Topics in the arithmetic of polynomials over finite fields

Ardavan Afshar

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Mathematics

August 3, 2020

I, Ardavan Afshar, 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

In this thesis, we investigate various topics regarding the arithmetic of polynomials over finite fields. In particular, we explore the analogy between the integers and this polynomial ring, and exploit the additional structure of the latter in order to derive arithmetic statistics which go beyond what can currently be proved in the integer setting.

First, we adapt the Selberg-Delange method to prove an asymptotic formula for counting polynomials with a given number of prime factors. We then extend this formula to cases in which these polynomials are restricted first to arithmetic progressions, and then to 'short intervals'. In both cases, we obtain better ranges for the associated parameters than in the integer setting, by using Weil's Riemann Hypothesis for curves over finite fields.

Then, we investigate highly composite polynomials and the divisor function for polynomials over a finite field, as inspired by Ramanujan's work on highly composite numbers. We determine a family of highly composite polynomials which is not too sparse, and use it to compute the maximum order of the divisor function up to an error which is much smaller than in the case of integers, even when the Riemann Hypothesis is assumed there.

Afterwards, we take a brief aside to discuss the connection between the Generalised Divisor Problem and the Lindelöf Hypothesis in the integer setting.

Next, we prove that for a certain set of multiplicative functions on the polynomial ring, the bound in Halász's Theorem can be improved. Conversely, we determine a criterion for when the general bound is actually attained, and construct an example which satisfies this criterion.

Finally, in the other direction, we develop a formula for the Möbius function of a number field which is related to Pellet's Formula for the Möbius function of the polynomial ring.

Impact Statement

Many of the important questions in Number Theory are intrinsically related to the statistical properties of the integers. Some of these, such as the Riemann Hypothesis, which is a claim about the distribution of the primes, are long-standing open conjectures whose proof would have far-reaching consequences for our general understanding.

In the setting of polynomials over finite fields, we are able to answer the analogues of some of these questions, and thus gain greater insight into the obstacles which prevent us from doing so in the setting of the integers.

The research presented in this thesis, which is comprised of various problems, follows this programme in two distinct ways. In Chapters 2, 3 and 5, we prove some results about the arithmetic statistics of polynomials over finite fields which go beyond what can be proved in the integer setting; and in Chapter 6, we use a formula to do with polynomials over finite fields to develop a tool which might be used in the integer setting.

Moreover, as an aside, in Chapter 4 we demonstrate a connection between two major open conjectures about the integers, with the hope that progress in one may be converted to progress in the other, and vice-versa.

Acknowledgements

I would like to thank my supervisor, Professor Andrew Granville, for his encouragement, advice and role in the shaping of various projects within this thesis, as well as Professor Yiannis Petridis, whose continued support in matters both mathematical and administrative I strongly appreciate. I am deeply grateful to the analytic number theory group at UCL, which has provided an extremely positive and engaging environment for discussion, collaboration and learning. In particular, I would like to thank Oleksiy Klurman, for always sharing his clarifying intuitions; Sam Porritt, for many stimulating conversations and an extremely enjoyable collaboration; James Cann, for his lucid wisdom and good spirit; and Niki Kalaydzhieva, for introducing me to many fun problems.

I would like to express my long-standing gratitude to my parents and my sister, Roshy, for always supporting my choices and endeavours; to my friends, Cristina, Maela, Tom, Sabrina, Dylan, Savannah, Logan and Hannah, without whom I would have never really understood my quest; and to my former teacher, Dr Julian Havil, whose beautiful approach to exposition inspired me to pursue mathematics all those years ago. I also owe a lot to Richard Hoyle, whose technical support and philosophical insight helped me preserve my sanity and remember my passion. Finally, I am eternally indebted to Dr Assarian and the late Professor Ganjavian for their invaluable guidance.

Contents

List of Tables

Chapter 1

Introduction

1.1 Arithmetic statistics

The study of the *arithmetic statistics* of the integers is a well-established branch of Analytic Number Theory, and it begins with a question about the multiplicative building blocks of the integers, the primes, namely: "how likely is it for a given number to be prime?" This question was answered in 1896 by Hadamard and de la Valée Poussin, following the strategy in Riemann's famous memoir of 1859, and resulting in the *Prime Number Theorem*, which gives an asymptotic main term for the prime counting function

$$\pi(x) := \#\{p \leqslant x : p \text{ is prime }\} \sim \int_2^x \frac{dt}{\log t} \qquad \text{as} \quad x \to \infty. \tag{1.1}$$

In other words, the probability that a positive integer near x is prime is asymptotically $\frac{1}{x}\int_2^x \frac{dt}{\log t}$ (or roughly $\frac{1}{\log x}$). The key ingredient in making Riemann's strategy work is to demonstrate that the analytic continuation of the *Riemann Zeta function*, defined for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ by

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

has no zeros on the line $\mathrm{Re}(s) = 1$. The Prime Number Theorem can also be shown to be equivalent to a statement about the mean value of the *Möbius function*, defined by

$$\mu(n) := \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square-free} \\ 0 & \text{else} \end{cases}$$

where $\omega(n)$ is the number of distinct prime factors of n, namely that

$$\frac{1}{x}\sum_{n\leqslant x}\mu(n)\to 0 \qquad \text{as} \quad x\to\infty$$

or in other words, that the average value of $\mu(n)$ is asymptotically zero. As an aside, we note that since the proof of the Prime Number Theorem, there has been some focus on the implicit error term in the asymptotic expansion in equation (1.1). The current best bound for this error term is $O\left(xe^{-c\frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}}\right)$ due to Vinogradov in [41] and Korobov in [26], and the celebrated Riemann Hypothesis conjectures that the error term should in fact be bounded by $O(\sqrt{x}\log x)$.

Once one has established the density of the primes in the integers, it is natural to begin asking questions about the factorisation properties of a 'typical' integer. An archetypal example, which gave birth to the application of techniques from Probability Theory to Number Theory, is about the number of (distinct) prime factors of a typical positive integer. This question was resolved by Erdős and Kac in [11], who proved that

$$\frac{1}{x}\left|\left\{n\leqslant x:\ \frac{\omega(n)-\log\log x}{\sqrt{\log\log x}}\in(a,b)\right\}\right|\longrightarrow\int_a^b\frac{1}{\sqrt{2\pi}}e^{-x^2/2}dx \qquad \text{as} \quad x\to\infty. \tag{1.2}$$

One method for proving this result is to use the so-called *Method of Moments*, wherein one computes the moments of $\omega(n)$ (for n up to x) and shows that they tend to the moments of a normal distribution with mean and variance $\log\log x$, in analogy with the classical proof of the Central Limit Theorem. The use of the Method of Moments, and other tools from Probability Theory, such as Stein's Method, has since become prevalent within the study of arithmetic statistics in Number Theory (see, for example, [21] and [19] respectively).

1.2 Polynomials over finite fields

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field of order q. The ring of polynomials $\mathbb{F}_q[t]$ has an arithmetic structure which is very similar to that of the integers, and it has long been studied in analogy with $\mathbb{Z}$. In particular, if we restrict to $\mathcal{M}$, the set of monic polynomials in $\mathbb{F}_q[t]$, we have that any element in $\mathcal{M}$ factorises uniquely into a product of primes (irreducibles) in $\mathcal{M}$. $\mathcal{M}$ is the analogue of the natural numbers, and we can ask questions about the arithmetic statistics of $\mathcal{M}$, just as we did for the natural numbers. Similarly to before, the prototypical question is: "how many primes are there of degree n?". This question is much easier to answer than in the case of the integers, and in fact one can show using a short elementary argument that for $\mathcal{M}_n = \{f \in \mathcal{M} : \deg f = n\}$

$$\pi(n) := \#\{p \in \mathcal{M}_n : p \text{ is prime}\} = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}.$$

This *Prime Polynomial Theorem* is originally due to Gauss, and gives a full asymptotic expansion for $\pi(n)$. We see that the main term is of size $\frac{q^n}{n}$, and since there are exactly q^n elements in $\mathcal{M}_n$, this is directly analogous to our result in the integers, whose main term is roughly $\frac{x}{\log x}$. Moreover, the secondary term is at most of size $\frac{q^{n/2}}{n}$, which means that $\mathcal{M}$ provably satisfies the analogue of the Riemann Hypothesis. These facts make $\mathcal{M}$ a useful toy model for the natural numbers, because not only are its statistics similar, but we are able to prove stronger results about it, which can give us an insight as to what might be going on in the integer setting which we cannot yet prove.

Just as in the integer setting, we can reformulate questions about arithmetic statistics in $\mathbb{F}_q[t]$, like counting primes, in the language of zeta functions. The analogue of the Riemann Zeta function for $\mathcal{M}$ is the function

$$Z(s) = \sum_{f \in \mathcal{M}} \frac{1}{|f|^s}$$

where $|f| = q^{\deg f}$. After the change of variable $T = q^{-s}$ we observe that

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

Now, the Riemann Hypothesis for the integers is equivalent to the claim that $\zeta(s)$ has no (non-trivial) zeros off the line $\mathrm{Re}(s) = 1/2$, and similarly the so-called Riemann Hypothesis for $\mathbb{F}_q[t]$ is equivalent to the fact that $Z(T)$ has no zeros off the circle $|T| = \frac{1}{\sqrt{q}}$. The latter is, of course, vacuously true since $Z(T)$ has no zeros at all, which explains why we easily obtain such an explicit formula for $\pi(n)$ in the case of $\mathcal{M}$.

Finally, we note that in the setting of $\mathbb{F}_q[t]$ there are two possible limits to consider. When we compute the statistics of $\mathcal{M}_n$, we can either keep q fixed and let n tend to infinity, or we can keep n fixed and allow q to tend to infinity. In the following work, we largely investigate the former, as for us it serves as a more direct analogue of what is happening in the setting of the integers. However, we do briefly discuss the regime where q tends to infinity at the end of Chapter 2, and indeed there is a significant amount of contemporary literature dedicated to analysing this regime (see, for example, [34] for a survey).

1.3 Outline of Thesis

So far, we have outlined the general notion of arithmetic statistics for the integers and for polynomial rings over finite fields, and we have noted the additional tools available in the study of the latter. The majority of the subsequent content of this thesis is dedicated to the study of certain arithmetic questions about $\mathbb{F}_q[t]$, where we use the extra structure of this ring to go beyond what it is possible to prove in the setting of the integers. In order to present each chapter in a self-contained fashion, each contains its own introduction, which recalls its context and adds further technical details and background information.

1.3.1 The Selberg Delange Method

An analytic approach to questions about arithmetic statistics is through the use of the Selberg-Delange Method, which was first used by Selberg in [37] to estimate the asymptotic order of $\pi_k(x) := \#\{n \leqslant x : n = p_1 \ldots p_k$ for some $p_1, \ldots, p_k$ distinct primes$\}$, where the parameter k is allowed to vary with x up to some height. This result not only generalises the Prime Number Theorem in equation (1.1), but can also be used to derive the Erdős-Kac Theorem in equation (1.2) (as demonstrated, for example, in Chapter 7 of [30]). So, we see that the Selberg-Delange Method is both very powerful and very general: in fact, it can be used to understand functions of the form

$$F(s,z) = G(s,z)\zeta(s)^z$$

where $s, z \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and $F(s,z) = \sum_{n \geqslant 1} \frac{a_n(z)}{n^s}$ is a Dirichlet series such that $G(s,z)$ is an entire function in s satisfying certain bounds. If $G(s,z)$ satisfies these conditions, then $F(s,z)$ and $\zeta(s)^z$ are in some sense 'close', and understanding the singularity of $F(s,z)$ at $s = 1$, from which we can derive arithmetic information, essentially reduces to computing the singularity of $\zeta(s)^z$ at $s = 1$. For a full account, see Part II, Chapter 5 of [39], whose notation we have borrowed. In the particular case of $\pi_k(x)$, Selberg takes

$$F(s,z) = \sum_{n \geqslant 1} \frac{\mu^2(n) z^{\omega(n)}}{n^s}$$

and having understood the pole of $F(s,z)$ at $s=1$, as described above, he uses Perron's Formula to extract the partial sum

$$A_z(x) := \sum_{n \leqslant x} \mu^2(n) z^{\omega(n)} = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} F(s,z) x^s \frac{ds}{s}.$$

Finally, since $\pi_k(x) = \#\{n \leqslant x : \mu^2(n) = 1 \text{ and } \omega(n) = k\}$, he notes that $A_z(x)$ can be re-written as

$$A_z(x) = \sum_{k \geqslant 1} \pi_k(x) z^k$$

and so he can compute $\pi_k(x)$ using Cauchy's formula

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

In doing so, he is able to get an asymptotic main term for $\pi_k(x)$ for k up to any constant multiple of $\log\log x$, namely that

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

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

In Chapter 2, we modify the Selberg-Delange method to the setting of $\mathbb{F}_q[t]$, and use it to derive a Sathé-Selberg formula for this setting.

Theorem 1. *Let $A > 1$. Then uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$*

$$\begin{aligned} \pi_k(n) &:= \#\{f \in \mathcal{M}_n : f = p_1 \dots p_k \textit{ for some } p_1, \dots, p_k \in \mathcal{I} \textit{ distinct}\} \\ &= \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right) \right) \end{aligned}$$

where $G(z) = \frac{F(1/q,z)}{\Gamma(1+z)}$ and $F(1/q,z) = \prod_{p \in \mathcal{I}} \left(1 + \frac{z}{q^{\deg p}}\right) \left(1 - \frac{1}{q^{\deg p}}\right)^z$, and the error term is independent of q.

We also demonstrate how to use our Sathé-Selberg formula to prove the analogue of the

Erdős-Kac formula in this setting.

In addition, we adapt this technique to Dirichlet L-functions in this setting in order to obtain a Sathé-Selberg formula in the case when our polynomials are restricted to an arithmetic progression.

Theorem 2. *Let $g, d \in \mathbb{F}_q[t]$ be coprime and $m = \deg d$. Let $A > 1$, $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$. Then for $m \leqslant \left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n$ we have*

$$\begin{aligned}\pi_k(n; g, d) &:= \#\{f \in \mathcal{M}_n \; f \equiv g \mod d : f = p_1 \dots p_k \textit{ for some } p_1, \dots, p_k \in \mathcal{I} \textit{ distinct}\} \\ &= \frac{1}{\Phi(d)} \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G_d\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)\end{aligned}$$

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 the Theorem 1.

In this setting, we define a *Dirichlet L-function* to be

$$L(T, \chi) := \sum_{f \in \mathcal{M}} \chi(f) T^{\deg f}$$

where we call the group homomorphism $\chi : (\mathbb{F}_q[t]/(d(t)))^\times \longrightarrow \mathbb{C}^\times$ a *Dirichlet character* modulo d for some $d \in \mathcal{M}$ (which we call its *conductor*). These functions, just like their integer setting counterparts, are used to understand statistics where we restrict to a particular arithmetic progression, since by the orthogonality of characters we have that

$$\sum_{\substack{f \in \mathcal{M}_n \\ f \equiv g \mod d}} 1 = \frac{1}{\Phi(d)} \sum_{\chi \mod d} \overline{\chi(g)} \sum_{f \in \mathcal{M}_n} \chi(f)$$

is the coefficient of T^n in

$$\frac{1}{\Phi(d)} \sum_{\chi \mod d} \overline{\chi(g)} L(T, \chi).$$

Moreover, the Riemann Hypothesis for these functions is also true - that is, they have no zeros off the circle $|T| = \frac{1}{\sqrt{q}}$ - but in this case the result is not elementary. Rather, it is a consequence of deep result from Algebraic Geometry, namely Weil's Riemann Hypothesis for curves over finite fields (Weil's original proof can be found in [42]).

Finally, we use an 'involution trick' (detailed in Section 2.4.1) to restrict instead to polynomials in a 'short interval'. In this setting, we define a *short interval* of length $h < n$ around a polynomial $g \in \mathcal{M}_n$ to be the set

$$\{f \in \mathcal{M}_n : \deg(f-g) \leqslant h\}.$$

Theorem 3. *Let $g \in \mathbb{F}_q[t]$. Let $A > 1$, $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$. Then for h satisfying $n-1 \geqslant h \geqslant \left(\frac{1}{2} + \frac{1+\log(1+\frac{A}{2})}{\log q}\right)(n+1)$, we have*

$$\begin{aligned}\pi_k(n;g;h) &:= \#\{f \in \mathcal{M}_n \quad \deg(f-g) \leqslant h : f = p_1 \dots p_k \textit{ for some } p_1, \dots, p_k \in \mathcal{I} \textit{ distinct}\} \\ &= \frac{q^{h+1}}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(H\left(\frac{k-1}{\log n}\right) + \frac{k-1}{q \log n} H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)\end{aligned}$$

where $H(z) = \frac{q}{q+z} G(z)$ and $G(z)$ is defined as as in Theorem 1.

On account of the Riemann Hypothesis for these Dirichlet L-functions, we are able to get a better range for the conductor of the arithmetic progression and the length of the short interval respectively in these variations of the problem. These ranges are analogous to what one would obtain in the integer setting when one assumes the Generalised Riemann Hypothesis there.

1.3.2 Divisor Functions

1.3.2.1 Average Estimates

As mentioned, a key ingredient of the Selberg-Delange method is to computing the singularity of $\zeta(s)^z$ at $s = 1$, which is related to another arithmetic statistic of the integers: the (generalised) divisor function. For $z \in C$, we define the *generalised divisor function* $d_z : \mathbb{N} \to \mathbb{C}$ by

$$\zeta(s)^z =: \sum_{n \geqslant 1} \frac{d_z(n)}{n^s}$$

where $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1$. When $z = k$ is a positive integer, $d_z(n) = d_k(n)$ is the number of ways of writing n as a product of exactly k factors, and we can relate its mean value to $\zeta(s)^k$ using Perron's formula

$$\sum_{n \leqslant x} d_k(n) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \zeta(s)^k x^s \frac{ds}{s}.$$

It can be shown, following Dirichlet and his Hyperbola Method in the case of $k = 2$, that

$$\sum_{n \leqslant x} d_k(n) = xP_{k-1}(\log x) + O_\epsilon(x^{1-1/k+\epsilon}) \tag{1.3}$$

where P_{k-1} is a monic polynomial of degree $k-1$. In other words, the average value of $d_k(n)$ for $n \leqslant x$ is asymptotically $\log^{k-1} x$. In the special case when $k = 2$, we call $d(n) := d_2(n)$ the *divisor function*, because it counts the number of divisors of n, and the result in equation (1.3) says that the average number of divisors of a positive integer $n \leqslant x$ is asymptotically $\log x$.

The problem of determining the order of the error term $O_\epsilon(x^{\alpha_k+\epsilon})$ in equation (1.3), which is conjectured to be $O_\epsilon(x^{1/2-1/2k+\epsilon})$, is known as the *Generalised Divisor Problem.* In Chapter 4, we take a brief aside to discuss the connection between the Generalised Divisor Problem and the Lindelöf Hypothesis in the integer setting. The *Lindelöf Hypothesis* is the conjecture that

$$\mu(1/2) := \min\{\mu \mid \forall \epsilon > 0 \ |\zeta(1/2 + it)| = O_\epsilon(t^{\mu+\epsilon})\} = 0$$

and it is equivalent to a weak form of the Riemann Hypothesis, namely that almost all zeros of $\zeta(s)$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$ (see Theorem 13.5 of [40]). We use Perron's formula, summation by parts and a tensor-power trick to show how to quantitatively convert upper bounds from one problem to upper bounds for the other.

Theorem 4. *For $k \geqslant 2$, we have that*

$$\mu(1/2) \leqslant \begin{cases} \frac{1}{2k}\frac{1}{1-\alpha_k} & \text{if } \alpha_k \leqslant \frac{1}{2} \\ \frac{1}{2\alpha_k}\left(\alpha_k - \frac{1}{2} + \frac{1}{k}\right) & \text{if } \alpha_k \geqslant \frac{1}{2} \end{cases}.$$

and

$$\alpha_k \leqslant \frac{1}{2} + \frac{(k-2)\mu(\frac{1}{2})}{2(1 + (k-2)\mu(\frac{1}{2}))}.$$

A well-known corollary of Theorem 4 is that $\mu(1/2) = 0$ if, and only if, $\alpha_k \leqslant \frac{1}{2}$ for all $k \geqslant 2$ (see, for example, Theorem 13.4 of [40]).

1.3.2.2 Pointwise bounds

The divisor function itself fluctuates rather wildly: the estimate for its mean value gives little information about its extreme values. On the one hand, we know that for any prime p, no matter how large, $d(p) = 2$; and on the other hand it was first shown by Wigert that there is an infinite sequence of positive integers n such that

$$d(n) \gg_\epsilon 2^{\frac{(1-\epsilon)\log n}{\log\log n}}.$$

This led to the study of the maximum order of the divisor function, which is intimately related to the notion of *highly composite numbers*: positive integers n such $d(n) > d(n')$ for all $n > n'$. Ramanujan investigated the latter in detail, and used them in [32] to show that

$$\log_2 d(n) \leqslant \int_2^{\log n} \frac{dt}{\log t} + O(e^{-c\sqrt{\log\log n}} \log n)$$

where the upper bound is sharp up to the error term. Moreover, assuming the Riemann Hypothesis, he was able to compute more terms in this asymptotic expansion and reduce the error term to $O\left(\frac{\sqrt{\log n}}{(\log\log n)^3}\right)$.

In Chapter 3, we investigate highly composite polynomials, in analogy to Ramanujan's highly composite numbers, and use them to compute the maximum order of the divisor function for $\mathcal{M}$, which counts the number of divisors of a polynomial $f \in \mathcal{M}$. In particular, we are able to use the discrete nature of the degree sequence of highly composite polynomials to construct a relatively dense set of such polynomials, which allows us to compute the maximum order of the divisor function in this setting to an accuracy significantly beyond what is possible in the integer setting, even when the Riemann Hypothesis is assumed in the latter.

Theorem 5. *Let $x = \frac{s\log q}{\log(1+1/r)}$ for positive integers r and s, and let*

$$\hat{h} = \hat{h}(x) = \prod_{k\geqslant 1}\prod_{p\in\mathcal{I}_k} p^{a_k} \quad \textit{where} \quad a_k = a_k(x) = \left\lfloor \frac{1}{q^{k/x}-1} \right\rfloor.$$

and

$$h(x) = \frac{\hat{h}(x)}{P_{i_1}\cdots P_{i_v}}$$

where $0 \leqslant v < \pi(s)$, $P_{i_1}, \cdots, P_{i_v} \in \mathcal{I}_s$ distinct, and $\deg h(x) = \deg \hat{h}(x) - vs$. Let $\tau(f)$ be *the number of monic divisors of* $f \in \mathcal{M}$ *and let* $T(N) := \max\{\tau(f) \mid f \in \mathcal{M}_N\}$. *Then, if* $N = \deg h - u$ *with* $0 \leqslant u \leqslant s-1$, *we have*

$$\log T(N) = \begin{cases} \log \tau(h) & \textit{if } u = 0 \\ \log \tau(h) - \epsilon(N) & \textit{otherwise} \end{cases}$$

where

$$\frac{u}{s} \log\left(1 + \frac{1}{r}\right) \leqslant \epsilon(N) \leqslant \log\left(1 + \frac{1}{a_u}\right)$$

Moreover, the size of this range for $\epsilon(N)$ *is at most* $\log\left(1 + \frac{1}{a_u(a_u+2)}\right) \leqslant \log \frac{4}{3}$.

Theorem 5 uses our classification of the highly composite polynomials h to determine the value of the divisor function, up to a bounded factor of $\frac{4}{3}$, on highly composite polynomials at every degree.

1.3.3 Halász's Theorem

In the examples of arithmetic statistics which we have surveyed so far, a recurring theme has been of mean values of certain arithmetic functions. In particular, we mentioned the mean values of $\mu(n)$ and of $d(n)$, both of which share the property that they are multiplicative. We say that an arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is *multiplicative* if $f(ab) = f(a)f(b)$ for all a and b which are coprime, and we study this set of functions in order to determine what we can deduce from this property alone. For in computing the mean values of $\mu(n)$ and $d(n)$ directly, we make use of the fact that they are connected to the definition of the Riemann Zeta function $\zeta(s)$, and it would be interesting to see how much we can ascertain just by the fact that they are multiplicative. In light of this, we come to an important theorem of Halász, originally from [17] and [18]. A modern formulation of this theorem is that, for a multiplicative function f such that $|f(n)| \leqslant 1$ for all n, we have

$$\frac{1}{x} \sum_{n \leqslant x} f(n) \ll (1 + M_f)e^{-M_f} + \frac{\log \log x}{\log x}$$

where $M_f = M_f(x)$ is defined by

$$e^{-M_f} \log x := \max_{|t| \leqslant (\log x)} \left| \frac{F(1 + 1/\log x + it)}{1 + 1/\log x + it} \right|.$$

and $F(s) = \sum_{n \geqslant 1} \frac{f(n)}{n^s}$ is the Dirichlet series associated to f. Halász Theorem gives us a very general tool for understanding multiplicative functions, and provides another way to recover results associated to particular cases. Note, for example, that the non-vanishing of $\zeta(s)$ on $\mathrm{Re}(s) = 1$ implies that $e^{-M_\mu} \asymp \frac{1}{\log x}$ and so by Halász Theorem we have

$$\frac{1}{x} \sum_{n \leqslant x} \mu(n) \ll \frac{\log \log x}{\log x}$$

which is equivalent to the Prime Number Theorem (albeit with a weak error term).

