mu_2 \times \mu_{\lambda^1_1}) \times \ldots \times (\mu_2 \times \mu_{\lambda^1_{n-p}})) \rtimes (S_{m_1(\lambda^1)} \times S_{m_2(\lambda^1)} \times \ldots) \\ \times ((\mu_2 \times \mu_{\lambda^2_1}) \times \ldots \times (\mu_2 \times \mu_{\lambda^2_l})) \rtimes (S_{m_1(\lambda^2)} \times S_{m_2(\lambda^2)} \times \ldots))}} (\varepsilon \psi)$$

where, $\lambda^1 = (\lambda^1_1, \ldots, \lambda^1_{n-p})$, $\lambda^2 = (\lambda^2_1, \ldots, \lambda^2_l)$, $|\lambda^1| = \lambda^1_1 + \ldots + \lambda^1_{n-p}$ and similarly for λ^2, ψ is the product of the standard inclusion characters $\mu_{\lambda^j_a} \hookrightarrow \mathbb{C}^\times$ and ε is the product of the sign characters of the $S_{m_i(\lambda^1)}$ components.

The space G_n can be thought of generalized permutation matrices where in each entry we replace the usual 1 with now a ±1. Now let's see how can we realize

$$H_{\lambda^1,\lambda^2} = ((\mu_2 \times \mu_{\lambda^1_1}) \times \ldots \times (\mu_2 \times \mu_{\lambda^1_{n-p}})) \rtimes (S_{m_1(\lambda^1)} \times S_{m_2(\lambda^1)} \times \ldots)$$
$$\times((\mu_2 \times \mu_{\lambda^2_1}) \times \ldots \times (\mu_2 \times \mu_{\lambda^2_l})) \rtimes (S_{m_1(\lambda^2)} \times S_{m_2(\lambda^2)} \times \ldots)$$

as a subgroup of G_n.

Definition 2.12 *A cell is a factor of the type $\mu_2 \times \mu_v$.*

For constructing a matrix representative of the group $\mu_2 \times \mu_v = C_v$ note that we can take as generators the $v \times v$ matrix

$$\mathfrak{g}_v = \begin{cases} g_{i+1,i} = 1 \text{ , for } 1 \leq i \leq v \text{ where index is taken modulo } v \\ 0 \text{ , otherwise} \end{cases}$$

and it's negative. Note that it's actually sufficient for v odd to take $-\mathfrak{g}_v$ since the group $\mu_2 \times \mu_v$ is cyclic.

Definition 2.13 *A block is a factor of the type $(\mu_2 \times \mu_v)^{m_v} \rtimes S_{m_v}$.*

Obviously we can think of blocks as a generalized permutation group on its cells.

To construct H_{λ^1,λ^2} we first arrange the blocks in descending order along the diagonal, first those for λ^1 by reading for each $1 \leq v \leq n$ it's multiplicity, say it is $m_{1,v}$, in the partition λ^1 and putting the block $(\mu_2 \times \mu_v)^{m_{1,v}} \rtimes S_{m_{1,v}}$, and then proceed in a similar fashion for λ^2.

Now we proceed to the actual computation of the inner products $\langle \chi_n, H^p(X_n;\mathbb{C})\rangle_{G_n}$. By theorem 5 and Frobenius reciprocity it is equivalent to computing

$$\langle \mathrm{Res}^{G_n}_{H_{\lambda^1,\lambda^2}} \chi_n, \mathrm{Res}^{G_n}_{H_{\lambda^1,\lambda^2}} \varepsilon_n \otimes \varepsilon\psi \rangle$$

, for each λ^1, λ^2 subject to the constraints in theorem 5.

First let us look closely at $\mathrm{Res}^{G_n}_{H_{\lambda^1,\lambda^2}}\varepsilon_n$.

Suppose the the block structure of H_{λ^1,λ^2} is given by the blocks $\mathcal{B}_1$, $\mathcal{B}_2$, …, $\mathcal{B}_j$. Then noting that there is natural identification of ε_n with the determinant of the corresponding permutation matrix

Proposition 2.14 *We have that* $\varepsilon_n = \det(\mathcal{B}_1) \otimes \det(\mathcal{B}_2) \otimes \ldots \otimes \det(\mathcal{B}_j)$.

We can restate this proposition also for our inner product

Proposition 2.15

$$\langle Res^{G_n}_{H_{\lambda^1,\lambda^2}}\chi_n, Res^{G_n}_{H_{\lambda^1,\lambda^2}}\varepsilon_n \otimes \varepsilon\psi\rangle = \langle \chi_{\mathcal{B}_1}, det \otimes (\varepsilon)_{\mathcal{B}_1}(\psi)_{\mathcal{B}_1}\rangle_{\mathcal{B}_1} \ldots \langle \chi_{\mathcal{B}_j}, det \otimes (\varepsilon)_{\mathcal{B}_j}(\psi)_{\mathcal{B}_j}\rangle_{\mathcal{B}_j}$$

Remark Here by abuse of notation we denote with $\chi_{\mathcal{B}}$ denotes the set of allowable signed permutations induced by the action of Frob_q.

Further let us say a given block $\mathcal{B}$ is given by the factor of the type $(\mu_2 \times \mu_v)^{m_v} \rtimes S_{m_v}$. Let us denote with $\mathcal{C}_1$, $\mathcal{C}_2$, …, $\mathcal{C}_{m_v}$ the cells composing this block. Also we ignore the signs on each cell. Then we have

Proposition 2.16 $\det(\mathcal{B}) = \det(\mathcal{C}_1) \otimes \det(\mathcal{C}_2) \otimes \ldots \otimes \det(\mathcal{C}_{m_v}) \otimes (\varepsilon_{m_v})^v$

Proof: We just have to note that to bring to diagonal form the block if we just think of cells as a unit we would need an even or an odd number of moves to diagonalize according to the sign of (ε_{m_v}). Since cells are $v \times v$ dimensional, to switch places of cells requires v moves. Thus the total number of moves needed to bring each cell on the diagonal is multiplied by v and thus it agrees with $(\varepsilon_{m_v})^v$. □

We will work at block level, since actually the blocks will correspond to factors of our polynomial, and the cycle decomposition of each block will determine the degrees of the irreducible factors. This cycle decomposition is influenced by the cells and the cycle structure of the permutation of the cells in the block. Let's give an example of how this will work.

Example 2.17 *We shall look* $(\mu_2 \times \mu_2)^3 \rtimes S_3$*. Consider the following element*

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

So for this example we have the three cells and the cycle structure in S_3 *the cycle* $(3, 1, 2)$*.*

This matrix corresponds to the signed permutation $x_1 \to -x_6 \to x_4 \to x_2 \to -x_5 \to x_3 \to x_1$ *which is a* 6*-cycle and according to our description of the set* L_n *we should take it into account.*

Thus we need to keep track of the cycle decomposition of our cell permutation. Also the order of the elements of the cells will matter. Namely if we take:

$$M' = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

this will corresponds to two cycles $x_1 \to -x_5 \to x_3 \to x_1$ *and* $x_2 \to -x_6 \to x_4 \to x_2$ *and these have a minus, thus an odd number of minuses, on each cycle structure so they cannot be in our count.*

We sum this example in the following proposition

Proposition 2.18 *Consider a block* $(\mu_2 \times \mu_v)^{m_v} \rtimes S_{m_v}$. *Let* σ *an element of* S_{m_v} *and let* $\mathcal{C}$ *be an arbitrary cycle of* σ. *Ignoring the sign component* μ_2, *let the order of the cells on the cycle be* $a_1, \dots, a_{l(\mathcal{C})}$ *modulo* v. *Then this arrangement will correspond to* $\dfrac{v}{\gamma_v(a_1 + ... + a_{l(\mathcal{C})})}$ *cycles of length* $l(\mathcal{C})\gamma_v(a_1 + ... + a_{l(\mathcal{C})})$ *in the block structure, where we denote with* $\gamma_v(x)$ *denotes the order of the element in the additive group* $\mathbb{Z}/v\mathbb{Z}$.

