Some topics in the analytic number theory of polynomials over a finite field

Sam Porritt

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Mathematics

I, Sam Porritt, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.

Abstract

There are striking similarities between the ring of integers and the ring of polynomials in one variable over a finite field. This thesis explores some of these similarities from an analytic number theoretic perspective.

It develops a polynomial analogue of techniques for extracting number theoretic information from analytic functions known as the Selberg–Delange method. A motivating problem for the original development of this theory was the problem of counting integers with a prescribed number of prime factors. After presenting the theory in the context of counting polynomials with a prescribed number of prime factors in arithmetic progressions and short intervals, a refined version of the method is presented to study some related quantities in more detail. This work has applications to the study of so-called prime number races questions for polynomials with a prescribed number of prime factors.

As a prelude to this work on the Selberg–Delange method, an application from the integer version is given. It concerns the distribution of the values of $\omega(n)$, the number of prime divisors of n, in different residue classes.

We also prove some results concerning the existence and number of prime polynomials whose coefficients satisfy certain conditions. These can be compared with results about the existence and number of prime numbers whose digits satisfy certain conditions. In particular, we study prime polynomials whose coefficients are restricted to a given subset of the underlying finite field and those whose coefficients satisfy a given linear equation. These results make use of additive characters and as prelude to them, a result concerning the correlation of the polynomial analogue of the exponential function with the multiplicative Möbius function is presented.

Impact Statement

Analytic number theory is characterised by its use of tools from analysis to answer questions about, and study the properties of, integers. Despite significant effort, many such questions have remained open for a long time. A notable example is the Riemann hypothesis, a solution to which would surely produce enormous new insights into, amongst other things, the distribution of the prime numbers.

It has been known for a long time that polynomials in one variable over a finite field share many salient features with integers. However, many of the polynomial analogues of open problems about integers have been solved. Certain counterparts to the Riemann hypothesis are a good example of this. The research presented in this thesis contributes to our understanding of this analogy by developing tools from analytic number theory and proving new results about polynomials.

There is a general technique for extracting formulae from analytic functions that arise in number theory known as the Selberg–Delange method. As well as proving some polynomial counterparts to known results about integers, we shall introduce a refined version of this method to exhibit new phenomena concerning sums of Dirichlet characters over polynomials with a prescribed number of prime factors. We leave as future work the problem of investigating whether this phenomena holds for integers too.

Acknowledgements

I would like to thank my supervisor, Andrew Granville, for his infectious enthusiasm and encouragement over the last few years. I have always looked forward to our meetings and have almost always left them with renewed motivation and confidence. I would also like to thank Yiannis Petridis for always being happy to talk to me and for patiently dealing with my many requests.

The analytic number theory group in London has been an important part of my mathematical development over the last few years and I would like to thank all my fellow PhD students and postdocs for creating such a stimulating and friendly group to be a part of. I am particularly grateful to Ardavan Afshar for some engaging discussions and for generously allowing me to include some joint work of ours in this thesis.

I owe many thanks to the London School of Geometry and Number Theory, the UCL Mathematics Department, and all the students and staff there for providing, and welcoming me into, such a supportive working environment. Sitting next to Emily Maw all this time has been a pleasure. I have particularly enjoyed being part of the Chalkdust magazine committee and the opportunities it has given me and would like to thank the whole team for this, especially Niki Kalaydzhieva for encouraging me to get involved.

My time at UCL and the LSGNT has been sponsored by a doctoral studentship provided by the Heilbronn Institute for Mathematical Research. I am very grateful for this and would like to thank all the people I met at the Institute for making my time spent there so enjoyable.

Finally, I would like to thank my parents, whose strong support of my education made it all possible, and Izzy, for everything else.

Contents

List of Figures

Chapter 1

Introduction

> One of the most fruitful analogues in mathematics is that between the integers and polynomials over a finite field.
>
> Serge Lang

We start by exploring some structural similarities of integers, permutations and polynomials over a finite field. Some of the key concepts, methods and questions addressed in chapters 2, 3 and 4 of this thesis are introduced with the aid of an extended example. We then go on in this introductory chapter to summarise the structure and content of the rest of the thesis.

1.1 Anatomy and counting primes

The *anatomy of integers* refers to the internal arithmetic structure, and in particular multiplicative structure, of integers. For example, the following is a question about the anatomy of integers.

Question. If n is a typical large integer, and d is chosen uniformly at random from the divisors of n, how large should we expect d to be relative to n?

We shall return to this question shortly. It should be no surprise that prime numbers play a fundamental role in the subject. In fact the Prime Number Theorem is perhaps the most important theorem in this area of analytic number theory. It says that

$$\pi(x) \sim \int_2^x \frac{ds}{\log s} \quad \text{as } x \to \infty \tag{1.1}$$

and makes precise an observation of Gauss that roughly one in every $\log s$ numbers of size

s is prime.

Just as positive integers factor uniquely into primes, monic polynomials in $\mathbb{F}_q[t]$ factor uniquely into monic prime polynomials. Multiplication of integers by ± 1 and multiplication of polynomials by non-zero elements of $\mathbb{F}_q[t]$ do not affect multiplicative structure, so the analogue of a positive integer is a monic polynomial. Let $\mathcal{M}$ and $\mathcal{P}$ denote the set of monic polynomials and monic prime polynomials respectively. Let $\mathcal{M}_n$ and $\mathcal{P}_n$ denote the subsets of degree n. The analogue of Gauss's observation, which is in fact also due to Gauss in the case that q is prime, is that roughly 1 in every n polynomials in $\mathcal{M}_n$ is prime. More precisely,

$$\mathcal{P}_n \sim \frac{|\mathcal{M}_n|}{n} \quad \text{as } q^n \to \infty. \tag{1.2}$$

In a similar fashion, permutations on the set $[n] = \{1, 2, \ldots, n\}$, the set of which we denote S_n, 'factor' uniquely into disjoint cycles. If we let C_n denote the set of n-cycles in S_n, then the analogue of the prime number theorem in this case is particularly nice

$$C_n = \frac{|S_n|}{n} \quad \text{for } n \geq 1. \tag{1.3}$$

1.1.1 Two limits

To ask the analogous question from the previous section about polynomials, we need to interpret what it means for a polynomial to be "large". A good notion of the *size* or *norm* of a polynomial $f \in \mathbb{F}_q[t]$ turns out to be $q^{\deg f}$. So f is large if either q or $\deg f$ (or both) is large. It is interesting therefore to consider asymptotic results in the two separate cases $q \to \infty$ and $n = \deg f \to \infty$.

In the limit $q \to \infty$, there is a very close connection between the anatomy of polynomials in $\mathcal{M}_n$ and the anatomy of permutations in S_n. In fact, for $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n$ with $\sum_j j\lambda_j = n$, let us say that a permutation $\sigma \in S_n$ has *factor type* λ if σ has λ_j cycles of length j for each $1 \leq j \leq n$. Similarly, let us say that a polynomial in $\mathcal{M}_n$ has a factor type λ if it has λ_j prime factors of degree j. Then Lemma 2.1 from [3] implies that for any given λ, the proportion of polynomials in $\mathcal{M}_n$ with factor type λ is equal to the proportion of permutations in S_n with factor type λ plus a constant of size at most $O(1/q)$.

However, for the rest of this introduction and most of the thesis we shall be mainly interested in the large n limit.

1.1.2 Zeta functions

The following proof of a quantitative form of (1.2) provides a nice opportunity to introduce the *zeta function* of $\mathbb{F}_q[t]$. For $\Re s > 1$ it is defined to be

$$Z(s) := \sum_{f \in \mathcal{M}} q^{-s \deg f}.$$

A convenient change of variables we will often use is $u = q^{-s}$. Since $|\mathcal{M}_n| = q^n$, we have

$$\zeta_q(u) := Z(s) = \sum_{n \geq 0} q^n u^n = \frac{1}{1 - qu} \quad \text{for } |u| < 1/q.$$

If we now let $\pi(k) = |\mathcal{P}_k|$ then unique factorisation implies the Euler product formula

$$\frac{1}{1 - qu} = \prod_{k \geq 1} (1 - u^k)^{-\pi(k)}.$$

The left hand side clearly has a simple pole at $u = 1/q$. This is not so clear just from looking at the right hand side without knowing the $\pi(k)$, but can be used to deduce an approximate rate of growth for $\pi(k)$. In fact the left hand side is simple enough that it is easy to deduce an exact formula for $\pi(k)$. One way to do this is to first take the logarithm converting the product into an easier to manage sum. Then taking the derivative converting the resulting logarithmic singularity into an easier to manage simple pole. The result is

$$\frac{qu}{1 - qu} = \sum_{k \geq 1} \frac{k\pi(k) u^k}{1 - u^k} = \sum_{k,d \geq 1} k\pi(k) u^{kd}.$$

We can then extract an expression with $\pi(k)$ using Cauchy's integral formula

$$\frac{1}{2\pi i} \oint \frac{qu}{1 - qu} \frac{du}{u^{n+1}} = \sum_{k | n} k\pi(k).$$

Shifting the contour to $|u| = R$ and letting R tend to infinity the left hand side is equal to the residue at $u = 1/q$ by the residue theorem. Therefore

$$q^n = \sum_{k | n} k\pi(k)$$

and by Möbius inversion using the Möbius μ function

$$\pi(n) = \frac{1}{n}\sum_{k|n}\mu(k)q^{n/k}.$$

This formula was known already to Gauss in the case that q is prime. Of course, the use of Cauchy's integral formula and the residue theorem to extract the coefficient of u^n was not necessary, but it illustrates the general approach which works well in more complicated situations when simply reading off the coefficient is not possible. We will see this several times again in different contexts and usually have to work harder to evaluate the resulting integral.

A broadly similar strategy for counting primes in $\mathbb{Z}$ was first put forward by Riemann using the Riemann zeta function defined for $\Re s > 1$ as

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_{p}(1-p^{-s})^{-1}.$$

There are a number of difficulties which make it significantly harder to actually carry out than the proof just given for $\mathbb{F}_q[t]$. As with $Z(s)$, one can show that $\zeta(s)$ has a simple pole at $s = 1$. This immediately implies that there are infinitely many primes. A more detailed examination of this pole, together with the Euler product representation allows one to quantity how many primes there are up to some number x. The most common approach uses the logarithmic derivative of $\zeta(s)$

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^{\infty}\left(\sum_{p^k\leq x}\log p\right)x^{-(s+1)}dx$$

and Mellin inversion formula

$$\sum_{p^k\leq x}\log p = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}-\frac{\zeta'(s)}{s\zeta(s)}x^s ds.$$

For one thing, the Riemann zeta function is much more complicated than $\zeta_q(s)$ and certainly has no neat closed form expression. Also, the quantity $\pi(x)$ is not recovered from $\zeta(s)$ by simply comparing coefficients of the logarithmic derivative, or Cauchy's integral formula, but with this infinite integral that requires non-trivial complex analysis to evaluate asymptotically.

Having introduced the analogy between integers, polynomials and permutations and seen how zeta functions can be used to count primes, we now move on and start to explore the similarities in the internal multiplicative structures of these three classes with an extended example.

1.2 Arcsin law

Let us return to the question from the previous section.

Question. If n is a typical large integer and d is chosen uniformly from the divisors of n, how large should we expect d to be relative to n?

Of course the answer depends very strongly on the multiplicative structure of n. For instance, the number of divisors $d(n) = \sum_{d|n} 1$ varies erratically with n. A nice way to formulate this question more precisely is to average over n.

Question. Let V_n be the random variable $\log d / \log n$ where d is chosen uniformly at random from the divisors of n. For large X, what is the distribution function $\mathcal{F}_X : [0,1] \to [0,1]$

$$\mathcal{F}_X(t) = \frac{1}{X} \sum_{1 \leq n \leq X} \mathbb{P}(V_n \leq t) \ ?$$

This question is addressed by Deshouillers, Dress and Tenenbaum in [10]. The proofs in this opening chapter are inspired by the argument from that paper as presented in [38]. We have seen that counting primes in $\mathbb{F}_q[t]$ is much easier than in $\mathbb{Z}$ and that counting cycles of length n is even easier. It is also the case that this question is easier to answer for polynomials and easier still for permutations.

1.2.1 Permutations

In the analogy between integers and permutations, prime divisors of an integer correspond to cycles of a permutation and divisors of an integer correspond to fixed sets of a permutation. We shall write $C \in \sigma$ to mean C is a cycle of σ and $A|\sigma$ to mean A is a fixed set of σ. Let $\mathrm{cyc}(\sigma)$ be the number of cycles of σ. It is easy to see that for a permutation σ on $[n]$ we have

$$2^{\mathrm{cyc}(\sigma)} = \sum_{A \subset [n] \,:\, A|\sigma} 1.$$

For such a permutation σ, let D_σ be the random variable l/n where l is the size of a fixed set of σ chosen uniformly at random so that

$$\mathbb{P}(D_\sigma \leq t) = \frac{1}{2^{\mathrm{cyc}(\sigma)}} \sum_{\substack{|A| \leq tn \\ A|\sigma}} 1.$$

Proposition 1.1. *Uniformly for $n \geq 1$ and $0 \leq t \leq 1$, we have*

$$\frac{1}{n!} \sum_{\sigma \in S_n} \mathbb{P}(D_\sigma \leq t) = \frac{2}{\pi} \arcsin \sqrt{t} + O\left(\frac{1}{\sqrt{n}}\right).$$

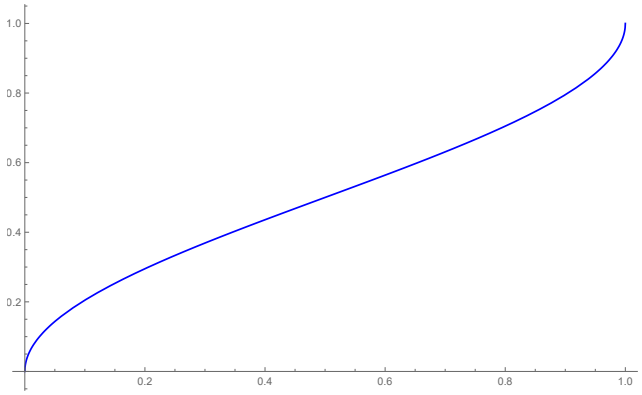


Figure 1.1: $\frac{2}{\pi} \arcsin(\sqrt{t})$

Proof. We start by proving[1] the following polynomial identity

$$F_n(z) := \sum_{\sigma \in S_n} z^{\mathrm{cyc}(\sigma)} = \sum_{k=0}^{n} z^k \pi(n,k) = z(z+1)\cdots(z+n-1). \tag{1.4}$$

where $\pi(n,k) = \#\{\sigma \in S_n \ : \ \mathrm{cyc}(\sigma) = k\}$. Note that for each $1 \leq i \leq n$, the function $\phi_i : \{\sigma \in S_n \mid \sigma(n) = i\} \to S_{n-1}$ defined by

$$\phi_i(\sigma)(j) = \begin{cases} \sigma(j) & \text{if } \sigma(j) \neq n \\ i & \text{if } \sigma(j) = n \end{cases}$$

is a bijection and satisfies $\mathrm{cyc}(\phi_i(\sigma)) = \mathrm{cyc}(\sigma) - \mathbf{1}_{i=n}$ because the effect of ϕ_i is just to

[1] We thank Ardavan Afshar for this simple proof of (1.4).

remove n from the cycle in which it appears. Therefore $F_n(z)$ is equal to

$$\sum_{i=1}^{n} \sum_{\substack{\sigma \in S_n \\ \sigma(n)=i}} z^{\mathrm{cyc}(\sigma)} = \sum_{\sigma \in S_{n-1}} z^{\mathrm{cyc}(\sigma)+1} + \sum_{i=1}^{n-1} \sum_{\sigma \in S_{n-1}} z^{\mathrm{cyc}(\sigma)} = (z+n-1)F_{n-1}(z)$$

so (1.4) follows by induction and the fact that $F_1(z) = z$.

After setting $z = 1/2$ we deduce that

$$\sum_{k=0}^{n} \frac{1}{2^k} \pi(n,k) = n! \binom{-1/2}{n} (-1)^n.$$

Now,

$$\frac{1}{n!} \sum_{\sigma \in S_n} \mathbb{P}(D_\sigma \le t) = \frac{1}{n!} \sum_{\sigma \in S_n} \frac{1}{2^{\mathrm{cyc}(\sigma)}} \sum_{\substack{|A| \le tn \\ A|\sigma}} 1 = \frac{1}{n!} \sum_{\substack{A \subset [n] \\ |A| \le tn}} \sum_{\substack{\sigma \in S_n \\ A|\sigma}} \frac{1}{2^{\mathrm{cyc}(\sigma)}}.$$

To evaluate the inner sum, we split the sum according to the number of cycles of $\sigma|_A$, that is, σ restricted to A, and $\sigma|_{[n]\setminus A}$. Thus, the inner sum is

$$\sum_{i=1}^{|A|} \sum_{j=1}^{n-|A|} \frac{1}{2^{i+j}} \pi(|A|,i)\pi(n-|A|,j) = |A|!(n-|A|)! \binom{-1/2}{|A|} \binom{-1/2}{n-|A|} (-1)^n.$$

With $k = |A|$ we therefore have

$$\frac{1}{n!} \sum_{\sigma \in S_n} \mathbb{P}(D_\sigma \le t) = \sum_{k \le tn} \frac{1}{4^k} \binom{2k}{k} \frac{1}{4^{n-k}} \binom{2(n-k)}{n-k}.$$

It follows from Stirling's formula that $4^{-n}\binom{2n}{n} = 1/\sqrt{n\pi}(1 + O(1/n))$. By symmetry, we may assume that $t \le 1/2$. Then using this approximation and approximating the sum with an integral we get

$$\begin{aligned} \frac{1}{\pi} \sum_{1 \le k \le tn} \frac{1}{\sqrt{k(n-k)}} (1 + O(1/k)) &= \frac{1}{\pi} \int_1^{tn} \frac{1}{\sqrt{s(n-s)}} ds + O(1/\sqrt{n}) \\ &= \frac{2}{\pi} \arcsin \sqrt{t} + O(1/\sqrt{n}) \end{aligned}$$

which proves Proposition 1.1 □

Although we didn't really need it, the reader is invited to acknowledge that it follows

from the binomial theorem and (1.4) that

$$\left(\frac{1}{1-u}\right)^z = \sum_{n=0}^{\infty}(-u)^n\binom{-z}{n} = \sum_{n=0}^{\infty}\frac{u^n}{n!}\sum_{k=0}^{n}\pi(n,k)z^k.$$

The same series, again with $z = 1/2$, appears in the proof for polynomials, albeit in a form decorated with certain arithmetic adjustments.

1.2.2 Polynomials

Turning to polynomials, now let D_f be the random variable $\deg d/\deg f$ as d varies uniformly over the divisors of a polynomial $f \in \mathcal{M}_n$ so that

$$\mathbb{P}(D_f \le t) = \frac{1}{\tau(f)}\sum_{\substack{d|f\\ \deg d \le t\deg f}} 1$$

where $\tau(f)$ is the number of monic divisors of f. We shall now prove the following strikingly similar analogue of Proposition 1.1.

Proposition 1.2. *Uniformly for $n \ge 1$ and $0 \le t \le 1$, we have*

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\mathbb{P}(D_f \le t) = \frac{2}{\pi}\arcsin\sqrt{t} + O\left(\frac{1}{\sqrt{n}}\right).$$

Let g be the multiplicative function[2] defined on prime powers by

$$g(p^k) = \left(\sum_{j\ge 0}\frac{q^{-j\deg p}}{1+j+k}\right)\left(\sum_{j\ge 0}\frac{q^{-j\deg p}}{1+j}\right)^{-1}. \tag{1.5}$$

and let $A_q = \prod_{p\in\mathcal{P}}\left(-\log(1-q^{-\deg p})(q^{2\deg p}-q^{\deg p})^{1/2}\right)$. These are the arithmetic decorations. We require two lemmas. The reader is again invited to acknowledge the role played by the series $(1-qu)^{-1/2}$ in the proofs of these lemmas, and in particular that, although these decorations present further technicalities that need to be overcome, the underlying approach is similar to that of the proof of Proposition 1.1.

[2]To say that a function g is multiplicative means that $g(xy) = g(x)g(y)$ for any pair x, y that are coprime.

Lemma 1.1. *Uniformly for $n \geq 1$ and $d \in \mathbb{F}_q[t]$, we have*

$$\sum_{f \in \mathcal{M}_n} \frac{1}{\tau(df)} = \frac{A_q q^n}{\sqrt{\pi n}} \left(g(d) + O(1/n)\right).$$

Lemma 1.2. *Uniformly for $n \geq 1$,*

$$\sum_{f \in \mathcal{M}_n} g(f) = \frac{q^n}{A_q \sqrt{\pi n}} \left(1 + O(1/n)\right).$$

Proof of Proposition 1.2. By symmetry we may suppose that $t \leq 1/2$. Therefore, using Lemmas 1.1 and 1.2 in the 3^{rd} and 4^{th} lines below respectively we have

$$\begin{aligned}
\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \mathbb{P}(D_f \leq t) &= \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \frac{1}{\tau(f)} \sum_{\substack{d \mid f \\ \deg d \leq t \deg f}} 1 \\
&= \frac{1}{q^n} \sum_{\substack{1 \leq k \leq tn \\ d \in \mathcal{M}_k}} \sum_{h \in \mathcal{M}_{n-k}} \frac{1}{\tau(hd)} \\
&= \sum_{1 \leq k \leq tn} \frac{A_q}{\sqrt{\pi(n-k)}} \frac{1}{q^k} \sum_{d \in \mathcal{M}_k} \left(g(d) + O(1/(n-k))\right) \\
&= \frac{1}{\pi} \sum_{1 \leq k \leq tn} \frac{1}{\sqrt{k(n-k)}} \left(1 + O(1/k)\right) \\
&= \frac{1}{\pi} \int_1^{tn} \frac{1}{\sqrt{s(n-s)}} ds + O(1/\sqrt{n}) = \frac{2}{\pi} \arcsin \sqrt{t} + O(1/\sqrt{n}). \quad \square
\end{aligned}$$

To prove Lemmas 1.1 and 1.2 we will define suitable generating series and apply Cauchy's integral formula to extract the coefficients. Due to what we have called the 'arithmetic decorations', we will require the following additional lemma.

Lemma 1.3. *Suppose $F(u)$ is holomorphic for $|u| \leq q^{-3/4}$ and is such that $F(u) = F(1/q) + O(M(1-qu))$ for some constant M uniformly in the range $|u| \leq q^{-3/4}$. Then*

$$\frac{1}{2\pi i} \int_{|u|=1/q^2} \frac{F(u)}{\sqrt{1-qu}} \frac{du}{u^{n+1}} = \frac{q^n}{\sqrt{n\pi}} \left(F(1/q) + O(M/n)\right).$$

Proof. First change to the variable $w = qu$ so that the integral becomes

$$\frac{q^n}{2\pi i} \int_{|w|=1/q} \frac{F(w/q)}{\sqrt{1-w}} \frac{dw}{w^{n+1}}.$$

Now shift to the contour which consists of the vertical segment $[1 - 1/n - iq^{1/4}, 1 - 1/n +$

$iq^{1/4}$] and the part of the circle centred at the origin which meets the endpoints of this segment so that the only pole of the integrand is at $w = 0$ still.

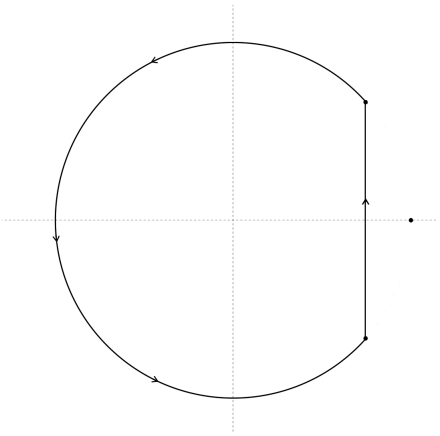


Figure 1.2: Contour of integration

Now we use $F(w/q) = F(1/q) + O(M(1-w))$, and pick up a residue from $w = 0$ equal to

$$(-1)^n \binom{-1/2}{n} = \frac{1}{4^n}\binom{2n}{n} = \frac{1}{\sqrt{n\pi}} + O(n^{-3/2}).$$

It remains to bound the integral of the $O(M(1-w))$ part. On the circular section it is bounded by $\ll nq^{3n/4}$, which is acceptable for the error term of the statement. On the vertical segment, it is bounded by

$$\ll M\int_{-\infty}^{\infty} \frac{|1/n - it|^{1/2}}{|1 - 1/n + it|^n} dt \ll Mn^{-3/2}\int_{-\infty}^{\infty} \frac{|1-it|^{1/2}}{|1-(1-it)/n|^n} dt \ll Mn^{-3/2}. \quad \square$$

Proof of Lemma 1.1. For $d \in \mathcal{M}$, define

$$F_d(u) = \sum_{f\in\mathcal{M}} \frac{u^{\deg f}}{\tau(df)} = \prod_{p\in\mathcal{P}} \left(\sum_{j\geq 0} \frac{u^{j\deg p}}{1 + j + \nu_p(d)} \right)$$

where $\nu_p(d)$ is the highest power of p which divides d. Then

$$\sum_{f\in\mathcal{M}_n} \frac{1}{\tau(df)} = \frac{1}{2\pi i}\int_{|u|=r} \frac{F_d(u)}{u^{n+1}} du.$$

We have

$$F_d(u) = G_d(u)F_1(u)$$

where

$$G_d(u) = \prod_{p|d} \left(\sum_{j\geq 0} \frac{u^{j \deg p}}{1 + j + \nu_p(d)} \right) \left(\sum_{j\geq 0} \frac{u^{j \deg p}}{1+j} \right)^{-1}.$$

Since

$$\frac{1}{1-qu} = \sum_f u^{\deg f} = \prod_{p\in\mathcal{P}} (1 - u^{\deg p})^{-1} \tag{1.6}$$

we have that

$$\begin{aligned} \widetilde{F}(u) &:= (1-qu)^{1/2} F_1(u) \\ &= \prod_{p\in\mathcal{P}} \left(\sum_{j\geq 0} \frac{u^{j\deg p}}{1+j} \right) (1 - u^{\deg p})^{1/2} \\ &= \prod_{p\in\mathcal{P}} \left(-\frac{\log(1-u^{\deg p})}{u^{\deg p}} (1-u^{\deg p})^{1/2} \right). \end{aligned}$$

Notice that $G_d(1/q) = g(d)$ where g is the multiplicative function defined by (1.5) and $\widetilde{F}(1/q) = A_q$. Now simply check that

$$G_d(u) = g(d) + O(1-qu)$$

and

$$\widetilde{F}(u) = A_q + O(1-qu)$$

and use the integral lemma, Lemma 1.3. □

Proof of Lemma 1.2. Define

$$\mathcal{G}(u) = \sum_{f\in\mathcal{M}} g(f) u^{\deg f}.$$

Then

$$\mathcal{G}(u) = (1-qu)^{-1/2} \widetilde{\mathcal{G}}(u)$$

where

$$\widetilde{\mathcal{G}}(u) = \prod_{p\in\mathcal{P}} \left((1-u^{\deg p})^{1/2} \sum_{k\geq 0} u^{k\deg p} \left(\sum_{j\geq 0} \frac{q^{-j\deg p}}{1+j+k} \right) \left(\sum_{j\geq 0} \frac{q^{-j\deg p}}{1+j} \right)^{-1} \right).$$

Notice that $\widetilde{\mathcal{G}}(1/q) = 1/A_q$. Now simply check that

$$\widetilde{\mathcal{G}}(u) = 1/A_q + O(1 - qu)$$

and

$$\sum_{f \in \mathcal{M}_n} g(f) = \frac{1}{2\pi i} \int (1 - qu)^{-1/2} \widetilde{\mathcal{G}}(u) \frac{du}{u^{n+1}}.$$

and use the integral lemma, Lemma 1.3. □

1.2.3 Integers

The corresponding statement for integers was proved by Deshouillers, Dress and Tenenbaum in [10].

Proposition 1.3. *Uniformly for $X \geq 2$ and $0 \leq t \leq 1$, we have*

$$\frac{1}{X} \sum_{1 \leq n \leq X} \mathbb{P}(V_n \leq t) = \frac{2}{\pi} \arcsin \sqrt{t} + O(1/\sqrt{\log X}).$$

Their proof follows broadly the same strategy as the one presented above for polynomials. Indeed, the proof presented above was modelled on their argument as presented in [38, II.6]. As with the proof of the prime number theorem, there are a number of differences which make the problem technically harder for integers than for polynomials. But, as with the proof of the prime number theorem, the strategy is broadly similar. In particular, Cauchy's integral formula is replaced with Perron's formula and the zeta function $\zeta_q(u)$ is replaced by the Riemann zeta function $\zeta(s)$. A key feature of similarity is the role played by the singularity of $(1-u)^{-1/2}$. This appeared in the proofs for both permutations and for polynomials. It also appears in the proof for integers after approximating $\zeta(s)$ by $1/(s-1)$ near the point $s = 1$.

1.3 Summary and overview of the thesis

We have seen how the anatomies of integers and polynomials show a close resemblance. We have also seen, with the aid of an extended example, that this can perhaps be explained in terms of the similarities of certain analytic functions – and in particular, the singularities of those analytic functions. There is a very general method for extracting information from the singularities of analytic functions in number theory known as the Selberg–Delange method.

Chapter 2 consists of a specific application of a formula from the paper in which Selberg first develops this method. It concerns the distribution of $\omega(n)$, the number of distinct prime divisors of n, in different residue classes. For integers $0 \leq a < q$, we shall consider quantities such as

$$\#\{n \leq x \,:\, \omega(n) \equiv a \mod q\} - \frac{x}{q}. \tag{1.7}$$

and answer prime number races style questions about the set of x for which they are positive or negative. It turns out that the natural way of measuring such sets is with loglog density rather than logarithmic density which is the appropriate notion of density to use for the regular prime number races. One of our results is that for $q > 2$, the set of x for which (1.7) is positive has loglog density $1/2$, but no natural or logarithmic density.

In chapter 3 we continue our exploration of the anatomy of polynomials by proving some results about polynomials with a given number of prime factors using a polynomial analogue of the Selberg–Delange method. This requires studying the sums of Dirichlet characters over polynomials with a fixed number of divisors. Our results here include formulae for the number of polynomials of a prescribed degree and prescribed number of prime factors in arithmetic progressions and "short intervals". The results are stronger than the corresponding results known for integers, primarily because the Riemann hypothesis is known to hold for the Dirichlet L-functions we make use of.

In chapter 4 we develop a refined version of the arguments from chapter 3 to study in more detail sums of Dirichlet characters over polynomials with a prescribed number of prime factors. We shall give a fuller account of the method and applications in chapter 4 but let us briefly explain here the main innovation.

