J. P. Keating and Z. Rudnick (2012) "Variance of the Number of Prime Polynomials,"
International Mathematics Research Notices, rns220, 30 pages.
doi:10.1093/imrn/rns220

The Variance of the Number of Prime Polynomials in Short Intervals and in Residue Classes

Jonathan P. Keating[1] and Zeév Rudnick[2]

[1]School of Mathematics, University of Bristol, Bristol BS8 1TW, UK and
[2]Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

Correspondence to be sent to: e-mail: rudnick@post.tau.ac.il

We resolve a function field version of two conjectures concerning the variance of the number of primes in short intervals (Goldston and Montgomery) and in arithmetic progressions (Hooley). A crucial ingredient in our work is the recent equidistribution results of N. Katz.

1 Introduction

In this note, we study a function field version of two outstanding problems in classical Prime Number Theory, concerning the variance of the number of primes in short intervals and in arithmetic progressions.

1.1 Problem 1: Primes in short intervals

The prime number theorem (PNT) asserts that the number $\pi(x)$ of primes up to x is asymptotically $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$. Equivalently, defining the von Mangoldt function as $\Lambda(n) = \log p$ if $n = p^k$ is a prime power, and 0 otherwise, then PNT is equivalent to the assertion that

$$\psi(x) := \sum_{n \le x} \Lambda(n) \sim x \quad \text{as } x \to \infty. \tag{1.1}$$

Received April 23, 2012; Revised September 9, 2012; Accepted September 10, 2012

To study the distribution of primes in short intervals, we define, for $1 \le H \le x$,

$$\psi(x; H) := \sum_{n \in [x-\frac{H}{2}, x+\frac{H}{2}]} \Lambda(n). \tag{1.2}$$

The Riemann Hypothesis (RH) guarantees an asymptotic formula $\psi(X; H) \sim H$ as long as $H > X^{\frac{1}{2}+o(1)}$. To understand the behavior in shorter intervals, Goldston and Montgomery [5] studied the variance of $\psi(x; H)$ and showed conditionally that for $X^{\delta} < H < X^{1-\delta}$,

$$\frac{1}{X}\int_2^X |\psi(x; H) - H|^2 \, dx \sim H(\log X - \log H), \tag{1.3}$$

assuming the RH and the ("strong") pair correlation conjecture. Furthermore, they showed that under RH (1.3) and the strong pair correlation conjecture are in fact equivalent. At this time (1.3) is still open.

1.2 Problem 2: Primes in arithmetic progressions

The PNT for arithmetic progression states that for a modulus Q and A coprime to Q, the number of primes $p \le X$ with $p = A \bmod Q$ is asymptotically $\pi(x)/\phi(Q)$, where $\pi(X)$ is the number of primes up to X and $\phi(Q)$ is the Euler totient function, giving the number of reduced residues modulo Q. Equivalently, if

$$\psi(X; Q, A) := \sum_{\substack{n \le X \\ n = A \bmod Q}} \Lambda(n), \tag{1.4}$$

then PNT for arithmetic progressions states that for a fixed modulus Q,

$$\psi(X; Q, A) \sim \frac{X}{\phi(Q)} \quad \text{as } X \to \infty. \tag{1.5}$$

In most arithmetic applications, it is crucial to allow the modulus to grow with X. Thus, the remainder term in (1.5) is of the essence. For very large moduli $Q > X$, there can be at most one prime in the arithmetic progression $P = A \bmod Q$ so that the interesting range is $Q < X$. Assuming the Generalized Riemann Hypothesis (GRH) gives (1.5) for $Q < X^{1/2-o(1)}$.

The fluctuations of $\psi(X; Q, A)$ have been studied over several decades, notably allowing also averaging over the modulus Q. Thus, define

$$G(X, Q) = \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \left| \psi(X; Q, A) - \frac{X}{\phi(Q)} \right|^2 \tag{1.6}$$

and

$$H(X, Q) = \sum_{Q' \le Q} G(X, Q'). \tag{1.7}$$

The study of the sum $H(X, Q)$ has a long history, going under the name of theorems of Barban–Davenport–Halberstam-type. Among other results is the one due to Montgomery [13] and Hooley [7] asserting that for $X/(\log X)^A < Q < X$ one has

$$H(X, Q) = QX \log Q - cQX + O\left(Q^{5/4} X^{3/4} + \frac{X^2}{(\log X)^A} \right), \tag{1.8}$$

for all $A > 0$, where

$$c = \gamma + \log(2\pi) + 1 + \sum_p \frac{\log p}{p(p-1)}. \tag{1.9}$$

Hooley [8] showed that assuming GRH, (1.8) holds for $X^{1/2+\epsilon} < Q < X$ with remainder $O(X^2/(\log X)^A)$.

The individual variance $G(X, Q)$ is much less understood. Hooley [6] conjectured that under some (unspecified) conditions,

$$G(X, Q) \sim X \log Q. \tag{1.10}$$

Friedlander and Goldston [4] show that in the range $Q > X$,

$$G(X, Q) = X \log X - X - \frac{X^2}{\phi(Q)} + O\left(\frac{X}{(\log X)^A} \right) + O((\log Q)^3). \tag{1.11}$$

Note that in this range, there is at most one integer $n = A \bmod Q$ with $n < X$. They conjecture that (1.10) holds if

$$X^{1/2+\epsilon} < Q < X \tag{1.12}$$

and further conjecture that if $X^{1/2+\epsilon} < Q < X^{1-\epsilon}$, then

$$G(X, Q) = X \log Q - X\left(\gamma + \log 2\pi + \sum_{p|Q} \frac{\log p}{p-1}\right) + o(X). \tag{1.13}$$

They show that both (1.10) (in the range $X^{1/2+\epsilon} < Q < X$) and (1.13) (in the range $X^{1/2+\epsilon} < Q < X^{1-\epsilon}$) hold assuming a Hardy–Littlewood conjecture with small remainders.

For $Q < X^{1/2}$ very little seems to be known. Hooley addresses this in paper V of his series of papers on the subject [9], which he opens by stating

> An interesting anomaly in the theory of primes is presented by the situation in which known forms of the PNT for arithmetic progressions are only valid for (relatively) small values of the common difference k, whereas the theorems of Barban–Davenport–Halberstam type discussed in I, II, IV are only fully significant for the (relatively) larger values of k. The most striking illustration of this contrast is perhaps provided by the conditional theorems at present available on the extended Riemann hypothesis, the ranges of significance of the PNT and of the Barban-Montgomery theorem given in II being then, respectively, $k < x^{1/2-\epsilon}$ and $k > x^{1/2+\epsilon}$.
>
> ... it is therefore certainly desirable to elicit further forms of the Barban–Davenport–Halberstam theorem that should be valid for the smaller values of k.

In the above Hooley's k corresponds to our Q and x to X, and the roman numerals refer to previous papers in the series written by him.

Concerning Conjectures (1.10) and (1.13) for $G(X, Q)$, Friedlander and Goldston say [4, p. 315]

> It may well be that these also hold for smaller Q, but below $X = Q^{1/2}$ we are somewhat skeptical.

In this paper, we resolve the function field versions of Conjectures (1.3) and (1.10), indicating that (1.10) should hold all the way down to $Q > X^{\epsilon}$. A crucial ingredient in our work are recent equidistribution results of Katz [11, 12] described in Sections 4 and 5.