The next proposition will give the inner product for $v \geq 2$

Proposition 2.19 *Suppose that* $v \geq 2$. *Consider the block* $\mathcal{B} = (\mu_2 \times \mu_v) \rtimes S_{m_v}$. *We have that*

$$\langle \chi_{\mathcal{B}}, det \otimes (\varepsilon)_{\mathcal{B}}(\psi)_{\mathcal{B}}\rangle_{\mathcal{B}} = \begin{cases} (-1)^{m_v+1}\frac{\frac{3}{4}(-\frac{3}{4}+1)...(-\frac{3}{4}+m_v-1)}{m_v!}, & v=2 \quad \mathcal{B}\in\lambda^1 \\ \frac{\frac{3}{4}(\frac{3}{4}+1)...(\frac{3}{4}+m_v-1)}{m_v!}, & v=2 \quad \mathcal{B}\in\lambda^2 \\ \frac{(-1)^{m_v}\frac{1}{2v}\left(\frac{1}{2v}+1\right)...\left(\frac{1}{2v}+m_v-1\right)}{m_v!}, & v=2^k \quad \mathcal{B}\in\lambda^1 \\ -\frac{\frac{1}{2v}\left(-\frac{1}{2v}+1\right)...\left(-\frac{1}{2v}+m_v-1\right)}{m_v!}, & v=2^k \quad \mathcal{B}\in\lambda^2 \\ 0, & otherwise \end{cases}$$

Proof: Let ω be a primitive root of unity of order v. Also note that we can consider for each individual permutation in S_{m_v} what the inner product is and moreover for a give permutation the inner product is multiplicative on cycles. Thus let $\sigma \in S_{m_v}$ and let $\mathcal{C}$ be a cycle in it's decomposition. We will use the same notations as we go through the subcases.

First suppose that v is odd. Note that the determinant evaluated on each cell is 1, since every cell is an odd cycle. For $\chi_{\mathcal{B}}$ to be nonzero we must have an even number of minuses on each cycle in $\mathcal{B}$. This means that for our cycle $\mathcal{C}$ we must an even number of cells with a minus using proposition 10. Thus we obtain that our sum for $\mathcal{C}$ is equal to

$$\sum_{0\leq a_i\leq v-1} 2^{l(\mathcal{C})-1}\omega^{a_1+..+a_{l(\mathcal{C})}} = 2^{l(\mathcal{C})-1}\left(\sum_{i=0}^{v-1}\omega^i\right)^{l(\mathcal{C})} = 0$$

It follows that for each $\sigma \in S_{m_v}$ the product is zero, and thus we obtain that inner product is zero.

Next suppose that $v = 2^a b$ where $a \geq 1$ and $b > 1$ is odd. Using proposition 10 we see that we have to split into two subcases; namely according to $\gamma_v(a_1 + ... + a_{l(\mathcal{C})})$

being odd or even. If this order is even, then we can take arbitrary signs on our cycle and otherwise we need to take an even number of minuses. Secondly the determinant of each cell is $(-1)^{a_j}$. Thus in this case we obtain

$$\sum_{\substack{0\le a_i\le v-1\\ \gamma_v(a_1+...+a_{l(\mathcal{C})})\text{even}}} 2^{l(\mathcal{C})}(-\omega)^{a_1+..+a_{l(\mathcal{C})}} + \sum_{\substack{0\le a_i\le v-1\\ \gamma_v(a_1+...+a_{l(\mathcal{C})})\text{odd}}} 2^{l(\mathcal{C})-1}(-\omega)^{a_1+..+a_{l(\mathcal{C})}}$$

Now obviously the sums $a_1+..+a_{l(\mathcal{C})}$ modulo v are distributed the same, namely for each $k\in\mathbb{Z}/v\mathbb{Z}$ there are $v^{l(\mathcal{C})-1}$ with sum k modulo v.

Thus our sums simplify to

$$2^{l(\mathcal{C})}v^{l(\mathcal{C})-1}\sum_{\substack{0\le j\le v-1\\ 2^a\nmid j}}(-\omega)^j + 2^{l(\mathcal{C})-1}v^{l(\mathcal{C})-1}\sum_{0\le j\le b-1}\omega^{2^a j} = 0$$

since both sums are zero.

All that is that is left is to deal with the case $v=2^a$. We need to consider $a=1$ separately. We can start from the last line above. What will modify is that the last sum $\sum_{0\le j\le b-1}\omega^{2^a j}=1$ and thus the other sum is -1. Thus for the cycle $\mathcal{C}$ we have the inner product sums to be equal to $-2^{l(\mathcal{C})-1}v^{l(\mathcal{C})-1}$.

Remembering that for σ we need to take the product over all these inner product sums of cycles, obtain that the inner product sum for a permutation is $(-1)^{c(\sigma)}(2v)^{m_v-c(\sigma)}$ where $c(\sigma)$ is the number of cycles of the permutation σ.

Further on we need to make a distinction between blocks appearing in λ^1 or λ^2; namely because the of ε_{m_v} appearing only in λ^1.

Now note that for any permutation $\varepsilon(\sigma)=(-1)^{m_v-c(\sigma)}$.

For the blocks appearing in λ^1 we obtain the inner product sum is

$$(-2v)^{m_v} \sum_{\sigma \in S_{m_v}} \left(\frac{1}{2v}\right)^{c(\sigma)}$$

It is well known that $\sum\limits_{\sigma \in S_n} X^{c(\sigma)} = X(X+1)...(X+n-1)$, see for example [42]. Thus the inner product is equal to

$$\frac{(-1)^{m_v} \frac{1}{2v} \left(\frac{1}{2v}+1\right) \dots \left(\frac{1}{2v}+m_v-1\right)}{m_v!}$$

For the blocks appearing in λ^2 we obtain that the inner product is

$$(2v)^{m_v} \frac{1}{(2v)^{m_v} m_v!} \sum_{\sigma \in S_{m_v}} \left(-\frac{1}{2v}\right)^{c(\sigma)} = -\frac{\frac{1}{2v} \left(-\frac{1}{2v}+1\right) \dots \left(-\frac{1}{2v}+m_v-1\right)}{m_v!}$$

Finally for $v = 2$ the inner product on each cycle is actually equal to $3 \cdot 4^{l(\mathcal{C})-1}$. Thus the inner product sum for a permutation is $3^{c(\sigma)}(4)^{m_v - c(\sigma)}$.

Thus if blocks with cells of size 2 appear in λ^1 we obtain the inner product is equal to

$$(-1)^{m_v} 4^{m_v} \frac{1}{4^{m_v} m_v!} \sum_{\sigma \in S_{m_v}} \left(-\frac{3}{4}\right)^{c(\sigma)} = (-1)^{m_v+1} \frac{\frac{3}{4}(-\frac{3}{4}+1) \dots (-\frac{3}{4}+m_v-1)}{m_v!}$$

If the blocks with cells of size 2 appear in λ^2 we obtain the inner product is equal to

$$\frac{\frac{3}{4}(\frac{3}{4}+1) \dots (\frac{3}{4}+m_v-1)}{m_v!}$$

□

For $v = 1$, looking at the block that contains 1 we note that it is isomorphic to a generalized permutation group G_k. Thus the inner product at block level just simplifies to computing the proportion $\frac{\#L_k}{\#G_k}$.