We can investigate the analogous phenomenon in $\mathbb{F}_q[t]$ by considering multiplicative functions $f : \mathcal{M} \to \mathbb{C}$. For such functions, we define $\Lambda_f(F)$ (the *von Mangoldt* function associated to f) by

$$\frac{z\mathcal{F}'}{\mathcal{F}}(z) =: \sum_{F \in \mathcal{M}} \Lambda_f(F) z^{\deg F}$$

where $\mathcal{F}(z) = \sum_{F \in \mathcal{M}} f(F) z^{\deg F}$, and then consider the set $\tilde{\mathcal{C}}(\kappa)$ of multiplicative functions f such that $f(1) = 1$ and $\left| \frac{1}{q^n} \sum_{F \in \mathcal{M}_n} \Lambda_f(F) \right| \leqslant \kappa$ for all $n \geqslant 1$.

In [14], Granville, Harper and Soundararajan improved the upper bound in Halász's Theorem for functions which are supported only on numbers which are $x^{1-\epsilon}$-smooth. In Chapter 5, we make the analogous improvement for Halász's Theorem in $\mathbb{F}_q[t]$.

Theorem 6. *Let $\kappa > 0$ and $f \in \tilde{\mathcal{C}}(\kappa)$, and for $n \geqslant 1$ define $M = M(n)$ by*

$$e^{-M}(2n)^\kappa := \max_{|z|=1} \left(\exp \left(\mathrm{Re} \left(\sum_{j=1}^{n-1} \frac{1}{q^j} \sum_{F \in \mathcal{M}_j} \Lambda_f(F) \frac{z^j}{j} \right) \right) \right).$$

Suppose that, for some $\delta > 0$, we have that $\sum_{F \in \mathcal{M}_j} \Lambda_f(F) = 0$ for all $j > (1-\delta)(n-1)$. Then we get that

$$\left| \frac{1}{q^n} \sum_{F \in \mathcal{M}_n} f(F) \right| \ll_\delta \kappa^2 e^{-M} (2n)^{\kappa - 1}.$$

The upper bound in Halász's Theorem in $\mathbb{F}_q[t]$ is $O(\kappa(\kappa + M)e^{-M}(2n)^{\kappa-1})$, which is improved for the functions in Theorem 6. However, the former is sometimes actually attained, and we derive a criterion for when this happens, and construct an example which satisfies this criterion. In doing so, we exploit the fact that the arithmetic generating functions in

$\mathbb{F}_q[t]$ are power series, rather than Dirichlet series, which leads to some simplifications.

Theorem 7. *Let $\kappa > 0$, $n \geqslant 1$ and $\frac{1}{2} - \frac{1}{2n} > \delta > 0$. Let $f \in \tilde{\mathcal{C}}(\kappa)$, and define $M = M(n)$ as in the Theorem 6. Then given the values of $f(P^k)$ for all prime powers P^k with $\deg P^k \leqslant (1-\delta)(n-1)$, there exists a choice of values of $f(P^k)$ for all prime powers P^k with $\deg P^k > (1-\delta)(n-1)$ such that*

$$\left| \frac{1}{q^n} \sum_{F \in \mathcal{M}_n} f(F) \right| \gg (1+M)e^{-M}(2n)^{\kappa-1}$$

if, and only if, for all $\delta \gg 1$ we have

$$\sum_{1 \leqslant j \leqslant 1+\delta(n-1)} \left| \frac{1}{q^j} \sum_{F \in \mathcal{M}_j} f(F) \right| \gg (1+M)e^{-M}(2n)^{\kappa}.$$

Theorem 7 follows from Theorem 5.4 and Remark 5.4.

1.3.4 Pellet's formula

Another perspective on why things are more straightforward in the setting of $\mathbb{F}_q[t]$ comes from Galois Theory. In particular, we note that for any irreducible $f \in \mathcal{M}_n$ we have that the Galois group of f is

$$\mathrm{Gal}(f) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

which is cyclic and generated by the Frobenius automorphism Frob_q which sends α to α^q. The simplicity of the Galois Theory of the base field leads, amongst other things, to a remarkable formula for the analogue of the Möbius function in this setting, which we define by

$$\mu(f) := \begin{cases} (-1)^k & \text{if } f = p_1 \cdots p_k \text{ distinct primes} \\ 0 & \text{else} \end{cases}.$$

This formula, which is known as *Pellet's formula*, states that

$$\mu(f) = (-1)^{\deg f} \chi(\mathrm{disc} f)$$

where χ is the quadratic character on $\mathbb{F}_q$, and can be used to prove results about the statistics of $\mathcal{M}$ which are significantly beyond what is possible for the natural numbers.

For example, Sawin and Shusterman use Pellet's formula in [36] to prove the analogue of the Twin Primes Conjecture in this setting, following work of Bary-Soroker in [5] and Pollack in [31].

We conclude, in Chapter 6, by doing something a little different. We go through a proof of Pellet's Formula in which we derive an intermediate formula, which we call *Proto-Pellet's Formula*, and use it as inspiration to construct an analogous formula for the Möbius function in the setting of number fields (including the usual integer setting).

Theorem 8 ("Proto-Pellet's Formula" for number fields)**.** *Let $A/\mathbb{Q}$ be a number field, let $\mathcal{O}_A$ be the ring of integers in A and let $\mathcal{I}_A$ be the set of non-zero ideals in $\mathcal{O}_A$. Let $\mu : \mathcal{I}_A \to \{-1, 0, 1\}$ be the Möbius Function for $A/\mathbb{Q}$ and let $\nu : \mathcal{I}_A \to \mathbb{N}$ be an additive function. Then there exists a Galois homomorphism $\sigma_\nu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and a family of polynomials $(f_{I,\nu})_{I\in\mathcal{I}_A}$ such that, for all $I \in \mathcal{I}_A$ square-free*

$$\mu_A(I) = (-1)^{\nu(I)}\mathrm{sign}(\sigma_\nu|f_{I,\nu})$$

where $\sigma_\nu|f$ denotes the action of σ_ν on the roots of f.

Chapter 2

The function field Sathé-Selberg formula

This chapter is based primarily on joint work with Sam Porritt and largely appears, with the exception of the addition of Section 2.6, in [3].

We use a function field analogue of a method of Selberg to derive an asymptotic formula for the number of (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 this 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. Finally, we briefly discuss the regime in which q tends to infinity.

2.1 Introduction

One natural generalisation of the problem of counting primes up to x is to count numbers up to x with exactly k distinct prime divisors. In [35], Sathé proved that for $A > 0$ an arbitrary constant we have

$$\begin{aligned}\pi_k(x) &:= \#\{n \leqslant x : n = p_1 \dots p_k \text{ for some } p_1, \dots, p_k \text{ distinct primes}\}\\ &\sim G\left(\frac{k-1}{\log\log x}\right)\frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\end{aligned}$$

uniformly for $x \geqslant 3$ and $1 \leqslant k \leqslant A\log\log x$, where $G(z) = \frac{1}{\Gamma(1+z)}\prod_{p \text{ prime}}(1+\frac{z}{p})(1-\frac{1}{p})^z$. In [37], 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 [38], Spiro showed that such a formula holds for $n \leqslant x$ restricted to $n \equiv a \mod q$, provided q does not exceed some fixed power of $\log x$.

We begin by proving an asymptotic formula for the number of monic polynomials in $\mathbb{F}_q[t]$ of degree n with exactly k distinct irreducible divisors, using an adaptation of Selberg's technique. If we let $\mathcal{M} = \{f \in \mathbb{F}_q[t] : f \text{ monic}\}$, $\mathcal{M}_n = \{f \in \mathcal{M} : \deg f = n\}$ and $\mathcal{I} = \{p \in \mathcal{M} : p \text{ irreducible}\}$, then we get

Theorem 2.1. *Let $A > 1$. Then uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$*

$$\begin{aligned}\pi_k(n) &:= \#\{f \in \mathcal{M}_n : f = p_1 \dots p_k \textit{ for some } p_1, \dots, p_k \in \mathcal{I} \textit{ distinct}\} \\ &= \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)\end{aligned}$$

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

Theorem 2.1 says that the asymptotic density of square-free polynomials in $\mathcal{M}_n$ with k distinct prime divisors is $\frac{1}{n}\frac{(\log n)^{k-1}}{(k-1)!} G\left(\frac{k-1}{\log n}\right)$. An asymptotic formula of this form was first derived by Car in [7], but with an error term which inexplicitly depends on k and q. Note that, when k is close to its mean $\log n$ (see Section 2.6) then $G\left(\frac{k-1}{\log n}\right)$ is close to $G(1) = 1 - \frac{1}{q}$, which is the density of square-free polynomials in $\mathcal{M}$.

With some additional technical work following Chapters II.5 and II.6 of [39], one could strengthen Theorem 2.1 to be of an analogous form to Chapter II.6 Theorem 4 of [39], namely that for any $J \geqslant 1$

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

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 2.2 and 2.3 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 difference of degree no bigger than roughly $n/2$.

Theorem 2.2. *Let $g, d \in \mathbb{F}_q[t]$ be coprime and $m = \deg d$. Let $A > 1$, $n \geqslant 2$ and*

$1 \leqslant k \leqslant A \log n$. Then for $m \leqslant \left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n$ we have

$$\begin{aligned}\pi_k(n;g,d) &:= \#\{f \in \mathcal{M}_n \ f \equiv g \mod d : f = p_1 \dots p_k \text{ for some } p_1, \dots, p_k \in \mathcal{I} \text{ distinct}\} \\ &= \frac{1}{\Phi(d)} \frac{q^n}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(G_d\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)\end{aligned}$$

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 2.1.

The range on the degree of the difference m in Theorem 2.2 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. A better range would require additional cancellation amongst these characters. This range corresponds to taking the difference up to roughly $\sqrt{x}$ in the number field setting, compared to any fixed power of $\log x$ as in Theorem 1 of [38].

Finally, by using an 'involution-trick', we apply Theorem 2.2 to derive an asymptotic formula for the number of such polynomials in a given 'short interval' of length no shorter than roughly $n/2$ (which again corresponds to roughly $\sqrt{x}$ in the number field setting).

Theorem 2.3. *Let $g \in \mathbb{F}_q[t]$. Let $A > 1$, $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$. Then for h satisfying $n - 1 \geqslant h \geqslant \left(\frac{1}{2} + \frac{1+\log(1+\frac{A}{2})}{\log q}\right)(n+1)$, we have*

$$\begin{aligned}\pi_k(n;g;h) &:= \#\{f \in \mathcal{M}_n \ \deg(f-g) \leqslant h : f = p_1 \dots p_k \text{ for some } p_1, \dots, p_k \in \mathcal{I} \text{ distinct}\} \\ &= \frac{q^{h+1}}{n} \frac{(\log n)^{k-1}}{(k-1)!} \left(H\left(\frac{k-1}{\log n}\right) + \frac{k-1}{q \log n} H\left(\frac{k-2}{\log(n-1)}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)\end{aligned}$$

where $H(z) = \frac{q}{q+z} G(z)$ and $G(z)$ is defined as in Theorem 2.1.

The two main terms in Theorem 2.3 come from counting polynomials with non-zero constant term and polynomials with zero constant term separately. 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.

Note that, since $G(z), G_d(z)$ and $H(z)$ are all $\gg_A 1$ for $0 \leqslant z \leqslant A$, the main terms in Theorems 2.1, 2.2 and 2.3 are larger than their respective error terms, which additionally do not depend on q. We briefly discuss the regime in which $q \to \infty$ in Section 2.5.

2.2 The function field Sathé-Selberg formula

2.2.1 Outline

Let $\omega(f) = \#\{p \in \mathcal{I} : p|f\}$ and define the Möbius function on $\mathcal{M}$ by

$$\mu(f) = \begin{cases} (-1)^{\omega(f)} & \text{if } f \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$$

so that μ^2 is the indicator function for the square-free polynomials in $\mathcal{M}$ and

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

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

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

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 $\pi_k(n)$ from the identity

$$\sum_{k \geqslant 0} \pi_k(n) z^k = A_z(n)$$

using Cauchy's formula

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

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

2.2.2 Proof of Theorem 1

First note that there are q^n polynomials in $\mathcal{M}_n$ and that therefore, for $|T| < 1/q$,

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

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

Lemma 2.1. *If we define $D_z(n)$ for $n \geqslant 0$ via the identity $Z(T)^z = \sum_{n\geqslant 0} D_z(n)T^n$, 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. The binomial theorem gives us

$$Z(T)^z = (1-qT)^{-z} = \sum_{n\geqslant 0}\binom{n+z-1}{n}q^nT^n.$$

□

Corollary 2.1. *For all $n \geqslant 1$ and $|z| \leqslant A$,*

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

Proof. By choosing the implied constant large enough, it is sufficient to prove this for $n \geqslant 2A$. 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 2.1 we can conclude that

$$\begin{aligned} D_z(n) &= q^n \binom{n+z-1}{n} \\ &= q^n \frac{\Gamma(n+z)}{\Gamma(n+1)\Gamma(z)} \\ &= q^n \frac{n^{z-1}}{\Gamma(z)} \left(1 + O_A\left(\frac{1}{n}\right)\right). \end{aligned}$$

□

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 $Z(T)^z$ at $T = 1/q$.

Proposition 2.1. *Let $C(T,z) = \sum_{n\geqslant 0} C_z(n)T^n$ and $M(T,z) = \sum_{n\geqslant 0} M_z(n)T^n$ be power series with coefficients depending on z satisfying $C(T,z) = M(T,z)Z(T)^z$. Suppose also that, uniformly for $|z| \leqslant A$,*

$$\sum_{a\geqslant 0} \frac{|M_z(a)|}{q^a} a^{2A+2} \ll_A 1. \qquad (\star)$$

Then, uniformly for $|z| \leqslant A$ and $n \geqslant 1$, we have

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

Proof. Using our expression for $D_z(n)$ from Corollary 2.1 and that $D_z(0) = 1$, we get

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

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

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

Combining this with ($\star$) we get

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

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

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

Finally, by ($\star$) we have that the last term is

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

Putting everything together proves the proposition. □

Remark 2.1. *This follows the same ideas as Theorem 7.18 of [30].*

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

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

First we check that the conditions of Proposition 2.1 are satisfied.

Proposition 2.2. *For $|z| \leqslant A$, $n \geqslant 2$ and $\sigma \geqslant \frac{1}{2}$*

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

where $c_{A,\sigma}$ is a constant depending on A and σ, and c_A is a constant depending on A.

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

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

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

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

then $F(T,z) = \sum_{f\in\mathcal{M}} b_z(f)T^{\deg f}$ and so $B_z(n) = \sum_{f\in M_n} b_z(f)$. 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

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

where $M_A = \sup_{|z|\leqslant A, |S|\leqslant \frac{1}{\sqrt{3/2}}} |(1+zS)(1-S)^z|$ is some constant depending on A.

Therefore, letting $\mathcal{M}_{\leqslant n} = \{f \in \mathcal{M} : \deg f \leqslant n\}$ and $\mathcal{I}_{\leqslant n} = \{p \in \mathcal{I} : \deg p \leqslant n\}$, we have

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

Taking the logarithm and using the prime polynomial theorem we get

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

Exponentiating then gives the stated result. □

Remark 2.2. *Proposition 2.2 also proves that $F(1/q, z)$ is absolutely uniformly convergent for $|z| \leqslant A$ and so holomorphic in z for $|z| \leqslant A$.*

Remark 2.3. *This follows the same ideas as the beginning of Chapter II.6 of [39].*

Corollary 2.2. *Uniformly for $|z| \leqslant A$ and $n \geqslant 1$, we have*

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

Proof. By Proposition 2.2, this follows from Proposition 2.1 with $C(T, z) = A(T, z)$ and $M(T, z) = F(T, z)$. □

We now turn to the proof of a generalisation of the main result in this section.

Proposition 2.3. *Let $A > 1$, $M(z)$ be a holomorphic function for $|z| \leqslant A$, and $C_z(n)$ be an arithmetic function such that uniformly for $|z| \leqslant A$ and $n \geqslant 1$*

$$C_z(n) = q^n \frac{n^{z-1}}{\Gamma(z)} M(z) + O_A(q^n n^{\mathrm{Re}(z)-3/2}).$$

Moreover, for $k \geqslant 1$ an integer, let $\alpha_k(n)$ be the arithmetic function defined by

$$\alpha_k(n) = \frac{1}{2\pi i} \oint \frac{C_z(n)}{z^{k+1}} dz.$$

Then for $N(z) = \frac{M(z)}{\Gamma(1+z)}$, we have that uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$

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

Proof. When $k = 1$ we integrate around the circle $|z| = 1/4$ to get

$$\begin{aligned}\alpha_1(n) = \frac{1}{2\pi i} \oint \frac{C_z(n)}{z^2} dz &= \frac{q^n}{n} \left(\frac{1}{2\pi i} \oint \frac{N(z) n^z}{z} dz + O_A(n^{-1/4})\right) \\ &= \frac{q^n}{n}\left(N(0) + O_A(n^{-1/4})\right)\end{aligned}$$

Now assume $k > 1$. We integrate the around the circle $|z| = r = \frac{k-1}{\log n} < A$ so that the contribution from the error term in $C_z(n)$ is

$$O_A\left(q^n \int_{|z|=r} \left| \frac{n^{\mathrm{Re}(z)-3/2} dz}{z^{k+1}} \right| \right) \ll_A q^n n^{r-3/2} r^{-k} = \frac{q^n}{n^{3/2}} e^{k-1} \frac{(\log n)^k}{(k-1)^k} \ll_A \frac{q^n}{n^{3/2}} \frac{(\log n)^k}{(k-1)!}$$

which is smaller than the error which we are aiming for in the theorem.

The contribution from the main term in $C_z(n)$ is

$$\frac{q^n}{n} \int_{|z|=r} \frac{N(z) n^z}{z^k} dz.$$

Integration by parts gives

$$\int_{|z|=r} \frac{n^z}{z^{k-1}} dz = \frac{k-1}{\log n} \int_{|z|=r} \frac{n^z}{z^k} dz = r \int_{|z|=r} \frac{n^z}{z^k} dz \implies \frac{1}{2\pi i} \int_{|z|=r} (z-r) \frac{n^z}{z^k} dz = 0.$$

Using this fact to determine that the last term in the following line vanishes, we have

$$\begin{aligned}\frac{1}{2\pi i} \int_{|z|=r} N(z) \frac{n^z}{z^k} dz &= \frac{N(r)}{2\pi i} \int_{|z|=r} \frac{n^z}{z^k} dz + \frac{1}{2\pi i} \int_{|z|=r} \left(N(z) - N(r) - N'(r)(z-r)\right) \frac{n^z}{z^k} dz \\ &= \frac{N(r)}{2\pi i} \int_{|z|=r} \frac{n^z}{z^k} dz + O\left(\left| \int_{|z|=r} N''(r)(z-r)^2 \, \frac{n^z}{z^k} dz \right| \right) \\ &= N(r) \frac{(\log n)^{k-1}}{(k-1)!} + O_A\left(\int_{|z|=r} |z-r|^2 \left| \frac{n^z}{z^k} \right| |dz| \right)\end{aligned}$$

where $N(z)$ is a composition of holomorphic functions and so holomorphic for $|z| \leqslant A$, so in the final line we can use that $N''(z)$ is uniformly bounded for $|z| \leqslant A$ by a constant depending on A. We can estimate this last integral as follows

$$\begin{aligned}\int_{|z|=r} |z-r|^2 \left|\frac{n^z}{z^k}\right| |dz| &= \int_0^{2\pi} r^{3-k}|e^{i\theta}-1|^2 e^{r\cos\theta\log n} d\theta \\ &= r^{3-k}\int_{-\pi}^{\pi} 4\sin^2(\theta/2) e^{(k-1)\cos\theta} d\theta \\ &\leqslant r^{3-k}\int_{-\pi}^{\pi} \theta^2 e^{(k-1)(1-\theta^2/5)} d\theta \\ &\leqslant r^{3-k}e^{k-1}\int_{-\infty}^{\infty} \theta^2 e^{-(k-1)(\theta^2/5)} d\theta \\ &\ll r^{3-k}e^{k-1}(k-1)^{-3/2}.\end{aligned}$$

The error is therefore

$$\ll_A \frac{q^n}{n}\frac{e^{k-1}}{(k-1)^{(k-3/2)}}(\log n)^{k-3} \ll_A \frac{q^n}{n}\frac{k(\log n)^{k-3}}{(k-1)!}$$

by Stirling's approximation again and the result follows. □

Remark 2.4. *This follows the same ideas as Theorem 7.19 of [30].*

Now, taking $M(z) = F(1/q, z)$, $N(z) = G(z)$, $C_z(n) = A_z(n)$ and $\alpha_k(n) = \pi_k(n)$ in Proposition 2.3, and using Remark 2.2 and Corollary 2.2 to verify its hypotheses, we prove Theorem 2.1.

Remark 2.5. *We can also estimate $\rho_k(n) := \#\{f \in \mathcal{M}_n : \omega(f) = k\}$ by first proving an analogue of Proposition 2.2 for the power series*

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

then applying Proposition 2.1 with $M(T,z) = \tilde{F}(T,z)$ and $C(T,z) = \tilde{A}(T,z)$ where

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

and finally applying Proposition 2.3 with $M(z) = \tilde{F}(1/q,z)$, $N(z) = \tilde{G}(z) = \frac{\tilde{F}(1/q,z)}{\Gamma(1+z)}$,

$C_z(n) = \tilde{A}_z(n)$ and $\alpha_k(n) = \rho_k(n)$, in order to obtain an analogue of Theorem 2.1, namely

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

uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$.

Using this, and following Theorem 7.20 and Theorem 7.21 of [30], we can prove the analogue of the Erdős-Kac theorem for $\mathbb{F}_q[T]$, which tells us the mean, variance and limiting distribution of the function ω. We detail this more explicitly in Section 2.6.

2.3 The Sathé-Selberg formula in arithmetic progressions

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

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

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

be the associated L-function. As for $Z(T)^z$, we define $L(T,\chi)^z = \exp(z \log L(T,\chi))$ for $|T| < 1/q$ where we choose the branch of the logarithm which is real for T real. Our first task is to relate the coefficients of $Z(T)^z$ and $L(T,\chi)^z$. Consider the following identities which follow from the binomial theorem,

$$Z(T)^z = \prod_{p \in \mathcal{I}} (1 - T^{\deg p})^{-z} = \prod_{p \in \mathcal{I}} \left(1 + \sum_{k \geqslant 1} \binom{z+k-1}{k} T^{k \deg p}\right)$$

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

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 $Z(T)^z = \sum_{f \in \mathcal{M}} d_z(f) T^{\deg f}$ 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 $L(T,\chi)^z$.

2.3.1 Generalised divisor sums twisted by non-principal characters

Proposition 2.4. *For $\chi \neq \chi_0$, $|z| \leqslant A$ and $n \geqslant 1$*

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

Proof. From Proposition 4.3 of [33], we know that for $\chi \neq \chi_0$ we have

$$L(T,\chi) = \sum_{j=1}^{m-1}\left(\sum_{f\in\mathcal{M}_j}\chi(f)\right)T^j = \prod_{j=1}^{m-1}(1-\alpha_j T)$$

where $|\alpha_j|$ is $0, 1$ or $\sqrt{q}$ as a consequence of Weil's Theorem (the 'Riemannn Hypothesis' for curves over $\mathbb{F}_q$). Now, from the binomial theorem we get

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

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

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

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 $m, n \geqslant 1$ we get

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

□

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

We are now interested in π_k twisted by a character, which we define as

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

which, by analogy to Section 2.2, we relate to the generating function

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

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

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

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

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

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

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

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

2.3.2.1 Non-principal characters

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

Lemma 2.2. *For $|z| \leqslant A$ and $n \geqslant 2$*

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

where c_A is a constant depending on A.

Proof.

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

by the proof of Proposition 2.2. □

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

Proposition 2.5. *For $A > 1$ and $n \geqslant 2$*

$$A_z(n,\chi) \leqslant q^{n/2} \binom{n+Am}{n} n^{c_A}.$$

Proof. Using Proposition 2.4 and Lemma 2.2 we get

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

□

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

Proposition 2.6. *For $A > 1$ and $n \geqslant 2$*

$$\pi_k(n;\chi) \leqslant q^{n/2} \binom{n+Am}{n} n^{c_A}.$$

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 2.5 gives us that this is

$$\leqslant q^{n/2}\binom{n+Am}{n}n^{c_A}\frac{1}{2\pi}\oint\frac{|dz|}{|z|^{k+1}} \leqslant q^{n/2}\binom{n+Am}{n}n^{c_A}.$$

□

2.3.2.2 The principal character

Definition 2.1. *Define F_d, B_z^d and b_z^d via the following formal power series equalities*

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

Lemma 2.3. *For $|z|\leqslant A$ and $\sigma\geqslant\frac{2}{3}$*

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

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

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

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

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

Now, by the proof of Proposition 2.2, $\sum_{f\in\mathcal{M}}\frac{|b_z(f)|}{q^{\sigma\deg f}} \ll_A 1$ for $\sigma\geqslant\frac{2}{3}$, which gives the result. □

Lemma 2.4. *For $d \in \mathbb{F}_q[t]$ of degree $m \geqslant 1$ and $1 \geqslant \sigma > \frac{1}{2}$, we have*

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

Proof. Arrange the primes $p_1, \ldots, p_r$ dividing d and the primes $P_1, \ldots$ in $\mathcal{M}$, in order of degree (where you can order those of the same degree arbitrarily). Then we must have that $\deg P_i \leqslant \deg p_i$.