Let $\chi : \mathbb{F}_q[t] \to \mathbb{C}$ be a non-trivial Dirichlet character and $\Omega(f)$ denote the number of prime factors of f counted with multiplicity. When applying the Selberg–Delange theory to study the quantity

$$\sum_{\substack{f \in \mathcal{M}_n \\ \Omega(f)=k}} \chi(f) \tag{1.8}$$

is it natural to do so via the auxiliary quantity

$$\sum_{f \in \mathcal{M}_n} z^{\Omega(f)} \chi(f)$$

where z is a complex variable and then apply Cauchy's integral formula in the way we have seen already. Now $z^{\Omega(f)}\chi(f)$ is a multiplicative function whose Dirichlet series has Euler product

$$G_z(u,\chi) := \sum_{f\in\mathcal{M}} z^{\Omega(f)}\chi(f)u^{\deg f} = \prod_{p\in\mathcal{P}} \left(1-\chi(p)zu^{\deg p}\right)^{-1}$$

which converges absolutely in the range $|u| < \min\{|z|^{-1}, q^{-1}\}$. As has been hinted at already in the proof of Proposition 1.2, it is desirable to extend this range of convergence so that we may expand the contour in our use of Cauchy's integral formula. A direct application of the Selberg–Delange method is to achieve this by writing

$$G_z(u,\chi) = L(u,\chi)^z E_z(u,\chi)$$

where $L(u,\chi)$ is the L-function associated to χ and $E_z(u,\chi)$ is an Euler product that now converges absolutely in the range $|u| < \min\{|z|^{-1}, q^{-1/2}\}$. The main novelty in the work of chapter 4 derives from the use of the three-way product

$$G_z(u,\chi) = L(u,\chi)^z L(u^2,\chi^2)^{\frac{z(z-1)}{2}} E_z(u,\chi)$$

where $E_z(u,\chi)$ is an Euler product that converges absolutely for $|u| < \min\{|z|^{-1}, q^{-1/3}\}$. Crucially, this allows us to expand the contour to incorporate the zeros of $L(u,\chi)$ which, by the Riemann hypothesis for such L-functions, lie on the circle $|u| = q^{-1/2}$, and thus deduce an asymptotic formula for (1.8) in terms of those zeros.

In chapter 5 we recall the definition of a function field analogue of the exponential function, given by Hayes [17], and present a short proof that it does not correlate with the Möbius function in a specific quantitative sense. The main result is the function field analogue of a result of Baker and Harman [4] which states that, under the generalized Riemann hypothesis, for all x and $\epsilon > 0$

$$\max_{\theta\in[0,1)} \left|\sum_{n\leq x} \mu(n)e^{2\pi in\theta}\right| \ll_\epsilon x^{\frac{3}{4}+\epsilon}$$

where μ is the integer Möbius function.

Having introduced the exponential function in chapter 5, we use it in chapter 6 as we

continue to explore the similarities of integers and polynomials by proving some results about prime polynomials whose coefficients satisfy certain restrictions. The first result is a formula for the number of polynomials in $\mathcal{P}_n$, all of whose coefficients lie is a given subset of $\mathbb{F}_q$. We also prove a formula for the number of polynomials in $\mathcal{P}_n$ whose coefficients satisfy a given linear condition. These results are analogous to results about integers whose digits satisfy certain restrictions.

To keep each chapter fairly self-contained, each starts with further context and background specific to the content of that chapter.

Chapter 2

Residue races for the prime divisor function

This chapter is based primarily on [29].

In this chapter we investigate the distribution of the function $\omega(n)$, the number of distinct prime divisors of n, in residue classes modulo q for natural numbers q greater than 2. In particular we ask 'prime number races' style questions, as suggested by Coons and Dahmen in their paper 'On the residue class distribution of the number of prime divisors of an integer' [7].

2.1 Introduction

Let $q \geq 2$ be an integer, $a \in \{0, 1, \ldots, q-1\}$ represent some residue class modulo q and $\omega(n)$ denote the number of distinct prime divisors of n. Define

$$N_{a,q}(x) := \#\{n \leq x : \omega(n) \equiv a \mod q\}.$$

Seeing no reason why $\omega(n)$ should favour any particular residue class, we expect that

$$N_{a,q}(x) \sim \frac{x}{q} \quad \text{as} \quad x \to \infty \quad \text{for each } a. \tag{2.1}$$

In fact, it was proved in [1] that

$$N_{a,q}(x) - \frac{x}{q} = O\left(\frac{x}{(\log x)^{c(q)}}\right)$$

with $c(q) = 1 - \cos(\frac{2\pi}{q})$. It was also proved that for $q > 2$ the error term here is best possible, since it was also determined that for $q > 2$

$$N_{a,q}(x) - \frac{x}{q} = \Omega_{\pm}\left(\frac{x}{(\log x)^{c(q)}}\right).$$

This is in stark contrast to the case $q = 2$ for which we expect "square-root cancellation". Indeed,

$$N_{a,2}(x) - \frac{x}{2} = O(x^{1/2+o(1)}) \quad \text{for } a = 0 \text{ and } 1$$

is equivalent to the Riemann Hypothesis. For $q = 2$, it is well known that (2.1) is equivalent to the prime number theorem. See [24, Section 8.1] for details of this equivalence.

In [7], the authors suggest that, in the spirit of prime number races, it would be interesting to investigate the sign changes of $N_{a,q}(x) - N_{b,q}(x)$. The traditional prime number races concern the popularity of residue classes for prime numbers rather than for the values of ω, that is, sign changes of $\pi(x;a,q) - \pi(x;b,q)$ where $\pi(x;a,q)$ is the number of primes less than or equal to x which are congruent to a modulo q. Rubinstein and Sarnak [34] proved under certain reasonable assumptions[1] that the set

$$\{x \in \mathbb{N} \,:\, \pi(x;3,4) < \pi(x;1,4)\},$$

for example, does not have a natural density in the integers but does have a *logarithmic density*, defined for a subset $E \subset \mathbb{N}$, if the limit exists, to be $\lim_{X\to\infty} \frac{1}{\log X} \sum_{\substack{x\le X \\ x\in E}} \frac{1}{x}$. Loosely speaking, the reason for this is that the difference $\pi(x;3,4) - \pi(x;1,4)$ can be written as a sum of terms of the form $\sin(\gamma \log x)/\gamma$, where γ ranges over the imaginary parts of the zeros of certain Dirichlet L-functions. For a more thorough introduction to this topic we recommend [14].

For our investigations it is natural to consider mean values of the multiplicative functions $n \mapsto z^{\omega(n)}$ where z is taken to be a complex q-th root of unity. By applying a classical result first due to Selberg concerning such mean values we will establish an asymptotic formula for $N_{a,q}(x)$ with main term and next highest order term in the case $q > 2$. This will be used to prove our main theorem. The formula will contain an expression of the form $\cos(A \log\log x + B)$ and so in our case we have neither natural nor logarithmic density,

[1] Specifically, the generalised Riemann hypothesis for Dirichlet L-functions and linear independence of the set of imaginary parts of non-trivial zeros.

but instead need to go further and define the notion of *loglog density*. We say a subset $E \subset \mathbb{N}$ has *loglog density* δ if

$$\frac{1}{\log\log X} \sum_{\substack{x \le X \\ x \in E}} \frac{1}{x \log x} \to \delta \text{ as } X \to \infty.$$

With this we can now state the main results of this chapter.

Theorem 2.1. *Let $q > 2$ be an integer and $a, b \in \{0, 1, \dots, q-1\}$ with $a \neq b$. The set*

$$E_{a,b} := \{x \in \mathbb{N} \,:\, N_{a,q}(x) < N_{b,q}(x)\}$$

has no natural density, in fact

$$\liminf_{X\to\infty} \frac{1}{X}[1, X] \cap E_{a,b} = 0 \quad \textit{and} \quad \limsup_{X\to\infty} \frac{1}{X}[1, X] \cap E_{a,b} = 1.$$

Theorem 2.2. *The set $E_{a,b}$, defined in Theorem 2.1, has no natural or logarithmic density, but has* loglog density *equal to* $1/2$.

Given a complete ordering on the residue classes, we can also ask how often the different 'competitors' in our race are in that order.

Theorem 2.3. *Let $q > 2$ be an integer and $a \in \{0, 1, \dots, q-1\}$. Each of the following sets has* loglog density $\frac{1}{2q}$

$$U_{a,q} := \{x \in \mathbb{N} \,:\, N_{a,q}(x) > N_{a-1,q}(x) > N_{a+1,q}(x) > \cdots > N_{a-i,q}(x) > N_{a+i,q}(x) > \cdots\}$$

$$V_{a,q} := \{x \in \mathbb{N} \,:\, N_{a,q}(x) > N_{a+1,q}(x) > N_{a-1,q}(x) > \cdots > N_{a+i,q}(x) > N_{a-i,q}(x) > \cdots\}.$$

Therefore, since there are $2q$ of them, these are the only permutations which appear with non-zero loglog densities.

Example 2.1. When $q = 6$ and $a = 4$ we get

$$\lim_{X\to\infty} \frac{1}{\log\log X} \sum_{\substack{x \le X \\ N_{4,6}(x) > N_{3,6}(x) > N_{5,6}(x) > N_{2,6}(x) > N_{0,6}(x) > N_{1,6}(x)}} \frac{1}{x \log x} = \frac{1}{12}$$

$$\lim_{X\to\infty}\frac{1}{\log\log X}\sum_{\substack{x\le X\\ N_{4,6}(x)>N_{5,6}(x)>N_{3,6}(x)>N_{0,6}(x)>N_{2,6}(x)>N_{1,6}(x)}}\frac{1}{x\log x}=\frac{1}{12}.$$

Theorem 2.1 follows easily from the proofs of Proposition 2.2 and Theorem 2.3. Theorem 2.2 shall follow from Theorem 2.3 because, up to a set of zero loglog density[2], the set $E_{a,b}$ is the union of q of the $2q$ sets from Theorem 2.3.

We also prove that certain orderings can occur only a finite number of times.

Theorem 2.4. *Any permutation σ of $\{0,1,\dots,q-1\}$ for which the set*

$$\{x\in\mathbb{N}\,:\,N_{\sigma(0),q}(x)\ge N_{\sigma(1),q}(x)\ge\ldots\ge N_{\sigma(q-1),q}(x)\}$$

is infinite is such that $\sigma(0)=\sigma(1)\pm 1 \mod q$.

Notice that there are $2q!/(q-1)$ such permutations so if q is large, a vanishingly small proportion of the possible permutations occur infinitely often.

Example 2.2. If $q=4$ then only 16 out of the 24 orderings can occur for arbitrarily large x. There is a point after which, if "0 is in the lead", then 2 cannot be second and vice versa. Similarly, they cannot simultaneously hold positions 3rd and 4th, and the same goes for the pair of residue classes 1 and 3.

Let us look at the start of the mod 4 race before moving on to the proofs. For a better view, the mean has been subtracted and the points are plotted on a loglog scale.

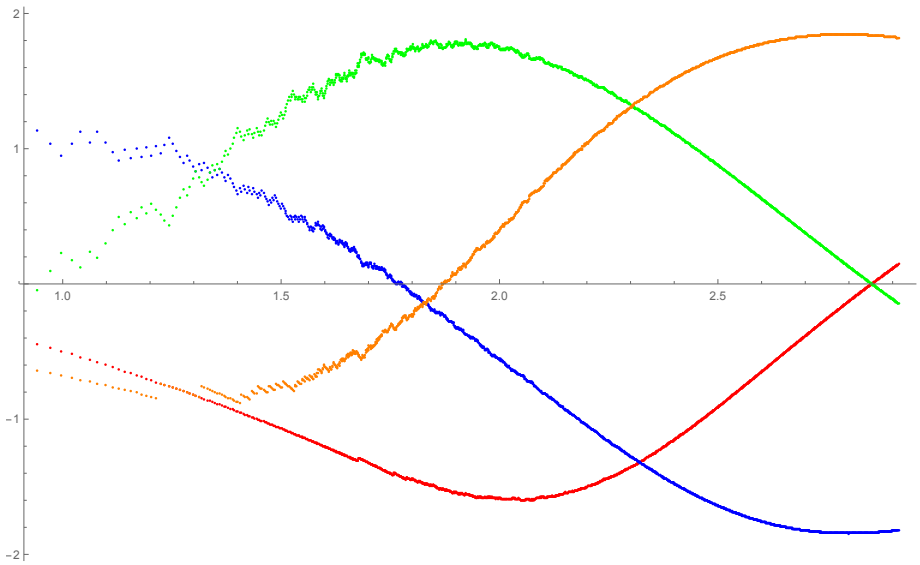


Figure 2.1: ω mod 4 race

[2]This set being $\{x\in\mathbb{N}\,:\,N_{a,q}(x)=N_{a',q}(x)$ for some $a\neq a'\}$.

The plotted points along with their colours are as follows:

$$\begin{aligned}
&\text{Orange: } \{ \big(\log\log x, (\frac{1}{x}N_{0,4}(x) - \frac{1}{4})\log x\big) \ : \ 10 \le x \le 10^8\},\\
&\text{Red: } \{ \big(\log\log x, (\frac{1}{x}N_{1,4}(x) - \frac{1}{4})\log x\big) \ : \ 10 \le x \le 10^8\},\\
&\text{Blue: } \{ \big(\log\log x, (\frac{1}{x}N_{2,4}(x) - \frac{1}{4})\log x\big) \ : \ 10 \le x \le 10^8\},\\
&\text{Green: } \{ \big(\log\log x, (\frac{1}{x}N_{3,4}(x) - \frac{1}{4})\log x\big) \ : \ 10 \le x \le 10^8\}.
\end{aligned}$$

This data strongly suggests, at least for the $q = 4$ race, that any ordering not of the form stated in Theorem 2.4 can *never* occur. It may not be unreasonable to conjecture that this is the case for all q.

We remark that similar results can be proved for the sets

$$\{n \le x \ : \ \Omega(n) \equiv a \mod q\} \text{ and } \{n, \text{ square-free } \le x \ : \ \omega(n) \equiv a \mod q\}$$

where $\Omega(n) = \sum_{p^k|n} 1$ counts prime divisors with multiplicities.

2.2 Preliminaries

To save space, we will use $\log_2 x$ and $e_2(x)$ to denote $\log\log x$ and $\exp(\exp(x))$ respectively. We start by proving an asymptotic formula for $N_{a,q}(x)$.

Proposition 2.1. *For $x \ge 3$ we have*

$$N_{a,q}(x) = \frac{x}{q}\left\{1 + 2|g(\phi)|\cos\Big(\sin\Big(\frac{2\pi}{q}\Big)\log_2 x + \theta - \frac{2\pi a}{q}\Big)(\log x)^{\cos(\frac{2\pi}{q})-1} + O\Big((\log x)^{\cos(\frac{4\pi}{q})-1}\Big)\right\}$$

where $g(z) := \frac{1}{\Gamma(z)}\prod_p \Big(1 + \frac{z}{p-1}\Big)(1-p^{-1})^z$ and $\phi = \phi(q) = e^{2\pi i/q}$ and $\theta = \arg g(\phi)$.

Proof. The main result we will make use of is [36, Theorem 2], from which it follows that for z a complex variable bounded in absolute value by 1, and $g(z)$ defined as in the proposition we have

$$A_z(x) := \sum_{n\le x} z^{\omega(n)} = g(z)x(\log x)^{z-1} + O\big(x(\log x)^{\Re z - 2}\big). \tag{2.2}$$

These mean values satisfy

$$A_{\phi^j}(x) = \sum_{n \le x} \phi^{j\omega(n)} = \sum_{k=0}^{q-1} \phi^{jk} N_{k,q}(x) \quad \text{for all } j = 0, \dots, q-1.$$

We can isolate the $N_{a,q}(x)$ as follows

$$\frac{1}{q}\sum_{j=0}^{q-1} \overline{\phi}^{aj} A_{\phi^j} = \frac{1}{q}\sum_{j=0}^{q-1} \overline{\phi}^{aj} \sum_{k=0}^{q-1} \phi^{jk} N_{k,q}(x) = \sum_{k=0}^{q-1} N_{k,q}(x) \frac{1}{q}\sum_{j=0}^{q-1} \phi^{j(k-a)} = N_{a,q}(x).$$

Substituting (2.2) into the line above gives

$$N_{a,q}(x) = \frac{x}{q}\left(1 + \sum_{j=1}^{q-1} \left(\overline{\phi}^{aj} g(\phi^j) e^{i\sin(\frac{2\pi j}{q})\log_2 x} (\log x)^{\cos(\frac{2\pi j}{q})-1} + O((\log x)^{\cos(\frac{2\pi j}{q})-2})\right)\right).$$

For sufficiently large x, the terms in this sum with largest absolute value are those with $j = 1$ and $j = q-1$. Each of the others is $\ll (\log x)^{\cos(\frac{4\pi}{q})-1}$. Combining this observation with the fact that $g(\overline{z}) = \overline{g(z)}$ we get, for $\theta = \arg g(\phi)$.

$$\begin{aligned} N_{a,q}(x) &= \frac{x}{q}\left(1 + 2\Re(\overline{\phi}^a g(\phi) e^{i\sin(\frac{2\pi}{q})\log_2 x})(\log x)^{\cos(\frac{2\pi}{q})-1} + O((\log x)^{\cos(\frac{4\pi}{q})-1})\right) \\ &= \frac{x}{q}\left(1 + 2|g(\phi)| \cos\left(\sin\left(\frac{2\pi}{q}\right)\log_2 x + \theta - \frac{2\pi a}{q}\right)(\log x)^{\cos(\frac{2\pi}{q})-1} \right. \\ &\qquad \left. + O((\log x)^{\cos(\frac{4\pi}{q})-1})\right). \qquad \square \end{aligned}$$

Notice that if $q = 2$ then $\phi = -1$ and $g(-1) = 0$. It is for this reason we cannot say any more in this most interesting case. Indeed we actually suspect a much stronger error term for $N_{a,2}(x) - \frac{x}{2}$ of $O(x^{1/2+o(1)})$, as predicted by the Riemann hypothesis. For $q > 2$ though, $g(\phi) \neq 0$, as Γ has no pole there and the product has only non-zero terms.

From this, we see immediately that

$$N_{a,q}(x) - \frac{x}{q} = O\left(\frac{x}{(\log x)^{1-\cos(\frac{2\pi}{q})}}\right)$$

and also

$$N_{a,q}(x) - \frac{x}{q} = \Omega_{\pm}\left(\frac{x}{(\log x)^{1-\cos(\frac{2\pi}{q})}}\right).$$

Before trying to understand when $N_{a,q}(x)$ is less than this average value of x/q, we

start with the simpler, but related, question of when the secondary term is negative. That is, when

$$\cos\Big(\sin\Big(\frac{2\pi}{q}\Big)\log_2 x+\theta-\frac{2\pi a}{q}\Big)<0.$$

Now cosine is negative "about half the time" which might suggest that $N_{a,q}(x)$ is less than its average value "about half the time" too. To be precise, the set $\{n\in\mathbb{N}:\cos n<0\}$ has *natural density* $1/2$ in $\mathbb{N}$. That is, $\lim_{x\to\infty}\frac{1}{x}\sum_{\substack{n\le x\\ \cos n<0}}1=\frac{1}{2}$. It is not true though that $\{n\in\mathbb{N}:\cos(\log_2 n)<0\}$ has natural density $1/2$. In fact this set has no natural density, as we shall see below. The presence of the $\cos(\log_2 x)$ type term is why we ought to be looking at the log log density.

The property of possessing a natural density is stronger than that of possessing a logarithmic density, which is stronger still than having a loglog density. In fact, a straightforward application of partial summation proves that if a set $E\subset\mathbb{N}$ has a natural density then it also has a logarithmic density and the two are equal. Likewise, if E has a logarithmic density then it has a loglog density and the two are equal. The following lemma, which follows in a straightforward manner by comparison with an integral, explains why our notions of logarithmic and loglog density are sound.

Lemma 2.1. *There exist constants γ, μ such that*

$$\sum_{1\le n\le x}\frac{1}{n}=\log x+\gamma+O\Big(\frac{1}{x}\Big).$$
$$\sum_{2\le n\le x}\frac{1}{n\log n}=\log_2 x+\mu+O\Big(\frac{1}{x\log x}\Big).$$

Proposition 2.2. *Let $A,B\in\mathbb{R}$ with $A>0$. The set*

$$E:=\{n\in\mathbb{N}:\cos(A\log_2(n)+B)<0\}$$

has loglog density *1/2 but no natural or logarithmic densities.*

Proof. For $N\in\mathbb{N}$, define

$$x_N:=e_2((2N\pi-\pi/2-B)/A)\quad\text{and}\quad y_N:=e_2((2N\pi+\pi/2-B)/A)$$

so that

$$\cos(A\log_2 x + B) > 0 \Leftrightarrow x \in (x_N, y_N) \text{ for some } N \text{ and}$$
$$\cos(A\log_2 x + B) < 0 \Leftrightarrow x \in (y_{N-1}, x_N) \text{ for some } N.$$

Writing $[\alpha]$ for the largest integer at most α, we therefore have

$$\frac{1}{x_N}\sum_{\substack{n\le x_N\\ n\in E}} 1 \ge \frac{[x_N]-[y_{N-1}]}{x_N} \to 1 \text{ as } N\to\infty$$

and

$$\frac{1}{y_N}\sum_{\substack{n\le y_N\\ n\in E}} 1 \le 1 - \frac{[y_N]-[x_N]}{y_N} \to 0 \text{ as } N\to\infty,$$

so E certainly doesn't have a natural density. When we look at the logarithmic density, we get, since $\log y_N = e^{\pi/A}\log x_N$,

$$\frac{1}{\log x_N}\sum_{\substack{n\le x_N\\ n\in E}}\frac{1}{n} = \frac{e^{\pi/A}}{\log y_N}\sum_{\substack{n\le y_N\\ n\in E}}\frac{1}{n},$$

so for the limit to exist as $N\to\infty$ we would need $e^{\pi/A}=1$ which is impossible.

When we look at the loglog density however, we get, using Lemma 2.1

$$\begin{aligned}
\limsup_{x\to\infty}\frac{1}{\log_2 x}\sum_{\substack{n\le x\\ n\in E}}\frac{1}{n\log n} &= \lim_{N\to\infty}\frac{1}{\log_2 x_N}\sum_{m=2}^{N}\sum_{n\in(y_{m-1},x_m)}\frac{1}{n\log n}\\
&= \lim_{N\to\infty}\frac{1}{\log_2 x_N}\sum_{m=2}^{N}\Big(\log_2 x_m - \log_2 y_{m-1} + O\Big(\frac{1}{m\log m}\Big)\Big)\\
&= \lim_{N\to\infty}\frac{1}{(2N\pi-\pi/2-B)/A}\sum_{m=2}^{N}\Big(\pi/A + O\Big(\frac{1}{m\log m}\Big)\Big)\\
&= \frac{1}{2}.
\end{aligned}$$

A similar calculation shows that $\liminf_{x\to\infty}\frac{1}{\log_2 x}\sum_{\substack{n\le x\\ n\log n\in E}}\frac{1}{n\log n} = \frac{1}{2}$ and the result follows. □

It is tempting to conclude that the set

$$\{x \in \mathbb{N} \,:\, N_{a,q}(x) < \frac{x}{q}\}$$

has no natural or logarithmic densities but has loglog density $1/2$. Unfortunately, to prove this rigorously we will need to account for the error introduced by the terms we have left out. We will do this shortly. If we forget about error terms for the moment though (which we can only really do when $\sin(2\pi/q)\log_2 x + \theta - \frac{2\pi a}{q}$ is not too close to a zero of cos), then asking "for which value of a is $N_{a,q}(x)$ largest" is tantamount to asking "for which value of a is $\frac{2\pi}{q}\left(\frac{q}{2\pi}(\sin(2\pi/q)\log_2 x + \theta) - a\right)$ closest to some $2n\pi \in 2\pi\mathbb{Z}$". The answer is the closest integer to $\frac{q}{2\pi}(\sin(2\pi/q)\log_2 x + \theta)$ modulo q which clearly depends on x. Any given a will therefore produce the most values of $n \leq x$ such that $\omega(n) \equiv a \mod q$ when there exists some $m \in \mathbb{Z}$ such that,

$$a - \frac{1}{2} < \frac{q}{2\pi}(\sin(2\pi/q)\log_2 x + \theta) + mq < a + \frac{1}{2}.$$

A similar calculation to that in the proof of Proposition 2.2 shows that for each a, the set of such x values has loglog density $1/q$.

We end this section with a picture of the curves

$$\cos\left(\sin\left(\frac{2\pi}{6}\right)\log_2 x + \theta - \frac{2\pi a}{6}\right)$$

for $a = 0, 1, \ldots, 5$ plotted with an x-axis scale which makes the oscillations visible.

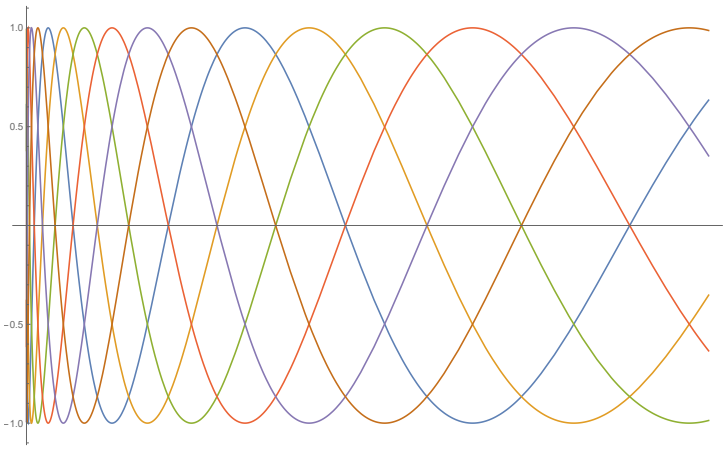


Figure 2.2: Shifted sinusoidal curves

Although this picture isn't to be taken too seriously it serves as a useful illustration to have in mind for comparing the secondary terms.

2.3 Proof of Theorem 2.3

Proof. Let $q \geq 3$ be some fixed integer, $a \in \{0, 1, \ldots, q-1\}$ and θ be defined as in Proposition 2.1. Let $\epsilon > 0$ be small and define

$$U_{a,q}^{\epsilon-} := \{x \in \mathbb{N} : -\frac{\pi}{q} + \sqrt{\epsilon} < \sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi a}{q} + 2n\pi < -\sqrt{\epsilon} \text{ for some } n \in \mathbb{Z}\},$$

$$U_{a,q}^{\epsilon+} := \{x \in \mathbb{N} : -\frac{\pi}{q} - \sqrt{\epsilon} < \sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi a}{q} + 2n\pi < \sqrt{\epsilon} \text{ for some } n \in \mathbb{Z}\}.$$

First let us see how, for small ϵ, these sets approximate $U_{a,q}$. Our formula for $N_{a,q}(x)$ gives

$$\frac{N_{a,q}(x) - N_{b,q}(x)}{(\log x)^{\cos(\frac{2\pi}{q})-1}} =$$
$$2|g(\phi)|\Big(\cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi a}{q}\Big) - \cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi b}{q}\Big)\Big) + o(1)$$

as $x \to \infty$ and for $q \geq 3$ we have $g(\phi) \neq 0$. Therefore, for all $\epsilon > 0$ there exists some $X_0(\epsilon)$ such that for $x \geq X_0$ and for each $a, b \in \{0, \ldots, q-1\}$,

$$\cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi a}{q}\Big) - \cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi b}{q}\Big) > \epsilon$$

which implies that $N_{a,q}(x) > N_{b,q}(x)$. We will use this fact to prove that for $x \geq X_0$ and ϵ sufficiently small we have

$$x \in U_{a,q}^{\epsilon-} \Rightarrow x \in U_{a,q} \tag{2.3}$$

and

$$x \in U_{a,q} \Rightarrow x \in U_{a,q}^{\epsilon+}. \tag{2.4}$$

It follows that

$$\sum_{\substack{x \leq X \\ x \in U_{a,q}^{\epsilon-}}} \frac{1}{x \log x} + O_\epsilon(1) \leq \sum_{\substack{x \leq X \\ n \in U_{a,q}}} \frac{1}{x \log x} \leq \sum_{\substack{x \leq X \\ x \in U_{a,q}^{\epsilon+}}} \frac{1}{x \log x} + O_\epsilon(1).$$

After showing that each of $U_{a,q}^{\epsilon\pm}$ has loglog density $\frac{1}{2q}+o_\epsilon(1)$ for arbitrarily small ϵ, where $o_\epsilon(1)$ is a quantity that tends to 0 as $\epsilon\to 0$, we will have shown that $U_{a,q}$ has loglog density $\frac{1}{2q}$. The result for $V_{a,q}$ is proved in much the same way.

Proof of (2.3) and (2.4).

Suppose $x\geq X_0$ and $x\in U_{a,q}^{\epsilon-}$ and ϵ is small enough so that $\sin(\frac{\pi}{q})\sin(\sqrt{\epsilon})>\epsilon$. For example, $\epsilon<1/q^2$ will do. In order to show that $x\in U_{a,q}$ we need to show

(a) $N_{a-i,q}(x)>N_{a+i,q}(x)$ for all $i\in\{1,2,\dots,[\frac{q-1}{2}]\}$

(b) $N_{a+i,q}(x)>N_{a-i-1,q}(x)$ for all $i\in\{0,1,\dots,[\frac{q-2}{2}]\}$.

To do so we will use the identity

$$\cos(\xi+A)-\cos(\xi+B)=-2\sin\left(\frac{A-B}{2}\right)\sin\left(\xi+\frac{A+B}{2}\right). \tag{2.5}$$

For (a), let $i\in\{1,2,\dots,\text{ or }[\frac{q-1}{2}]\}$, then

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a-i)}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a+i)}{q}\Big)$$
$$=-2\sin(\frac{2\pi i}{q})\sin(\xi)$$

where $\xi=\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}\in\Big(-\frac{\pi}{q}+\sqrt{\epsilon},-\sqrt{\epsilon}\Big)$ which is $>\epsilon$. This proves (a). For (b), let $i\in\{0,1,\dots,\text{ or }[\frac{q-2}{2}]\}$, then

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a+i)}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a-i-1)}{q}\Big)$$
$$=2\sin(\frac{\pi(2i+1)}{q})\sin(\xi+\frac{\pi}{q})$$

where again $\xi\in\Big(-\frac{\pi}{q}+\sqrt{\epsilon},-\sqrt{\epsilon}\Big)$ which is again $>\epsilon$. This proves (b) and that $x\in U_{a,q}$.

Now suppose $x\geq X_0$ and $x\in U_{a,q}$. To show that $x\in U_{a,q}^{\epsilon+}$ we need to find some $n\in\mathbb{Z}$ such that

$$-\frac{\pi}{q}-\sqrt{\epsilon}<\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}+2n\pi<\sqrt{\epsilon}.$$

Suppose this is not the case. Then either we can find some n such that

$$-\pi-\sqrt{\epsilon}\le \sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}+2n\pi\le -\frac{\pi}{q}-\sqrt{\epsilon}.$$

In which case

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a-1)}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}\Big)$$
$$=-2\sin(\frac{\pi}{q})\sin(\xi+\frac{\pi}{q})$$

for some $\xi\in\Big[-\pi-\sqrt{\epsilon},-\frac{\pi}{q}-\sqrt{\epsilon}\Big]$. This is then $>\epsilon$ and so $N_{a-1,q}(x)>N_{a,q}(x)$, contrary to our assumption on x. Or else we can find some n such that

$$\sqrt{\epsilon}\le \sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}+2n\pi\le \pi-\sqrt{\epsilon}.$$

In which case

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a+1)}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi(a-1)}{q}\Big)$$
$$=-2\sin(-\frac{2\pi}{q})\sin(\xi)$$

for some $\xi\in(\sqrt{\epsilon},\pi-\sqrt{\epsilon})$. Again making the difference $>\epsilon$ and so $N_{a+1,q}(x)>N_{a-1,q}(x)$, again contrary to our assumption on x. We must therefore have $x\in U^{\epsilon+}_{a,q}$.

