Keating, J. P., & Rudnick, Z. (2016). Squarefree polynomials and möbius values in short intervals and arithmetic progressions. Algebra and Number Theory, 10(2), 375-420. 10.2140/ant.2016.10.375

Peer reviewed version

Link to published version (if available):
10.2140/ant.2016.10.375

Link to publication record in Explore Bristol Research
PDF-document

SQUAREFREE POLYNOMIALS AND MÖBIUS VALUES IN SHORT INTERVALS AND ARITHMETIC PROGRESSIONS

J.P. KEATING AND Z. RUDNICK

Abstract. We calculate the mean and variance of sums of the Möbius function μ and the indicator function of the squarefrees μ^2, in both short intervals and arithmetic progressions, in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q \to \infty$. We do this by relating the sums in question to certain matrix integrals over the unitary group, using recent equidistribution results due to N. Katz, and then by evaluating these integrals. In many cases our results mirror what is either known or conjectured for the corresponding problems involving sums over the integers, which have a long history. In some cases there are subtle and surprising differences. The ranges over which our results hold is significantly greater than those established for the corresponding problems in the number field setting.

Contents

Date: October 12, 2015.

2010 *Mathematics Subject Classification.* Primary 11T55; Secondary 11M38, 11M50.

JPK gratefully acknowledges support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms, a grant from Leverhulme Trust, a Royal Society Wolfson Merit Award, a Royal Society Leverhulme Senior Research Fellowship, and by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant number FA8655-10-1-3088. ZR is similarly grateful for support from the Friends of the Institute for Advanced Study, the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755, and from the Israel Science Foundation (grant No. 925/14).

1. Introduction

The goal of this paper is to investigate the fluctuation of sums of two important arithmetic functions, the Möbius function μ and the indicator function of the squarefrees μ^2, in the context of the the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q\to\infty$. The problems we address, which concern sums over short intervals and arithmetic progressions, mirror long-standing questions over the integers, where they are largely unknown. In our setting we succeed in giving definitive answers.

Our approach differs from those traditionally employed in the number field setting: we use recent equidistribution results due to N. Katz, valid in the large-q limit, to express the mean and variance of the fluctuations in terms of matrix integrals over the unitary group. Evaluating these integrals leads to explicit formulae and precise ranges of validity. For many of the problems we study, the formulae we obtain match the corresponding number-field results and conjectures exactly, providing further support in the latter case. However, the ranges of validity that we can establish are significantly greater than those known or previously conjectured for the integers, and we see our results as supporting extensions to much wider ranges of validity in the integer setting. Interestingly, in some other problems we uncover subtle and surprising differences between the function-field and number-field asymptotics, which we examine in detail.

We now set out our main results in a way that enables comparison with the corresponding problems for the integers.

1.1. **The Möbius function.**

It is a standard heuristic to assume that the Möbius function behaves like a random ±1 supported on the squarefree integers, which have density $1/\zeta(2)$ (see e.g. [8]). Proving anything in this direction is not easy. Even demonstrating cancellation in the sum $M(x) := \sum_{1\leq n\leq x}\mu(n)$, that is that $M(x) = o(x)$, is equivalent to the Prime Number Theorem. The Riemann Hypothesis is equivalent to square-root cancellation: $M(x) = O(x^{1/2+o(1)})$.

For sums of $\mu(n)$ in blocks of length H,

$$M(x;H) := \sum_{|n-x|<H/2} \mu(n) \tag{1.1}$$

it has been shown that there is cancellation for $H \gg x^{7/12+o(1)}$ [25, 30], and assuming the Riemann Hypothesis one can take $H \gg x^{1/2+o(1)}$. If one wants cancellation only for "almost all" values of x, then more is known. In particular, very recently Mätomaki and Radziwiłł [23] have shown (unconditionally) that

$$\frac{1}{X}\int_X^{2X} M(x;H)^2 dx = o(H^2)$$

whenever $H = H(X) \to \infty$ as $X \to \infty$, and in particular $M(x;H) = o(H)$ for almost all $x \in [X, 2X]$.

We expect the normalized sums $M(x;H)/\sqrt{H}$ to have mean zero (this follows from the Riemann Hypothesis) and variance $6/\pi^2 = 1/\zeta(2)$:

$$\frac{1}{X}\int_X^{2X} |M(x;H)|^2 \sim \frac{H}{\zeta(2)}. \tag{1.2}$$

Moreover, $M(x;H)/\sqrt{H/\zeta(2)}$ is believed to have a normal distribution asymptotically. These conjectures were formulated and investigated numerically by Good and Churchhouse [11] in 1968, and further studied by Ng [27], who carried out an analysis using the Generalized Riemann Hypothesis (GRH) and a strong version of Chowla's conjecture on correlations of Möbius, showing that (1.2) is valid for $H \ll X^{1/4-o(1)}$ and that Gaussian distribution holds (assuming these conjectures) for $H \ll X^{\epsilon}$. It is important that the length H of the interval be significantly smaller than its location, that is $H < X^{1-\epsilon}$, since otherwise one expects non-Gaussian statistics, see [26].

Concerning arithmetic progressions, Hooley [14] studied the following averaged form of the total variance (averaged over moduli)

$$V(X,Q) := \sum_{Q'\leq Q}\sum_{A \bmod Q'}\Big(\sum_{\substack{n\leq X\\ n=A \bmod Q'}}\mu(n)\Big)^2 \tag{1.3}$$

and showed that for $Q \leq X$,

$$V(X,Q) = \frac{6QX}{\pi^2} + O(X^2(\log X)^{-C}) \tag{1.4}$$

for all $C>0$, which yields an asymptotic result for $X/(\log X)^C \ll Q < X$.

For polynomials over a finite field $\mathbb{F}_q$, the Möbius function is defined as for the integers, namely by $\mu(f) = (-1)^k$ if f is a scalar multiple of a product of k distinct monic irreducibles, and $\mu(f)=0$ if f is not squarefree. The analogue of the full sum $M(x)$ is the sum over all monic polynomials $\mathcal{M}_n$ of given degree n, for which we have

$$\sum_{f\in\mathcal{M}_n}\mu(f) = \begin{cases}1, & n=0\\ -q, & n=1\\ 0, & n\geq 2\end{cases} \tag{1.5}$$

so that in particular the issue of size is trivial[1]. However that is no longer the case when considering sums over "short intervals", that is over sets of the form

$$I(A;h) = \{f : ||f-A|| \leq q^h\} \tag{1.6}$$

where $A\in\mathcal{M}_n$ has degree n, $0\leq h\leq n-2$ and[2] the norm is

$$||f|| := \#\mathbb{F}_q[t]/(f) = q^{\deg f}\ . \tag{1.7}$$

To facilitate comparison between statements for number field results and for function fields, we use a rough dictionary

$$\begin{aligned} X &\leftrightarrow q^n, \quad \log X \leftrightarrow n\\ H &\leftrightarrow q^{h+1}, \quad \log H \leftrightarrow h+1 \end{aligned} \tag{1.8}$$

Set

$$\mathcal{N}_\mu(A;h) := \sum_{f\in I(A;h)}\mu(f)\ . \tag{1.9}$$

The number of summands here is $q^{h+1} =: H$ and we want to display cancellation in this sum and study its statistics as we vary the "center" A of the interval.

We can demonstrate cancellation in the short interval sums $\mathcal{N}_\mu(A;h)$ in the large finite field limit $q\to\infty$, n fixed (we assume q is odd throughout the paper):

[1] This ceases to be the case when dealing with function fields of higher genus, see e.g. [7, 15]

[2] For $h=n-1$, $I(A;n-1)=\mathcal{M}_n$ is the set of all monic polynomials of degree n

Theorem 1.1. *If $2 \le h \le n-2$ then for all A of degree n,*

$$\Big|\mathcal{N}_\mu(A;h)\Big| \ll_n \frac{H}{\sqrt{q}}$$

the implied constant uniform in A, depending only on $n = \deg A$.

For $h = 0, 1$ this is no longer valid, that is there are A's for which there is no cancellation, see § 3.

We next investigate the statistics of $\mathcal{N}_\mu(A;h)$ as A varies over all monic polynomials of given degree n, and $q \to \infty$. It is easy to see that for $n \ge 2$, the mean value of $\mathcal{N}_\mu(A;h)$ is 0. Our main result concerns the variance:

Theorem 1.2. *If $0 \le h \le n-5$ then as $q \to \infty$, q odd,*

$$\operatorname{Var}\mathcal{N}_\mu(\bullet;h) = \frac{1}{q^n}\sum_{A\in\mathcal{M}_n}|\mathcal{N}_\mu(A;h)|^2 \sim H\int\limits_{U(n-h-2)}|\operatorname{tr}\operatorname{Sym}^n U|^2 dU = H$$

This is consistent with the Good-Churchhouse conjecture (1.2) if we write it as $H/\zeta_q(2)$, where

$$\zeta_q(s) = \sum_{f\, monic}\frac{1}{||f||^s}, \quad \operatorname{Re}(s) > 1,$$

which tends to 1 as $q \to \infty$, and $H = q^{h+1}$ is the number of monic polynomials in the short interval.

A version of Theorem 1.2 valid for $h < n/2$ ("very short" intervals) has recently been obtained by Bae, Cha and Jung [4] using the method of our earlier paper [22].

Analogous results can be obtained for sums over arithmetic progressions, see § 8.

1.2. **Squarefrees.**

It is well known that the density of squarefree integers is $1/\zeta(2) = 6/\pi^2$, and an elementary sieve shows

$$Q(x) := \#\{n \le x : n \text{ squarefree}\} = \frac{x}{\zeta(2)} + O(x^{1/2})\ . \tag{1.10}$$

No better exponent is known for the remainder term. Using zero-free regions for $\zeta(s)$, Walfisz gave a remainder term of the form $x^{1/2}\exp(-c(\log x)^{3/5+o(1)})$. Assuming RH, the exponent 1/2 has been improved [1, 24, 2], currently to $17/54 = 0.31$ [16]. It is expected that

$$Q(x) = \frac{x}{\zeta(2)} + O(x^{1/4+o(1)})\ . \tag{1.11}$$

Since the density is known, we wish to understand to what extent we can guarantee the existence of squarefrees in short intervals $(x, x+H]$; moreover, when do we still expect to have an asymptotic formula for the number

$$Q(x,H) := \sum_{|n-x|\le\frac{H}{2}}\mu^2(n) = Q(x+H) - Q(x) \tag{1.12}$$

of squarefrees in the interval $(x, x+H]$; that is when do we still have

$$Q(x;H) \sim \frac{H}{\zeta(2)}\ . \tag{1.13}$$

In view of the bound of $O(x^{1/2})$ for the remainder term in (1.10), this holds for $H \gg x^{1/2+o(1)}$. However, one can do better without improving on the remainder term in (1.10). This was first done by Roth [34] who by an elementary method showed that the asymptotic (1.13) persists for $H \gg x^{1/3+o(1)}$. Following improvements by Roth himself (exponent 3/13) and Richert [32] in 1954 (exponenent 2/9), the current best bound is by Tolev [37] (2006) (building on earlier work by Filaseta and Trifonov) who gave $H \gg x^{1/5+o(1)}$. It is believed that (1.13) should hold for $H \gg x^{\epsilon}$ for any $\epsilon > 0$, though there are intervals of size $H \gg \log x/\log\log x$ which contain no squarefrees, see [9].

As for almost-everywhere results, one way to proceed goes through a study of the variance of $Q(x, H)$. In this direction, Hall [12] showed that provided $H = O(x^{2/9-o(1)})$, the variance of $Q(x, H)$ admits an asymptotic formula:

$$\frac{1}{x}\sum_{n\leq x}\left|Q(n,H)-\frac{H}{\zeta(2)}\right|^2 \sim A\sqrt{H}\ , \tag{1.14}$$

with

$$A = \frac{\zeta(3/2)}{\pi}\prod_p\left(\frac{p^3-3p+2}{p^3}\right)\ . \tag{1.15}$$

Based on our results below, we expect this asymptotic formula to hold for H as large as $x^{1-\epsilon}$.

Concerning arithmetic progressions, denote by

$$S(x;Q,A) = \sum_{\substack{n\leq x\\ n=A \bmod Q}} \mu(n)^2$$

the number of squarefree integers in the arithmetic progression $n = A \bmod Q$. Prachar [29] showed that for $Q < x^{2/3-\epsilon}$, and A coprime to Q,

$$S(x;Q,A) \sim \frac{1}{\zeta(2)}\prod_{p\mid Q}(1-\frac{1}{p^2})^{-1}\frac{x}{Q} = \frac{1}{\zeta(2)}\prod_{p\mid Q}(1+\frac{1}{p})^{-1}\frac{x}{\phi(Q)} \tag{1.16}$$

In order to understand the size of the remainder term, one studies the variance

$$\mathrm{Var}(S) = \frac{1}{\phi(Q)}\sum_{\gcd(A,Q)=1}\left|S(x;Q,A)-\frac{1}{\zeta(2)}\prod_{p\mid Q}(1-\frac{1}{p^2})^{-1}\frac{x}{Q}\right|^2 \tag{1.17}$$

as well as a version where the sum is over all residue classes $A \bmod Q$, not necessarily coprime to Q, and the further averaged form over all moduli $Q' \leq Q$ a-la Barban, Davenport & Halberstam, see [38].

Without averaging over moduli, Blomer [5, Theorem 1.3] gave an upper bound for the variance, which was very recently improved by Nunes [28], who gave an asymptotic for the variance in the range $X^{\frac{31}{41}+\epsilon} < Q < X^{1-\epsilon}$

$$\mathrm{Var}(S) \sim A \prod_{p|Q} (1-\frac{1}{p})^{-1}(1+\frac{2}{p})^{-1} \cdot \frac{X^{1/2}}{Q^{1/2}} \tag{1.18}$$

where A is given by (1.15). It is apparently not known in what range of Q to expect (1.18) to hold. Based on our results below, we conjecture that (1.18) holds down to $X^\epsilon < Q$.

Our goal here is to study analogous problems for $\mathbb{F}_q[t]$. The total number of squarefree monic polynomials of degree $n > 1$ is (exactly)

$$\sum_{f\in\mathcal{M}_n} \mu(f)^2 = \frac{q^n}{\zeta_q(2)} \ . \tag{1.19}$$

The number of squarefree polynomials in the short interval $I(A;h)$ is

$$\mathcal{N}_{\mu^2}(A;h) = \sum_{f\in I(A;h)} \mu(f)^2 \ . \tag{1.20}$$

1.2.1. *Asymptotics.* We show that for any short interval/arithmetic progression, we still have an asymptotic count of the number of squarefrees:

Theorem 1.3. *i) If* $\deg Q < n$ *and* $\gcd(A,Q)=1$ *then*

$$\#\{f\in\mathcal{M}_n : f = A \bmod Q \; f \text{ squarefree}\} = \frac{q^n}{|Q|}\left(1+O_n(\frac{1}{q})\right) \ .$$

ii) If $0 < h \le n-2$ *then for all* $A\in\mathcal{M}_n$*,*

$$\#\{f\in I(A;h) : f \text{ squarefree}\} = \frac{H}{\zeta_q(2)} + O(\frac{H}{q}) = H + O_n(\frac{H}{q}) \ .$$

In both cases the implied constants depend only on n*.*

Note that for $h=0$, Theorem 1.3(ii) need not hold: If $q=p^k$ with p a fixed odd prime, $n=p$ then the short interval $I(t^n;0) = \{t^n+b : b\in\mathbb{F}_q\}$ has no squarefrees, since $t^p+b=(t+b^{q/p})^p$ has multiple zeros for any $b\in\mathbb{F}_q$.