Now, for some $N \in \mathbb{N}$, we have that $\sum_{P:\deg P \leqslant N-1} \deg P < m \leqslant \sum_{P:\deg P \leqslant N} \deg P$. This means that d has at most $\#\{P : \deg P \leqslant N\}$ prime factors, and so, by the observation in the paragraph above

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

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

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

where $\pi(n) = \pi_1(n) = \#\{f \in \mathcal{M}_n : f \text{ is prime}\}$. Our choice of N tells us that $q^N \leqslant qm$ (so $N \leqslant (1+2\log m)$), since we have from the prime polynomial theorem that

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

Putting everything together we get that

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

□

Proposition 2.7. *For $|z| \leqslant A$ we have that*

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

where K_A is a constant depending on A.

Proof. When $\log m < 10A + 10$ it suffices to show that $\sum_{a \geqslant 0} \frac{|B_z^d(a)|}{q^a} a^{2A+2} \ll_A 1$. This is indeed true in this case, since $m \ll_A 1$, and so by Lemma 2.3 we have that for $\sigma \geqslant \frac{2}{3}$

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

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

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

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

So overall we have that $a^{2A+2} \leqslant (\log m)^{4A+4} q^{\tau a}$. Using this fact and Lemmas 2.3 and 2.4 we get that

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

□

Proposition 2.8. *Uniformly for $|z| \leqslant A$ and $n \geqslant 1$, we have*

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

Proof. The first equality follows from the proof of Proposition 2.1 (carrying throughout an additional factor of $(1+\log m)^{K_A}$ in the error term) and Proposition 2.7 after noting that

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

The second equality follows from the observation that

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

□

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

Proposition 2.9. *Let $A>1$, $\sqrt{n}\geqslant(1+\log m)^{K_A}$ and*

$$G_d(z) = \left(\prod_{p|d}\left(1+\frac{z}{q^{\deg p}}\right)^{-1}\right)\frac{F(1/q,z)}{\Gamma(1+z)}.$$

Then

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

uniformly for all $n\geqslant 2$ and $1\leqslant k\leqslant A\log n$.

Proof. For $|z|\leqslant A$, by Proposition 2.8 and our condition on n,

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

Now, we use Proposition 2.3 with $M(z) = \left(\prod_{p|d}\left(1+\frac{z}{q^{\deg p}}\right)^{-1}\right)F(1/q,z)$ (which is holomorphic for $|z|\leqslant A$ by Remark 2.2), $N(z)=G_d(z)$, $C_z(n)=A_z(n,\chi_0)$ and $\alpha_k(n)=\pi_k(n,\chi_0)$ to deduce the result.

□

2.3.3 Proof of Theorem 2.2

We are now ready to present the proof of Theorem 2.2.

Proof of Theorem 2.2. We begin with the orthogonality of characters,

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

where the sum is over characters $\chi : \left(\frac{\mathbb{F}_q[t]}{d(t)}\right)^\times \longrightarrow \mathbb{C}^\times$, and $\Phi(d) = \left|\left(\frac{\mathbb{F}_q[t]}{d(t)}\right)^\times\right|$.

We use this to get that

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

where we use Proposition 2.4 in the third line and Proposition 2.9 (which is applicable since the condition $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n \geqslant m$ implies the condition $\sqrt{n} \gg_A (1+\log m)^{K_A}$) in the fourth line.

Then note that, using Stirling's inequalities $\sqrt{2\pi} n^{n+1/2}e^{-n} \leqslant n! \leqslant e n^{n+1/2}e^{-n}$ we get that for $a,b \geqslant 1$

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

Using this and the condition $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n \geqslant m$ we get

$$q^{n/2}\binom{n+Am}{n}n^{c_A+2} \leqslant q^{n/2}\binom{n+\frac{A}{2}n}{n}n^{c_A+2} \leqslant q^{n/2}\left(1+\frac{A}{2}\right)^n\left(1+\frac{2}{A}\right)^{\frac{A}{2}n} n^{c_A+2}$$
$$\ll_A q^{n/2}\left(1+\frac{A}{2}\right)^n e^n \leqslant q^{n-m}.$$

From this, we then get that

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

□

Remark 2.6. *It is convenient for our proof of Theorem 2.3 to restate the result of Theorem 2.2 as it appears in the end of the proof, that is (under the same conditions as Theorem 2.2) as*

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

2.4 The Sathé-Selberg formula in short intervals

2.4.1 The Involution Trick

As in [24], 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 has been known for a long time (see for example [20]). The following lemma, for example, appears as Lemma 4.2 in [24].

Lemma 2.5. *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 $f = p_1^{a_1} \dots p_r^{a_r} \in \mathbb{F}_q[t]$ where p_i are distinct irreducibles none of which are t, then $f^* = (p_1^*)^{a_1} \dots (p_r^*)^{a_r}$ 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 $\mu(f^*) = \mu(f)$. □

In order to apply our result concerning polynomials from an arithmetic progression to prove one about polynomials belonging to a short interval, we use the following observation.

Lemma 2.6. *Let f and g be polynomials of degree n and h an integer $\leqslant n$. Then* $\deg(f - g) \leqslant h$ *if and only if* $f^* \equiv g^* \mod t^{n-h}$.

Proof. Write

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

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

where a_n and b_n are non-zero. Then

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

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

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

Remark 2.7. *Notice that f^* and g^* have non-zero constant terms.*

2.4.2 Proof of Theorem 2.3

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

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

Using Lemma 2.6 on the first sum we get

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

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 $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right) n > n - h \geqslant 1$, we may apply Remark 2.6 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,

$$\sum_{\substack{f\in\mathcal{M}_{n-1} \\ \deg(tf-g)\leqslant h \\ \omega(tf)=k}} \mu^2(tf) = \sum_{\substack{f\in\mathcal{M}_{n-1} \\ \deg(tf-g)\leqslant h \\ \omega(f)=k-1 \\ f(0)\neq 0}} \mu^2(tf) + \sum_{\substack{f\in\mathcal{M}_{n-1} \\ \deg(tf-g)\leqslant h \\ \omega(f)=k \\ f(0)=0}} \mu^2(tf)$$

and then apply Lemma 2.6 to the former to get

$$\sum_{\substack{\deg f=n-1 \\ f\equiv g^* \mod t^{n-h} \\ \omega(f)=k-1}} \mu^2(f) = \sum_{a\in\mathbb{F}_q^*} \sum_{\substack{f\in\mathcal{M}_{n-1} \\ f\equiv a^{-1}g^* \mod t^{n-h} \\ \omega(f)=k-1}} \mu^2(f) = \sum_{a\in\mathbb{F}_q^*} \pi_{k-1}(n-1; a^{-1}g^*, t^{n-h}).$$

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 $\left(\frac{1}{2} - \frac{1+\log(1+\frac{A}{2})}{\log q}\right)(n-1) \geqslant n-h \geqslant 1$, we may apply Remark 2.6 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 the theorem.

2.5 The q-limit

We conclude by briefly discussing what happens in the regime in which q tends to infinity. First, note that

$$\begin{aligned}
\pi_k(n) = \sum_{\substack{f\in\mathcal{M}_n\\ \omega(f)=k}} \mu^2(f) &= \frac{1}{k!}\sum_{\substack{p_1,\dots,p_k\in\mathcal{I}\\ \text{pairwise distinct}\\ \deg(p_1\dots p_k)=n}} 1\\
&= \frac{1}{k!}\left(\sum_{\substack{p_1,\dots,p_k\in\mathcal{I}\\ \deg(p_1\dots p_k)=n}} 1 + O\left(\binom{k}{2}\sum_{\substack{p_1,\dots,p_k\in\mathcal{I}\\ p_{k-1}=p_k\\ \deg(p_1\dots p_k)=n}} 1\right)\right)\\
&= \frac{1}{k!}\left(\sum_{\substack{p_1,\dots,p_k\in\mathcal{I}\\ \deg(p_1\dots p_k)=n}} 1 + O\left(k^2\sum_{\substack{p_1,\dots,p_{k-1}\in\mathcal{I}\\ \deg(p_1\dots p_{k-1})\leqslant n-1}} 1\right)\right)
\end{aligned}$$

where the error term comes from bounding the over count by terms where (at least) two of the p_i are the same. Now, using the prime polynomial theorem, and taking $k = O(q)$ for the third equality below we get that our sum is

$$\sum_{\substack{p_1,\dots,p_k\in\mathcal{I}\\ \deg(p_1\dots p_k)=n}} 1 = \sum_{\substack{n_1+\dots+n_k=n\\ n_i\geqslant 1}}\prod_{i=1}^{k}\frac{1}{n_i}(q^{n_i}+O(q^{\lfloor n_i/2\rfloor})) \quad = q^n\sum_{\substack{n_1+\dots+n_k=n\\ n_i\geqslant 1}}\frac{1}{n_1\dots n_k}(1+O(1/q))^k$$

and on using the fact that $n_1 + \ldots + n_k = n$, that

$$\sum_{\substack{p_1,\ldots,p_k \in \mathcal{I} \\ \deg(p_1 \ldots p_k) = n}} 1 = \frac{q^n}{n} \sum_{\substack{n_1+\ldots+n_k=n \\ n_i \geqslant 1}} \frac{n_1 + \ldots + n_k}{n_1 \ldots n_k}(1 + O(k/q))$$
$$= \frac{q^n}{n} k \sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1 \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}}(1 + O(k/q)).$$

Similarly, using the second equality above, and again taking $k = O(q)$, the sum in the error term is

$$\sum_{\substack{p_1,\ldots,p_{k-1} \in \mathcal{I} \\ \deg(p_1 \ldots p_{k-1)} \leqslant n-1}} 1 = \sum_{r \leqslant n-1} \sum_{\substack{p_1,\ldots,p_{k-1} \in \mathcal{I} \\ \deg(p_1 \ldots p_{k-1)} = r}} 1$$
$$\leqslant \sum_{r \leqslant n-1} q^r \sum_{\substack{n_1+\ldots+n_{k-1}=r \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}}(1 + O(1/q))^k$$
$$\leqslant q^{n-1} \sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1 \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}}(1 + O(k/q)).$$

Putting these results together we get, as long as $k = O(q)$, that

$$\pi_k(n) = \frac{q^n}{n} \frac{1}{(k-1)!} \sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1 \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}}(1 + O(kn/q))$$

which gives us an asymptotic formula for $\pi_k(n)$ as $q \to \infty$, as long as $k = o(q/n)$.

Moreover, note that, when $k = O(\log n / \log\log n)$, we have that

$$\sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1 \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}} \geqslant \left(\sum_{r \leqslant \frac{n-1}{k}} \frac{1}{r} \right)^{k-1} = \log^{k-1} n \left(1 + O\left(\frac{k \log k}{\log n} \right) \right)$$

and

$$\sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1 \\ n_i \geqslant 1}} \frac{1}{n_1 \ldots n_{k-1}} \leqslant \left(\sum_{r \leqslant n} \frac{1}{r} \right)^{k-1} = \log^{k-1} n \left(1 + O\left(\frac{k}{\log n} \right) \right)$$

so that, as long as $k = o(\log n/\log\log n)$, we get, as $n \to \infty$, that

$$\frac{q^n}{n}\frac{1}{(k-1)!}\sum_{\substack{n_1+\ldots+n_{k-1}\leqslant n-1\\ n_i\geqslant 1}}\frac{1}{n_1\ldots n_{k-1}} \sim \frac{q^n}{n}\frac{\log^{k-1} n}{(k-1)!}.$$

This agrees with Theorem 2.1 in this range for k (after noting that $G(z) = 1 + O(|z|)$).

One can use similar elementary calculations, along with the input of the prime polynomial theorem in arithmetic progressions, to get asymptotic formulae for $\pi_k(n; g, d)$, and consequently $\pi_k(n; g; h)$ using the involution trick (as in Section 2.4) for the same range of k.

2.6 The function field Erdős-Kac Theorem

In Remark 2.5, we outlined how to show, uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A\log n$, that

$$\rho_k(n) := \#\{f \in \mathcal{M}_n : \omega(f) = k\} \sim \frac{q^n}{n}\frac{(\log n)^{k-1}}{(k-1)!}\left(\tilde{G}\left(\frac{k-1}{\log n}\right) + O_A\left(\frac{k}{(\log n)^2}\right)\right)$$

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

Now, we will use this result to prove that the limiting distribution of the of the function ω is normal, with a given mean and variance, which we compute below. This is the analogue of the *Erdős-Kac Theorem* for the integers, and can also be proved, both in the setting of the integers and in the setting of function fields, using the *Method of Moments* (see, for example, Example 1 and Example 3 in [27]).

We begin to compute the mean value of $\omega(f)$ for $f \in \mathcal{M}_n$, using the prime polynomial theorem, thus

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\omega(f) = \frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\sum_{p\in\mathcal{I}:p|f}1 = \sum_{p\in\mathcal{I}_{\leqslant n}}\frac{1}{q^{\deg p}} = \sum_{k\leqslant n}\frac{\pi(k)}{q^k} = \sum_{k\leqslant n}\left(\frac{1}{k} + \sum_{d|k:d\neq 1}\frac{\mu(d)}{kq^{k(1-1/d)}}\right).$$

We observe that the sum over the secondary term tends to a constant with an error of at most $O\left(\frac{1}{q^{n/2}}\right)$, and then recall that $\sum_{k\leqslant n}\frac{1}{k} = \log n + \gamma + O\left(\frac{1}{n}\right)$, where γ is the

Euler-Mascheroni constant. Putting this all together, we get that

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\omega(f)=\log n+\beta+O\left(\frac{1}{n}\right)$$

where $\beta=\gamma+\sum_{k\geqslant 1}\sum_{d|k:d\neq 1}\frac{\mu(d)}{kq^{k(1-1/d)}}$ is a constant. So, the mean of $\omega(f)$ is about $\log\deg f$. Next we begin computing the variance, as follows

$$\begin{aligned}\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}(\omega(f)-\log\deg f)^2&=\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\omega(f)^2-2\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\omega(f)\log n+(\log n)^2\\&=\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\omega(f)^2-(\log n)^2-2\beta\log n+O\left(\frac{\log n}{n}\right)\end{aligned}$$

The first sum can be written as

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\left(\sum_{p\in\mathcal{I}:p|f}1\right)^2=\frac{1}{q^n}\sum_{p\in\mathcal{I}_{\leqslant n}}\sum_{q\in\mathcal{I}_{\leqslant n}}\sum_{\substack{f\in\mathcal{M}_n\\p|f,q|f}}1.$$

The terms for which $p=q$ contribute,

$$\sum_{p\in\mathcal{I}_{\leqslant n}}\frac{1}{q^{\deg p}}=\log n+\beta+O\left(\frac{1}{n}\right).$$

where we recognise the same expression as when we computed the mean. Using this result again, and recalling that for $p\neq q$ we have $p|f$ and $q|f$ if, and only if, $pq|f$, the remaining terms contribute

$$\begin{aligned}\frac{1}{q^n}\sum_{\substack{p,q\in\mathcal{I}_{\leqslant n}\\p\neq q}}\sum_{\substack{f\in\mathcal{M}_n\\pq|n}}1&=\sum_{\substack{p,q\in\mathcal{I}_{\leqslant n}\\p\neq q}}\frac{1}{q^{\deg p+\deg q}}\\&=\left(\sum_{p\in\mathcal{I}_{\leqslant n}}\frac{1}{q^{\deg p}}\right)^2-\sum_{p\in\mathcal{I}_{\leqslant n}}\frac{1}{q^{2\deg p}}\\&=(\log n)^2+2\beta\log n+\beta^2-\delta+O\left(\frac{\log n}{n}\right)\end{aligned}$$

where, for some constant δ,

$$\sum_{p\in\mathcal{I}_{\leqslant n}}\frac{1}{q^{2\deg p}}=\sum_{k\leqslant n}\frac{\pi(k)}{q^{2k}}=\sum_{k\leqslant n}\left(\frac{1}{kq^k}+O\left(\frac{1}{kq^{3k/2}}\right)\right)=:\delta+O\left(\frac{1}{q^n}\right).$$

Putting this together we have

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}(\omega(f)-\log\deg f)^2=\log n+\beta^2+\beta-\delta+O\left(\frac{\log n}{n}\right).$$

So, the variance of $\omega(f)$ is also about $\log\deg f$. If $\omega(f)$ really were distributed randomly then we would expect that the proportion of $\omega(f)$ which differs from the mean by some multiple of the standard deviation should go to 0 as that multiple tends to infinity. The next proposition makes a precise statement along these lines.

Proposition 2.10. *Let $h(n)$ be any real valued function such that $h(n)\to\infty$ as $n\to\infty$. Then for sufficiently large n,*

$$\alpha_h(n):=\frac{1}{q^n}\#\{f\in\mathcal{M}_n\ :\ |\omega(f)-\log\deg f|>h(n)\sqrt{\log\deg f}\}\leqslant\frac{2}{h(n)^2}.$$

In particular, $\alpha_h(n)\to 0$ as $n\to\infty$.

Proof.

$$\begin{aligned}\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}(\omega(f)-\log\deg f)^2&\geqslant\frac{1}{q^n}\sum_{\substack{f\in\mathcal{M}_n\\|\omega(f)-\log\deg f|>h(n)\sqrt{\log\deg f}}}(\omega(f)-\log\deg f)^2\\&\geqslant\alpha_h(x)h(n)^2\log n\end{aligned}$$

If instead we had $\alpha_h(n)h(n)^2>2$ for arbitrarily large n this would contradict the estimate for the variance of ω derived above. □

We will use this result, together with the following lemma (related to the Central Limit Theorem) and our results for $\rho_k(n)$ to show that for $\omega(f)$ does indeed look like a normally distributed random variable with mean $\log\deg f$ and variance $\log\deg f$.

Lemma 2.7. *Let k be a positive integer and let x be a positive real number such that $|k-x|\leqslant x^{2/3}$. Then*

$$\frac{e^{-x}x^{k-1}}{(k-1)!}=\frac{e^{-\frac{(k-x)^2}{2x}}}{\sqrt{2\pi x}}\left(1+O\left(\frac{1}{\sqrt{x}}\right)+O\left(\frac{|k-x|^3}{x^2}\right)\right).$$

Proof. Let $\theta=k-x$ so $|\theta|^3\leqslant x^2$ and note that for $x\geqslant 8$ we have $\frac{|\theta|}{x}\leqslant\frac{1}{2}$ so that

$\log(1+\frac{\theta}{x}) = \frac{\theta}{x} - \frac{\theta^2}{2x^2} + O\left(\frac{|\theta|^3}{x^3}\right)$. Also note that,

$$\frac{\theta^2}{x^2} \leqslant \frac{|\theta|}{x}$$

and moreover, by the AM-GM inequality, we have that:

$$\frac{|\theta|}{x} = \sqrt[3]{\frac{|\theta|^3}{x^3}} \leqslant \frac{1}{3}\left(\frac{|\theta|^3}{x^2} + \frac{1}{\sqrt{x}} + \frac{1}{\sqrt{x}}\right) \leqslant \frac{|\theta|^3}{x^2} + \frac{1}{\sqrt{x}}$$

We now apply Stirling's approximation in the form $\frac{1}{(k-1)!} = \frac{1}{\sqrt{2\pi k}} e^k k^{-k+1}(1+O(\frac{1}{k}))$ to get

$$\begin{aligned}
\frac{e^{-x}x^{k-1}}{(k-1)!} &= \frac{1}{\sqrt{2\pi k}} e^{-x}x^{k-1}e^k k^{-k+1}\left(1+O\left(\frac{1}{k}\right)\right) \\
&= \frac{1}{\sqrt{2\pi}} \exp\left((x+\theta-1)\log x + \theta - (x+\theta-1)\log(x+\theta) - \frac{1}{2}\log(x+\theta)\right) \\
&\times \left(1+O\left(\frac{1}{x}\right)\right) \\
&= \frac{1}{\sqrt{2\pi x}} \exp\left(\theta - \left(x+\theta-\frac{1}{2}\right)\log\left(1+\frac{\theta}{x}\right)\right)\left(1+O\left(\frac{1}{x}\right)\right) \\
&= \frac{1}{\sqrt{2\pi x}} \exp\left(\theta - \left(x+\theta-\frac{1}{2}\right)\left(\frac{\theta}{x} - \frac{\theta^2}{2x^2} + O\left(\frac{|\theta|^3}{x^3}\right)\right)\right)\left(1+O\left(\frac{1}{x}\right)\right) \\
&= \frac{1}{\sqrt{2\pi x}} \exp\left(\theta - \left(\theta + \frac{\theta^2}{2x} - \frac{\theta}{2x} + \frac{\theta^2}{4x^2} + O\left(\frac{|\theta|^3}{x^2}\right)\right)\right)\left(1+O\left(\frac{1}{x}\right)\right) \\
&= \frac{1}{\sqrt{2\pi x}} \exp\left(-\frac{\theta^2}{2x} + O\left(\frac{1}{\sqrt{x}}\right) + O\left(\frac{|\theta|^3}{x^2}\right)\right)\left(1+O\left(\frac{1}{x}\right)\right) \\
&= \frac{1}{\sqrt{2\pi x}} \exp\left(-\frac{\theta^2}{2x}\right)\left(1+O\left(\frac{1}{\sqrt{x}}\right) + O\left(\frac{|\theta|^3}{x^2}\right)\right)
\end{aligned}$$

by our observations above. □

Theorem 2.4. *(Erdős-Kac) For all real λ satisfying $\lambda \leqslant (\log n)^{1/6}$ we have*

$$\frac{1}{q^n}\#\{f \in \mathcal{M}_n : \omega(f) \leqslant \log\deg f + \lambda\sqrt{\log\deg f}\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\lambda} e^{-t^2/2}dt + O((\log n)^{-1/3}).$$

Proof. Let $\lambda \leqslant (\log n)^{1/6}$ and $y = \log n$. Proposition 2.10, applied with $h(n) = (\log n)^{1/6}$ gives:

$$\frac{1}{q^n}\sum_{k\leqslant y+\lambda y^{1/2}} \rho_k(n) = \frac{1}{q^n}\sum_{y-y^{2/3}\leqslant k\leqslant y+\lambda y^{1/2}} \rho_k(n) + O(y^{-1/3})$$

Recall that $\tilde{G}(z) = \frac{1}{\Gamma(1+z)} \prod_{p \in \mathcal{I}} \left(1 + \frac{zT^{\deg p}}{1-T^{\deg p}}\right)(1 - T^{\deg p})^z$, so that by Taylor expansion,

$$\tilde{G}\left(\frac{k-1}{y}\right) = \tilde{G}(1) + O\left(\left|\frac{k-1}{y} - 1\right|\right) = 1 + O\left(\frac{|k-y|}{y}\right)$$

and since $|k-y| \leqslant y^{2/3}$, just as in the proof of the Lemma 2.7, this is

$$1 + O\left(\frac{1}{\sqrt{y}}\right) + O\left(\frac{|k-y|^3}{y^2}\right).$$

Combining our estimate for $\rho_k(x)$ with the previous lemma then gives

$$\begin{aligned}\frac{1}{q^n} \sum_{y - y^{2/3} \leqslant k \leqslant y + \lambda y^{1/2}} \rho_k(n) &= \sum_{y - y^{2/3} \leqslant k \leqslant y + \lambda y^{1/2}} \frac{e^{-y} y^{k-1}}{(k-1)!} \left(\tilde{G}\left(\frac{k-1}{y}\right) + O(ky^{-2})\right) \\ &= \sum_{y - y^{2/3} \leqslant k \leqslant y + \lambda y^{1/2}} \frac{e^{-\frac{(k-y)^2}{2y}}}{\sqrt{2\pi y}} \left(1 + O\left(\frac{1}{\sqrt{y}}\right) + O\left(\frac{|k-y|^3}{y^2}\right)\right)\end{aligned}$$

It is now just a case of approximating these sums with integrals. The summand is monotonic for $k < y$ and for $k > y$ and attains its maximum $1/(2\pi\sqrt{y})$ at $k = y$. Therefore

$$\begin{aligned}\sum_{y - y^{2/3} \leqslant k \leqslant y + \lambda y^{1/2}} \frac{e^{-\frac{(k-y)^2}{2y}}}{\sqrt{2\pi y}} &= \int_{y - y^{2/3}}^{y + \lambda y^{1/2}} \frac{e^{-\frac{(u-y)^2}{2y}}}{\sqrt{2\pi y}} du + O\left(\frac{1}{\sqrt{y}}\right) \\ &= \frac{1}{\sqrt{2\pi}} \int_{-y^{1/6}}^{\lambda} e^{-t^2/2} \mathrm{d}t + O\left(\frac{1}{\sqrt{y}}\right) \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-t^2/2} \mathrm{d}t + O\left(\frac{1}{\sqrt{y}}\right)\end{aligned}$$

after the substitution $u = y + \sqrt{y}t$. Similarly,

$$\begin{aligned}\sum_{y - y^{2/3} \leqslant k \leqslant y + \lambda y^{1/2}} \frac{e^{-\frac{(k-y)^2}{2y}}}{\sqrt{2\pi y}} \frac{|k-y|^3}{y^2} &= \int_{y - y^{2/3}}^{y + \lambda y^{1/2}} \frac{e^{-\frac{(u-y)^2}{2y}}}{\sqrt{2\pi y}} \frac{|u-y|^3}{y^2} du + O\left(\frac{1}{\sqrt{y}}\right) \\ &= \frac{1}{\sqrt{2\pi}} \int_{-y^{1/6}}^{\lambda} e^{-t^2/2} \frac{t^3}{\sqrt{y}} \mathrm{d}t + O\left(\frac{1}{\sqrt{y}}\right) \\ &= O\left(\frac{1}{\sqrt{y}}\right)\end{aligned}$$

after the same substitution and the result follows.