Proposition 2.20 *Suppose we have a block made of ones i.e* $\mathcal{B} = (\mu_2)^m \rtimes S_m = G_m$. *Then we have*

$$\langle \chi_{\mathcal{B}}, det \otimes (\varepsilon)_{\mathcal{B}}(\psi)_{\mathcal{B}} \rangle_{\mathcal{B}} = \begin{cases} \frac{\binom{2m}{m}}{4^m} & \mathcal{B} \in \lambda^1 \\ \frac{(-1)^{m+1}}{2m} \cdot \frac{\binom{2m-2}{m-1}}{4^{m-1}} & \mathcal{B} \in \lambda^2 \end{cases}$$

Proof: We can repeat the same argument as in the previous proposition's proof, but it will be much simpler since our cells have size 1 so the ψ and det of the cells components is trivial.

Thus for blocks of 1 appearing in λ^1 since the ε_m components cancel out and we just need to have an even number of $-$ on each cycle the inner product is just

$$\frac{1}{2^m \cdot m!} \sum_{\sigma \in S_m} 2^{m-c(\sigma)} = \frac{\frac{1}{2} \cdot (\frac{1}{2}+1) \dots (\frac{1}{2}+m-1)}{m!} = \frac{\binom{2m}{m}}{4^m}$$

For the blocks of 1 appearing in λ^2 we have

$$\frac{1}{2^m \cdot m!} \sum_{\sigma \in S_m} (-2)^m \cdot (-2)^{-c(\sigma)} = (-1)^m \frac{-\frac{1}{2} \cdot (-\frac{1}{2}+1) \dots (-\frac{1}{2}+m-1)}{m!} = \frac{(-1)^{m+1}}{2m} \cdot \frac{\binom{2m-2}{m-1}}{4^{m-1}}$$

□

Finally we can gather propositions 2.15, 2.19 and 2.20 proved in this section into a proposition which characterizes λ^1 and λ^2 that will actually give a nonzero inner product .

Proposition 2.21 *Suppose* $\langle Res^{G_n}_{H_{\lambda^1,\lambda^2}} \chi_n, Res^{G_n}_{H_{\lambda^1,\lambda^2}} \varepsilon_n \otimes \varepsilon\psi \rangle \neq 0$. *Then both of the* λ^1 *and* λ *should be composed only of nonnegative powers of* 2.

Definition 2.22 *A pair (λ^1, λ^2) will be called acceptable if it satisfies the conditions of proposition 2.21.*

2.5 Some explicit computations

Before we proceed to the proof of theorem 2.7, let us first show how our propositions 2.15,2.19 and 2.20 explicitly compute the inner products for H^0, H^1, H^2, H^3.

1. H^0. For H^0 from our description we only have A^0 and this is just the partitions $\lambda^1_1 + \ldots + \lambda^1_n = n$ so that means $\lambda^1_1 = \ldots = \lambda^1_n = 1$. Thus we get the inner product to be

$$\frac{|L_n|}{|G_n|} = \frac{\binom{2n}{n}}{4^n}$$

2. H^1. We only have A^0 and A^1.

   - For A^0 we have $\lambda^1_1 + \ldots + \lambda^1_{n-1} = n$ thus the only partition that works is $(2, 1, \ldots, 1)$. We obtain that the inner product is

$$\frac{3}{4} \cdot \frac{|L_{n-2}|}{|G_{n-2}|} = \frac{3}{4} \cdot \frac{\binom{2(n-2)}{n-2}}{4^{n-2}}$$

   - For A^1 we have $\lambda^1_1 + \ldots + \lambda^1_{n-1} + \lambda^2 1 = n$ so the only solution is $\lambda^1 = (1, ..., 1)$ and $\lambda^2_1 = 1$. Thus the inner product is

$$\frac{1}{2} \cdot \frac{|L_{n-1}|}{|G_{n-1}|} = \frac{1}{2} \frac{\binom{2(n-1)}{n-1}}{4^{n-1}}$$

3. H^2. We have three parts A^0, A^1 and A^2.

- For A^0 we have partitions $\lambda_1^1 + \ldots + \lambda_{n-2}^1 = n$ and they have to consist of 1's and powers of 2 thus the only one is $(2, 2, 1, \ldots, 1)$. Thus the inner product is

$$\frac{-\frac{3}{4}(-\frac{3}{4}+1)}{2!} \cdot \frac{|L_{n-4}|}{|G_{n-4}|} = -\frac{3}{32} \cdot \frac{\binom{2(n-4)}{n-4}}{4^{n-4}}$$

- For A^1 we have partitions $\lambda_1^1 + \ldots + \lambda_{n-2}^1 + \lambda_1^2 = n$ and we either have $\lambda^1 = (2, 1, \ldots, 1)$ and $\lambda_1^2 = 1$ or $\lambda^1 = (1, \ldots, 1)$ and $\lambda_1^2 = 2$. Thus the inner product is

$$\frac{3}{4} \cdot \frac{|L_{n-3}|}{|G_{n-3}|} \cdot \frac{1}{2} + \frac{|L_{n-2}|}{|G_{n-2}|} \cdot \frac{3}{4} = \frac{3}{8} \cdot \frac{\binom{2(n-3)}{n-3}}{4^{n-3}} + \frac{3}{4} \cdot \frac{\binom{2(n-2)}{n-2}}{4^{n-2}}$$

- For A^2 we have the relation $\lambda_1^1 + \ldots + \lambda_{n-2}^1 + \lambda_1^2 + \lambda_2^2 = n$ and again the only solution is $\lambda^1 = (1, \ldots, 1)$ and $\lambda^2 = (1, 1)$. Thus the inner product is

$$\frac{-\frac{1}{2}(-\frac{1}{2}+1)}{2!} \cdot \frac{|L_{n-2}|}{|G_{n-2}|} = -\frac{1}{8} \cdot \frac{\binom{2(n-2)}{n-2}}{4^{n-2}}$$

4. H^3. We need to look at four pieces, A^0, A^1, A^2 and A^3.

- For A^0 we look at partitions made up of 1's and powers of 2 such that $\lambda_1^1 + \ldots + \lambda_{n-3}^1 = n$. The only ones that work are $\lambda^1 = (4, 1, \ldots, 1)$ and $\lambda^1 = (2, 2, 2, 1, \ldots, 1)$. Thus the inner product is

$$-\frac{1}{8} \cdot \frac{|L_{n-4}|}{|G_{n-4}|} + \frac{\frac{3}{4}(-\frac{3}{4}+1))(-\frac{3}{4}+2)}{3!} \cdot \frac{|L_{n-6}|}{|G_{n-6}|} = -\frac{1}{8} \cdot \frac{\binom{2(n-4)}{n-4}}{4^{n-4}} + \frac{5}{128} \frac{\binom{2(n-6)}{n-6}}{4^{n-6}}$$

- For A^1 we have $\lambda_1^1 + \ldots + \lambda_{n-3}^1 + \lambda_1^2 = n$. This is similar to the case A^0 for H^2 and we get two possibilities $\lambda^1 = (2, 2, 1, \ldots, 1)$ and $\lambda_1^2 = 1$ or $\lambda^1 = (2, 1, \ldots, 1)$ and $\lambda_1^2 = 2$. Thus the inner product is

$$-\frac{\frac{3}{4}(-\frac{3}{4}+1)}{2!} \cdot \frac{|L_{n-5}|}{|G_{n-5}|} \cdot \frac{1}{2} + \frac{3}{4} \cdot \frac{|L_{n-4}|}{|G_{n-4}|} \cdot \frac{3}{4} = -\frac{3}{64} \cdot \frac{\binom{2(n-5)}{n-5}}{4^{n-5}} + \frac{3}{16} \cdot \frac{\binom{2(n-4)}{n-4}}{4^{n-4}}$$