It remains to calculate the loglog densities of $U^{\epsilon-}_{a,q}$ and $U^{\epsilon+}_{a,q}$. This is similar to the proof of Proposition 2.2. For $N\in\mathbb{N}$ define $x_N:=e_2((2N\pi+2a\pi/q-\theta-\pi/q+\sqrt{\epsilon})/\sin(2\pi/q))$ and $y_N:=e_2((2N\pi+2a\pi/q-\theta-\sqrt{\epsilon})/\sin(2\pi/q))$, then for $x\ge X_0$ we have $x\in U^{\epsilon-}_{a,q}$ if and only if $x\in(x_N,y_N)$ for some N and we therefore have

$$\begin{aligned}\liminf_{X\to\infty}\frac{1}{\log_2 X}\sum_{\substack{n\le x\\ n\in U^{\epsilon-}_{a,q}}}\frac{1}{n\log n}&=\lim_{N\to\infty}\frac{1}{\log_2 x_N}\sum_{m=1}^{N-1}\sum_{n\in(x_m,y_m)}\frac{1}{n\log n}\\
&=\lim_{N\to\infty}\frac{1}{\log_2 x_N}\sum_{m=1}^{N-1}\Big(\frac{(\pi/q)-2\sqrt{\epsilon}}{\sin(2\pi/q)}+O\Big(\frac{1}{m\log m}\Big)\Big)\\
&=\lim_{N\to\infty}\frac{\sin(2\pi/q)}{2N\pi+2a\pi/q-\theta-\pi/q+\sqrt{\epsilon}}\Big((N-1)\frac{(\pi/q)-2\sqrt{\epsilon}}{\sin(2\pi/q)}+O(\log N)\Big)\\
&=\frac{1}{2q}-\frac{\sqrt{\epsilon}}{\pi}.\end{aligned}$$

Also,

$$\limsup_{X\to\infty}\frac{1}{\log_2 X}\sum_{\substack{n\le x\\ n\in U_{a,q}^{\epsilon-}}}\frac{1}{n\log n}=\lim_{N\to\infty}\frac{1}{\log_2(y_N))}\sum_{m=1}^{N}\sum_{n\in(x_m,y_m)}\frac{1}{n\log n}=\frac{1}{2q}-\frac{\sqrt{\epsilon}}{\pi}$$

Hence the loglog density of $U_{a,q}^{\epsilon-}$ exists and is equal to $\frac{1}{2q}-\frac{\sqrt{\epsilon}}{\pi}$. A very similar calculation shows that the loglog density of $U_{a,q}^{\epsilon+}$ is $\frac{1}{2q}+\frac{\sqrt{\epsilon}}{\pi}$ and so by (4) and the fact that ϵ can be taken arbitrarily small we can conclude that $U_{a,q}$ has loglog density $\frac{1}{2q}$. □

2.4 Proof of Theorem 2.4

As in the previous proof, let ϵ be small enough and X_0 large enough so that $\sin(\frac{\pi}{q})\sin(\sqrt{\epsilon})>\epsilon$ and that for $x\ge X_0$ we have

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi b}{q}\Big)>\epsilon\Rightarrow N_{a,q}(x)>N_{b,q}(x)$$

and

$$x\in U_{a,q}^{\epsilon-}\Rightarrow x\in U_{a,q}$$

and

$$x\in U_{a,q}\Rightarrow x\in U_{a,q}^{\epsilon+}.$$

We will show that only the permutations stated in Theorem 2.4 can occur for $x\ge X_0$. Suppose that we have some $x\ge X_0$ for which $N_{a,q}(x)$ is leading, that is, $\max_{c \mod q} N_{c,q}(x)=N_{a,q}(q)$. It follows that $x\in U_{a,q}^{\epsilon+}\cup V_{a,q}^{\epsilon+}$ since otherwise there would be some integer n such that

$$\frac{\pi}{q}+\sqrt{\epsilon}\le\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}+2n\pi\le 2\pi-\frac{\pi}{q}-\sqrt{\epsilon}$$

and hence

$$\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi b}{q}\Big)-\cos\Big(\sin(\frac{2\pi}{q})\log_2 x+\theta-\frac{2\pi a}{q}\Big)$$
$$=-2\sin(\frac{\pi(a-b)}{q})\sin(\xi+\frac{\pi(a-b)}{q})$$

for some $\xi\in(\frac{\pi}{q}+\sqrt{\epsilon}\,,\ 2\pi-\frac{\pi}{q}-\sqrt{\epsilon})$. But then this is $>\epsilon$ for either $b=a+1 \mod q$ or

$b = a - 1 \mod q$ contradicting the assumption that $N_{a,q}(x)$ was leading.

To prove Theorem 2.4 it suffices to prove that $\max_{\pm 1} N_{a\pm 1,q}(x) > N_{b,q}(x)$ for all $b \neq a, a \pm 1 \mod q$. This follows, in a by now familiar fashion, from the fact that there exists an integer n such that

$$-\frac{\pi}{q} - \sqrt{\epsilon} < \sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi a}{q} + 2n\pi < \frac{\pi}{q} + \sqrt{\epsilon}$$

since then

$$\begin{aligned}
&\max_{\pm} \quad \cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi(a \pm 1)}{q}\Big) - \cos\Big(\sin(\frac{2\pi}{q}) \log_2 x + \theta - \frac{2\pi b}{q}\Big) \\
&= \max_{\pm} \quad -2\sin(\pi \frac{b - (a \pm 1)}{q}) \sin(\xi - \frac{\pi(b - a \pm 1)}{q}) \\
&= \max_{\pm} \quad 2\sin(\pi \frac{b - (a \pm 1)}{q}) \sin(\pi \frac{(b - a \pm 1)}{q} - \xi)
\end{aligned}$$

where $\xi \in (-\frac{\pi}{q} - \sqrt{\epsilon}\,,\ \frac{\pi}{q} + \sqrt{\epsilon})$, so this is $> \epsilon$ for $b \neq a, a \pm 1 \mod q$ which proves the claim.

Chapter 3

The Selberg–Delange method in $\mathbb{F}_q[t]$

This chapter is based on joint work with Ardavan Afshar [2].

We develop a function field analogue of the Selberg–Delange method to derive asymptotic formulae for the number of monic and square-free monic polynomials in $\mathbb{F}_q[t]$ of degree n with precisely k irreducible factors, in the limit as n tends to infinity. We then adapt the method to count such polynomials in arithmetic progressions and short intervals, and by making use of Weil's 'Riemann hypothesis' for curves over $\mathbb{F}_q$, obtain better ranges for these formulae than are currently known for their analogues in the number field setting.

3.1 Introduction

In the context of understanding the anatomy of integers it is natural to want to count not just prime numbers but numbers with exactly k distinct prime divisors for $k \geq 1$. Let

$$\pi_k(x) = \#\{n \leq x \,:\, \Omega(n) = \omega(n) = k\}.$$

In [35], Sathé proved that for any fixed $A > 0$, uniformly in the range $x \geq 3$ and $1 \leq k \leq A \log\log x$ we have

$$\pi_k(x) \sim G\left(\frac{k-1}{\log\log x}\right) \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!}$$

where $G(z) = \frac{1}{\Gamma(1+z)} \prod_{p \text{ prime}} (1 + \frac{z}{p})(1 - \frac{1}{p})^z$.

In [36], Selberg gave a simpler proof of this result, now known as the "Sathé–Selberg Formula". One might ask whether such a formula also holds for numbers restricted to a given arithmetic progression or short interval. For example, in [37], Spiro showed that such a formula holds for $n \leq x$ restricted to $n \equiv a \mod q$, provided q does not exceed some fixed power of $\log x$.

We begin this chapter by adapting Selberg's method to prove an asymptotic formula for the number of monic polynomials in $\mathbb{F}_q[t]$ of degree n with exactly k distinct irreducible divisors. Let us (re)define

$$\pi_k(n) := \#\{f \in \mathcal{M}_n : f = p_1 \cdots p_k \text{ for some } p_1, \cdots, p_k \in \mathcal{P} \text{ distinct}\}.$$

Theorem 3.1. *Let $A > 1$. Then uniformly for all $n \geq 2$ and $1 \leq k \leq A \log n$ we have*

$$\pi_k(n) = \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

where $G(z) = \frac{F(1/q,z)}{\Gamma(1+z)}$ and $F(1/q, z) = \prod_{p \in \mathcal{P}} \left(1 + \frac{z}{q^{\deg p}}\right)\left(1 - \frac{1}{q^{\deg p}}\right)^z$.

So the asymptotic density of square-free polynomials in $\mathcal{M}_n$ with k distinct prime divisors is $\frac{1}{n}\frac{(\log n)^{k-1}}{(k-1)!} G\left(\frac{k-1}{\log n}\right)$.

With some additional technical work following Chapters II.5 and II.6 of [38], one could strengthen Theorem 3.1 to be of an analogous form to Chapter II.6 Theorem 4 of [38], namely

$$\pi_k(n) = \frac{q^n}{n} \left(\sum_{j=0}^{J} \frac{P_{j,k}(\log n)}{n^j} + O_A\left(\left(\frac{cJ+1}{n}\right)^{J+1} \frac{(\log n)^k}{k!}\right)\right)$$

where $P_{j,k}(x)$ is a polynomial of degree at most $k-1$, J is a non-negative integer, and c is some absolute constant.

Such an improvement could also be carried through to Theorems 3.2 and 3.3 below, to give similarly strengthened versions of what they state.

Next, we apply our method to Dirichlet L-functions for $\mathbb{F}_q[t]$, to derive an asymptotic formula for the number of such polynomials in a given arithmetic progression with common difference of degree no bigger than roughly $n/2$. Let

$$\pi_k(n; g, d) := \#\{f \in \mathcal{M}_n \ f \equiv g \mod d : f = p_1 \cdots p_k \text{ for some } p_1, \cdots, p_k \in \mathcal{P} \text{ distinct}\}.$$

Theorem 3.2. *Let $g, d \in \mathbb{F}_q[t]$ be coprime and $m = \deg d$. For any $A > 1$, $n \geq 2$ and*

$1 \leq k \leq A \log n$ *with* $m \leq \left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n$ *we have*

$$\pi_k(n; g, d) = \frac{1}{\phi(d)} \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G_d\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

where $\phi(d) = \left|(\mathbb{F}_q[t]/(d(t)))^\times\right|$, *and* $G_d(z) = \left(\prod_{p|d}\left(1 + \frac{z}{q^{\deg p}}\right)^{-1}\right) G(z)$ *where* $G(z)$ *is defined as in Theorem 3.1.*

This range on the degree of the common difference is obtained by our use of Weil's 'Riemann Hypothesis', which allows us to bound the contributions from the non-principal characters as roughly square-root of the contribution from the principal character. This is stronger than anything that can likely be proved for integers without also proving something close to the Riemann hypothesis for Dirichlet L-functions.

We end this chapter by deducing from Theorem 3.2 an asymptotic formula for the number of such polynomials in a given 'short interval' of length no shorter than roughly $n/2$. This uses the duality between short intervals and arithmetic progressions in $\mathbb{F}_q[t]$ as explained in for example [18]. Let

$$\psi_k(n; g; h) := \#\{f \in \mathcal{M}_n \ \ \deg(f-g) \leq h : f = p_1 \cdots p_k \text{ for some } p_1, \cdots, p_k \in \mathcal{P} \text{ distinct}\}.$$

Theorem 3.3. *Let* $g \in \mathbb{F}_q[t]$. *Let* $A > 1$, $n \geq 2$ *and* $1 \leq k \leq A \log n$.
Then for h *satisfying* $n - 1 \geq h \geq \left(\frac{1}{2} + \frac{1+\log(1+\frac{A}{2})}{\log q}\right)(n+1)$, *we have*

$$\psi_k(n; g; h) = \frac{q^{h+1}}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(H\left(\frac{k-1}{\log n}\right) + \frac{k-1}{q \log n} H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

where $H(z) = \frac{q}{q+z} G(z)$ *and* $G(z)$ *is defined as in Theorem 3.1.*

The two main terms in Theorem 3.3 come from counting polynomials with non-zero constant term and polynomials with zero constant term separately. We note that in the range where $k \asymp \log n$, the latter is roughly a factor of q smaller than the former, and so of the same order of magnitude in the limit as n tends to infinity.

These results give quite precise information about the number of polynomials with a specific number of irreducible factors in different situations. Results about the average number of irreducible divisors, such as the analogue of the Erdös–Kac Theorem can readily be deduced from these.

3.2 The function field Sathé–Selberg formula

3.2.1 Outline

In our study of $\pi_k(n)$ we will make use of a two variable zeta function for $\mathcal{M}$ which will serve to count irreducible factors, namely,

$$A(T,z) = \sum_{f\in\mathcal{M}} \mu^2(f) z^{\omega(f)} T^{\deg f} = \prod_{p\in\mathcal{P}} (1 + zT^{\deg p})$$

where $\mu(f)$ is the Möbius function, defined to be $(-1)^k$ if f is the product of k distinct irreducibles and 0 otherwise. By taking $z \in \mathbb{C}$ and considering $A(T,z)$ as a power series in T we will derive estimates for its coefficients, which we denote by $A_z(n) = \sum_{f\in\mathcal{M}_n} \mu^2(f) z^{\omega(f)}$. Then we can recover $\pi_k(n)$ using Cauchy's integral formula and the pair of identities

$$\sum_{k\geq 0} \pi_k(n) z^k = A_z(n), \qquad \pi_k(n) = \frac{1}{2\pi i} \oint \frac{A_z(n)}{z^{k+1}} dz.$$

This plan will be carried out by first deriving an estimate for the coefficients of the power series of $\zeta(T)^z$, where $\zeta(T) = \sum_{f\in\mathcal{M}} T^{\deg f}$ is the zeta function for $\mathcal{M}$, and then relating this to the estimate we want for $A_z(n)$, the coefficients of the related series $A(T,z)$. Throughout, $A > 1$ will be an arbitrary positive constant and z a complex variable satisfying $|z| \leq A$.

3.2.2 Proof of Theorem 3.1

Recall that for $|T| < 1/q$

$$\zeta(T) = \sum_{f\in\mathcal{M}} T^{\deg f} = \sum_{n\geq 0} q^n T^n = \frac{1}{1-qT}.$$

For T in this range, we define $\zeta(T)^z = \exp(z \log \zeta(T))$, where we choose the branch of the logarithm that is defined on the cut plane $\mathbb{C}\backslash[0,\infty)$ and is real for T real.

Lemma 3.1. *If we define $D_z(n)$ for $n \geq 0$ via the identity $\zeta(T)^z = \sum_{n\geq 0} D_z(n) T^n$, then we have that*

$$D_z(n) = q^n \binom{n+z-1}{n}$$

where $\binom{w}{n} = \frac{1}{n!} \prod_{j=0}^{n-1} (w-j)$.

Proof. This is just the binomial theorem

$$\zeta(T)^z = (1-qT)^{-z} = \sum_{n\geq 0} \binom{n+z-1}{n} q^n T^n. \qquad \square$$

Corollary 3.1. *For all $n \geq 1$ and $|z| \leq A$,*

$$D_z(n) = q^n \frac{n^{z-1}}{\Gamma(z)} + O_A\left(q^n n^{\Re z - 2}\right).$$

Proof. It suffices to prove this for $n \geq 2A$. In this range, we consider two cases. The first is when z is a non-positive integer, in which case $D_z(n) = 0 = \frac{q^n}{\Gamma(z)} n^{z-1}$. Otherwise we can use the Weierstrass Product Formula for $\Gamma(z)$ in the second line below to get

$$\begin{aligned}
\frac{\Gamma(n+z)}{\Gamma(n+1)} &= \frac{1}{n+z}\left(\prod_{k=1}^{n} \frac{k+z}{k}\right) z\Gamma(z) \\
&= \frac{1}{n+z}\left(\prod_{k=1}^{n} \frac{k+z}{k}\right) e^{-\gamma z}\left(\prod_{k=1}^{\infty} \frac{k}{k+z} e^{z/k}\right) \\
&= \frac{e^{-\gamma z}}{n+z}\left(\prod_{k=1}^{n} e^{z/k}\right)\left(\prod_{k=n+1}^{\infty} \frac{k}{k+z} e^{z/k}\right) \\
&= \frac{e^{-\gamma z}}{n+z} \exp\left(\sum_{k=1}^{n} \frac{z}{k}\right) \exp\left(\sum_{k=n+1}^{\infty} \left(\frac{z}{k} - \log\left(1+\frac{z}{k}\right)\right)\right) \\
&= \frac{e^{-\gamma z}}{n+z} \exp\left(z\left(\log n + \gamma + O\left(\frac{1}{n}\right)\right)\right) \exp\left(\sum_{k=n+1}^{\infty}\sum_{m=2}^{\infty} (-1)^m \frac{z^m}{mk^m}\right) \\
&= \frac{n^z}{n+z}\left(1 + O_A\left(\frac{1}{n}\right)\right) \exp\left(O_A\left(\frac{1}{n}\right)\right) = n^{z-1}\left(1 + O_A\left(\frac{1}{n}\right)\right).
\end{aligned}$$

From this and Lemma 3.1 we can conclude that

$$D_z(n) = q^n \binom{n+z-1}{n} = q^n \frac{\Gamma(n+z)}{\Gamma(n+1)\Gamma(z)} = q^n \frac{n^{z-1}}{\Gamma(z)}\left(1 + O_A\left(\frac{1}{n}\right)\right). \qquad \square$$

It was fairly straightforward to derive an asymptotic formula for $D_z(n)$. The following technical proposition will allow us to use this result to deduce asymptotic formulae for the coefficients of more general series provided their behaviour at $1/q$ is similar to the singularity of $\zeta(T)^z$ at $T = 1/q$. This proof is modelled on that of Theorem 7.18 from [24].

Proposition 3.1. *Let $C(T,z) = \sum_{n\geq 0} C_z(n)T^n$ and $M(T,z) = \sum_{n\geq 0} M_z(n)T^n$ be power*

series with coefficients depending on z satisfying $C(T,z) = M(T,z)\zeta(T)^z$. Suppose also that, uniformly for $|z| \le A$,

$$\sum_{a\ge 0} \frac{|M_z(a)|}{q^a} a^{2A+2} \ll_A 1. \tag{3.1}$$

Then, uniformly for $|z| \le A$ and $n \ge 1$, we have

$$C_z(n) = q^n \frac{n^{z-1}}{\Gamma(z)} M(1/q, z) + O_A(q^n n^{\Re z - 2}).$$

Proof. Using our expression for $D_z(n)$ from Corollary 3.1 and that $D_z(0) = 1$, we get

$$\begin{aligned} C_z(n) &= \sum_{0\le a\le n} M_z(a) D_z(n-a) \\ &= q^n \left[\sum_{0\le a<n} \frac{M_z(a)}{q^a} \frac{(n-a)^{z-1}}{\Gamma(z)} + O_A\left(\sum_{0\le a<n} \frac{|M_z(a)|}{q^a} (n-a)^{\Re z - 2} \right) + \frac{M_z(n)}{q^n} \right]. \end{aligned}$$

Here we split the first sum at $n/2$ and use the fact that

$$(n-a)^{z-1} = \begin{cases} n^{z-1}\left(1 + O_A(a/n)\right), & \text{if } 0 \le a \le n/2 \\ O_A(n^{A-1}), & \text{if } n/2 < a < n. \end{cases}$$

Combining this with (3.1) we get

$$\begin{aligned} &\sum_{0\le a<n} \frac{M_z(a)}{q^a} \frac{(n-a)^{z-1}}{\Gamma(z)} \\ &= \sum_{0\le a\le n/2} \frac{M_z(a)}{q^a} \frac{n^{z-1}}{\Gamma(z)} \left(1 + O_A(a/n)\right) + O_A\left(\sum_{n/2<a<n} \frac{|M_z(a)|}{q^a} n^{A-1} \right) \\ &= \sum_{0\le a\le n/2} \frac{M_z(a)}{q^a} \frac{n^{z-1}}{\Gamma(z)} + O_A\left(n^{\Re z - 2} \sum_{0\le a\le n/2} \frac{|M_z(a)|a}{q^a} + n^{\Re z - 2} \sum_{n/2<a<n} \frac{|M_z(a)|a^{2A+1}}{q^a} \right) \\ &= \frac{n^{z-1}}{\Gamma(z)} M(1/q,z) + O_A\left(n^{\Re z - 1} \sum_{a>n/2} \frac{|M_z(a)|}{q^a} + n^{\Re z - 2} \right) \\ &= \frac{n^{z-1}}{\Gamma(z)} M(1/q,z) + O_A\left(n^{\Re z - 2} \sum_{a>n/2} \frac{|M_z(a)|a}{q^a} + n^{\Re z - 2} \right) \\ &= \frac{n^{z-1}}{\Gamma(z)} M(1/q,z) + O_A\left(n^{\Re z - 2} \right). \end{aligned}$$

Where, in the final term of the second line, we use that $n^{\Re z-2}a^{2A+1} \gg n^{-A-2}n^{2A+1} = n^{A-1}$ for $n/2 < a < n$.

Similarly, for the second sum we get

$$\begin{aligned}
&\sum_{0\le a<n} \frac{|M_z(a)|}{q^a}(n-a)^{\Re z-2} \\
&= \sum_{0\le a\le n/2} \frac{|M_z(a)|}{q^a} n^{\Re z-2}\left(1+O_A(a/n)\right) + O_A\left(\sum_{n/2<a<n} \frac{|M_z(a)|}{q^a} n^{A-2}\right) \\
&\ll_A n^{\Re z-2} \sum_{0\le a\le n/2} \frac{|M_z(a)|}{q^a} + n^{\Re z-3} \sum_{0\le a\le n/2} \frac{|M_z(a)|a}{q^a} + n^{\Re z-3} \sum_{n/2<a<n} \frac{|M_z(a)|a^{2A+1}}{q^a} \\
&\ll_A n^{\Re z-2}.
\end{aligned}$$

Finally, by (3.1) we have that the last term is

$$\frac{M_z(n)}{q^n} \ll n^{\Re z-2}\frac{|M_z(n)|n^{A+2}}{q^n} \ll n^{\Re z-2}\sum_{a\ge 0}\frac{|M_z(a)|}{q^a}a^{A+2} \ll_A n^{\Re z-2}.$$

Putting everything together proves the proposition. □

We will apply the previous proposition with the series $F(T,z) = \sum_{n\ge 0} B_z(n)T^n$ defined by

$$F(T,z) := A(T,z)\zeta(T)^{-z} = \prod_{p\in\mathcal{P}}(1+zT^{\deg p})(1-T^{\deg p})^z.$$

First we check that the conditions of Proposition 3.1 are satisfied as in done in the integer setting at the beginning of Chapter II.6 of [38].

Proposition 3.2. *For $|z| \le A$, $n \ge 2$ and $\sigma \ge \frac{1}{2}$*

$$\sum_{0\le a\le n} \frac{|B_z(a)|}{q^{\sigma a}} \le \begin{cases} C_{A,\sigma} & \text{if } \sigma > \frac{1}{2} \\ n^{C_A} & \text{if } \sigma = \frac{1}{2}, \end{cases}$$

where $C_{A,\sigma}$ is a constant depending only on A and σ, and C_A is a constant depending only on A.

Consequently, since $a^{2A+2} \le q^{a/3}$ for a sufficiently large, we have for $|z| \le A$ that

$$\sum_{a\ge 0}\frac{|B_z(a)|}{q^a}a^{2A+2} \ll_A \sum_{a\ge 0}\frac{|B_z(a)|}{q^{2a/3}} \ll_A 1.$$

Proof. If we let $b_z(f)$ be the multiplicative function defined on powers of monic irreducible polynomials p by the power series identity

$$1 + \sum_{k\geq 1} b_z(p^k)S^k = (1+zS)(1-S)^z$$

then $F(T,z) = \sum_{f\in\mathcal{M}} b_z(f)T^{\deg f}$ and so $B_z(n) = \sum_{f\in\mathcal{M}_n} b_z(f)$. From this definition, we see that $b_z(p) = 0$ on irreducible p and, by Cauchy's inequality after integrating over the complex circle $|S| = \frac{1}{\sqrt{3/2}}$, that

$$|b_z(p^k)| \leq (3/2)^{k/2} M_A, \text{ for } k \geq 2$$

where $M_A = \sup_{|z|\leq A, |S|\leq \frac{1}{\sqrt{3/2}}} |(1+zS)(1-S)^z|$ is some constant depending on A. Therefore, letting $\mathcal{M}_{\leq n} = \{f \in \mathcal{M} : \deg f \leq n\}$ and $\mathcal{P}_{\leq n} = \{p \in \mathcal{P} : \deg p \leq n\}$, we have

$$\begin{aligned}
\sum_{0\leq a\leq n} \frac{|B_z(a)|}{q^{\sigma a}} &\leq \sum_{f\in\mathcal{M}_{\leq n}} \frac{|b_z(f)|}{q^{\sigma \deg f}} \\
&\leq \prod_{p\in\mathcal{P}_{\leq n}} \left(1 + \sum_{k\geq 1} \frac{|b_z(p^k)|}{q^{k\sigma\deg p}}\right) \\
&\leq \prod_{p\in\mathcal{P}_{\leq n}} \left(1 + M_A \sum_{k\geq 2} \left(\frac{\sqrt{3/2}}{q^{\sigma\deg p}}\right)^k\right) \\
&= \prod_{p\in\mathcal{P}_{\leq n}} \left(1 + \frac{3M_A/2}{q^{\sigma\deg p}(q^{\sigma\deg p} - \sqrt{3/2})}\right).
\end{aligned}$$

Taking the logarithm and using the prime polynomial theorem we get

$$\begin{aligned}
\sum_{p\in\mathcal{P}_{\leq n}} \log\left(1 + \frac{3M_A/2}{q^{\sigma\deg p}(q^{\sigma\deg p} - \sqrt{3/2})}\right) &\leq 6M_A \sum_{1\leq d\leq n} \frac{q^{d(1-2\sigma)}}{d} \\
&\leq \begin{cases} \frac{6M_A}{q^{2\sigma-1}-1} & \text{if } \sigma > \frac{1}{2} \\ 12M_A \log n & \text{if } \sigma = \frac{1}{2}. \end{cases}
\end{aligned}$$

Exponentiating then gives the stated result. □

Remark. Proposition 3.2 also proves that $F(1/q, z)$ is absolutely uniformly convergent for $|z| \leq A$ and so holomorphic in z for $|z| \leq A$.

Corollary 3.2. *Uniformly for $|z| \leq A$ and $n \geq 1$, we have*

$$A_z(n) = q^n \frac{n^{z-1}}{\Gamma(z)} F(1/q, z) + O_A(q^n n^{\Re z - 2}).$$

Proof. Proposition 3.2 allows us to apply, Proposition 3.1 with $C(T, z) = A(T, z)$ and $M(T, z) = F(T, z)$ and the result follows. □

We now turn to the proof of a generalisation of the main result in this section. We require the following lemma which is a simple application of the saddle point method.

Lemma 3.2. *Let $A > 0$ and let $p_n(z) = \sum_{k \geq 0} c_k(n) z^k$ be a sequence of polynomials such that uniformly for $n \geq 1$ and $|z| \leq A$ the following approximation holds*

$$p_n(z) = n^{az} \left(f(z) + O\left(\frac{1}{n}\right)\right) \tag{3.2}$$

for some real constant $a > 0$ and some function $f(z)$ that is holomorphic on $\{z \in \mathbb{C} : |z| \leq A\}$. Then uniformly for $1 \leq k \leq aA \log n$,

$$c_k(n) = \frac{(a \log n)^k}{k!} \left(f\left(\frac{k}{a \log n}\right) + O\left(\frac{k}{(\log n)^2}\right)\right).$$

Proof. The starting point is Cauchy's formula

$$c_k(n) = \frac{1}{2\pi i} \int_{|z|=r} p_n(z) \frac{dz}{z^{k+1}}.$$

We choose r to minimise the trivial bound

$$|c_k(n)| \ll r \cdot \max_{|z|=r} \left| \frac{n^{az}}{z^{k+1}} \right| = \frac{n^{ar}}{r^k}.$$

Since $a > 0$, the maximum occurs at $z = r = k/(a \log n)$. From (3.2) we have

$$c_k(n) = \frac{1}{2\pi i} \int_{|z|=r} n^{az} f(z) \frac{dz}{z^{k+1}} + O(E)$$

where $E = \frac{1}{n} \int_{|z|=r} \left| \frac{n^{az}}{z^{k+1}} \right| |dz|$. Using

$$\frac{1}{2\pi i} \int_{|z|=r} (z - r) n^{az} \frac{dz}{z^{k+1}} = \frac{(a \log n)^{k-1}}{(k-1)!} - r \frac{(a \log n)^k}{k!} = 0$$

and the approximation

$$f(z) = f(r) + f'(r)(z-r) + O(|z-r|^2)$$

this becomes

$$c_k(n) = f(r)\frac{(a\log n)^k}{k!} + O\left(r^{-k}\int_{|z|=r} |n^{az}(z-r)^2||dz| + E\right).$$

The integral in the error term is bounded by

$$r^2\int_{-\pi}^{\pi} |1-e^{i\theta}|^2 e^{k\cos\theta}d\theta \ll r^2\int_{-\infty}^{\infty}\theta^2 e^{k(1-\theta^2/5)}d\theta \ll r^2 e^k k^{-3/2}$$

which contributes an error of

$$(k/(a\log n))^{2-k}e^k k^{-3/2} \ll a^k(\log n)^{k-2}\frac{e^k\sqrt{k}}{k^k} \ll a^k\frac{k(\log n)^{k-2}}{k!}$$

by Stirling's formula. The other term E in the error contributes at most

$$\ll \frac{r^{-k-1}}{n}\int_{|z|=r}\left|n^{a(z-r)}\right||dz| \ll \frac{r^{-k}}{n}\int_{-1/2}^{1/2} n^{-art^2}dt \ll \frac{1}{n}(a\log n)^k\frac{e^k}{k^{k+1/2}} \ll \frac{1}{n}\frac{(a\log n)^k}{k!}$$

again by Stirling's formula. □

All the ingredients to prove Theorem 3.1 have now been assembled. We apply Lemma 3.2 with $c_k(n) = n\pi_{k+1}(n)/q^n$ and $p_n(z) = \frac{n}{q^n}\sum_{k\geq 0}\pi_{k+1}(n)z^k = \frac{n}{q^n}zA_z(n)$. Corollary 3.2 is the condition we need to apply Lemma 3.2 with $a = 1$ and $f(z) = \frac{z}{\Gamma(z)}F(1/q,z) = \frac{F(1/q,z)}{\Gamma(1+z)}$. The conclusion is then precisely the statement of Theorem 3.1.

Remark. We can also estimate $\rho_k(n) := \{f \in \mathcal{M}_n : \omega(f) = k\}$ by first proving an analogue of Proposition 3.2 for the power series

$$\widetilde{F}(T,z) := \zeta(T)^{-z}\sum_{f\in\mathcal{M}} z^{\omega(f)}T^{\deg f} = \prod_{p\in\mathcal{P}}\left(1+\frac{zT^{\deg p}}{1-T^{\deg p}}\right)(1-T^{\deg p})^z$$

then applying Proposition 3.1 with $M(T,z) = \widetilde{F}(T,z)$ and $C(T,z) = \widetilde{A}(T,z)$ where

$$\widetilde{A}(T,z) = \sum_{n\geq 0}\widetilde{A}_z(n)T^n := \sum_{f\in\mathcal{M}} z^{\omega(f)}T^{\deg f} = \widetilde{F}(T,z)\zeta(T)^z$$

and finally applying Lemma 3.2 as above in order to obtain an analogue of Theorem 3.1, namely

$$\rho_k(n) = \frac{q^n}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(\widetilde{G}\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

uniformly for all $n \geq 2$ and $1 \leq k \leq A \log n$ where $\widetilde{G}(z) = \frac{\widetilde{F}(1/q,z)}{\Gamma(1+z)}$.

3.3 The Sathé–Selberg formula in arithmetic progressions

We now follow a broadly similar strategy, but with Dirichlet L-functions, in order to count polynomials in arithmetic progressions. In the next section, we will see how this can then be used to count irreducible polynomials from a "short interval".

Let $d \in \mathcal{M}$ be some polynomial of degree $m \geq 1$. Consider the Dirichlet characters $\chi : (\mathbb{F}_q[t]/(d))^\times \longrightarrow \mathbb{C}^\times$, with χ_0 being the principal character, and let

$$L(T,\chi) = \sum_{f\in\mathcal{M}} \chi(f)T^{\deg f} = \prod_{p\in\mathcal{P}}(1-\chi(p)T^{\deg p})^{-1}$$

be the L-function associated to χ. For $\chi \neq \chi_0$, it known that $L(T,\chi)$ is a polynomial of degree at most $m-1$ that can be factored as

$$L(T,\chi) = \prod_{j=1}^{m-1}(1-\alpha_j T) \tag{3.3}$$

such that $|\alpha_j| = 0, 1$ or $\sqrt{q}$. This is a consequence of Weil's Theorem (the Riemann hypothesis for curves $\mathbb{F}_q$). See for example Proposition 4.3 from [33].

Using (3.3), we can define $L(T,\chi)^z$ for complex numbers z as

$$L(T,\chi)^z = \exp\left(z\sum_{j=1}^{m-1}\log(1-\alpha_i T)\right) \text{ for } |T| < 1/q$$

where log is defined on the set $\mathbb{C}\backslash[0,-\infty)$ and takes real values on the positive reals.

Our first task is to relate the coefficients of $\zeta(T)^z$ and $L(T,\chi)^z$. Consider the following identities which follow from the binomial theorem,

$$\zeta(T)^z = \prod_{p\in\mathcal{P}}(1-T^{\deg p})^{-z} = \prod_{p\in\mathcal{P}}\left(1+\sum_{k\geq 1}\binom{z+k-1}{k}T^{k\deg p}\right)$$

$$L(T,\chi)^z = \prod_{p\in\mathcal{P}} (1-\chi(p)T^{\deg p})^{-z} = \prod_{p\in\mathcal{P}} \left(1 + \sum_{k\geq 1} \binom{z+k-1}{k} \chi(p^k) T^{k\deg p}\right).$$

We see that if $d_z(f)$ is the multiplicative function defined on irreducible powers p^k as $d_z(p^k) = \binom{z+k-1}{k}$ then $\zeta(T)^z = \sum_{f\in\mathcal{M}} d_z(f)T^{\deg f}$ and $L(T,\chi)^z = \sum_{f\in\mathcal{M}} d_z(f)\chi(f)T^{\deg f}$. Hence, $D_z(n,\chi) := \sum_{f\in\mathcal{M}_n} d_z(f)\chi(f)$ is the coefficient of T^n in $L(T,\chi)^z$.

3.3.1 Generalised divisor sums twisted by non-principal characters

Proposition 3.3. *For $\chi \neq \chi_0$, $|z| \leq A$ and $n \geq 1$*

$$|D_z(n,\chi)| \leq q^{n/2} \binom{n+Am-(A+1)}{n} \leq q^{n/2} \binom{n+Am}{n}.$$

Proof. From (3.3) and the binomial theorem we get

$$L(T,\chi)^z = \prod_{j=1}^{m-1} (1-\alpha_j T)^z = \sum_{n\geq 0} \left(\sum_{r_1+\cdots+r_{m-1}=n} \binom{z}{r_1} \cdots \binom{z}{r_{m-1}} \alpha_1^{r_1} \cdots \alpha_{m-1}^{r_{m-1}} \right) (-1)^n T^n.$$

Using that $|\alpha_j| \leq \sqrt{q}$ and $|z| \leq A$ we get that

$$\begin{aligned} |D_z(n,\chi)| &= \left| \sum_{r_1+\cdots+r_{m-1}=n} \binom{z}{r_1} \cdots \binom{z}{r_{m-1}} \alpha_1^{r_1} \cdots \alpha_{m-1}^{r_{m-1}} \right| \\ &\leq \sum_{r_1+\cdots+r_{m-1}=n} \left|\binom{z}{r_1}\right| \cdots \left|\binom{z}{r_{n-1}}\right| \sqrt{q}^{r_1+\cdots+r_{m-1}} \\ &\leq q^{n/2} \sum_{r_1+\cdots+r_{m-1}=n} \binom{A+r_1-1}{r_1} \cdots \binom{A+r_{m-1}-1}{r_{m-1}}. \end{aligned}$$

Now, we recognise the sum as the coefficient of T^n in the expansion of

$$((1-T)^{-A})^{m-1} = (1-T)^{-A(m-1)}$$

which is also $\binom{n+A(m-1)-1}{n} = \binom{n+Am-(A+1)}{n}$. Indeed, this shows that the power series expansion of $L(T,\chi)^z$ is majorised by that of $(1-\sqrt{q}T)^{-A(m-1)}$. Since $m,n \geq 1$ we get that

$$|D_z(n,\chi)| \leq q^{n/2} \binom{n+Am-(A+1)}{n} \leq q^{n/2} \binom{n+Am}{n}. \quad \square$$

3.3.2 Formulae for $\pi_k(n, \chi)$

We are now interested in π_k twisted by a character, that is, the following sum

$$\pi_k(n, \chi) := \sum_{\substack{f \in \mathcal{M}_n \\ \omega(f)=k}} \mu^2(f)\chi(f).$$

We shall embark on a more refined study of this sum in the next chapter but for now, we show how to adapt the proofs from Section 3.2 to prove Theorems 3.2 and 3.3.

In particular, we make use of the generating function

$$A(T, z, \chi) := \sum_{f \in \mathcal{M}} \mu^2(f) z^{\omega(f)} \chi(f) T^{\deg f} = \prod_{p \in \mathcal{P}} (1 + z\chi(p) T^{\deg p})$$

whose power series coefficients are

$$A_z(n, \chi) := \sum_{f \in \mathcal{M}_n} \mu^2(f)\chi(f) z^{\omega(f)}$$

so that, similarly to before,

$$\sum_{k \geq 0} \pi_k(n, \chi) z^k = A_z(n, \chi)$$

and by Cauchy's Theorem

$$\pi_k(n, \chi) = \frac{1}{2\pi i} \oint \frac{A_z(n, \chi)}{z^{k+1}} dz.$$

Moreover, recall that we had

$$F(T, z) = \sum_{f \in \mathcal{M}} b_z(f) T^{\deg f} = \prod_{p \in \mathcal{P}} (1 + zT^{\deg p})(1 - T^{\deg p})^z = A(T, z)\zeta(T)^{-z}$$

so we naturally define $F(T, z, \chi)$ by

$$F(T, z, \chi) := \sum_{f \in \mathcal{M}} b_z(f)\chi(f) T^{\deg f} = \prod_{p \in \mathcal{P}} (1 + \chi(p) z T^{\deg p})(1 - \chi(p) T^{\deg p})^z = A(T, z, \chi) L(T, \chi)^{-z}$$

and let $B_z(n, \chi) := \sum_{f \in \mathcal{M}_n} b_z(f)\chi(f)$ so that $A_z(m, \chi) = \sum_{a+b=m} B_z(a, \chi) D_z(b, \chi)$.

3.3.2.1 Non-principal characters

In this subsection χ will be a non-principal character.

Lemma 3.3. *For $|z| \leq A$ and $n \geq 2$*

$$\sum_{0 \leq a \leq n} \frac{|B_z(a,\chi)|}{q^{a/2}} \leq n^{C_A}$$

where C_A is a constant depending only on A.

Proof. Since

$$\sum_{0 \leq a \leq n} \frac{|B_z(a,\chi)|}{q^{a/2}} \leq \sum_{f \in \mathcal{M}_{\leq n}} \frac{|b_z(f)|}{q^{\deg f/2}}$$

this follows directly from the proof of Proposition 3.2. □

We can use this to get an estimate for $A_z(n,\chi)$ as follows:

Proposition 3.4. *For $A > 1$ and $n \geq 2$*

$$|A_z(n,\chi)| \leq q^{n/2} \binom{n+Am}{n} n^{C_A}.$$

Proof. Using Proposition 3.3 and Lemma 3.3 we get

$$\begin{aligned} |A_z(n;\chi)| &= \left| \sum_{0 \leq a \leq n} B_z(a,\chi) D_z(n-a,\chi) \right| \\ &\leq q^{n/2} \sum_{0 \leq a \leq n} \frac{|B_z(a,\chi)|}{q^{a/2}} \binom{n-a+Am}{n-a} \\ &\leq q^{n/2} \binom{n+Am}{n} \sum_{0 \leq a \leq n} \frac{|B_z(a,\chi)|}{q^{a/2}} \leq q^{n/2} \binom{n+Am}{n} n^{C_A}. \end{aligned}$$

□

We can now use Cauchy's Theorem to bound $\pi_k(m;\chi)$.

Proposition 3.5. *For $A > 1$ and $n \geq 2$*

$$|\pi_k(n;\chi)| \leq q^{n/2} \binom{n+Am}{n} n^{C_A}.$$

Proof. Recall the identity

$$\pi_k(n;\chi) = \frac{1}{2\pi i} \oint \frac{A_z(n;\chi)}{z^{k+1}} dz$$

where we take the contour to be the circle of radius $r = 1$ centred at 0.

Then Proposition 3.4 gives us that this is

$$\leq q^{n/2}\binom{n+Am}{n}n^{C_A}\frac{1}{2\pi}\oint\frac{|dz|}{|z|^{k+1}} \leq q^{n/2}\binom{n+Am}{n}n^{C_A}. \quad \square$$

3.3.2.2 The principal character

Define F_d, B_z^d and b_z^d via the following formal power series identities

$$F_d(T,z) = \sum_{n\geq 0} B_z^d(n)T^n = \sum_{f\in\mathcal{M}} b_z^d(f)T^{\deg f} = \prod_{p\nmid d}(1+zT^{\deg p})(1-T^{\deg p})^z\prod_{p|d}(1-T^{\deg p})^z.$$

Lemma 3.4. *For $|z|\leq A$ and $\sigma\geq\frac{2}{3}$*

$$\sum_{a\geq 0}\frac{|B_z^d(a)|}{q^{\sigma a}} \ll_A \prod_{p|d}(1-q^{-\sigma\deg p})^{-A}.$$

Proof. By making a change of variable $S = T^{\deg p}$, we see that the multiplicative coefficients $b_z^d(f)$ are defined on prime powers $f = p^k$ by the formal power series identity

$$1+\sum_{k\geq 1} b_z^d(p^k)S^k = \begin{cases}(1-S)^z & \text{if } p|d\\ (1+zS)(1-S)^z & \text{if } p\nmid d.\end{cases}$$

So if $p|d$, we have that $|b_z^d(p^k)| = |\binom{z}{k}| \leq \binom{A+k-1}{k}$, and if $p\nmid d$ we have that $b_z^d(p^k) = b_z(p^k)$. Therefore, we get

$$\begin{aligned}\sum_{a\geq 0}\frac{|B_z^d(a)|}{q^{\sigma a}} &\leq \sum_{f\in\mathcal{M}}\frac{|b_z^d(f)|}{q^{\sigma\deg f}}\\ &\leq \prod_{p|d}\left(1+\sum_{k\geq 1}\frac{|b_z^d(p^k)|}{q^{k\sigma\deg p}}\right)\prod_{p\nmid d}\left(1+\sum_{k\geq 1}\frac{|b_z^d(p^k)|}{q^{k\sigma\deg p}}\right)\\ &\leq \prod_{p|d}\left(\sum_{k\geq 0}\binom{A+k-1}{k}q^{-k\sigma\deg p}\right)\prod_{p\in\mathcal{P}}\left(1+\sum_{k\geq 1}\frac{|b_z(p^k)|}{q^{k\sigma\deg p}}\right)\\ &= \prod_{p|d}(1-q^{-\sigma\deg p})^{-A}\sum_{f\in\mathcal{M}}\frac{|b_z(f)|}{q^{\sigma\deg f}}.\end{aligned}$$

Now, by the proof of Proposition 3.2, $\sum_{f\in\mathcal{M}}\frac{|b_z(f)|}{q^{\sigma\deg f}} \ll_A 1$ for $\sigma\geq\frac{2}{3}$, which gives the result. $\square$

Lemma 3.5. *For $d \in \mathbb{F}_q[t]$ of degree $m \geq 1$ and $1 \geq \sigma > \frac{1}{2}$, we have*

$$\prod_{p|d}(1-q^{-\sigma \deg p})^{-1} \leq (2+2\log m)^{8(qm)^{1-\sigma}}.$$

Proof. Arrange the primes $p_1, \dots, p_r$ dividing d and the primes $P_1, P_2, \dots$ in $\mathcal{M}$, in order of degree (where you can order those of the same degree arbitrarily). Then we must have that $\deg P_i \leq \deg p_i$. Now, for some $N \in \mathbb{N}$, we have that $\sum_{\deg P \leq N-1} \deg P < m \leq \sum_{\deg P \leq N} \deg P$. This means that d has at most $\#\{P : \deg P \leq N\}$ prime factors, and so

$$\prod_{p|d}(1-q^{-\sigma \deg p})^{-1} \leq \prod_{\deg P \leq N}(1-q^{-\sigma \deg P})^{-1}.$$

Taking the logarithm of the right hand side, and using the fact that $-\log(1-\frac{1}{x}) \leq \frac{1}{x-1}$ for $x > 1$, combined with the prime polynomial theorem, we get

$$\begin{aligned}\sum_{\deg P \leq N} -\log(1-q^{-\sigma \deg p}) &\leq \sum_{r \leq N} \frac{\pi(r)}{q^{\sigma r}-1} \\ &\leq 4\sum_{r \leq N} \frac{\pi(r)}{q^{\sigma r}} \leq 4\sum_{r \leq N} \frac{q^{(1-\sigma)r}}{r} \leq 8q^{(1-\sigma)N}(\log(1+N)).\end{aligned}$$

Our choice of N tells us that $q^N \leq qm$ (so $N \leq (1+2\log m)$), since we have from the prime polynomial theorem

$$m > \sum_{\deg P \leq N-1} \deg P = \sum_{r \leq N-1} \pi(r) r \geq \sum_{r | N-1} \pi(r) r = q^{N-1}.$$

Putting everything together we get that

$$\prod_{p|d}(1-q^{-\sigma \deg p})^{-1} \leq \exp(8q^{(1-\sigma)N}(\log(1+N))) \leq (2+2\log m)^{8(qm)^{1-\sigma}}. \quad \square$$

Proposition 3.6. *For $|z| \leq A$ we have that*

$$\sum_{a \geq 0} \frac{|B_z^d(a)|}{q^a} a^{2A+2} \ll_A (1+\log m)^{K_A}$$

where K_A is a constant depending on A.

Proof. When $\log m < 10A + 10$ it suffices to show that $\sum_{a \geq 0} \frac{|B_z^d(a)|}{q^a} a^{2A+2} \ll_A 1$.

This is indeed true in this case, since $m \ll_A 1$, and so by Lemma 3.4 we have that for $\sigma \geq \frac{2}{3}$

$$\sum_{a\geq 0} \frac{|B_z^d(a)|}{q^{\sigma a}} \ll_{A,\sigma} \prod_{p|d}(1-q^{-\sigma \deg p})^{-A} \ll_{A,\sigma} (1-q^{-\sigma})^{-Am} \ll_{A,\sigma} 1$$

and consequently that $\sum_{a\geq 0} \frac{|B_z^d(a)|}{q^a} a^{2A+2} \ll_A 1$.

When $\log m \geq 10A+10$, let $\tau = \frac{2A+2}{\log m \log q} \leq \frac{1}{5\log 2} \leq \frac{1}{3}$ so that $1-\tau \geq \frac{2}{3}$ and moreover

$$a \geq (\log m)^2 \implies (2A+2)\frac{\log a}{a} \leq (2A+2)\frac{2\log\log m}{(\log m)^2} \leq \frac{2A+2}{\log m} = \tau \log q \implies a^{2A+2} \leq q^{\tau a}.$$

So overall we have that $a^{2A+2} \leq (\log m)^{4A+4} q^{\tau a}$. Using this fact and Lemmas 3.4 and 3.5 we get that

$$\begin{aligned}
\sum_{a\geq 0} \frac{|B_z^d(a)|}{q^a} a^{2A+2} &\leq (\log m)^{4A+4} \sum_{a\geq 0} \frac{|B_z^d(a)|}{q^{(1-\tau)a}} \\
&\ll_A (\log m)^{4A+4} \prod_{p|d}(1-q^{-(1-\tau)\deg p})^{-A} \\
&\ll_A (\log m)^{4A+4} (2(1+\log m))^{8(qm)^\tau} \\
&\ll_A (1+\log m)^{K_A}.
\end{aligned}$$

□

Proposition 3.7. *Uniformly for $|z| \leq A$ and $n \geq 1$, we have*

$$\begin{aligned}
A_z(n,\chi_0) &= q^n \frac{n^{z-1}}{\Gamma(z)} F_d(1/q,z) + O_A(q^n n^{\Re z - 2}(1+\log m)^{K_A}) \\
&= \left(\prod_{p|d}\left(1+\frac{z}{q^{\deg p}}\right)^{-1}\right) F(1/q,z) q^n \frac{n^{z-1}}{\Gamma(z)} + O_A(q^n n^{\Re z-2}(1+\log m)^{K_A}).
\end{aligned}$$

Proof. The first equality follows from the proof of Proposition 3.1 (carrying throughout an additional factor of $(1+\log m)^{K_A}$ in the error term) and Proposition 3.6 after noting that

$$\begin{aligned}
A(T,z,\chi_0) &= \prod_{p\in\mathcal{P}}(1+z\chi(p)T^{\deg p}) \\
&= \zeta(T)^z \prod_{p\nmid d}(1+zT^{\deg p})(1-T^{\deg p})^z \prod_{p|d}(1-T^{\deg p})^z = \zeta(T)^z F_d(T,z).
\end{aligned}$$

The second equality follows from the observation that

$$F_d(T,z) = \prod_{p\in\mathcal{P}}(1+zT^{\deg p})(1-T^{\deg p})^z \prod_{p|d}(1+zT^{\deg p})^{-1} = F(T,z)\prod_{p|d}(1+zT^{\deg p})^{-1}. \quad \square$$

We now turn to the proof of the main result of this subsection.

Proposition 3.8. *Let* $G_d(z) = \frac{F(1/q,z)}{\Gamma(1+z)}\prod_{p|d}\left(1+\frac{z}{q^{\deg p}}\right)^{-1}$. *Then for Let* $A > 1$ *and* $\sqrt{n} \geq (1+\log m)^{K_A}$ *we have*

$$\pi_k(n,\chi_0) = \frac{q^n}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

uniformly for all $n \geq 2$ *and* $1 \leq k \leq A\log n$.

Proof. For $|z| \leq A$, by Proposition 3.7 and our condition on n,

$$A_z(n,\chi_0) = \left(\prod_{p|d}\left(1+\frac{z}{q^{\deg p}}\right)^{-1}\right)\frac{F(1/q,z)}{\Gamma(z)}q^n n^{z-1} + O_A(q^n n^{\Re z - 3/2}).$$

We may therefore apply Proposition 3.2 with $a = 1$ and $c_k(n) = n\pi_{k+1}(n,\chi_0)/q^n$ and $p_n(z) = \frac{n}{q^n}\sum_{k\geq 0}\pi_{k+1}(n,\chi_0)z^k = \frac{n}{q^n}zA_z(n,\chi_0)$. The result then follows with $G_d(z)$ as stated. $\square$

3.3.3 Proof of Theorem 3.2

We are now ready to put the pieces together and present the proof of Theorem 3.2.

Proof. Using the orthogonality of characters,

$$\sum_{\substack{f\in\mathcal{M}_n \\ f\equiv g \bmod d}} 1 = \frac{1}{\phi(d)}\sum_{f\in\mathcal{M}_n}\sum_{\chi}\bar{\chi}(g)\chi(f)$$

where the sum is over characters $\chi : (\mathbb{F}_q[t]/(d))^\times \to \mathbb{C}^\times$ and $\phi(d) = \left|(\mathbb{F}_q[t]/(d))^\times\right|$, we get

that

$$\begin{aligned}
\pi_k(n;g,d) &= \sum_{\substack{f\in\mathcal{M}_n\\ f\equiv g \bmod d\\ \omega(f)=k}} \mu^2(f)\\
&= \frac{1}{\phi(d)}\sum_{\chi}\bar{\chi}(g)\pi_k(n,\chi)\\
&= \frac{1}{\phi(d)}\pi_k(n,\chi_0) + O\left(\frac{1}{\phi(d)}\sum_{\chi\neq\chi_0} q^{n/2}\binom{n+Am}{n}n^{C_A}\right)\\
&= \frac{1}{q^m\prod_{p|d}(1-\frac{1}{q^{\deg p}})}\frac{q^n}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right)+O_A\left(\frac{k}{(\log n)^2}\right)\right)\\
&\qquad + O\left(q^{n/2}\binom{n+Am}{n}n^{C_A}\right)\\
&= \left(\prod_{p|d}\left(1-\frac{1}{q^{\deg p}}\right)^{-1}\right)\frac{q^{n-m}}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right)+O_A\left(\frac{k}{(\log n)^2}\right)\right)\\
&\qquad + O\left(q^{n/2}\binom{n+Am}{n}n^{C_A}\right)
\end{aligned}$$

where we have used Proposition 3.3 in the third line and Proposition 3.8 in the fourth line. Note that the condition $\left(\frac{1}{2}-\frac{1+\log(1+\frac{A}{2})}{\log q}\right)n \geq m$ certainly implies the condition $\sqrt{n} \gg_A (1+\log m)^{K_A}$ required to apply Proposition 3.8.

To finish the proof we shall show that the second error term can be absorbed into the first using the Stirling inequalities $\sqrt{2\pi}n^{n+1/2}e^{-n} \leq n! \leq en^{n+1/2}e^{-n}$. For $a,b\geq 1$ we have

$$\begin{aligned}
\binom{a+b}{a} = \frac{(a+b)!}{a!b!} &\leq \frac{e(a+b)^{a+b+1/2}e^{-(a+b)}}{2\pi a^{a+1/2}b^{b+1/2}e^{-(a+b)}}\\
&\leq \frac{e}{2\pi}\left(\frac{1}{a}+\frac{1}{b}\right)^{1/2}\left(1+\frac{b}{a}\right)^a\left(1+\frac{a}{b}\right)^b \leq \left(1+\frac{b}{a}\right)^a\left(1+\frac{a}{b}\right)^b
\end{aligned}$$

and using this and the condition $\left(\frac{1}{2}-\frac{1+\log(1+\frac{A}{2})}{\log q}\right)n \geq m$ we have

$$\begin{aligned}
q^{n/2}\binom{n+Am}{n}n^{C_A+2} &\leq q^{n/2}\binom{n+\frac{A}{2}n}{n}n^{C_A+2}\\
&\leq q^{n/2}\left(1+\frac{A}{2}\right)^n\left(1+\frac{2}{A}\right)^{\frac{A}{2}n}n^{C_A+2} \ll_A q^{n/2}\left(1+\frac{A}{2}\right)^n e^n \leq q^{n-m}.
\end{aligned}$$

From this, we then get that

$$\pi_k(n;g,d) = \left(\prod_{p|d}\left(1-\frac{1}{q^{\deg p}}\right)^{-1}\right)\frac{q^{n-m}}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right)+O_A\left(\frac{k}{(\log n)^2}\right)\right)$$
$$= \frac{1}{\phi(d)}\frac{q^n}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right)+O_A\left(\frac{k}{(\log n)^2}\right)\right). \qquad \square$$

Remark. Note that the conclusion of Theorem 3.2 can be stated in the equivalently as

$$\pi_k(n;g,d) = \left(\prod_{p|d}\left(1-\frac{1}{q^{\deg p}}\right)^{-1}\right)\frac{q^{n-m}}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(G_d\left(\frac{k-1}{\log n}\right)+O_A\left(\frac{k}{(\log n)^2}\right)\right). \tag{3.4}$$

3.4 The Sathé–Selberg formula in short intervals

3.4.1 The Involution of a polynomial

As in [18], we define the *involution* of a polynomial $f \in \mathbb{F}_q[t]$ to be the polynomial

$$f^*(t) := t^{\deg f} f(1/t).$$

The idea that such an involution links arithmetic progressions and short intervals goes back at least to Hayes' paper[16].

Lemma 3.6. *For $f \in \mathbb{F}_q[t]$ not divisible by t, $\omega(f^*) = \omega(f)$ and $\mu(f^*) = \mu(f)$.*

Proof. First of all, we note that for $f, g \in \mathbb{F}_q[t]$

$$(fg)^*(t) = t^{\deg fg} fg(1/t) = t^{\deg f} f(1/t) t^{\deg g} g(1/t) = f^*(t)g^*(t).$$

Moreover, if $f \in \mathbb{F}_q[t]$ is not divisible by t, then $\deg f^*(t) = \deg f(t)$ so

$$(f^*)^*(t) = t^{\deg f^*} f^*(1/t) = t^{\deg f^*} t^{-\deg f} f(t) = f(t).$$

Together, these imply that if $f = p_1^{a_1} \cdots p_r^{a_r} \in \mathbb{F}_q[t]$ where p_i are distinct irreducibles none of which are t, then $f^* = (p_1^*)^{a_1} \cdots (p_r^*)^{a_r}$ where p_i^* are distinct irreducibles none of which are t. So, if $f \in \mathbb{F}_q[t]$ is not divisible by t, then $\omega(f^*) = \omega(f)$ and $\mu(f^*) = \mu(f)$. $\square$

The following observation is what allows us to use our result concerning polynomials from an arithmetic progression, namely (3.4), to prove one about polynomials belonging

to a short interval.

Lemma 3.7. *Let f and g be polynomials of degree n and h an integer $\leq n$. Then* $\deg(f-g) \leq h$ *if and only if* $f^* \equiv g^* \mod t^{n-h}$.

Proof. Write

$$f(t) = a_n t^n + \cdots + a_h t^h + \cdots + a_0$$

$$g(t) = b_n t^n + \cdots + b_h t^h + \cdots + b_0$$

where a_n and b_n are non-zero. Then

$$f^*(t) = a_n + \cdots + a_h t^{n-h} + \cdots + a_0 t^n$$

$$g^*(t) = b_n + \cdots + b_h t^{n-h} + \cdots + b_0 t^n.$$

From this we can see that each condition is satisfied if and only if $a_i = b_i$ for each $i = h+1, \ldots, n$. □

Notice that f^* and g^* have non-zero constant terms.

3.4.2 Proof of Theorem 3.3

We first split the sum defining $\pi_k(n; g; h)$ into two

$$\pi_k(n;g;h) = \sum_{\substack{f\in\mathcal{M}_n \\ \deg(f-g)\leq h \\ \omega(f)=k}} \mu^2(f) = \sum_{\substack{f\in\mathcal{M}_n \\ \deg(f-g)\leq h \\ \omega(f)=k \\ f(0)\neq 0}} \mu^2(f) + \sum_{\substack{f\in\mathcal{M}_n \\ \deg(f-g)\leq h \\ \omega(f)=k \\ f(0)=0}} \mu^2(f).$$

Using Lemma 3.7 on the first sum we get

$$\begin{aligned}\sum_{\substack{f\in\mathcal{M}_n \\ f^*\equiv g^* \bmod t^{n-h} \\ \omega(f^*)=k \\ \deg f^*=n}} \mu^2(f^*) &= \sum_{\substack{\deg f=n \\ f\equiv g^* \bmod t^{n-h} \\ \omega(f)=k}} \mu^2(f) \\ &= \sum_{a\in\mathbb{F}_q^*} \sum_{\substack{f\in\mathcal{M}_n \\ f\equiv a^{-1}g^* \bmod t^{n-h} \\ \omega(f)=k}} \mu^2(f) \\ &= \sum_{a\in\mathbb{F}_q^*} \pi_k(n; a^{-1}g^*, t^{n-h}).\end{aligned}$$

Since $a^{-1}g^*$ has non-zero constant term for each $a \in \mathbb{F}_q^*$, and from the condition of the theorem we have that $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n > n - h \geq 1$, so we may apply (3.4) to get

$$\begin{aligned}
&(q-1)\frac{q}{q-1}\frac{q^h}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(H\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right) \\
&= \frac{q^{h+1}}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(H\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right).
\end{aligned}$$

Now, we split the second sum into two sums, the latter of which is zero, and then apply Lemma 3.7 to the former

$$\begin{aligned}
\sum_{\substack{f\in\mathcal{M}_{n-1}\\ \deg(tf-g)\leq h\\ \omega(tf)=k}} \mu^2(tf) &= \sum_{\substack{f\in\mathcal{M}_{n-1}\\ \deg(tf-g)\leq h\\ \omega(f)=k-1\\ f(0)\neq 0}} \mu^2(tf) + \sum_{\substack{f\in\mathcal{M}_{n-1}\\ \deg(tf-g)\leq h\\ \omega(f)=k\\ f(0)=0}} \mu^2(tf) \\
&= \sum_{\substack{\deg f = n-1\\ f\equiv g^* \bmod t^{n-h}\\ \omega(f)=k-1}} \mu^2(f) \\
&= \sum_{a\in\mathbb{F}_q^*} \sum_{\substack{f\in\mathcal{M}_{n-1}\\ f\equiv a^{-1}g^* \bmod t^{n-h}\\ \omega(f)=k-1}} \mu^2(f) \\
&= \sum_{a\in\mathbb{F}_q^*} \pi_{k-1}(n-1; a^{-1}g^*, t^{n-h}).
\end{aligned}$$

Since $a^{-1}g^*$ has non-zero constant term and for each $a \in \mathbb{F}_q^*$, and from the condition of the theorem we have $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right)(n-1) \geq n - h \geq 1$, we may apply (3.4) again to get

$$\begin{aligned}
&(q-1)\frac{q}{q-1}\frac{q^{h-1}}{n-1}\frac{(\log(n-1))^{k-2}}{(k-2)!}\left(H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k-1}{(\log(n-1))^2}\right)\right) \\
&= \frac{q^h}{n}\frac{(\log n)^{k-2}}{(k-2)!}\left(H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right) \\
&= \frac{q^{h+1}}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(\frac{k-1}{q\log n}H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right).
\end{aligned}$$

Putting everything together proves Theorem 3.3.

Chapter 4

An application to a race in $\mathbb{F}_q[t]$

In the previous chapter we developed a function field analogue of the Selberg–Delange method and applied it with Dirichlet L-functions to count polynomials with a given number of prime divisors in arithmetic progressions and short intervals. This required bounding certain sums of non-trivial Dirichlet characters. In this chapter we show how a more refined application of the method leads to a better understanding of $\pi_k(n, \chi)$. This would allow for example one to investigate prime number races style questions for products of k irreducible polynomials as is done in [23]. We also exhibit new phenomena concerning Chebyshev-type biases of character sums over polynomials with a very large number of irreducible factors and ask whether the same phenomena holds for integers with a very large number of prime factors.

4.1 Introduction

Let $\chi : \mathbb{F}_q[t] \to \mathbb{C}$ be a non-principal Dirichlet character. In this chapter we are interested in the sum

$$\pi_k(n, \chi) = \sum_{\substack{f \in \mathcal{M}_n \\ \Omega(f)=k}} \chi(f)$$

where $\Omega(f)$ is the number of prime divisors of f counted with multiplicity. The L-function associated to χ is

$$L(u, \chi) := \sum_{f \in \mathcal{M}} \chi(f) u^{\deg f} = \prod_{p \in \mathcal{P}} (1 - \chi(p) u^{\deg p})^{-1}$$

and as we saw in the previous chapter, it is known that $L(u,\chi)$ is a polynomial that can be written as a product of linear factors

$$L(u,\chi) =: (1-\sqrt{q}u)^{m_+}(1+\sqrt{q}u)^{m_-}\prod_{j=1}^{d_\chi}(1-\alpha_j(\chi)u)^{m_j}\prod_{j'=1}^{d'_\chi}(1-\beta_{j'}(\chi)u) \tag{4.1}$$

where $|\beta_{j'}(\chi)|=1$ and $\alpha_j(\chi)=\sqrt{q}e^{i\gamma_j(\chi)}$ is non-real and has absolute value $\sqrt{q}$ (see [23], equation (1)). The α_j are distinct for distinct j and appear with multiplicity m_j. The $\beta_{j'}$ are less important so may be repeated but we don't care about, and have not named, their multiplicities. Our aim in this chapter is to use analytic arguments to relate the quantity $\pi_k(n,\chi)$ to the zeros of $L(u,\chi)$. We are interested in uniformity with respect to the variables n and k so implied constants may depend on anything except n and k (in particular χ and q). It is convenient to use the normalisation

$$\widetilde{\pi_k}(n,\chi) := \pi_k(n,\chi)\frac{n(k-1)!(-1)^k}{q^{n/2}(\log n)^{k-1}}.$$

4.1.1 Brief background on Chebyshev's bias

"There is a notable difference in the splitting of the prime numbers between the two forms $4n+3$ *and* $4n+1$*: the first form contains a lot more than the second."* - Chebyshev 1853.

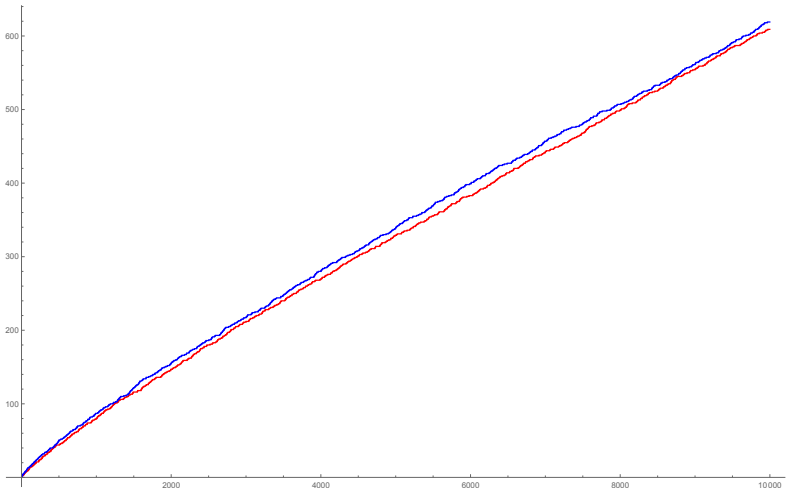


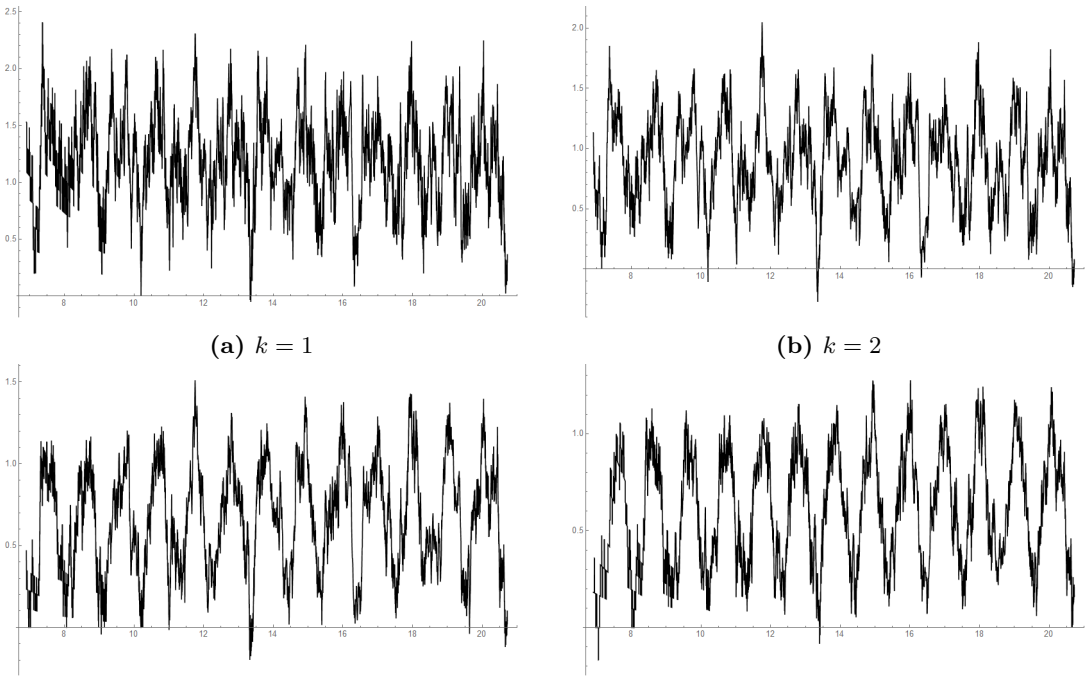
Figure 4.1: Number of primes up to x equal to 1 (red) and 3 (blue) mod 4

Assume for the time being that $L(\pm q^{-1/2},\chi)\neq 0$ and that each zero of $L(u,\chi)$ is simple. The corresponding assumption, that $L(1/2,\chi)\neq 0$ and all zeros are simple, is conjectured to hold for all number field Dirichlet L-functions. Then it follows from the

work of Devin and Meng [23], and Theorems 4.1 and 4.3 below, that for each *fixed* k,

$$\widetilde{\pi_k}(n,\chi) = \mathbf{1}_{\chi^2=\chi_0}\frac{1+(-1)^n}{2^k} + \sum_{\gamma_j\neq 0,\pi} e^{in\gamma_j} + O_k\left(\frac{1}{\log n}\right). \tag{4.2}$$

The terms in this formula corresponding to non-real zeros of $L(u,\chi)$ oscillate around 0 as n increases. We can think of the other term as a 'bias' term which biases $\pi_k(n,\chi)$ away from 0. It follows that, if χ is real then for each fixed k, the quantity $(-1)^k\pi_k(n,\chi)$ is biased towards being positive rather than negative, but that "as k increases, the biases become smaller and smaller"–[23]. The results of this chapter include and generalise (4.2) to $k(n)$ varying with n. We shall see that the bias term does indeed tend to 0 for certain sequences $k(n)\to\infty$, but, perhaps surprisingly, not if $k(n)$ grows too quickly. In particular, there is a constant $\gamma\approx 1.2021\ldots$ such that if $\gamma < k/\log n < \sqrt{q}$, then the bias term is larger than the oscillating terms for every large even n.



(a) $k=1$ **(b)** $k=2$

(c) $k=3$ **(d)** $k=4$

Figure 4.2: Chebyshev bias of $\widetilde{\pi_k^{\text{int}}}(x)$ for x up to 10^9

In the case that $k=1$, the integer analogue of the explicit formula (4.2) has a corresponding bias term that is responsible for the phenomena known as *Chebyshev's bias*, illustrated in Figure 4.1. Chebyshev's observation was formalised by Rubenstein and Sarnak [34] who proved, given certain conjectures on the zeros of Dirichlet L-functions,

that, if

$$S_k = \left\{ x \in \mathbb{N} \,:\, (-1)^k \sum_{\substack{n \le x \\ \Omega(n)=k}} \chi(n) > 0 \right\}$$

where χ is the non-trivial Dirichlet character mod 4, then the set S_1 has logarithmic density ≈ 0.996. Figure 4.2 shows the plots of the normalised character sum

$$\widetilde{\pi_k^{\text{int}}}(x) = \frac{(-1)^k (k-1)! \log x}{\sqrt{x} (\log\log x)^{k-1}} \sum_{\substack{n \le x \\ \Omega(n)=k}} \chi(n).$$

The phenomena has since been extensively studied and generalised in a number of directions. See [14] for an introduction to the topic. Ford and Sneed [13] proved, again under certain conjectures on the zeros of $L(s,\chi)$, that the set S_2 has logarithmic density ≈ 0.894. A more general theorem capturing the Chebyshev bias for fixed $k \ge 1$ was proved for integers by Meng [22] and for polynomials by Devin and Meng [23]. For example, it follows from [22] and standard conjectures on the zeros of Dirichlet L-functions that the set S_k has logarithmic density δ_k where $1/2 < \delta_k < 1$ and $\delta_k \to 1/2$ as $k \to \infty$. This suggests that in some sense the bias dissipates as $k \to \infty$. However, we shall see that, for polynomials and $k(n)$ increasing with n, sometimes the bias is strong enough to ensure that $(-1)^k \pi_k(n,\chi) > 0$ for all large even n.

From now on, χ will always denote a non-principal Dirichlet character modulo a fixed polynomial $d \in \mathbb{F}_q[t]$ and χ_0 will denote the principal character mod d. It may be helpful to bear in mind that for large values of n, the distribution of $\Omega(f)$, given a polynomial f selected uniformly at random from $\mathcal{M}_n$, is approximately normal with mean $\log n$ and standard deviation $\sqrt{\log n}$.

Because the behaviour of $\pi_k(n,\chi)$ depends on whether or not χ is real, we shall present the results for the two cases separately.

4.1.2 When χ is not real

Theorem 4.1. *Suppose $\chi^2 \neq \chi_0$ and let $\epsilon > 0$. With the same notation as in equation (4.1)*

$$\widetilde{\pi_k}(n,\chi) = \sum_{\gamma_j \neq 0,\pi} m_j^k e^{in\gamma_j} + m_+^k + (-1)^n m_-^k + O\left(\frac{k}{\log n} \left(\sum_{\gamma_j \neq 0,\pi} m_j^k + m_+^k + m_-^k \right) \right)$$

uniformly for $1 \leq k \leq q^{1/2-\epsilon} \log n$.

When k is large with respect to n, this improves upon [23, Theorem 5.1] which requires that $k = o(\sqrt{\log n})$ and has an error term involving a factor $(\deg d)^k$ where d is the conductor of χ.

Theorem 4.1 gives a main term and smaller error term in the range $k = o(\log n)$. A more general formula which describes the behaviour of $\widetilde{\pi_k}(n, \chi)$ in the full range $1 \leq k \leq q^{1/2-\epsilon} \log n$ can be extracted from the proof but is significantly more complicated to write down. If we assume certain simplifying assumptions though, we can state the more general formula as follows.

Theorem 4.2. *Assume that* $m_j = 1$ *for each* j *and that* $m_\pm = 0$. *Suppose* $k(n)$ *is a sequence tending to infinity as* $n \to \infty$ *such that* $\alpha = \lim_{n\to\infty} \frac{k}{\log n}$ *exists and* $0 < \alpha < q^{1/2}$. *Then there exist non-zero constants* $h_j(\alpha)$ *such that*

$$\widetilde{\pi_k}(n, \chi) = \sum_{\gamma_j \neq 0, \pi} h_j(\alpha) e^{in\gamma_j} + o(1).$$

Remark. The coefficients $h_j(\alpha)$ are explicitly defined in terms of α and χ in the course of the proof but are quite lengthy to write down in full. An even more general formula that does not require $\lim_{n\to\infty} \frac{k}{\log n}$ to exist can be extracted form the proof but is more complicated to write down.

4.1.3 When χ is real

The next two theorems both show how the behaviour of $\pi_k(n, \chi)$ differs significantly when χ is real. The first deals with 'small' values of k and again extends the range of a formula given in [23].

Theorem 4.3. *Suppose* $\chi^2 = \chi_0$. *With the same notation as in equation (4.1), uniformly for* $1 \leq k \leq (\log n)^{1/2}$ *we have*

$$\widetilde{\pi_k}(n, \chi) = \sum_{\gamma_j \neq 0, \pi} m_j^k e^{in\gamma_j} + (m_+ + 1/2)^k + (-1)^n (m_- + 1/2)^k + O\left(\frac{k}{\log n} \sum_{\gamma_j \neq 0, \pi} m_j^k + \frac{k^2}{\log n} \max_{\pm} \left\{ (m_\pm + 1/2)^k \right\} \right).$$

Moreover, uniformly in the range $1 \le k \le (\log n)^{2/3}$ *we have*

$$\widetilde{\pi_k}(n,\chi) = \sum_{\gamma_j \neq 0,\pi} m_j^k e^{in\gamma_j} + (m_+ + 1/2)^k e^{\frac{(k-1)^2}{2(m_+ + 1/2)^2 \log n}} + (-1)^n (m_- + 1/2)^k e^{\frac{(k-1)^2}{2(m_- + 1/2)^2 \log n}} + O\left(\frac{k}{\log n} \sum_{\gamma_j \neq 0,\pi} m_j^k + \left(\frac{1}{k} + \frac{k^3}{(\log n)^2} \right) \max_{\pm} \left\{ (m_\pm + 1/2)^k e^{\frac{(k-1)^2}{2(m_\pm + 1/2)^2 \log n}} \right\} \right).$$

Notice that the error terms in the formulae above are essentially the same as the corresponding main terms but with certain extra factors involving k and $\log n$. It is not too difficult to see that these extra factors are $o(1)$ in the first formula if $k = o(\sqrt{\log n})$. They are $o(1)$ in the second if $k \to \infty$ and $k = o((\log n)^{2/3})$. The change in behaviour and appearance of extra terms for k around $\sqrt{\log n}$ may explain why [23, Theorem 5.1] required $k = o(\sqrt{\log n})$. The significance of the threshold k around $(\log n)^{2/3}$ will become apparent from the proof.

If we make the same simplifying assumptions as in Theorem 4.2, that is, the limit $\lim_{n\to} \frac{k}{\log n}$ exists and $m_j = 1$, $m_\pm = 0$, then we get a corresponding version for real χ that includes the bias term. The size of the bias term can be described in terms of the continuous function $b(\alpha)$ defined by

$$b(\alpha) = \alpha \left(\frac{s(\alpha) - 1}{2} - \log(2s(\alpha)) \right), \quad \text{where} \quad s(\alpha) = \frac{1}{8\alpha} \left(\sqrt{1 + 16\alpha} - 1 \right). \tag{4.3}$$

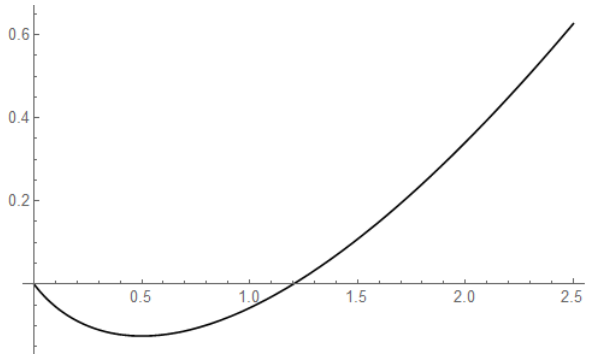


Figure 4.3: Plot of $b(\alpha)$

Of particular significance is the fact that, if the real constants $\beta \approx 0.3637\ldots$ and

$\gamma \approx 1.2021\ldots$ are defined by the two equations

$$e^{\beta-1} = 4\beta^2 \qquad \text{and} \qquad \gamma = \frac{1-\beta}{4\beta^2},$$

then $b(\alpha) < 0$ for $0 < \alpha < \gamma$ and $b(\alpha) > 0$ for $\alpha > \gamma$.

Theorem 4.4. *Suppose $\chi^2 = \chi_0$. Assume that $m_j = 1$ for each j and that $m_\pm = 0$. Suppose $k(n)$ is a sequence tending such that $\alpha = \lim_{n\to\infty} \frac{k}{\log n}$ exists and $0 < \alpha < q^{1/2}$. Then there exist non-zero constants $h_j(\alpha)$ and positive constants $h_\pm(\alpha) > 0$ such that*

$$\widetilde{\pi_k}(n,\chi) = \{h_+(\alpha) + (-1)^n h_-(\alpha) + o(1)\}\, n^{b((k-1)/\log n)} + \sum_{\gamma_j \neq 0,\pi} h_j(\alpha) e^{in\gamma_j} + o(1).$$

Remark. It follows that the oscillating terms dominate if $0 < \alpha < \gamma$, but that the bias terms dominate if $\gamma < \alpha < q^{1/2}$, at least if n is even. This is perhaps surprising given the results in [22] and [23], which, as explained in section 4.1.1 above, suggest that in some sense "as k increases, the biases become smaller and smaller". Since the conditions we assumed on the zeros of $L(u,\chi)$ are conjectured to hold for number field Dirichlet L-functions, we wonder whether something analogous happens in the number field setting.

Remark. The remark following Theorem 4.3 concerning the coefficients $h_j(\alpha)$ applies verbatim to the coefficients $h_j, h_\pm$ here.

4.2 A Selberg–Delange type argument

Let $A > 0$ and u and z be complex variables satisfying $|z| \leq A$ and $|zu| < 1$. The crucial identity for the proof is the following

$$G_z(u,\chi) := \sum_f \chi(f) z^{\Omega(f)} u^{\deg f} = L(u,\chi)^z L(u^2,\chi^2)^{\frac{z(z-1)}{2}} E_z(u,\chi) \tag{4.4}$$

where

$$E_z(u,\chi) = \prod_p \left(1-\chi(p)zu^{\deg p}\right)^{-1} \left(1-\chi(p)u^{\deg p}\right)^{z} \left(1-\chi^2(p)u^{2\deg p}\right)^{\frac{z(z-1)}{2}}$$

is holomorphic for $|u| < \min\{|z|^{-1}, q^{-1/3}\}$. This is because then

$$|1-\chi(p)zu^{\deg p}| \geq 1 - |zu^{\deg p}| \geq 1 - |zu| > 0$$

so the factors $(1-\chi(p)zu^{\deg p})^{-1}$ have no poles. And

$$\begin{aligned}&(1-zT)^{-1}(1-T)^{z}\left(1-T^2\right)^{\frac{z(z-1)}{2}}\\&=\left(1+zT+z^2T^2+O(T^3)\right)\left(1-zT+\frac{z(z-1)}{2}T^2+O(T^3)\right)\left(1-\frac{z(z-1)}{2}T^2+O(T^4)\right)\\&=1+O(T^3)\end{aligned}$$

so each factor in the Euler product of $E_z(u,\chi)$ is $1+O(u^{3\deg p})$, hence the product converges absolutely and defines a holomorphic fucntion for $|u|<\min\{|z|^{-1},q^{-1/3}\}$.

Having an explicit representation of the generating function for $\chi(f)z^{\Omega(f)}$ beyond the radius $q^{-1/2}$ allows us to extract a formula for $\sum_{f\in\mathcal{M}_n}\chi(f)z^{\Omega(f)}$. We use this to deduce a formula for $\sum_{\substack{f\in\mathcal{M}_n\\ \Omega(f)=k}}\chi(f)$. In particular, this is why we can get an explicit formula involving the zeros which are on the circle $|u|=q^{-1/2}$.

Define also

$$F_z(u,\chi)=L(u^2,\chi^2)^{\frac{z(z-1)}{2}}E_z(u,\chi)=\prod_p(1-\chi(p)zu^{\deg p})^{-1}(1-\chi(p)u^{\deg p})^z$$

where the second product representation is valid inside $|u|<\min\{|z|^{-1},q^{-1/2}\}$.

Before starting the proof, let's take a minute to be clear about what these expressions mean. Having factored $L(u,\chi)$ over its zeros ρ as

$$L(u,\chi)=\prod_\rho(1-u/\rho)^{m_\rho}$$

as in equation (4.1), we define

$$L(u,\chi)^z:=\exp(z\sum_\rho m_\rho\log(1-u/\rho))$$

where log defined on the set $\mathbb{C}\backslash[0,-\infty)$ takes real values on the positive reals and define $L(u^2,\chi^2)^{z(z-1)/2}$ similarly. These expressions define functions $L(u,\chi)^z$ and $L(u^2,\chi^2)^{z(z-1)/2}$, holomorphic in u and z for all $z\in\mathbb{C}$ and all $u\in\mathbb{C}\backslash\bigcup_\rho\{u:1-u/\rho\in\mathbb{R}_{\leq 0}\}$.

The formula $\sum_{f\in\mathcal{M}_n}\chi(f)z^{\Omega(f)}$ we need is given by Proposition 4.1 below. First though we prove a simple integral lemma.

Lemma 4.1. *Let $A, \delta > 0$. Let $\mathcal{H}$ be the Hankel contour of radius 1 around 0 going along the negative real axis to $-n\delta$. Uniformly for $|z| \leq A$ we have*

$$\frac{1}{2\pi i}\int_{\mathcal{H}} w^z \frac{dw}{(1-w/n)^{n+1}} = \frac{1}{\Gamma(-z)} + O(1/n)$$

Proof. We may suppose n is sufficiently large. By Corollary 0.18 from [38] we have

$$\frac{1}{2\pi i}\int_{\mathcal{H}} w^z e^w dw = \frac{1}{\Gamma(-z)} + O(e^{-n\delta/2})$$

so it suffices to show that

$$\int_{\mathcal{H}} \left| w^z \left(\frac{1}{(1-w/n)^{n+1}} - e^w \right) \right| |dw| = O(1/n).$$

On the region $\Re w > -n/2$ we have

$$\frac{1}{(1-w/n)^{n+1}} - e^w = e^{-(n+1)\log(1-w/n)} - e^w = e^{w+O(1/n)} - e^w = O(e^w/n)$$

and $\int_{\mathcal{H}} |w^z e^w|\,|dw| = O(1)$. On the rest of the integral

$$\int_{-n/2}^{-n\delta} \left| w^z \left(\frac{1}{(1-w/n)^{n+1}} - e^w \right) \right| |dw| \ll n^{A+1} e^{-cn}$$

for some $c > 0$ when $|z| \leq A$. This proves the lemma. □

Proposition 4.1. *Let $M_z(n,\chi) := \sum_{f \in \mathcal{M}_n} \chi(f) z^{\Omega(f)}$. For all $\epsilon > 0$ the following holds uniformly for $|z| \leq q^{1/2-\epsilon}$. If $\chi^2 \neq \chi_0$,*

$$M_z(n,\chi) = \sum_{\substack{\rho\,:\\ L(\rho,\chi)=0\\ |\rho|=q^{-1/2}}} \rho^{-n} n^{-zm_\rho - 1} \left\{ \frac{F_z(\rho,\chi) c_\rho^z}{\Gamma(-zm_\rho)} + O\left(n^{-1}\right) \right\}$$

and if $\chi^2 = \chi_0$,

$$M_z(n,\chi) = \sum_{\substack{\rho: \\ L(\rho,\chi)=0 \\ |\rho|=q^{-1/2} \\ \rho\neq\pm q^{-1/2}}} \rho^{-n} n^{-zm_\rho-1} \left\{ \frac{F_z(\rho,\chi)c_\rho^z}{\Gamma(-zm_\rho)} + O\left(n^{-1}\right) \right\}$$

$$+ \sum_{\pm} (\pm 1)^n q^{n/2} n^{-1-zm_\pm+z(z-1)/2} \left\{ \frac{E_z(\pm q^{-1/2},\chi)c_\pm^z \left(\frac{\phi(M)}{2q^{\deg M}}\right)^{z(z-1)/2}}{\Gamma(-zm_\pm + z(z-1)/2)} + O\left(n^{-1}\right) \right\}$$

for some constants c_ρ, $c_\pm$ *defined in the course of the proof.*

Proof. Applying Cauchy's formula with $r < q^{-1/2}$ gives

$$M_z(n,\chi) = \frac{1}{2\pi i} \int_{|u|=r} G_\chi(u,z) \frac{du}{u^{n+1}}. \tag{4.5}$$

We shift this contour to write the left hand side in terms of the singularities of $G_z(u,\chi)$ with $|u| = q^{-1/2}$. For each such singularity ρ, let $\mathcal{H}_\rho$ be the contour that consists of a circle of radius $1/n$ traversed clockwise around ρ and the two line segments on the ray from 0 to ρ joining this small circle to the circle $|u| = q^{\epsilon/2-1/2}$. We may replace ϵ by $\min\{1/10, \epsilon\}$ if necessary to ensure $q^{\epsilon/2-1/2} < q^{-1/3}$.

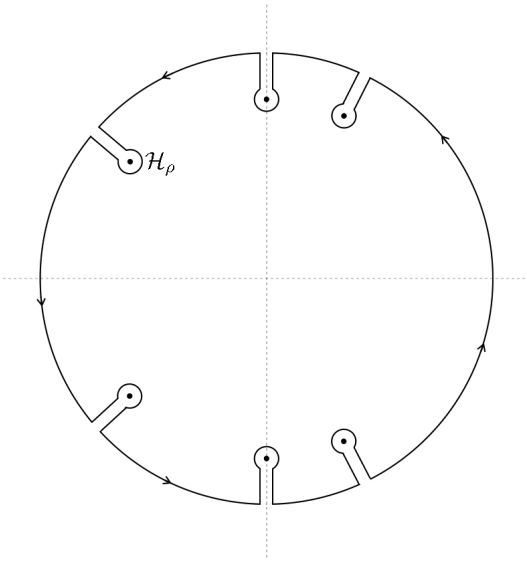


Figure 4.4: Keyhole contour

Then (4.4) becomes

$$\sum_{\rho\in\mathcal{S}}\frac{1}{2\pi i}\int_{\mathcal{H}_\rho}G_z(u,\chi)\frac{du}{u^{n+1}}+O\left(\int_{|u|=q^{\epsilon/2-1/2}}\left|G_z(u,\chi)\frac{du}{u^{n+1}}\right|\right)=:\sum_{\rho\in\mathcal{S}}I_\rho+O\left(q^{n(\frac{1}{2}-\epsilon/2)}\right)$$

Here we have used the fact that $G_z(u,\chi)$ is uniformly bounded in the region $|u|\le q^{\epsilon/2-1/2}$, $|z|\le q^{1/2-\epsilon}$. Let us now evaluate each of these Hankel contours, first the non-real ρ, then $\rho=\pm q^{-1/2}$.

Case 1: Non-real ρ.

Since $F_z(u,\chi)$ is holomorphic in u on $\mathcal{H}_\rho$ we may use the approximation $F_z(u,\chi)=F_z(\rho,\chi)+O(|u-\rho|)$ for the singularities $\rho=q^{-1/2}e^{-i\gamma_j}\neq\pm q^{-1/2}$ to get

$$I_\rho=F_z(\rho,\chi)\frac{1}{2\pi i}\int_{\mathcal{H}_\rho}L(u,\chi)^z\frac{du}{u^{n+1}}+O\left(\int_{\mathcal{H}_\rho}|u-\rho||L(u,\chi)^z|\frac{|du|}{|u|^{n+1}}\right).$$

In the error term, we change variable to $w=n(1-u/\rho)$ so $u=\rho(1-w/n)$ to get

$$\begin{aligned}\int_{\mathcal{H}_\rho}\left|(1-u/\rho)^{1+zm_\rho}\left(\frac{L(u,\chi)}{(1-u/\rho)^{m_\rho}}\right)^z\right|\frac{|du|}{|u|^{n+1}}&\ll q^{n/2}|n^{-2-zm_\rho}|\int_{\mathcal{H}}|w^{1+zm_\rho}|\frac{|dw|}{|(1-w/n)^{n+1}|}\\&\ll q^{n/2}|n^{-2-zm_\rho}|\end{aligned}$$

since $|L(u,\chi)/(1-u/\rho)^{m_\rho}|$ is bounded above and below by positive constants on the contour of integration.

To evaluate the main term, again change to the variable $w=n(1-u/\rho)$ in the first integral above to get

$$\frac{\rho^{-n}n^{-1}}{2\pi i}\int_{\mathcal{H}}L(\rho(1-w/n),\chi)^z\frac{dw}{(1-w/n)^{n+1}}.$$

If we define $c_\rho\neq 0$ by $L(u,\chi)=(1-u/\rho)^{m_\rho}(c_\rho+O(|1-u/\rho|))$, that is, $c_\rho=[L(u,\chi)/(1-u/\rho)^{m_\rho}]_{u=\rho}$ and $c_\rho^z=\exp(z\sum_{\rho'\neq\rho}m_{\rho'}\log(1-\rho/\rho'))$, then

$$\left(\frac{L(u,\chi)}{(1-u/\rho)^{m_\rho}}\right)^z=c_\rho^z+O(|1-u/\rho|)$$

and

$$L(\rho(1-w/n),\chi)^z=(w/n)^{zm_\rho}c_\rho^z+O(|w/n|^{zm_\rho+1}).$$

By Lemma 4.1, the main term is

$$\frac{c_\rho^z \rho^{-n} n^{-zm_\rho - 1}}{2\pi i} \int_{\mathcal{H}} w^{zm_\rho} \frac{dw}{(1-w/n)^{n+1}} = \frac{c_\rho^z \rho^{-n} n^{-zm_\rho - 1}}{\Gamma(-zm_\rho)} + O(q^{n/2}|n^{-zm_\rho - 2}|)$$

and the error term is

$$\ll q^{n/2}|n^{-zm_\rho-2}| \int_{\mathcal{H}} |w^{zm_\rho+1}| \frac{|dw|}{|(1-w/n)^{n+1}|} \ll q^{n/2}|n^{-zm_\rho-2}|.$$

Case 2: Real ρ.

Now let's look at the singularities $\pm q^{-1/2}$. If χ^2 is not principal, then exactly the same argument still works with $\rho = \pm q^{-1/2}$ and the convention $m_{\pm q^{-1/2}} = m_\pm$ because in that case $F_z(u,\chi) = L(u^2,\chi^2)E_z(u,\chi)$ is holomorphic near $u = \pm q^{-1/2}$.

Suppose then that $\chi^2 = \chi_0$ is principal. We now have to worry about the extra poles of $L(u^2,\chi_0)$ at $u = \pm q^{-1/2}$. First near $u = q^{-1/2}$, change to the variable $w = n(1-q^{1/2}u)$ so $u = q^{-1/2}(1-w/n)$. Then we want to evaluate

$$\frac{q^{n/2}n^{-1}}{2\pi i} \int_{\mathcal{H}} L\left(\frac{1-w/n}{q^{1/2}},\chi\right)^z L\left(\frac{(1-w/n)^2}{q},\chi_0\right)^{\frac{z(z-1)}{2}} E_z\left(\frac{1-w/n}{q^{1/2}},\chi\right) \frac{dw}{(1-w/n)^{n+1}}$$

Defining $c_+ \neq 0$ by $L(u,\chi)/(1-uq^{1/2})^{m_+} = c_+ + O(|1-uq^{1/2}|)$, along the contour of integration we have

$$L\left(\frac{1-w/n}{q^{1/2}},\chi\right)^z = (w/n)^{zm_+} c_+^z + O(|w/n|^{zm_+ + 1})$$

and since $L(u,\chi_0) = \frac{1}{1-qu}\prod_{p|M}(1-u^{\deg p})$ and $\prod_{p|M}(1-q^{-\deg p}) = q^{-\deg M}\phi(M)$ we have

$$L\left(\frac{(1-w/n)^2}{q},\chi_0\right)^{\frac{z(z-1)}{2}} = \left(\frac{n}{2w}\frac{\phi(M)}{q^{\deg M}}\right)^{\frac{z(z-1)}{2}} + O(|n/w|^{\frac{z(z-1)}{2}-1}).$$

We also have,

$$E_z\left(\frac{1-w/n}{q^{1/2}},\chi\right) = E_z(q^{-1/2},\chi) + O(|w/n|)$$

which together give the main term as

$$q^{n/2}n^{-1-zm_+ +z(z-1)/2}E_z(q^{-1/2},\chi)c_+^z\left(\frac{\phi(M)}{2q^{\deg M}}\right)^{z(z-1)/2}\frac{1}{2\pi i}\int_{\mathcal{H}}\frac{w^{zm_+ -z(z-1)/2}}{(1-w/n)^{n+1}}dw$$
$$= q^{n/2}n^{-1-zm_+ +z(z-1)/2}\frac{E_z(q^{-1/2},\chi)c_+^z\left(\frac{\phi(M)}{2q^{\deg M}}\right)^{z(z-1)/2}}{\Gamma(-zm_+ +z(z-1)/2)}+O\left(q^{n/2}|n^{-zm_+ +z(z-1)/2-2}|\right)$$

with the error terms all being $O(q^{n/2}|n^{-zm_+ +z(z-1)/2-2}|)$.

The $-q^{-1/2}$ term is essentially the same. Together this proves Proposition 4.1. □

4.3 Saddle point lemmas

Recall Lemma 3.2 from the previous chapter.

Lemma 4.2. *Let $A>0$ and let $p_n(z)=\sum_{k\geq 0}c_k(n)z^k$ be a sequence of polynomials such that uniformly for $n\geq 1$ and $|z|\leq A$*

$$p_n(z)=n^{az}\left(f(z)+O\left(n^{-1}\right)\right) \tag{4.6}$$

for some real constant $a>0$ and some function $f(z)$ that is holomorphic on $\{z\in\mathbb{C}:|z|\leq A\}$. Then uniformly for $1\leq k\leq aA\log n$,

$$c_k(n)=\frac{(a\log n)^k}{k!}\left(f\left(\frac{k}{a\log n}\right)+O\left(\frac{k}{(\log n)^2}\right)\right).$$

We also need the following quadratic variant.

Lemma 4.3. *Let $A>0$ and let $p_n(z)=\sum_{k\geq 0}c_k(n)z^k$ be a sequence of polynomials such that uniformly for $n\geq 1$ and $|z|\leq A$*

$$p_n(z)=n^{az^2+bz}\left(f(z)+O\left(n^{-1}\right)\right) \tag{4.7}$$

for some real constants $a>0$ and $b>0$ and some function $f(z)$ that is holomorphic on $\{z\in\mathbb{C}:|z|\leq A\}$ with $f(0)=1$. Let r be the positive root of the quadratic

$$r^2+\frac{b}{2a}r-\frac{k}{2a\log n}=0.$$

Then uniformly for $1\leq k\leq\min\{(\log n)^{1/2},bA\log n\}$ we have

(a)

$$c_k(n) = \frac{(b\log n)^k}{k!}\left(1 + O\left(\frac{k^2}{\log n}\right)\right).$$

In the range $1 \le k \le \min\{(\log n)^{2/3}, bA\log n\}$ *we have*

(b)

$$c_k(n) = \frac{(b\log n)^k}{k!} e^{\frac{ak^2}{b^2\log n}}\left(1 + O\left(\frac{1}{k} + \frac{k^3}{(\log n)^2}\right)\right).$$

In the range $1 \le k \le 2aA^2\log n$ *we have*

(c)

$$c_k(n) = \frac{n^{ar^2+br}}{r^k}\left(\frac{f(r)}{\sqrt{2\pi(4ar^2+br)\log n}} + O\left((r\log n)^{-3/2}\right)\right).$$

Proof. Part (a) follows from the proof of Lemma 4.2 with $r = k/(b\log n)$ and the approximation

$$n^{az^2} = 1 + O(k^2/\log n)$$

which holds for $|z| = r$. For part (c) we again use Cauchy's formula and the saddle point method. This time we choose r to minimise the bound

$$|c_k(n)| \ll r \cdot \max_{|z|=r}\left|\frac{n^{az^2+bz}}{z^{k+1}}\right| = \frac{n^{ar^2+br}}{r^k}.$$

The maximum occurs at $z = r$ because $a > 0$ and $b > 0$. By differentiating, this is minimised when

$$r^2 + \frac{b}{2a}r - \frac{k}{2a\log n} = 0 \qquad \text{or} \qquad r = \frac{b}{4a}\left(\sqrt{1 + \frac{8ak}{b^2\log n}} - 1\right).$$

Notice that in the range $k \le 2aA^2\log n$ we have

$$r \le \frac{b}{4a}\left(\sqrt{1 + \frac{16a^2A^2}{b^2}} - 1\right) \le A$$

since $\sqrt{1+x} \le 1 + \sqrt{x}$ for all $x > 0$ so this is a valid choice for r. Now from (4.6) and

$$f(z) = f(r) + f'(r)(z-r) + O(|z-r|^2)$$

it follows that

$$c_k(n) = f(r)I_1 + f'(r)I_2 + O(I_3) + O(E)$$

where

$$\begin{aligned} I_1 &= \frac{1}{2\pi i}\int_{|z|=r} \frac{n^{az^2+bz}}{z^{k+1}} dz \\ I_2 &= \frac{1}{2\pi i}\int_{|z|=r} \frac{n^{az^2+bz}}{z^{k+1}} (z-r) dz \\ I_3 &= \int_{|z|=r} \left| \frac{n^{az^2+bz}}{z^{k+1}} (z-r)^2 \right| |dz| \\ E &= \frac{n^{ar^2+br-1}}{r^k}. \end{aligned}$$

Writing $z = re^{2\pi it}$ and rearranging slightly this can we written

$$c_k(n) = \frac{n^{ar^2+br}}{r^k} \left\{ f(r)J_1 + rf'(r)J_2 + O(r^2 J_3) + O(1/n) \right\}$$

where

$$\begin{aligned} J_1 &= \int_{-1/2}^{1/2} n^{(ar^2(e^{4\pi it}-1)+br(e^{2\pi it}-1)} e^{-k2\pi it} dt \\ J_2 &= \int_{-1/2}^{1/2} n^{(ar^2(e^{4\pi it}-1)+br(e^{2\pi it}-1)} e^{-k2\pi it} (1-e^{2\pi it}) dt \\ J_3 &= \int_{-1/2}^{1/2} n^{(ar^2(\cos(4\pi t)-1)+br(\cos(2\pi t)-1)} |1-e^{2\pi it}|^2 dt. \end{aligned}$$

The integrals I_1 and I_2 could be written explicitly as a sum of k terms. Instead, we will asymptotically evaluate J_1 by expanding around the point $t = 0$. This will give a main term and smaller error term provided $k \to \infty$. This is akin to approximating the integral $\frac{1}{2\pi i}\oint \frac{e^z}{z^{k+1}} dz = \frac{1}{k!}$ by $\frac{e^k k^{-k}}{\sqrt{2\pi k}}$. For small values of k, part (a) is better.

Let $\delta = (r \log n)^{-1/4}$. Using $e^{ix} = 1 + ix - x^2/2 - ix^3/6 + O(x^4)$ and the definition of

r we have

$$\begin{aligned} J_1 &= \int_{-\delta}^{\delta} n^{ar^2(-8\pi^2t^2-i32\pi^3t^3/3+O(t^4))+br(-2\pi^2t^2-i4\pi^3t^3/3+O(t^4))}dt + O\left(n^{-br\delta^2}\right) \\ &= \int_{-\delta}^{\delta} n^{-(4ar^2+br)2\pi^2t^2}(1+O(t^6(r\log n)^2+t^4r\log n))dt + O(n^{-br\delta^2}) \\ &= \frac{1}{\sqrt{2\pi(4ar^2+br)\log n}} + O((r\log n)^{-3/2}). \end{aligned}$$

And in a similar vein,

$$\begin{aligned} J_2 &= \int_{-\delta}^{\delta} n^{ar^2(-8\pi^2t^2-i32\pi^3t^3/3+O(t^4))+br(-2\pi^2t^2-i4\pi^3t^3/3+O(t^4))}(-2\pi it+O(t^2))dt + O\left(n^{-br\delta^2}\right) \\ &\ll \int_{-\delta}^{\delta} n^{-(4ar^2+br)2\pi^2t^2}(t^6(r\log n)^2+t^4r\log n+t^2)dt + n^{-br\delta^2} \ll (r\log n)^{-3/2} \end{aligned}$$

and

$$J_3 \ll \int_{-\infty}^{\infty} n^{-brt^2}t^2dt \ll (r\log n)^{-3/2},$$

which proves part (c).

To prove part (b), we approximate r and eliminate it from the expression given in part (c). Recall the definition of r

$$r = \frac{b}{4a}\left(\sqrt{1+\frac{8ak}{b^2\log n}}-1\right) = \frac{k}{b\log n} - \frac{2ak^2}{b^3(\log n)^2} + O\left(\frac{k^3}{(\log n)^3}\right) \tag{4.8}$$

so $k/2 \le br\log n \le 2k$ for n sufficiently large and

$$f(r) = f(0) + O(r) = 1 + O(k/\log n)$$

and the expression from part (c) becomes

$$\frac{n^{ar^2+br}}{r^k}\frac{1}{\sqrt{2\pi(4ar^2+br)\log n}}\left(1+O\left(\frac{1}{k}+\frac{k}{\log n}\right)\right).$$

Using the identity $ar^2 + \frac{br}{2} - \frac{k}{2\log n} = 0$ and (4.7) the main term rearranges to

$$\frac{n^{\frac{k}{2\log n}+\frac{br}{2}}r^{-k}}{\sqrt{2\pi(2k-br\log n)}} = \frac{(b\log n)^k e^k e^{-\frac{ak^2}{b^2\log n}+O(\frac{k^3}{(\log n)^2})}}{\sqrt{2\pi(k+\frac{2ak^2}{b^2\log n}+O(\frac{k^3}{(\log n)^2})}}\left(k-\frac{2ak^2}{b^2\log n}+O(\frac{k^3}{(\log n)^2})\right)^{-k}$$
$$= \frac{(b\log n)^k e^k}{k^k\sqrt{2\pi k}}e^{-\frac{ak^2}{b^2\log n}}\left(1+O(\frac{k}{\log n}+\frac{k^3}{(\log n)^2})\right)\left(1-\frac{2ak}{b^2\log n}+O(\frac{k^2}{(\log n)^2})\right)^{-k}$$
$$= \frac{(b\log n)^k}{k!}e^{\frac{ak^2}{b^2\log n}}\left(1+O(\frac{1}{k}+\frac{k}{\log n}+\frac{k^3}{(\log n)^2})\right).$$

Here we have used $(1-x+O(y))^{-k} = e^{xk}(1+O(kx^2+ky))$ when $kx^2, ky \ll 1$. Finally, we may leave out the $\frac{k}{\log n}$ term because $\frac{1}{k} + \frac{k^3}{(\log)^2} \geq \frac{k}{\log n}$. □

4.4 Proofs of Theorems

The proofs proceed by applying Lemmas 4.2 and 4.3 to Proposition 4.1.

4.4.1 Proof of Theorem 4.1

Suppose $\chi^2 \neq \chi_0$. We shall apply Lemma 4.2 to the polynomial

$$p_n(z) = \frac{1}{z}M_{-z}(n,\chi) = -\sum_{f\in\mathcal{M}_n}\chi(f)(-z)^{\Omega(f)-1} = \sum_{k\geq 1}(-1)^k\pi_k(n,\chi)z^{k-1}$$

so that $(-1)^k\pi_k(n,\chi)$ is the coefficient of z^{k-1}. Actually, this isn't entirely correct because $p_n(z)$ isn't of the form required by Lemma 4.2. By Proposition 4.1, it is a sum over ρ of terms of the required form. However, it is clear from the proof of Lemma 4.2 that we can apply it to each summand separately which is what we shall do. So in our application of Lemma 4.2 to the summand ρ from Proposition 4.1, we may take $A = q^{1/2-\epsilon}$ and have $a = m_\rho > 0$ and

$$f(z) = \frac{1}{z}\frac{F_{-z}(\rho,\chi)c_\rho^{-z}}{\Gamma(zm_\rho)} = m_\rho\frac{F_{-z}(\rho,\chi)c_\rho^{-z}}{\Gamma(1+zm_\rho)}.$$

Then Theorem 4.1 follows after using

$$f((k-1)/(a\log n)) = f(0) + O(k/\log n) = m_\rho + O(k/(\log n)).$$

4.4.2 Proof of Theorem 4.3

Suppose $\chi^2 = \chi_0$. With the same $p_n(z)$ as in the proof of Theorem 4.1, this time we need Lemma 4.2 and Lemma 4.3 parts (a) and (b). Again, strictly speaking we shouldn't be

able to apply these lemmas directly as stated but it is clear from the proofs that we may apply them to each summand in Proposition 4 separately. For the $\rho \neq \pm q^{-1/2}$ terms we apply Lemma 4.2 just as above. For the $\rho = \pm q^{-1/2}$ terms we apply Lemma 4.3 part (a) in the range $1 \leq k \leq (\log n)^{1/2}$ and part (b) in the range $1 \leq k \leq (\log n)^{2/3}$ with $a = 1/2$, $b = m_\pm + 1/2$ and

$$\begin{aligned} f(z) &= \frac{E_{-z}(\pm q^{1/2}, \chi) c_\pm^{-z} \left(\frac{\phi(M)}{2^{\deg M}}\right)^{z(z+1)/2}}{z\Gamma(zm_\pm + z(z+1)/2)} \\ &= (m_\pm + (z+1)/2) \frac{E_{-z}(\pm q^{1/2}, \chi) c_\pm^{-z} \left(\frac{\phi(M)}{2^{\deg M}}\right)^{z(z+1)/2}}{\Gamma(1 + zm_\pm + z(z+1)/2)} \end{aligned}$$

so that $f(0) = m_\pm + 1/2$.

4.4.3 Proof of Theorems 4.2 and 4.4

Suppose $m_j = 1$ for each j and $m_\pm = 0$. This time we apply Lemma 4.2 and Lemma 4.3 part (c) to the same $p_n(z)$ using Proposition 4.1. For $\chi^2 \neq \chi_0$ and Theorem 4.2 we just apply the proof of Theorem 4.1 and the approximation

$$f((k-1)/(\log n)) = f(\alpha) + o(1).$$

We see therefore that $h_j(\alpha) = F_{-\alpha}(\rho, \chi) c_\rho^{-\alpha} / \Gamma(1+\alpha)$ where $\rho = \alpha_j(\chi)^{-1}$. Also, in the case that $m_\rho = 1$, it follows from the definition of c_ρ given in the proof of Proposition 4.1 that $c_\rho = -\rho L'(\rho, \chi)$.

For $\chi^2 = \chi_0$ and Theorem 4.4, we have the two extra terms $\rho = \pm q^{-1/2}$. We can evaluate these with Lemma 4.3 part (c) applied with $a = b = 1/2$ and

$$f_\pm(z) = \frac{E_{-z}(\pm q^{1/2}, \chi) c_\pm^{-z} \left(\frac{\phi(M)}{2^{\deg M}}\right)^{z(z+1)/2}}{z\Gamma(z(z+1)/2)}.$$

Then $r > 0$ satisfies

$$r^2 + \frac{r}{2} - \frac{k-1}{\log n} = 0.$$

Since $k(n) \to \infty$ as $n \to \infty$ we also have $r \log n \to \infty$ as $n \to \infty$. To finish the proof of Theorem 4.4 it therefore suffices to show that for some coefficient $h_\pm(\alpha)$ we have

$$\frac{n^{r^2/2 + r/2}}{r^{k-1}} \frac{f_\pm(r)}{\sqrt{2\pi(2r^2 + r/2)\log n}} = (h_\pm(\alpha) + o(1)) \frac{(\log n)^{k-1}}{(k-1)!} n^{b((k-1)/\log n)} \tag{4.9}$$

where b is defined by (4.3). This is a simple calculation using the definition of r and Stirling's formula. The left hand side of (4.9) is

$$\begin{aligned}
&\frac{(\log n)^{k-1}}{(k-1)!}\frac{(k-1)!}{(r\log n)^{k-1}}\frac{f_\pm(r)}{\sqrt{2\pi(k-1)(\frac{\log n}{k-1}r^2+1)}}n^{\frac{r}{4}+\frac{k-1}{2\log n}} \\
&\quad=\frac{(\log n)^{k-1}}{(k-1)!}\frac{(k-1)!e^{k-1}}{(k-1)^{k-1}}\frac{f_\pm(r)}{\sqrt{2\pi(k-1)(\frac{\log n}{k-1}r^2+1)}}n^{\frac{r}{4}-\frac{k-1}{2\log n}+\frac{k-1}{\log n}\log(\frac{k-1}{r\log n})} \\
&\quad=(h_\pm(\alpha)+o(1))\frac{(\log n)^{k-1}}{(k-1)!}n^{u\left(\frac{s-1}{2}-\log(2s)\right)}
\end{aligned}$$

by Stirling's formula where $u=(k-1)/\log n$ and $s=\frac{r}{2u}$. Now s is the positive root of the quadratic equation

$$s^2+\frac{s}{4u}-\frac{1}{4u}=0$$

so

$$u=\frac{1-s}{4s^2}$$

and

$$s=\frac{1}{8u}\left(-1+\sqrt{1+16u}\right)$$

from which it follows that $0\le s\le 1$ This proves (4.9) for some explicit $h_\pm(\alpha)$ with b defined by (4.3) since $\alpha=\lim_{n\to\infty}u$. Finally, it is easy to check the conditions on the sign of $b(\alpha)$ by noting that $\frac{s-1}{2}-\log(2s)$ is strictly decreasing on $(0,1)$ and equal to 0 at $s=\beta$ where β is the unique solution to $\frac{\beta-1}{2}=\log(2\beta)$ with $0\le\beta\le 1$.

Chapter 5

The Möbius exponential sum in $\mathbb{F}_q[t]$

This chapter is based on [28].

In 1991, Baker and Harman proved, under the assumption of the generalized Riemann hypothesis, that $\max_{\theta\in[0,1)}\left|\sum_{n\le x}\mu(n)e(n\theta)\right| \ll_\epsilon x^{3/4+\epsilon}$. The purpose of this chapter is to deduce an analogous bound in the context of polynomials over a finite field using Weil's Riemann Hypothesis for curves over a finite field. Our approach is based on the work of Hayes who studied exponential sums over irreducible polynomials.

Acknowledgements. We are grateful to Pierre Bienvenu for pointing out a mistake in an earlier version of our proof of Theorem 5.1.

5.1 Introduction

Let μ be the Möbius function and write $e(\theta) = e^{2\pi i\theta}$. Baker and Harman [4] proved under the assumption of the generalized Riemann hypothesis that for all $\epsilon > 0$,

$$\max_{\theta\in[0,1)}\left|\sum_{n\le x}\mu(n)e(n\theta)\right| \ll_\epsilon x^{\frac{3}{4}+\epsilon}. \tag{5.1}$$

It is conjectured that (5.1) holds for all $\epsilon > 0$ with $\frac{3}{4}$ replaced by $\frac{1}{2}$. The best unconditional result is due to Davenport [9] who showed that for all $A > 0$

$$\max_{\theta\in[0,1)}\left|\sum_{n\le x}\mu(n)e(n\theta)\right| \ll_A \frac{x}{(\log x)^A}.$$

In this chapter we deduce an analogue of (5.1) for the polynomial ring $\mathbb{F}_q[t]$. First, let us go through some definitions required to state the result. The function field analogue of the real numbers is the completion of the field of fractions of $\mathbb{F}_q[t]$ with respect to the

norm defined by

$$|f/g| = \begin{cases} q^{\deg f - \deg g} & \text{if } f \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

This completion is naturally identified with the ring of formal Laurent series $\mathbb{F}_q((1/t)) = \{\sum_{i \leq j} x_i t^i \ : \ x_i \in \mathbb{F}_q,\ j \in \mathbb{Z}\}$. The norm defined above is extended to $x = \sum_{i \leq j} x_i t^i \in \mathbb{F}_q((1/t))$ by setting $|x| = q^j$ where j is the largest index with $x_j \neq 0$. The analogue of the unit interval is $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, and is a subring of $\mathbb{F}_q((1/t))$.

Define the additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ by

$$\psi(x) = e(\mathrm{tr}(x)/p),$$

where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace map and p is the characteristic of $\mathbb{F}_q$. Define also the exponential map $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$ by

$$\mathbf{e}_q(x) = \psi(x_{-1}).$$

Now let μ denote the Möbius function on the ring $\mathbb{F}_q[t]$ defined to be $(-1)^k$ if f is the product of k distinct irreducibles and 0 otherwise. Let $\phi(f)$ be the size of the unit group $(\mathbb{F}_q[t]/(f))^\times$, that is $|f| \prod_{\omega | f}(1 - 1/|\omega|)$, where the product is over all monic irreducibles dividing f. Finally, let $\pi(n)$ be the number of monic, irreducible polynomials of degree n and recall the prime number theorem in the form $\sum_{d|n} d\pi(d) = q^n$. All sums over polynomials are sums over monic polynomials.

Theorem 5.1. *Suppose $n \geq 3$. Then*

$$\max_{\theta \in \mathbb{T}} \left| \sum_{f \in \mathcal{M}_n} \mu(f) \boldsymbol{e}_q(f\theta) \right| \leq 4q^{\frac{3n+1}{4}} \left(\frac{3\sqrt{3}}{2} \right)^n.$$

Remark. It follows that for all $\epsilon > 0$ and q large enough with respect to ϵ we have

$$\max_{\theta \in \mathbb{T}} \left| \sum_{f \in \mathcal{M}_n} \mu(f) \mathbf{e}_q(f\theta) \right| \leq 4q^{(\frac{3}{4} + \epsilon)n}.$$

Our proof of Theorem 5.1 will follow the strategy of Hayes employed in his study of

the exponential sum

$$\sum_{\omega \in \mathcal{P}_n} \mathbf{e}_q(\omega\theta).$$

We note that Bienvenu and Lê have independently derived a similar result to Theorem 5.1 in [5]. Their Theorem 9 corresponds to our Lemma 5.1 and their Theorem 11 closely resembles our Theorem 5.1.

5.2 Lemmas

Whilst investigating the distribution of irreducible polynomials over $\mathbb{F}_q$, Hayes [17] introduced certain congruences classes on $\mathcal{M}$ defined as follows. Let $s \geq 0$ be an integer and $g \in \mathbb{F}_q[t]$. We define an equivalence relation $\mathcal{R}_{s,g}$ on $\mathcal{M}$ by

$$a \equiv b \bmod \mathcal{R}_{s,g} \Leftrightarrow g \text{ divides } a-b \text{ and } \left| \frac{a}{t^{\deg a}} - \frac{b}{t^{\deg b}} \right| < \frac{1}{q^s}$$

It is easy to check that this is indeed an equivalence relation and that for all $c \in \mathcal{M}$,

$$a \equiv b \bmod \mathcal{R}_{s,g} \Rightarrow ac \equiv bc \bmod \mathcal{R}_{s,g}$$

so we can define the quotient monoid $\mathcal{M}/\mathcal{R}_{s,g}$. Hayes showed that an element of $\mathbb{F}_q[t]$ is invertible modulo $\mathcal{R}_{s,g}$ if and only if it is coprime to g and that the units of this quotient monoid form an abelian group of order $q^s\phi(g)$ which we denote $\mathcal{R}^*_{s,g} = (\mathcal{M}/\mathcal{R}_{s,g})^\times$. Given a character (group homomorphism) $\chi : \mathcal{R}^*_{s,g} \to \mathbb{C}$ we can lift this to a character of $\mathcal{M}$ by setting $\chi(f) = 0$ if f is not invertible modulo $\mathcal{R}_{s,g}$. Associated to each such character is the L-function $L(u,\chi)$ defined for $u \in \mathbb{C}$ with $|u| < 1/q$ by

$$L(u,\chi) = \sum_{f \in \mathcal{M}} \chi(f) u^{\deg f} = \prod_{\omega \in \mathcal{P}} (1 - \chi(\omega) u^{\deg \omega})^{-1}.$$

When χ is a non-trivial character it can be shown, as we have already seen in the case that χ is a Dirichlet character, that $L(u,\chi)$ is a polynomial that factorises as

$$L(u,\chi) = \prod_{i=1}^{d(\chi)} (1 - \alpha_i(\chi) u)$$

for some $d(\chi) \leq s + \deg g - 1$ and each $\alpha_i(\chi)$ satisfies $|\alpha_i(\chi)| = 1$ or $\sqrt{q}$. This follows from Weil's Riemann Hypothesis and appears to have been first proved by Rhin in [31].

When $\chi = \chi_0$ is the trivial character we have

$$L(u,\chi_0) = \sum_{\substack{f\in\mathcal{M}\\(f,g)=1}} u^{\deg f} = \sum_{f\in\mathcal{M}} u^{\deg f}\prod_{\omega|g}(1-u^{\deg\omega}) = \frac{1}{1-qu}\prod_{\omega|g}(1-u^{\deg\omega}).$$

Lemma 5.1. *Let χ be a character modulo $\mathcal{R}^*_{s,g}$ and $\deg g \le n/2$. Then*

$$\left|\sum_{f\in\mathcal{M}_n}\mu(f)\chi(f)\right| \le \begin{cases} \binom{n+s+\deg g-2}{s+\deg g-2}q^{n/2} & \text{if } \chi\neq\chi_0 \\ \binom{n+r-1}{r-1}(q+1) & \text{if } \chi=\chi_0 \end{cases}$$

where r is the number of distinct irreducible divisors of g.

Remark. The bound for χ_0 is smaller than the one for $\chi\neq\chi_0$ when $n\ge 3$ because $\deg g$ is an upper bound for r and for $n\ge 3$

$$(q+1)\binom{n+\deg g-1}{n} \le \binom{n+\deg g-2}{n}q^{n/2}.$$

Proof. Suppose first that $\chi\neq\chi_0$. Then

$$\sum_{f\in\mathcal{M}}\chi(f)\mu(f)u^{\deg f} = L(u,\chi)^{-1} = \prod_{i=1}^{d(\chi)}(1-\alpha_i(\chi)u)^{-1} = \sum_{n\ge 0}\left(\sum_{\substack{r_1+\cdots r_{d(\chi)}=n\\0\le r_i\le n}}\prod_{i=1}^{d(\chi)}\alpha_i(\chi)^{r_i}\right)u^n.$$

Comparing coefficients and using the triangle inequality we get

$$\begin{aligned}\left|\sum_{f\in\mathcal{M}_n}\chi(f)\mu(f)\right| = \left|\sum_{\substack{r_1+\cdots+r_{d(\chi)}=n\\0\le r_i\le n}}\prod_{i=1}^{d(\chi)}\alpha_i(\chi)^{r_i}\right| &\le \binom{n+d(\chi)-1}{d(\chi)-1}q^{n/2}\\ &\le \binom{n+s+\deg g-2}{s+\deg g-2}q^{n/2}.\end{aligned}$$

When $\chi=\chi_0$ is the principal character

$$L(u,\chi_0)^{-1} = (1-qu)\prod_{\omega|g}(1+u^{\deg\omega}+u^{2\deg\omega}+\cdots).$$

If we write $\omega_1,\omega_2,\ldots,\omega_r$ for the distinct irreducible divisors of g then we get, by equating

coefficients again,

$$\begin{aligned}\left|\sum_{f\in\mathcal{M}_n}\chi_0(f)\mu(f)\right| &\le \sum_{\substack{a_i\in\mathbb{Z}_{\ge 0}\\ \sum_{1\le i\le r}a_i\deg\omega_i=n}} 1 + q\sum_{\substack{a_i\in\mathbb{Z}_{\ge 0}\\ \sum_{1\le i\le r}a_i\deg\omega_i=n-1}} 1\\ &\le (q+1)\sum_{\substack{b_i\in\mathbb{Z}_{\ge 0}\\ \sum_{1\le i\le r}b_i=n}} 1\\ &= (q+1)\binom{n+r-1}{r-1}.\end{aligned}$$

□

Lemma 5.2. *For each $\theta\in\mathbb{T}$ there exist unique coprime polynomials $a,g\in\mathbb{F}_q[t]$ with g monic and $\deg a<\deg g\le n/2$ such that*

$$\left|\theta-\frac{a}{g}\right|<\frac{1}{q^{\frac{n}{2}+\deg g}}.$$

Proof. See Lemma 3 from [27]. □

Lemma 5.3. *Let $\theta\in\mathbb{T}$ and let a,g be the unique polynomials defined as in Lemma 5.2 with respect to θ and n. Set $s=n-[\frac{n}{2}]-\deg g$. For any $f_1,f_2\in\mathcal{M}$ of degree n such that $f_1\equiv f_2$ mod $\mathcal{R}_{s,g}$ we have*

$$\boldsymbol{e}_q(f_1\theta)=\boldsymbol{e}_q(f_2\theta).$$

Proof. See Lemma 5.2 from [17]. □

Lemma 5.4. *Suppose $g\in\mathbb{F}_q[t]$ is square-free. Then*

$$\sum_{d|g}\frac{1}{q^{\deg d}}\le(1+\log_q(\deg g))e.$$

Proof. Order the monic irreducibles $\omega_1,\omega_2,\dots,\omega_r$ dividing g and the monic irreducibles $P_1,\dots$ in $\mathbb{F}_q[t]$ in order of degree (and those of the same degree arbitrarily). Define N by the inequalities $\sum_{\deg P\le N-1}\deg P<\deg g\le\sum_{\deg P\le N}\deg P$. Then g has at most $\sum_{1\le k\le N}\pi(N)$ irreducible factors. Therefore, since $\deg P_i\le\deg\omega_i$, we have

$$\sum_{d|g}\frac{1}{q^{\deg d}}\le\prod_{\omega|g}\left(1+\frac{1}{q^{\deg\omega}}\right)\le\prod_{\deg P\le N}\left(1+\frac{1}{q^{\deg P}}\right)=\prod_{1\le k\le N}\left(1+\frac{1}{q^k}\right)^{\pi(k)}.$$

Using $\pi(k) \leq \frac{q^k}{k}$ this is bounded by

$$\prod_{1\leq k\leq N}\left(1+\frac{1}{q^k}\right)^{\frac{q^k}{k}} \leq \prod_{1\leq k\leq N} e^{\frac{1}{k}} \leq e^{1+\log N} = Ne.$$

Now we bound N in terms of $\deg g$ as follows

$$\deg g > \sum_{\deg P\leq N-1} \deg p = \sum_{1\leq k\leq N-1} \pi(k)k \geq \sum_{k|N-1} \pi(k)k = q^{N-1}$$

by the prime number theorem in $\mathbb{F}_q[t]$. This gives $N \leq 1 + \log_q \deg g$ which completes the proof of the Lemma. □

5.3 Proof of Theorem 5.1

Let $\theta \in \mathbb{T}$ and choose g and s as in Lemma 5.3. We start by giving an explicit description of a set a representatives for the equivalence relation $\mathcal{R}_{s,g}$. It is not hard to show that

$$\mathcal{S}_{s,g} = \{t^{[\frac{n}{2}]}gb_1 + b_2 \mid \deg b_1 = s, b_1 \text{ monic}, \deg b_2 < \deg g\}$$

is such a set. Furthermore,

$$\mathcal{S}^*_{s,g} = \{t^{[\frac{n}{2}]}gb_1 + b_2 \mid \deg b_1 = s, b_1 \text{ monic}, \deg b_2 < \deg g, (b_2, g) = 1\}$$

defines a set of reduced representatives modulo $\mathcal{R}_{s,g}$. See [17] Lemma 7.1 for details.

Then by Lemma 5.3 and the orthogonality of characters modulo $\mathcal{R}^*_{s,g}$ we can write

$$\begin{aligned}
\sum_{f\in\mathcal{M}_n} \mu(f)\mathbf{e}_q(f\theta) &= \sum_{b\in\mathcal{S}_{s,g}} \sum_{\substack{f\in\mathcal{M}_n \\ f\equiv b \bmod \mathcal{R}_{s,g}}} \mu(f)\mathbf{e}_q(f\theta) \\
&= \sum_{d|g} \sum_{\substack{b\in\mathcal{S}_{s,g} \\ (g,b)=d}} \mathbf{e}_q(b\theta) \sum_{\substack{f\in\mathcal{M}_n \\ f\equiv b \bmod \mathcal{R}_{s,g}}} \mu(f) \\
&= \sum_{d|g} \sum_{\substack{b\in\mathcal{S}_{s,g/d} \\ (g/d,b)=1}} \mathbf{e}_q(bd\theta) \sum_{\substack{f\in\mathcal{M}_{n-d} \\ f\equiv b \bmod \mathcal{R}_{s,g/d}}} \mu(fd) \\
&= \sum_{d|g} \sum_{b\in\mathcal{S}^*_{s,g/d}} \mathbf{e}_q(bd\theta) \sum_{f\in\mathcal{M}_{n-d}} \frac{1}{q^s\phi(g/d)} \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \overline{\chi}(b)\chi(f)\mu(fd).
\end{aligned}$$

Notice that $\mu(fd) = \mu(f)\mu(d)\chi_d(f)$ where $\chi_d(f)$ is the trivial character modulo $\mathcal{R}^*_{s,d}$. We can therefore rewrite the above as

$$= \sum_{d|g} \frac{\mu(d)}{q^s\phi(g/d)} \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left(\sum_{b \in \mathcal{S}^*_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right) \left(\sum_{\deg f = n - \deg d} \mu(f)\chi\chi_d(f) \right).$$

Now χ is a character modulo $\mathcal{R}^*_{s,g/d}$ and χ_d is a character modulo $\mathcal{R}^*_{s,d}$. Therefore, $\chi\chi_d$ is a character modulo $\mathcal{R}^*_{s,g}$, and so using the triangle inequality and Lemma 5.1 we can bound this in absolute value by

$$q^{n/2} \sum_{\substack{d|g \\ g \text{ square-free}}} \frac{1}{q^{s+\deg d/2}\phi(g/d)} \binom{n - \deg d + s + \deg g - 2}{s + \deg g - 2} \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b \in \mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right|$$

We bound the Gauss sum over $\chi \bmod \mathcal{R}^*_{s,g/d}$ in the standard way using the Cauchy–Schwarz inequality and Parseval's identity as follows

$$\begin{aligned}
\sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b \in \mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right| &\le \left(\sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} 1 \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b \in \mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right|^2 \right)^{1/2} \\
&= \left(q^s\phi(g/d) \sum_{b_1, b_2 \in \mathcal{S}_{s,g/d}} \mathbf{e}_q(d(b_1 - b_2)\theta) \sum_{\chi \bmod \mathcal{R}^*_{s,g}} \overline{\chi}(b_1)\chi(b_2) \right)^{1/2} \\
&= \left((q^s\phi(g/d))^2 \sum_{b_1 = b_2 \in \mathcal{S}^*_{s,g/d}} \mathbf{e}_q((b_1 - b_2)\theta) \right)^{1/2} \\
&= (q^s\phi(g/d))^{3/2}.
\end{aligned}$$

Recall that $s + \deg g = n - [\frac{n}{2}] \ge n/2$ so that

$$\binom{n - \deg d + s + \deg g - 2}{s + \deg g - 2} \le \binom{2n - [\frac{n}{2}] - 2}{n - [\frac{n}{2}] - 2}.$$

We can bound this binomial coefficient using the fact that for all positive integers k,

$$\sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k+1}} < k! < \sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k}}.$$

This precise form of Stirling's formula is due to Robbins [32]. It follows that if $k = [\frac{n}{2}]$

then

$$\binom{2n-[\frac{n}{2}]-2}{n-[\frac{n}{2}]-2} < \binom{3k}{k} < \frac{1}{\sqrt{2\pi}} e^{\frac{1}{36k}-\frac{1}{12k+1}-\frac{1}{24k+1}} \frac{(3k)^{3k+\frac{1}{2}}}{k^{k+\frac{1}{2}}(2k)^{2k+\frac{1}{2}}} < \frac{1}{\sqrt{4\pi k/3}} \left(\tfrac{3\sqrt{3}}{2}\right)^{2k}.$$

Putting it all together with $\phi(g/d) \le q^{\deg g - \deg d}$ and Lemma 5.4 we get

$$\begin{aligned}\left|\sum_{f\in\mathcal{M}_n} \mu(f)\mathbf{e}_q(f\theta)\right| &\le q^{n/2} \frac{1}{\sqrt{2\pi(n-1)/3}} \left(\tfrac{3\sqrt{3}}{2}\right)^n \sum_{d|g} \frac{(q^s\phi(g/d))^{1/2}}{q^{\deg d/2}} \\ &\le q^{n-\frac{1}{2}[\frac{n}{2}]} \frac{(1+\frac{\log n}{\log q})e}{\sqrt{2\pi(n-1)/3}} \left(\tfrac{3\sqrt{3}}{2}\right)^n\end{aligned}$$

and Theorem 5.1 easily follows after a short numerical calculation.

Chapter 6

Coefficients of irreducible polynomials

The first section of this chapter is based on [30].

Many theorems concerning the existence of irreducible polynomials over a finite field of a special form have been proved. A discussion of such results can be found in [39]. In this chapter we will prove some new results in this direction. Section 6.1 contains a function field analogue of Maynard's celebrated result about primes with restricted digits. That is, for certain ranges of parameters n and q, we prove an asymptotic formula for the number of irreducible polynomials of degree n over a finite field $\mathbb{F}_q$ whose coefficients are restricted to lie in a given subset of $\mathbb{F}_q$. In Section 6.2 we prove an asymptotic formula for the number of irreducible polynomials over $\mathbb{F}_q$ whose coefficients satisfy some given linear equation. This may be regarded as a function field analogue of a famous result by Mauduit-Rivat [20] who showed that the sum of digits of rational primes written in a given base is equidistributed in arithmetic progressions. Our result answers (a generalisation of) Problem 1.1 from [39] and Open Problem 18 from [26], Section 4.4 for polynomials of degree at least 25.

6.1 Missing coefficients

6.1.1 Introduction

In this section we will prove a function field analogue of a result of Maynard [21] concerning primes with missing digits. He proved that for large enough integers b, the primes have the expected asymptotic density inside those integers that can be written in base b using only certain specified digits. We will prove the following natural analogue of this result for polynomials in $\mathbb{F}_q[t]$, explaining afterwards why it gives the 'expected asymptotic density'.

Theorem 6.1. *Let $\mathcal{R} \subset \mathbb{F}_q$ be a subset of size s and assume that s is less than $\sqrt{q}/2$.*

Suppose that $q \geq 500$ *and* $n \geq 100(\log q)^2$*. The number of irreducible, monic polynomials of degree* n *with coefficients only from* $\mathbb{F}_q \backslash \mathcal{R}$ *(except possibly the leading 1) is given by*

$$\frac{q}{q-1}\frac{(q-s)^n}{n}\left(\Lambda + O\left(q^{-n^{1/2}/7}\right)\right),$$

where

$$\Lambda = \begin{cases} 1 & \text{if } 0 \in \mathcal{R} \\ 1 - \frac{1}{q-s} & \text{if } 0 \notin \mathcal{R}. \end{cases}$$

Let us take a moment to explain why the constant Λ is entirely to be expected. If $0 \notin \mathcal{R}$, then restricting the coefficients of f to lie in $\mathbb{F}_q \backslash \mathcal{R}$ increases the chance that $f(0) = 0$ relative to those f chosen uniformly from $\mathcal{M}_n$. Now $f(0) = 0$ implies that t divides f, and therefore f is not prime. Conversely, if $0 \in \mathcal{R}$ then f is more likely to be such that $f(0) \neq 0$, and is therefore more likely to be prime. It is reasonable to suspect that this is the only real affect restricting the coefficients to lie in $\mathbb{F}_q \backslash \mathcal{R}$ has on the chance of f being prime (at least for large n and/or q). In other words, it is reasonable to expect that

$$\mathbb{P}(f \in \mathcal{P}_n \mid \text{coefficients of } f \notin \mathcal{R}) \approx \mathbb{P}(f \in \mathcal{P}_n \mid f(0) \notin \mathcal{R}).$$

By Bayes' theorem and the polynomial version of Dirichlet's theorem mod t, this is equal to

$$\frac{\mathbb{P}(f \in \mathcal{P}_n)}{\mathbb{P}(f(0) \notin \mathcal{R})}\mathbb{P}(f(0) \notin \mathcal{R} \mid f \in \mathcal{P}_n) \approx \frac{1}{n} \cdot \frac{1}{\frac{q-s}{q}} \cdot \begin{cases} \frac{q-s}{q-1} & \text{if } 0 \in \mathcal{R} \\ \frac{q-s-1}{q-1} & \text{if } 0 \notin \mathcal{R} \end{cases} = \frac{q}{q-1} \cdot \frac{\Lambda}{n}.$$

Since there are $(q-s)^n$ monic polynomials of degree n whose coefficients come only from $\mathbb{F}_q \backslash \mathcal{R}$, this explains the formula appearing in Theorem 6.1.

Remark. Beyond stipulating that $s < \sqrt{q}/2$, the constraints on the sizes of s, q and n in Theorem 6.1 are somewhat artificial, and were chosen with the aim of producing a more presentable error term. A more complicated, but more widely applicable error term is presented at the end of Section 6.1.4 from which the following two examples follow.

Example 6.1. In the special case of $s = 1$, we get an asymptotic formula for any $q \geq 17$. In particular, we show that the number of irreducible polynomials of degree n with a single coefficient from $\mathbb{F}_{17}$ unavailable is asymptotic to $\Lambda \frac{16}{17}(16)^n/n$ as $n \to \infty$.

Example 6.2. An asymptotic formula still holds in the case of fixed n and $q \to \infty$ provided that $s = o(q^{1/2})$.

As in the integer setting, we can take s to be larger when the set $\mathcal{R}$ has additional structure. For example, in Section 6.1.5 we will prove the following.

Theorem 6.2. *Suppose $\delta > 0$ and p is a prime sufficiently large in terms of δ. Then for any subset $\mathcal{R} = \{r, r+1, \dots, r+s-1\} \subset \mathbb{F}_p$ of s consecutive coefficients with $p - s > p^{3/4+\delta}$, the number of irreducible, monic polynomials of degree n with coefficients only from $\mathbb{F}_p \backslash \mathcal{R}$ (except possibly the leading 1) is given by*

$$\frac{p}{p-1}\frac{(p-s)^n}{n}\left(\Lambda + O\left(e^{-cn^{1/2}}\right)\right),$$

for some positive constant c depending on p and δ.

The integer version of Theorem 6.1 was proved in [21] under the assumption that the number of restricted digits s satisfies $s \leq b^{1/4-\delta}$ and the base b is sufficiently large in terms of δ. An analogue of Theorem 6.2 was proved under the assumption that $\mathcal{R} = \{0, 1, \dots, s-1\}$ and $s \leq b - b^{3/4+\delta}$. The proofs of Theorems 6.1 and 6.2 will use the circle method over $\mathbb{F}_q[t]$ along the lines of [15] and [21]. Two features make our arguments substantially simpler. First, we may make use of Weil's Riemann hypothesis for curves over a finite field which gives very good control for exponential sums over irreducibles. Second, we do not have to deal with any technicalities which arise from the fact that sometimes digits are 'carried' when rational integers are added. This doesn't happen with polynomials over a finite field.

For an overview of digit related results in the integers, see the recent work of Dietmann, Elsholtz and Shparlinski [11] which also contains a section on finite fields, improving an earlier result of Dartyge, Mauduit and Sárközy [8]. See also [25], which contains an extensive list of references to related problems.

6.1.2 Definitions and set up

We now define a few objects we will make use of in addition to those concepts defined in the previous chapters. Let $\mathcal{R} = \{r_1, \dots, r_s\} \subset \mathbb{F}_q$ be a subset of *forbidden* coefficients. We are interested in counting elements of $\mathcal{P}_n$, all of whose coefficients, apart from possibly the leading 1, are in the set $\mathcal{R}^c := \mathbb{F}_q \backslash \mathcal{R}$.

Fix a Haar measure on the additive group $\mathbb{T}$ normalised so that $\int_{\mathbb{T}} dx = 1$. Then for all $a \in \mathbb{F}_q[t]$, we have

$$\int_{\mathbb{T}} \mathbf{e}_q(ax)dx = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{if } a \neq 0. \end{cases}$$

For $x \in \mathbb{T}$, define the sum over monic irreducible polynomials of degree n

$$\widehat{\mathcal{P}_n}(x) = \sum_{\omega \in \mathcal{P}_n} \mathbf{e}_q(\omega x).$$

Let $\mathcal{M}_{\mathcal{R}}(n)$ be the set of monic polynomials of degree n with non-leading coefficients taken from $\mathcal{R}^c$ and define

$$S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx).$$

So $S_{\mathcal{R}}(x)$ depends on n even though this is not apparent from the notation. The main quantity of interest, the number of irreducible polynomials in $\mathcal{M}_{\mathcal{R}}(n)$, is then given by

$$N(\mathcal{R}, n) = \int_{\mathbb{T}} \widehat{\mathcal{P}_n}(x)\overline{S_{\mathcal{R}}(x)}dx. \tag{6.1}$$

We will make use of the important fact that for each $x \in \mathbb{T}$, there exist unique $a, g \in \mathbb{F}_q[t]$ with g monic, a and g coprime, and $|a| < |g| \leq q^{n/2}$ such that

$$\left| x - \frac{a}{g} \right| < \frac{1}{q^{\deg g + n/2}}.$$

This fact is Lemma 3 from [27]. It implies that we can partition $\mathbb{T}$ into the so-called Farey arcs as

$$\mathbb{T} = \bigcup_{\substack{|a|<|g|\leq q^{n/2} \\ (a,g)=1}} \mathcal{F}\left(\frac{a}{g}\,,\, q^{\deg g + n/2}\right)$$

where $\mathcal{F}\left(\frac{a}{g}\,,\,\lambda\right) = \{x \in \mathbb{T} \,:\, \left|\frac{a}{g} - x\right| < \frac{1}{\lambda}\}$.

6.1.3 Lemmas

The sum $\widehat{\mathcal{P}_n}(x)$ was analysed in [17]. Our first lemma is Lemma 5 in [27] and is a consequence of Weil's Riemann Hypothesis for curves over a finite field.

Lemma 6.1. *Let $a, g \in \mathbb{F}_q[t]$ be two polynomials with $(a, g) = 1$ and $\gamma \in \mathbb{T}$, satisfying*

$|a| < |g| \le q^{n/2}$ *and* $|\gamma| < 1/q^{\deg g + n/2}$. *We have*

$$\widehat{\mathcal{P}_n}\left(\frac{a}{g} + \gamma\right) = \frac{\mu(g)}{\phi(g)}\pi(n)\boldsymbol{e}_q(\gamma t^n)\boldsymbol{1}_{|\gamma|<1/q^n} + E$$

with $|E| \le q^{n-\frac{1}{2}[\frac{n}{2}]}$.

For a subset $A \subset \mathbb{F}_q$, define the Fourier coefficient $\widehat{\mathbf{1}_A}(r) := \sum_{n\in A}\psi(nr)$. It turns out that the average value of $|S_{\mathcal{R}}(x)|$ can be written quite neatly in terms of the Fourier coefficients of the set $\mathcal{R}^c$.

Lemma 6.2.

$$\int_{\mathbb{T}} |S_{\mathcal{R}}(x)|dx = \left(\frac{1}{q}\sum_{r\in\mathbb{F}_q} |\widehat{\boldsymbol{1}_{\mathcal{R}^c}}(r)|\right)^n.$$

Proof. First

$$\begin{aligned} S_{\mathcal{R}}(x) &= \sum_{m\in\mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx) \\ &= \mathbf{e}_q(xt^n)\prod_{i=0}^{n-1}\left(\sum_{n_i\in\mathcal{R}^c}\mathbf{e}_q(xn_it^i)\right) \\ &= \mathbf{e}_q(xt^n)\prod_{i=0}^{n-1}\left(\sum_{n_i\in\mathcal{R}^c}\psi(n_ix_{-i-1})\right). \end{aligned}$$

Notice that $|S_{\mathcal{R}}(x)|$ only depends on the leading n coefficients $(x_{-1},\dots,x_{-n})$ of x and so, for each $a \in \mathbb{F}_q[t]$, $|S_{\mathcal{R}}(a/t^n+\gamma)|$ is constant in the range $|\gamma| < 1/q^n$, a set of measure $1/q^n$. Therefore,

$$\begin{aligned}\int_{\mathbb{T}} \left|S_{\mathcal{R}}(x)\right|dx &= \frac{1}{q^n} \sum_{\deg a<n} \left|S_{\mathcal{R}}\left(\frac{a}{t^n}\right)\right| \\ &= \frac{1}{q^n} \sum_{\deg a<n} \left|\prod_{i=0}^{n-1} \sum_{n_i\in\mathcal{R}^c} \psi(n_i a_{n-i-1})\right| \\ &= \frac{1}{q^n} \sum_{\deg a<n} \prod_{i=0}^{n-1} \left|\widehat{\mathbf{1}_{\mathcal{R}^c}}(a_{n-i-1})\right| \\ &= \frac{1}{q^n} \left(\sum_{r\in\mathbb{F}_q} \left|\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)\right|\right)^n\end{aligned}$$

which completes the proof of the lemma. □

Corollary 6.1.

$$\int_{\mathbb{T}} |S_{\mathcal{R}}(x)|dx \le (\sqrt{s} + 1 - 2s/q)^n,$$

with equality in the case $s = 1$.

Proof. Notice that

$$\widehat{\mathbf{1}_{\mathcal{R}^c}}(r) + \widehat{\mathbf{1}_{\mathcal{R}}}(r) = \sum_{n\in\mathbb{F}_q} \psi(rn) = \begin{cases} q & \text{if } r = 0 \\ 0 & \text{if } r \neq 0. \end{cases}$$

And hence,

$$\sum_{r\in\mathbb{F}_q} |\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)| = \sum_{r\in\mathbb{F}_q\setminus 0} |\widehat{\mathbf{1}_{\mathcal{R}}}(r)| + |q - \widehat{\mathbf{1}_{\mathcal{R}}}(0)| = \sum_{r\in\mathbb{F}_q} |\widehat{\mathbf{1}_{\mathcal{R}}}(r)| + q - 2s.$$

It therefore suffices to show that $\sum_{r\in\mathbb{F}_q} |\widehat{\mathbf{1}_{\mathcal{R}}}(r)| \le q\sqrt{s}$. By the Cauchy–Schwarz inequality,

$$\begin{aligned}\left(\sum_{r\in\mathbb{F}_q} |\widehat{\mathbf{1}_{\mathcal{R}}}(r)|\right)^2 &\le \left(\sum_{r\in\mathbb{F}_q} 1\right)\left(\sum_{r\in\mathbb{F}_q} \left|\sum_{n\in\mathcal{R}} \psi(rn)\right|^2\right) \\ &= q \sum_{r\in\mathbb{F}_q} \sum_{n_1,n_2\in\mathcal{R}} \psi(r(n_1 - n_2)).\end{aligned}$$

By swapping the order of summation we see that the total contribution from the terms with $n_1 \neq n_2$ is 0. The terms $n_1 = n_2$ contribute $q^2 s$ as required. □

The next lemma is similar to Lemma 7 from [27].

Lemma 6.3. *Let $a, g \in \mathbb{F}_q[t]$ be coprime polynomials with $|a| < |g|$ and g not a power of t and let $d = \deg g > 0$. Then*

$$\left|S_{\mathcal{R}}(\frac{a}{g})\right| \leq (q-s)^{n-[\frac{n}{d}]}s^{[\frac{n}{d}]}.$$

Proof. Write $a/g = \sum_{i<0} x_i t^i$ and let z be the number of non-zeros amongst the x_i in the range $-n \leq i \leq -1$. Then, by our expression for $S_{\mathcal{R}}(a/q)$ from the start of the proof of Lemma 6.2 we have that

$$|S_{\mathcal{R}}(a/g)| = (q-s)^{n-z} \prod_{\substack{i=0 \\ x_{-i-1}\neq 0}}^{n-1} \left|\sum_{n_i \in \mathcal{R}} \psi(n_i x_{-i-1})\right| \leq (q-s)^{n-z}s^z$$

by the triangle inequality. Since $q - s \geq s$, it suffices to show that $z \geq [\frac{n}{d}]$. We use proof by contradiction. Suppose $z \leq [\frac{n}{d}] - 1$. Then, by the pigeonhole principle, there is some string of at least d consecutive zeros in $(x_{-n}, \ldots, x_{-1})$. Hence, $|\{t^r a/g\}| \leq 1/q^{d+1}$ for some integer $r \geq 0$ where $\{x\} = \sum_{i<0} x_i t^i$ denotes the fractional part of x. But this is a contradiction since g does not divide $t^r a$ so we must have $|\{t^r a/g\}| \geq 1/q^d$. □

Lemma 6.4. *For $d \leq n/2$ we have*

$$\sum_{\substack{\deg a < \deg g \leq d \\ (a,g)=1}} \left|S_{\mathcal{R}}\left(\frac{a}{g}\right)\right| \leq (q-s)^{n-2d}(q(1+\sqrt{s}) - 2s)^{2d}.$$

Proof. For any integer Y and $x \in \mathbb{T}$, define

$$S_{\mathcal{R}}^Y(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(Y)} \mathbf{e}_q(mx)$$

so that $S_{\mathcal{R}}(x) = S_{\mathcal{R}}^n(x)$. Then

$$\begin{aligned}|S_{\mathcal{R}}^n(x)| &= \left|\prod_{i=0}^{n-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\right| \\ &= \left|\prod_{i=0}^{Y-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\prod_{i=Y}^{n-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\right| \\ &= \left|S_{\mathcal{R}}^Y(x)S_{\mathcal{R}}^{n-Y}(xt^Y)\right|.\end{aligned}$$

Applying this with $Y = 2d$ gives

$$\begin{aligned}\sum_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}\left(\frac{a}{g}\right)\right| &= \sum_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}^{2d}\left(\frac{a}{g}\right)S_{\mathcal{R}}^{n-2d}\left(\frac{t^{2d}a}{g}\right)\right| \\ &\le \max_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}^{n-2d}\left(\frac{t^{2d}a}{g}\right)\right|\sum_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}^{2d}\left(\frac{a}{g}\right)\right| \\ &\le (q-s)^{n-2d}\sum_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}^{2d}\left(\frac{a}{g}\right)\right|,\end{aligned}$$

where we have used the trivial bound $|S_{\mathcal{R}}^{n-2d}(x)| \le (q-s)^{n-2d}$. Notice that $S_{\mathcal{R}}^{2d}(a/g+\gamma)$ is constant in the range $|\gamma| < 1/q^{2d}$ and recall that the Farey arcs $\mathcal{F}(a/g, q^{2d})$ are disjoint. Therefore

$$\frac{1}{q^{2d}}\sum_{\substack{\deg a<\deg g\le d\\(a,g)=1}}\left|S_{\mathcal{R}}^{2d}\left(\frac{a}{g}\right)\right| = \sum_{a,q}\int_{\mathcal{F}(a/g,q^{2d})}\left|S_{\mathcal{R}}^{2d}\left(\frac{a}{g}+\gamma\right)\right|d\gamma \le (\sqrt{s}+1-2s/q)^{2d}$$

by Corollary 6.1 where the sum is over all distinct fractions a/g with $\deg g \le d$. □

We make use of the following simple bound which is similar to Lemma 5.4 from the previous chapter.

Lemma 6.5. *For each $g \in \mathbb{F}_q[t]$ we have*

$$\frac{q^{\deg g}}{\phi(g)} = \prod_{\omega|g}\left(1-\frac{1}{q^{\deg\omega}}\right)^{-1} \le (1+\log_q(\deg g))e^2.$$

Proof. Arrange the monic, irreducibles $\omega_1, \dots, \omega_r$ dividing g and the monic irreducibles $P_1, \dots$ in $\mathbb{F}_q[t]$ in order of degree (ordering those of the same degree arbitrarily). Then we

must have that $\deg P_i \leq \deg \omega_i$. Now, for some N, we have that $\sum_{P:\deg P\leq N-1} \deg P < \deg g \leq \sum_{P:\deg P\leq N} \deg P$. This implies that g has at most $\pi(N)$ irreducible factors, and so, since $\deg P_i \leq \deg \omega_i$ we have

$$\prod_{\omega|g}(1-q^{-\deg \omega})^{-1} \leq \prod_{P:\deg P\leq N}(1-q^{-\deg P})^{-1}.$$

Taking the logarithm of the right hand side, and using the fact that $-\log(1-\frac{1}{x}) \leq \frac{1}{x-1}$ for $x>1$, and that $\sum_{d|r} d\pi(d) = q^r$ so $\pi(r)r \leq q^r - 1$ for $r > 1$ we get

$$\sum_{P:\deg P\leq N} -\log(1-q^{-\deg P}) \leq \sum_{r\leq N} \frac{\pi(r)}{q^r-1} \leq \frac{q}{q-1} + \sum_{2\leq r\leq N} \frac{1}{r} \leq 2 + \log N.$$

Now N is bounded in terms of $\deg g$ as follows,

$$\deg g > \sum_{P:\deg P\leq N-1} \deg P = \sum_{r\leq N-1} \pi(r)r \geq \sum_{r|N-1} \pi(r)r = q^{N-1},$$

and hence $N \leq 1 + \log_q \deg g$. Combining these inequalities gives the result. □

6.1.4 Proof of Theorem 6.1

Recall that our aim is to evaluate $N(\mathcal{R},n) = \int_{\mathbb{T}} \widehat{\mathcal{P}_n}(x)\overline{S_{\mathcal{R}}(x)}dx$. Now each $x \in \mathbb{T}$ can be written as $a/g+\gamma$ for unique a, g, γ as in Lemma 6.1 which allows us to write

$$N(\mathcal{R},n) = \int_{\mathbb{T}} \overline{S_{\mathcal{R}}(x)} \left(\frac{\mu(g)}{\phi(g)} \pi(n)\mathbf{e}_q(\gamma t^n)\mathbf{1}_{|\gamma|<1/q^n} + E \right) dx,$$

where $|E| \leq q^{n-\frac{1}{2}[\frac{n}{2}]}$ uniformly. The error term is bounded by using Corollary 6.1 as

$$\left| \int_{\mathbb{T}} \overline{S_{\mathcal{R}}(x)} E dx \right| \leq q^{n-\frac{1}{2}[\frac{n}{2}]}(\sqrt{s}+1-2s/q)^n. \tag{6.2}$$

We can write what's left as

$$\int_{\mathbb{T}} \overline{S_{\mathcal{R}}(x)} \frac{\mu(g)}{\phi(g)} \pi(n)\mathbf{e}_q(\gamma t^n)\mathbf{1}_{|\gamma|<1/q^n} dx = \sum_{a,g} \int_{\mathcal{F}(a/g,\, q^n)} \overline{S_{\mathcal{R}}\left(\frac{a}{g}+\gamma\right)} \frac{\mu(g)}{\phi(g)} \pi(n)\mathbf{e}_q(\gamma t^n) d\gamma$$

where the sum is over all distinct fractions a/g such that $\deg g \leq n/2$. These are the so-called major arcs.

Since $|\gamma| < 1/q^n$, from the definition we get

$$S_{\mathcal{R}}\left(\frac{a}{g}+\gamma\right) = \sum_{m\in\mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(am/g)\mathbf{e}_q(m\gamma) = \mathbf{e}_q(\gamma t^n) S_{\mathcal{R}}\left(\frac{a}{g}\right)$$

and therefore, since the integrand is constant on each of these major arcs which have measure $1/q^n$ the contribution becomes

$$\frac{\pi(n)}{q^n}\sum_{a,g}\overline{S_{\mathcal{R}}\left(\frac{a}{g}\right)}\frac{\mu(g)}{\phi(g)}. \tag{6.3}$$

Let us first analyse the terms with $g = 1$ and $g = t$, that is, look at

$$M = \frac{\pi(n)}{q^n}\left(S_{\mathcal{R}}(0) + \sum_{b\in\mathbb{F}_q\setminus 0}\overline{S_{\mathcal{R}}\left(\frac{b}{t}\right)}\frac{\mu(t)}{\phi(t)}\right).$$

The $g = 1$ term gives $S_{\mathcal{R}}(0) = (q-s)^n$. Using our expression for $S_{\mathcal{R}}(\frac{b}{t})$ from the start of the proof of Lemma 6.2, the terms $g = t$ are

$$\sum_{b\in\mathbb{F}_q\setminus 0} S_{\mathcal{R}}(\tfrac{b}{t}) = (q-s)^{n-1}\sum_{b\in\mathbb{F}_q\setminus 0}\sum_{n\in\mathcal{R}^c}\mathbf{e}_q(\tfrac{nb}{t}) = -(q-s)^{n-1}\sum_{b\in\mathbb{F}_q\setminus 0}\sum_{r\in\mathcal{R}}\psi(br).$$

Using

$$\sum_{b\in\mathbb{F}_q\setminus 0}\psi(br) = \begin{cases} q-1 & \text{if } r=0\\ -1 & \text{if } r\neq 0,\end{cases}$$

this becomes

$$\begin{cases} -(q-s)^n & \text{if } 0\in\mathcal{R}\\ (q-s)^{n-1}s & \text{if } 0\notin\mathcal{R}.\end{cases}$$

Hence, since $\mu(t) = -1$ and $\phi(t) = q-1$ we have

$$\begin{aligned} M &= \frac{\pi(n)}{q^n}\left((q-s)^n - \frac{1}{q-1}\sum_{b\in\mathbb{F}_q\setminus 0} S_{\mathcal{R}}(b/t)\right)\\ &= \frac{q\Lambda}{q-1}\pi(n)(1-s/q)^n,\end{aligned}$$

where

$$\Lambda = \begin{cases} 1 & \text{if } 0 \in \mathcal{R} \\ 1 - \frac{1}{q-s} & \text{if } 0 \notin \mathcal{R}. \end{cases}$$

Using $\pi(n) \le q^n/n$, the remaining terms in (6.3) are bounded by

$$\frac{1}{n} \sum_{\substack{1 \le \deg g \le n/2 \\ g \ne t}} \frac{|\mu(g)|}{\phi(g)} \sum_{\substack{\deg a < \deg g \\ (a,g)=1}} \left| S_{\mathcal{R}}\left(\frac{a}{g}\right)\right|.$$

Let U be some parameter $1 \le U \le n/2$ to be specified shortly. Grouping the g according to their degree and using Lemma 6.3 for the terms with $d = \deg g \le U$ and Lemmas 6.4 and 6.5 for the terms with $\deg g > U$ we get

$$\begin{aligned}
&\sum_{\substack{1 \le \deg g \le n/2 \\ g \ne t}} \frac{|\mu(g)|}{\phi(g)} \sum_{\substack{\deg a < \deg g \\ (a,g)=1}} \left| S_{\mathcal{R}}\left(\frac{a}{g}\right)\right| \\
&\le \sum_{1 \le d \le U} q^d (q-s)^{n-[\frac{n}{d}]} s^{[\frac{n}{d}]} + e^2 \sum_{U < d \le n/2} q^{-d} (q-s)^{n-2d} (q(1+\sqrt{s}) - 2s)^{2d} (1 + \log_q(d)) \\
&= (q-s)^n \left(\sum_{1 \le d \le U} q^d \left(\frac{s}{q-s}\right)^{[\frac{n}{d}]} + e^2 \sum_{U < d \le n/2} q^d \left(\frac{1+\sqrt{s}-2s/q}{q-s}\right)^{2d} (1 + \log_q(d)) \right) \\
&\ll (q-s)^n \left(n \left(q^U \left(\frac{s}{q-s}\right)^{n/U} + q^{U/2} \left(\frac{\sqrt{s}+1-2s/q}{q-s}\right)^U \right) \right)
\end{aligned}$$

We have trivially bounded the first sum. The bound for the second sum follows after using $1 + \log_q(d) \le n$ and bounding the resulting geometric sum using $s \le \sqrt{q}/2$ so that

$$\frac{\sqrt{q}(\sqrt{s}+1-2s/q)}{q-s} \le \frac{q/2+\sqrt{q}}{q-\sqrt{q}/2} < 1$$

for $q \ge 11$. Taking $U = (2n/5)^{1/2}$ and using $s \le \sqrt{q}/2$ this becomes

$$\begin{aligned}
&\ll (q-s)^n \left(n \left(q^{\sqrt{\frac{2}{5}n}} \left(\frac{q^{1/2}}{2q-q^{1/2}}\right)^{\sqrt{\frac{5}{2}n}} + q^{\sqrt{\frac{1}{10}n}} \left(\frac{q^{1/4}/\sqrt{2}+1}{q-q^{1/2}/2}\right)^{\sqrt{\frac{2}{5}n}} \right) \right) \\
&\ll n(q-s)^n q^{-n^{1/2}/(2\sqrt{10})},
\end{aligned}$$

since $\sqrt{\frac{2}{5}} - \frac{1}{2}\sqrt{\frac{5}{2}} = -\frac{1}{2\sqrt{10}}$ and $\sqrt{\frac{1}{10}} - \frac{3}{4}\sqrt{\frac{2}{5}} = -\frac{1}{2\sqrt{10}}$. Combining this with our expression

for the main term M and error estimate (6.2) we get

$$N(\mathcal{R}, n) = \frac{q}{q-1}\frac{(q-s)^n}{n}\left(\Lambda + O\left(n\mathcal{E}\right)\right) \tag{6.4}$$

where

$$\mathcal{E} \ll q^{-n^{1/2}/(2\sqrt{10})} + \left(\frac{q^{3/4}(s^{1/2}+1)}{q-s}\right)^n. \tag{6.5}$$

Since $s \leq \sqrt{q}/2$, we then have

$$\mathcal{E} \ll q^{-n^{1/2}/(2\sqrt{10})} + \left(\frac{q/\sqrt{2}+q^{3/4}}{q-\sqrt{q}/2}\right)^n. \tag{6.6}$$

A calculation reveals that for $n \geq 100(\log q)^2$, the first expression is larger then the second when $q \geq 500$ and that both are $\ll q^{-n^{1/2}/7}/n$ which completes the proof of Theorem 6.1.

Remark. The conditions on the sizes of s, q and n were made in order to simplify the statement of Theorem 6.1 but (6.5) is also interesting for other choices. For example, when n is fixed, we have that $\mathcal{E} \to 0$ as $q \to \infty$ provided $s = o(q^{1/2})$.

Recall that in the special case $s = 1$, we have equality in Corollary 6.1. Feeding this through the rest of the proof gives

$$\mathcal{E} \ll q^{-n^{1/2}/(2\sqrt{10})} + \left(\frac{q^{3/4}(2-2/q)}{q-1}\right)^n.$$

For $q \geq 17$, the expression in the brackets is less than 1 which proves $n\mathcal{E} \to 0$ as $n \to \infty$ in this case.

6.1.5 Proof of Theorem 6.2

Our proof of Theorem 6.2 is the same as Theorem 6.1 except that we use modified versions of Corollary 6.1 and Lemma 6.3 which we will now prove. In this section, we assume that p is a prime, $\mathcal{R} \subset \mathbb{F}_p$ is subset of consecutive coefficients and use the same notation already introduced.

Corollary 6.2.

$$\int_{\mathbb{T}} |S_{\mathcal{R}}(x)|dx \leq (\log p + 1 - s/p)^n.$$

Proof. Write $\mathcal{R} = \{d, d+1, \dots, d+s-1\}$, then, if $r = 0$, $|\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)| = p - s$, and if $r \neq 0$,

$$|\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)| = \left| \sum_{k=d}^{d+s-1} e^{2\pi i k r/p} \right| = \left| \frac{1 - e^{2\pi i s r/p}}{1 - e^{2\pi i r/p}} \right| \leq \frac{1}{|\sin \pi r/p|}.$$

Therefore,

$$\sum_{r \in \mathbb{F}_p} |\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)| \leq p - s + \sum_{r=1}^{p-1} \frac{1}{|\sin \pi r/p|} < p - s + 2 \sum_{r=1}^{\frac{p-1}{2}} \frac{p}{2r} < p - s + p \log p.$$

Now use Lemma 6.2. □

Consequently, the bound in Lemma 6.4 is replaced by $(p-s)^{n-2d}(p(\log p + 1) - s)^{2d}$.

Lemma 6.6. *Let $a, g \in \mathbb{F}_p[t]$ be coprime polynomials with $|a| < |g|$ and g not a power of t and let $d = \deg g > 0$. Then*

$$|S_{\mathcal{R}}(a/g)| \leq (p-s)^n e^{-[\frac{n}{d}]\frac{1}{p^3}}.$$

Proof. As in the proof of Lemma 6.3 we have

$$|S_{\mathcal{R}}(a/g)| = (p-s)^{n-z} \prod_{\substack{i=0 \\ x_{-i-1} \neq 0}}^{n-1} \left| \sum_{n_i \in \mathcal{R}} e^{2\pi i (n_i x_{-i-1})/p} \right|.$$

For $x \in \mathbb{F}_p \backslash \{0\}$, we have

$$\left| e^{2\pi i \frac{x}{p} n} + e^{2\pi i \frac{x}{p}(n+1)} \right|^2 = 2 + 2\cos(\frac{2\pi x}{p}) < 4e^{-2/p^2},$$

and therefore

$$\left| \sum_{n_i \in \mathcal{R}} e^{2\pi i (n_i x_{-i-1})/p} \right| \leq p - s - 2 + 2e^{-1/p^2} \leq (p-s)e^{-1/p^3}.$$

Recalling from the proof of Lemma 6.3 that $z \geq [n/d]$ completes the proof. □

Provided p is large enough to ensure that $\frac{\sqrt{p}(\log p + 1 - s/p)}{p-s} < 1$ (so the resulting geometric sum we saw earlier converges) we may just insert these new bounds into the proof

of Theorem 6.1 to get (6.4) with

$$\mathcal{E} \ll p^U e^{-[\frac{n}{U}]\frac{1}{p^3}} + \left(\frac{\sqrt{p}(\log p + 1 - s/p)}{p-s}\right)^U + \left(\frac{p^{3/4}(\log p + 1 - s/p)}{p-s}\right)^n$$

for some parameter U. Taking $U = cn^{1/2}$, and since we are assuming $p - s > p^{3/4+\delta}$, this proves Theorem 6.2 for some $c > 0$ sufficiently small in terms of p and δ.

6.2 Linear forms in coefficients

Let $n \geq 3$ be an integer and for any $L = (L_0, \ldots, L_{n-1}) \in \mathbb{F}_q^n$, define the *sum-of-coefficients function* $\mathcal{S}_L : \mathcal{M}_n \to \mathbb{F}_q$ of $f(t) = t^n + f_{n-1}t^{n-1} + \cdots + f_0$ to be

$$\mathcal{S}_L(f) = \sum_{0 \leq i \leq n-1} L_i f_i.$$

The main result of this section is that

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} = \frac{q^{n-1}}{n}\Lambda + O(q^{n-\frac{1}{2}[\frac{n}{2}]})$$

for some (possibly zero) number Λ. This number, Λ, depends on the closest rational approximation b/h to $\sum_{0 \leq i \leq n-1} \frac{L_i}{t^{i+1}}$ in the field of fractions $\mathbb{F}_q(t)$ with $\deg h \leq n/2$. The precise statement of our Theorem is therefore slightly technical.

Theorem 6.3. *Let $L = (L_0, \ldots, L_{n-1}) \in \mathbb{F}_q^n \backslash \{0\}^n$ and $r \in \mathbb{F}_q$. Define $\widetilde{L} = \sum_{0 \leq i \leq n-1} \frac{L_i}{t^{i+1}}$ and let $b/h = \sum_{i<0} \theta_i t^i$ be the unique rational function with $|b| < |h| \leq q^{n/2}$, $(b, h) = 1$ and h monic such that $|\widetilde{L} - b/h| < 1/q^{\deg h + n/2}$. (Recall that b and h are uniquely defined by these properties.) Then*

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} = \frac{\pi(n)}{q}\Lambda + O(q^{n-\frac{1}{2}[\frac{n}{2}]})$$

where

$$\Lambda = \begin{cases} 1 & \text{if } |\widetilde{L} - b/h| \geq 1/q^n \\ 1 + \frac{\mu(h)}{\phi(h)}(q-1) & \text{if } |\widetilde{L} - b/h| < 1/q^n \text{ and } r = -\theta_{-n-1} \\ 1 - \frac{\mu(h)}{\phi(h)} & \text{if } |\widetilde{L} - b/h| < 1/q^n \text{ and } r \neq -\theta_{-n-1} \end{cases}$$

The implied constant may be taken to be 1.

6.2.1 Existence result

The following problem was posed by Tuxanidy and Wang in [39]:

Problem. Let $n \geq 2$. For what elements $r \in \mathbb{F}_q$ and subsets $A \subset \{0, 1, \ldots, n-1\}$ can we find irreducible polynomials $f(t) = t^n + \sum_{0 \leq i \leq n-1} f_i t^i$ such that $\sum_{i \in A} f_i = r$?

They solve this problem in the case $q = 2$ by proving that such an irreducible exists provided $(A, r) \neq (\{0\}, 0)$ or $(\{0, 1 \ldots, n-1\}, 1)$. If (A, r) did equal $(\{0\}, 0)$ or $(\{0, 1 \ldots, n-1\}, 1)$, then any f with $\sum_{i \in A} f_i = r$ would be divisible by t or $t + 1$ respectively and so

would not be irreducible. For general q, we see that for each $a \in \mathbb{F}_q$, divisibility by $t-a$ is equivalent to the coefficients of f satisfying some linear equation. In particular, f is divisible by $t-a$ if and only if $f(a) = a^n + \sum_{0\le i\le n-1} a^i f_i = 0$.

Theorem 6.3 can be used to show that these linear forms arising from divisibility by linear factors are the *only* obstructions to the existence of irreducible polynomials with prescribed sums of coefficients. By specialising to the case $L_i \in \{0,1\}$, this answers the problem posed above when $q \ge 3$ and $n \ge 25$.

Theorem 6.4. *Supose $q \ge 3$ and $n \ge 25$ and use the same notation as in Theorem 6.3.*

- *If $L \ne (v, vu, vu^2, \dots, vu^{n-1})$ for all $u, v \in \mathbb{F}_q$ then*

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} > 0 \text{ for all } r \in \mathbb{F}_q.$$

- *If $L = (v, vu, vu^2, \dots, vu^{n-1})$ for some $u, v \in \mathbb{F}_q$ then*

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} > 0 \text{ if and only if } r \ne -vu^n.$$

Proof. For each L there is a unique monic h of degree at most $n/2$ such that $|\widetilde{L} - b/h| < 1/q^{\deg h + n/2}$. We will split the proof into the three cases $\deg h \ge 2$, $\deg h = 1$ and $h = 1$.

Case 1: $\deg h \ge 2$.

It follows from Theorem 6.3 that for any r and any L,

$$\begin{aligned}\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} &\ge \frac{\pi(n)}{q}\left(1 - \frac{q-1}{\phi(h)}\right) - q^{n-\frac{1}{2}[\frac{n}{2}]} \\ &\ge \frac{\pi(n)}{q}\left(1 - \frac{1}{q-1}\right) - q^{n-\frac{1}{2}[\frac{n}{2}]}.\end{aligned}$$

Using the explicit inequality $\pi(n) \ge \frac{q^n}{n} - 2\frac{q^{n/2}}{n}$, this is > 0 for all $n \ge 25$.

Case 2: $\deg h = 1$.

Say, $h = t - u$ where $u \in \mathbb{F}_q$ and $b = v \in \mathbb{F}_q \backslash \{0\}$, then we have

$$\widetilde{L} = \sum_{0\le i\le n-1} \frac{L_i}{t^{i+1}} = \frac{v}{t-u} + \delta = v\left(\frac{1}{t} + \frac{u}{t^2} + \frac{u^2}{t^3} + \cdots\right) + \delta,$$

for some δ with $|\delta| < 1/q^{n/2+1}$. If $|\delta| \geq 1/q^n$, then Theorem 6.3 implies

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} \geq \frac{\pi(n)}{q} - q^{n-\frac{1}{2}[\frac{n}{2}]} > 0.$$

Otherwise $\delta < 1/q^n$, and so $L_i = vu^i$ for all $0 \leq i \leq n-1$. Since $\theta_{-n-1} = vu^n$, Theorem 6.3 then says

$$\begin{aligned}\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} &= \begin{cases} \frac{\pi(n)}{q}\left(1 + \frac{\mu(h)}{\phi(h)}(q-1)\right) + O(q^{n-\frac{1}{2}[\frac{n}{2}]}) & \text{if } r = -vu^n \\ \frac{\pi(n)}{q}\left(1 - \frac{\mu(h)}{\phi(h)}\right) + O(q^{n-\frac{1}{2}[\frac{n}{2}]}) & \text{if } r \neq -vu^n \end{cases} \\ &= \begin{cases} O(q^{n-\frac{1}{2}[\frac{n}{2}]}) & \text{if } r = -vu^n \\ \frac{\pi(n)}{q-1} + O(q^{n-\frac{1}{2}[\frac{n}{2}]}) & \text{if } r \neq -vu^n. \end{cases}\end{aligned}$$

In fact, $\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = -vu^n\} = 0$ because $\mathcal{S}_L(f) = -vu^n$ implies $vf(u) = \mathcal{S}_L(f) + vu^n = 0$ so $t - u$ divides f.

Case 3: $h = 1$.

In this case, we can argue as above that $|\widetilde{L}| < 1/q^n$ implies $L = 0$, which we are not allowing. Hence we have $|\widetilde{L}| \geq 1/q^n$ and so

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} \geq \frac{\pi(n)}{q} - q^{n-\frac{1}{2}[\frac{n}{2}]} > 0. \quad \square$$

6.2.2 Proofs

Fix an $L = (L_0, \ldots, L_{n-1}) \in \mathbb{F}_q^n \backslash \{0\}^n$ and define the polynomials b and h and the rational functions $\widetilde{L} = \sum_{0 \leq i \leq n-1} \frac{L_i}{t^{i+1}}$ and the coefficients θ_i by $b/h = \sum_{i<0} \theta_i t^i$ all as in the statement of Theorem 6.3. Note that all of these quantities only depend on L. For $\alpha \in \mathbb{T}$ and $k \in \mathbb{F}_q$, define the following exponential sums

$$\begin{aligned}\widehat{\mathcal{P}_n}(\alpha) &= \sum_{f \in \mathcal{P}_n} \mathbf{e}_q(f\alpha) \\ F_{L,k}(\alpha) &= \sum_{f \in \mathcal{M}_n} \psi(k\mathcal{S}_L(f))\mathbf{e}_q(f\alpha) \\ G_L(k) &= \sum_{f \in \mathcal{P}_n} \psi(-k\mathcal{S}_L(f)).\end{aligned}$$

We first reduce the problem to understanding $G_L(k)$.

Lemma 6.7.

$$\#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} = \frac{1}{q}\sum_{k\in\mathbb{F}_q} \psi(kr)G_L(k).$$

Proof. By the orthogonality of characters the left hand side is

$$\sum_{f\in\mathcal{M}_n} \mathcal{P}_n(f)\mathbf{1}_{\mathcal{S}_L(f)=r} = \sum_{f\in\mathcal{M}_n} \mathcal{P}_n(f)\frac{1}{q}\sum_{k\in\mathbb{F}_q} \psi(k(r-\mathcal{S}_L(f)))$$

which is equal to the right hand side. □

Next, we rewrite $G_L(k)$ using $\widehat{\mathcal{P}_n}(\alpha)$ and $F_{L,k}(\alpha)$.

Lemma 6.8.

$$G_L(k) = \int_{\mathbb{T}} \widehat{\mathcal{P}_n}(\alpha)\overline{F_{L,k}(\alpha)}d\alpha.$$

Proof. Again, expanding and using orthogonality both sides are equal to

$$\sum_{f,g\in\mathcal{M}_n} \mathcal{P}_n(f)\psi(-k\mathcal{S}_L(g)) \int_{\mathbb{T}} \mathbf{e}_q\left((f-g)\alpha)\right) d\alpha. \quad \square$$

As for the problem of missing coefficients from Section 6.1, it turns out we have quite a nice analytic description for the exponential sum over our polynomials with special coefficients, $F_{L,k}(\alpha)$.

Lemma 6.9. *For $\alpha \in \mathbb{T}$ write $\alpha = \sum_{i<1} \alpha_i t^i$.*

$$\frac{1}{q^n}F_{L,k}(\alpha) = \begin{cases} \psi(\alpha_{-n-1}) & \text{if } \alpha_{-i-1} = -kL_i \text{ for all } 0 \le i \le n-1 \\ 0 & \text{otherwise .} \end{cases}$$

Proof.

$$\begin{aligned} F_{L,k}(\alpha) = \sum_{f\in\mathcal{M}_n} \psi(k\mathcal{S}_L(f))\mathbf{e}_q(f\alpha) &= \sum_{f\in\mathcal{M}_n} \psi\left(k\sum_{0\le i\le n-1} f_iL_i + \sum_{0\le i\le n-1} f_i\alpha_{-i-1} + \alpha_{-n-1}\right) \\ &= \psi(\alpha_{-n-1})\sum_{f\in\mathcal{M}_n} \psi\left(\sum_{0\le i\le n-1} f_i(kL_i+\alpha_{-i-1})\right) \\ &= \psi(\alpha_{-n-1})\prod_{0\le i\le n-1}\left(\sum_{n_i\in\mathbb{F}_q} \psi\left(n_i(kL_i+\alpha_{-i-1})\right)\right) \\ &= \psi(\alpha_{-n-1})\prod_{0\le i\le n-1}\left(q\mathbf{1}_{\alpha_{-i-1}+kL_i=0}\right). \end{aligned}$$

□

We will shortly see how to combine Lemmas 6.8 and 6.9 with Lemma 6.1 concerning the sum over primes to get the following final Lemma.

Lemma 6.10.

$$G_L(k) = \lambda\pi(n) + O(q^{n-\frac{1}{2}[\frac{n}{2}]})$$

where

$$\lambda = \begin{cases} 1 & \text{if } k = 0 \\ \mathbf{1}_{|\widetilde{L}-b/h|<1/q^n} \frac{\mu(h)}{\phi(h)} \psi\left(k\theta_{-n-1}\right) & \text{if } k \neq 0. \end{cases}$$

Before we prove this final Lemma, let us see how it implies Theorem 6.3.

Proof. (Of Theorem 6.3).

$$\begin{aligned} \#\{f \in \mathcal{P}_n \mid \mathcal{S}_L(f) = r\} &= \frac{1}{q} \sum_{k \in \mathbb{F}_q} \psi(kr) G_L(k) && \text{(by Lemma 6.7)} \\ &= \frac{\pi(n)}{q} \left(1 + \frac{\mu(h)}{\phi(h)} \mathbf{1}_{|\widetilde{L}-b/h|<1/q^n} \sum_{k \in \mathbb{F}_q \setminus \{0\}} \psi\left(k(r + \theta_{-n-1})\right) \right) \\ &\qquad + O\left(q^{n-\frac{1}{2}[\frac{n}{2}]}\right) && \text{(by Lemma 6.10)} \\ &= \frac{\pi(n)}{q} \left(1 + \frac{\mu(h)}{\phi(h)} \mathbf{1}_{|\widetilde{L}-b/h|<1/q^n} \left(q\mathbf{1}_{\theta_{-n-1}=-r} - 1 \right) \right) + O(q^{n-\frac{1}{2}[\frac{n}{2}]}). \square \end{aligned}$$

Proof. (Of Lemma 6.10).

For any $\alpha \in \mathbb{T}$, there are unique a, g, γ satisfying the conditions of Lemma 6.1. It therefore makes sense to write

$$\begin{aligned} G_L(k) &= \int_{\mathbb{T}} \widehat{\mathcal{P}_n}(\alpha) \overline{F_{L,k}(\alpha)} d\alpha && \text{(by Lemma 6.8)} \\ &= q^n \int_{\mathbb{T}} \psi\left(-\alpha_{-n-1}\right) \mathbf{1}_{\alpha \in \Omega_{L,k}} \left(\frac{\mu(g)}{\phi(g)} \pi(n) \mathbf{e}_q(\gamma t^n) \mathbf{1}_{|\gamma|<1/q^n} + E \right) d\alpha \end{aligned}$$

where $\Omega_{L,k} = \{\alpha \in \mathbb{T} \ : \ \alpha_{-i-1} = -kL_i \text{ for all } 0 \leq i \leq n-1\}$ by Lemmas 6.1 and 6.9. Now, $\Omega_{L,k}$ is a set of measure $1/q^n$ and therefore, using $|E| \leq q^{n-\frac{1}{2}[\frac{n}{2}]}$ and the triangle inequality, we get

$$G_L(k) = \pi(n) q^n \int_{\mathbb{T}} \frac{\mu(g)}{\phi(g)} \psi\left(\gamma_{-n-1} - \alpha_{-n-1}\right) \mathbf{1}_{\alpha \in \Omega_{L,k}} \mathbf{1}_{|\gamma|<1/q^n} d\alpha + O(q^{n-\frac{1}{2}[\frac{n}{2}]}).$$

Let us focus on the integral

$$\int_{\mathbb{T}} \frac{\mu(g)}{\phi(g)} \psi\left(\gamma_{-n-1} - \alpha_{-n-1}\right) \mathbf{1}_{\alpha \in \Omega_{L,k}} \mathbf{1}_{|\gamma|<1/q^n} d\alpha.$$

Recall that $\widetilde{L} = \sum_{0 \le i \le n-1} \frac{L_i}{t^{i+1}}$ and notice that $\Omega_{L,k} = \mathcal{F}(-k\widetilde{L}, q^n)$. The key point is that $\widetilde{L}$ is contained in the unique Farey arc $\mathcal{F}(b/h, q^{\deg g + n/2})$ and that the integral is over the intersection of two open balls $\mathcal{F}(-kb/h, q^n) \cap \mathcal{F}(-k\widetilde{L}, q^n)$.

Since $|\cdot|$ is an ultrametric, any point in an open ball is a centre of that ball. Therefore there are two cases. Either $|\widetilde{L} - b/h| \ge 1/q^n$, in which case this intersection is empty. Or else $|\widetilde{L} - b/h| < 1/q^n$, in which case $\mathcal{F}(-kb/h, q^n) = \mathcal{F}(-k\widetilde{L}, q^n)$ and so the region of integration is a set of measure $1/q^n$. On this set we have $\alpha = -kb/h + \gamma$ and so $\gamma_{-n-1} - \alpha_{-n-1} = k\theta_{-n-1}$. Hence the integrand is constant over the region of integration and equal to $\frac{\mu(h)}{\phi(h)} \psi\left(k\theta_{-n-1}\right)$. This completes the proof of Lemma 6.10. □

6.2.3 Multiple forms

We end this section with a suggestion and line of enquiry for further work concerning the existence of irreducible polynomials whose coefficients satisfy multiple linear constraints. Fix an $\mathbf{L} = (L_{ij}) \in \mathbb{F}_q^{n \times m}$ of full rank and define functions $\widetilde{L_j} = \sum_{0 \le i \le n-1} \frac{L_{ij}}{t^{i+1}}$ for $1 \le j \le m$. Let $\mathbf{r} \in \mathbb{F}_q^m$. Define also the exponential sums

$$F_{\mathbf{L},\mathbf{k}}(\alpha) = \sum_{f \in \mathcal{M}_n} \psi(-\mathbf{k} \cdot \mathcal{S}_{\mathbf{L}}(f)) \mathbf{e}_q(f\alpha)$$
$$G_{\mathbf{L}}(\mathbf{k}) = \sum_{f \in \mathcal{P}_n} \psi(\mathbf{k} \cdot \mathcal{S}_{\mathbf{L}}(f)).$$

Everything presented above for the $m = 1$ case goes through the same and we end up with the following result.

Theorem 6.5. *Let $\boldsymbol{L} = (L_{ij}) \in \mathbb{F}_q^{n \times m}$ and $\boldsymbol{r} \in \mathbb{F}_q^m$. Define $\widetilde{\boldsymbol{L}_j} = \sum_{0 \le i \le n-1} \frac{L_{ij}}{t^{i+1}}$ and let $b/h = \sum_{i<0} \theta_i t^i$ be the unique rational function with $|b| < |h| \le q^{n/2}$, $(b,h) = 1$ and h monic such that $|\boldsymbol{k} \cdot \widetilde{\boldsymbol{L}} - b/h| < 1/q^{\deg h + n/2}$. Then*

$$\#\{f \in \mathcal{P}_n \,|\, \mathcal{S}_{\boldsymbol{L}}(f) = \boldsymbol{r}\} = \frac{\pi(n)}{q^m} \sum_{\boldsymbol{k} \in \mathbb{F}_q^m} \frac{\mu(h)}{\phi(h)} \boldsymbol{1}_{|\boldsymbol{k} \cdot \widetilde{\boldsymbol{L}} - b/h| < 1/q^n} \psi\left(\boldsymbol{k} \cdot \boldsymbol{r} + (b/h)_{-n-1}\right) + O(q^{n - \frac{1}{2}[\frac{n}{2}]})$$

where the implied constant may be taken to be 1.

This main term here can also be written as

$$\frac{\pi(n)}{q^m} \sum_{\substack{\deg b<\deg h \\ (b,h)=1 \\ h \text{ monic}}} \frac{\mu(h)}{\phi(h)} \sum_{\substack{\mathbf{k}\in\mathbb{F}_q^m \\ |\mathbf{k}\cdot\widetilde{\mathbf{L}}-b/h|<1/q^n}} \psi\left(\mathbf{k}\cdot\mathbf{r}+(b/h)_{-n-1}\right).$$

It would be interesting to know when this "main term" is actually positive. In particular, we saw that the obstruction to the existence of irreducibles with coefficients satisfying a single given linear condition came from the fact that certain linear constraints came from a divisibility condition on a linear polynomial. Perhaps the existence of irreducibles with coefficients satisfying m given linear conditions comes from divisibility conditions concerning polynomial of degree up to m. This may be a worthwhile avenue for further investigation.

Bibliography

[1] Addison, A. W. (1957). A note on the compositeness of numbers. *Proc. Amer. Math. Soc.*, 8:151–154.

[2] Afshar, A. and Porritt, S. (2019). The function field Sathe-Selberg formula in arithmetic progressions and 'short intervals'. *Acta Arith.*, 187(2):101–124.

[3] Andrade, J. C., Bary-Soroker, L., and Rudnick, Z. (2015). Shifted convolution and the Titchmarsh divisor problem over Fq[t]. *Philos. Trans. Roy. Soc. A*, 373(2040):20140308, 18.

[4] Baker, R. C. and Harman, G. (1991). Exponential sums formed with the Möbius function. *J. London Math. Soc. (2)*, 43(2):193–198.

[5] Bienvenu, P.-Y. and Lê, T. H. (2019). Linear and quadratic uniformity of the Möbius function over $\mathbb{F}_q[t]$. *Mathematika*, 65(3):505–529.

[6] Cha, B. (2008). Chebyshev's bias in function fields. *Compos. Math.*, 144(6):1351–1374.

[7] Coons, M. and Dahmen, S. R. (2011). On the residue class distribution of the number of prime divisors of an integer. *Nagoya Math. J.*, 202:15–22.

[8] Dartyge, C., Mauduit, C., and Sárközy, A. (2015). Polynomial values and generators with missing digits in finite fields. *Funct. Approx. Comment. Math.*, 52(1):65–74.

[9] Davenport, H. (1937). On some infinite series involving arithmetical functions (ii). *The Quarterly Journal of Mathematics*, 8(1):313–320.

[10] Deshouillers, J.-M., Dress, F., and Tenenbaum, G. (1979). Lois de répartition des diviseurs. I. *Acta Arith.*, 34(4):273–285 (loose errata).

[11] Dietmann, R., Elsholtz, C., and Shparlinski, I. E. (2017). Prescribing the binary digits of squarefree numbers and quadratic residues. *Trans. Amer. Math. Soc.*, 369(12):8369–8388.

[12] Flajolet, P. and Sedgewick, R. (2009). *Analytic combinatorics*. Cambridge University Press, Cambridge.

[13] Ford, K. and Sneed, J. (2010). Chebyshev's bias for products of two primes. *Experiment. Math.*, 19(4):385–398.

[14] Granville, A. and Martin, G. (2006). Prime number races. *Amer. Math. Monthly*, 113(1):1–33.

[15] Ha, J. (2016). Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 40:10–25.

[16] Hayes, D. R. (1965). The distribution of irreducibles in GF[q, x]. *Trans. Amer. Math. Soc.*, 117:101–127.

[17] Hayes, D. R. (1966). The expression of a polynomial as a sum of three irreducibles. *Acta Arith.*, 11:461–488.

[18] Keating, J. P. and Rudnick, Z. (2014). The variance of the number of prime polynomials in short intervals and in residue classes. *Int. Math. Res. Not. IMRN*, (1):259–288.

[19] Lê, T. H. (2011). Green-Tao theorem in function fields. *Acta Arith.*, 147(2):129–152.

[20] Mauduit, C. and Rivat, J. (2010). Sur un problème de Gelfond: la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646.

[21] Maynard, J. (2019). Primes with restricted digits. *Invent. Math.*, 217(1):127–218.

[22] Meng, X. (2018). Chebyshev's bias for products of k primes. *Algebra Number Theory*, 12(2):305–341.

[23] Meng, X. and Devin, L. (2018). Chebyshev's bias for products of irreducible polynomials. *https://mysite.science.uottawa.ca/ldevin2/ChebyshevProductPoly.pdf*.

[24] Montgomery, H. L. and Vaughan, R. C. (2007). *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.

[25] Oppenheim, A. and Shusterman, M. (2018). Squarefree polynomials with prescribed coefficients. *J. Number Theory*, 187:189–197.

[26] Panario, D. (2014). Open problems for polynomials over finite fields and applications. In *Open problems in mathematics and computational science*, pages 111–126. Springer, Cham.

[27] Pollack, P. (2013). Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 22:70–78.

[28] Porritt, S. (2018a). A note on exponential-Möbius sums over $\mathbb{F}_q[t]$. *Finite Fields Appl.*, 51:298–305.

[29] Porritt, S. (2018b). Residue races of the number of prime divisors function. *J. Number Theory*, 190:241–253.

[30] Porritt, S. (2019). Irreducible polynomials over a finite field with restricted coefficients. *Canad. Math. Bull.*, 62(2):429–439.

[31] Rhin, G. (1972). Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)*, 95:75.

[32] Robbins, H. (1955). A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29.

[33] Rosen, M. (2002). *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[34] Rubinstein, M. and Sarnak, P. (1994). Chebyshev's bias. *Experiment. Math.*, 3(3):173–197.

[35] Sathe, L. G. (1953). On a problem of Hardy on the distribution of integers having a given number of prime factors. I. *J. Indian Math. Soc. (N.S.)*, 17:63–82.

[36] Selberg, A. (1954). Note on a paper by L. G. Sathe. *J. Indian Math. Soc. (N.S.)*, 18:83–87.

[37] Spiro, C. A. (1985). Extensions of some formulae of A. Selberg. *Internat. J. Math. Math. Sci.*, 8(2):283–302.

[38] Tenenbaum, G. (2015). *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition. Translated from the 2008 French edition by Patrick D. F. Ion.

[39] Tuxanidy, A. and Wang, Q. (2016). *Irreducible polynomials with prescribed sums of coefficients*. arXiv:1605.00351. preprint.