□

Chapter 3

Highly Composite Polynomials in $\mathbb{F}_q[t]$

This chapter is based primarily on and largely appears, with the exception of the additions of Sections 3.2 and 3.6, in [1].

We investigate the analogues, in $\mathbb{F}_q[t]$, of highly composite numbers and the maximum order of the divisor function, as studied by Ramanujan. In particular, we determine a family of highly composite polynomials which is not too sparse, and we use it to compute the logarithm of the maximum of the divisor function at every degree up to an error of a constant, which is significantly smaller than in the case of the integers, even assuming the Riemann Hypothesis.

3.1 Introduction

In [32], Ramanujan investigated the divisor function $d(n)$, the number of divisors of n. Being interested in the maximum order of $d(n)$, he defined highly composite integers n to be those for which $d(n) > d(n')$ for all $n > n'$, so that $D(N) := \max\{d(n) \mid n \leqslant N\}$ is given by $d(n')$ for the largest highly composite $n' \leqslant N$. He was able to compute $\log D(N)$ up to an error of at most $O(e^{-c\sqrt{\log\log N}} \log N)$ unconditionally and $O\left(\frac{\sqrt{\log N}}{(\log\log N)^3}\right)$ assuming the Riemann Hypothesis. Ramanujan studied carefully the prime factorisation of the highly composite integers, and his results were improved by Alaoglu and Erdős in [4], who determined the exponent of each prime in the factorisation of a highly composite number up to an error of at most 1.

We consider the question of maximising the divisor function in the function field setting. Let $\mathbb{F}_q$ be a finite field, $\mathcal{M} = \{f \in \mathbb{F}_q[t] \text{ monic}\}$, $\mathcal{M}_n = \{f \in \mathcal{M} : \deg f = n\}$, $\mathcal{I} = \{f \in \mathcal{M} \text{ irreducible}\}$, $\mathcal{I}_n = \{f \in \mathcal{I} : \deg f = n\}$, and $\pi(n) = |\mathcal{I}(n)| = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$ where

$\mu(d)$ is the Möbius function. For $f \in \mathcal{M}$, let $\tau(f)$ be the number of monic divisors of f, and observe that a generic polynomial f in $\mathcal{M}$ is of the form

$$f = \prod_{p \in \mathcal{I}} p^{a_p} \quad \text{with} \quad \deg f = \sum_{p \in \mathcal{I}} a_p \deg p \quad \text{and} \quad \tau(f) = \prod_{p \in \mathcal{I}} (1 + a_p) \tag{3.1}$$

where only finitely many a_p are non-zero. We wish to understand the polynomials which maximise the function τ up to a given degree, defined thus:

Definition 3.1. *We call $f \in \mathcal{M}$ a* highly composite polynomial *of degree n if $\tau(f) = \max\{\tau(g) \mid g \in \bigcup_{m \leqslant n} \mathcal{M}_m\}$.*

Remark 3.1. *Highly composite polynomials of a given degree are not necessarily unique. For example, all linear polynomials in $\mathcal{M}_1$ are highly composite polynomials of degree 1.*

Remark 3.2. *There is (at least) one new highly composite polynomial at each degree. Indeed, let f be a highly composite polynomial of degree n and suppose otherwise, so that $\deg f = m < n$. Then pick some $g \in \mathcal{M}_{n-m}$, so that $fg \in \mathcal{M}_n$ but $\tau(fg) = \#\{d \in \mathcal{M} : d|fg\} \geqslant \#(\{d \in \mathcal{M} : d|f\} \cup \{fg\}) > \tau(f)$, which is a contradiction.*

Remark 3.3. *If $f = \prod_{p \in \mathcal{I}} p^{a_p}$ is a highly composite polynomial, then $\deg p_i < \deg p_j$ implies $a_{p_i} \geqslant a_{p_j}$. Indeed, suppose otherwise and set $g = f p_i^{a_{p_j} - a_{p_i}} p_j^{a_{p_i} - a_{p_j}}$, so that $\tau(g) = \tau(f)$ but $\deg g = \deg f - (a_{p_j} - a_{p_i})(p_j - p_i) < \deg f$, which contradicts Remark 3.2.*

Remark 3.4. *See Section 3.5 for an illustrative table of highly composite polynomials in $\mathbb{F}_2[t]$.*

In [32], Ramanujan defines n to be a *superior highly composite number* if for some $x > 0$

$$\frac{d(n)}{n^{1/x}} \begin{cases} \geqslant \frac{d(n')}{n'^{1/x}} & \text{if } n > n' \\ > \frac{d(n')}{n'^{1/x}} & \text{if } n < n' \end{cases} \tag{3.2}$$

so that $d(n) > d(n')$ for all $n' < n$ and therefore n is highly composite. Then, by comparing the prime factorisation of n with the prime factorisations of n/p and np for each prime p dividing n, and using equation (3.2), he demonstrates that for each x there is a unique superior highly composite number

$$n = n(x) = \prod_{p \text{ prime}} p^{e_p} \quad \text{where} \quad e_p = e_p(x) = \left\lfloor \frac{1}{p^{1/x} - 1} \right\rfloor. \tag{3.3}$$

He then uses these numbers to get an upper bound for the divisor function, the analogue of which we discuss in Section 3.6.

Inspired by Ramanujan's idea, we first investigate a family of highly composite polynomials $\{h(x)\}_{x>0}$, which we define as follows:

Definition 3.2. *Let $x > 0$. We say that $h = h(x) \in \mathcal{M}$ is an x-*superior highly composite *polynomial, or just x-SHC, if for all $f \in \mathcal{M}$ we have*

$$\frac{\tau(h)}{q^{\deg h/x}} \begin{cases} \geqslant \frac{\tau(f)}{q^{\deg f/x}} & \text{if } \deg h \geqslant \deg f \\ > \frac{\tau(f)}{q^{\deg f/x}} & \text{if } \deg h < \deg f \end{cases} \tag{3.4}$$

*and we say that h is an x-*semi-superior highly composite *polynomial, or x-SSHC, if for all $f \in \mathcal{M}$ we have*

$$\frac{\tau(h)}{q^{\deg h/x}} \geqslant \frac{\tau(f)}{q^{\deg f/x}}. \tag{3.5}$$

A polynomial which is x-SHC or x-SSHC for some $x > 0$ is called superior highly composite *or* semi-superior highly composite *respectively.*

Remark 3.5. *Clearly, if $h \in \mathcal{M}$ is x-SHC, then it is x-SSHC. Moreover, any polynomial h which is x-SSHC is highly composite, since if $f \in \mathcal{M}$ with $\deg f \leqslant \deg h$, then by equation* (3.5) *we have that*

$$\tau(f) \leqslant \frac{\tau(h)}{q^{(\deg h - \deg f)/x}} \leqslant \tau(h).$$

After defining a particular set for the parameter x of an x-SSHC:

Definition 3.3. *Let*

$$S = S_q := \left\{ \frac{s \log q}{\log(1 + 1/r)} \ : \ s, r \geqslant 1 \right\}.$$

we are able to determine the structure of the superior highly composite polynomials and semi-superior highly composite polynomials. Our arguments are based on Ramanujan's proof of equation (3.3), and our results have a similar flavour, but we are able to be more precise on account of the discrete nature of the degree sequence of highly composite polynomials in this setting. In particular, we consider more precisely the parameter x, and this leads to

Theorem 3.1. *Let $x > 0$.*

1. *There is one, and only one, x-SHC polynomial, namely*

$$\hat{h} = \hat{h}(x) = \prod_{k \geqslant 1} \prod_{p \in \mathcal{I}_k} p^{a_k} \quad \textit{where} \quad a_k = a_k(x) = \left\lfloor \frac{1}{q^{k/x} - 1} \right\rfloor \tag{3.6}$$

   Moreover, $\hat{h}$ is the unique highly composite polynomial of its degree.

2. *If $x' < x''$ are two consecutive elements of S, then $\hat{h}(x) = \hat{h}(x')$ for all $x' \leqslant x < x''$. So, there is a one-to-one correspondence between S and the set of superior highly composite polynomials, given by $x \to \hat{h}(x)$.*

and

Theorem 3.2. *Let $x > 0$.*

1. *If $x \notin S$, then there is only one x-SSHC polynomial, namely the polynomial $\hat{h}(x)$ defined in equation* (3.6)*.*

2. *If $x = \frac{s \log q}{\log(1+1/r)} \in S$, then there are $2^{\pi(s)}$ x-SSHC polynomials of the form*

$$h(x) = \frac{\hat{h}(x)}{P_{i_1} \cdots P_{i_v}}$$

   where $\hat{h}(x)$ is as in equation (3.6)*, $0 \leqslant v \leqslant \pi(s)$, $P_{i_1}, \cdots, P_{i_v} \in \mathcal{I}_s$ distinct, and* $\deg h(x) = \deg \hat{h}(x) - vs$*. Moreover, the unique polynomials h given by $v = \pi(s)$ and $v = 0$ are two (distinct) consecutive superior highly composite polynomials.*

3. *If $h(x)$ is x-SSHC and $g \in \mathcal{M}_{\deg h(x)}$ is a highly composite polynomial, then g is also x-SSHC.*

This family of semi-superior highly composite polynomials is not too sparse, so we can use it to construct polynomials at every degree which make the divisor function close to its maximum. In particular, if we let $T(N) := \max\{\tau(f) \mid f \in \mathcal{M}_N\}$, then we are able to compute $\log T(N)$ to within an error of at most $\log \frac{4}{3}$:

Theorem 3.3. *Let $x = \frac{s \log q}{\log(1+1/r)} \in S$, $\hat{h} = \hat{h}(x)$ and $a_k = a_k(x)$ be defined as in equation* (3.6)*, and h be an x-SSHC polynomial of degree* $\deg \hat{h}(x) - vs$ *with $0 \leqslant v < \pi(s)$. Then,* *if* $N = \deg h - u$ *with* $0 \leqslant u \leqslant s-1$, *we have*

$$\log T(N) = \begin{cases} \log \tau(h) & \textit{if } u = 0 \\ \log \tau(h) - \epsilon(N) & \textit{otherwise} \end{cases}$$

where

$$\frac{u}{s} \log\left(1 + \frac{1}{r}\right) \leqslant \epsilon(N) \leqslant \log\left(1 + \frac{1}{a_u}\right).$$

Moreover, the size of this range for $\epsilon(N)$ *is at most* $\log\left(1 + \frac{1}{a_u(a_u+2)}\right) \leqslant \log \frac{4}{3}$.

Remark 3.6. *From the final sentence of part 2 of Theorem 3.2, we know that the (distinct) superior highly composite polynomial* $\hat{h}(x')$ *immediately preceding* $\hat{h}(x)$ *has degree* $\deg \hat{h}(x') = \deg \hat{h}(x) - \pi(s)s$. *So, the form of* N *in Theorem 3.3 accounts for all integers between the degrees of these two consecutive superior highly composite polynomials. Therefore, for any* $N \geqslant 1$, *we can find* $x > 0$ *so as to express* N *in the form presented in Theorem 3.3.*

3.2 An elementary upper bound on the divisor function

Before we determine the form of our first family of highly composite polynomials, the superior highly composite polynomials, we first establish an elementary upper bound for the divisor function on $\mathcal{M}$.

Proposition 3.1. *If* $f \in \mathcal{M}_n$, *then for* n *sufficiently large*

$$\log_q \tau(f) \leqslant \frac{n \log 2}{\log n}\left(1 + \frac{1}{\log n}\left(3 \log\log n + o(1)\right)\right).$$

Proof. Write $f = \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i}$, where p_i are the distinct monic irreducibles dividing f, so that $n = \sum_{1 \leqslant i \leqslant r} \alpha_i \deg p_i$ and $\tau(f) = \prod_{1 \leqslant i \leqslant r}(1 + \alpha_i)$. Then, for $\lambda > 0$ to be chosen later, we have $\tau(f) = q^{\lambda n} \prod_{1 \leqslant i \leqslant r} \frac{1+\alpha_i}{q^{\lambda \alpha_i \deg p_i}}$. The factors in this product with $\deg p_i \geqslant \frac{\log 2}{\lambda \log q}$ are bounded by 1, since $1 + \alpha_i \leqslant 2^{\alpha_i}$. The other factors, with $1 \leqslant \deg p_i < \frac{\log 2}{\lambda \log q}$, are bounded by $\frac{1+\alpha_i}{q^{\lambda \alpha_i}} \leqslant e^{\sqrt{2\alpha_i} - \lambda \alpha_i \log q} \leqslant e^{\frac{1}{2\lambda \log q}}$ (using the fact that $1 + x \leqslant e^{\sqrt{2x}}$ for $x > 0$, and then the AM-GM inequality). We can bound the number of such factors as follows:

let $N = \lfloor \frac{\log 2}{\lambda \log q} \rfloor$, then

$$\sum_{1 \leqslant m \leqslant N} \pi(m) \leqslant \sum_{1 \leqslant m \leqslant N} \frac{q^m}{m} \leqslant \sum_{1 \leqslant m \leqslant N/2} q^m + \frac{2}{N} \sum_{N/2 < m \leqslant N} q^m$$
$$\leqslant q^{\frac{N}{2}} \left(1 + \frac{1}{q-1}\right) + \frac{4}{N} q^N \leqslant \frac{8}{N} q^N \leqslant 2^{\frac{1}{\lambda}} \frac{8\lambda \log q}{\log 2}$$

Therefore we have

$$\tau(f) \leqslant q^{\lambda n} \left(e^{\frac{1}{2\lambda \log q}}\right)^{2^{\frac{1}{\lambda}} \frac{8\lambda \log q}{\log 2}} = q^{\lambda n + 2^{\frac{1}{\lambda}} \frac{4}{\log 2 \log q}}.$$

Finally, we set $\lambda = \frac{\log 2}{\log n}(1 + 3\frac{\log \log n}{\log n})$ and take the logarithm to get

$$\begin{aligned}
\log_q \tau(f) &\leqslant \frac{n \log 2}{\log n}\left(1 + 3\frac{\log \log n}{\log n}\right) + \frac{4}{\log 2 \log q} n^{\frac{1}{1+3\frac{\log \log n}{\log n}}} \\
&= \frac{n \log 2}{\log n}\left(1 + 3\frac{\log \log n}{\log n}\right) + \frac{4n}{\log 2 \log q} e^{-\frac{3 \log \log n}{1+3\frac{\log \log n}{\log n}}} \\
&= \frac{n \log 2}{\log n}\left(1 + \frac{1}{\log n}\left(3 \log \log n + \frac{4}{\log^2 2 \log q}\left(\frac{1}{\log n}\right)^{\frac{1-6\frac{\log \log n}{\log n}}{1+3\frac{\log \log n}{\log n}}}\right)\right).
\end{aligned}$$

Note that, as n tends to infinity, $\frac{\log \log n}{\log n}$ tends to 0, so $\frac{1-6\frac{\log \log n}{\log n}}{1+3\frac{\log \log n}{\log n}}$ tends to 1, and $\left(\frac{1}{\log n}\right)^{\frac{1-6\frac{\log \log n}{\log n}}{1+3\frac{\log \log n}{\log n}}}$ tends to 0. □

Remark 3.7. *We can see that the main term in Proposition 3.1 is sharp by calculating $\tau(f)$ for the family of monic polynomials $f_m = \prod_{r \leqslant m} \prod_{p \in \mathcal{I}_r} p$. Observe that*

$$n := \deg f = \sum_{1 \leqslant k \leqslant m} k\pi(k) \geqslant \sum_{k|m} k\pi(k) = q^m$$

and so

$$\tau(f) = 2^{\sum_{1 \leqslant k \leqslant m} \pi(k)} \geqslant 2^{\frac{1}{m} \sum_{1 \leqslant k \leqslant m} k\pi(k)} = 2^{\frac{\deg f}{m}} \geqslant 2^{\frac{n}{\log_q n}} = q^{\frac{n \log 2}{\log n}}.$$

However, the error term in Proposition 3.1 is quite crude on account of our naive bound for $\pi(n)$.

3.3 Superior highly composite polynomials

We begin by showing, contingent on some auxiliary lemmas proven subsequently, that

Proposition 3.2. *For each $x > 0$, the function $\frac{\tau(f)}{q^{\deg f/x}}$ is maximised over all $f \in \mathcal{M}$ by (at least one) $h = h(x) \in \mathcal{M}$. Moreover, if we write $h = \prod_{p\in\mathcal{I}} p^{a_p} = \prod_{p\in\mathcal{I}} p^{a_p(x)}$, we have that*

1. *If $x \notin S$, then $a_p(x) = \left\lfloor \frac{1}{q^{\deg p/x}-1} \right\rfloor$ for each $p \in \mathcal{I}$ and so h is unique.*
2. *Else, if $x = \frac{s\log q}{\log(1+1/r)} \in S$, so that $r = \frac{1}{q^{s/x}-1}$, then*
$$a_p(x) = \begin{cases} \left\lfloor \frac{1}{q^{\deg p/x}-1} \right\rfloor & \text{if } \deg p \neq s \\ r \text{ or } r-1 & \text{if } \deg p = s \end{cases}$$
and so there are $2^{\pi(s)}$ such polynomials h.

Proof. From (3.1), we can write

$$\frac{\tau(f)}{q^{\deg f/x}} = \prod_{p\in\mathcal{I}} \frac{1+a_p}{q^{a_p \deg p/x}} = \exp\left(\sum_{p\in\mathcal{I}} \log(1+a_p) - \frac{a_p \deg p \log q}{x}\right)$$

so that to maximise $\frac{\tau(f)}{q^{\deg f/x}}$, for each $p \in \mathcal{I}$ we must maximise the quantity $\phi_{a_p} := \log(1+a_p) - \alpha a_p$ with $\alpha = \frac{\deg p \log q}{x}$.

If $x \notin S$, then α cannot be written as $\log(1+\frac{1}{j})$ for any integer j, so by Lemma 3.1 we have that ϕ_{a_p} is maximised if and only if $a_p = \left\lfloor \frac{1}{e^{\alpha}-1} \right\rfloor = \left\lfloor \frac{1}{q^{\deg p/x}-1} \right\rfloor$.

Otherwise, if $x \in S$, then by Lemma 3.2 there is a unique pair (s, r) such that $x = \frac{s\log q}{\log(1+1/r)}$. Therefore, if $\deg p \neq s$, then α cannot be written as $\log(1+\frac{1}{j})$ for any integer j, so by Lemma 3.1 we have that ϕ_{a_p} is maximised if and only if $a_p = \left\lfloor \frac{1}{e^{\alpha}-1} \right\rfloor = \left\lfloor \frac{1}{q^{\deg p/x}-1} \right\rfloor$. Else, if $\deg p = s$, then $\alpha = \log(1+\frac{1}{r})$ and so by Lemma 3.1 we have that ϕ_{a_p} is maximised if and only if $a_p = r$ or $r-1$. □

Remark 3.8. *Notice in both cases that $a_p(x)$ is zero for $\deg p > \frac{x\log 2}{\log q}$, so that the factorisation of h is in fact a finite product.*

This leads us first to the proof of Theorem 3.1:

Proof of Theorem 3.1. For $x > 0$, let $\hat{h} = \hat{h}(x) = \prod_{k \geqslant 1} \prod_{p \in \mathcal{I}_k} p^{a_k}$ with $a_k(x) = \left\lfloor \frac{1}{q^{k/x}-1} \right\rfloor$, and for $x = \frac{s \log q}{\log(1+1/r)} \in S$, let $E = E(x)$ be the set of polynomials defined in part 2 of Proposition 3.2.

1. If $x \notin S$, then from part 1 of Proposition 3.2, we know that for all $f \in \mathcal{M}$, we have

$$\frac{\tau(\hat{h})}{q^{\deg \hat{h}/x}} > \frac{\tau(f)}{q^{\deg f/x}}$$

and so $\hat{h}$ is the unique x-SHC. Moreover, if $\deg f \leqslant \deg \hat{h}$ then

$$\tau(\hat{h}) > \tau(f) q^{(\deg \hat{h} - \deg f)/x} \geqslant \tau(f)$$

and so $\hat{h}$ is the unique highly composite polynomial of its degree.

Otherwise, if $x = \frac{s \log q}{\log(1+1/r)} \in S$, so that $r = \frac{1}{q^{s/x}-1}$, we observe that $\hat{h} = \prod_{p \in \mathcal{I}} p^{\hat{a}_p}$ with

$$\hat{a}_p = \hat{a}_p(x) = \left\lfloor \frac{1}{q^{\deg p/x} - 1} \right\rfloor = \begin{cases} \left\lfloor \frac{1}{q^{\deg p/x}-1} \right\rfloor & \text{if } \deg p \neq s \\ r & \text{if } \deg p = s \end{cases}$$

so that $\hat{h}(x) \in E$. Therefore, by part 2 of Proposition 3.2, we have that

$$\frac{\tau(\hat{h})}{q^{\deg \hat{h}/x}} \begin{cases} = \frac{\tau(f)}{q^{\deg f/x}} & \text{if } f \in E \\ > \frac{\tau(f)}{q^{\deg f/x}} & \text{if } f \notin E \end{cases}.$$

and that for all $f \in E \setminus \{\hat{h}\}$, we have $\deg f \leqslant \deg \hat{h} - s < \deg \hat{h}$. Therefore $\hat{h}$ is the unique x-SHC, and moreover, if $\deg f \leqslant \deg \hat{h}$ then

$$\tau(\hat{h}) \begin{cases} = \tau(f) q^{(\deg \hat{h} - \deg f)/x} > \tau(f) & \text{if } f \in E \\ > \tau(f) q^{(\deg \hat{h} - \deg f)/x} \geqslant \tau(f) & \text{if } f \notin E \end{cases}$$

and so $\hat{h}$ is the unique highly composite polynomial of its degree.

2. Let $x' < x''$ be two consecutive elements of S, and let $\tilde{x} = \min\{x > x' : \hat{h}(x) \neq \hat{h}(x')\}$. Then there is some $\tilde{k}$ such that $a_{\tilde{k}}(\tilde{x}) = m > a_{\tilde{k}}(x')$. Therefore we must

have that

$$x' < \frac{\tilde{k}\log q}{\log\left(1+\frac{1}{m}\right)} \leqslant \tilde{x} < \frac{\tilde{k}\log q}{\log\left(1+\frac{1}{1+m}\right)}$$

and by the minimality of $\tilde{x}$ we must have that

$$\tilde{x} = \frac{\tilde{k}\log q}{\log\left(1+\frac{1}{m}\right)} \in S.$$

So, by the minimality of $\tilde{x}$ and the definition of x'', we conclude that $\tilde{x} = x''$, and therefore that $\hat{h}(x) = \hat{h}(x')$ for all $x' \leqslant x < x''$. It follows that there is a one-to-one correspondence between S and the set of superior highly composite polynomials, given by $x \to \hat{h}(x)$.

□

and then to the proof of Theorem 3.2:

Proof of Theorem 3.2. For $x > 0$, let $\hat{h} = \hat{h}(x) = \prod_{k\geqslant 1}\prod_{p\in\mathcal{I}_k} p^{a_k}$ with $a_k(x) = \left\lfloor \frac{1}{q^{k/x}-1} \right\rfloor$, and for $x = \frac{s\log q}{\log(1+1/r)} \in S$, let $E = E(x)$ be the set of polynomials defined in part 2 of Proposition 3.2.