- For A^2 we look at $\lambda_1^1 + \ldots + \lambda_{n-3}^1 + \lambda_1^2 + \lambda_2^2 = n$. The only solutions are $\lambda^1 = (2, 1, \ldots, 1)$ and $\lambda^2 = (1, 1)$ or $\lambda^1 = (1, \ldots, 1)$ and $\lambda^2 = (2, 1)$. Thus the inner product is

$$\frac{3}{4} \cdot \frac{|L_{n-4}|}{|G_{n-4}|} \cdot \frac{-\frac{1}{2}(-\frac{1}{2}+1)}{2!} + \frac{|L_{n-3}|}{|G_{n-3}|} \cdot \frac{3}{4} \cdot \frac{1}{2} = -\frac{3}{32} \cdot \frac{\binom{2(n-4)}{n-4}}{4^{n-4}} + \frac{3}{8} \frac{\binom{2(n-3)}{n-3}}{4^{n-3}}$$

- Finally for A^3 since $\lambda_1^1 + \ldots + \lambda_{n-3}^1 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2 = n$ the only possibility is $\lambda^1 = (1, \ldots, 1)$ and $\lambda^2 = (1, 1, 1)$. Thus the inner product is

$$\frac{|L_{n-3}|}{|G_{n-3}|} \cdot \frac{\frac{1}{2}(-\frac{1}{2}+1)(-\frac{1}{2}+2)}{3!} = \frac{1}{16} \cdot \frac{\binom{2(n-3)}{n-3}}{4^{n-3}}$$

Putting everything together in the corollary of theorem 1.4 and using the notation $h_k = \frac{\binom{2k}{k}}{4^k}$ (same as in [3]) we obtain

$$S_n^o(q) = q^n h_n - q^{n-1}\left(\frac{1}{2} \cdot h_{n-1} + \frac{3}{4} \cdot h_{n-2}\right) + q^{n-2} \cdot \left(\frac{5}{8} \cdot h_{n-2} + \frac{3}{8} h_{n-3} - \frac{3}{32} h_{n-4}\right) -$$
$$-q^{n-3}\left(\frac{5}{16} h_{n-3} - \frac{1}{32} h_{n-4} - \frac{3}{64} h_{n-5} - \frac{5}{128} h_{n-6}\right) + O(q^{n-4})$$

Using the relation $S_q(n) = S_q^o(n) + S_q^o(n-1)$ in section 1 (2.1)and the formula $B_q(n) = \sum_{i=0}^{\lceil \frac{n}{2} \rceil} q^i S_q(n-2i)$ obtained in section 7(2.7) we obtain

$$B_q(n) = q^n h_n + q^{n-1}\left(\frac{1}{2}h_{n-1} + \frac{1}{4}h_{n-2}\right) + q^{n-2}\left(\frac{1}{8}h_{n-2} + \frac{1}{8}h_{n-3} - \frac{27}{32}h_{n-4}\right) +$$
$$+q^{n-3}\left(\frac{5}{16}h_{n-3} + \frac{17}{32}h_{n-4} + \frac{5}{64}h_{n-5} - \frac{55}{128}h_{n-6}\right) + O(q^{n-4})$$

2.6 Proof of Theorem 2.7

We start looking at the equality $\lambda_1^1 + ... + \lambda_{n-p}^1 + \lambda_1^2 + \ldots + \lambda_l^2 = n$, for a fixed $0 \leq l < p$ where (λ^1, λ^2) is an acceptable pair. First let us characterize the multiplicity of 1 in (λ^1, λ^2).

Proposition 2.23 1 *can appear in an acceptable pair* (λ^1, λ^2) *with multiplicity equal to* $n - 2k$*, where* k *is any integer* $0 \leq k \leq p - l$*. Moreover the multiplicity of* 1 *in* λ^1*, call it* a*, satisfies* $n - 2p + l \leq a \leq n - p$*.*

Proof: Let a the multiplicity of 1 in λ^1 and b the multiplicity of 1 in λ^2 in a random acceptable pair (λ^1, λ^2) with $\lambda_1^1 + ... + \lambda_{n-p}^1 + \lambda_1^2 + \ldots + \lambda_l^2 = n$. Then using proposition 14 the other number appearing in λ^1 and λ^2 are powers of 2 so $a + b$ has to have the same parity as n.

Now let $a + b = n - 2k$. Then since the other numbers appearing are at least equal to 2 we have $n - 2k + 2((n - p + l) - (n - 2k)) \leq n$ so simplifying yields the bound $k + l \leq p$. Now since $b \leq l$ it follows that $a \geq n - 2k - l \geq n - 2p + l$. □

We can now proceed to the proof of theorem 2.7. We will obtain bounds, but these will be far from optimal. Also we will not write an explicit formula for the coefficient of each h_i term appearing; the previous two sections provide the recipe for computing out this coefficient. The combinatorics involved in simplifying further the expressions seems hard.

Proof Theorem 2.7

We will group terms by looking at a, the multiplicity of 1 in λ^1. We will consider a fixed l and afterwards will sum over the l's.

By the previous proposition we know it satisfies $n-2p+l \leq a \leq n-p$. Thus we are left to write $n-a = \lambda^1_1 + ... + \lambda^1_{n-a-p} + \lambda^2_1 + \ldots + \lambda^2_l$.

Note that the stabilization is just a combinatorial statement. If $n \geq 2p$ it allows us to take any $n-2p \leq a \leq n-p$ and we can write every possibility out for $n-a$ as a sum of positive exponent powers of 2 and 1's.

Let b be the multiplicity of 1 in λ^2. Thus from the previous proposition we have $k = \mu^1_1 + ... + \mu^1_{n-a-p} + \mu^2_1 + \ldots + \mu^2_{l-b}$ where $(\mu^1, \mu^2) = \frac{1}{2}(\lambda^1, \lambda^2)$.

Now to obtain the bound we just need to write k as a sum of nonnegative powers of 2 with a fixed number of summands. We can trivially upper bound this by the number of ways we can write k as a sum of nonnegative powers of 2 times the number of ways in which we can reconstruct λ^2.

Say we have a writing $k = \sum_{i=1}^r m_i 2^{a_i}$ where $a_1 < \ldots < a_r$ are nonnegative integers. To construct μ^2 we need positive integers $x_1, \ldots, x_s$ such that $x_1 + \ldots + x_s = l - b$ and $x_i \leq m_{j_i}$ for some subset $\{j_1, \ldots, j_s\}$ of $\{1, .., r\}$.

Now using proposition 11, we know that each of inner product at block level for λ^2 are in absolute value less than $\dfrac{1}{2m}$ where m is the multiplicity of the power of 2 bigger than 1 and for a block that corresponds to 2 the inner product is bounded in absolute value by 1. The inner products for λ^1 we will absolutely bound them by 1.

Thus we conclude that summing over all possibilities, the inner products we get at most $\sum \frac{1}{2^s x_1 \ldots x_s}$

if $a_1 > 0$ and $\sum \frac{1}{2^{s-1} x_2 \ldots x_s}$ if $a_1 = 0$ and we are taking 1's in μ_2, or equivalently 2's in λ^2.

We can trivially upper bound these contributions by

$$(\max m_i)\left(1+\frac{1}{2}+\frac{1}{4}+\ldots+\frac{1}{2m_2}\right)\ldots\left(1+\frac{1}{2}+\ldots+\frac{1}{2m_r}\right)$$

Now using $1+\frac{1}{2}+\ldots+\frac{1}{2n} < \ln(n)$ we obtain that our inner products are bounded by

$$\max(m_i)\ln(m_1)\ldots\ln(m_r) < k(\ln(k))^{r-1} < k(\ln(k))^{\log_2(k)}$$

since k can be written as a sum of at most $\log_2(k)$ distinct powers.