2 Results for Function Fields

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[T]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. Let $\mathcal{P}_n = \{f \in \mathbb{F}_q[T] : \deg f = n\}$ be the set of polynomials of degree n and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

The von Mangoldt function in this case is defined as $\Lambda(N) = \deg P$, if $N = cP^k$ with P an irreducible monic polynomial, and $c \in \mathbb{F}_q^\times$, and $\Lambda(N) = 0$ otherwise. The Prime Polynomial Theorem in this context is the identity

$$\sum_{f \in \mathcal{M}_n} \Lambda(f) = q^n. \tag{2.1}$$

2.1 Short intervals

For $A \in \mathcal{P}_n$ of degree n, and $h < n$, we define "short intervals"

$$I(A; h) := \{f : \|f - A\| \le q^h\} = A + \mathcal{P}_{\le h}, \tag{2.2}$$

where the norm of a polynomial $0 \ne f \in \mathbb{F}_q[T]$ is

$$\|f\| := q^{\deg f} \tag{2.3}$$

and

$$\mathcal{P}_{\le h} = \{0\} \cup \bigcup_{0 \le m \le h} \mathcal{P}_m \tag{2.4}$$

is the space of polynomials of degree at most h (including 0). We have

$$\#I(A; h) = q^{h+1}. \tag{2.5}$$

Note: For $h < n$, if $\|f - A\| \le q^h$, then A 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.

We define, for $1 \le h < n$ and $A \in \mathcal{P}_n$,

$$\nu(A; h) = \sum_{\substack{f \in I(A;h) \\ f(0) \ne 0}} \Lambda(f) \tag{2.6}$$

to be the number of prime powers co-prime to T in the interval $I(A; h)$, weighted by the degree of the corresponding prime.

We will show in Lemma 4.3 that the mean value of $\nu(A; h)$ when we average over monic $A \in \mathcal{M}_n$ is

$$\langle \nu(\bullet; h) \rangle := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \nu(A; h) = q^{h+1} \left(1 - \frac{1}{q^n}\right). \tag{2.7}$$

Our goal is to compute the variance

$$\mathrm{Var} \nu(\bullet; h) = \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\nu(A; h) - \langle \nu(\bullet; h) \rangle|^2$$

in the limit $q \to \infty$.

Theorem 2.1. Let $h < n - 3$. Then

$$\lim_{q \to \infty} \frac{1}{q^{h+1}} \mathrm{Var}(\nu(\bullet; h)) = n - h - 2. \tag{2.8}$$

□

We may compare (2.8) with (1.3), if we make the dictionary

$$X \leftrightarrow q^n, \quad H \leftrightarrow q^{h+1}, \quad \log X \leftrightarrow n, \quad \log H \leftrightarrow h + 1, \tag{2.9}$$

the conclusion being that Theorem 2.1 is precisely the analog of the conditional result (1.3) of Goldston and Montgomery.

2.2 Arithmetic progressions

Our second result concerns the analog of the conjectures of Hooley (1.10) and Friedlander–Goldston (1.13) and allows us to make a definite conjecture in that case.

For a polynomial $Q \in \mathbb{F}_q[T]$ of positive degree, and $A \in \mathbb{F}_q[T]$ coprime to Q and any $n > 0$, set

$$\Psi(n; Q, A) = \sum_{N \in \mathcal{M}_n \ \mathbb{N} = A \bmod Q} \Lambda(N) \tag{2.10}$$

(the sum over monic polynomials). The Prime Polynomial Theorem in arithmetic progressions states that as $n \to \infty$,

$$\Psi(n; Q, A) \sim \frac{q^n}{\Phi(Q)}, \tag{2.11}$$

where $\Phi(Q)$ is the Euler totient function for this context, namely the number of reduced residue classes modulo Q. Now set

$$G(n; Q) = \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \left| \Psi(n; Q, A) - \frac{q^n}{\Phi(Q)} \right|^2. \tag{2.12}$$

We wish to show an analog of Conjecture (1.10) in the limit of large finite field size, that is, $q \to \infty$.

Theorem 2.2. (i) Given a finite field $\mathbb{F}_q$, let $Q \in \mathbb{F}_q[T]$ be a polynomial of positive degree, and $1 \leq n < \deg Q$. Then

$$G(n; Q) = nq^n - \frac{q^{2n}}{\Phi(Q)} + O(n^2 q^{n/2}) + O((\deg Q)^2), \tag{2.13}$$

where the implied constant is absolute.

(ii) Fix $n \geq 2$. Given a sequence of finite fields $\mathbb{F}_q$ and square-free polynomials $Q(T) \in \mathbb{F}_q[T]$ of positive degree with $n \geq \deg Q - 1$, then as $q \to \infty$,

$$G(n; Q) \sim q^n(\deg Q - 1). \tag{2.14}$$

□

We can compare (2.14) with (1.10) in the range (1.12), if we make the dictionary

$$Q \leftrightarrow \|Q\| = q^{\deg Q}, \quad \log Q \leftrightarrow \deg Q, \quad X \leftrightarrow q^n, \quad \log X \leftrightarrow n. \tag{2.15}$$

The result (1.11) in the range $Q > X$ corresponds to $n < \deg Q$, and the range $X^{1/2} < Q < X$ of (1.12) corresponds to $\deg Q < n < 2 \deg Q$, so that we recover the function field version of conjecture (1.10). Note that (2.14) holds for all n, not just that range. Thus, Conjecture (1.10) may well be valid for all $Q > X^{\epsilon}$.

3 Background on Characters and L-functions

We review some standard background concerning Dirichlet L-functions for the rational function field; see, for example, [15, 16].

3.1 The prime polynomial theorem

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[T]$ the polynomials over $\mathbb{F}$. The zeta function $Z(u)$ of $\mathbb{F}_q[T]$ is

$$Z(u) := \prod_P (1 - u^{\deg P})^{-1} \tag{3.1}$$

where the product is over all monic irreducible polynomials in $\mathbb{F}_q[T]$. The product is absolutely convergent for $|u| < 1/q$.

By unique factorization into irreducibles in $\mathbb{F}_q[T]$, we have for $|u| < 1/q$,

$$Z(u) = \frac{1}{1 - qu}. \tag{3.2}$$

Taking the logarithmic derivative of (3.1) and (3.2) leads to the "Explicit formula"

$$\Psi(n) := \sum_{N \in \mathcal{M}_n} \Lambda(N) = q^n \tag{3.3}$$

from which we immediately deduce the Prime Polynomial Theorem, for the number $\pi(n)$ of monic irreducible polynomials of degree n:

$$\pi(n) = \frac{q^n}{n} + O(q^{n/2}). \tag{3.4}$$

Lemma 3.1.

$$\sum_{N \in \mathcal{M}_n} \Lambda(N)^2 = nq^n + O(n^2 q^{n/2}), \tag{3.5}$$

where the implied constant is absolute (independent of q and n). □

Proof. We start with the Explicit Formula (3.3)

$$\sum_{d|m} d\pi(d) = q^m \tag{3.6}$$

and hence

$$m\pi(m) \le q^m. \tag{3.7}$$

Now

$$q^n = \sum_{d|n} d\pi(d) = nq^n + \sum_{\substack{d|n \\ d<n}} d\pi(d) \tag{3.8}$$

and hence

$$\pi(n) = \frac{q^n}{n} + O(q^{n/2}). \tag{3.9}$$

Likewise

$$\sum_{N\in\mathcal{M}_n} \Lambda(N)^2 = \sum_{d|n} d^2\pi(d) = n^2\pi(n) + \sum_{\substack{d|n \\ d<n}} d^2\pi(d) \tag{3.10}$$

with remainder term bounded by

$$\sum_{\substack{d|n \\ d<n}} d^2\pi(d) \le \sum_{d\le n/2} d^2\pi(d) \le \sum_{1\le d\le n/2} nq^{d/2} \le nq\frac{q^{n/2}-1}{q-1} < 2nq^{n/2}. \tag{3.11}$$

Inserting (3.9) into (3.10) gives the claim. ■

3.2 Dirichlet characters

For a polynomial $Q(x)\in\mathbb{F}_q[T]$ of positive degree, we denote by $\Phi(Q)$ the order of the group $(\mathbb{F}_q[T]/(Q))^\times$ of invertible residues modulo Q. A Dirichlet character modulo Q is a homomorphism

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

that is, after extending χ to vanish on polynomials which are not coprime to Q, we require $\chi(fg)=\chi(f)\chi(g)$ for all $f,g\in\mathbb{F}_q[T]$, $\chi(1)=1$ and $\chi(f+hQ)=\chi(f)$ for all $f,h\in\mathbb{F}_q[T]$. The number of Dirichlet characters modulo Q is $\Phi(Q)$.