1. If $x \notin S$, then the result follows from part 1 of Proposition 3.2.

2. If $x = \frac{s\log q}{\log(1+1/r)} \in S$, then from part 2 of Proposition 3.2, we have that the x-SSHC polynomials are precisely the $2^{\pi(s)}$ polynomials in the set E, which we can rewrite as

$$E = \left\{ h(x) = \frac{\hat{h}(x)}{P_{i_1}\cdots P_{i_v}} \;:\; 0 \leqslant v \leqslant \pi(s) \text{ and } P_{i_1}, \cdots, P_{i_v} \in \mathcal{I}_s \text{ distinct} \right\}.$$

When $v = 0$, $h(x) = \hat{h}(x)$ is superior highly composite. When $v = \pi(s)$, $h(x) = \prod_{k\geqslant 1}\prod_{p\in\mathcal{I}_k} p^{\tilde{a}_k}$ where

$$\tilde{a}_k = \tilde{a}_k(x) = \begin{cases} a_k(x) & \text{if } k \neq s \\ r-1 & \text{if } k = s \end{cases}.$$

Now, let $y = \max\{x' \in S : x' < x\}$ so that, by the definition of x and y, we have

$$\frac{s \log q}{\log\left(1 + \frac{1}{r-1}\right)} \leqslant y < x = \frac{s \log q}{\log\left(1 + \frac{1}{r}\right)}$$

and so $a_k(y) = r - 1$. When $k \neq s$, by Lemma 3.2, we cannot have that $x = \frac{k \log q}{\log(1+1/a_k(x))} \in S$, and so

$$\frac{k \log q}{\log\left(1 + \frac{1}{a_k(x)}\right)} < x < \frac{k \log q}{\log\left(1 + \frac{1}{1+a_k(x)}\right)}.$$

This means that, by the definition of y, we have for $k \neq s$ that

$$\frac{k \log q}{\log\left(1 + \frac{1}{a_k(x)}\right)} \leqslant y < x < \frac{k \log q}{\log\left(1 + \frac{1}{1+a_k(x)}\right)}$$

and so $a_k(y) = a_k(x)$. Therefore, we have that $\hat{h}(y) = h(x)$ and so, by part 2 of Theorem 3.1, $h(x)$ is the (distinct) superior highly composite polynomial immediately preceding $\hat{h}(x)$.

3. Let $h(x)$ be x-SSHC and $g \in \mathcal{M}_{\deg h(x)}$ be a highly composite polynomial. If $x \notin S$, then by part 1 of Theorem 3.2, $h(x) = \hat{h}(x)$, and by part 1 of Theorem 3.1, $\hat{h}(x)$ is the unique highly composite polynomial of its degree, so $g = \hat{h}(x) = h(x)$. Else, if $x \in S$, then by part 2 of Proposition 3.2, we have that $h \in E$ and

$$\frac{\tau(h)}{q^{\deg h/x}} \begin{cases} = \frac{\tau(f)}{q^{\deg f/x}} & \text{if } f \in E \\ > \frac{\tau(f)}{q^{\deg f/x}} & \text{if } f \notin E \end{cases}.$$

Therefore $\tau(g) = \tau(h)$ if, and only if, $g \in E$ which means that g is also x-SSHC.

□

Finally we conclude by proving the auxiliary lemmas used in the proof of Proposition 3.2, namely

Lemma 3.1. *Let $\alpha > 0$ and consider the sequence $(\phi_n)_{n\geqslant 0}$ defined by $\phi_n = \log(1+n) - \alpha n$. We have that*

1. *If* $\log(1+\frac{1}{j+1}) < \alpha < \log(1+\frac{1}{j})$ *for some integer* j*, then* ϕ_n *is maximised if and only if* $n = j = \left\lfloor \frac{1}{e^\alpha - 1} \right\rfloor$.

2. *Else, if* $\alpha = \log(1+\frac{1}{j})$ *for some integer* j*, then* ϕ_n *is maximised if and only if* $n = j$ *or* $j-1$.

Proof. Let $\Delta_n = \phi_n - \phi_{n-1} = \log(1+\frac{1}{n}) - \alpha$ for $n \geqslant 1$. Then we have that

1. If $\log(1+\frac{1}{j+1}) < \alpha < \log(1+\frac{1}{j})$, then $\Delta_n > 0$ when $n \leqslant j$, and $\Delta_n < 0$ when $n > j$.

2. Else, if $\alpha = \log(1+\frac{1}{j})$ then $\Delta_n > 0$ when $n < j$, $\Delta_j = 0$ and $\Delta_n < 0$ when $n > j$.

□

and

Lemma 3.2. *Let* $x \in S$*. Then there is a unique pair* (s, r) *such that* $x = \frac{s \log q}{\log(1+1/r)}$.

Proof. Suppose otherwise, so that $x = \frac{s \log q}{\log(1+1/r)} = \frac{S \log q}{\log(1+1/R)}$ with (r, s) and (R, S) distinct. If $s = S$ then $r = R$, so it must be that $s \neq S$ and in particular we may assume without loss of generality that $S > s$ so that $\frac{S}{s} > 1$.
Now $\frac{s \log q}{\log(1+1/r)} = \frac{S \log q}{\log(1+1/R)}$ implies $\left(1+\frac{1}{R}\right)^s = \left(1+\frac{1}{r}\right)^S$ and therefore $\frac{(R+1)^s}{R^s} = \frac{(r+1)^S}{r^S}$. However, $\frac{(R+1)^s}{R^s}$ and $\frac{(r+1)^S}{r^s}$ are irreducible fractions, so we must have that $R^s = r^S$ and $(R+1)^s = (r+1)^S$. So, $(1+r)^{S/s} = 1 + R = 1 + r^{S/s}$, but $(1+x)^\alpha > 1 + x^\alpha$ for $x > 0$ and $\alpha > 1$, which is a contradiction. □

3.4 The maximum value of the divisor function

Since the family of semi-superior highly composite polynomials is not too sparse, we can use it to construct polynomials at every degree which make the divisor function close to its maximum, and thus prove Theorem 3.3:

Proof of Theorem 3.3. If $u = 0$, then $N = \deg h$, and by Theorem 3.2, h is highly composite, so $T(N) = \tau(h)$. Otherwise, if $1 \leqslant u \leqslant s-1$, we have by Remark 3.3 that $a_u(x) \geqslant a_s(x) = r \geqslant 1$. So, if we pick $P \in \mathcal{I}_u$ and let $g = \frac{h}{P}$, then $g \in \mathcal{M}$ with $\deg g = \deg h - u = N$ and therefore

$$T(N) \geqslant \tau(g) = \tau(h)\frac{a_u}{1+a_u} = \frac{\tau(h)}{1+\frac{1}{a_u}}.$$

On the other hand, by Theorem 3.2, h is x-SSHC, and so for any $f \in \mathcal{M}_N$, we have

$$\tau(f) \leqslant \tau(h) q^{(\deg f - \deg h)/x} = \tau(h) q^{-u/x}$$

and therefore

$$T(N) \leqslant \tau(h) q^{-u/x} = \tau(h) \left(1 + \frac{1}{r}\right)^{\frac{-u}{s}}.$$

Overall, this gives us that

$$\log q^{u/x} = \frac{u}{s} \log\left(1 + \frac{1}{r}\right) \leqslant \log \tau(h) - \log T(N) \leqslant \log\left(1 + \frac{1}{a_u}\right). \tag{3.7}$$

Now, since

$$a_u = \left\lfloor \frac{1}{q^{u/x} - 1} \right\rfloor \geqslant \frac{1}{q^{u/x} - 1} - 1$$

we have that

$$q^{u/x} \geqslant 1 + \frac{1}{1 + a_u}$$

and so the size of the range in equation (3.7) is at most

$$\log\left(1 + \frac{1}{a_u}\right) - \log\left(1 + \frac{1}{1 + a_u}\right) = \log\left(1 + \frac{1}{a_u(a_u + 2)}\right) \leqslant \log \frac{4}{3}.$$

□

3.5 Table of highly composite polynomials in $\mathbb{F}_2[t]$

We conclude with a table of highly composite polynomials in $\mathbb{F}_2[t]$, in which SSHC polynomials are additionally marked with $*$ and SHC polynomials are additionally marked with $**$. We denote the monic irreducible polynomials in $\mathbb{F}_2[t]$ by $P_1(t), P_2(t), \cdots$ in ascending order of the value which they take on $t = 2$ (so that, if $\deg P_i > \deg P_j$, then $i > j$), and we write $f \in \mathcal{M}$ in the form $f = P_1^{a_1} P_2^{a_2} \cdots$ in order to shorten the printing. We have listed the explicit values of $P_1(t), \cdots, P_{14}(t)$, which are all of the irreducible polynomials which appear in the factorisations of polynomials in our table of highly composite polynomials, in their own table below, along with the values which they take on $t = 2$.

Table 3.1: Table of ordered monic irreducible polynomials in $\mathbb{F}_2[t]$

i	$P_i(t) \in \mathcal{I}$	$\deg P_i$	$P_i(2)$
1	t	1	2
2	$t+1$	1	3
3	t^2+t+1	2	7
4	t^3+t+1	3	11
5	t^3+t^2+1	3	13
6	t^4+t+1	4	19
7	t^4+t^3+1	4	25
8	$t^4+t^3+t^2+t+1$	4	31
9	t^5+t^2+1	5	37
10	t^5+t^3+1	5	41
11	$t^5+t^3+t^2+t+1$	5	47
12	$t^5+t^4+t^2+t+1$	5	55
13	$t^5+t^4+t^3+t+1$	5	59
14	$t^5+t^4+t^3+t^2+1$	5	61

The algorithm which we use to compute highly composite polynomials is an adaption of the algorithm used to compute highly composite numbers in [25]. Though we take $q = 2$, it works in the same way for any $\mathbb{F}_q[t]$, and we give a brief description as follows.

We first define the set $\mathcal{M}^{(k)} \subseteq \mathcal{M}$ of polynomials whose prime factors are in $\{P_1, \cdots, P_k\}$, and we call $f \in \mathcal{M}^{(k)}$ a *k-highly composite polynomial* if $\tau(f) = \max\{\tau(g) \mid g \in \mathcal{M}^{(k)} \text{ and } \deg g \leqslant \deg f\}$. Then we let $\mathrm{HC}(k,n) \subseteq \mathcal{M}^{(k)}$ be the set of k-highly composite polynomials of degree exactly n, and make the following observations:

- If $f = P_1^{a_1}P_2^{a_2}\cdots P_{k-1}^{a_{k-1}}P_k^{a_k} \in \mathrm{HC}(k,n)$, then $g = P_1^{a_1}P_2^{a_2}\cdots P_{k-1}^{a_{k-1}} \in \mathrm{HC}(k-1, n - a_k \deg P_k)$. Otherwise, if we had some $h \in \mathrm{HC}(k-1, n-a_k\deg P_k)$ with $\tau(h) > \tau(g)$ then we would have $\tau(hP_k^{a_k}) > \tau(f)$ even though $hP_k^{a_k} \in \mathcal{M}^{(k)}$ with $\deg hP_k^{a_k} = n$, which would be a contradiction.

- If $f \in \mathrm{HC}(k,n)$, and $P_i^{a_i}P_j^{a_j}$ divides f with $\deg P_j > \deg P_i$, then $a_i \geqslant a_j$. The proof of this is identical to that presented in Remark 3.3.

The first observation allows us to iteratively compute $\mathrm{HC}(k,n)$, as long as we know $\mathrm{HC}(k-1,m)$ for all $m \leqslant n$. In particular, for each $j \geqslant 0$ with $n - j \deg P_k \geqslant 0$, we pick any (one) $g_j \in \mathrm{HC}(k-1, n-j\deg P_k)$, and determine which values of j maximise $\tau(g_j P_k^j)$. Once we have determined such a set $J = \{j_1, \cdots, j_r\}$ we can conclude that

$$\mathrm{HC}(k,n) = \{f_j P_k^j : j \in J,\ f_j \in \mathrm{HC}(k-1, n-j\deg P_k)\}.$$

It is trivial to observe that the base case $\mathrm{HC}(1,n) = \{P_1^n\}$ for all $n \geqslant 0$, and we proceed inductively from there.

The second observation allows to note that, if $\{P_1, \cdots, P_k\} = \cup_{a \leqslant b} \mathcal{I}_a$ for some $b \geqslant 1$, and $\deg P_1 \cdots P_k \geqslant n$, then the set $\mathrm{HC}(k,n)$ is in fact the set of highly composite polynomials of degree n. Thus, once we have $\mathrm{HC}(k,n)$, by taking k sufficiently large, we are able to compute the highly composite polynomials of degree n.

Table 3.2: Table of highly composite polynomials in $\mathbb{F}_2[t]$

$f \in \mathcal{M}$	$\deg f$	$\tau(f)$
$^*P_1^1$	1	2
$^*P_2^1$	1	2
$^{**}P_1^1P_2^1$	2	4
$^*P_1^2P_2^1$	3	6
$^*P_1^1P_2^2$	3	6
$^{**}P_1^2P_2^2$	4	9
$P_1^3P_2^2$	5	12
$P_1^2P_2^3$	5	12
$P_1^2P_2^1P_3^1$	5	12
$P_1^1P_2^2P_3^1$	5	12
$^{**}P_1^2P_2^2P_3^1$	6	18
$^*P_1^3P_2^2P_3^1$	7	24
$^*P_1^2P_2^3P_3^1$	7	24

$^{**}P_1^3P_2^3P_3^1$	8	32
$P_1^4P_2^3P_3^1$	9	40
$P_1^3P_2^4P_3^1$	9	40
$P_1^4P_2^4P_3^1$	10	50
$^{*}P_1^3P_2^3P_3^1P_4^1$	11	64
$^{*}P_1^3P_2^3P_3^1P_5^1$	11	64
$P_1^4P_2^3P_3^1P_4^1$	12	80
$P_1^3P_2^4P_3^1P_4^1$	12	80
$P_1^4P_2^3P_3^1P_5^1$	12	80
$P_1^3P_2^4P_3^1P_5^1$	12	80
$P_1^4P_2^4P_3^1P_4^1$	13	100
$P_1^4P_2^4P_3^1P_5^1$	13	100
$^{**}P_1^3P_2^3P_3^1P_4^1P_5^1$	14	128
$^{*}P_1^4P_2^3P_3^1P_4^1P_5^1$	15	160
$^{*}P_1^3P_2^4P_3^1P_4^1P_5^1$	15	160
$^{**}P_1^4P_2^4P_3^1P_4^1P_5^1$	16	200
$P_1^5P_2^4P_3^1P_4^1P_5^1$	17	240
$P_1^4P_2^5P_3^1P_4^1P_5^1$	17	240
$P_1^4P_2^3P_3^2P_4^1P_5^1$	17	240
$P_1^3P_2^4P_3^2P_4^1P_5^1$	17	240
$^{**}P_1^4P_2^4P_3^2P_4^1P_5^1$	18	300
$^{*}P_1^5P_2^4P_3^2P_4^1P_5^1$	19	360
$^{*}P_1^4P_2^5P_3^2P_4^1P_5^1$	19	360
$^{**}P_1^5P_2^5P_3^2P_4^1P_5^1$	20	432
$P_1^6P_2^5P_3^2P_4^1P_5^1$	21	504
$P_1^5P_2^6P_3^2P_4^1P_5^1$	21	504
$P_1^4P_2^4P_3^2P_4^1P_5^1P_6^1$	22	600
$P_1^4P_2^4P_3^2P_4^1P_5^1P_7^1$	22	600
$P_1^4P_2^4P_3^2P_4^1P_5^1P_8^1$	22	600
$P_1^5P_2^4P_3^2P_4^1P_5^1P_6^1$	23	720
$P_1^4P_2^5P_3^2P_4^1P_5^1P_6^1$	23	720

$P_1^5P_2^4P_3^2P_4^1P_5^1P_7^1$	23	720
$P_1^4P_2^5P_3^2P_4^1P_5^1P_7^1$	23	720
$P_1^5P_2^4P_3^2P_4^1P_5^1P_8^1$	23	720
$P_1^4P_2^5P_3^2P_4^1P_5^1P_8^1$	23	720
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_6^1$	24	864
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_7^1$	24	864
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_8^1$	24	864
$P_1^6P_2^5P_3^2P_4^1P_5^1P_6^1$	25	1008
$P_1^5P_2^6P_3^2P_4^1P_5^1P_6^1$	25	1008
$P_1^6P_2^5P_3^2P_4^1P_5^1P_7^1$	25	1008
$P_1^5P_2^6P_3^2P_4^1P_5^1P_7^1$	25	1008
$P_1^6P_2^5P_3^2P_4^1P_5^1P_8^1$	25	1008
$P_1^5P_2^6P_3^2P_4^1P_5^1P_8^1$	25	1008
$P_1^4P_2^4P_3^2P_4^1P_5^1P_6^1P_7^1$	26	1200
$P_1^4P_2^4P_3^2P_4^1P_5^1P_6^1P_8^1$	26	1200
$P_1^4P_2^4P_3^2P_4^1P_5^1P_7^1P_8^1$	26	1200
$P_1^5P_2^4P_3^2P_4^1P_5^1P_6^1P_7^1$	27	1440
$P_1^4P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1$	27	1440
$P_1^5P_2^4P_3^2P_4^1P_5^1P_6^1P_8^1$	27	1440
$P_1^4P_2^5P_3^2P_4^1P_5^1P_6^1P_8^1$	27	1440
$P_1^5P_2^4P_3^2P_4^1P_5^1P_7^1P_8^1$	27	1440
$P_1^4P_2^5P_3^2P_4^1P_5^1P_7^1P_8^1$	27	1440
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1$	28	1728
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_6^1P_8^1$	28	1728
$^*P_1^5P_2^5P_3^2P_4^1P_5^1P_7^1P_8^1$	28	1728
$P_1^6P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1$	29	2016
$P_1^5P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1$	29	2016
$P_1^6P_2^5P_3^2P_4^1P_5^1P_6^1P_8^1$	29	2016
$P_1^5P_2^6P_3^2P_4^1P_5^1P_6^1P_8^1$	29	2016
$P_1^6P_2^5P_3^2P_4^1P_5^1P_7^1P_8^1$	29	2016
$P_1^5P_2^6P_3^2P_4^1P_5^1P_7^1P_8^1$	29	2016

$P_1^4P_2^4P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	30	2400
$P_1^5P_2^4P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	31	2880
$P_1^4P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	31	2880
$^{**}P_1^5P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	32	3456
$^{*}P_1^6P_2^5P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	33	4032
$^{*}P_1^5P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	33	4032
$^{**}P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	34	4704
$P_1^7P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	35	5376
$P_1^6P_2^7P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1$	35	5376
$P_1^6P_2^5P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	35	5376
$P_1^5P_2^6P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	35	5376
$^{**}P_1^6P_2^6P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	36	6272
$P_1^7P_2^6P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	37	7168
$P_1^6P_2^7P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	37	7168
$P_1^7P_2^7P_3^3P_4^1P_5^1P_6^1P_7^1P_8^1$	38	8192
$P_1^6P_2^6P_3^3P_4^2P_5^1P_6^1P_7^1P_8^1$	39	9408
$P_1^6P_2^6P_3^3P_4^1P_5^2P_6^1P_7^1P_8^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_9^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_{10}^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_{11}^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_{12}^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_{13}^1$	39	9408
$P_1^6P_2^6P_3^2P_4^1P_5^1P_6^1P_7^1P_8^1P_{14}^1$	39	9408

Remark 3.9. *In $\mathbb{F}_2[t]$, there are certain degrees at which there is a unique highly composite polynomial of that degree, but where that polynomial is neither SHC nor SSHC (see degrees 10, 30 and 38 in the table of highly composite polynomials, for example). We leave for further investigation the question of whether there are infinitely many degrees with this property.*

3.6 Ramanujan's upper bound for the divisor function

For the sake of completeness, we add an aside in which we derive an analogue of Ramanujan's explicit upper bound for the divisor function, as in [32]. Ramanujan uses his expression for superior highly composite numbers in equation (3.3), and the defining property of superior highly composite numbers in equation (3.2), to get a sharp upper bound for the divisor function of the form

$$\log d(n) \leqslant \sum_{n\geqslant 1} \pi\left(\left(\frac{n+1}{n}\right)^{x}\right)\log\left(\frac{n+1}{n}\right)$$

where $\pi(m) = \sum_{p\leqslant m \text{ prime}} 1$, and x is defined by

$$\sum_{n\geqslant 1} \theta\left(\left(\frac{n+1}{n}\right)^{y}\right)\begin{cases} < \log n & \text{if } y < x \\ > \log n & \text{if } y > x \end{cases}$$

where $\theta(m) = \sum_{p\leqslant m \text{ prime}} \log p$. Ramanujan's strategy is essentially identical to the one which we use below to get the analogous bound in Proposition 3.3. Finally, assuming the Riemann Hypothesis, he uses a version of Riemann's explicit formulae

$$\pi(x) = \mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(\sqrt{x}) - \sum_{\rho:\zeta(\rho)=0} \mathrm{Li}(x^{\rho}) + O(x^{\frac{1}{3}})$$
$$\text{and } \theta(x) = x - \sqrt{x} - \sum_{\rho:\zeta(\rho)=0} \frac{x^{\rho}}{\rho} + O(x^{\frac{1}{3}})$$

to derive the explicit sharp upper bound

$$\log d(n) \leqslant \mathrm{Li}(\log n)\log 2 + \mathrm{Li}\left((\log n)^{\log(\frac{3}{2})/\log 2}\right)\log\left(\frac{3}{2}\right) - \frac{(\log n)^{\log(\frac{3}{2})/\log 2}}{\log\log n}\log 2$$
$$- R(\log n)\log 2 + O\left(\frac{\sqrt{\log n}}{(\log\log n)^{3}}\right)$$

where $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$ and $R(x) = \frac{1}{(\log x)^2}\left(2\sqrt{x} + \sum_{\rho:\zeta(\rho)=0} \frac{x^{\rho}}{\rho^2}\right)$. We instead use the Prime Polynomial Theorem to get an analogous bound in Theorem 3.4.

We begin with a reformulation of our form for an x-SHC, which is the following corollary of Theorem 3.1:

Corollary 3.1. *If $\hat{h} = \hat{h}(x)$ is x-SHC, then we can write it as*

$$\hat{h} = \prod_{n \geqslant 1} \prod_{k \leqslant c_n(x)} \prod_{p \in \mathcal{I}_k} p$$

where $c_n(x) = x \log_q(1 + \frac{1}{n})$.

Proof. From equation (3.6), we know that we have

$$\hat{h}(x) = \prod_{k \geqslant 1} \prod_{p \in \mathcal{I}_k} p^{a_k} \quad \text{where} \quad a_k = a_k(x) = \left\lfloor \frac{1}{q^{k/x} - 1} \right\rfloor.$$

Now, let $\tilde{h}(x) = \prod_{n \geqslant 1} \prod_{k \leqslant c_n(x)} \prod_{p \in \mathcal{I}_k} p$ where $c_n(x) = x \log_q(1 + \frac{1}{n})$, so that

$$\tilde{h}(x) = \prod_{k \geqslant 1} \prod_{p \in \mathcal{I}_k} p^{b_k(x)}$$

where

$$b_k(x) = \#\{n : k \leqslant c_n(x)\} = \#\{n : k \leqslant x \log_q(1 + \tfrac{1}{n})\} = \left\lfloor \frac{1}{q^{k/x} - 1} \right\rfloor = a_k(x)$$

and therefore $\tilde{h}(x) = \hat{h}(x)$. □

Remark 3.10. *Notice that $\lfloor c_n(x) \rfloor$ is zero for n sufficiently large so that, as expected, this factorisation is in fact a finite product.*

Corollary 3.2. *If $\hat{h} = \hat{h}(x)$ is x-SHC then we have that $\deg \hat{h} = \sum_{n \geqslant 1} \sum_{1 \leqslant k \leqslant c_n(x)} k\pi(k)$ and $\tau(\hat{h}) = \prod_{n \geqslant 1}(1 + \frac{1}{n})^{\pi_1(c_n(x))}$, where $\pi(n) = |\mathcal{I}_n|$ and $\pi_1(n) = \sum_{r \leqslant n} \pi(r)$.*

Proof. Using Corollary 3.1, the degree of $\hat{h}$ follows easily, and moreover we have that

$$\tau(\hat{h}) = \prod_{k \geqslant 1} \prod_{p \in \mathcal{I}_k} (1 + a_k(x)) = \prod_{n \geqslant 1} (1 + n)^{d_n(x)}$$

where $d_n(x) = \sum_{k : a_k(x) = n} \pi(k)$. Now, in order to have $a_k(x) = n$, we must have

$$n \leqslant \frac{1}{q^{k/x} - 1} < n + 1$$

or equivalently that

$$c_n(x) = x \log_q \left(1 + \frac{1}{n}\right) \geqslant k > x \log_q \left(1 + \frac{1}{n+1}\right) = c_{n+1}(x).$$

Therefore we conclude that $d_n(x) = \pi_1(c_n(x)) - \pi_1(c_{n+1}(x))$ and so

$$\tau(\hat{h}) = \prod_{n\geqslant 1}(1+n)^{\pi_1(c_n(x))-\pi_1(c_{n+1}(x))} = \frac{\prod_{n\geqslant 1}(1+n)^{\pi_1(c_n(x))}}{\prod_{n\geqslant 2} n^{\pi_1(c_n(x))}} = \prod_{n\geqslant 1}(1+\tfrac{1}{n})^{\pi_1(c_n(x))}.$$

□

We can use x-SHC polynomials to get a sharp upper bound for the number of divisors of $g \in \mathcal{M}_N$, which is the analogue of Ramanujan's result in [32] and improves upon the elementary bound in Proposition 3.1, as follows:

Proposition 3.3. *For all $g \in \mathcal{M}_N$, we have*

$$\log_q \tau(g) \leqslant F_N(x_0(N))$$

where

$$F_N(x) := \frac{1}{x}\left(N + \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} \pi(k)\,(c_n(x)-k)\right)$$

and

$$x_0(N) := \inf\{x \,:\, \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} k\pi(k) \geqslant N\}.$$