1.2.2. *Variance.* We are able to compute the variance, the size of which turns out to depend on the parity of the interval-length parameter h in a surprising way:

Theorem 1.4. *Let* $0\le h\le n-6$*. Assume* $q\to\infty$ *with all* q*'s coprime to* 6*.*

i) If h *is even then*

$$\mathrm{Var}\,\mathcal{N}_{\mu^2}(\bullet;h) \sim q^{\frac{h}{2}} \int\limits_{U(n-h-2)} \left|\mathrm{tr}\,\mathrm{Sym}^{\frac{h}{2}+1} U\right|^2 dU = \frac{\sqrt{H}}{\sqrt{q}}$$

(the matrix integral works out to be 1*).*

ii) If h is odd then

$$\operatorname{Var}\mathcal{N}_{\mu^2}(\bullet;h) \sim q^{\frac{h-1}{2}} \int\limits_{U(n-h-2)} \left|\operatorname{tr} U\right|^2 dU \int\limits_{U(n-h-2)} \left|\operatorname{tr}\operatorname{Sym}^{\frac{h+3}{2}} U'\right|^2 dU' = \frac{\sqrt{H}}{q}$$

(both matrix integrals equal 1*).*

To compare with Hall's result (1.14), where the variance is of order $\sqrt{H}$, one wants to set $H = \#I(A;h) = q^{h+1}$ and then in the limit $q \to \infty$ we get smaller variance - either $\sqrt{H}/q^{1/2}$ (h even) or $\sqrt{H}/q$ (h odd). We found this sufficiently puzzling to check the analogue of Hall's result for the polynomial ring $\mathbb{F}_q[t]$ for the large degree limit of *fixed* q and $n \to \infty$. The result, presented in Appendix A, is consistent with Theorem 1.4 in that for $H < (q^n)^{\frac{2}{9}-o(1)}$, the variance is

$$\operatorname{Var}(\mathcal{N}_{\mu^2}(\bullet;h)) \sim \sqrt{H}\frac{\beta_q}{1-\frac{1}{q^3}}\begin{cases}\frac{1+\frac{1}{q^2}}{\sqrt{q}}, & h \text{ even},\\ \\ \frac{1+\frac{1}{q}}{q}, & h \text{ odd},\end{cases}$$

so that it is of order $\sqrt{H}$ for fixed q.

We also obtain a similar result for arithmetic progressions. Let $Q \in \mathbb{F}_q[t]$ be a squarefree polynomial of degree ≥ 2, and A coprime to Q. we set

$$\mathcal{S}(A) = \sum_{\substack{f=A \bmod Q\\ f\in\mathcal{M}_n}} \mu^2(f)\ . \tag{1.21}$$

The expected value over such A is

$$\langle\mathcal{S}\rangle_Q = \frac{1}{\Phi(Q)}\sum_{\substack{f\in\mathcal{M}_n\\ (f,Q)=1}} \mu^2(f) \sim \frac{q^n/\zeta_q(2)}{\Phi(Q)} \sim \frac{q^n}{|Q|}. \tag{1.22}$$

We will show that the variance satisfies:

Theorem 1.5. *Fix $N \geq 1$. For any sequence of finite fields $\mathbb{F}_q$, with q odd, and squarefree polynomials $Q \in \mathbb{F}_q[t]$ with $\deg Q = N+1$, as $q \to \infty$,*

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}} \times \begin{cases} 1/\sqrt{q}, & n \neq \deg Q \bmod 2\\ \\ 1/q, & n = \deg Q \bmod 2\ .\end{cases}$$

1.3. **General approach.** It may be helpful to give an informal sketch of the general approach we take in proving most of the theorems stated above. Short intervals are transformed into sums over special arithmetic progressions, a feature special to function fields that was used in our earlier work [22]. Sums involving μ and μ^2 that run over all monic polynomials of a given degree may be evaluated in terms of a zeta function that is the function-field analogue of the Riemann zeta function. Restricting to short intervals or arithmetic progressions leads to sums over Dirichlet characters involving the associated L-functions. The L-functions in question may be written in terms of unitary matrices. It has recently been established by N. Katz that, in the limit when $q \to \infty$, these matrices become equidistributed in the unitary group, in the sense that the character sums we need are, in the large-q limit, equal to integrals over the unitary group. Evaluating these integrals leads to the formulae appearing in our theorems.

2. Asymptotics for squarefrees: Proof of Theorem 1.3

We want to show that almost all polynomials in an arithmetic progression, or in a short interval are squarefree. We recall the statement:

i) If $\deg Q < n$ and $\gcd(A,Q) = 1$ then

$$\#\{f \in \mathcal{M}_n : f = A \bmod Q, f \text{ squarefree}\} \sim \frac{q^n}{|Q|} \sim \frac{q^n}{\Phi(Q)} \; . \tag{2.1}$$

ii) If $0 < h \leq n-2$ then

$$\#\{f \in I(A;h) : f \text{ squarefree}\} = \frac{H}{\zeta_q(2)} + O(\frac{H}{q}) = H + O(\frac{H}{q}) \; . \tag{2.2}$$

These follow from a general result [35]:

Theorem 2.1. *Given a separable polynomial $F(x,t) \in \mathbb{F}_q[x,t]$, with squarefree content then the number of monic polynomials $a \in \mathcal{M}_m$, $m > 0$, for which $F(a(t),t)$ is squarefree (in $\mathbb{F}_q[t]$) is asymptotically*

$$q^m + O\Big(q^{m-1}(m \deg F + \operatorname{Ht}(F)) \deg F\Big) \; .$$

Here if $F(x,t) = \sum_{j=0}^{\deg F} \gamma_j(t) x^j$ with $\gamma_j(t) \in \mathbb{F}_q[t]$ polynomials, the content of F is $\gcd(\gamma_0, \gamma_1, \dots,)$ and the height is $\operatorname{Ht}(f) = \max_j \deg \gamma_j$.

For an arithmetic progression $f = A \mod Q$, $f \in \mathcal{M}_n$ monic of degree n, with $\gcd(A,Q) = 1$, $\deg A < \deg Q$, we take the corresponding polynomial to be

$$F(x,t) = A(t) + \frac{1}{\operatorname{sign} Q} Q(t) x$$

where $\operatorname{sign} Q \in \mathbb{F}_q^\times$ is such that $Q(t)/\operatorname{sign} Q$ is monic. Then $F(x,t)$ has degree one (in x), hence is certainly separable, and has content equal to $\gcd(A,Q) = 1$ so is in fact primitive. The height of F is $\max(\deg Q, \deg A) = \deg Q < n$ which is independent of q.

Since $\deg A < \deg Q$, then $f = A + aQ/\operatorname{sign}(Q)$ is monic of degree n if and only if a is monic of degree $n - \deg Q > 0$, and by Theorem 2.1 the number of such a for which $F(a(t),t)$ is squarefree is

$$q^{n-\deg Q} + O(q^{n-\deg Q-1}) = \frac{q^n}{|Q|}(1 + O(\frac{1}{q})) \; .$$

This proves (2.1).

To deal with the short interval case, let $0 < h \leq n-2$, and $A \in \mathcal{M}_n$ be monic of degree n. We want to show that the number of polynomials

f in the short interval $I(A;h)$ which are squarefree is $H+O(H/q)$ (recall $H=\#I(A;h)=q^{h+1}$).

We write

$$I(A;h)=(A+\mathcal{P}_{\leq h-1})\cup\coprod_{c\in\mathbb{F}_q^\times}(A+c\mathcal{M}_h)\ .$$

The number of squarefrees in $A+\mathcal{P}_{\leq h-1}$ is at most $\#\mathcal{P}_{\leq h-1}=q^h$. The squarefrees in $A+c\mathcal{M}_h$ are the squarefree values at monic polynomials of degree h of the polynomial $F(x,t)=A(t)+cx$, which has degree 1, content $\gcd(A(t),c)=1$ and height $\operatorname{Ht}(F)=\deg A=n$. By Theorem 2.1 the number of substitutions $a\in\mathcal{M}_h$ for which $F(a)$ is squarefree is

$$q^h+O(nq^{h-1})\ .$$

Hence number of squarefrees in $I(A;h)$ is

$$\sum_{c\in\mathbb{F}_q^\times}(q^h+O(nq^{h-1}))+O(q^h)=H+O(\frac{H}{q})\ ,$$

proving (2.2).

3. Asymptotics for Möbius sums

In this section we deal with cancellation in the individual sums

$$\mathcal{N}_\mu(A;h)=\sum_{f\in I(A;h)}\mu(f)\ .$$

Note that the interval $I(A;h)$ consists of all polynomials of the form $A+g$, where $g\in\mathcal{P}_{\leq h}$ is the set of all polynomials of degree at most h.

3.1. **Small** h.

We first point out that for $h=0,1$ there need not be any cancellation. We recall Pellet's formula for the discriminant (in odd characteristic)

$$\mu(f)=(-1)^{\deg f}\chi_2(\operatorname{disc} f) \tag{3.1}$$

where $\chi_2:\mathbb{F}_q^\times\to\{\pm1\}$ is the quadratic character of $\mathbb{F}_q$ and $\operatorname{disc} f$ is the discriminant of f. From Pellet's formula we find (as in [6])

$$\mathcal{N}_\mu(A;h)=(-1)^{\deg A}\sum_{g\in\mathcal{P}_{\leq h}}\chi_2(\operatorname{disc}(A+g))\ . \tag{3.2}$$

Let $A(t)=t^n$. The discriminant of the trinomial t^n+at+b is (see e.g. [36])

$$\operatorname{disc}(t^n+at+b)=(-1)^{n(n-1)/2}\Big(n^nb^{n-1}+(1-n)^{n-1}a^n\Big)\ . \tag{3.3}$$

Hence for the interval $I(t^n;1)=\{t^n+at+b:a,b\in\mathbb{F}_q\}$ we obtain

$$\mathcal{N}_\mu(t^n;1)=(-1)^n\chi_2(-1)^{n(n-1)/2}\sum_{a,b\in\mathbb{F}_q}\chi_2\Big(n^nb^{n-1}+(1-n)^{n-1}a^n\Big)\ . \tag{3.4}$$

Therefore if $q = p^k$ with p an odd prime and $2p \mid n$ then

$$\mathcal{N}_\mu(t^n; 1) = \chi_2(-1)^{n/2} q \sum_{a\in\mathbb{F}_q} \chi_2(a)^n = \pm q(q-1) \tag{3.5}$$

so that $|\mathcal{N}_\mu(t^n; 1)| \gg q^2 = H$. A similar construction also works for $h = 0$.

3.2. **Large h.**

We also note that for $h = n-2$, and $p \nmid n$ (p is the characteristic of $\mathbb{F}_q$) the Möbius sums all coincide. This is because $\mu(f(t)) = \mu(f(t+c))$ if $\deg f \geq 1$. Therefore

$$\mathcal{N}_\mu(A(t); h) = \mathcal{N}_\mu(A(t+c); h) \ .$$

Now if $A(t) = t^n + a_{n-1}t^{n-1} + \dots$ is the center of the interval, then choosing $c = -a_{n-1}/n$ gives

$$A(t+c) = t^n + \tilde{a}_{n-2}t^{n-2} + \dots$$

which contains no term of the form t^{n-1}. Therefore if $h = n-2$ then

$$\mathcal{N}_\mu(t^n + a_{n-1}t^{n-1}; n-2) = \mathcal{N}_\mu(t^n; n-2)$$

has just one possible value.

Thus we may assume that $h \leq n-3$.

We note that the same is true for the squarefree case.

3.3. **Proof of Theorem 1.1.**

Now we prove Theorem 1.1; that is, we show that for $h \geq 2$, for any (monic) $A(t)$ of degree n,

$$\sum_{a\in\mathcal{P}_{\leq h}} \mu(A+a) \ll \frac{H}{\sqrt{q}} \tag{3.6}$$

Writing $a(t) = a_h t^h + \dots + a_1 t + b$, it suffices to show that there is a constant $C = C(n,h)$ (independent of A and $\vec{a} = (a_1, \dots, a_h)$) so that for "most" choices of $\vec{a}$, (i.e. for all but $O(q^{h-1})$) we have

$$\left| \sum_{b\in\mathbb{F}_q} \mu(A(t) + a_h t^h + \dots + a_1 t + b) \right| \leq C\sqrt{q}. \tag{3.7}$$

Using Pellet's formula, we need to show that for most $\vec{a}$,

$$\left| \sum_{b\in\mathbb{F}_q} \chi_2 \Big(\mathrm{disc}(A(t) + a_h t^h + \dots + a_1 t + b) \Big) \right| \leq C\sqrt{q} \tag{3.8}$$

Now $D_a(b) := \mathrm{disc}(A(t) + a_h t^h + \dots + a_1 t + b)$ is a polynomial in b, of degree $\leq n-1$, and if we show that for most $\vec{a}$ it is non-constant and squarefree then by Weil's theorem we will get that (3.8) holds for such $\vec{a}$'s, with $C = n-2$. The argument in [6, Section 4] works verbatim here to prove that. □

An alternative argument is to use the work of Bank, Bary-Soroker and Rosenzweig [3] who prove equidistribution of cycle types of polynomials in any short interval $I(A; h)$ for $2 \leq h \leq n-2$ and q odd (this also uses [6]). Now for $f \in \mathcal{M}_n$ squarefree, $\mu(f) = (-1)^n \operatorname{sign}(\sigma_f)$ where $\sigma_f \subset S_n$ is the conjugacy class of permutations induced by the Frobenius acting on the roots of f, and sign is the sign character. For any $f \in \mathcal{M}_n$, not necessarily squarefree, we denote by $\lambda(f) = (\lambda_1, \dots, \lambda_n)$ the cycle structure of f, which for squarefree f coincides with the cycle structure of the permutation σ_f. Then $\operatorname{sign}(\sigma_f) = \operatorname{sign}(\lambda(f)) := \prod_{j=1}^n (-1)^{(j-1)\lambda_j}$. Thus

$$\sum_{f \in I(A;h)} \mu(f) = (-1)^n \sum_{\substack{f \in I(A;h) \\ \text{squarefree}}} \operatorname{sign}(\sigma_f) \tag{3.9}$$

By Theorem 1.3, all but $O_n(H/q)$ of the polynomials in the short interval $I(A;h)$ are squarefree, hence

$$\begin{aligned} \sum_{\substack{f \in I(A;h) \\ \text{squarefree}}} \operatorname{sign}(\sigma_f) &= \sum_{f \in I(A;h)} \operatorname{sign}(\sigma_f) + O(\frac{H}{q}) \\ &= H\left(\frac{1}{n!}\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) + O(\frac{1}{\sqrt{q}})\right) = O(\frac{H}{\sqrt{q}}) \end{aligned} \tag{3.10}$$

by equidistribution of cycle types in short intervals [3], and recalling that $\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) = 0$ for $n > 1$.