The orthogonality relations for Dirichlet characters are

$$\frac{1}{\Phi(Q)}\sum_{\chi \bmod Q} \bar\chi(A)\chi(N) = \begin{cases} 1 & N = A \bmod Q, \\ 0 & \text{otherwise}, \end{cases} \tag{3.12}$$

where the sum is over all Dirichlet characters mod Q and A is coprime to Q, and

$$\frac{1}{\Phi(Q)}\sum_{A \bmod Q} \chi_1(A)\bar\chi_2(A) = \begin{cases} 1 & \chi_1=\chi_2, \\ 0 & \text{otherwise}. \end{cases} \tag{3.13}$$

A Dirichlet character χ is "even" if $\chi(cF) = \chi(F)$ for $0 \neq c \in \mathbb{F}_q$. This is in analogy to the number field case, where a Dirichlet character is called "even" if $\chi(-1) = +1$, and "odd" if $\chi(-1) = -1$. The number $\Phi^{\mathrm{ev}}(Q)$ of even characters modulo Q is

$$\Phi^{\mathrm{ev}}(Q) = \frac{1}{q-1}\Phi(Q). \tag{3.14}$$

We require the following orthogonality relations for even Dirichlet characters.

Lemma 3.2. Let χ_1 and χ_2 be Dirichlet characters modulo T^m, $m > 1$. Suppose $\bar{\chi}_1\chi_2$ is even. Then

$$\frac{1}{q^{m-1}} \sum_{\substack{B \bmod T^m \\ B(0)=1}} \bar{\chi}_1(B)\chi_2(B) = \delta_{\chi_1,\chi_2}. \tag{3.15}$$

□

Proof. We start with the standard orthogonality relation

$$\frac{1}{\Phi(T^m)} \sum_{B \bmod T^m} \bar{\chi}_1(B)\chi_2(B) = \delta_{\chi_1,\chi_2}. \tag{3.16}$$

The only nonzero contributions in the sum are those B with $B(0) \neq 0$ (equivalently coprime to T^m). We can write each such B uniquely as $B = cB_1$, with $B_1(0) = 1$. Since $\bar{\chi}_1\chi_2$ is even, we have

$$\bar{\chi}_1\chi_2(cB_1) = \bar{\chi}_1\chi_2(B_1) \tag{3.17}$$

and hence

$$\sum_{B \bmod T^m} \bar{\chi}_1(B)\chi_2(B) = (q-1) \sum_{\substack{B \bmod T^m \\ B(0)=1}} \bar{\chi}_1(B)\chi_2(B). \tag{3.18}$$

Comparing with (3.16) and using $\Phi(T^m) = (q-1)q^{m-1}$ gives the required result. ■

3.3 Primitive characters

A character is *primitive* if there is no proper divisor $Q' \mid Q$ so that $\chi(F) = 1$ whenever F is coprime to Q and $F = 1 \bmod Q'$. Denoting by $\Phi_{\mathrm{prim}}(Q)$ the number of primitive characters

modulo Q, we clearly have $\Phi(Q) = \sum_{D|Q} \Phi_{\text{prim}}(D)$ and hence by Möbius inversion,

$$\Phi_{\text{prim}}(Q) = \sum_{D|Q} \mu(D)\Phi\left(\frac{Q}{D}\right) \tag{3.19}$$

the sum over all monic polynomials dividing Q. Therefore,

$$\left|\frac{\Phi_{\text{prim}}(Q)}{\Phi(Q)} - 1\right| \leq \frac{2^{\deg Q}}{q}. \tag{3.20}$$

Hence as $q \to \infty$, almost all characters are primitive in the sense that

$$\frac{\Phi_{\text{prim}}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right), \tag{3.21}$$

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

Likewise, the number $\Phi^{\text{ev}}_{\text{prim}}(Q)$ of primitive even characters is given by

$$\Phi^{\text{ev}}_{\text{prim}}(Q) = \sum_{D|Q} \mu(D)\Phi^{\text{ev}}\left(\frac{Q}{D}\right) = \frac{1}{q-1}\sum_{D|Q} \mu(D)\Phi\left(\frac{Q}{D}\right). \tag{3.22}$$

For instance, for $Q(T) = T^m$, $m \geq 2$, we find

$$\Phi^{\text{ev}}_{\text{prim}}(T^m) = q^{m-2}(q-1). \tag{3.23}$$

The number $\Phi^{\text{prim}}_{\text{odd}}(Q)$ of odd primitive characters is then

$$\Phi^{\text{odd}}_{\text{prim}}(Q) = \Phi_{\text{prim}}(Q) - \Phi^{\text{ev}}_{\text{prim}}(Q) = \left(1 - \frac{1}{q-1}\right)\Phi_{\text{prim}}(Q) \tag{3.24}$$

and hence we find that as $q \to \infty$ with $\deg Q$ fixed, almost all characters are primitive and odd:

$$\frac{\Phi^{\text{odd}}_{\text{prim}}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right), \tag{3.25}$$

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

3.4 L-functions

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

$$\mathcal{L}(u, \chi) = \prod_{P \nmid Q} (1 - \chi(P) u^{\deg P})^{-1}, \tag{3.26}$$

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

$$\mathcal{L}(u, \chi_0) = Z(u) \prod_{P | Q} (1 - u^{\deg P}). \tag{3.27}$$

The basic fact about $\mathcal{L}(u, \chi)$ is that 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 $\mathcal{L}(u, \chi)$ is a polynomial in u of degree $\deg Q - 1$.

Moreover, if χ is an "even" character, that is, $\chi(cF) = \chi(F)$ for $0 \neq c \in \mathbb{F}_q$, then there is a "trivial" zero at $u = 1$: $\mathcal{L}(1, \chi) = 0$ and hence

$$\mathcal{L}(u, \chi) = (1 - u) P(u, \chi), \tag{3.28}$$

where $P(u, \chi)$ is a polynomial of degree $\deg Q - 2$.

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

$$\mathcal{L}(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j(\chi) u). \tag{3.29}$$

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

$$|\alpha_j(\chi)| = q^{1/2}. \tag{3.30}$$

We define

$$\Psi(n, \chi) := \sum_{\deg f = n} \Lambda(f) \chi(f), \tag{3.31}$$

the sum over monic polynomials of degree n. Taking logarithmic derivative of the L-function gives a formula for $\Psi(n, \chi)$ in terms of the inverse roots $\alpha_j(\chi)$: If $\chi \neq \chi_0$ is non-trivial, then

$$\Psi(n, \chi) = -\sum_{j=1}^{\deg Q-1} \alpha_j(\chi)^n. \tag{3.32}$$

Weil's theorem (3.30) gives for $n > 0$

$$|\Psi(n, \chi)| \leq (\deg Q - 1)q^{n/2}, \quad \chi \neq \chi_0. \tag{3.33}$$

3.5 The unitarized Frobenius matrix

We may state the results in cleaner form if we assume that χ is a *primitive* character modulo Q.