Proof. From equation (3.4) and Corollary 3.2, we have for any $x > 0$ that

$$\tau(g) \leqslant q^{N/x}\frac{\tau(\hat{h}(x))}{q^{\deg \hat{h}(x)/x}} = q^{N/x}\prod_{n\geqslant 1}\left((1+\tfrac{1}{n})^{\pi_1(c_n(x))} q^{-\frac{1}{x}\sum_{1\leqslant k\leqslant c_n(x)} k\pi(k)}\right).$$

with equality when $g = \hat{h}(x)$ is x-SHC. After taking the logarithm we get

$$\begin{aligned}\log_q \tau(g) \leqslant F_N(x) &:= \frac{1}{x}\left(N + \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} \pi(k)\,(c_n(x)-k)\right)\\ &= \frac{1}{x}\left(N + \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} \pi(k)\int_k^{c_n(x)} dt\right)\\ &= \frac{1}{x}\left(N + \sum_{n\geqslant 1}\int_1^{c_n(x)} \pi_1(t)dt\right).\end{aligned}$$

It is clear that $F_N(x)$ is continuous. It is also differentiable apart from at points x for which $c_n(x)$ is an integer for some n. Away from those points we have

$$\begin{aligned}F'_N(x) &= -\frac{1}{x^2}\left(N + \sum_{n\geqslant 1}\int_1^{c_n(x)} \pi_1(t)dt\right) + \frac{1}{x}\sum_{n\geqslant 1}\log_q(1+\tfrac{1}{n})\pi_1(c_n(x)) \\ &= -\frac{1}{x^2}\left(N + \sum_{n\geqslant 1}\left(\int_1^{c_n(x)} \pi_1(t)dt - c_n(x)\pi_1(c_n(x))\right)\right) \\ &= -\frac{1}{x^2}\left(N - \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} k\pi(k)\right).\end{aligned}$$

Now, $F'_N(x)$ is negative for small x and positive for large x, changing sign exactly once. It follows that the best upper bound for $F_N(x)$ is attained by the unique $x_0(N)$ defined by $x_0(N) := \inf\{x : \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} k\pi(k) \geqslant N\}$, since by definition, for all $x < x_0(N)$, we have $F'_N(x) > 0$. □

Unfortunately, it seems difficult to give a precise value for $x_0(N)$ which is of a nice form. However, we can show that $x_0(N) = \frac{\log N}{\log 2} + O_q(1)$ thus

Lemma 3.3. *Let $\alpha(x,N) = N - \sum_{n\geqslant 1}\sum_{1\leqslant k\leqslant c_n(x)} k\pi(k)$. Then*

1. $x \geqslant \frac{\log N}{\log 2} + \frac{\log q}{\log 2} \implies \alpha(x,N) < 0.$

2. $x \leqslant \frac{\log N}{\log 2} - \left(\log_2\left(1+\frac{1}{q-1}\right) + \log_2\left(1+\frac{\log_q N}{\log 2}(\frac{3}{4})^{\log_q N}\right)\right) \implies \alpha(x,N) > 0.$

Proof. We deal with each part of the lemma in turn:

1. When $x \geqslant \frac{\log N}{\log 2} + \frac{\log q}{\log 2}$ we have that $c_1(x) = x\log_q 2 \geqslant \log_q N + 1$, and so

$$\begin{aligned}\alpha(x,N) < N - \sum_{1\leqslant k\leqslant c_1(x)} k\pi(k) < N - \sum_{k\mid\lfloor c_1(x)\rfloor} k\pi(k) \\ = N - q^{\lfloor c_1(x)\rfloor} < N - q^{\log_q N} = 0\end{aligned}$$

2. When $x \leqslant \frac{\log N}{\log 2} - \left(\log_2\left(1+\frac{1}{q-1}\right) + \log_2\left(1+\frac{\log_q N}{\log 2}(\frac{3}{4})^{\log_q N}\right)\right)$, we have

$$\begin{aligned}\alpha(N) &= N - \sum_{n \leqslant \frac{1}{q^{1/x}-1}} \sum_{1 \leqslant k \leqslant c_n(x)} k\pi(k) \\ &> N - \sum_{n \leqslant \frac{x}{\log q}} \sum_{1 \leqslant k \leqslant c_n(x)} q^k \\ &> N - \left(1 + \frac{1}{q-1}\right) \sum_{n \leqslant \frac{x}{\log q}} q^{c_n(x)} \\ &> N - \left(1 + \frac{1}{q-1}\right) 2^x \left(1 + \tfrac{x}{\log q}(\tfrac{3}{4})^x\right) \\ &> N - 2^x \left(1 + \frac{1}{q-1}\right)\left(1 + \tfrac{\log_q N}{\log 2}(\tfrac{3}{4})^{\log_q N}\right) > 0\end{aligned}$$

□

Now that we know a range for $x_0(N)$, we can take a value of $x = x(N)$ in this range to obtain a good upper bound which has a nice expression, giving us the following:

Theorem 3.4. *For all $g \in \mathcal{M}_N$, we have*

$$\log_q \tau(g) \leqslant \frac{\log 2}{\log q} \frac{N}{\lfloor \frac{\log N}{\log q} \rfloor} + \frac{q}{q-1} \frac{\log 2}{\log q} \int_1^{\lfloor \frac{\log N}{\log q} \rfloor} \frac{q^{\lfloor t \rfloor}}{t^2} dt + \sum_{1 \leqslant k \leqslant \lfloor \frac{\log N}{\log q} \rfloor \frac{\log(3/2)}{\log 2}} \frac{q^k}{k} + O(\sqrt{N})$$

Proof. Using that $\pi(k) = \frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\right)$, we have from Proposition 3.3 that for $x \leqslant \log_2 N$

$$\begin{aligned}\log_q \tau(g) &\leqslant F_N(x) \\ &= \frac{N}{x} + \sum_{n \geqslant 1} \log_q(1 + \tfrac{1}{n}) \sum_{1 \leqslant k \leqslant x \log_q(1+\frac{1}{n})} q^k \left(\frac{1}{k} - \frac{1}{x \log_q(1+\frac{1}{n})}\right) + O(\sqrt{N}) \\ &= \frac{N}{x} + \sum_{n \geqslant 1} \log_q(1 + \tfrac{1}{n}) \int_1^{x \log_q(1+\frac{1}{n})} \sum_{1 \leqslant k \leqslant t} q^k \frac{dt}{t^2} + O(\sqrt{N}).\end{aligned}$$

Now, if in particular we take $x = \frac{\log q}{\log 2}\lfloor \frac{\log N}{\log q}\rfloor$ then we get

$$\begin{aligned}\log_q \tau(g) &\leqslant \frac{\log 2}{\log q}\frac{N}{\lfloor \frac{\log N}{\log q}\rfloor} + \sum_{n\geqslant 1}\frac{\log(1+\frac{1}{n})}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor \frac{\log(1+1/n)}{\log 2}} \frac{q}{q-1}q^{\lfloor t\rfloor} + O(1)\frac{dt}{t^2} + O(\sqrt{N})\\
&= \frac{\log 2}{\log q}\frac{N}{\lfloor \frac{\log N}{\log q}\rfloor} + \frac{q}{q-1}\frac{\log 2}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor} \frac{q^{\lfloor t\rfloor}}{t^2}dt + \frac{q}{q-1}\frac{\log\frac{3}{2}}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor \frac{\log(3/2)}{\log 2}} \frac{q^{\lfloor t\rfloor}}{t^2}dt\\
&+ \sum_{n\geqslant 3}\frac{q}{q-1}\frac{\log(1+\frac{1}{n})}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor \frac{\log(1+1/n)}{\log 2}} \frac{q^{\lfloor t\rfloor}}{t^2}dt + O(\sqrt{N})\\
&= \frac{\log 2}{\log q}\frac{N}{\lfloor \frac{\log N}{\log q}\rfloor} + \frac{q}{q-1}\frac{\log 2}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor} \frac{q^{\lfloor t\rfloor}}{t^2}dt + \frac{q}{q-1}\frac{\log\frac{3}{2}}{\log q}\int_1^{\lfloor \frac{\log N}{\log q}\rfloor \frac{\log(3/2)}{\log 2}} \frac{q^{\lfloor t\rfloor}}{t^2}dt\\
&+ O(\sqrt{N})\end{aligned}$$

In going from the first equality to the second we use summation by parts on the inner sum. In going to the final line we note that, in the sum with terms $n \geqslant 3$, only the terms with $n \leqslant \frac{\log N}{\log 2 \log q}$ are non-zero, and for each such n, the integral is $O(N^{\log_2 4/3}) = O(N^{0.42})$, meaning that this sum is absorbed into the $O(\sqrt{N})$ error term. □

Remark 3.11. *The main term here is* $\frac{N\log 2}{\log N} + O(\frac{N}{\log^2 N})$*, and the subsequent terms are of size* $O(\frac{N}{\log^2 N})$ *and* $O(\frac{N^{\log_2(3/2)}}{\log^2 N})$ *respectively. This upper bound is attained (up to the error term* $O(\sqrt{N})$*) when* g *is* x*-SHC. The lower order main terms can be determined explicitly from this calculation. In particular, each integral is closely related to the logarithmic integral and, for* $N > q$ *we have*

$$\frac{1}{\lfloor \frac{\log N}{\log q}\rfloor} = \frac{\log q}{\log N}\left(\frac{1}{1-\frac{\log q}{\log N}\{\frac{\log N}{\log q}\}}\right) = \frac{\log q}{\log N}\sum_{j\geqslant 0}\left(\frac{\log q}{\log N}\left\{\frac{\log N}{\log q}\right\}\right)^j.$$

Of course, using the full formula for $\pi(k)$ *and keeping track of more terms in the sum from the expression for* $F(x)$ *would give an even more precise upper bound.*

Chapter 4

The Generalised Divisor Problem and the Lindelöf Hypothesis

We observe a connection between the Generalised Divisor Problem and the Lindelöf Hypothesis, using Perron's formula, summation by parts and a tensor-power trick. In particular, we show how to quantitatively convert upper bounds from one problem to upper bounds for the other.

4.1 Introduction

For positive integers k and n, let $d_k(n)$ be the the *k-fold divisor function* of n, which counts the number of ways that n can be written as the product of exactly k factors. This *generalised divisor function* is related to the Riemann Zeta Function $\zeta(s)$ by

$$\zeta^k(s) = \sum_{n\geqslant 1} \frac{d_k(n)}{n^s}$$

where $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. It can be shown (see, for example, Chapter 12 of [40]), following Dirichlet in the case of $k = 2$, that

$$D_k(x) := \sum_{n\leqslant x} d_k(n) = xP_{k-1}(\log x) + \Delta_k(x)$$

where $P_{k-1}(y)$ is a polynomial of degree $k-1$, and $\Delta_k(x) = O_\epsilon(x^{1-1/k+\epsilon})$. For $k \geqslant 1$, we let

$$\alpha_k := \min\{\alpha \mid \forall\epsilon > 0\ \Delta_k(x) = O_\epsilon(x^{\alpha+\epsilon})\}$$

and we call the α_k *generalised divisor exponents*. The *Generalised Divisor Problem* is the problem of finding the values of these generalised divisor exponents, and the conjectured answer to this problem is

Conjecture 4.1 (The Generalised Divisor Problem). *For $k \geqslant 1$, $\alpha_k = \frac{1}{2} - \frac{1}{2k}$.*

A related problem is that of determining the maximal value of $\zeta(s)$ in the critical strip, where $0 \leqslant \mathrm{Re}(s) \leqslant 1$. For $0 \leqslant \sigma \leqslant 1$, we define

$$\mu(\sigma) = \min\{\mu \mid \forall \epsilon > 0 \ |\zeta(\sigma + it)| = O_\epsilon(t^{\mu+\epsilon})\}.$$

We are particularly interested in the value of $\mu(\frac{1}{2})$, which we call the *Lindelöf exponent*. The best known upper bound is $\mu(\frac{1}{2}) \leqslant \frac{13}{84}$ due to Bourgain (see [6]), and the conjecture states that

Conjecture 4.2 (The Lindelöf Hypothesis). $\mu(\frac{1}{2}) = 0$.

Remark 4.1. *Let $N(\sigma, T)$ denote the number of zeros of $\zeta(s)$ with real part at least σ and imaginary part at most T. It follows from Theorem 9.14 of [40] that*

$$N\left(\frac{1}{2}, T+1\right) - N\left(\frac{1}{2}, T\right) \gg \log T.$$

The Lindelöf Hypothesis is equivalent to the statement that,

$$N(\sigma, T+1) - N(\sigma, T) = o(\log T)$$

for any $\sigma > \frac{1}{2}$ (see Theorem 13.5 of [40]), or in other words, that almost all zeros of $\zeta(s)$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

In this note, we demonstrate how to use upper bounds for the generalised divisor exponents α_k to determine an upper bound for the Lindelöf exponent $\mu(\frac{1}{2})$, and vice-versa. In the case of the former, we use analytic continuation by summation by parts to show that

Theorem 4.1. *For $k \geqslant 1$,* $\mu(\frac{1}{2}) \leqslant \begin{cases} \frac{1}{2k}\frac{1}{1-\alpha_k} & \textit{if } \alpha_k \leqslant \frac{1}{2} \\ \frac{1}{2\alpha_k}\left(\alpha_k - \frac{1}{2} + \frac{1}{k}\right) & \textit{if } \alpha_k \geqslant \frac{1}{2} \end{cases}.$

and in the case of the latter, we use Perron's formula to show that

Theorem 4.2. *For $k \geqslant 2$, $\alpha_k \leqslant \frac{1}{2} + \frac{(k-2)\mu(\frac{1}{2})}{2(1+(k-2)\mu(\frac{1}{2}))}$.*

4.2 Proofs of Theorems 4.1 and 4.2

We begin with by proving an explicit form of the well-known subconvexity estimate for $\mu(\frac{1}{2})$, which we will use in our proof of Theorem 4.1.

Lemma 4.1 (Subconvexity of $\mu(\sigma)$)**.** *For $0 \leqslant \sigma \leqslant 1$, we have*

$$\mu\left(\frac{1}{2}\right) \leqslant \begin{cases} \frac{1}{2}\frac{\mu(\sigma)}{1-\sigma} & \text{if } \sigma \leqslant \frac{1}{2} \\ \frac{1}{2\sigma}\left(\sigma - \frac{1}{2} + \mu(\sigma)\right) & \text{if } \sigma \geqslant \frac{1}{2} \end{cases}$$

Proof. Since $\zeta(s)$ converges absolutely for $\mathrm{Re}(s) > 1$, then by the continuity of $\zeta(s)$ we have that $\mu(1) = 0$. Moreover, by the functional equation

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

it follows that $\mu(0) = \frac{1}{2}$. Now, by applying the Phragmén-Lindelöf principle to $\zeta(s)$, we can get an upper bound for the value of $\mu(\frac{1}{2})$ by linearly interpolating between $\mu(\sigma)$ and $\mu(1) = 0$ if $\sigma \leqslant \frac{1}{2}$, or between $\mu(\sigma)$ and $\mu(0) = \frac{1}{2}$ if $\sigma \geqslant \frac{1}{2}$. Following this procedure gives the stated result. □

Remark 4.2. *Observe the following:*

1. *By the functional equation for $\zeta(s)$, we have $\mu(\sigma) = \frac{1}{2} - \sigma + \mu(1-\sigma)$, so the inequalities in Lemma 4.1 are in fact equivalent.*

2. *By interpolating between $\mu(\frac{1}{2})$ and $\mu(1)$, we can show similarly that $\mu(\sigma) \leqslant 2\mu(\frac{1}{2})(1-\sigma)$ for $\frac{1}{2} \leqslant \sigma \leqslant 1$.*

3. *In particular, if the Lindelöf hypothesis is true, we can deduce from the previous points that $\mu(\sigma) = 0$ for all $\sigma \geqslant \frac{1}{2}$ and $\mu(\sigma) = \frac{1}{2} - \sigma$ for all $\sigma \leqslant \frac{1}{2}$.*

Next, we use analytic continuation by summation by parts, the the subconvexity of $\mu(\sigma)$, and a tensor-power trick to get an upper bound for $\mu(\frac{1}{2})$ depending on α_k.

Proof of Theorem 4.1. Using summation by parts we have, for $\mathrm{Re}(s) > 1$, that

$$\sum_{n \leqslant X} \frac{d_k(n)}{n^s} = \frac{D_k(X)}{X^s} + s\int_1^X \frac{P_{k-1}(\log x)}{x^s} + \frac{\Delta(x)}{x^{s+1}} dx$$

and we can take $X \to \infty$ to get

$$\zeta^k(s) = s\int_1^\infty \frac{P_{k-1}(\log x)}{x^s} + \frac{\Delta(x)}{x^{s+1}} dx.$$

By using integration by parts we note that

$$\int_1^\infty \frac{\log^m(x)}{x^s} dx = \left[\frac{\log^m(x)}{(s-1)x^{s-1}}\right]_\infty^1 + \frac{m}{s-1}\int_1^\infty \frac{\log^{m-1}(x)}{x^s} dx = \frac{m}{s-1}\int_1^\infty \frac{\log^{m-1}(x)}{x^s} dx$$

and so we obtain

$$\zeta^k(s) = sQ_k\left(\frac{1}{s-1}\right) + s\int_1^\infty \frac{\Delta(x)}{x^{s+1}} dx$$

where $Q_k(y)$ is a polynomial of degree k. Since $\Delta_k(x) = O_\epsilon(x^{\alpha_k+\epsilon})$ for all $\epsilon > 0$, the integral converges absolutely for $\mathrm{Re}(s) > \alpha_k$ and therefore, if $s = \sigma + it$ with $\alpha_k < \sigma \leqslant 1$ and $t \geqslant 2$, we have

$$|\zeta(s)| \ll |s|^{\frac{1}{k}} \ll |t|^{\frac{1}{k}}.$$

This means that $\mu(\sigma) < \frac{1}{k}$ and so $\mu(\alpha_k) \leqslant \frac{1}{k}$ by the continuity of $\zeta(s)$. The result now follows by applying Lemma 4.1. □

Moreover, this argument shows that something weaker than the Generalised Divisor Problem implies the Lindelöf Hypothesis:

Corollary 4.1. *If there is a sequence of $k \to \infty$ such that $\alpha_k \leqslant \frac{1}{2} + o_{k\to\infty}(1)$, then $\mu(\frac{1}{2}) = 0$.*

Finally, we use Perron's formula to get an upper bound for α_k depending on $\mu(\frac{1}{2})$.

Proof of Theorem 4.2. Using the truncated version of Perron's formula, we have that

$$D_k(x) = \frac{1}{2\pi i}\int_{1+\epsilon-iT}^{1+\epsilon+iT} \zeta^k(s)\frac{x^s}{s} ds + O_\epsilon\left(\frac{x^{1+\epsilon}}{T}\right)$$

Using Cauchy's Residue Formula for the rectangular contour with points at $\frac{1}{2} \pm iT, 1+\epsilon \pm iT$

we get

$$D_k(x) = \operatorname{res}_{s=1}\left(\zeta^k(s)\frac{x^s}{s}\right)+\frac{1}{2\pi i}\left(\int_{1+\epsilon-iT}^{1/2-iT}+\int_{1/2-iT}^{1/2+iT}+\int_{1/2+iT}^{1+\epsilon+iT}\right)\zeta^k(s)\frac{x^s}{s}ds+O_\epsilon\left(\frac{x^{1+\epsilon}}{T}\right)$$

First note that $\operatorname{res}_{s=1}\left(\zeta^k(s)\frac{x^s}{s}\right) = xP_{k-1}(\log x) = D_k(x) - \Delta_k(x)$. Now, let $s = \sigma + it$, and recall that by Remark 4.2 we have $|\zeta(s)| \ll_\delta t^{2\mu(\frac{1}{2})(1-\sigma)+\delta}$ for $\frac{1}{2} \leqslant \sigma \leqslant 1$. Moreover, when $\sigma > 1$, $\zeta(s)$ converges absolutely, and so $|\zeta(s)| \ll 1$. Therefore, we have

$$\begin{aligned}\left|\int_{1/2\pm iT}^{1+\epsilon\pm iT}\zeta^k(s)\frac{x^s}{s}ds\right| &\ll_\delta \frac{T^{k(2\mu(\frac{1}{2})+\delta)}}{T}\int_{1/2}^{1}\left(\frac{x}{T^{2k\mu(\frac{1}{2})}}\right)^\sigma d\sigma+\frac{1}{T}\int_1^{1+\epsilon}x^\sigma d\sigma\\ &\ll_\delta \frac{x}{T}T^{k\delta}+\frac{x^{\frac{1}{2}}}{T}T^{k(\mu(\frac{1}{2})+\delta)}+\frac{x^{1+\epsilon}}{T}\end{aligned}$$

Moreover, as a corollary of Ingham's asymptotic formula for the second moment of $\zeta(\frac{1}{2}+it)$ (see [22]), we know that $\int_{-T}^{T}|\zeta(\frac{1}{2}+it)|^2dt \ll_\delta T^{1+2\delta}$, and so

$$\left|\int_{1/2-iT}^{1/2+iT}\zeta^k(s)\frac{x^s}{s}ds\right| \ll x^{\frac{1}{2}}T^{(k-2)(\mu(\frac{1}{2})+\delta)-1}\int_{-T}^{T}\left|\zeta\left(\frac{1}{2}+it\right)\right|^2dt \ll_\delta x^{\frac{1}{2}}T^{(k-2)\mu(\frac{1}{2})+k\delta}$$

Therefore, putting everything together and noting that $\mu(\frac{1}{2}) \leqslant \frac{1}{4} < \frac{1}{2}$ by Lemma 4.1, we have

$$\begin{aligned}\Delta_k(x) &\ll_{\delta,\epsilon} \frac{x}{T}\left(T^{k\delta}+x^\epsilon\right)+x^{\frac{1}{2}}\left(T^{k(\mu(\frac{1}{2})+\delta)-1}+T^{(k-2)\mu(\frac{1}{2})+k\delta}\right)\\ &\ll \frac{x}{T}\left(T^{k\delta}+x^\epsilon\right)+x^{\frac{1}{2}}T^{(k-2)\mu(\frac{1}{2})+k\delta}\end{aligned}$$

and then we optimise the error terms (up to ϵ and δ) by taking $T = x^{\frac{1}{2(1+(k-2)\mu(\frac{1}{2}))}}$ to get

$$\Delta_k(x) \ll_{\delta,\epsilon} x^{\frac{1}{2}+\frac{(k-2)\mu(\frac{1}{2})}{2(1+(k-2)\mu(\frac{1}{2}))}}\left(x^\epsilon+x^{\frac{k\delta}{2(1+(k-2)\mu(\frac{1}{2}))}}\right).$$

The result now follows from the definition of α_k. □

Moreover, this argument leads to a converse of Corollary 4.1, namely that the Lindelöf Hypothesis implies something slightly weaker than the Generalised Divisor Problem:

Corollary 4.2. *If $\mu(\frac{1}{2}) = 0$, then $\alpha_k \leqslant \frac{1}{2}$ for all $k \geqslant 2$.*

Remark 4.3. *Corollaries 4.1 and 4.2 are well known: see Theorem 13.4 of [40].*

Chapter 5

Halász's Theorem in $\mathbb{F}_q[t]$

In the setting of the integers, Granville, Harper and Soundararajan showed that the upper bound in Halász's Theorem can be improved for smoothly supported functions. We derive the analogous result for Halász's Theorem in $\mathbb{F}_q[t]$, and then consider the converse question of when the general upper bound in this version of Halász's Theorem is actually attained.

5.1 Introduction

5.1.1 Halász's Theorem for the integers

Let $f : \mathbb{N} \to \mathbb{C}$ be a multiplicative function such that $f(1) = 1$, with associated Dirichlet Series and Euler Product (respectively)

$$\mathcal{F}(s) := \sum_{n \geqslant 1} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \sum_{k \geqslant 0} \frac{f(p^k)}{p^{ks}}$$

defined and absolutely convergent for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Then define the $\Lambda_f(n)$, the von Mangoldt function associated to f, by

$$-\frac{\mathcal{F}'}{\mathcal{F}}(s) =: \sum_{n \geqslant 2} \frac{\Lambda_f(n)}{n^s}$$

and consider the set of such functions f such that, for some $\kappa > 0$, we have $|\Lambda_f(n)| \leqslant \kappa \Lambda(n)$ for all $n \geqslant 1$ (where Λ is the usual von Mangoldt function), which we denote $\mathcal{C}(\kappa)$. In [15], Granville, Harper and Soundararajan generalise Halász's Theorem to this class of functions:

Theorem 5.1 (Halász's Theorem). *Let $\kappa > 0$ and $f \in \mathcal{C}(\kappa)$, and define $M = M(x)$ by*

$$e^{-M} (\log x)^\kappa := \max_{|t| \leqslant (\log x)^\kappa} \left| \frac{\mathcal{F}(1 + 1/\log x + it)}{1 + 1/\log x + it} \right| .$$

Then we have that

$$S(x) := \frac{1}{x}\sum_{n\leqslant x} f(n) \ll_\kappa (1+M)e^{-M}(\log x)^{\kappa-1} + \frac{(\log\log x)^\kappa}{\log x}.$$

Remark 5.1. *In the case of $f \in \mathcal{C}(1)$ the inequality in Theorem 5.1 becomes*

$$S(x) \ll (1+M)e^{-M} + \frac{(\log\log x)}{\log x}. \tag{5.1}$$

Now, for simplicity, consider the multiplicative functions f with $f(1) = 1$ and $|f(n)| \leqslant 1$ for all n, which form a subset of $\mathcal{C}(1)$. For this set, the same authors show that if f is supported only on primes of size $p \leqslant x^{1-\delta}$ for some $\delta > 0$, then we can improve equation (5.1) *to*

$$S(x) \ll_\delta e^{-M} + \frac{(\log\log x)}{\log x}. \tag{5.2}$$

This observation is presented in Remark 3.2 of [14], albeit with a different set of notation associated to this simplified setting.