4. Variance in arithmetic progressions: General theory

Let $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ be a function on polynomials, which is "even" in the sense that

$$\alpha(cf) = \alpha(f)$$

for the units $c \in \mathbb{F}_q^\times$. We assume that

$$\max_{\deg f \le n} |\alpha(f)| \le A_n \tag{4.1}$$

with A_n independent of q. We will require some further constraints on α later on.

We denote by $\langle \alpha \rangle_n$ the mean value of α over all monic polynomials of degree n:

$$\langle \alpha \rangle_n := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha(f) \ . \tag{4.2}$$

Let $Q \in \mathbb{F}_q[t]$ be squarefree, of positive degree. For an arithmetic function $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$, we define its mean value over coprime residue classes by

$$\langle \alpha \rangle_Q := \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \alpha(A) \ . \tag{4.3}$$

The sum of α over all monic polynomials of degree n lying in the arithmetic progressions $f = A \mod Q$ is

$$\mathcal{S}_{\alpha,n,Q}(A) := \sum_{\substack{f\in\mathcal{M}_n \\ f=A \bmod Q}} \alpha(f) \;. \tag{4.4}$$

We wish to study the fluctuations in $\mathcal{S}(A)$ as we vary A over residue classes coprime to Q. The mean value of $\mathcal{S}$ is

$$\langle \mathcal{S}_\alpha \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ (f,Q)=1}} \alpha(f) \tag{4.5}$$

where $\Phi(Q)$ is the number of invertible residues modulo Q.

Our goal is to compute the variance

$$\mathrm{Var}_Q(\mathcal{S}_\alpha) = \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ (A,Q)=1}} |\mathcal{S}_\alpha(A) - \langle \mathcal{S}_\alpha \rangle|^2 \;. \tag{4.6}$$

4.1. **A formula for the variance.** Expanding in Dirichlet characters modulo Q gives

$$\mathcal{S}(A) = \frac{1}{\Phi(Q)} \sum_{\chi \bmod Q} \bar\chi(A)\mathcal{M}(n;\alpha\chi) \tag{4.7}$$

where

$$\mathcal{M}(n;\alpha\chi) := \sum_{f\in\mathcal{M}_n} \chi(f)\alpha(f) \;. \tag{4.8}$$

The mean value is the contribution of the trivial character χ_0:

$$\langle \mathcal{S} \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,Q)=1}} \alpha(f) \tag{4.9}$$

so that

$$\mathcal{S}(A) - \langle \mathcal{S} \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\chi\neq\chi_0 \bmod Q} \bar\chi(A)\mathcal{M}(n;\alpha\chi) \;. \tag{4.10}$$

Inserting (4.7) and using the orthogonality relations for Dirichlet characters as in [22], we see that the variance is

$$\mathrm{Var}_Q(\mathcal{S}) = \left\langle \left| \mathcal{S} - \langle \mathcal{S} \rangle_Q \right|^2 \right\rangle_Q = \frac{1}{\Phi(Q)^2} \sum_{\chi\neq\chi_0} |\mathcal{M}(n;\alpha\chi)|^2 \;. \tag{4.11}$$

4.2. **Small n.** If $n < \deg Q$, then there is at most one f with $\deg f = n$ and $f = A \bmod Q$, and in this case

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^n}{\Phi(Q)} \left\langle \alpha^2 \right\rangle_n , \quad n < \deg Q \; . \tag{4.12}$$

Indeed, if $n < \deg Q$, then

$$| \left\langle \mathcal{S} \right\rangle_Q | = | \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=1}} \alpha(f) | \leq \frac{1}{\Phi(Q)} \sum_{f \in \mathcal{M}_n} |\alpha(f)| \leq \frac{A_n q^n}{\Phi(Q)} \ll_n \frac{1}{q} \; . \tag{4.13}$$

Hence

$$\begin{aligned} \mathrm{Var}_Q(\mathcal{S}) &= \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} |\mathcal{S}(A)|^2 (1 + O(q^{-1})) \\ &= \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=1}} |\alpha(f)|^2 (1 + O(q^{-1})) \\ &= \frac{q^n}{\Phi(Q)} \left\langle |\alpha|^2 \right\rangle_n (1 + O(\frac{1}{q})) \end{aligned}$$

as claimed.

5. Variance in short intervals: General theory

Given an arithmetic function $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$, define its sum on short intervals as

$$\mathcal{N}_\alpha(A; h) = \sum_{f \in I(A;h)} \alpha(f) \; . \tag{5.1}$$

The mean value of $\mathcal{N}_\alpha$ is (see Lemma 5.2)

$$\left\langle \mathcal{N}_\alpha(\bullet, h) \right\rangle = q^{h+1} \left\langle \alpha \right\rangle_n = H \left\langle \alpha \right\rangle_n \; . \tag{5.2}$$

Our goal will be to compute the variance of $\mathcal{N}_\alpha$,

$$\mathrm{Var}\, \mathcal{N}_\alpha = \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\mathcal{N}_\alpha(A) - \left\langle \mathcal{N}_\alpha \right\rangle|^2 \tag{5.3}$$

and more generally, given two such functions α, β, to compute the covariance

$$\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta) = \Big\langle \Big(\mathcal{N}_\alpha - \left\langle \mathcal{N}_\alpha \right\rangle \Big) \Big(\mathcal{N}_\beta - \left\langle \mathcal{N}_\beta \right\rangle \Big) \Big\rangle \; . \tag{5.4}$$

5.1. **Background on short intervals (see** [22]**).** Let

$$\mathcal{P}_n = \{f \in \mathbb{F}_q[t] : \deg f = n\} \tag{5.5}$$

be the set of polynomials of degree n,

$$\mathcal{P}_{\leq n} = \{0\} \cup \bigcup_{0 \leq m \leq n} \mathcal{P}_m \tag{5.6}$$

the space of polynomials of degree at most n (including 0), and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

By definition of short intervals,

$$I(A;h) = A + \mathcal{P}_{\leq h} \ , \tag{5.7}$$

and hence

$$\#I(A;h) = q^{h+1} =: H \ . \tag{5.8}$$

For $h = n-1$, $I(A;n-1) = \mathcal{M}_n$ is the set of all monic polynomials of degree n. For $h \leq n-2$, if $||f - A|| \leq q^h$ then $\deg f = \deg A$ and A is monic if and only if f is monic. Hence for A monic, $I(A;h)$ consists of only monic polynomials and all monic f's of degree n are contained in one of the intervals $I(A;h)$ with A monic of degree n. Moreover,

$$I(A_1;h) \bigcap I(A_2;h) \neq \emptyset \leftrightarrow \deg(A_1 - A_2) \leq h \leftrightarrow I(A_1;h) = I(A_2;h) \tag{5.9}$$

and we get a partition of $\mathcal{P}_n$ into disjoint "intervals" parameterized by $B \in \mathcal{P}_{n-(h+1)}$:

$$\mathcal{P}_n = \coprod_{B \in \mathcal{P}_{n-(h+1)}} I(t^{h+1}B;h) \tag{5.10}$$

and likewise for monics (recall $h \leq n-2$):

$$\mathcal{M}_n = \coprod_{B \in \mathcal{M}_{n-(h+1)}} I(t^{h+1}B;h) \tag{5.11}$$

5.2. **An involution.** Let $n \geq 0$. We define a map $\theta_n : \mathcal{P}_{\leq n} \to \mathcal{P}_{\leq n}$ by

$$\theta_n(f)(t) = t^n f(\frac{1}{t})$$

which takes $f(t) = f_0 + f_1 t + \cdots + f_n t^n$, $n = \deg f$ to the "reversed" polynomial

$$\theta_n(f)(t) = f_0 t^n + f_1 t^{n-1} + \cdots + f_n \ . \tag{5.12}$$

For $0 \neq f \in \mathbb{F}_q[t]$ we define

$$f^*(t) := t^{\deg f} f(\frac{1}{t}) \tag{5.13}$$

so that $\theta_n(f) = f^*$ if $f(0) \neq 0$. Note that if $f(0) = 0$ then this is false, for example $(t^k)^* = 1$ but $\theta_n(t^k) = t^{n-k}$ if $k \leq n$.

We have $\deg \theta_n(f) \leq n$ with equality if and only if $f(0) \neq 0$. Moreover for $f \neq 0$, $f^*(0) \neq 0$ and $f(0) \neq 0$ if and only if $\deg f^* = \deg f$. Restricted to polynomials which do not vanish at 0, equivalently are co-prime to t, then $*$ is an involution:

$$f^{**} = f, \quad f(0) \neq 0 \ . \tag{5.14}$$

We also have multiplicativity:

$$(fg)^* = f^* g^* \ . \tag{5.15}$$

The map θ_m gives a bijection

$$\begin{aligned} \theta_m : \mathcal{M}_m &\to \{C \in \mathcal{P}_{\leq m} : C(0) = 1\} \\ B &\mapsto \theta_m(B) \end{aligned} \tag{5.16}$$

with polynomials of degree $\leq m$ with constant term 1. Thus as B ranges over $\mathcal{M}_m$, $\theta_m(B)$ ranges over all invertible residue class $C \mod t^{m+1}$ so that $C(0) = 1$.

5.3. Short intervals as arithmetic progressions modulo t^{n-h}.

Suppose $h \leq n-2$. Define the arithmetic progression

$$\mathcal{P}_{\leq n}(t^{n-h}; C) = \{g \in \mathcal{P}_{\leq n} : g \equiv C \mod t^{n-h}\} = C + t^{n-h}\mathcal{P}_{\leq h} \ . \tag{5.17}$$

Note that the progression contains q^{h+1} elements.

Lemma 5.1. *Let $h \leq n-2$ and $B \in \mathcal{M}_{n-h-1}$. Then the map θ_n takes the "interval" $I(t^{h+1}B; h)$ bijectively onto the arithmetic progression $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$, with those $f \in I(t^{h+1}B; h)$ such that $f(0) \neq 0$ mapping onto those $g \in \mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$ of degree exactly n.*

Proof. We first check that θ_n maps the interval $I(t^{h+1}B; h)$ to the arithmetic progression $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$. Indeed if $B = b_0 + \dots + b_{n-h-1}t^{n-h-1}$, with $b_{n-h-1} = 1$, and $f = f_0 + \dots + f_n t^n \in I(t^{h+1}B; h)$ then

$$f = f_0 + \dots + f_h t^h + t^{h+1}(b_0 + \dots + b_{n-h-1}t^{n-h-1}) \tag{5.18}$$

so that

$$\begin{aligned} \theta_n(f) &= f_0 t^n + \dots + f_h t^{n-h} + b_0 t^{n-h-1} + \dots + b_{n-h-1} \\ &= \theta_{n-h-1}(B) \mod t^{n-h} \ . \end{aligned} \tag{5.19}$$

Hence $\theta_n(f) \in \mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$.

Now the map $\theta_n : \mathcal{P}_{\leq n} \to \mathcal{P}_{\leq n}$ is a bijection, and both $I(t^{h+1}B; h)$ and $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$ have size q^{h+1}, and therefore $\theta_n : I(t^{h+1}B; h) \to \mathcal{P}_{\leq n}(t^{n-h}; B^*)$ is a bijection. □

5.4. The mean value.

Lemma 5.2. *The mean value of $\mathcal{N}_\alpha(\bullet; h)$ over $\mathcal{M}_n$ is*

$$\langle \mathcal{N}_\alpha(\bullet; h) \rangle = q^{h+1} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha(f) = H \langle \alpha \rangle_n \ . \tag{5.20}$$

Proof. From the definition, we have

$$
\begin{aligned}
\langle \mathcal{N}_\alpha(\bullet;h)\rangle &= \frac{1}{\#\mathcal{M}_{n-h-1}} \sum_{B\in\mathcal{M}_{n-h-1}} \mathcal{N}_\alpha(t^{h+1}B;h) \\
&= \frac{1}{q^{n-h-1}} \sum_{B\in\mathcal{M}_{n-h-1}} \sum_{f\in I(t^{h+1}B;h)} \alpha(f) \qquad (5.21)\\
&= q^{h+1}\frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\alpha(f) = q^{h+1}\left\langle \alpha\right\rangle_n \ .
\end{aligned}
$$

□

5.5. **A class of arithmetic functions.** Let $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ be a function on polynomials, which is:

- **Even** in the sense that
$$\alpha(cf) = \alpha(f), \quad c \in \mathbb{F}_q^\times \ .$$
- **Multiplicative**, that is $\alpha(fg) = \alpha(f)\alpha(g)$ if f and g are co-prime. In fact we will only need a weaker condition , "weak multiplicativity": If $f(0) \neq 0$, i.e. $\gcd(f,t) = 1$ then
$$\alpha(t^k f) = \alpha(t^k)\alpha(f), \quad f(0) \neq 0 \ .$$
- **Bounded**, that is it satisfies the growth condition
$$\max_{f\in\mathcal{M}_n} |\alpha(f)| \leq A_n$$
independently of q.
- **Symmetric** under the map $f^*(t) := t^{\deg f} f(\frac{1}{t})$,
$$\alpha(f^*) = \alpha(f), \quad f(0) \neq 0 \ .$$

Examples are the Möbius function μ, its square μ^2 which is the indicator function of squarefree-integers, and the divisor functions (see [21]).

Note that multiplicativity (and the "weak multiplicativity" condition) excludes the case of the von Mangoldt function, treated in [22] where we are counting prime polynomials in short intervals or arithmetic progressions. A related case of almost primes was treated by Rodgers [33].

5.6. **A formula for $\mathcal{N}_\alpha(A;h)$.** We present a useful formula for the short interval sums $\mathcal{N}_\alpha(\bullet,h)$ in terms of sums over even Dirichlet characters modulo t^{n-h}. Recall that a Dirichlet character χ is "even" if $\chi(cf) = \chi(f)$ for all scalars $c \in \mathbb{F}_q^\times$, and we say that χ is "odd" otherwise. The number of even characters modulo t^m is $\Phi_{ev}(t^m) = q^{m-1}$. We denote by χ_0 the trivial character.