We also define

$$\lambda_\chi := \begin{cases} 1 & \chi \text{ "even"}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.34}$$

Then for $Q \in \mathbb{F}_q[T]$ a polynomial of degree ≥ 2, and χ a primitive Dirichlet character modulo Q,

$$L^*(u, \chi) := (1 - \lambda_\chi u)^{-1} L(u, \chi)$$

is a polynomial of degree

$$N = \deg Q - 1 - \lambda_\chi \tag{3.35}$$

so that $L^*(u, \chi) = \prod_{j=1}^{N}(1 - \alpha_j(\chi)u)$ and

$$|\alpha_j| = \sqrt{q} \quad \forall j = 1, \ldots, N. \tag{3.36}$$

For a primitive character modulo Q, we write the inverse roots as $\alpha_j = q^{1/2}\, e^{i\theta_j}$ and the completed L-function $L^*(u, \chi)$ as

$$L^*(u, \chi) = \det(I - uq^{1/2}\Theta_\chi), \quad \Theta_\chi = \operatorname{diag}(e^{i\theta_1}, \ldots, e^{i\theta_N}). \tag{3.37}$$

The unitary matrix Θ_χ (or rather, the conjugacy class of unitary matrices) is called the unitarized Frobenius matrix of χ.

Taking the logarithmic derivative of (3.37) we obtain an explicit formula for primitive characters:

$$\Psi(n,\chi) = -q^{n/2}\mathrm{tr}\Theta_\chi^n - \lambda_\chi. \tag{3.38}$$

4 Prime Polynomials in Short Intervals

In this section, we prove Theorem 2.1, the analog of the Goldston–Montgomery result (1.3).

4.1 An involution

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

$$f^*(T) := T^{\deg f} f\left(\frac{1}{T}\right) \tag{4.1}$$

or if $f(T) = f_0 + f_1 T + \cdots + f_n T^n$, $n = \deg f$ (so that $f_n \neq 0$), then f^* is the "reversed" polynomial

$$f^*(T) = f_0 T^n + f_1 T^{n-1} + \cdots + f_n. \tag{4.2}$$

We also set $0^* = 0$.

Note that $f^*(0) \neq 0$ and $f(0) \neq 0$ if and only if $\deg f^* = \deg f$. Moreover restricted to polynomials which do not vanish at 0, equivalently are co-prime to T, then $*$ is an involution:

$$f^{**} = f, \quad f(0) \neq 0. \tag{4.3}$$

We also have multiplicativity:

$$(fg)^* = f^* g^*. \tag{4.4}$$

Lemma 4.1. For $f \in \mathcal{P}_n$ with $f(0) \neq 0$, we have $\Lambda(f^*) = \Lambda(f)$. □

Proof. For polynomials which do not vanish at 0, that is, are co-prime to T, P is irreducible if and only if P^* is irreducible. This is because if $P = AB$ with A, B of positive degree, then $P^* = (AB)^* = A^* B^*$ and if $P(0) \neq 0$, then the same holds for A, B and then $\deg A^* = \deg A > 0$, $\deg B^* = \deg B > 0$ so P is reducible; applying * again and using that it is an involution (since $P(0) \neq 0$) gives the reverse implication. ■

4.2 A fundamental relation

We can now express the number of primes in our short intervals in terms of the number of primes in a suitable arithmetic progression. Define

$$\tilde{\Psi}(n; Q, A) = \sum_{\substack{f \in \mathcal{P}_n \\ f = A \bmod Q}} \Lambda(f), \tag{4.5}$$

the sum over all polynomials of degree n, not necessarily monic.

Lemma 4.2. For $B \in \mathcal{P}_{n-h-1}$,

$$\nu(T^{h+1}B; h) = \tilde{\Psi}(n; T^{n-h}, B^*). \tag{4.6}$$

□

Proof. Let $B \in \mathcal{P}_{n-h-1}$. We have $f = T^{h+1}B + g \in I(T^{h+1}B; h)$, $g \in \mathcal{P}_{\leq h}$ if and only if $f^* = B^* + T^{n-h}g^*$, and thus we find

$$f \in I(T^{h+1}B; h) \Leftrightarrow f^* \equiv B^* \bmod T^{n-h}. \tag{4.7}$$

As f runs over $I(T^{h+1}B; h)$ with the proviso that $f(0) \neq 0$, f^* runs over all polynomials of degree exactly n satisfying $f^* \equiv B^* \bmod T^{n-h}$, and for these $\Lambda(f) = \Lambda(f^*)$. ■

4.3 Averaging

We want to compute the mean value and variance of $\nu(A, h)$. To perform the average over A, note that every monic polynomial $f \in \mathcal{M}_n$ can be written uniquely as

$$f = T^{h+1}B + g, \quad B \in \mathcal{M}_{n-(h+1)}, \quad g \in \mathcal{P}_{\leq h}. \tag{4.8}$$

We therefore can decompose $\mathcal{M}_n$ as the disjoint union of "intervals" $I(T^{h+1}B; h)$ parameterized by $B \in \mathcal{M}_{n-(h+1)}$:

$$\mathcal{M}_n = \coprod_{B \in \mathcal{M}_{n-(h+1)}} I(T^{h+1}B; h). \tag{4.9}$$

To compute averages ν on short intervals, it suffices, by the foregoing, to take $A = T^{h+1}B$ and to average over all $B \in \mathcal{M}_{n-(h+1)}$.

The map $*$ gives a bijection

$$\begin{aligned} *: \mathcal{M}_{n-(h+1)} &\to \{B^* \in \mathcal{P}_{\leq (n-h-1)} : B^*(0) = 1\}, \\ B &\mapsto B^* \end{aligned} \tag{4.10}$$

with polynomials of degree $\leq n-(h+1)$ with constant term 1. Thus, as B ranges over $\mathcal{M}_{n-(h+1)}$, B^* ranges over $(\mathbb{F}_q[T]/(T^{n-h}))^\times$, all invertible residue class mod T^{n-h} so that $B^*(0) = 1$.

Thus, the mean value is

$$\begin{aligned} \langle \nu(\bullet; h)\rangle &= \frac{1}{\#\mathcal{M}_{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \nu(T^{h+1}B; , h) \\ &= \frac{1}{q^{n-h-1}} \sum_{\substack{B^* \bmod T^{n-h} \\ B^*(0)=1}} \tilde{\Psi}(n; T^{n-h}, B^*) \end{aligned} \tag{4.11}$$

and the variance is

$$\begin{aligned} \mathrm{Var}(\nu(\bullet; h)) &= \frac{1}{\#\mathcal{M}_{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} |\nu(T^{h+1}B; , h) - \langle \nu\rangle|^2 \\ &= \frac{1}{q^{n-h-1}} \sum_{\substack{B^* \bmod T^{n-h} \\ B^*(0)=1}} |\tilde{\Psi}(n; T^{n-h}, B^*) - \langle \nu\rangle|^2. \end{aligned} \tag{4.12}$$

4.4 The mean value

The computation of the mean value $\langle \nu(\bullet; h)\rangle = \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \nu(A; h)$ is a simple consequence of the Prime Polynomial Theorem. The result is the following.