Finally we need to account for how many distinct writings of k as nonnegative powers of 2. can we have, since we are summing over all of these. This is well known sequence; we can find it under A000123 in the Online Encyclopedia of Integer sequences and the precise asymptotic of it is given in [11]. We can restate state this in a weaker upper bound, namely

Proposition 2.24 *Let $b_2(y)$ the number of partitions of a positive integer y into nonnegative powers of 2. Then there is an absolute constant A such that*

$$b_2(y) < Ae^{\ln(y)^2}$$

Finally we need to sum over all the possibilities of b. Using $k \leq p-l$ we get that h_a appear with coefficient bounded in absolute value by

$$Al(\ln(p-l))^{\log_2(p-l)} e^{\ln(p-l)^2} < B(1.1)^{p-l}$$

for some absolute constant B. Summing up over l gives that the coefficient of $h_{n-(p+j)}$ with $0 \leq j \leq p$ is at most

$$B(1.1)^p \sum_{l=0}^{p-j} (1.1)^{-l} < 10B(1.1)^p$$

since we can trivially bound the last sum by the total geometric series.

2.7 Proof of Theorem 2.4

We now have all the ingredients in place to prove theorem 2.4. First let us show the connection between theorem 2.4 and theorem 2.7.

Proposition 2.25 *We have that*

$$b_{k,n} = \sum_{j=0}^{k} (-1)^{k-j} (c_{j,n-2k+2j} + c_{j,n-2k+2j-1})$$

Proof: First let us remark that $B_q(n)$ is invariant under which quadratic extension of $\mathbb{F}_q[T]$ we consider.

Next we note that since every monic polynomial of degree n factors uniquely as U^2V and the fact that U^2V is a norm iff V is a norm, we obtain the recurrence

$$B_q(n) = \sum_{i=0}^{\lceil \frac{n}{2} \rceil} q^i S_q(n-2i)$$

We can rewrite this as $B_q(n) = \sum\limits_{0 \leq 2i+j \leq n} (-1)^j (c_{j,n-2i} + c_{j,n-2i-1}) q^{n-i-j}$. Denoting with $i+j=k$ and letting k range from 0 to n we can further rewrite as

$$B_q(n) = \sum_{k=0}^{n} \left(\sum_{2k-n \leq j \leq k} (-1)^j (c_{j,n-2k+2j} + c_{j,n-2k+2j-1}) \right) q^{n-k}$$

The stated result thus follows.

□

We can use this proposition to obtain the relation between the coefficients Γ and δ namely

Proposition 2.26 *We have that*

a) $\delta_{k,j,n} = \sum\limits_{l=0}^{j} (-1)^{j-l} (\Gamma_{l,2k+l-j,n+2l-2j} + \Gamma_{l,2k+l-j,n+2l-2j-1})$ *;*

b) $|\delta_{k,j,n}| \leq C(1.1)^k$.

Proof: Part a) is just a formal manipulation of proposition 19 and the description of the expansion of $c_{k,n}$ in theorem 2. For the second part applying the bounds on the gamma coefficients from theorem 2.7 it follows

$$|\delta_{k,j,n}| \leq 2B \sum_{l=0}^{j} (1.1)^l \leq 20B(1.1)^{j+1} \leq 22B(1.1)^k$$

and thus the claim follows.

□

2.8 Number of irreducible polynomials

This statistic might not be new, but we will obtain an exact count of the number of split polynomials and thus we can estimate the difference between the split and non-split. This is motivated by a prime number race. Namely we can think about irreducible of form A^2+TB^2 as corresponding to primes which are congruent to $1 \pmod 4$; namely this is in the norm in the extension $\mathbb{F}_q[\sqrt{-T}]/\mathbb{F}_q[T]$ and number field extension it corresponds to is $\mathbb{Q}(i)/\mathbb{Q}$. The split primes in the extension $\mathbb{Q}(i)/\mathbb{Q}$ are precisely the primes congruent to $1 \pmod 4$. Here we have switched from our norm $|A^2-TB^2|$ to A^2+TB^2, but for function fields over finite fields the count is not affected by which quadratic extension we consider.

The analogous problem over the integer is estimating how the difference between the count primes congruent to 1 modulo 4 and primes congruent to 3 modulo 4 in the interval $[X, 2X]$ behaves as $X \to \infty$ and this is what is referred in the literature as a prime number race.

We already know by using the Chebotarev density theorem for the extension $\mathbb{Q}(i)/\mathbb{Q}$ that there should be roughly half and half, but our count suggests a potential error term on the order of $\dfrac{\sqrt{X}}{\log(X)}$.

Definition 2.27 *Let $\pi^s_{n,q}$ and $\pi^{ns}_{n,q}$ be the number of split, respectively nonsplit polynomials in the extension $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$.*

In general we have the relation $\pi^s_{n,q}+\pi^{ns}_{n,q}=\pi_{n,q}$ except for $n=1$ where $\pi^s_{1,q}+\pi^s_{1,q}=q-1$, since T is ramified in this quadratic extension. Moreover, we actually have $\pi^s_{1,q}=\pi^{ns}_{1,q}=\dfrac{q-1}{2}$ since a polynomial, $T-a$, is split in $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$ if and only if a is a square in $\mathbb{F}_q^\times$.

The following theorem gives a precise count.

Theorem 2.28 *We have that for $n \geq 2$*

$$\pi^s_{n,q} = \begin{cases} \frac{1}{2n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d, \textit{if } n \ \textit{odd} \\ \frac{1}{2^{a+1}}(q^{2^a} - 2q^{2^{a-1}} + 1), \textit{if } n = 2^a \\ \frac{1}{2^{a+1}b}(\sum_{d|b} \mu(d) q^{2^a b/d} - 2\sum_{d|b} \mu(d) q^{2^{a-1}b/d}), \textit{if } n = 2^a b, b > 1 \ \textit{odd} \end{cases}$$

We will offer to alternative proofs to the theorem. The first one only uses a description of the split polynomials and a recurrence relation, while the second one relies on our cohomological description and computing the inner products. Let's start the proof with a proposition which characterizes irreducible split polynomials in $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$.

Proposition 2.29 *A polynomials $f \in \mathcal{M}_{n,q}$ is split in the extension $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$ if and only if there is a $g \in \mathcal{M}_{n,q}$ such that $f(T) = (-1)^n g(\sqrt{T})g(-\sqrt{T})$.*

Proof: Suppose $f(T) = h_1(\sqrt{T})\dots h_r(\sqrt{T})$, where each $h_i \in \mathcal{M}_{n,q}$. Note that if $\alpha \in \overline{\mathbb{F}}_q$ is a root of h_i then α^2 is a root of f so that means that $h_1(-\alpha)\dots h_r(-\alpha) = 0$ and thus we have that exists an index j such that $h_j(\sqrt{T}) = h_i(-\sqrt{T})$.

Now if $r \geq 3$ then noting that $h(\sqrt{T})h(-\sqrt{T})$ is a polynomial in $\mathbb{F}_q[T]$, it would follow that f is not irreducible which is a contradiction.

□

We can now turn to our recurrence relation which will produce the desired count.

Proposition 2.30 *We have that for $n \geq 2$*

$$\pi^s_{n,q} = \begin{cases} \dfrac{\pi_{n,q}}{2}, \textit{ if } n \ \ \textit{odd} \\ \dfrac{\pi_{n,q}}{2} - \dfrac{\pi_{n/2,q}}{2} + \dfrac{\pi^s_{n/2,q}}{2} \quad \textit{otherwise.} \end{cases}$$

Proof: The key to the proof is the above proposition. We will count f by condition on what possible g arise. Note that we need to exclude two things to get the precise count: $g(\sqrt{T}) = \pm g(-\sqrt{T})$ and the fact that we can switch $g(T)$ with $\pm g(-T)$ and obtain the same decomposition of f.