Lemma 5.3. *If $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ is even, symmetric and weakly multiplicative, and $0 \le h \le n-2$, then for all $B \in \mathcal{M}_{n-h-1}$,*

$$\begin{aligned} \mathcal{N}_\alpha(t^{h+1}B;h) &= \langle \mathcal{N}_\alpha(\bullet;h)\rangle \\ &\quad + \frac{1}{\Phi_{ev}(t^{n-h})}\sum_{m=0}^{n}\alpha(t^{n-m}) \sum_{\substack{\chi \bmod t^{n-h} \\ \chi\neq\chi_0 \ \textit{even}}} \bar{\chi}(\theta_{n-h-1}(B))\mathcal{M}(m;\alpha\chi) \end{aligned} \tag{5.22}$$

where

$$\mathcal{M}(n;\alpha\chi) = \sum_{f\in\mathcal{M}_n}\alpha(f)\chi(f)\ . \tag{5.23}$$

Proof. Writing each $f \in \mathcal{M}_n$ uniquely as $f = t^{n-m}f_1$ with $f_1 \in \mathcal{M}_m$ and $f_1(0) \neq 0$, for which $\theta_n(f) = \theta_m(f_1) = f_1^*$, we obtain, using (weak) multiplicativity,

$$\begin{aligned} \mathcal{N}_\alpha(t^{h+1}B;h) &= \sum_{m=0}^{n} \sum_{\substack{f_1\in\mathcal{M}_m \\ f_1(0)\neq 0 \\ t^{n-m}f_1\in I(t^{h+1}B;h)}} \alpha(t^{n-m}f_1) \\ &= \sum_{m=0}^{n}\alpha(t^{n-m}) \sum_{\substack{f_1\in\mathcal{M}_m \\ f_1(0)\neq 0 \\ t^{n-m}f_1\in I(t^{h+1}B;h)}} \alpha(f_1)\ . \end{aligned} \tag{5.24}$$

Since $f_1(0) \neq 0$, we have that $f_1^* = \theta_m(f_1)$ runs over all polynomials g of degree m (not necessarily monic) so that $g \equiv \theta_{n-h-1}(B) \mod t^{n-h}$ by Lemma 5.1, and moreover $\alpha(f_1) = \alpha(f_1^*) = \alpha(\theta_m(f_1))$. Hence

$$\mathcal{N}_\alpha(t^{h+1}B;h) = \sum_{m=0}^{n}\alpha(t^{n-m}) \sum_{\substack{\deg g=m \\ g\equiv\theta_{n-h-1}(B) \bmod t^{n-h}}} \alpha(g)\ . \tag{5.25}$$

Using characters to pick out the conditions $g \equiv \theta_{n-h-1}(B) \bmod t^{n-h}$ (note that since B is monic, $\theta_{n-h-1}(B)$ is coprime to t^{n-h}) gives

$$\sum_{\substack{\deg g=m \\ g\equiv\theta_{n-h-1}(B) \bmod t^{n-h}}} \alpha(g) = \frac{1}{\Phi(t^{n-h})}\sum_{\chi \bmod t^{n-h}} \bar{\chi}(\theta_{n-h-1}(B))\tilde{\mathcal{M}}(m;\alpha\chi) \tag{5.26}$$

where

$$\tilde{\mathcal{M}}(m;\alpha\chi) = \sum_{\deg g=m}\chi(g)\alpha(g)\ , \tag{5.27}$$

the sum running over all g of degree m.

Since α is even, we find that

$$\begin{aligned}\tilde{\mathcal{M}}(m;\alpha\chi) &= \sum_{f\in\mathcal{M}_m}\sum_{c\in\mathbb{F}_q^\times}\chi(cf)\alpha(cf)\\ &= \sum_{f\in\mathcal{M}_m}\alpha(f)\chi(f)\sum_{c\in\mathbb{F}_q^\times}\chi(c)\\ &= \begin{cases}(q-1)\sum_{f\in\mathcal{M}_m}\alpha(f)\chi(f), & \chi \text{ even}\\ 0, & \chi \text{ odd}\end{cases}\end{aligned}$$

where now the sum is over monic polynomials of degree m.

Thus we get, on noting that $\Phi(t^{n-h})/(q-1)=\Phi_{ev}(t^{n-h})$, that

(5.28)
$$\sum_{\substack{\deg g=m\\ g\equiv\theta_{n-h-1}(B) \mod t^{n-h}}}\alpha(g) = \frac{1}{\Phi_{ev}(t^{n-h})}\sum_{\substack{\chi \bmod t^{n-h}\\ \chi \text{ even}}}\bar\chi(\theta_{n-h-1}(B))\mathcal{M}(m;\alpha\chi)\ .$$

Therefore

(5.29)
$$\mathcal{N}_\alpha(t^{h+1}B;h) = \sum_{m=0}^{n}\alpha(t^{n-m})\frac{1}{\Phi_{ev}(t^{n-h})}\sum_{\substack{\chi \bmod t^{n-h}\\ \chi \text{ even}}}\bar\chi(\theta_{n-h-1}(B))\mathcal{M}(m;\alpha\chi)\ .$$

The trivial character χ_0 contributes a term

$$\frac{1}{\Phi_{ev}(t^{n-h})}\sum_{m=0}^{n}\sum_{\substack{g\in\mathcal{M}_m\\ g(0)\neq 0}}\alpha(t^{n-m})\alpha(g) = \frac{q^{h+1}}{q^n}\sum_{f\in\mathcal{M}_n}\alpha(f) \tag{5.30}$$

on using weak multiplicativity. Inserting this into (5.29) and using Lemma 5.2 we obtain the formula claimed. □

5.7. **Formulae for variance and covariance.** Given an arithmetic function α, the variance of $\mathcal{N}_\alpha$ is

$$\begin{aligned}\operatorname{Var}(\mathcal{N}_\alpha) &= \left\langle |\mathcal{N}_\alpha - \langle\mathcal{N}_\alpha\rangle\,|^2\right\rangle\\ &= \frac{1}{q^{n-h-1}}\sum_{B\in\mathcal{M}_{n-h-1}}|\mathcal{N}_\alpha(t^{h+1}B;h)-\langle\mathcal{N}_\alpha\rangle\,|^2\end{aligned} \tag{5.31}$$

and likewise given two such functions α,β, the covariance of $\mathcal{N}_\alpha$ and $\mathcal{N}_\beta$ is

$$\operatorname{cov}(\mathcal{N}_\alpha,\mathcal{N}_\beta) = \left\langle\Big(\mathcal{N}_\alpha - \langle\mathcal{N}_\alpha\rangle\Big)\Big(\mathcal{N}_\beta - \langle\mathcal{N}_\beta\rangle\Big)\right\rangle\ . \tag{5.32}$$

We use the following lemma, an extension of the argument of [22]:

Lemma 5.4. *If α,β are even, symmetric and weakly multiplicative, and $0\leq h\leq n-2$, then*

$$\operatorname{cov}(\mathcal{N}_\alpha,\mathcal{N}_\beta) = \frac{1}{\Phi_{ev}(t^{n-h})^2}\sum_{\substack{\chi \bmod t^{n-h}\\ \chi\neq\chi_0 \text{ even}}}\sum_{m_1,m_2=0}^{n}\alpha(t^{n-m_1})\overline{\beta(t^{n-m_2})}\mathcal{M}(m_1;\alpha\chi)\overline{\mathcal{M}(m_2;\beta\chi)}\ . \tag{5.33}$$

Proof. By Lemma 5.3, $\operatorname{cov}(\mathcal{N}_\alpha,\mathcal{N}_\beta)$ equals

$$\frac{1}{\Phi_{ev}(t^{n-h})^2}\sum_{\substack{\chi_1,\chi_2 \bmod t^{n-h}\\ \chi_1,\chi_2\neq\chi_0 \text{ even}}}\sum_{m_1,m_2=0}^{n}\alpha(t^{n-m_1})\overline{\beta(t^{n-m_2})}\mathcal{M}(m_1;\alpha\chi_1)\overline{\mathcal{M}(m_2;\beta\chi_2)}$$
$$\times\frac{1}{q^{n-h-1}}\sum_{B\in\mathcal{M}_{n-h-1}}\bar\chi_1(\theta_{n-h-1}(B))\chi_2(\theta_{n-h-1}(B))\ .$$

As B runs over the monic polynomials $\mathcal{M}_{n-h-1}$, the image $\theta_{n-h-1}(B)$ runs over all polynomials $C \bmod t^{n-h}$ with $C(0)=1$ (see (5.16)). Thus

$$\sum_{B\in\mathcal{M}_{n-h-1}}\bar\chi_1(\theta_{n-h-1}(B))\chi_2(\theta_{n-h-1}(B)) = \sum_{\substack{C \bmod t^{n-h}\\ C(0)=1}}\bar\chi_1(C)\chi_2(C)\ . \tag{5.34}$$

Since χ_1,χ_2 are both even, we may ignore the condition $C(0)=1$ and use the orthogonality relation (recall $\Phi_{ev}(t^{n-h})=q^{n-h-1}$) to get (see [22, Lemma 3.2])

$$\frac{1}{q^{n-h-1}}\sum_{\substack{C \bmod t^{n-h}\\ C(0)=1}}\bar\chi_1(C)\chi_2(C) = \delta(\chi_1,\chi_2) \tag{5.35}$$

so that

$$\operatorname{cov}(\mathcal{N}_\alpha,\mathcal{N}_\beta) = \frac{1}{\Phi_{ev}(t^{n-h})^2}\sum_{\substack{\chi \bmod t^{n-h}\\ \chi\neq\chi_0 \text{ even}}}\sum_{m_1,m_2=0}^{n}\alpha(t^{n-m_1})\overline{\beta(t^{n-m_2})}\mathcal{M}(m_1;\alpha\chi)\overline{\mathcal{M}(m_2;\beta\chi)} \tag{5.36}$$

as claimed. □

6. Characters, L-functions and equidistribution

Before applying the variance formulae of § 5.7, we survey some background on Dirichlet characters, their L-functions and recent equidistribution theorems due to N. Katz.

6.1. **Background on Dirichlet characters and L-functions.** Recall that a Dirichlet character χ is "even" if $\chi(cf) = \chi(f)$ for all scalars $c \in \mathbb{F}_q^\times$, and we say that χ is "odd" otherwise. The number of even characters modulo t^m is $\Phi_{ev}(t^m) = q^{m-1}$. We denote by χ_0 the trivial character.

A character χ is *primitive* if there is no proper divisor $Q' \mid Q$ so that $\chi(F) = 1$ whenever F is coprime to Q and $F = 1 \mod Q'$. We denote by $\Phi_{prim}(Q)$ the number of primitive characters modulo Q. As $q \to \infty$, almost all characters are primitive in the sense that

$$\frac{\Phi_{prim}(Q)}{\Phi(Q)} = 1 + O(\frac{1}{q}) \ , \tag{6.1}$$

the implied constant depending only on $\deg Q$.

Moreover, as $q \to \infty$ with $\deg Q$ fixed, almost all characters are primitive and odd:

$$\frac{\Phi_{prim}^{odd}(Q)}{\Phi(Q)} = 1 + O(\frac{1}{q}) \ , \tag{6.2}$$

the implied constant depending only on $\deg Q$.

One also has available similar information about the number $\Phi_{prim}^{ev}(Q)$ of even primitive characters. What we will need to note is that for $Q(t) = t^m$, $m \geq 2$,

$$\Phi_{prim}^{ev}(t^m) = q^{m-2}(q-1) \ . \tag{6.3}$$

The L-function $L(u, \chi)$ attached to χ is defined as

$$L(u, \chi) = \prod_{P \nmid Q} (1 - \chi(P) u^{\deg P})^{-1} \tag{6.4}$$

where the product is over all monic irreducible polynomials in $\mathbb{F}_q[t]$. The product is absolutely convergent for $|u| < 1/q$. If $\chi = \chi_0$ is the trivial character modulo Q, then

$$L(u, \chi_0) = Z(u) \prod_{P \mid Q} (1 - u^{\deg P}) \ , \tag{6.5}$$

where

$$Z(u) = \prod_{P \text{ prime}} (1 - u^{\deg P})^{-1} = \frac{1}{1 - qu}$$

is the zeta function of $\mathbb{F}_q[t]$. Also set $\zeta_q(s) := Z(q^{-s})$.

If $Q \in \mathbb{F}_q[t]$ is a polynomial of degree $\deg Q \geq 2$, and $\chi \neq \chi_0$ a nontrivial character mod Q, then the L-function $L(u, \chi)$ is a polynomial in u of degree $\deg Q - 1$. Moreover, if χ is an "even" character, then there is a "trivial" zero at $u = 1$.

We may factor $L(u, \chi)$ in terms of the inverse roots

$$L(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j(\chi) u) \ . \tag{6.6}$$

The Riemann Hypothesis, proved by Andre Weil (1948), is that for each (nonzero) inverse root, either $\alpha_j(\chi)=1$ or

$$|\alpha_j(\chi)| = q^{1/2} \; . \tag{6.7}$$

If χ is a *primitive* and *odd* character modulo Q, then all inverse roots α_j have absolute value $\sqrt{q}$, and for χ primitive and *even* the same holds except for the trivial zero at 1. We then write the nontrivial inverse roots as $\alpha_j = q^{1/2}e^{i\theta_j}$ and define a unitary matrix

$$\Theta_\chi = \operatorname{diag}(e^{i\theta_1},\dots,e^{i\theta_N}) \; . \tag{6.8}$$

which determines a unique conjugacy class in the unitary group $U(N)$, where $N=\deg Q-1$ for χ odd, and $N=\deg Q-2$ for χ even. The unitary matrix Θ_χ (or rather, the conjugacy class of unitary matrices) is called the unitarized Frobenius matrix of χ.

6.2. **Katz's equidistribution theorems.**

Crucial ingredients in our results on the variance are equidistribution and independence results for the Frobenii Θ_χ due to N. Katz.

Theorem 6.1. *i)* [18] *Fix*[3] *$m \geq 4$. The unitarized Frobenii Θ_χ for the family of even primitive characters mod T^{m+1} become equidistributed in the projective unitary group $PU(m-1)$ of size $m-1$, as $q\to\infty$.*

ii) [19] *If $m\geq 5$ and in addition the q's are coprime to* 6*, then the set of pairs of conjugacy classes $(\Theta_\chi,\Theta_{\chi^2})$ become equidistributed in the space of conjugacy classes of the product $PU(m-1)\times PU(m-1)$.*

For odd characters, the corresponding equidistribution and independence results are

Theorem 6.2. *i)* [17] *Fix $m\geq 2$. Suppose we are given a sequence of finite fields $\mathbb{F}_q$ and squarefree polynomials $Q(T)\in\mathbb{F}_q[T]$ of degree m. As $q\to\infty$, the conjugacy classes Θ_χ with χ running over all primitive odd characters modulo Q, are uniformly distributed in the unitary group $U(m-1)$.*

ii) [20] *If in addition we restrict to q odd, then the set of pairs of conjugacy classes $(\Theta_\chi,\Theta_{\chi^2})$ become equidistributed in the space of conjugacy classes of the product $U(m-1)\times U(m-1)$.*

7. Variance of the Möbius function in short intervals

For $n\geq 2$, the mean value of $\mathcal{N}_\mu(A;h)$ over all $A\in\mathcal{M}_n$ is :

$$\langle \mathcal{N}_\mu(\bullet;h)\rangle = 0 \; . \tag{7.1}$$

Indeed, by Lemma 5.2

$$\langle \mathcal{N}_\mu(\bullet;h)\rangle = \frac{H}{q^n}\sum_{f\in\mathcal{M}_n}\mu(f) \; . \tag{7.2}$$

[3] If the characteristic of $\mathbb{F}_q$ is different than 2 or 5 then the result also holds for $m=3$.

Now as is well known and easy to see, for $n \geq 2$,

$$\sum_{f \in \mathcal{M}_n} \mu(f) = 0 \ , \tag{7.3}$$

hence we obtain (7.1).