Lemma 4.3. Let $0 < h < n$. The mean value of $\nu(A, ; h)$ is

$$\langle \nu(\bullet; h)\rangle = q^{h+1}\left(1 - \frac{1}{q^n}\right). \tag{4.13}$$

□

Proof. We do the computation in two different ways as a check of the all-important relation (4.6). By using the definition of ν, we obtain

$$\langle \nu(\bullet; h)\rangle = \frac{1}{\#\mathcal{M}_{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \sum_{\substack{f \in I(T^{h+1}B; h) \\ f(0) \neq 0}} \Lambda(f)$$

$$= \frac{1}{\#\mathcal{M}_{n-h-1}} \left(\sum_{f \in \mathcal{M}_n} \Lambda(f) - \Lambda(T^n) \right). \tag{4.14}$$

Note that

$$\#\mathcal{M}_{n-h-1} = q^{n-h-1} = \frac{\Phi(T^{n-h})}{q-1}. \tag{4.15}$$

Using (4.6), the mean value of $\nu(\bullet; h)$ is

$$\begin{aligned}
\langle \nu(\bullet; h) \rangle &= \frac{1}{\Phi(T^{n-h})} \sum_{\substack{B^* \bmod T^{n-h} \\ B^*(0)=1}} \tilde{\Psi}(n; T^{n-h}, B^*) \\
&= \frac{1}{\Phi(T^{n-h})} \sum_{\substack{\deg f^* = n \\ f^*(0)=1}} \Lambda(f^*) \\
&= \frac{1}{\Phi(T^{n-h})} \left(\sum_{\deg f^* = n} \Lambda(f^*) - \sum_{c \in \mathbb{F}_q^*} \Lambda(cT^n) \right) \\
&= \frac{1}{q^{n-h-1}} \left(\sum_{f^* \in \mathcal{M}_n} \Lambda(f^*) - \Lambda(T^n) \right).
\end{aligned} \tag{4.16}$$

Hence

$$\langle \nu(\bullet; h) \rangle = \frac{1}{q^{n-h-1}} (q^n - 1) = q^{h+1} \left(1 - \frac{1}{q^n} \right) \tag{4.17}$$

on using the Prime Polynomial Theorem in the form (3.3). ■

4.5 An alternate expression for $\nu(A; h)$

Using the standard orthogonality relation (3.16) for Dirichlet characters modulo T^{n-h} gives an alternate expression for $\tilde{\Psi}(n; T^{n-h}, B^*)$ and hence for $\nu(T^{h+1}B; h)$:

$$\tilde{\Psi}(n; T^{n-h}, B^*) = \frac{1}{\Phi(T^{n-h})} \sum_{\chi \bmod T^{n-h}} \bar{\chi}(B^*) \sum_{\deg f^* = n} \Lambda(f^*) \chi(f^*). \tag{4.18}$$

Only *even* characters give a nonzero term, because $\Lambda(cf) = \Lambda(f)$ for $c \in \mathbb{F}_q^\times$, and each even character contributes a term

$$\bar{\chi}(B^*) \frac{q-1}{\Phi(T^{n-h})} \sum_{\substack{\deg f = n \\ \text{monic}}} \Lambda(f) \chi(f) = \bar{\chi}(B^*) \frac{1}{q^{n-h-1}} \Psi(n, \chi), \tag{4.19}$$

where

$$\Psi(n,\chi)=\sum_{\substack{\deg f=n\\ \text{monic}}}\Lambda(f)\chi(f). \tag{4.20}$$

Note that the number of even characters mod T^{n-h} is exactly $\frac{1}{q-1}\Phi(T^{n-h})=q^{n-h-1}$.

The trivial character χ_0 contributes the term

$$\frac{(q-1)(q^n-1)}{\Phi(T^{n-h})}=q^{h+1}\left(1-\frac{1}{q^n}\right)=\langle\nu\rangle. \tag{4.21}$$

Thus, we find that the difference between $\nu(T^{h+1}B;h)$ and its mean $\langle\nu\rangle$ is

$$\nu(T^{h+1}B;h)-\langle\nu\rangle=\frac{1}{q^{n-h-1}}\sum_{\chi\neq\chi_0\ \underset{\text{even}}{\bmod} T^{n-h}}\bar{\chi}(B^*)\Psi(n,\chi). \tag{4.22}$$

4.6 The variance

Our result here is the following.

Theorem 4.4. Fix $n>0$ and let $0<h<n$. As $q\to\infty$, the variance of ν is given by

$$\mathrm{Var}(\nu)=q^{h+1}\cdot\left(\frac{1}{q^{n-h-1}}\sum_{\chi}^{*}|\mathrm{tr}\Theta_\chi^n|^2+O\left(\frac{n-h}{q^{n/2}}+\frac{n^2}{q}\right)\right), \tag{4.23}$$

where the sum is over primitive even characters modulo T^{n-h}, the implied constant depending only on n. □

Proof. By (4.22), we have

$$\mathrm{Var}(\nu)=\frac{1}{q^{n-h-1}}\sum_{\substack{B^*\ \bmod T^{n-h}\\ B^*(0)=1}}\frac{1}{q^{2(n-h-1)}}\left|\sum_{\substack{\chi\neq\chi_0\\ \text{even}}}\bar{\chi}(B^*)\Psi(n,\chi)\right|^2. \tag{4.24}$$

Expanding the sum over characters, and interchanging the order of summation to use the orthogonality relation of Lemma 3.2 gives

$$\mathrm{Var}(\nu)=\frac{1}{q^{2(n-h-1)}}\sum_{\substack{\chi\neq\chi_0\\ \text{even}}}|\Psi(n,\chi)|^2. \tag{4.25}$$

There are altogether $\varphi(T^{n-h})/(q-1) = q^{n-h-1}$ even characters modulo T^{n-h}, of which $O(q^{n-h-2})$ are nonprimitive. We bound the contribution of the nontrivial nonprimitive characters by $\Psi(n,\chi) = O(nq^{n/2})$ via the RH. Thus, the nonprimitive characters contribute a total of $O(n^2q^h)$ to $\mathrm{Var}(\nu)$.

Using the explicit formula (3.38) for primitive even characters and the RH gives

$$|\Psi(n,\chi)|^2 = q^n|\mathrm{tr}\Theta_\chi^n|^2 + O((n-h)q^{n/2}). \tag{4.26}$$

Therefore,

$$\mathrm{Var}(\nu) = q^{h+1}\cdot\left(\frac{1}{q^{n-h-1}}\sideset{}{^*}\sum_\chi |\mathrm{tr}\Theta_\chi^n|^2 + O\left(\frac{n-h}{q^{n/2}} + \frac{n^2}{q}\right)\right), \tag{4.27}$$

where the sum is over primitive even characters modulo T^{n-h}, whose number is $q^{n-h-1}(1-\frac{1}{q})$. ■

4.7 Proof of Theorem 2.1

Thus, we found that for $h < n-3$, the variance of ν is given by

$$\frac{1}{q^{h+1}}\mathrm{Var}(\nu) = \left(1-\frac{1}{q}\right)\langle|\mathrm{tr}\Theta_\chi^n|^2\rangle + O\left(\frac{n-h}{q^{n/2}} + \frac{n^2}{q}\right) \tag{4.28}$$

with $\langle|\mathrm{tr}\Theta_\chi^n|^2\rangle$ being the mean value of $|\mathrm{tr}\Theta_\chi^n|^2$ over the set of all primitive even Dirichlet characters modulo T^{n-h}. Thus, as $q\to\infty$, $\mathrm{Var}(\nu)/q^{h+1}$ is asymptotically equal to the "form factor" $\langle|\mathrm{tr}\Theta_\chi^n|^2\rangle$.

To proceed further, we need to invoke a recent result of Katz [12]:

Theorem 4.5. [12, Theorem 1.2] Fix $m\geq 3$. The unitarized Frobenii Θ_χ for the family of even primitive characters mod T^{m+1} become equidistributed in the projective unitary group $\mathrm{PU}(m-1)$ of size $m-1$, as $q\to\infty$. □

Applying Theorem 4.5 gives

$$\lim_{q\to\infty}\frac{1}{q^{n-h-1}(1-\frac{1}{q})}\sideset{}{^*}\sum_\chi |\mathrm{tr}\Theta_\chi^n|^2 = \int_{\mathrm{PU}(n-h-2)}|\mathrm{tr}U^n|^2\,\mathrm{d}U. \tag{4.29}$$

We may pass from the projective unitary group $\mathrm{PU}(n-h-2)$ to the unitary group because the function $|\mathrm{tr}U^n|^2$ being averaged is invariant under scalar multiplication. As is well known (see, e.g., [3]), for $n>0$,

$$\int_{U(N)} |\mathrm{tr}U^n|^2 \, \mathrm{d}U = \min(n, N). \tag{4.30}$$

Therefore, we find

$$\mathrm{Var}(\nu) \sim q^{h+1}(n-h-2), \quad q \to \infty. \tag{4.31}$$

This concludes the proof of Theorem 2.1.