If n is odd then we have to exclude $g(\sqrt{T}) = -g(-\sqrt{T})$. This means that $g(\sqrt{T}) = \sqrt{T}h(T)$ so $g = Th(T^2)$, but g is irreducible so $g = T$ so n must be 1. Since we've assumed $n \geq 2$ we obtain a contradiction. Thus for n odd only switching matters and we obtained the desired count.

If n is even then we have to exclude $g(\sqrt{T}) = g(-\sqrt{T})$. This means that $g = h(T^2)$, where $h \in \mathcal{M}_{n/2,q}$. These are polynomials with the property that $h(T)$ and $h(T^2)$ are both irreducible. But this obviously is the same as saying that h is not split in the extension $\mathbb{F}_q[\sqrt{T}]/\mathbb{F}_q[T]$. We have to account again for switching and this ends the proof of the proposition.

□

Putting together these two propositions and using the formula for $\pi_{n,q}$ in theorem 1.12 we end the first proof of the above theorem.

We turn to the cohomological proof. Theorem 2.10 in section 2.2 is valid for any class function we pick. Since G_n is naturally a permutation group, but with signed elements, it makes sense to talk about the standard characters of S_n, X_i, as class functions of G_n by just ignoring the signs on each element. Now counting irreducible polynomials is the same as counting n cycles under the Frob_q action, so all we have to do is take $\chi = \chi_n X_n$

and compute the inner products.

The next proposition will tell us which factors are automatically zero in this count.

Proposition 2.31 *Suppose that $\langle \chi_n X_n, H^p \rangle \neq 0$. Then either:*

(i) $n - p = d$ is a divisor of n and the only partitions that contribute to this inner product are $\lambda^1_1 = \ldots = \lambda^1_d = \dfrac{n}{d}$;

(ii) $p = n$, $l|n$ and $\lambda^2_1 = \ldots = \lambda^2_l = \dfrac{n}{l}$

Proof: If $p < n$, because of the way we construct the subgroup H_{λ^1,λ^2} as blocks along the main diagonal of our signed permutation matrix, to have an n-cycle means that we only have one block. Thus we must have no λ^2 part and since the cells in the block have the same size the proposition follows.

The second part of the proposition follows along the same lines, since in this case there is no λ^1 component so we have to arrange only blocks in λ^2 and again there can be only one. □

The last ingredient we need is a version of proposition 2.19.

Proposition 2.32 *We have that for d a divisor of n*

$$\langle \chi_n X_n, H^{n-d} \rangle = \begin{cases} \dfrac{\mu(\frac{n}{d})}{2n}, \textit{if } n \textit{ odd} \\ (-1)^d \dfrac{\mu(\frac{2^a b}{d})}{2^a b}, \textit{if } n = 2^a b,\ b \textit{ odd and } 2^a \nmid d \\ \dfrac{\mu(\frac{2^a b}{d})}{2^{a+1} b}, \textit{if } n = 2^a b,\ b \textit{ odd and } 2^a | d \end{cases}$$

Proof: We will use the same notations as in proposition 2.19. First let's suppose that n is odd. Using the proposition 2.16 and since every odd cell is an odd cycle, we have that ε components cancel out.

To get an n-cycle from the block $(\mu_2 \times \mu_{n/d})^d \rtimes S_d$ we must arrange the cells in a d cycle and moreover the sums of the orders of the cells in proposition 2.19 has to equal to n/d. Thus we must have that $a_1 + \ldots + a_d$ is coprime to n/d, where $a_1, \ldots, a_d$ are the orders of the cells in the decomposition. We know that there are $(d-1)!$ cycles of length d. Our sum for the inner product is

$$\sum_{\substack{0\leq a_i \leq n/d-1 \\ \gamma_{n/d}(a_1+\ldots+a_d)=n/d}} 2^{d-1}\omega^{a_1+\ldots+a_d} = 2^{d-1}\left(\frac{n}{d}\right)^{d-1} \sum_{\substack{1\leq k\leq n/d \\ (k,n/d)=1}} \omega^k = 2^{d-1}\left(\frac{n}{d}\right)^{d-1}\mu(\frac{n}{d})$$

since we can pick arbitrarly $d-1$ of the orders of the cells and the sum of the primitive roots of unity is given by the mobius function, i.e $\sum_{\zeta\in\mu_k \text{ primitive}} \zeta = \mu(k)$.

Dividing by the size of the group which is $2^d\left(\frac{n}{d}\right)^d d!$ we obtain the first part.

Suppose now that $n = 2^a b$ where $b > 1$ odd. We now have to split according to two types of divisors; this is due to proposition 2.16 because the ε_{m_v} will cancel or not. If 2^a does not divide d then it cancels out since it appears at an even power, namely $2^a b/d$. Again as in the previous paragraph we $(d-1)!$ cycles of length d and the sum for the inner product is

$$(-1)^{d-1} \sum_{\substack{0\leq a_i \leq n/d-1 \\ \gamma_{n/d}(a_1+\ldots+a_d)=n/d}} 2^d(-\omega)^{a_1+\ldots+a_d} = 2^d(-1)^{d-1}\left(\frac{n}{d}\right)^{d-1} \sum_{\substack{1\leq k\leq n/d \\ (k,n/d)=1}} (-\omega)^k = (-1)^d 2^d\left(\frac{n}{d}\right)^{d-1}\mu(\frac{n}{d})$$

This is since the d cycle we get in the permutation has signature equal to $(-1)^{d-1}$, the determinant of each cell is $(-1)^{a_i}$, we can take arbitrary signs on cells and k is odd since it is coprime to n/d which is even.

Thus we obtain that the inner product is equal to $(-1)^{d-1}\dfrac{\mu(\frac{2^a b}{d})}{2^a b}$.

If d is divisible by 2^a, then the ε_{m_v} does not cancel out but it does so in the inner product. Moreover the above sum is halved since we cannot take arbitrary signs on cells; we have to take an even number of minuses. Lastly, $-\omega$ is still is primitive root of unity and this finishes the proof of the proposition.

□

The only thing left to compute is the inner product with H^n.

Proposition 2.33 *We have that*

$$\langle \chi_n X_n, H^n \rangle = \begin{cases} \dfrac{1}{2^{a+1}}, \mathit{if}\, n = 2^a,\ a \geq 0 \\ 0, \mathit{otherwise} \end{cases}$$

Proof: The proof goes along the same lines as the above. All we need to at the end do is to sum over all the possibilities of l.

If n is odd, then we have that for each $l|n$ we have the inner product is equal to $\dfrac{\mu(\frac{n}{l})}{2n}$; even though we do not have the signature character in λ^2 the l cycle has odd length so signature. Thus we obtain that the inner product with H^n is equal to $\dfrac{1}{2n}\sum_{l|n}\mu(\dfrac{l}{n})$ and this is equal to $\frac{1}{2}$ for $n = 1$ and 0 otherwise.

If $n = 2^a b$ we again need to divide into two parts.

For $2^a \nmid l$ we obtain almost the same inner product, except the $(-1)^{l-1}$ since the signature component in proposition 2.16 will be trivial; being raised to an even power it will cancel out. Thus we obtain that the inner product is $-\dfrac{\mu(\frac{2^ab}{l})}{2^ab}$

For $2^a \nmid l$, the signature will matter and it will not cancel out in the inner product since it does appear in the induced character since that takes into account only λ^1. Since it is an even cycle we get signature -1 and so the inner product is $-\dfrac{\mu(\frac{2^ab}{l})}{2^{a+1}b}$

Summing up we have

$$-\frac{1}{2^ab}\sum_{\substack{l|2^ab\\2^a\nmid l}}\mu(\frac{2^ab}{l})-\frac{1}{2^{a+1}b}\sum_{\substack{l|2^ab\\2^a|l}}\mu(\frac{2^ab}{l})=\frac{1}{2^ab}\sum_{\substack{l|2^ab\\2^a|l}}\mu(\frac{2^ab}{l})-\frac{1}{2^{a+1}b}\sum_{\substack{l|2^ab\\2^a|l}}\mu(\frac{2^ab}{l})=\frac{1}{2^{a+1}b}\sum_{m|b}\mu(\frac{b}{m})$$

and again we obtain for the inner sum the value 1 for $b = 1$ and 0 otherwise.