We will show that the variance is

Theorem 7.1. *If* $0 \leq h \leq n-5$ *then*

$$\operatorname{Var} \mathcal{N}_\mu(\bullet; h) \sim H, \quad q \to \infty \tag{7.4}$$

We use the general formula of Lemma 5.4 which gives

$$\operatorname{Var}(\mathcal{N}_\mu(\bullet; h)) = \frac{1}{q^{2(n-h-1)}} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \neq \chi_0 \text{ even}}} |\mathcal{M}(n; \mu\chi) - \mathcal{M}(n-1; \mu\chi)|^2 \tag{7.5}$$

where

$$\mathcal{M}(n; \mu\chi) = \sum_{f \in \mathcal{M}_n} \mu(f)\chi(f) \ . \tag{7.6}$$

We claim that

Lemma 7.2. *Suppose that* χ *is a primitive even character modulo* t^{n-h}. *Then*

$$\mathcal{M}(n; \mu\chi) = \sum_{k=0}^{n} q^{k/2} \operatorname{tr} \operatorname{Sym}^k \Theta_\chi \tag{7.7}$$

where Sym^n *is the symmetric* n*-th power representation* ($n = 0$ *corresponds to the trivial representation). In particular,*

$$\mathcal{M}(n; \mu\chi) - \mathcal{M}(n-1; \mu\chi) = q^{n/2} \operatorname{tr} \operatorname{Sym}^n \Theta_\chi \ . \tag{7.8}$$

If $\chi \neq \chi_0$ *is not primitive, then*

$$|\mathcal{M}(n; \mu\chi)| \ll_n q^{n/2} \ . \tag{7.9}$$

Proof. We compute the generating function

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu\chi) u^n = \sum_{f \text{ monic}} \chi(f)\mu(f) u^{\deg f} = \frac{1}{L(u, \chi)} \tag{7.10}$$

where $L(u, \chi) = \sum_{f \text{ monic}} \chi(f) u^{\deg f}$ is the associated Dirichlet L-function. Now if χ is *primitive* and *even*, then

$$L(u, \chi) = (1-u) \det(I - uq^{1/2}\Theta_\chi) \tag{7.11}$$

where $\Theta_\chi \in U(n-h-2)$ is the unitarized Frobenius class. Therefore we find

$$(1-u) \sum_{n=0}^{\infty} \mathcal{M}(n; \mu\chi) u^n = \frac{1}{\det(I - uq^{1/2}\Theta_\chi)} = \sum_{k=0}^{\infty} q^{k/2} \operatorname{tr} \operatorname{Sym}^k \Theta_\chi u^k \ , \tag{7.12}$$

where we have used the identity

$$\frac{1}{\det(I-uA)} = \sum_{k=0}^{\infty} u^k \operatorname{tr}\operatorname{Sym}^k A \ . \tag{7.13}$$

Comparing coefficients gives (7.7).

For non-primitive but non-trivial characters $\chi \neq \chi_0$, the L-function still has the form $L(u,\chi) = \prod_{j=1}^{n-h-1}(1-\alpha_j u)$ with all inverse roots $|\alpha_j| \leq \sqrt{q}$, and hence we obtain (7.9). □

We can now compute the variance using (7.5). We start by bounding the contribution of non-primitive characters, whose number is $O(\frac{1}{q}\Phi_{\mathrm{ev}}(t^{n-h})) = O(q^{n-h-2})$, and by (7.9) each contributes $O(q^n)$ to the sum in (7.5), hence the total contribution of non-primitive characters is bounded by $O_n(q^h)$. Consequently we find

$$\operatorname{Var}\mathcal{N}_\mu(\bullet;h) = \frac{q^{h+1}}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ even and primitive}}} |\operatorname{tr}\operatorname{Sym}^n \Theta_\chi|^2 + O(q^h) \ . \tag{7.14}$$

Using Theorem 6.1(i) we get, once we replace the projective group by the unitary group,

$$\lim_{q\to\infty} \frac{\operatorname{Var}(\mathcal{N}_\mu(\bullet;h))}{q^{h+1}} = \int\limits_{U(n-h-2)} |\operatorname{tr}\operatorname{Sym}^n U|^2\, dU \ . \tag{7.15}$$

Note that by Schur-Weyl duality (and Weyl's unitary trick), Sym^n is an *irreducible* representation. Hence

$$\int\limits_{U(n-h-2)} |\operatorname{tr}\operatorname{Sym}^n U|^2\, dU = 1 \tag{7.16}$$

and we conclude that $\operatorname{Var}(\mathcal{N}_\mu(\bullet;h)) \sim q^{h+1} = H$, as claimed.

8. Variance of the Möbius function in arithmetic progressions

We define

$$\mathcal{S}_{\mu,n,Q}(A) = \mathcal{S}_\mu(A) = \sum_{\substack{f\in\mathcal{M}_n \\ f=A \bmod Q}} \mu(f) \ .$$

Theorem 8.1. *If $n \geq \deg Q \geq 2$ then the mean value of $\mathcal{S}_\mu(A)$ tends to 0 as $q\to\infty$, and*

$$\operatorname{Var}_Q(\mathcal{S}_\mu) \sim \frac{q^n}{\Phi(Q)} \int\limits_{U(Q-1)} \Big|\operatorname{tr}\operatorname{Sym}^n U\Big|^2 dU = \frac{q^n}{\Phi(Q)} \ . \tag{8.1}$$

The mean value over all residues coprime to Q is

$$\langle \mathcal{S}_\mu \rangle = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,Q)=1}} \mu(f) = \frac{1}{\Phi(Q)}\mathcal{M}(n,\mu\chi_0) \ . \tag{8.2}$$

To evaluate this quantity, we consider the generating function

$$\begin{aligned} \sum_{n=0}^\infty \mathcal{M}(n,\mu\chi_0)u^n &= \sum_{\gcd(f,Q)=1} \mu(f)u^{\deg f} \\ &= \prod_{P\nmid Q}(1-u^{\deg P}) = \frac{1-qu}{\prod_{P\mid Q}(1-u^{\deg P})} \\ &= \frac{1-qu}{\prod_k(1-u^k)^{\lambda_k}} \end{aligned} \tag{8.3}$$

where λ_k is the number of prime divisors of Q of degree k. Using the expansion

$$\frac{1}{(1-z)^\lambda} = \sum_{n=0}^\infty \binom{n+\lambda-1}{\lambda-1} z^n$$

gives

$$\frac{1}{\prod_k(1-u^k)^{\lambda_k}} = \sum_{n=0}^\infty C(n)u^n$$

with

$$C(n) = \sum_{\sum_k kn_k=n} \prod_k \binom{n_k+\lambda_k-1}{\lambda_k-1}$$

and hence for $n\geq 1$,

$$\mathcal{M}(n,\mu\chi_0) = C(n)-qC(n-1) \ .$$

Thus we find that for $n\geq 1$,

$$\langle \mathcal{S}_\mu \rangle = \frac{C(n)-qC(n-1)}{\Phi(Q)} \tag{8.4}$$

and in particular for $\deg Q>1$,

$$|\,\langle \mathcal{S}_\mu \rangle\,| \ll \frac{q}{|Q|} \to 0, \quad q\to\infty \ . \tag{8.5}$$

For the variance we use (4.11) which gives

$$\mathrm{Var}_Q(\mathcal{S}_\mu) = \frac{1}{\Phi(Q)^2} \sum_{\chi\neq\chi_0} |\mathcal{M}(n;\mu\chi)|^2 \ . \tag{8.6}$$

As in (7.10), the generating function of $\mathcal{M}(n;\mu\chi)$ is $1/L(u,\chi)$. Now for χ odd and primitive, $L(u,\chi)=\det(I-uq^{1/2}\Theta_\chi)$ with $\Theta_\chi\in U(\deg Q-1)$ unitary. Hence for χ odd and primitive,

$$\mathcal{M}(n;\mu\chi) = q^{n/2}\operatorname{tr}\operatorname{Sym}^n\Theta_\chi \ . \tag{8.7}$$

For $\chi \neq \chi_0$ which is not odd and primitive, we can still write $L(u,\chi) = \prod_{j=1}^{\deg Q-1}(1-\alpha_j u)$ with all inverse roots $|\alpha_j| \leq \sqrt{q}$, and hence for $\chi \neq \chi_0$ we have a bound

$$|\mathcal{M}(n;\mu\chi)| \ll_n q^{n/2} \ . \tag{8.8}$$

The number of even characters is $\Phi_{\mathrm{ev}}(Q) = \Phi(Q)/(q-1)$ and the number of non-primitive characters is $O(\Phi(Q)/q)$, hence the number of characters which are not odd and primitive is $O(\Phi(Q)/q)$. Inserting the bound (8.8) into (8.6) shows that the contribution of such characters is $O(q^{n-1}/\Phi(Q))$. Hence

$$\operatorname{Var}_Q \mathcal{S}_\mu = \frac{q^n}{\Phi(Q)}\frac{1}{\Phi(Q)} \sum_{\chi \text{ odd primitive}} |\operatorname{tr}\operatorname{Sym}^n \Theta_\chi|^2 + O(\frac{q^{n-1}}{\Phi(Q)}) \ . \tag{8.9}$$

Using Theorem 6.2(i) gives that as $q \to \infty$,

$$\operatorname{Var}_Q \mathcal{S}_\mu \sim \frac{q^n}{\Phi(Q)} \int\limits_{U(Q-1)} \Big|\operatorname{tr}\operatorname{Sym}^n U\Big|^2 dU = \frac{q^n}{\Phi(Q)} \ . \tag{8.10}$$

9. The variance of squarefrees in short intervals

In this section we study the variance of the number of squarefree polynomials in short intervals. The total number of squarefree monic polynomials of degree $n > 1$ is (exactly)

$$\sum_{f \in \mathcal{M}_n} \mu(f)^2 = \frac{q^n}{\zeta_q(2)} = q^n(1-\frac{1}{q}) \ . \tag{9.1}$$

The number of squarefree polynomials in the short interval $I(A;h)$ is

$$\mathcal{N}_{\mu^2}(A;h) = \sum_{f \in I(A;h)} \mu(f)^2 \ . \tag{9.2}$$

Theorem 9.1. *Let $0 \leq h \leq n-6$. Assume $q \to \infty$ with all q's coprime to 6.*

i) If h is even then

$$\operatorname{Var}\mathcal{N}_{\mu^2}(\bullet;h) \sim q^{\frac{h}{2}} \int\limits_{U(n-h-2)} \Big|\operatorname{tr}\operatorname{Sym}^{\frac{h}{2}+1} U\Big|^2 dU = \frac{\sqrt{H}}{\sqrt{q}} \ . \tag{9.3}$$

ii) If h is odd then

$$\begin{aligned}\operatorname{Var}\mathcal{N}_{\mu^2}(\bullet;h) &\sim q^{\frac{h-1}{2}} \int\limits_{U(n-h-2)} |\operatorname{tr} U|^2 dU \int\limits_{U(n-h-2)} |\operatorname{tr}\operatorname{Sym}^{\frac{h+3}{2}} U'|^2 dU' \\ &= \frac{\sqrt{H}}{q} \ .\end{aligned} \tag{9.4}$$

Proof. To compute the variance, we use Lemma 5.4. Since $\mu^2(t^m) = 1$ for $m = 0, 1$ and equals 0 for $m > 1$, we obtain

$$\operatorname{Var}(\mathcal{N}_{\mu^2}(\bullet; h)) = \frac{1}{\Phi_{ev}(t^{n-h})^2} \sum_{\substack{\chi \neq \chi_0 \bmod t^{n-h} \\ \text{even}}} |\mathcal{M}(n; \mu^2\chi) + \mathcal{M}(n-1; \mu^2\chi)|^2 \tag{9.5}$$

where

$$\mathcal{M}(n; \mu^2\chi) = \sum_{f \in \mathcal{M}_n} \mu(f)^2 \chi(f) \; . \tag{9.6}$$

To obtain an expression for $\mathcal{M}(n; \mu^2\chi)$, we consider the generating function

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu^2\chi) u^n = \sum_f \mu(f)^2 \chi(f) u^{\deg f} = \frac{L(u, \chi)}{L(u^2, \chi^2)} \; . \tag{9.7}$$

Assume that χ is primitive, and that χ^2 is also[4] primitive (modulo t^{n-h}). Then

$$L(u, \chi) = (1-u) \det(I - uq^{1/2}\Theta_\chi), \quad L(u^2, \chi^2) = (1-u^2) \det(I - u^2 q^{1/2} \Theta_{\chi^2}) \; .$$

Writing for $U \in U(N)$

$$\det(I - xU) = \sum_{j=0}^{N} \lambda_j(U) x^j, \quad \frac{1}{\det(I - xU)} = \sum_{k=0}^{\infty} \operatorname{tr} \operatorname{Sym}^k U x^k \tag{9.8}$$

gives, on abbreviating

$$\lambda_j(\chi) := \lambda_j(\Theta_\chi), \quad \operatorname{Sym}^k(\chi^2) = \operatorname{tr} \operatorname{Sym}^k \Theta_{\chi^2}$$

that

$$\begin{aligned} \frac{L(u, \chi)}{L(u^2, \chi^2)} &= \frac{\det(I - uq^{1/2}\Theta_\chi)}{(1+u) \det(I - u^2 q^{1/2} \Theta_{\chi^2})} \\ &= \sum_{m=0}^{\infty} \sum_{0 \le j \le N} \sum_{k=0}^{\infty} (-1)^m \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{(j+k)/2} u^{m+j+2k} \end{aligned}$$

and hence

$$\mathcal{M}(n; \mu^2\chi) = (-1)^n \sum_{\substack{j+2k \le n \\ 0 \le j \le N \\ k \ge 0}} (-1)^j \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{(j+k)/2} \; . \tag{9.9}$$

[4] If q is odd then primitivity of χ and of χ^2 are equivalent.

Therefore

$$\begin{aligned}\mathcal{M}(n;\mu^2\chi)+\mathcal{M}(n-1;\mu^2\chi) &= (-1)^n \sum_{\substack{j+2k\leq n\\ 0\leq j\leq N\\ k\geq 0}} (-1)^j \lambda_j(\chi)\operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}\\ &\quad + (-1)^{n-1} \sum_{\substack{j+2k\leq n-1\\ 0\leq j\leq N\\ k\geq 0}} (-1)^j \lambda_j(\chi)\operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}\\ &= (-1)^n \sum_{\substack{j+2k= n\\ 0\leq j\leq N\\ k\geq 0}} (-1)^j \lambda_j(\chi)\operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}\\ &= q^{n/4} \sum_{\substack{0\leq j\leq N\\ j=n \bmod 2}} \lambda_j(\chi)\operatorname{Sym}^{\frac{n-j}{2}}(\chi^2) q^{j/4}\ .\end{aligned}$$

Therefore, recalling that $N=n-h-2$,

$$\begin{aligned}&\mathcal{M}(n;\mu^2\chi)+\mathcal{M}(n-1;\mu^2\chi)\\ &= (-1)^n \begin{cases} q^{\frac{n}{2}-\frac{h+1}{4}-\frac{1}{4}}\lambda_N(\chi)\operatorname{Sym}^{\frac{h+2}{2}}(\chi^2), & n=N \bmod 2\\ q^{\frac{n}{2}-\frac{h+1}{4}-\frac{1}{2}}\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{h+3}{2}}(\chi^2), & n\neq N \bmod 2\end{cases} \times(1+O(q^{-1/2}).\end{aligned}$$

Noting that $n=N \bmod 2$ is equivalent to h even, we finally obtain

$$\begin{aligned}&|\mathcal{M}(n;\mu^2\chi)+\mathcal{M}(n-1;\mu^2\chi)|^2\\ &\quad= \begin{cases} q^{n-\frac{h+1}{2}-\frac{1}{2}}|\lambda_N(\chi)\operatorname{Sym}^{\frac{h+2}{2}}(\chi^2)|^2, & h \text{ even}\\ q^{n-\frac{h+1}{2}-1}|\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{h+3}{2}}(\chi^2)|^2, & h \text{ odd}\end{cases} \times (1+O(q^{-1/2})\ .\end{aligned}\tag{9.10}$$

Inserting (9.10) into (9.5) gives an expression for the variance, up to terms which are smaller by $q^{-1/2}$. The contribution of non-primitive characters is bounded as in previous sections and we skip this verification. We separate cases according to h even or odd.