5 Prime Polynomials in Arithmetic Progressions

In this section, we prove Theorem 2.2, giving the function field analog of the conjectures of Hooley (1.10) and Friedlander–Goldston (1.13).

5.1 The range $n < \deg Q$

We prove the result in the range $n < \deg Q$ by elementary arguments:

Proposition 5.1. For $0 < n < \deg Q$, we have

$$G(n; Q) = nq^n - \frac{q^{2n}}{\Phi(Q)} + O(n^2 q^{n/2}) + O((\deg Q)^2), \tag{5.1}$$

where the implied constant is independent of q, n, and Q. □

Proof. Assume as we may that $\deg A < \deg Q$. If $n < \deg Q$ then the only solution to the congruence $N = A \bmod Q$, with $\deg N = n < \deg Q$ is A (if $\deg A = n$) or else there is no solution. Therefore, if $n < \deg Q$, then

$$\Psi(n; Q, A) = \begin{cases} \Lambda(A) & A \text{ is monic and } \deg A = n, \\ 0 & \text{otherwise.} \end{cases} \tag{5.2}$$

Thus,

$$G(n;\,Q)=\sum_{\gcd(A,Q)=1}\left|\frac{q^n}{\Phi(Q)}-\begin{cases}\Lambda(A) & A \text{ is monic and } \deg A=n\\ 0 & \text{otherwise}\end{cases}\right|^2$$

$$=\sum_{\substack{\deg A=n\\ A \text{ monic}\\ \gcd(A,Q)=1}}\Lambda(A)^2-2\frac{q^n}{\Phi(Q)}\sum_{\substack{\deg A=n\\ A \text{ monic}\\ \gcd(A,Q)=1}}\Lambda(A)+\frac{q^{2n}}{\Phi(Q)}.$$

By the Prime Polynomial Theorem (3.3),

$$\sum_{\substack{\deg A=n\\ A \text{ monic}\\ \gcd(A,Q)=1}}\Lambda(A)=q^n-\sum_{\substack{P\mid Q \text{ prime}\\ \deg P\mid n}}\deg P=q^n+O(\deg Q). \tag{5.3}$$

According to Lemma 3.1,

$$\sum_{\substack{\deg A=n\\ A \text{ monic}\\ \gcd(A,Q)=1}}\Lambda(A)^2=\sum_{\deg A=n}\Lambda(A)^2-\sum_{\substack{P\mid Q\\ \deg P\mid n}}(\deg P)^2$$

$$=nq^n+O(n^2q^{n/2})+O((\deg Q)^2) \tag{5.4}$$

and so we find

$$G(n;\,Q)=nq^n-\frac{q^{2n}}{\Phi(Q)}+O(n^2q^{n/2})+O((\deg Q)^2)+O\left(\frac{q^n}{\Phi(Q)}\deg Q\right). \tag{5.5}$$

Since for $n<\deg Q$,

$$\frac{q^n}{\Phi(Q)}\le\frac{1}{q}\prod_{\substack{P\mid Q\\ \text{prime}}}\left(1-\frac{1}{|P|}\right)^{-1}\le\frac{1}{q}\prod_{\substack{\deg P\le\deg Q\\ \text{prime}}}\left(1-\frac{1}{|P|}\right)^{-1}\ll\frac{\deg Q}{q}, \tag{5.6}$$

we find

$$G(n;\,Q)=nq^n-\frac{q^{2n}}{\Phi(Q)}+O(n^2q^{n/2})+O((\deg Q)^2) \tag{5.7}$$

as claimed. ■

5.2 The range $n \geq \deg Q$

To deal with the range $n \geq \deg Q$ we relate the problem to an equidistribution statement for the unitarized Frobenii of primitive odd characters. It transpires that $G(n; Q)$ is related to the mean value of the modulus squared of the trace of the Frobenius matrices associated with the family of Dirichlet L-functions for characters modulo Q:

Theorem 5.2. Fix n and let $Q \in \mathbb{F}_q[T]$ have degree $\deg Q \geq 2$. Then

$$\frac{G(n; Q)}{q^n} = \langle |\mathrm{tr}\Theta_\chi^n|^2 \rangle \left(1 + \frac{1}{q}\right) + O\left(\frac{(\deg Q)^2}{q}\right), \tag{5.8}$$

where $\langle\rangle$ denotes the average over all odd primitive characters modulo Q. □

Proof. The orthogonality relation (3.12) gives

$$\begin{aligned}\Psi(n; Q, A) &= \frac{1}{\Phi(Q)} \sum_{\chi \bmod Q} \bar{\chi}(A) \sum_{\deg N = n} \chi(N)\Lambda(N) \\ &= \frac{1}{\Phi(Q)} \sum_{\chi \bmod Q} \bar{\chi}(A)\Psi(n, \chi).\end{aligned} \tag{5.9}$$

The trivial character χ_0 gives a contribution of

$$\frac{1}{\Phi(Q)} \sum_{\substack{\deg N = n \\ \gcd(N, Q) = 1}} \Lambda(N) = \frac{q^n}{\Phi(Q)} - \frac{1}{\Phi(Q)} \sum_{\substack{P | Q \\ \deg P | n}} \deg P. \tag{5.10}$$

Hence,

$$\Psi(n; Q, A) - \frac{q^n}{\Phi(Q)} = -\frac{1}{\Phi(Q)} \sum_{\substack{P | Q \\ \deg P | n}} \deg P + \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0} \chi(A)\Psi(n, \chi). \tag{5.11}$$

We square out and average over all A mod Q coprime with Q. Using the orthogonality relation (3.13) gives

$$G(n; Q) = \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0} |\Psi(n, \chi)|^2 + \frac{1}{\Phi(Q)} \left(\sum_{\substack{P | Q \\ \deg P | n}} \deg P \right)^2. \tag{5.12}$$

For nontrivial characters which are either even or imprimitive, we use the RH (3.33) to bound $|\Psi(n,\chi)|^2 \le q^n(\deg Q-1)^2$. Therefore, we find

$$G(n;Q)=\frac{1}{\Phi(Q)}\sum_{\chi \text{ primitive, odd}}|\Psi(n,\chi)|^2 + O\left(q^n(\deg Q)^2\frac{\#\{\chi \text{ either even or imprimitive}\}}{\Phi(Q)}\right). \tag{5.13}$$

The number of even characters is $\Phi(Q)/(q-1)$, and the number of imprimitive characters is $O(\Phi(Q)/q)$. Hence the remainder term above is bounded by $O(q^{n-1}(\deg Q)^2)$.

For each primitive odd character, the "explicit formula" (3.38) says

$$\Psi(n,\chi)=-q^{n/2}\mathrm{tr}\Theta_\chi^n \tag{5.14}$$

and therefore

$$G(n;Q)=q^n\frac{1}{\Phi(Q)}\sum_{\chi \text{ odd primitive}}\left|\mathrm{tr}\Theta_\chi^n\right|^2+O(q^{n-1}(\deg Q)^2). \tag{5.15}$$

Replacing $\Phi(Q)$ by the number of odd primitive characters times $1+O(\frac{1}{q})$ gives (5.8). ■

We now use another recent equidistribution result of Katz [11]:

Theorem 5.3 (Katz [11]). Fix $m\ge 2$. Suppose that we are given a sequence of finite fields $\mathbb{F}_q$ and square-free 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 $U(m-1)$. □

Note that Theorem 5.3 gives a "nonstandard" form of equidistribution, in that it deals with a family of L-functions which are not parameterized by an algebraic variety. Its proof in [11] relies on the recent book [10] which studies such cases.