□

Putting propositions 2.32 and 2.33 in theorem 2.10, we obtain a cohomological proof for the number of irreducible polynomials.

2.9 Expected number of roots

Another interesting statistic to consider is how many roots on average does our family of polynomials have, or in other words what is the expected number of roots. A rough analogy with the integers picture is how many small prime factors does a number of the form $x^2 + y^2$ have on average.

We will rely on theorem 2.10 for the proof, and we shall just obtain the first two terms. Using this approach we just need to compute $\langle X_1\chi_n, H^0\rangle$ and $\langle X_1\chi_n, H^1\rangle$. The combinatorics seems difficult to approach with a uniform method, even though as before the blocks of 1's will play a central role. It would be interesting if one could find a general recipe to compute out all the inner products.

Let us state the main theorem.

Theorem 2.34 *We have that*

$$\sum_{f\in \mathrm{Conf}_n^0} X_1(f)\chi_n(f) = \frac{\binom{(2n-2)}{n-1}}{2\cdot 4^{n-1}}q^n+\left(\frac{\binom{(2n-2)}{n-1}}{2\cdot 4^{n-1}}+\frac{3\binom{(2n-4)}{n-2}}{4^{n-1}}+\frac{3\binom{(2n-6)}{n-3}}{4^{n-2}}\right)q^{n-1}+O(q^{n-2})$$

Corollary 2.35 *We have that the expected number of roots as $n, q \to \infty$ is*

$$\lim_{n,q\to\infty} \frac{1}{B_q(n)} \sum_{f\in \mathrm{Conf}_n^0} X_1(f)\chi_n(f) = \frac{1}{2}$$

Remark 2.36 *We can still say that the expected number of root is 1 because in the above we have not accounted for the fact that a linear polynomial, $T-a$, is split in $\mathbb{F}_q[\sqrt{T}]$ if and only if a is a square in $\mathbb{F}_q^\times$. Since the number of squares is $(q-1)/2$ so with $1/2$ density, we can renormalize the above result by multiplying by 2.*

Remark 2.37 *We could bootstrap the result to Conf^n, by saying we either have zero as a root so by deleting it we end up in Conf_{n-1}^0 and we can us the linearity of the inner product, or we do not zero as a root and we up in Conf_n^0.*

To prove we just need the following key proposition.

Proposition 2.38 *We have that for $n \geq 1$,*

$$\langle X_1\chi_n, \mathbf{1}\rangle_{G_n} = \frac{1}{2}\cdot\frac{\binom{(2n-2)}{n-1}}{4^{n-1}}$$

where by $\mathbf{1}$ we mean the trivial character of G_n.

Proof: Unlike the previous proofs we rely heavily on the cycle structure of our permutation. Namely the given sum for the inner product is

$$\sum \frac{n!}{1^{m_1}2^{m_2}\dots n^{m_n}m_1!\dots m_n!} \cdot 2^{m_1(1-1)}2^{m_2(2-1)}\dots 2^{m_n(n-1)} \cdot m_1$$

since we must have an even number of minuses on each cycle. The sum is over all partitions $1m_1 + 2m_2 + \ldots + nm_n = n$ and we use the fact for a cycle structure there are exactly $\frac{n!}{1^{m_1}2^{m_2}\dots n^{m_n}m_1!\dots m_n!}$ permutations that have cycle type $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$.

Rearraging terms we have that the desired sum is

$$2^n n! \sum \frac{1}{(2)^{m_1}(4)^{m_2}\dots(2n)^{m_n}m_1!\dots m_n!} \cdot m_1$$

where we sum over all partitions $1m_1 + 2m_2 + \ldots + nm_n = n$. Now we need only consider those where $m_1 \geq 1$ and simplifying we obtain

$$\frac{1}{2}\sum \frac{1}{(2)^{m_1-1}(4)^{m_2}\dots(2n)^{m_n}(m_1-1)!\dots m_n!}$$

The main trick in computing the sum is the fact that it is equal to the number of permutations of $1, 2, \dots, 2n-2$ that only have even length cycles, divided by the total number of permutations.

We can compute the number of such permutations of $\{1, 2, \dots, 2k\}$ using a recurrence relation and let's call this number $C_2(k)$. Since 1 cannot be fixed it must go to one of the other $2k-1$ values, call it x, and x must go to one of the other $2k-2$ values or 1. Thus if we delete 1 and x, we still get an even cycle structure. We conclude that $C_2(k) = (2k-1)(2k-2+1)C_2(k-1) = (2k-1)^2C_2(k-1)$. We thus obtain $C_2(k) = ((2k-1)!!)^2$.

Thus we obtain that the inner product sum is equal to $\dfrac{2^n n!((2n-3)!!)^2}{2(2n-2)!}$ and thus the inner product is $\dfrac{((2n-3)!!)^2}{2(2n-2)!} = \dfrac{\binom{(2n-2)}{n-1}}{2\cdot 4^{n-1}}$

□

The next proposition will give us the theorem.

Proposition 2.39 *We have that* $\langle X_1\chi_n, H^0\rangle = \langle X_1\chi_n, \mathbf{1}\rangle_{G_n}$ *and* $\langle X_1\chi_n, H^1\rangle = \dfrac{\langle X_1\chi_{n-1}, \mathbf{1}\rangle_{G_{n-1}}}{2} + \dfrac{3\langle X_1\chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{4} + \dfrac{\langle \chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{2} + \dfrac{\langle \chi_{n-1}, \mathbf{1}\rangle_{G_{n-1}}}{2}$.

Proof: For H^0 the statement is trivial since we only have the partition $\lambda_1^1 = \ldots = \lambda_n^1 = 1$ and $\varepsilon\psi = \mathbf{1}$.

For H^1 there are two possibilities: either $\lambda^1 = 2$ and $\lambda_2^1 = \ldots = \lambda_{n-1}^1 = 1$ or $\lambda_1^1 = \ldots = \lambda_{n-1}^1 = 1$ and $\lambda_1^2 = 1$.

In the first case we have two blocks and again for both of them $\varepsilon\psi = \mathbf{1}$. We are only allowed the following structures for the size 2×2 block, I_2, $\mathfrak{g}_2$ and $-\mathfrak{g}_2$. In the case of I_2 we have that X_1 has two extra fixed points added to it's restriction to G_{n-2} block, so we obtain that the inner product is equal to $\dfrac{\langle (X_1+2)\chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{4}$. In both cases of $\mathfrak{g}_2$ and $-\mathfrak{g}_2$ there are no extra fixed points added so we obtain $\dfrac{\langle X_1\chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{2}$.

For the second case $\lambda_1^1 = \ldots = \lambda_{n-1}^1 = 1$ and $\lambda_1^2 = 1$ we have that X_1 has an extra fixed point added from λ^2 so we obtain $\dfrac{\langle (X_1+1)\chi_{n-1}, \mathbf{1}\rangle_{G_{n-1}}}{2}$

Adding up and using linearity we obtain $\dfrac{\langle X_1\chi_{n-1}, \mathbf{1}\rangle_{G_{n-1}}}{2} + \dfrac{3\langle X_1\chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{4} + \dfrac{\langle \chi_{n-2}, \mathbf{1}\rangle_{G_{n-2}}}{2} + \dfrac{\langle \chi_{n-1}, \mathbf{1}\rangle_{G_{n-1}}}{2}$. □

To finish the proof of theorem 2.36 we just need to understand what the inner product $\langle \chi_k, \mathbf{1}\rangle_{G_k}$ is. We have already computed it in proposition 2.20 and it is equal to $\dfrac{\binom{2k}{k}}{4^k}$.