9.0.1. *h even.* We have $|\lambda_N(\chi)|=|\det\Theta_\chi|=1$, so that

$$\operatorname{Var}\mathcal{N}_{\mu^2}(\bullet;h)\sim q^{\frac{h}{2}}\frac{1}{\Phi_{ev}(t^{n-h})}\sum_{\substack{\chi \bmod t^{n-h}\\ \text{primitive even}}}|\operatorname{Sym}^{\frac{h+2}{2}}(\chi^2)|^2\ .\tag{9.11}$$

Here change variables $\chi\mapsto\chi^2$, which is an automorphism of the group of even characters if q is odd, since then the order of the group is $\Phi_{ev}(t^{n-h})=q^{n-h-1}$ is odd. Using Theorem 6.1(i) for even primitive characters modulo t^{n-h} allows us to replace the average over characters by a matrix integral, leading to

$$\operatorname{Var}\mathcal{N}_{\mu^2}(\bullet;h)\sim q^{\frac{h}{2}}\int\limits_{U(n-h-2)}\left|\operatorname{tr}\operatorname{Sym}^{\frac{h}{2}+1}U\right|^2 dU\ .\tag{9.12}$$

Since the symmetric powers Sym^k are irreducible representations, the matrix integral works out to be 1. Hence (with $H = q^{h+1}$)

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\bullet; h) \sim q^{h/2} = \frac{\sqrt{H}}{\sqrt{q}} \ . \tag{9.13}$$

9.0.2. *h odd.* Next, assume h is odd. Then

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\bullet; h) \sim q^{\frac{h-1}{2}} \frac{1}{\Phi_{ev}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \text{primitive even}}} |\lambda_{N-1}(\chi) \operatorname{Sym}^{\frac{h+3}{2}}(\chi^2)|^2 \ . \tag{9.14}$$

Note that $|\lambda_{N-1}(U)| = |\operatorname{tr} U|$, because $\lambda_{N-1}(U) = (-1)^{N-1} \det U \operatorname{tr} U^{-1}$ and for unitary matrices, $|\det U| = 1$ and $\operatorname{tr} U^{-1} = \overline{\operatorname{tr} U}$.

We now use Theorem 6.1(ii), which asserts that, for $0 \le h \le n-6$ and $q \to \infty$ with q coprime to 6, both Θ_χ and Θ_{χ^2} are uniformly distributed in $PU(n-h-2)$ and that Θ_χ, Θ_{χ^2} are *independent.* We obtain

$$\begin{aligned} \operatorname{Var} \mathcal{N}_{\mu^2}(\bullet; h) &\sim q^{\frac{h-1}{2}} \int\limits_{U(n-h-2)} |\operatorname{tr} U|^2 dU \int\limits_{U(n-h-2)} |\operatorname{tr} \operatorname{Sym}^{\frac{h+3}{2}} U'|^2 dU' \\ &= \frac{\sqrt{H}}{q} \end{aligned} \tag{9.15}$$

by irreducibility of the symmetric power representations. □

10. SQUAREFREES IN ARITHMETIC PROGRESSIONS

As in previous sections, we set

$$\mathcal{S}(A) = \sum_{\substack{f = A \bmod Q \\ f \in \mathcal{M}_n}} \mu^2(f) \ . \tag{10.1}$$

We have the expected value

$$\langle \mathcal{S} \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f,Q)=1}} \mu^2(f) \sim \frac{q^n/\zeta_q(2)}{\Phi(Q)} \sim \frac{q^n}{|Q|} \tag{10.2}$$

and the variance

$$\operatorname{Var}_Q(\mathcal{S}) = \frac{1}{\Phi(Q)^2} \sum_{\chi \ne \chi_0} |\mathcal{M}(n; \mu^2 \chi)|^2 \ . \tag{10.3}$$

Theorem 10.1. *Fix $N \ge 1$. For any sequence of finite fields $\mathbb{F}_q$, with q odd, and squarefree polynomials $Q \in \mathbb{F}_q[t]$ with $\deg Q = N+1$, as $q \to \infty$,*

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}} \times \begin{cases} 1/\sqrt{q}, & n \ne \deg Q \bmod 2 \\ \\ 1/q, & n = \deg Q \bmod 2 \ . \end{cases}$$

Proof. The generating function of $\mathcal{M}(n;\mu^2\chi)$ is

$$\sum_{n=0}^{\infty}\mathcal{M}(n;\mu^2\chi)u^n=\sum_f \mu(f)^2\chi(f)u^{\deg f}=\frac{L(u,\chi)}{L(u^2,\chi^2)}\ . \tag{10.4}$$

If both χ, χ^2 are primitive, odd, characters (which happens for almost all χ), then

$$L(u,\chi)=\det(I-uq^{1/2}\Theta_\chi),\quad L(u^2,\chi^2)=\det(I-u^2q^{1/2}\Theta_{\chi^2}) \tag{10.5}$$

and writing (with $N=\deg Q-1$)

$$\det(I-uq^{1/2}\Theta_\chi)=\sum_{j=0}^{N}\lambda_j(\chi)q^{j/2}u^j \tag{10.6}$$

$$\frac{1}{\det(I-q^{1/2}u^2\Theta_{\chi^2})}=\sum_{k=0}^{\infty}\operatorname{Sym}^k(\chi^2)q^{k/2}u^{2k} \tag{10.7}$$

we get, for $n\geq N$, (which is the interesting range)

$$\begin{aligned}\mathcal{M}(n;\mu^2\chi)&=\sum_{\substack{j+2k=n\\0\leq j\leq N\\k\geq 0}}\lambda_j(\chi)\operatorname{Sym}^k(\chi^2)q^{\frac{j+k}{2}}\\&=q^{n/4}\sum_{\substack{j=0\\j=n\bmod 2}}^{N}\lambda_j(\chi)\operatorname{Sym}^{\frac{n-j}{2}}(\chi^2)q^{j/4}\end{aligned} \tag{10.8}$$

and hence

$$\mathcal{M}(n;\mu^2\chi)= \tag{10.9}$$
$$(1+O(q^{-\frac12}))\times q^{\frac{n+N}{4}}\begin{cases}\lambda_N(\chi)\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2), & n=N\bmod 2\\[2ex] q^{-\frac14}\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2), & n\neq N\bmod 2\end{cases}$$

Since $\lambda_N(\chi)=\det\Theta_\chi$, which has absolute value one, we find

$$|\mathcal{M}(n;\mu^2\chi)|^2= \tag{10.10}$$
$$(1+O(q^{-\frac12}))\times q^{\frac{n+N}{2}}\begin{cases}|\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2, & n=N\bmod 2\\[2ex] q^{-\frac12}|\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2)|^2, & n\neq N\bmod 2\ .\end{cases}$$

If $\chi\neq\chi_0$ is not odd, or not primitive, we may use the same computation to show that

$$|\mathcal{M}(n;\mu^2\chi)|\ll_n q^{(n+N)/4},\quad \chi\neq\chi_0 \text{ even or imprimitive.} \tag{10.11}$$

We thus have a formula for $\mathrm{Var}(\mathcal{S})$. We may neglect the contribution of characters χ for which χ or χ^2 are non-primitive, or even as these form a proportion $\leq 1/q$ of all characters, and thus their contribution is

$$\ll \frac{1}{\Phi(Q)}\frac{1}{q}q^{(n+N)/2} \ll \frac{1}{q}\frac{q^{n/2}}{|Q|^{1/2}\sqrt{q}}$$

which is negligible relative to the claimed main term in the Theorem.

To handle the contribution of primitive odd characters we invoke Theorem 6.2(ii) which asserts that both Θ_χ and Θ_{χ^2} are uniformly distributed in $U(\deg Q - 1)$ and are independent (for q odd). To specify the implications, we separate into cases:

If $n = N \bmod 2$ (i.e. $n \neq \deg Q \bmod 2$) then

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}q^{1/2}} \cdot \frac{1}{\Phi(Q)} \sum_{\chi,\chi^2 \text{ primitive}} |\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2 \,. \tag{10.12}$$

By equidistribution

$$\frac{1}{\Phi(Q)} \sum_{\chi,\chi^2 \text{ primitive}} |\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2 \sim \int\limits_{U(N)} \left|\operatorname{tr}\operatorname{Sym}^{\frac{n-N}{2}} U\right|^2 dU \,. \tag{10.13}$$

Note that $\int_{U(N)} \left|\operatorname{tr}\operatorname{Sym}^{\frac{n-N}{2}} U\right|^2 dU = 1$ by irreducibility of Sym^k. Thus we obtain

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}q^{1/2}}, \quad n \neq \deg Q \bmod 2 \,. \tag{10.14}$$

If $n \neq N \bmod 2$ (i.e. $n = \deg Q \bmod 2$), then we get

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{q|Q|^{1/2}}\frac{1}{\Phi(Q)} \sum_{\chi,\chi^2 \text{ primitive}} \left|\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2)\right|^2 \,. \tag{10.15}$$

Note that as in § 9, $|\lambda_{N-1}(\chi)| = |\operatorname{tr}\Theta_\chi|$. By Theorem 6.2(ii),

$$\frac{1}{\Phi(Q)} \sum_{\chi,\chi^2 \text{ primitive}} \left|\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2)\right|^2 \sim \iint\limits_{U(N)\times U(N)} |\operatorname{tr} U|^2 \cdot \left|\operatorname{tr}\operatorname{Sym}^{\frac{n-N+1}{2}} U'\right|^2 dU dU' = 1 \tag{10.16}$$

and hence

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{q|Q|^{1/2}} \,. \tag{10.17}$$

Thus we find

$$\operatorname{Var}_Q(\mathcal{S}) \sim \begin{cases} \frac{q^{n/2}}{|Q|^{1/2}q^{1/2}}, & n \neq \deg Q \bmod 2 \\ \\ \frac{q^{n/2}}{|Q|^{1/2}q}, & n = \deg Q \bmod 2 \end{cases} \tag{10.18}$$

as claimed. □

Appendix A. Hall's theorem for $\mathbb{F}_q[t]$: The large degree limit

Let $Q(n, H)$ be the number of squarefree integers in an interval of length H about n:

$$Q(n, H) := \sum_{j=1}^{H} \mu^2(n + j) \ . \tag{A.1}$$

Hall [12] studied the variance of $Q(n, H)$ as n varies up to X. He showed that provided $H = O(X^{2/9-o(1)})$, the variance grows like $\sqrt{H}$ and in fact admits an asymptotic formula:

$$\frac{1}{X} \sum_{n \leq X} \left| Q(n, H) - \frac{H}{\zeta(2)} \right|^2 \sim A\sqrt{H} \tag{A.2}$$

with

$$A = \frac{\zeta(3/2)}{\pi} \prod_p (1 - \frac{3}{p^2} + \frac{2}{p^3}) \ . \tag{A.3}$$

We give a version of Hall's theorem for the polynomial ring $\mathbb{F}_q[t]$ with q fixed. Let

$$\mathcal{N}(A) = \sum_{|f-A| \leq q^h} \mu^2(f)$$

be the number of squarefree polynomials in a short interval $I(A; h)$ around $A \in \mathcal{M}_n$, with $h \leq n - 2$. Note that

$$\#I(A; h) = q^{h+1} =: H \ .$$

We wish to compute the variance of $\mathcal{N}$ as we average over all short intervals with q fixed and $n \to \infty$.

Let

$$\beta_q = \prod_P (1 - \frac{3}{|P|^2} + \frac{2}{|P|^3}) \ . \tag{A.4}$$

Our result is

Theorem A.1. *As $h \to \infty$,*

$$\operatorname{Var} \mathcal{N} = \sqrt{H} \frac{\beta_q}{1 - \frac{1}{q^3}} \begin{cases} \frac{1 + \frac{1}{q^2}}{\sqrt{q}}, & h \text{ even} \\ \\ \frac{1 + \frac{1}{q}}{q}, & h \text{ odd} \end{cases} + O(\frac{H^2 n}{q^{n/3}}) + O_q(H^{1/4+o(1)}) \ .$$

In particular we get an asymptotic result provided $h < (\frac{2}{9} - o(1))n$. i.e. $H < (q^n)^{\frac{2}{9}-o(1)}$. It is likely that one can improve the factor 2/9 a bit.

A.1. The probability that f and $f+J$ are both squarefree.

As in the number field case, we start with an expression for the probability that both f and $f+J$ are squarefree. For a non-zero polynomial $J \in \mathbb{F}_q[t]$, define the "singular series"

$$\mathfrak{S}(J) = \prod_P (1 - \frac{2}{|P|^2}) \cdot \prod_{P^2 | J} \frac{|P|^2 - 1}{|P|^2 - 2} , \tag{A.5}$$

the product over all prime polynomials. We will first show

Theorem A.2. *For $0 \neq J \in \mathbb{F}_q[t]$, $\deg J < n$,*

$$S(J;n) := \sum_{f \in \mathcal{M}_n} \mu^2(f)\mu^2(f+J) = \mathfrak{S}(J) q^n + O(nq^{\frac{2n}{3}}) , \tag{A.6}$$

the implied constant absolute, with $\mathfrak{S}(J)$ given by (A.5).

Note that Theorem A.2 is uniform in J as long as $\deg J < n$.

Theorem A.2 is the exact counterpart for the analogous quantity over the integers, which has been known in various forms since the 1930's. The proof below is roughly the same as the one given in [12, Theorem 1]. The exponent 2/3 has been improved, by Heath Brown [13] to 7/11 and by Reuss [31] to about $0.578\dots$.

A.2. A decomposition of μ^2.

We start with the identity

$$\mu^2(f) = \sum_{d^2 | f} \mu(d) \tag{A.7}$$

(the sum over monic d). Pick an integer parameter $0 < z \leq n/2$, write $Z = q^z$, and decompose the sum into two parts, one over "small" divisors, that is with $\deg d < z$, and one over "large" divisors:

$$\mu^2 = \mu_z^2 + e_z \tag{A.8}$$

$$\mu_z^2(f) = \sum_{\substack{d^2 | f \\ \deg d < z}} \mu(d), \quad e_z(f) = \sum_{\substack{d^2 | f \\ \deg d \geq z}} \mu(d) . \tag{A.9}$$

Let

$$S_z(J;n) := \sum_{f \in \mathcal{M}_n} \mu_z^2(f)\mu_z^2(f+J) . \tag{A.10}$$

We want to replace S by S_z.

A.3. **Bounding** $S(J;n)-S_z(n;J)$**.**

Proposition A.3. *If* $z\leq n/2$ *then*

$$\Big|S(J;n)-S_z(J;n)\Big|\ll\frac{q^n}{Z}\ ,$$

where $Z=q^z$*.*

Proof. Note that

$$\begin{aligned}\mu^2(f)\mu^2(f+J)&=\mu_z^2(f)\mu_z^2(f+J)\\&\quad+e_z(f)\mu^2(f+J)-\mu^2(f)e_z(f+J)-e_z(f)e_z(f+J)\end{aligned}\tag{A.11}$$

so that (recall $\mu^2(f)\leq 1$)

$$\begin{aligned}\Big|\mu^2(f)\mu^2(f+J)-\mu_z^2(f)\mu_z^2(f+J)\Big|&\leq|e_z(f)|+|e_z(f+J)|+|e_z(f)e_z(f+J)|\\&\leq|e_z(f)|+|e_z(f+J)|+\frac12|e_z(f)|^2+\frac12|e_z(f+J)|^2\end{aligned}\tag{A.12}$$

and therefore, summing (A.12) over $f\in\mathcal{M}_n$ and noting that since $\deg J<n$, sums of $f+J$ are the same as sums of f,

$$\Big|S(J;n)-S_z(J;n)\Big|\leq 2\sum_{f\in\mathcal{M}_n}|e_z(f)|+\sum_{f\in\mathcal{M}_n}|e_z(f)|^2\ .\tag{A.13}$$

We have

$$|e_z(f)|=|\sum_{\substack{d^2|f\\ \deg d\geq z}}\mu(d)|\leq\sum_{\substack{d^2|f\\ \deg d\geq z}}1$$

so that

$$\begin{aligned}\sum_{f\in\mathcal{M}_n}|e_z(f)|&\leq\sum_{f\in\mathcal{M}_n}\sum_{\substack{d^2|f\\ \deg d\geq z}}1\\&=\sum_{z\leq\deg d\leq n/2}\#\{f\in\mathcal{M}_n:d^2\mid f\}\\&=\sum_{z\leq\deg d\leq n/2}\frac{q^n}{|d|^2}\leq\frac{2q^n}{Z}\ .\end{aligned}\tag{A.14}$$

Moreover,

$$\begin{aligned}\sum_{f\in\mathcal{M}_n}|e_z(f)|^2&\leq\sum_{f\in\mathcal{M}_n}\sum_{\substack{d_1^2|f\\ \deg d_1\geq z}}\sum_{\substack{d_2^2|f\\ \deg d_2\geq z}}1\\&\leq\sum_{z\leq\deg d_1,\deg d_2\leq n/2}\#\{f\in\mathcal{M}_n:d_1^2\mid f\text{ and }d_2^2\mid f\}\ .\end{aligned}$$

Now the conditions $d_1^2 \mid f$ and $d_2^2 \mid f$ are equivalent to $[d_1,d_2]^2 \mid f$, where $[d_1,d_2]$ is the least common multiple of d_1 and d_2, and this can only happen if $\deg[d_1,d_2] \le \deg f/2 = n/2$, in which case the number of such f is $q^n/|[d_1,d_2]|^2$ and is zero otherwise. Thus

$$\tag{A.15} \begin{aligned} \sum_{f\in\mathcal{M}_n} |e_z(f)|^2 &\le \sum_{\substack{z\le \deg d_1, \deg d_2 \le n/2\\ \deg[d_1,d_2]\le n/2}} \frac{q^n}{|[d_1,d_2]|^2} \\ &\le q^n \sum_{\deg d_1,\deg d_2\ge z} \frac{1}{|[d_1,d_2]|^2} \,. \end{aligned}$$

We claim that (this is the analogue of [12, Lemma 2])

Lemma A.4.

$$\sum_{\deg d_1,\deg d_2\ge z} \frac{1}{|[d_1,d_2]|^2} \ll \frac{1}{Z}$$

Inserting Lemma A.4 in (A.15) we will get

$$\tag{A.16} \sum_{f\in\mathcal{M}_n} |e_z(f)|^2 \ll \frac{q^n}{Z} \,.$$

Inserting (A.14) and (A.16) in (A.13) we conclude Proposition A.3.

To prove Lemma A.4, use $[d_1,d_2] = d_1d_2/\gcd(d_1,d_2)$ to rewrite the sum as

$$\begin{aligned} \sum_{\deg d_1,\deg d_2\ge z} \frac{1}{|[d_1,d_2]|^2} &= \sum_{\deg d_1,\deg d_2\ge z} \frac{|\gcd(d_1,d_2)|^2}{|d_1|^2|d_2|^2} \\ &= \sum_{k \text{ monic}} |k|^2 \sum_{\substack{\deg d_1,\deg d_2\ge z\\ \gcd(d_1,d_2)=k}} \frac{1}{|d_1|^2|d_2|^2} \,. \end{aligned}$$

In the sum above, we write $d_j = k\delta_j$ with $\gcd(\delta_1,\delta_2)=1$. The condition $\deg d_j \ge z$ gives no restriction on δ_j if $\deg k \ge z$, and otherwise translates into $\deg \delta_j \ge z - \deg k$. Thus

$$\begin{aligned} \sum_{\deg d_1,\deg d_2\ge z} \frac{1}{|[d_1,d_2]|^2} &\ll \sum_{k \text{ monic}} \frac{1}{|k|^2} \sum_{\substack{\deg \delta_1,\deg\delta_2\ge z-\deg k\\ \gcd(\delta_1,\delta_2)=1}} \frac{1}{|\delta_1|^2|\delta_2|^2} \\ &\le \sum_{k \text{ monic}} \frac{1}{|k|^2} \Big(\sum_{\deg\delta\ge z-\deg k} \frac{1}{|\delta|^2} \Big)^2 \end{aligned}$$

after ignoring the coprimality condition. Therefore

$$\begin{aligned}\sum_{k \text{ monic}} \frac{1}{|k|^2}\Big(\sum_{\deg\delta\geq z-\deg k}\frac{1}{|\delta|^2}\Big)^2 &\leq \sum_{\deg k\leq z}\frac{1}{|k|^2}\Big(\sum_{\deg\delta\geq z-\deg k}\frac{1}{|\delta|^2}\Big)^2\\ &\quad+\sum_{\deg k>z}\frac{1}{|k|^2}\Big(\sum_{\delta}\frac{1}{|\delta|^2}\Big)^2\\ &\ll \sum_{\deg k\leq z}\frac{1}{|k|^2}(\frac{|k|}{q^z})^2+\frac{1}{q^{z+1}}\\ &\ll \frac{1}{Z}\ ,\end{aligned}$$

which proves Lemma A.4. □

A.4. **Evaluating $S_z(J;n)$.**

Proposition A.5. *If $z\leq n/2$ then*

$$S_z(J;n)=q^n\mathfrak{S}(J)+O(\frac{q^n z}{Z})+O(Z^2),$$

with $Z=q^z$.

Proof. Using the definition of μ_z^2, we obtain

$$\begin{aligned}S_z(J;n) &:= \sum_{f\in\mathcal{M}_n}\mu_z^2(f)\mu_z^2(f+J)\\ &= \sum_{\deg d_1\leq z}\sum_{\deg d_2\leq z}\mu(d_1)\mu(d_2)\#\{f\in\mathcal{M}_n : d_1^2\mid f, d_2^2\mid f+J\}\ .\end{aligned}$$

Decomposing into residue classes modulo $[d_1,d_2]^2$ gives

$$\begin{aligned}&\#\{f\in\mathcal{M}_n : d_1^2\mid f, d_2^2\mid f+J\}\\ &\qquad=\sum_{\substack{c \bmod [d_1,d_2]^2\\ c=0 \bmod d_1^2\\ c=-J \bmod d_2^2}}\#\{f\in\mathcal{M}_n : f=c \bmod [d_1,d_2]^2\}\ .\end{aligned}$$

If $\deg[d_1,d_2]^2\leq n$ then

$$\#\{f\in\mathcal{M}_n : f=c \bmod [d_1,d_2]^2\}=\frac{q^n}{|[d_1,d_2]|^2}\ .$$

Otherwise there is at most *one* $f\in\mathcal{M}_n$ with $f=c \bmod [d_1,d_2]^2$. So we write

$$\#\{f\in\mathcal{M}_n : f=c \bmod [d_1,d_2]^2\}=\frac{q^n}{|[d_1,d_2]|^2}+O(1)\ .$$

Let $\kappa(d_1,d_2;J)$ be the number of solutions $c \bmod [d_1,d_2]^2$ of the system of congruences $c=0 \bmod d_1^2$, $c=-J \bmod d_2^2$; it is either 1 or 0 depending on whether $\gcd(d_1,d_2)^2 \mid J$ or not. Then we have found that

$$\begin{aligned} S_z(J;n) &= \sum_{\deg d_1\le z}\sum_{\deg d_2\le z} \mu(d_1)\mu(d_2)\kappa(d_1,d_2;J)\Big(\frac{q^n}{|[d_1,d_2]|^2}+O(1)\Big) \\ &= q^n \sum_{\deg d_1\le z}\sum_{\deg d_2\le z}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2}+O(Z^2)\,. \end{aligned}$$

The double sum can be extended to include all d_1,d_2:

$$\begin{aligned} \sum_{\deg d_1\le z}\sum_{\deg d_2\le z}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2} &= \sum_{d_1,d_2}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2} \\ &\quad + O\Big(\sum_{\deg d_1>z}\sum_{d_2}\frac{1}{|[d_1,d_2]|^2}\Big)\,, \end{aligned}$$

so that

$$\begin{aligned} S_z(J;n) = q^n\sum_{d_1,d_2}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2} \\ + O\Big(\sum_{\deg d_1>z}\sum_{d_2}\frac{1}{|[d_1,d_2]|^2}\Big)+O(Z^2)\,. \end{aligned} \tag{A.17}$$

We bound the sum in the remainder term of (A.17) by (this is the analogue of [12, Lemma 3]):

Lemma A.6.

$$\sum_{\deg d_1>z}\sum_{d_2}\frac{1}{|[d_1,d_2]|^2} \ll \frac{z}{q^z}=\frac{z}{Z}\,.$$

Proof. We argue as in the proof of Lemma A.4: We write the least common multiple as $[d_1,d_2]=d_1d_2/\gcd(d_1,d_2)$ and sum over all pairs of d_1,d_2 with given gcd:

$$\begin{aligned} \sum_{\deg d_1>z}\sum_{d_2}\frac{1}{|[d_1,d_2]|^2} &= \sum_k |k|^2 \sum_{\deg d_1>z}\sum_{\substack{d_2\\ \gcd(d_1,d_2)=k}}\frac{1}{|d_1|^2|d_2|^2} \\ &= \sum_k |k|^2 \sum_{\deg \delta_1>z-\deg k}\frac{1}{|k|^2|\delta_1|^2}\sum_{\substack{\delta_2\\ \gcd(\delta_1,\delta_2)=1}}\frac{1}{|k|^2|\delta_2|^2}\,, \end{aligned}$$

after writing $d_j=k\delta_j$ with δ_1, δ_2 coprime.

Ignoring the coprimality condition gives

$$\begin{aligned}\sum_{\deg d_1>z}\sum_{d_2}\frac{1}{|[d_1,d_2]|^2} &\ll \sum_k \frac{1}{|k|^2}\sum_{\deg\delta_1>z-\deg k}\frac{1}{|\delta_1|^2}\sum_{\delta_2}\frac{1}{|\delta_2|^2}\\ &\ll \sum_{\deg k\leq z}\frac{1}{|k|^2}\sum_{\deg\delta_1>z-\deg k}\frac{1}{|\delta_1|^2}+\sum_{\deg k>z}\frac{1}{|k|^2}\sum_{\delta_1}\frac{1}{|\delta_1|^2}\\ &\ll \sum_{\deg k\leq z}\frac{1}{|k|^2}\frac{|k|}{q^z}+\sum_{\deg k>z}\frac{1}{|k|^2}\\ &\ll \frac{z}{q^z}=\frac{z}{Z}\ ,\end{aligned}$$

which proves Lemma A.6. □

Putting together (A.17) and Lemma A.6, we have shown that

$$S_z(J;n)=q^n\sum_{d_1}\sum_{d_2}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2}+O(\frac{q^nz}{Z})+O(Z^2)\ . \tag{A.18}$$

It remains to show that the infinite sum in (A.18) coincides with the singular series $\mathfrak{S}(J)$:

Lemma A.7.

$$\sum_{d_1}\sum_{d_2}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2}=\mathfrak{S}(J)$$

Proof. This is done exactly as in [12, Appendix]. We write

$$\sum_{d_1}\sum_{d_2}\mu(d_1)\mu(d_2)\frac{\kappa(d_1,d_2;J)}{|[d_1,d_2]|^2}=\sum_m\frac{s(m;J)}{|m|^2}$$

where

$$s(m;J)=\sum_{\substack{[d_1,d_2]=m\\ \gcd(d_1,d_2)^2|J}}\mu(d_1)\mu(d_2)$$

One checks that $s(m;J)$ is multiplicative in m, and that for P prime

$$s(P^\alpha;P^j)=\sum_{\substack{\max(u,v)=\alpha\\ 2\min(u,v)\leq j}}\mu(P^u)\mu(P^v)$$

so that $s(P^\alpha;P^j)=0$ for $\alpha\geq 2$ while for $\alpha=1$

$$s(P;P^j)=\sum_{\substack{\max(u,v)=1\\ \min(u,v)\leq j/2}}\mu(P^u)\mu(P^v)$$

If $j<2$ (that is if $P^2\nmid P^j$), then the sum is over $\max(u,v)=1$ and $\min(u,v)=0$ i.e. $(u,v)=(0,1),(1,0)$ which works out to $s(P,P^j)=-2$

for $j = 0, 1$, while for $j \geq 2$ the only restriction is $\max(u, v) = 1$, i.e. $(u, v) = (1, 0), (0, 1), (1, 1)$ which gives $s(P, P^j) = -1$ for $j \geq 2$. Thus

$$\begin{aligned}\sum_m \frac{s(m; J)}{|m|^2} &= \prod_P \left(1 + \frac{s(P, J)}{|P|^2}\right) \\ &= \prod_{P^2 \mid J} (1 - \frac{1}{|P|^2}) \prod_{P^2 \nmid J} (1 - \frac{2}{|P|^2})\end{aligned}$$

which is exactly $\mathfrak{S}(J)$. □

We now conclude the proof of Proposition A.5: By Propositions A.3, A.5 we have shown that for $z \leq n/2$,

$$S(J; n) = q^n \mathfrak{S}(J) + O(\frac{q^n z}{Z}) + O(Z^2)$$

Taking $z \approx n/3$ gives that for all $J \neq 0$ with $\deg J < n$,

$$S(J; n) = q^n \mathfrak{S}(J) + O(nq^{2n/3})$$

as claimed. □

A.5. **Computing the variance.** As described in § 5.1, we have a partition of the set $\mathcal{M}_n$ of monic polynomials of degree n as

$$\mathcal{M}_n = \coprod_{A \in \mathcal{A}} I(A; h)$$

where

$$\mathcal{A} = \left\{A = t^n + a_{n-1} t^{n_1} + \cdots + a_{h+1} t^{h+1} : a_j \in \mathbb{F}_q\right\} .$$