Using Theorem 5.3 we obtain for $n>0$,

$$\lim_{q\to\infty}\langle|\mathrm{tr}\Theta_\chi^n|^2\rangle=\int_{U(\deg Q-1)}|\mathrm{tr}U^n|^2\,dU, \tag{5.16}$$

where $\mathrm{d}U$ is the Haar probability measure on the unitary group $U(N)$. Since [3]

$$\int_{U(N)} |\mathrm{tr}U^n|^2 \, \mathrm{d}U = \min(n, N), \tag{5.17}$$

we find

$$\lim_{q\to\infty} \frac{G(n; Q)}{q^n} = \min(n, \deg Q - 1), \tag{5.18}$$

which is the statement of Theorem 2.2.

Acknowledgements

We thank Nick Katz for several discussions, and Julio Andrade and the referees for their comments.

Funding

J.P.K was supported by a grant from the Leverhulme Trust and by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant number FA8655-10-1-3088. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purpose notwithstanding any copyright notation thereon. Z.R. was supported by the Israel Science Foundation (grant No. 1083/10).

Appendix 1. A Calculation Based on a Hardy–Littlewood-Type Conjecture

In the number-field setting, the problems we have considered here have previously been explored using the Hardy–Littlewood conjecture relating to the density of generalized twin primes [4, 14]. In this appendix, we sketch a heuristic calculation showing how the corresponding conjecture in the function field setting may be used in the same way. As an example, we focus on estimating $G(n, Q)$.

The twin prime conjecture of Hardy and Littlewood for the rational function field $\mathbb{F}_q[T]$ states that, given a polynomial $0 \neq K \in \mathbb{F}_q[T]$, and $n > \deg K$,

$$\sum_{\deg f = n} \Lambda(f)\Lambda(f + K) \sim \mathfrak{S}(K) q^n \tag{A.1}$$

as $q^n \to \infty$, where the "singular series" $\mathfrak{S}(K)$ is given by

$$\mathfrak{S}(K) = \prod_P \left(1 - \frac{1}{|P|}\right)^{-2} \left(1 - \frac{\nu_K(P)}{|P|}\right), \tag{A.2}$$

with the product involving all monic irreducible P and

$$\nu_K(P) = \#\{A \bmod P : A(A+K) = 0 \bmod P\} = \begin{cases} 1, & P \mid K, \\ 2, & P \nmid K. \end{cases} \tag{A.3}$$

While for fixed q and $n \to \infty$ the problem is currently completely open, for fixed n and $q \to \infty$, (A.1) is known to hold [1, 2] for q odd, in the form

$$\sum_{\deg f = n} \Lambda(f)\Lambda(f+K) = q^n + O_n(q^{n-\frac{1}{2}}). \tag{A.4}$$

Note that $\mathfrak{S}(K) = 1 + O_n(\frac{1}{q})$.

We want to use (A.1) to compute $G(n; Q)$ and to show that the result is consistent with

$$G(n; Q) \sim q^n(\deg Q - 1), \quad n > \deg Q. \tag{A.5}$$

It turns out that this can be done if we ignore the contribution from the remainder implicit in (A.1). The remainder term in (A.4) is insufficient for our purposes.

Starting with

$$G(n; Q) = \sum_{\gcd(A,Q)=1} \left| \Psi(n; Q, a) - \frac{q^n}{\Phi(Q)} \right|^2, \tag{A.6}$$

we have

$$G(n; Q) = \sum_{\gcd(A,Q)=1} \Psi(n; Q, A)^2 - 2\frac{q^n}{\Phi(Q)} \sum_{\gcd(A,Q)=1} \Psi(n; Q, A) + \frac{q^{2n}}{\Phi(Q)}. \tag{A.7}$$

The first moment of $\Psi(n; Q, A)$ is

$$\sum_{\gcd(A,Q)=1} \Psi(n; Q, A) = \sum_{\substack{\deg f=n \\ \gcd(f,Q)=1}} \Lambda(f)$$

$$= \sum_{\deg f=n} \Lambda(f) - \sum_{\substack{\deg f=n \\ \deg \gcd(f,Q)>0}} \Lambda(f)$$

$$= q^n - \sum_{\substack{\deg P \mid n \\ P \mid Q \text{ prime}}} \deg P. \tag{A.8}$$

By Lemma 3.1, we may safely replace

$$\sum_{\gcd(A,Q)=1} \Psi(n; Q, A) = q^n + \text{negligible}. \tag{A.9}$$

For the second moment of $\Psi(n; Q, A)$ we have

$$\sum_{\gcd(A,Q)=1} \Psi(n; Q, A)^2 = \sum_{\substack{\deg f=\deg g=n \\ f\equiv g \bmod Q \\ \gcd(f,Q)=1}} \Lambda(f)\Lambda(g)$$

$$= \sum_{\substack{\deg f=n \\ \gcd(f,Q)=1}} \Lambda(f)^2 + \sum_{\substack{\deg f=\deg g=n \\ f\equiv g \bmod Q \\ f\neq g \\ \gcd(f,Q)=1}} \Lambda(f)\Lambda(g). \tag{A.10}$$

Now

$$\sum_{\substack{\deg f=n \\ \gcd(f,Q)=1}} \Lambda(f)^2 = nq^n + O(n^2 q^{n/2}) - \sum_{\substack{P \mid Q \\ \deg P \mid n}} (\deg P)^2. \tag{A.11}$$

For the sum over $f \neq g$, we write the condition $f = g \bmod Q$ as $g = f + JQ$, $J \neq 0$, $\deg J < n - \deg Q$ (the number of such J of degree j is $(q-1)q^j$) and then

$$\sum_{\substack{\deg f=\deg g=n \\ f\equiv g \bmod Q \\ f\neq g \\ \gcd(f,Q)=1}} \Lambda(f)\Lambda(g) = \sum_{\substack{\deg J<n-\deg Q \\ J\neq 0}} \psi_2(n; JQ), \tag{A.12}$$

where for $K \neq 0$, $\deg K < n$,

$$\psi_2(n; K) := \sum_{\substack{\deg f = n \\ f \text{ monic}}} \Lambda(f)\Lambda(f+K). \tag{A.13}$$

Clearly, we can split the right-hand side of (A.12 as follows:

$$\sum_{\substack{\deg f = \deg g = n \\ f \equiv g \bmod Q \\ f \neq g \\ \gcd(f,Q)=1}} \Lambda(f)\Lambda(g) = \sum_{j=0}^{n-\deg Q} \sum_{\substack{\deg J = j \\ J \neq 0}} \psi_2(n; JQ). \tag{A.14}$$

The J-sum here is not restricted to monic polynomials. We can restrict it to monics, multiplying by $q-1$. Then inserting (A.1), we have

$$\sum_{\substack{\deg f = \deg g = n \\ f \equiv g \bmod Q \\ f \neq g \\ \gcd(f,Q)=1}} \Lambda(f)\Lambda(g) \sim q^n(q-1) \sum_{j=0}^{n-\deg Q} \sum_{\substack{\deg J = j \\ J \neq 0 \\ J \text{ monic}}} \mathfrak{S}(JQ) \tag{A.15}$$

as $q^n \to \infty$.