2.10 Further Directions of Work

One further direction is of course obtaining a complete description of the terms that appear in theorem 2.34. There also seems to be a recurring theme among the results obtained in [8],[39], [9]- namely that the expected number of roots is 1 and also in our case if we renormalize. Is this theorem true in more generality?

Another problem which is similar in spirit to the present work, already posed in [8], is finding the number of $f \in \mathcal{M}_{n,q}$ such that $f = A^d - TB^d$. Henderson's result still holds in this situation, our setup goes through but there are slight tweaks to be worked out in the combinatorics of the situation. This problem is the same as finding explicitly how many integers from $[1, X]$ can be written as $a^d + b^d$, in our dictionary of analogies.

Finally we can also ask whether this stability phenomena is true in more generality. It is remarked in [8] that our class function χ_n is not a character polynomial. Our result gives a new type of stability. We can say that the binomial is a kind of universal function and the coefficients that appear with it stabilize after a certain threshold. Is this type of result true in more generality? More specifically what class functions, that are not character polynomials, exhibit this type of behavior when we compute the inner products with the cohomology groups.

Bibliography

[1] V. Arnol'd, *On some topological invariants of algebraic functions*, Trans. Math. Moscow Math. Soc., 21 (1970), pp. 30–52.

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. II. Analytischer Teil*, Mathematische Zeitschrift, 19 (1924), pp. 207–246.

[3] E. Bank, L. Bary-Soroker, and A. Fehm, *Sums of two squares in short intervals in polynomial rings over finite fields*, American Journal of Mathematics, in press.

[4] L. Bary-Soroker, *Hardy-Littlewood tuple conjecture over large finite fields*, Int.Math. Res. Not., (2012), pp. 1–8.

[5] L. Bary-Soroker, Y. Smilanski, and A. Wolf, *On the function field analogue of Landau's theorem on sums of squares*, Finite Fields Appl., 39 (2016), pp. 195–215.

[6] M. Bhargava, *The density of discriminants of quartic rings and fields*, Annals of Mathematics, 162(2) (2005), pp. 1031–1063.

[7] ——, *The density of discriminants of quintic rings and fields*, Annals of Mathematics, 172(3) (2010), pp. 1559–1591.

[8] K. Casto, *FI_G-modules and arithmetic statistics.* online preprint https://arxiv.org/abs/1703.07295.

[9] T. Church, J. S. Ellenberg, and B. Farb, *Representation stability in cohomology and asymptotics for families of varieties over finite fields*, Contemporary Mathematics, 620 (2014), pp. 1–54.

[10] T. Church and B. Farb, *Representation theory and homological stability*, Adv.Math., (2013), pp. 250–314.

[11] N. de Brujin, *On mahler's partition problem*, Indagationes Mathematicae, X (1948), pp. 210–220.

[12] P. Deligne, *La conjecture de Weil I*, Inst. Hautes Études Sci. Publ. Math., 48 (1974), pp. 273–308.

[13] P. Deligne, *La conjecture de Weil II*, Inst. Hautes Études Sci. Publ. Math., 52 (1975), pp. 313–428.

[14] P. Deligne, J.-F. Boutot, L. Illusie, and J.-L. Verdier, *Cohomologie étale*, Springer Lecture Notes, 1977.

[15] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics, 82 (1960), pp. 631–648.

[16] B. Efrat, L. Bary-Soroker, and L. Rosenzweig, *Prime polynomial values in short intervals and in arithmetic progressions*, Duke Math.J., 164 (2015), pp. 277–295.

[17] J. S. Ellenberg, *Geometric Analytic Number Theory.* http://swc.math.arizona.edu/aws/2014/2014EllenbergNotes.pdf.

[18] J. S. Ellenberg, T. Tran, and C. Westerland, *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and malle's conjecture for function fields.* https://arxiv.org/abs/1701.04541.

[19] L. Euler, *Variae observationes circa series infinitas*, Comm. Acd. Sci. Petropolitanae, 9 (1737), pp. 222–236.

[20] Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs New Series, 21, The Clarendon Press, Oxford University Press, New York, 2000.

[21] O. Gorodetsky, *A polynomial analogue of landau's theorem and related problems.* online preprint http://arxiv.org/abs/1603.02890.

[22] A. Grothendieck, *Cohomologie l-adique et fonctions L (1965-1966)*, Spinger Lecture Notes 1977.

[23] A. Grothendieck, *Formule de lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, (1965), pp. 41–55.

[24] A. Grothendieck, M. Artin, and J.-L. Verdier, *Théory des topos et cohomologie étale des schémas (1963-1964)*, Springer Lecture Notes 1972-1973.

[25] J. Hadamard, *Sur la distrubution des zeros de la function* $\zeta(s)$ *et ses consequences arithméthiques*, Bull. Soc. Math. Frances, 24 (1896), pp. 199–220.

[26] A. Henderson, *Bases for certain cohomology representations of the symmetric group*, J. Algebraic Combin., 24 (2006), pp. 361–390.

[27] A. Ivíc, *The Riemann zeta-function:theory and applications*, Dover Publications, 2003.

[28] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer.Soc.Colloq. Publ. 53, American Mathematical Society, Providence, 2004.

[29] J. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick, *Sums of divisors functions in $\mathbb{F}_q[t]$ and matrix integrals*, https://arxiv.org/abs/1504.07804.

[30] J. Keating and Z. Rudnick, *The variance of prime polynomials in short intervals and in residue classes*, Int Math Res Notices, (2014), pp. 259–288.

[31] ——, *Squarefree polynomials and mobius values in short intervals and arithmetic progressions*, Algebra& Number Theory, 10 (2016), pp. 375–420.

[32] M. Kim, *Weights in cohomology groups arising from hyperplane arrangements*, Proc. Amer. Math. Soc., 120 (1994), pp. 697–703.

[33] I. Lehrer, *The l-adic cohomology of hyperplane complements*, Bull. London Math.Soc., 24 (1992), pp. 76–82.

[34] J. Milne, *Etale cohomology lecture notes.* http://www.jmilne.org/math/CourseNotes/LEC.pdf.

[35] ——, *Etale cohomology*, Princeton University Press, 1980.

[36] W. Narkiewicz, *Number Theory*, World Scientific Publishing Co., Singapore, 1983.

[37] C. Poussin, *Recherce analytiques la théorie des nombres premiers*, Ann. Soc. scient. Bruxelles, 20 (1896), pp. 183–256.

[38] G. Riemann, *Über die Anzahl der Primazahlen unter einer gegebenen Gröse*, Monatsber.Knigl.Preuss.Akad.Wiss.Berlin, (1859), pp. 671–680.

[39] R. J. Rolland and J. C. Wilson, *Stability for hyperplane complements of type B/C and statistics on squarefree polynomials over finite fields.*

[40] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.

[41] Z. Rudnick, *Some problems in analytic number theory for polynomials over a finite field*, Proceedings of ICM, vol 2 (2014), pp. 443–460.

[42] P. R. Stanley, *Enumerative Combinatorics*, Cambridge University Press, 1986.

[43] A. Weil, *Number of solutions of equations in finite fields*, Bull. AMS, 55 (1949), pp. 497–508.

[44] J. Wilson, *FI_W-modules and stability criteria for representations of classical Weyl groups*, Journal of Algebra, 420 (2014), pp. 269–332.

[45] L. L. Yudell, *The special functions and their approximations*, vol. 1, Academic Press, 1969.