The mean value of $\mathcal{N}$ is, for $n \geq 2$,

$$\langle \mathcal{N} \rangle = \frac{1}{\#\mathcal{A}} \sum_{A \in \mathcal{A}} \mathcal{N}(A) = \frac{q^{h+1}}{\zeta(2)}, \quad n \geq 2 .$$

The variance is

$$\operatorname{Var} \mathcal{N} = \left\langle \mathcal{N}^2 \right\rangle - \left\langle \mathcal{N} \right\rangle^2 . \tag{A.19}$$

We have

$$\begin{aligned}\left\langle \mathcal{N}^2 \right\rangle &= \frac{1}{\#\mathcal{A}} \sum_{A \in \mathcal{A}} \sum_{|f - A| \leq q^h} \sum_{|g - A| \leq q^h} \mu^2(f) \mu^2(g) \\ &= \frac{1}{\#\mathcal{A}} \sum_{f \in \mathcal{M}_n} \mu^2(f) + \frac{1}{\#\mathcal{A}} \sum_{\substack{f \neq g \\ |f - g| \leq q^h}} \mu^2(f) \mu^2(g) \\ &= \langle \mathcal{N} \rangle + q^{h+1} \sum_{0 \neq J \in \mathcal{P}_{\leq h}} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \mu^2(f) \mu^2(f + J) .\end{aligned}$$

We use Theorem A.2

$$\sum_{f \in \mathcal{M}_n} \mu^2(f) \mu^2(f + J) = q^n \mathfrak{S}(J) + O\Big(nq^{2n/3}\Big) \tag{A.20}$$

where

$$\mathfrak{S}(J) = \prod_P (1 - \frac{2}{|P|^2}) \cdot \prod_{P^2 | J} \frac{|P|^2 - 1}{|P|^2 - 2} = \alpha \mathfrak{s}(J) \tag{A.21}$$

with

$$\alpha = \prod_P (1 - \frac{2}{|P|^2}) \tag{A.22}$$

and

$$\mathfrak{s}(J) = \prod_{P^2|J} \frac{|P|^2-1}{|P|^2-2} \ .$$

This gives that

(A.23)

$$\begin{aligned} \mathrm{Var} &= \langle \mathcal{N} \rangle - \langle \mathcal{N} \rangle^2 + \alpha q^{h+1} \sum_{0 \neq J \in \mathcal{P}_{\leq h}} \mathfrak{s}(J) + O(H^2 n q^{-n/3}) \\ &= \frac{q^{h+1}}{\zeta(2)} - (\frac{q^{h+1}}{\zeta(2)})^2 + \alpha q^{h+1}(q-1) \sum_{j=0}^{h} \sum_{J \in \mathcal{M}_j} \mathfrak{s}(J) + O(H^2 n q^{-n/3}) \ , \end{aligned}$$

the last step using homogeneity: $\mathfrak{S}(cJ) = \mathfrak{S}(J)$, $c \in \mathbb{F}_q^\times$.

A.6. **Computing $\sum_J \mathfrak{s}(J)$.** To evaluate the sum of $\mathfrak{s}(J)$ in (A.23), we form the generating series

$$F(u) = \sum_{J \text{ monic}} \mathfrak{s}(J) u^{\deg J} \ .$$

Since $\mathfrak{s}(J)$ is multiplicative, and $\mathfrak{s}(P^k) = 1$ if $k = 0, 1$, and $\mathfrak{s}(P^k) = \mathfrak{s}(P^2) = \frac{|P|^2-1}{|P|^2-2}$ if $k \geq 2$, we find

$$\begin{aligned} F(u) &= \prod_P (1 + u^{\deg P} + \mathfrak{s}(P^2) \sum_{k \geq 2} u^{k \deg P}) \\ &= \prod_P (1 + u^{\deg P} + \frac{|P|^2-1}{|P|^2-2} \frac{u^{2 \deg P}}{1 - u^{\deg P}}) \\ &= Z(u) \prod_P (1 + \frac{1}{|P|^2 - 2} u^{2 \deg P}) \end{aligned}$$

with

$$Z(u) = \prod_P (1 - u^{\deg P})^{-1} = \frac{1}{1 - qu} \ .$$

We further factor

$$\prod_P (1 + \frac{1}{|P|^2-2} u^{2 \deg P}) = Z(u^2/q^2) \prod_P (1 + \frac{2u^{2 \deg P} - u^{4 \deg P}}{|P|^2(|P|^2-2)}) \ ,$$

with the product absolutely convergent for $|u| < q^{3/4}$.

We have

$$\begin{aligned}\sum_{j=0}^{h}\sum_{J\in\mathcal{M}_j}\mathfrak{s}(J) &= \frac{1}{2\pi i}\oint F(u)\frac{1-u^{-(h+1)}}{u-1}du \\ &= \frac{1}{2\pi i}\oint F(u)\frac{1}{u-1}du + \frac{1}{2\pi i}\oint F(u)\frac{u^{-(h+1)}}{1-u}du \end{aligned} \tag{A.24}$$

where the contour of integration is a small circle around the origin not including any pole of $F(u)$, say $|u| = 1/q^2$, traversed counter-clockwise.

The first integral is zero, because the integrand is analytic near $u = 0$. As for the second integral, we shift the contour of integration to $|u| = q^{3/4-\delta}$, and obtain

$$\frac{1}{2\pi i}\oint F(u)\frac{u^{-(h+1)}}{1-u}du = -\operatorname*{Res}_{u=1/q} - \operatorname*{Res}_{u=1} - \operatorname*{Res}_{u=\pm\sqrt{q}} + \frac{1}{2\pi i}\oint\limits_{|u|=q^{3/4-\delta}} F(u)\frac{u^{-(h+1)}}{1-u}du$$

As $h\to\infty$, we may bound the integral around $|u| = q^{3/4-\delta}$ by

$$\frac{1}{2\pi i}\oint\limits_{|u|=q^{3/4-\delta}} F(u)\frac{u^{-(h+1)}}{1-u}du \ll_q q^{-(3/4-\delta)(h+1)} \ ,$$

the implied constant depending on q.

The residue at $u = 1/q$ gives

$$-\operatorname*{Res}_{u=1/q} = \frac{1}{\alpha\zeta(2)^2}\frac{q^{h+1}}{(q-1)}$$

and hence its contribution to $\operatorname{Var}\mathcal{N}$ is

$$\left(\frac{q^{h+1}}{\zeta(2)}\right)^2 \tag{A.25}$$

which exactly cancels out the term $-\langle\mathcal{N}\rangle^2$ in (A.23).

The residue at $u = 1$ gives

(A.26)

$$-\operatorname*{Res}_{u=1}\frac{F(u)u^{-(h+1)}}{1-u} = F(1) = \frac{1}{1-q}\prod_P(1+\frac{1}{|P|^2-2}) = -\frac{1}{(q-1)\alpha\zeta_q(2)}$$

and its contribution to $\operatorname{Var}\mathcal{N}$ is

$$-\frac{q^{h+1}}{\zeta_q(2)} \tag{A.27}$$

which exactly cancels out the term $\langle\mathcal{N}\rangle$ in (A.23).

The residue at $u = +\sqrt{q}$ gives

$$-\operatorname*{Res}_{u=+\sqrt{q}} = \frac{\beta_q}{2\alpha}\frac{q^{-\frac{h}{2}-2}}{(1-\frac{1}{q^{3/2}})(1-\frac{1}{q^{1/2}})} \tag{A.28}$$

and the residue at $u = -\sqrt{q}$ gives

$$-\operatorname*{Res}_{u=-\sqrt{q}} = \frac{\beta_q}{2\alpha}(-1)^h \frac{q^{-\frac{h}{2}-2}}{(1+\frac{1}{q^{3/2}})(1+\frac{1}{q^{1/2}})}$$

with $\beta_q = \prod_P (1 - \frac{3}{|P|^2} + \frac{2}{|P|^3})$. Hence

$$-\operatorname*{Res}_{u=+\sqrt{q}} - \operatorname*{Res}_{u=-\sqrt{q}} = +\frac{\beta_q}{\alpha} q^{-\frac{h}{2}-1} \frac{(1+\frac{1}{q^2})^{\frac{1+(-1)^h}{2}} + \frac{1}{q^{1/2}}(1+\frac{1}{q})^{\frac{1-(-1)^h}{2}}}{(1-\frac{1}{q^3})(q-1)} .$$

Therefore we find

$$\operatorname{Var}\mathcal{N} = \frac{\beta_q}{1-\frac{1}{q^3}} q^{(h+1)/2} \begin{cases} \frac{1+\frac{1}{q^2}}{\sqrt{q}}, & h \text{ even} \\ \\ \frac{1+\frac{1}{q}}{q}, & h \text{ odd} \end{cases} + O(H^2 n q^{-n/3}) + O_q(H^{1/4+\delta}) .$$

This concludes the proof of Theorem A.1.

References

[1] A. Axer, *Über einige Grenzwert sätze.* S.-B. Math.-Natur. K1. Akad. Wiss. Wien (2a) 120 (1911), 1253–1298.

[2] R. C. Baker and J. Pintz, *The distribution of squarefree numbers.* Acta Arith. 46 (1985), no. 1, 73–79.

[3] E. Bank, L. Bary-Soroker and L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*, Duke J. of Math., to appear. arXiv:1302.0625 [math.NT].

[4] S. Bae, B. Cha and H. Jung, *Möbius function in short intervals for function fields.* Finite Fields Appl. 34 (2015), 235–249.

[5] V. Blomer, The average value of divisor sums in arithmetic progressions, Q. J. Math. 59 (2008) 275–286.

[6] D. Carmon and Z. Rudnick, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field.* Q. J. Math. 65 (2014), no. 1, 53–61.

[7] B. Cha, *The summatory function of the Möbius function in function fields*, manuscript. arXiv:1008.4711 [math.NT]

[8] S. Chatterjee and K. Soundararajan, *Random multiplicative functions in short intervals.* Int. Math. Res. Not. IMRN 2012, no. 3, 479–492.

[9] P. Erdös, *Some problems and results in elementary number theory*, Publ. Math. Debrecen 2 (1951) 103–109.

[10] M. Filaseta. *Short interval results for squarefree numbers.* J. Number Theory 35 (1990), no. 2, 128–149.

[11] I. J. Good and R. F. Churchhouse. *The Riemann Hypothesis and Pseudorandom Features of the Möbius Sequence*, Mathematics of Computation 22, No. 104, (1968), 857–861.

[12] R. R. Hall. *Squarefree numbers on short intervals.* Mathematika 29 (1982), no. 1, 7–17.

[13] D. R. Heath-Brown. *The square sieve and consecutive squarefree numbers.* Math. Ann. 266 (1984), no. 3, 251–259.

[14] C. Hooley. *On the Barban-Davenport-Halberstam theorem.* III. J. London Math. Soc. (2) 10 (1975), 249–256.

[15] P. Humphries. *On the Mertens conjecture for function fields*. Int. J. Number Theory 10 (2014), no. 2, 341–361.

[16] C. H. Jia, *The distribution of squarefree numbers*. Sci. China Ser. A 36 (1993), no. 2, 154–169.

[17] N. M. Katz, *On a Question of Keating and Rudnick about Primitive Dirichlet Characters with Squarefree Conductor*, Int. Math. Res. Not. IMRN 2013, no. 14, 3221–3249.

[18] N. M. Katz. *Witt vectors and a question of Keating and Rudnick*, Int. Math. Res. Not. IMRN 2013, no. 16, 3613–3638.

[19] N. M. Katz. *Witt vectors and a question of Entin, Keating and Rudnick*, to appear in Int. Math. Res. Not. IMRN.

[20] N. M. Katz. *On two question of Entin, Keating and Rudnick on primitive Dirichlet characters*, to appear in Int. Math. Res. Not. IMRN.

[21] J. P. Keating, E. Roditty-Gershon and Z. Rudnick, in preparation.

[22] J. P. Keating and Z. Rudnick. *The variance of the number of prime polynomials in short intervals and in residue classes*. Int. Math. Res. Not. IMRN 2014, no. 1, 259–288.

[23] K. Matomäki and M. Radziwłł, *Multiplicative functions in short intervals*. arXiv:1501.04585 [math.NT].

[24] H. L. Montgomery and R. C. Vaughan, *The distribution of squarefree numbers*. Recent progress in analytic number theory, Vol. 1 (Durham, 1979), pp. 247–256, Academic Press, London-New York, 1981.

[25] Y. Motohashi, *On the sum of the Möbius function in a short segment*, Proc. Japan Acad. 52 (1976) 477–479.

[26] N. Ng, *The distribution of the summatory function of the Möbius function*. Proc. London Math. Soc. (3) 89 (2004), no. 2, 361–389.

[27] N. Ng, *The Möbius function in short intervals*. Anatomy of integers, 247–257, CRM Proc. Lecture Notes, 46, Amer. Math. Soc., Providence, RI, 2008.

[28] Ramon M. Nunes, *On the distribution of squarefree numbers in arithmetic progressions*. arXiv:1402.0684 [math.NT]

[29] K. Prachar, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*. Monatsh. Math. 62 (1958), 173–176.

[30] K. Ramachandra, *Some problems of analytic number theory*, Acta Arith. 31 (1976) 313–324.

[31] T. Reuss. *Pairs of k-free Numbers, consecutive square-full Numbers*. arXiv:1212.3150 [math.NT]

[32] H.-E. Richert. *On the difference between consecutive squarefree numbers.* J. London Math. Soc. 29, (1954). 16–20.

[33] B. Rodgers, *The covariance of almost-primes in $\mathbb{F}_q[T]$*, to appear in Int. Math. Res. Not. IMRN. arXiv:1311.4905 [math.NT]

[34] K. F. Roth. *On the gaps between squarefree numbers.* J. London Math. Soc. 26, (1951). 263–268.

[35] Z. Rudnick. *squarefree values of polynomials over the rational function field*, J. of Number Theory, 135 (2014), Pages 60–66.

[36] R. G. Swan, *Factorization of polynomials over finite fields*. Pacific J. Math. 12 1962 1099–1106.

[37] D. I. Tolev. *On the distribution of r-tuples of squarefree numbers in short intervals*. Int. J. Number Theory 2 (2006), no. 2, 225–234.

[38] R. Warlimont, *Squarefree numbers in arithmetic progressions*, J. London Math. Soc. (2) 22 (1980) 21–24.

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
E-mail address: `j.p.keating@bristol.ac.uk`

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: rudnick@post.tau.ac.il