In order to estimate the J-sum in (A.15), consider

$$\sum_{J \text{ monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha \sum_{J \text{ monic}} \frac{1}{|J|^s} \prod_{P \mid JQ} \frac{|P|-1}{|P|-2}, \tag{A.16}$$

where the equality follows from inserting (A.2) and

$$\alpha = \prod_P \left(1 - \frac{1}{(|P|-1)^2}\right). \tag{A.17}$$

Hence,

$$\sum_{J \text{ monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha \prod_{P \mid Q} \frac{|P|-1}{|P|-2} \sum_{J \text{ monic}} \frac{1}{|J|^s} \prod_{\substack{P \mid J \\ P \nmid Q}} \frac{|P|-1}{|P|-2}. \tag{A.18}$$

Since the summand on the right-hand side is multiplicative, we may write this as

$$\sum_{J \text{ monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha \prod_{P \mid Q} \frac{|P|-1}{|P|-2} \prod_{P \nmid Q} \left(1 + \frac{1}{|P|^s - 1} \frac{|P|-1}{|P|-2}\right) \prod_{P \mid Q} \left(1 - \frac{1}{|P|^s}\right)^{-1}. \tag{A.19}$$

Therefore,

$$\sum_{J\,\text{monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha\zeta_A(s) \prod_{P|Q} \frac{|P|-1}{|P|-2} \prod_{P\nmid Q} \left(1 + \frac{1}{|P|^s(|P|-2)}\right) \tag{A.20}$$

with

$$\zeta_A(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1}. \tag{A.21}$$

Hence,

$$\sum_{J\,\text{monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha\zeta_A(s) \prod_{P|Q} \frac{|P|-1}{|P|-2} \left(1 + \frac{1}{|P|^s(|P|-2)}\right)^{-1} \prod_P \left(1 + \frac{1}{|P|^s(|P|-2)}\right). \tag{A.22}$$

Furthermore,

$$\sum_{J\,\text{monic}} \frac{\mathfrak{S}(JQ)}{|J|^s} = \alpha\zeta_A(s)\zeta_A(s+1) \prod_{P|Q} \frac{|P|-1}{|P|-2} \left(1 + \frac{1}{|P|^s(|P|-2)}\right)^{-1} \times \prod_P \left(1 + \frac{2}{|P|^{s+1}(|P|-2)} - \frac{|P|}{|P|-2}\frac{1}{|P|^{2s+2}}\right). \tag{A.23}$$

It is convenient to re-express these formulae in terms of the variable $u = 1/q^s$. Thus, $|J| = u^{-\deg J}$, $|P| = u^{-\deg P}$, and

$$\sum_{J\,\text{monic}} \mathfrak{S}(JQ)u^{\deg J} = \alpha Z(u)Z(u/q) \prod_{P|Q} \frac{|P|-1}{|P|-2} \left(1 + \frac{u^{\deg P}}{(|P|-2)}\right)^{-1} \times \prod_P \left(1 + \frac{2u^{\deg P}}{|P|(|P|-2)} - \frac{u^{2\deg P}}{|P|(|P|-2)}\right) \tag{A.24}$$

with

$$Z(u) = \prod_P (1 - u^{\deg P})^{-1} = \frac{1}{1-qu}. \tag{A.25}$$

We can now estimate the J-sum in (A.15) by denoting

$$F(u) = \sum_{J\,\text{monic}} \mathfrak{S}(JQ)u^{\deg J} \tag{A.26}$$

and using

$$\sum_{\substack{\deg J=j\\ J\neq 0\\ J\,\text{monic}}} \mathfrak{S}(JQ) = \frac{1}{2\pi \mathrm{i}} \oint \frac{F(u)}{u^{j+1}}\,\mathrm{d}u, \tag{A.27}$$

where the contour is a small circle enclosing the origin but no other singularities of the integrand. Expanding the contour beyond the poles of $F(u)$ at $u=1/q$ and $u=1$ (coming from the factors of $Z(u)$ and $Z(u/q)$ in (A.24)), we find that as $q\to\infty$

$$\sum_{\substack{\deg J=j\\ J\neq 0\\ J\,\text{monic}}} \mathfrak{S}(JQ) \sim q^j \frac{|Q|}{\Phi(Q)} - \frac{1}{q-1}, \tag{A.28}$$

where we have used

$$\prod_{P\mid Q} \frac{|P|}{|P|-1} = \frac{|Q|}{\Phi(Q)}. \tag{A.29}$$

Note that the first term in (A.28) coincides after the usual translation with that in the corresponding expression in the number field calculation [4], but that interestingly the second term has a different form.

Finally, substituting (A.28) into (A.15) and incorporating the estimates for the other terms in (A.7), we find that

$$G(n;\,Q) \sim q^n \left(\deg Q - \frac{|Q|}{\Phi(Q)}\right). \tag{A.30}$$

We now observe that as $q\to\infty$

$$\frac{|Q|}{\Phi(Q)} \to 1 \tag{A.31}$$

and so in this limit, when n is fixed with $\deg Q \le n+1$, this calculation matches Theorem 2.2. Furthermore, when $\deg Q\to\infty$ with q fixed we have that

$$G(n;\,Q) \sim q^n \deg Q, \tag{A.32}$$

which is consistent with the Hooley's conjecture (1.10) in the number field case.

References

[1] Bary-Soroker, L. "Twin prime analog over large finite fields." (2012): preprint arXiv:1206.3930v1.

[2] Bender, A. and P. Pollack. "On quantitative analogues of the Goldbach and twin prime conjectures over $\mathbb{F}_q[t]$." (2009): preprint arXiv:0912.1702v1.

[3] Diaconis, P. and M. Shahshahani. "On the eigenvalues of random matrices." Studies in applied probability. *Journal of Applied Probability* 31 (1994): 49–62.

[4] Friedlander, J. B. and D. A. Goldston. "Variance of distribution of primes in residue classes." *Quarterly Journal of Mathematics. Oxford Second Series* 47, no. 187 (1996): 313–36.

[5] Goldston, D. A. and H. L. Montgomery. "Pair Correlation of Zeros and Primes in Short Intervals." *Analytic Number Theory and Diophantine Problems (Stillwater, OK, 1984)*, 183–203. Progress in Mathematics 70. Boston, MA: Birkhäuser Boston, 1987.

[6] Hooley, C. "The Distribution of Sequences in Arithmetic Progression." *Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974)*, Vol. 1, 357–64. Canadian Mathematical Congress, Montreal, Quebec, 1975.

[7] Hooley, C. "On the Barban–Davenport–Halberstam theorem. I." Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday. III. *Journal für die Reine und Angewandte Mathematik* 274/275 (1975): 206–23.

[8] Hooley, C. "On the Barban–Davenport–Halberstam theorem. II." *J. London Math. Soc.* (2) 9 (1974/75): 625–36.

[9] Hooley, C. "On the Barban–Davenport–Halberstam theorem. V." *Proceedings of the London Mathematical Society. Third Series* 33, no. 3 (1976): 535–48.

[10] Katz, N. M. *Convolution and Equidistribution: Sato–Tate Theorems for Finite-Field Mellin Transforms*. Annals of Mathematics Studies 180. Princeton, NJ: Princeton University Press, 2012.

[11] Katz, N. M. "On a question of keating and rudnick about primitive dirichlet characters with squarefree conductor." *International Mathematics Research Notices* first published online June 4, 2012. doi:10.1093/imrn/rns143.

[12] Katz, N. M. "Witt vectors and a question of Keating and Rudnick." *International Mathematics Research Notices*, first published online June 20, 2012. doi:10.1093/imrn/rns144.

[13] Montgomery, H. L. "Primes in arithmetic progressions." *The Michigan Mathematical Journal* 17 (1970): 33–9.

[14] Montgomery, H. L. and K. Soundararajan. "Primes in short intervals." *Communications in Mathematical Physics* 252, no. 1–3 (2004): 589–617.

[15] Rosen, M. *Number Theory in Function Fields*. Graduate Texts in Mathematics 210. New York: Springer, 2002.

[16] Weil, A. *Basic Number Theory*, 3rd ed. Die Grundlehren der Mathematischen Wissenschaften, Band 144. New York/Berlin: Springer, 1974.