Remark 5.2. *The upper bound in* (5.2) *does not hold for general multiplicative functions. It has been shown by a variety of authors (see [28], [29] and [16]), following the idea of Montgomery in [28], that there exists a multiplicative function f with $f(1) = 1$ and $|f(n)| \leqslant 1$ for all n, such that*

$$S(x) \gg (1+M)e^{-M} + \frac{(\log\log x)}{\log x}. \tag{5.3}$$

5.1.2 Halász's Theorem in $\mathbb{F}_q[t]$

We work in the setting of polynomials over a finite field, and set up the quantities analogous to those in the setting of the integers by following the notation in [13]. Let $\mathbb{F}_q$ be a finite field, $\mathcal{M} = \{F \in \mathbb{F}_q[t] \text{ monic}\}$ and $\mathcal{I} = \{P \in \mathcal{M} : P \text{ is irreducible}\}$. We define $f : \mathcal{M} \to \mathbb{C}$ to be a multiplicative function such that $f(1) = 1$, and let

$$\mathcal{F}(z) := \sum_{F\in\mathcal{M}} f(F)z^{\deg F} = \prod_{P\in\mathcal{I}}\sum_{k\geqslant 0} f(P^k)z^{k\deg P}$$

be the power series associated to f, along with its Euler Product. By taking the logarithmic derivative of the latter, and multiplying by z, we acquire a new power series through which we can define $\Lambda_f(F)$ (the von Mangoldt function associated to f):

$$\frac{z\mathcal{F}'}{\mathcal{F}}(z) =: \sum_{F\in\mathcal{M}} \Lambda_f(F) z^{\deg F}.$$

Then, we let $\mathcal{M}_n = \{F \in \mathcal{M} : \deg F = n\}$, and define

$$\sigma(n) = \sigma(n; f) := \frac{1}{q^n} \sum_{F\in\mathcal{M}_n} f(F)$$

to be the mean value of f over polynomials of degree n and

$$\chi(n) = \chi(n; f) := \frac{1}{q^n} \sum_{F\in\mathcal{M}_n} \Lambda_f(F)$$

to be the corresponding weighted average over prime powers.

As in the setting of the integers, we consider the set $\mathcal{C}(\kappa)$ of such f such that, for some $\kappa > 0$, we have $|\Lambda_f(F)| \leqslant \kappa\Lambda(F)$ for all $F \in \mathcal{M}$, where

$$\Lambda(f) = \begin{cases} \deg P & \text{if } F = P^k \\ 0 & \text{else} \end{cases}.$$

In particular, given the prime polynomial theorem in the form $\sum_{F\in\mathcal{M}_n} \Lambda_f(F) = q^n$, for $f \in \mathcal{C}(\kappa)$ we have that

$$|\chi(n)| \leqslant \frac{1}{q^n} \sum_{F\in\mathcal{M}_n} |\Lambda_f(F)| \leqslant \kappa$$

and so we consider the more general set $\tilde{\mathcal{C}}(\kappa)$ of f with $|\chi(j)| = |\chi(j; f)| \leqslant \kappa$ for all $j \geqslant 1$.

Finally, we define $f^{\perp} = f^{\perp,n}$ by setting

$$\Lambda_{f^{\perp}}(F) = \begin{cases} \Lambda_f(F) & \text{if } \deg F < n \\ 0 & \text{else} \end{cases}$$

and then we set $\mathcal{F}^{\perp}(z) := \sum_{F\in\mathcal{M}} f^{\perp}(F) z^{\deg F}$, $\sigma^{\perp}(j) := \frac{1}{q^j} \sum_{F\in\mathcal{M}_j} f^{\perp}(F)$ and $\chi^{\perp}(j) := \frac{1}{q^n} \sum_{F\in\mathcal{M}_j} \Lambda_{f^{\perp}}(F)$. We observe that $\chi^{\perp}(j) = \chi(j)$ if $j < n$ and $\chi^{\perp}(j) = 0$ otherwise, and from equation (1.8) of [13] we have

$$j\sigma(j) = \sum_{k=1}^{j} \chi(k)\sigma(j-k) \tag{5.4}$$

from which we conclude that $\sigma^{\perp}(j) = \sigma(j)$ if $j < n$ and $\sigma^{\perp}(n) = \sigma(n) - \frac{\chi(n)}{n}$.

We also note that, from their definitions and our observations above, we have

$$\mathcal{F}\left(\frac{z}{q}\right) = \sum_{j\geqslant 0} \sigma(j) z^j = \exp\left(\sum_{j\geqslant 1} \frac{\chi(j)}{j} z^j\right) \tag{5.5}$$

and

$$\mathcal{F}^{\perp}\left(\frac{z}{q}\right) = \sum_{j\geqslant 0} \sigma^{\perp}(j) z^j = \exp\left(\sum_{j\geqslant 1} \frac{\chi^{\perp}(j)}{j} z^j\right) = \exp\left(\sum_{j=1}^{n-1} \frac{\chi(j)}{j} z^j\right). \tag{5.6}$$

With these definitions in place, we are able to formulate the analogue of Halász's Theorem in $\mathbb{F}_q[t]$, which Granville, Harper and Soundararajan prove in [13]:

Theorem 5.2 (Halász's Theorem in $\mathbb{F}_q[t]$)**.** *Let $\kappa > 0$ and $f \in \tilde{\mathcal{C}}(\kappa)$, and define $M = M(n)$ by*

$$e^{-M}(2n)^{\kappa} := \max_{|z|=\frac{1}{q}} |\mathcal{F}^{\perp}(z)|.$$

Then we have that

$$|\sigma(n)| \leqslant 2\kappa(\kappa + 1 + M)e^{-M}(2n)^{\kappa-1}. \tag{5.7}$$

We consider the case analogous to that discussed in Remark 5.1, and show that Halász's Theorem can be improved when f has a property related to being smoothly supported:

Theorem 5.3. *Let $\kappa > 0$ and $f \in \tilde{\mathcal{C}}(\kappa)$, and define $M = M(n)$ as in Theorem 5.2. Suppose in addition that, for some $\delta > 0$, we have that $\chi(j) = \chi(j; f) = 0$ for all $j > (1-\delta)(n-1)$. Then we get that*

$$\begin{aligned} |\sigma(n)| &\leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1 - \log\left(1 - e^{-\frac{\delta}{2\sqrt{1-\delta}}}\right) + \frac{1}{\kappa}\left(1 - \frac{e^{M/\kappa}}{2n}\right)^{\delta(n-1)}\right) \\ &\ll_{\delta} \kappa^2 e^{-M}(2n)^{\kappa-1}. \end{aligned}$$

Remark 5.3. *In particular, note that if f is supported only on irreducibles of degree*

$\deg P \leqslant m$, then for $j > m$ we have

$$\chi(j) = \frac{1}{q^j} \sum_{F \in \mathcal{M}_j} \Lambda_f(F) = \frac{1}{q^j} \sum_{k \geqslant 1} \sum_{\substack{P \in \mathcal{I}_{\leqslant m} \\ P^k \in \mathcal{M}_j}} \Lambda_f(P^k) \ll \min(q^{-j/2}, q^{m-j}) \ll q^{-m/2}$$

and so, when $\delta > 0$ is small and $m = \lfloor (1-\delta)(n-1) \rfloor$, then $\chi(j)$ is close to zero.

Conversely, we derive a criterion for when the upper bound in equation (5.7) of Halász's Theorem is asymptotically attained:

Theorem 5.4. *Let $\kappa > 0$ and $f \in \tilde{\mathcal{C}}(\kappa)$, and define $M = M(n)$ as in Theorem 5.2. Then*

$$|\sigma(n)| \gg (1+M)e^{-M}(2n)^{\kappa-1}$$

if, and only if, for all $\delta \gg 1$ we have

$$\left| \sum_{(1-\delta)(n-1) < j \leqslant n} \chi(j)\sigma(n-j) \right| \gg (1+M)e^{-M}(2n)^{\kappa}.$$

Moreover, inspired by the idea in the setting of the integers (see [28]), we compute an example for which the criterion in Theorem 5.4 holds, in the case of $\kappa = 1$.

Current work in progress, and future work, is dedicated to using the criterion in Theorem 5.4 to effectively categorise the cases in which the upper bound in Halász's Theorem is asymptotically attained.

5.2 Proofs of Theorems 5.3 and 5.4

Let $\kappa > 0$, and let $f \in \tilde{\mathcal{C}}(\kappa)$. From equation (3.3) of [13] we have that

$$\sigma(n) - \frac{\chi(n)}{n} = \frac{1}{nq^n} \int_0^1 \frac{1}{2\pi i} \int_{|z| = \frac{1}{q\sqrt{t}}} \left(\sum_{j=1}^{n-1} \chi(j)(qz)^j \right) \left(\sum_{j=1}^{n-1} \chi(j)(qtz)^j \right) \mathcal{F}^{\perp}(tz) \frac{dz}{z^{n+1}} \frac{dt}{t}. \tag{5.8}$$

We define a new quantity

$$\sigma_m(n) := \frac{1}{nq^n} \int_0^1 \frac{1}{2\pi i} \int_{|z| = \frac{1}{q\sqrt{t}}} \left(\sum_{j=1}^{m} \chi(j)(qz)^j \right) \left(\sum_{j=1}^{n-1} \chi(j)(qtz)^j \right) \mathcal{F}^{\perp}(tz) \frac{dz}{z^{n+1}} \frac{dt}{t} \tag{5.9}$$

so that $\sigma_{n-1}(n) = \sigma(n) - \frac{\chi(n)}{n}$, and bound it following the strategy in [13].

Proposition 5.1. *Let $\kappa > 0$, $f \in \tilde{\mathcal{C}}(\kappa)$ and $M = M(n)$ as in Theorem 5.2. Then for $m < n-1$ we have*

$$\sigma_m(n) \leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1 - \log\left(1 - e^{-\frac{(n-1)-m}{2\sqrt{m(n-1)}}}\right) + \frac{1}{\kappa}\left(1 - \frac{e^{M/\kappa}}{2n}\right)^{(n-1)-m}\right)$$

Proof. First we use Cauchy-Schwarz on the inner integral in equation (5.9)

$$\left|\frac{1}{2\pi i}\int_{|z|=\frac{1}{q\sqrt{t}}}\left(\sum_{j=1}^{m}\chi(j)(qz)^j\right)\left(\sum_{j=1}^{n-1}\chi(j)(qtz)^j\right)\mathcal{F}^{\perp}(tz)\frac{dz}{z^{n+1}}\right|$$
$$\leqslant (q\sqrt{t})^n\left(\max_{|z|=\frac{1}{q\sqrt{t}}}|\mathcal{F}^{\perp}(tz)|\right)\sqrt{I_m\left(1, \frac{1}{q\sqrt{t}}\right)I_{n-1}\left(t, \frac{1}{q\sqrt{t}},\right)}$$

where, for $s \geqslant 0$, we have

$$I_a(s,R) := \frac{1}{2\pi}\int_{|z|=R}\left|\sum_{j=1}^{a}\chi(j)(qsz)^j\right|^2\frac{|dz|}{|z|} = \sum_{j=1}^{a}|\chi(j)|^2(qsR)^{2j} \leqslant \kappa^2\sum_{j=1}^{a}(qsR)^{2j}$$

by Parseval. Using this, we bound the inner integral by the quantity

$$\kappa^2(q\sqrt{t})^n\left(\max_{|z|=\frac{1}{q\sqrt{t}}}|\mathcal{F}^{\perp}(tz)|\right)\left(\sum_{j=1}^{m}t^{-j}\right)^{\frac{1}{2}}\left(\sum_{j=1}^{n-1}t^{j}\right)^{\frac{1}{2}}$$
$$= \kappa^2 q^n\left(\max_{|z|=\frac{\sqrt{t}}{q}}|\mathcal{F}^{\perp}(z)|\right)t^{\frac{n-m+1}{2}}\left(\frac{\sqrt{(1-t^m)(1-t^{n-1})}}{1-t}\right)$$

and then recall the bound from equation (3.6) of [13], which for $t \in (0,1)$, states that

$$\max_{|z|=\frac{\sqrt{t}}{q}}|\mathcal{F}^{\perp}(z)| \leqslant \min(e^{-M}(2n)^{\kappa}, (1-\sqrt{t})^{-\kappa})$$

where $e^{-M}(2n)^{\kappa} := \max_{|z|=\frac{1}{q}}|\mathcal{F}^{\perp}(z)|$.

Putting this all back into the full integral we get

$$\sigma_m(n) \leqslant \frac{\kappa^2}{n}\int_0^1 \min(e^{-M}(2n)^{\kappa}, (1-\sqrt{t})^{-\kappa})\, t^{\frac{(n-1)-m}{2}}\left(\frac{\sqrt{(1-t^m)(1-t^{n-1})}}{1-t}\right)dt$$

and after the substitution $t = (1-u)^2$ we have

$$\begin{aligned}
\sigma_m(n) &\leqslant \frac{\kappa^2}{n}\int_0^1 \min(e^{-M}(2n)^\kappa, u^{-\kappa})\ (1-u)^{(n-1)-m} \\
&\quad \times \min\left(\sqrt{m(n-1)}, \frac{1}{u(2-u)}\right) 2(1-u)\ du \\
&\leqslant \frac{\kappa^2}{n}\int_0^1 \min(e^{-M}(2n)^\kappa, u^{-\kappa})\ (1-u)^{(n-1)-m} \min\left(2\sqrt{m(n-1)}, \frac{1}{u}\right) du \\
&\leqslant \frac{\kappa^2}{n}\left(\int_0^{\frac{1}{2\sqrt{m(n-1)}}} 2\sqrt{m(n-1)}e^{-M}(2n)^\kappa du + \int_{\frac{1}{2\sqrt{m(n-1)}}}^{\frac{e^{M/\kappa}}{2n}} e^{-M}(2n)^\kappa (1-u)^{(n-1)-m}\frac{du}{u}\right. \\
&\quad \left. + \int_{\frac{e^{M/\kappa}}{2n}}^1 (1-u)^{(n-1)-m}\frac{du}{u^{\kappa+1}}\right). \\
&= \frac{\kappa^2}{n}\left(e^{-M}(2n)^\kappa + e^{-M}(2n)^\kappa \sum_{j=1}^{\lceil e^{M/\kappa}\frac{\sqrt{m(n-1)}}{n}-1\rceil} \int_{\frac{j}{2\sqrt{m(n-1)}}}^{\frac{j+1}{2\sqrt{m(n-1)}}} (1-u)^{(n-1)-m}\frac{du}{u}\right. \\
&\quad \left. + \left(1 - \frac{e^{M/\kappa}}{2n}\right)^{(n-1)-m} \int_{\frac{e^{M/\kappa}}{2n}}^1 \frac{du}{u^{\kappa+1}}\right).
\end{aligned}$$

When $m < n-1$ we get

$$\begin{aligned}
\sigma_m(n) &\leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1 + \sum_{j\geqslant 1}\left(1 - \frac{j}{2\sqrt{m(n-1)}}\right)^{(n-1)-m} \log\left(1+\frac{1}{j}\right)\right. \\
&\quad \left. + \frac{1}{\kappa}\left(1 - \frac{e^{M/\kappa}}{2n}\right)^{(n-1)-m}\right) \\
&\leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1 + \sum_{j\geqslant 1}\frac{e^{-\frac{j((n-1)-m)}{2\sqrt{m(n-1)}}}}{j} + \frac{1}{\kappa}\left(1 - \frac{e^{M/\kappa}}{2n}\right)^{(n-1)-m}\right) \\
&\leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1 - \log\left(1 - e^{-\frac{(n-1)-m}{2\sqrt{m(n-1)}}}\right) + \frac{1}{\kappa}\left(1 - \frac{e^{M/\kappa}}{2n}\right)^{(n-1)-m}\right).
\end{aligned}$$

□

Corollary 5.1. *Let* $\kappa > 0$, $f \in \tilde{\mathcal{C}}(\kappa)$ *and* $M = M(n)$ *as in Theorem 5.2. Then for* $\delta > 0$

and $m \leqslant (1-\delta)(n-1)$ *we have that*

$$\begin{aligned}\sigma_m(n) &\leqslant 2\kappa^2 e^{-M}(2n)^{\kappa-1}\left(1-\log\left(1-e^{-\frac{\delta}{2\sqrt{1-\delta}}}\right)+\frac{1}{\kappa}\left(1-\frac{e^{M/\kappa}}{2n}\right)^{\delta(n-1)}\right)\\ &\ll_\delta \kappa^2 e^{-M}(2n)^{\kappa-1}.\end{aligned}$$

Then we relate our quantity $\sigma_m(n)$ to $\sigma(n)$ with the following observation

Lemma 5.1.

$$\sigma(n) = \sigma_m(n) + \frac{1}{n}\sum_{j=m+1}^{n}\chi(j)\sigma(n-j).$$

Proof. From the definition of $\sigma_m(n)$ in equation (5.9), and our observation in equation (5.6) we have

$$\begin{aligned}\sigma_m(n) &= \frac{1}{nq^n}\int_0^1 \frac{1}{2\pi i}\int_{|z|=\frac{1}{q\sqrt{t}}}\left(\sum_{j=1}^{m}\chi(j)(qz)^j\right)\left(\sum_{k=1}^{n-1}\chi(k)(qtz)^k\right)\left(\sum_{l\geqslant 0}\sigma^{\perp}(l)(qtz)^l\right)\frac{dz}{z^{n+1}}\frac{dt}{t}\\ &= \frac{1}{nq^n}\int_0^1 \frac{1}{2\pi i}\int_{|z|=\frac{1}{q\sqrt{t}}}\left(\sum_{j=1}^{m}\chi(j)(qz)^j\right)\left(\sum_{k=1}^{n-1}\chi(k)(qtz)^k\right)\left(\sum_{l=0}^{n-1}\sigma^{\perp}(l)(qtz)^l\right)\frac{dz}{z^{n+1}}\frac{dt}{t}\\ &= \frac{1}{nq^n}\int_0^1 \frac{1}{2\pi i}\int_{|z|=\frac{1}{q\sqrt{t}}}\left(\sum_{j=1}^{m}\chi(j)(qz)^j\right)\left(\sum_{k=1}^{n-1}\chi(k)(qtz)^k\right)\left(\sum_{l=0}^{n-1}\sigma(l)(qtz)^l\right)\frac{dz}{z^{n+1}}\frac{dt}{t}\\ &= \frac{1}{nq^n}\int_0^1 \sum_{\substack{j+k+l=n\\ j\leqslant m}}\chi(j)\chi(k)\sigma(l)q^{j+k+l}t^{k+l}\frac{dt}{t}\\ &= \frac{1}{n}\sum_{\substack{j+k+l=n\\ j\leqslant m}}\frac{\chi(j)\chi(k)\sigma(l)}{k+l}\\ &= \frac{1}{n}\sum_{j=1}^{m}\chi(j)\frac{1}{n-j}\sum_{k=1}^{n-j}\chi(k)\sigma(n-j-k) = \frac{1}{n}\sum_{j=1}^{m}\chi(j)\sigma(n-j)\end{aligned}$$

where in the third equality we use the fact that $\sigma^{\perp}(j) = \sigma(j)$ for $j < n$, and in the final equality we use equation (5.4). Finally, using equation (5.4) once more we get that

$$\sigma(n) = \frac{1}{n}\sum_{j=1}^{n}\chi(j)\sigma(n-j) = \sigma_m(n) + \frac{1}{n}\sum_{j=m+1}^{n}\chi(j)\sigma(n-j).$$

□

This bring us to our proof of Theorem 5.3

Proof of Theorem 5.3. If $\chi(j) = 0$ for all $j > (1-\delta)(n-1)$, then by Lemma 5.1 we have that $\sigma(n) = \sigma_m(n)$ for $m = \lfloor (1-\delta)(n-1) \rfloor$, and so the result follows from Corollary 5.1. □

and our proof of Theorem 5.4

Proof of Theorem 5.4. For any $\delta \gg 1$, let $m = \lfloor (1-\delta)(n-1) \rfloor$, so that, by Lemma 5.1 we have that

$$\sigma(n) = \sigma_m(n) + \frac{1}{n} \sum_{j=m+1}^{n} \chi(j)\sigma(n-j) = \sigma_m(n) + \frac{1}{n} \sum_{(1-\delta)(n-1)<j\leqslant n} \chi(j)\sigma(n-j).$$

and from Corollary 5.1 we know that $\sigma_m(n) \ll \kappa^2 e^{-M}(2n)^{\kappa-1}$. Therefore,

$$|\sigma(n)| \gg (1+M)e^{-M}(2n)^{\kappa-1}$$

if, and only if,

$$\left| \sum_{(1-\delta)(n-1)<j\leqslant n} \chi(j)\sigma(n-j) \right| \gg (1+M)e^{-M}(2n)^{\kappa} \tag{5.10}$$

□

5.3 A sharp example

We conclude with an example for which the criterion in Theorem 5.4 holds, and thus which attains the upper bound in Halász's Theorem.

Remark 5.4. *First we observe that, if* $0 < \delta < \frac{1}{2} - \frac{1}{2n}$*, then the values taken by* $\sigma(n-j)$ *in equation* (5.10) *are independent of those taken by* $\chi(j)$*. So, we may for example take* $\chi(j) = e^{i(\theta - \phi_{n-j})}$ *where* $\sigma(j) =: |\sigma(j)|e^{i\phi_j}$ *(for some* $\theta \in [0, 2\pi)$*) for* $j > (1-\delta)(n-1)$ *and then in this case Theorem 5.4 becomes*

$$\sigma(n) \gg (1+M)e^{-M}(2n)^{\kappa-1} \Leftrightarrow \sum_{j<1+\delta(n-1)} |\sigma(j)| \gg (1+M)e^{-M}(2n)^{\kappa}.$$

For simplicity, we let $\kappa = 1$, and we use this observation to construct the following example:

Example 5.1. *For $0 < \delta < \frac{1}{2} - \frac{1}{2n}$, let*

$$\chi(j) = \begin{cases} i & \text{if } 1 \leqslant j < 1 + \delta(n-1) \\ 0 & \text{if } 1 + \delta(n-1) \leqslant j \leqslant (1-\delta)(n-1) \\ e^{-i\phi_{n-j}} & \text{if } j > (1-\delta)(n-1) \end{cases}$$

where $\sigma(j) =: |\sigma(j)|e^{i\phi_j}$. Then

$$\sum_{j<1+\delta(n-1)} |\sigma(j)| \gg (1+M)e^{-M}(2n)^{\kappa}$$

and therefore

$$\sigma(n) \gg (1+M)e^{-M}(2n)^{\kappa-1}.$$

Proof. In this case, we have from equation (5.6) that

$$\begin{aligned} \max_{|z|=\frac{1}{q}} \log|\mathcal{F}^{\perp}(z)| &= \max_{|z|=\frac{1}{q}} \operatorname{Re}\left(\sum_{j=1}^{n-1} \frac{\chi(j)}{j}(qz)^j\right) \\ &= \max_{\theta\in[0,2\pi)}\left(\sum_{1\leqslant j<1+\delta(n-1)} \frac{-\sin(j\theta)}{j} + \sum_{(1-\delta)(n-1)<j\leqslant n-1} \frac{\cos(j(\theta-\phi_{n-j}))}{j}\right). \end{aligned}$$

Now, we know that uniformly for θ and x,

$$\left|\sum_{j\leqslant x} \frac{\sin(j\theta)}{j}\right| \ll 1$$

and moreover we have that

$$\left|\sum_{(1-\delta)(n-1)<j\leqslant n-1} \frac{\cos(j(\theta-\phi_{n-j}))}{j}\right| \leqslant \sum_{(1-\delta)(n-1)<j\leqslant n-1} \frac{1}{j} \ll -\log(1-\delta) \ll 1.$$

Therefore, we have that $\max_{|z|=\frac{1}{q}} \log|\mathcal{F}^{\perp}(z)| \ll 1$, and conversely, by the maximum modulus principle, $\max_{|z|=\frac{1}{q}} |\mathcal{F}^{\perp}(z)| \geqslant |\mathcal{F}^{\perp}(0)| \gg 1$. This means that

$$e^{-M}(2n) := \max_{|z|=\frac{1}{q}} |\mathcal{F}^{\perp}(z)| \asymp 1$$

and

$$M = \log(2n) - \max_{|z|=\frac{1}{q}} \log|\mathcal{F}^{\perp}(z)| \sim \log(2n)$$

so that overall we get have that $(1+M)e^{-M}(2n) \asymp \log(2n)$.

On the other hand, by Cauchy's Theorem, we have for $j < 1 + \delta(n-1)$ and $R < 1$ that

$$\begin{aligned}
\sigma(j) &= \frac{1}{q^j}\frac{1}{2\pi i}\int_{|z|=\frac{R}{q}} \mathcal{F}(z)\frac{dz}{z^{j+1}} \\
\sigma(j) &= \frac{1}{2\pi i}\int_{|w|=R} \mathcal{F}\left(\frac{w}{q}\right)\frac{dw}{w^{j+1}} \\
&= \frac{1}{2\pi i}\int_{|w|=R} \exp\left(\sum_{k\geqslant 1}\frac{\chi(k)}{k}w^k\right)\frac{dw}{w^{j+1}} \\
&= \frac{1}{2\pi i}\int_{|w|=R} \exp\left(\sum_{k=1}^{j}\frac{\chi(k)}{k}w^k\right)\frac{dw}{w^{j+1}} \\
&= \frac{1}{2\pi i}\int_{|w|=R} \exp\left(i\sum_{k=1}^{j}\frac{w^k}{k}\right)\frac{dw}{w^{j+1}} \\
&= \frac{1}{2\pi i}\int_{|w|=R} \exp\left(i\sum_{k\geqslant 1}\frac{w^k}{k}\right)\frac{dw}{w^{j+1}} \\
&= \frac{1}{2\pi i}\int_{|w|=R} \frac{1}{(1-w)^i}\frac{dw}{w^{j+1}} \\
&= \binom{i+j-1}{j} \\
&\sim \frac{j^{i-1}}{\Gamma(i)}
\end{aligned}$$

where we use equation (5.6) in the third line, and the final line follows as in the proof of Corollary 2.1. From this we conclude that

$$\sum_{j<1+\delta(n-1)} |\sigma(j)| \asymp \sum_{j<1+\delta(n-1)} \frac{1}{j} \gg_{\delta} \log n \gg (1+M)e^{-M}(2n).$$

□

Chapter 6

A “Proto-Pellet’s Formula” for the Möbius Function

This chapter is based primarily on [2].

We give a short proof of “Pellet’s Formula” for the Möbius Function on $\mathbb{F}_q[t]$, deriving an intermediate formula (which we call “Proto-Pellet’s Formula”) along the way. We then construct and prove an analogous “Proto-Pellet’s Formula” for the Möbius Function for a number field (including the usual Möbius function on the integers).

6.1 Introduction

Let q be an odd prime power, and let $\mathcal{M} = \{f \in \mathbb{F}_q[t] : f \text{ monic}\}$. We define the Möbius Function for $f \in \mathcal{M}$, in analogy with the usual Möbius Function on the integers, by

$$\mu(f) = \begin{cases} (-1)^r & \text{if } f = p_1 \cdots p_r \text{ distinct primes} \\ 0 & \text{else} \end{cases}.$$

In $\mathcal{M}$ we have the following formula for μ

Theorem 6.1 (“Pellet’s Formula”)**.** *Let $f \in \mathcal{M}$, and let χ be the quadratic character on $\mathbb{F}_q$. Then we have that*

$$\mu(f) = (-1)^{\deg f} \chi(\mathrm{disc} f)$$

a proof of which can be found, for example, as Lemma 4.1 in [10]. This is an important ingredient in the setting of $\mathbb{F}_q[t]$, and has been used in computing the statistics of Möbius sums in $\mathbb{F}_q[t]$ (see [23]) and in work on Chowla’s conjecture in $\mathbb{F}_q[t]$ (see [8] and [36]).

We give another short proof of this formula, and in proving it, we derive an intermediate formula, which we call "Proto-Pellet's Formula". We believe that this proof, and the intermediate formula, are known (at least as folklore), but we were not able to find either stated explicitly in the literature. In order to present the formula, we let Frob_q be the Frobenius element on $\overline{\mathbb{F}}_q$, which sends α to α^q, and then we have

Theorem 6.2 ("Proto-Pellet's Formula"). *Let $f \in \mathcal{M}$ square free, then*

$$\mu(f) = (-1)^{\deg f}\mathrm{sign}(\mathrm{Frob}_q|f)$$

where $\mathrm{Frob}_q|f$ denotes the action of Frob_q on the roots of f.

We then construct and prove an analogue of this formula for the Möbius Function for any number field $A/\mathbb{Q}$, which we define as follows. Let $\mathcal{O}_A$ be the ring of integers in A, and let $\mathcal{I}_A$ be the set of non-zero ideals in $\mathcal{O}_A$. Then the Möbius Function for $A/\mathbb{Q}$, $\mu_A : \mathcal{I}_A \to \{-1, 0, 1\}$ is defined by

$$\mu_A(I) = \begin{cases} (-1)^r & \text{if } I = \mathfrak{p}_1 \cdots \mathfrak{p}_r \text{ distinct prime ideals} \\ 0 & \text{else} \end{cases}$$

so that $\mu_{\mathbb{Q}} = \mu$ is the usual Möbius function on the integers. To do this, we first pick some arbitrary additive function $\nu : \mathcal{I}_A \to \mathbb{N}$ to mimic the role of degree in $\mathbb{F}_q[t]$, and for each prime ideal $\mathfrak{p}$ we construct a polynomial $f_{\mathfrak{p},\nu}$ whose Galois group is isomorphic to $\mathbb{Z}/\nu(\mathfrak{p})\mathbb{Z}$ and generated by some homomorphism $\sigma_{\mathfrak{p},\nu}$. We then lift these homomorphisms to an appropriate profinite Galois group and compose them to get a homomorphism σ_ν (which mimics the role of Frob_q in $\mathbb{F}_q[t]$), and set $f_{I,\nu} = \prod_{\mathfrak{p}|I \text{ prime}} f_{\mathfrak{p},\nu}$ to prove

Theorem 6.3 ("Proto-Pellet's Formula" for number fields). *Let $\nu : \mathcal{I}_A \to \mathbb{N}$ be an additive function. Then there exists a Galois homomorphism $\sigma_\nu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and a family of polynomials $(f_{I,\nu})_{I \in \mathcal{I}_A}$ such that, for all $I \in \mathcal{I}_A$ square-free*

$$\mu_A(I) = (-1)^{\nu(I)}\mathrm{sign}(\sigma_\nu|f_{I,\nu})$$

where $\sigma_\nu|f$ denotes the action of σ_ν on the roots of f.

6.2 Pellet's Formula in $\mathbb{F}_q[t]$

We begin with a proof of Theorem 6.2:

Proof of Theorem 6.2. For a square-free polynomial $f = p_1 \cdots p_r \in \mathcal{M}$, Frob_q acts on the roots of f as a product of cycles $\tau_1, \cdots, \tau_r$, where τ_i permutes the roots of p_i as a cycle of length $\deg p_i$. Therefore $\text{sign}(\text{Frob}_q|f) = (-1)^{\deg p_1 - 1} \cdots (-1)^{\deg p_r - 1} = (-1)^{\deg f - r}$. □

To move from this to Pellet's formula, we first define

Definition 6.1. *For a polynomial f, let $\text{Aut}(f)$ be the automorphism group on the roots of f and let $\text{Gal}(f)$ be its Galois closure. Let $\text{Sym}(f)$ be the symmetric group, and $\text{Alt}(f)$ the alternating group, on the roots of f.*

and then prove an auxiliary result, which is a well known fact from Galois Theory (see for example Theorem 14.1 in [12]).

Proposition 6.1. *Let K be a field with $\text{char}K \neq 2$ and $f \in K[t]$ square-free, and let*

$$\rho_f : \text{Gal}(f) \hookrightarrow \text{Sym}(f)$$

be the natural inclusion map. Then $\rho_f(\text{Gal}f) \subseteq \text{Alt}(f) \iff \text{disc}f$ is a square in $K^\times$.

Proof. Let f have roots $\alpha_1, \cdots \alpha_n$ in $\overline{K}$ so that $\text{disc}f = \text{disc}_K f = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Then

$$\begin{aligned}
\text{disc}f \text{ is a square in } K^\times &\iff \forall \sigma \in \text{Gal}(f) \quad \sigma(\sqrt{\text{disc}f}) = \sqrt{\text{disc}f} \\
&\iff \forall \sigma \in \text{Gal}(f) \quad \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = \prod_{i<j}(\alpha_i - \alpha_j) \\
&\iff \forall \sigma \in \text{Gal}(f) \quad \prod_{i<j}(\alpha_i - \alpha_j) = \left(\prod_{i<j}\sigma(\alpha_i) - \sigma(\alpha_j)\right) \\
&\iff \forall \sigma \in \text{Gal}(f) \quad \prod_{i<j}(\alpha_i - \alpha_j) = \text{sign}(\sigma)\prod_{i<j}(\alpha_i - \alpha_j) \\
&\iff \forall \sigma \in \text{Gal}(f) \quad \text{sign}(\sigma) = 1.
\end{aligned}$$

□

Corollary 6.1. *Let $f \in \mathcal{M}$ square-free, and let χ be the quadratic character on $\mathbb{F}_q$. Then*

$$\text{sign}(\text{Frob}_q|f) = \chi(\text{disc}f)$$

Proof. For $f \in \mathcal{M}$ square-free, $\mathrm{Gal}(f)$ is generated by Frob_q, so by Proposition 6.1

$$\mathrm{disc} f \text{ is a square in } \mathbb{F}_q^\times \iff \mathrm{sign}(\mathrm{Frob}_q | f) = 1$$

from which the corollary follows. □

So, combining Theorem 6.2 with Corollary 6.1, and noting that the discriminant vanishes on non-square-free polynomials, we get a proof of Theorem 6.1.

6.3 "Proto-Pellet's Formula" in number fields

To begin, we pick some additive function $\nu : \mathcal{I}_A \to \mathbb{N}$ to mimic the role of degree in $\mathbb{F}_q[t]$.

Let $\mathcal{P}_A$ be the set of prime ideals in A, and put some order relation $<_A$ on $\mathcal{P}_A$: for example, one can order the prime ideals first by the size of their norm and then order those with the same norm arbitrarily (since there are only finitely many). For $\mathfrak{p}$ a prime ideal, pick $q = q(\mathfrak{p}, \nu)$ to be the minimal prime such that $q \equiv 1 \mod \nu(\mathfrak{p})$ and $q \neq q(\mathfrak{p}', \nu)$ for some $\mathfrak{p}' <_A \mathfrak{p}$ prime (which is always possible, by Dirichlet's Theorem for primes in arithmetic progression). Then consider $L = L_{\mathfrak{p},\nu} = \mathbb{Q}(\zeta_q)$ where $\zeta_q = e^{2\pi i/q}$ and note that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. So, since $\nu(\mathfrak{p})$ divides $q-1$, there is some subgroup H of $\mathrm{Gal}(L/\mathbb{Q})$ such that $H \cong \mathbb{Z}/\frac{q-1}{\nu(\mathfrak{p})}\mathbb{Z}$. Therefore, if we let $K = K_{\mathfrak{p},\nu} = L^H := \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\}$, we know by the Galois Correspondence that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/\nu(\mathfrak{p})\mathbb{Z}$.

Moreover, by the Primitive Element Theorem, there exists some $\alpha_{\mathfrak{p},\nu} \in L$ such that $K = \mathbb{Q}(\alpha_{\mathfrak{p},\nu})$. So, if we let $f_{\mathfrak{p},\nu}$ be the minimal polynomial of $\alpha_{\mathfrak{p},\nu}$, then we have that $\mathrm{Gal}(f_{\mathfrak{p},\nu}) \cong \mathbb{Z}/\nu(\mathfrak{p})\mathbb{Z}$ and is generated by some $\sigma_{\mathfrak{p},\nu}$ which acts as a $\nu(\mathfrak{p})$-cycle on the roots of $f_{\mathfrak{p},\nu}$. In particular, this means that $\mathrm{sign}(\sigma_{\mathfrak{p},\nu} | f_{\mathfrak{p},\nu}) = (-1)^{\nu(\mathfrak{p})-1}$.

Next, let $K_\nu = \mathbb{Q}(\{\alpha_{\mathfrak{p},\nu} \mid \mathfrak{p} \in \mathcal{P}_A\})$ and extend each $\sigma_{\mathfrak{p},\nu}$ to a map $\overline{\sigma}_{\mathfrak{p},\nu} \in \mathrm{Gal}(K_\nu/\mathbb{Q})$ by

$$\overline{\sigma}_{\mathfrak{p},\nu}(\alpha_{\mathfrak{p}',\nu}) = \begin{cases} \sigma_{\mathfrak{p},\nu}(\alpha_{\mathfrak{p},\nu}) & \text{if } \mathfrak{p} = \mathfrak{p}' \\ \alpha_{\mathfrak{p}',\nu} & \text{if } \mathfrak{p} \neq \mathfrak{p}' \end{cases}.$$

The fact that we can do this follows from Proposition 6.2. Then consider $\sigma_\nu \in \mathrm{Gal}(K_\nu/\mathbb{Q})$ defined by $\sigma_\nu(\alpha_{\mathfrak{p},\nu}) = \sigma_{\mathfrak{p},\nu}(\alpha_{\mathfrak{p},\nu})$ for all prime ideals $\mathfrak{p} \in \mathcal{P}_A$, so that by construction we have that $\mathrm{sign}(\sigma_\nu | f_{\mathfrak{p},\nu}) = \mathrm{sign}(\sigma_{\mathfrak{p},\nu} | f_{\mathfrak{p},\nu})$. We observe that σ_ν is well-defined by noting that it is a composition of the $\overline{\sigma}_{\mathfrak{p},\nu}$ over all prime ideals $\mathfrak{p} \in \mathcal{P}_A$.

We take a brief aside to prove Proposition 6.2 as promised:

Proposition 6.2. *Let $\alpha_{\mathfrak{p},\nu}$ and $\sigma_{\mathfrak{p},\nu}$ be defined as above. Let $\{\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ be a set of distinct prime ideals in $\mathcal{P}_A$. Then we can extend $\sigma_{\mathfrak{p},\nu}$ to a map $\sigma^{(k)}_{\mathfrak{p},\nu} \in \mathrm{Gal}(\mathbb{Q}(\{\alpha_{\mathfrak{p}',\nu} \mid \mathfrak{p}' \in \{\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_k\}\})/\mathbb{Q})$ by*

$$\sigma^{(k)}_{\mathfrak{p},\nu}(\alpha_{\mathfrak{p}',\nu}) = \begin{cases} \sigma_{\mathfrak{p},\nu}(\alpha_{\mathfrak{p},\nu}) & \text{if } \mathfrak{p}' = \mathfrak{p} \\ \alpha_{\mathfrak{p}',\nu} & \text{if } \mathfrak{p}' \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\} \end{cases}$$

Proof. We proceed by induction and note that the case $k = 0$ is trivial. Suppose that the case $k = l$ is true, so that we have constructed our desired function $\sigma^{(l)}_{\mathfrak{p},\nu}$ on $K^{(l)}$, where $K^{(m)} := \mathbb{Q}(\{\alpha_{\mathfrak{p}',\nu} \mid \mathfrak{p}' \in \{\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_m\}\})$, and we seek to extend this to $\sigma^{(l+1)}_{\mathfrak{p},\nu}$ on $K^{(l+1)}$.

Let $K = \mathbb{Q}(\alpha_{\mathfrak{p}_{l+1},\nu})$ so that $K^{(l+1)} = K^{(l)}K$, and so that, by Theorem 1.1 of [9] there is an injective homomorphism

$$\rho : \mathrm{Gal}(K^{(l+1)}/\mathbb{Q}) = \mathrm{Gal}(K^{(l)}K/\mathbb{Q}) \to \mathrm{Gal}(K^{(l)}/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$$

given by $\rho(\sigma) = (\sigma\big|_{K^{(l)}}, \sigma\big|_K)$. Moreover, ρ is an isomorphism if, and only if, $K^{(l)}$ and K are linearly disjoint over $\mathbb{Q}$, or equivalently if $K^{(l)} \cap K = \mathbb{Q}$.

But $K^{(l)} \subseteq L^{(l)} := \mathbb{Q}(\{\zeta_{q(\mathfrak{p}',\nu)} \mid \mathfrak{p}' \in \{\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_l\}\})$ and $K \subseteq L := \mathbb{Q}(\zeta_{q(\mathfrak{p}_{l+1},\nu)})$, where $q(\mathfrak{p}', \nu)$ is defined as above. So, since $\{q(\mathfrak{p}', \nu) \mid \mathfrak{p}' \in \{\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_{l+1}\}\}$ is a set of distinct primes, $L^{(l)} \cap L = \mathbb{Q}$ and therefore $K^{(l)} \cap K = \mathbb{Q}$.

Therefore ρ is an isomorphism, and so we can set $\sigma^{(l+1)}_{\mathfrak{p},\nu} = \rho^{-1}(\sigma^{(l)}_{\mathfrak{p},\nu}, \iota)$, where ι is the identity function on K. □

To put this all together, for $I \in \mathcal{I}_A$ we define $f_{I,\nu} = \prod_{\mathfrak{p} \in \mathcal{P}_A : \mathfrak{p} | I} f_{\mathfrak{p},\nu}$, where the product counts prime ideals with multiplicity. This allows us to formulate the following analogue of a "Proto-Pellet's Formula" for the Möbius function for A:

Theorem 6.4. *Let $\nu : \mathcal{I}_A \to \mathbb{N}$ be an additive function, and $I \in \mathcal{I}_A$ square-free. Then for σ_ν and $f_{I,\nu}$ as defined above, we have:*

$$\mu(I) = (-1)^{\nu(I)} \mathrm{sign}(\sigma_\nu | f_{I,\nu})$$

Proof. For $I \in \mathcal{I}_A$ square-free we have that $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some distinct prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r \in \mathcal{P}_A$ and so

$$\mathrm{sign}(\sigma_\nu | f_{I,\nu}) = \prod_{\mathfrak{p} \in \mathcal{P}_A : \mathfrak{p} | I} \mathrm{sign}(\sigma_\nu | f_{\mathfrak{p},\nu}) = \prod_{\mathfrak{p} \in \mathcal{P}_A : \mathfrak{p} | I} (-1)^{\nu(\mathfrak{p})-1} = (-1)^{\nu(I)-r} = (-1)^{\nu(n)} \mu(I).$$

□

Theorem 6.3 now follows as an immediate corollary.

Finally, we consider the trivial example as a check

Example 6.1. *Let $\nu = \omega_A$ where $\omega_A(I) = \#\{\mathfrak{p} \in \mathcal{P}_A \text{ distinct} : \mathfrak{p} | I\}$ so that $\omega_A(\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{p} \in \mathcal{P}_A$. Then for each $\mathfrak{p}$, $\mathrm{Gal}(f_{\mathfrak{p},\omega_A}) \cong \mathbb{Z}/\omega_A(\mathfrak{p})\mathbb{Z}$ is trivial and $\sigma_{\mathfrak{p},\omega_A}$ is just the identity map, which means that $\mathrm{sign}(\sigma_{\mathfrak{p},\omega_A} | f_{\mathfrak{p},\omega_A}) = 1$. Therefore, for all square-free $I \in \mathcal{I}_A$, we have that $\mathrm{sign}(\sigma_{\omega_A} | f_{I,\omega_A}) = 1$, which by Theorem 6.4 implies that $\mu_A(I) = (-1)^{\omega_A(I)}$, recovering the definition of μ_A.*

Current work in progress, and future work, is dedicated to exploring non-trivial explicit cases of our formula in Theorem 6.4 for various additive functions ν. In particular, we seek to find a ν which might serve as an analogue to degree in $\mathbb{F}_q[t]$ and to understand the implications of specialising our formula to such a function ν.

Bibliography

[1] Afshar, A. (2020a). *Highly Composite Polynomials and the maximum order of the Divisor Function in $\mathbb{F}_q[t]$*. arXiv:2001.05635. preprint, accepted for publication in The Ramanujan Journal.

[2] Afshar, A. (2020b). *A "Proto-Pellet's Formula" for the Möbius Function*. arXiv:2001.05641. preprint.

[3] Afshar, A. and Porritt, S. (2019). The function field Sathe-Selberg formula in arithmetic progressions and 'short intervals'. *Acta Arith.*, 187(2):101–124.

[4] Alaoglu, L. and Erdös, P. (1944). On highly composite and similar numbers. *Trans. Amer. Math. Soc.*, 56:448–469.

[5] Bary-Soroker, L. (2014). Hardy-Littlewood tuple conjecture over large finite fields. *Int. Math. Res. Not. IMRN*, (2):568–575.

[6] Bourgain, J. (2017). Decoupling, exponential sums and the Riemann zeta function. *J. Amer. Math. Soc.*, 30(1):205–224.

[7] Car, M. (1982). Factorisation dans $F_q[X]$. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(4):147–150.

[8] Carmon, D. and Rudnick, Z. (2014). The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field. *Q. J. Math.*, 65(1):53–61.

[9] Conrad, K. The galois correspondence at work. *https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorrthms.pdf (retrieved 15 January 2020).*

[10] Conrad, K. (2005). Irreducible values of polynomials: a non-analogy. In *Number fields and function fields—two parallel worlds*, volume 239 of *Progr. Math.*, pages 71–85. Birkhäuser Boston, Boston, MA.

[11] Erdös, P. and Kac, M. (1940). The Gaussian law of errors in the theory of additive number theoretic functions. *Amer. J. Math.*, 62:738–742.

[12] Garling, D. J. H. (1986). *A course in Galois theory.* Cambridge University Press, Cambridge.

[13] Granville, A., Harper, A. J., and Soundararajan, K. (2015). Mean values of multiplicative functions over function fields. *Res. Number Theory*, 1:Paper No. 25, 18.

[14] Granville, A., Harper, A. J., and Soundararajan, K. (2018). A more intuitive proof of a sharp version of Halász's theorem. *Proc. Amer. Math. Soc.*, 146(10):4099–4104.

[15] Granville, A., Harper, A. J., and Soundararajan, K. (2019). A new proof of Halász's theorem, and its consequences. *Compos. Math.*, 155(1):126–163.

[16] Granville, A. and Soundararajan, K. (2003). Decay of mean values of multiplicative functions. *Canad. J. Math.*, 55(6):1191–1230.

[17] Halász, G. (1968). Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen. *Acta Math. Acad. Sci. Hungar.*, 19:365–403.

[18] Halász, G. (1971). On the distribution of additive and the mean values of multiplicative arithmetic functions. *Studia Sci. Math. Hungar.*, 6:211–233.

[19] Harper, A. J. (2009). Two new proofs of the Erdős-Kac theorem, with bound on the rate of convergence, by Stein's method for distributional approximations. *Math. Proc. Cambridge Philos. Soc.*, 147(1):95–114.

[20] Hayes, D. R. (1965). The distribution of irreducibles in GF[q, x]. *Trans. Amer. Math. Soc.*, 117:101–127.

[21] Hughes, C. P. and Rudnick, Z. (2004). On the distribution of lattice points in thin annuli. *Int. Math. Res. Not.*, (13):637–658.

[22] Ingham, A. E. (1927). Mean-Value Theorems in the Theory of the Riemann Zeta-Function. *Proc. London Math. Soc. (2)*, 27(4):273–300.

[23] Keating, J. and Rudnick, Z. (2016). Squarefree polynomials and Möbius values in short intervals and arithmetic progressions. *Algebra Number Theory*, 10(2):375–420.

[24] 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.

[25] Kedlaya, K. (2018). An algorithm for computing highly composite numbers. *https://shreevatsa.github.io/site/assets/hcn/hcn-algorithm.pdf (retrieved 28th May 2020).*

[26] Korobov, N. M. (1958). Estimates of trigonometric sums and their applications. *Uspehi Mat. Nauk*, 13(4 (82)):185–192.

[27] Liu, Y.-R. (2004). A generalization of the erdös-kac theorem and its applications. *Canadian Mathematical Bulletin*, 47(4):589–606.

[28] Montgomery, H. L. (1978). A note on mean values of multiplicative functions. *Report No. 17, Institut Mittag-Leffler, Djursholm.*

[29] Montgomery, H. L. and Vaughan, R. C. (2001). Mean values of multiplicative functions. *Period. Math. Hungar.*, 43(1-2):199–214.

[30] 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.

[31] Pollack, P. (2008). A polynomial analogue of the twin prime conjecture. *Proc. Amer. Math. Soc.*, 136(11):3775–3784.

[32] Ramanujan, S. (2000). Highly composite numbers [Proc. London Math. Soc. (2) **14** (1915), 347–409]. In *Collected papers of Srinivasa Ramanujan*, pages 78–128. AMS Chelsea Publ., Providence, RI.

[33] Rosen, M. (2002). *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[34] Rudnick, Z. (2014). Some problems in analytic number theory for polynomials over a finite field. In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. II*, pages 443–459. Kyung Moon Sa, Seoul.

[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] Sawin, W. and Shusterman, M. (2018). *On the Chowla and Twin Prime conjectures over* $\mathbb{F}_q[t]$. arXiv:1808.04001. preprint.

[37] Selberg, A. (1954). Note on a paper by L. G. Sathe. *J. Indian Math. Soc. (N.S.)*, 18:83–87.

[38] Spiro, C. A. (1985). Extensions of some formulae of A. Selberg. *Internat. J. Math. Math. Sci.*, 8(2):283–302.

[39] 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.

[40] Titchmarsh, E. C. (1986). *The theory of the Riemann zeta-function*. The Clarendon Press, Oxford University Press, New York, second edition. Edited and with a preface by D. R. Heath-Brown.

[41] Vinogradov, I. M. (1958). A new estimate of the function $\zeta(1+it)$. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 22:161–164.

[42] Weil, A. (1948). *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris.