AN UNCERTAINTY PRINCIPLE FOR FUNCTION FIELDS

FRANK THORNE

Abstract. In a recent paper, Granville and Soundararajan [8] proved an "uncertainty principle" for arithmetic sequences, which limits the extent to which such sequences can be well-distributed in both short intervals and arithmetic progressions. In the present paper we follow the methods of [8] and prove that a similar phenomenon holds in $\mathbb{F}_q[t]$.

1. Introduction and Statement of Results

In a recent work [8], Granville and Soundararajan established a so-called "uncertainty principle" for arithmetic sequences. Loosely speaking, this means that sequences of integers which are determined by arithmetic constraints cannot always be well-distributed. In particular, suppose that $\mathcal{A}$ is a sequence of integers and $\mathcal{S}$ is an integer, such that for all d with $(d, \mathcal{S}) = 1$, the proportion of elements of $\mathcal{A}$ divisible by d is asymptotic to $h(d)/d$, for a multiplicative function $h(d)$ taking values in $[0, 1]$. We assume further that a suitable weighted average of $h(p)$ is sufficiently smaller than 1. If this happens we will refer to $\mathcal{A}$ as an "arithmetic sequence".

Under appropriate technical hypotheses, Granville and Soundararajan then prove that $\mathcal{A}$ cannot be uniformly well-distributed in both short intervals and arithmetic progressions to large moduli. For example, if $\mathcal{A}$ is a subset of $[1, x]$, and u is a positive integer (either fixed or a slowly increasing function of x), then $\mathcal{A}$ must be irregularly distributed in short intervals of length $\geq (\log x)^u$, arithmetic progressions to moduli $\leq \exp(2(\log x)^{1-\eta})$ for a certain quantity η (related to the density of $\mathcal{A}$), or both.

Their results can be considered as a far-reaching generalization of a result of Maier [9], who proved that the primes are not uniformly well-distributed in short intervals. In particular, he proved that for any fixed $\lambda_0 > 0$,

$$\limsup_{x \to \infty} \frac{\pi(x + (\log x)^{\lambda_0}) - \pi(x)}{(\log x)^{\lambda_0 - 1}} > 1, \tag{1.1}$$

and

$$\liminf_{x \to \infty} \frac{\pi(x + (\log x)^{\lambda_0}) - \pi(x)}{(\log x)^{\lambda_0 - 1}} < 1. \tag{1.2}$$

Maier's result contracted probabilistic heuristics and was quite surprising.

Maier proved his results by constructing a "Maier matrix" where the rows were short intervals and the columns were certain arithmetic progressions. Playing these off against one another, Maier constructed matrices such that the number of primes in the whole matrix was either more or fewer than expected, thereby obtaining (1.1) and (1.2).

Maier's method was extended by many others to prove a variety of similar results; we refer to the excellent survey articles of Granville [7] and Soundararajan [15] as well as the introduction of [8] for a more detailed discussion. One may also see [15] for an enlightening description of how the

Date: January 14, 2008.

2000 *Mathematics Subject Classification.* 11N05, 11N25, 11T55.

methods of [9] motivated those in [8].

Maier matrices and irregularities in $\mathbb{F}_q[t]$. In light of the well-known analogy between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, it is natural to ask questions about the distribution of primes and related sequences in $\mathbb{F}_q[t]$. The prime number theorem for $\mathbb{F}_q[t]$ says that $\pi(n) = q^n/n + O(q^{n/2}/n)$, where $\pi(n)$ denotes the number of monic irreducibles of degree n. (See Section 2 for additional details and related results.)

This suggests that probabilistic heuristics may be used to make conjectures about the distribution of primes in $\mathbb{F}_q[t]$. In some cases these conjectures have proved more tractable than their analogues in $\mathbb{Z}$. For example, Pollack [12] has recently proved an $\mathbb{F}_q[t]$ version of the quantitative Bateman-Horn conjecture (which includes the Hardy-Littlewood prime tuple conjecture as a special case) which is valid when q is coprime to $2n$ and large in relation to n. Conversely, when q is not coprime to n, Conrad, Conrad, and Gross [4] have found a global obstruction to this conjecture related to a certain average of the Möbius function, and they propose a revised conjecture based on geometric considerations as well as numerical calculations.

In this paper we are primarily interested in irregularities similar to (1.1) and (1.2). In a previous paper [16], the present author adapted the Maier matrix method to $\mathbb{F}_q[t]$ and proved the analogue of Maier's result, as well as the analogue of a result of Shiu concerning strings of congruent primes. In unpublished work, Udovina [17] similarly proved the analogous result for primes in arithmetic progressions to large moduli.

One expects that the mechanism of [8] can be translated to $\mathbb{F}_q[t]$, and the object of the present paper is to prove that this is indeed the case. In particular we will obtain the following two theorems as our main results. These results are somewhat technical, and the theorem statements involve notation which will be defined in Section 2.

Our first result is the analogue of Corollary 1.3 of [8], and establishes that arithmetic sequences must fail to be well-distributed uniformly in arithmetic progressions to large moduli:

Theorem 1.1. *Assume a large integer y is given, such that all primes of $\mathcal{S}$ are of degree less than $12 \log y$. Assume furthermore that*

$$\sum_{\deg p \leq y} \frac{1 - h(p)}{|p|} \deg p \geq \alpha y \tag{1.3}$$

for some $\alpha \geq 39 \log y/y$. Write $\eta = \min(\alpha/3, 1/100)$. Then for every $u \in [5y/\eta^2, e^{\eta y/2}]$ (if $q = 2$, for every $u \in [5y/\eta^2, e^{\eta y/5}]$) and every $n \geq 5q^y$ there exists an arithmetic progression $a \pmod m$ with $\deg m \leq n - u$ and $(m, \mathcal{S}) = 1$ which satisfies

$$\left| \mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m} \mathcal{A}(n) \right| \Big/ \frac{\mathcal{A}(n)}{\phi(m)} \geq \frac{1}{3} \exp\left(- \frac{u}{\eta y}(1 + 25\eta) \log\left(\frac{2u}{y\eta^3} \right) \right).$$

Our second main result is the "uncertainty principle", and establishes that arithmetic sequences must be poorly distributed either in short intervals, or in arithmetic progressions to much smaller moduli:

Theorem 1.2. *Assume a large integer y is given, such that all primes of $\mathcal{S}$ are of degree less than $12 \log y$. Assume furthermore that*

$$\sum_{\deg p \leq y} \frac{1 - h(p)}{|p|} \deg p \geq \alpha y \tag{1.4}$$

for some $\alpha \geq 39 \log y/y$. Write $\eta = \min(\alpha/3, 1/100)$. Then for every $u \in [5y/\eta^2, e^{\eta y/2}]$ (if $q = 2$, for every $u \in [5y/\eta^2, e^{\eta y/5}]$) and every $n \geq 5q^y$, at least one of the following is true:

(i) There exists an arithmetic progression $a \pmod m$ *with* $\deg m \le 2q^{1+(1-\eta)y}$ *and* $(m, \mathcal{S}) = 1$ *which satisfies*

$$\left|\mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n)\right| \Big/ \frac{\mathcal{A}(n)}{\phi(m)} \ge \frac{1}{2}\exp\left(-\frac{u}{\eta y}(1+25\eta)\log\left(\frac{2u}{y\eta^3}\right)\right).$$

(ii) There exists an interval $(f, u-1)$ *with* $\deg f = n$*, such that*

$$\left|\mathcal{A}(f, u-1) - \frac{\mathcal{A}(n)}{q^{n-u}}\right| \Big/ \frac{\mathcal{A}(n)}{q^{n-u}} \ge \frac{1}{2}\exp\left(-\frac{u}{\eta y}(1+25\eta)\log\left(\frac{2u}{y\eta^3}\right)\right).$$

These results imply the existence of irregularities in the distribution of the primes, in both short intervals and in arithmetic progressions to large moduli. (To obtain irregularities in short intervals, we apply Theorem 1.2 and observe that (i) contradicts the prime number theorem for arithmetic progressions (2.7).) Following [8], we will analyze the primes separately and prove somewhat better results.

Our first such result concerns irregularities in short intervals, and improves upon a previous result of the present author ([16], Theorem 1.1).

Theorem 1.3. *Assume that* z*,* D*, and* u *are positive integers satisfying* $z \ge z_0$*,* $D \ge 5q^z$*, and* $B < u/z \ll e^{2z/3}/z$ *for certain absolute constants* z_0 *and* B*. If* $q = 2$*, further assume* $u/z < 2^{2z/3}/z$*. Then there exist monic polynomials* $f_\pm$ *of degree* D *so that*

$$\pi(f_+, u) \ge \frac{q^{u+1}}{D}\left[1 + \exp\left(-\frac{u}{z}\left(\log\left(\frac{u}{z}\right) + \log\log\left(\frac{u}{z}\right) + O(1)\right)\right)\right],$$

and

$$\pi(f_-, u) \le \frac{q^{u+1}}{D}\left[1 - \exp\left(-\frac{u}{z}\left(\log\left(\frac{u}{z}\right) + \log\log\left(\frac{u}{z}\right) + O(1)\right)\right)\right].$$

The implied constants are absolute.

Remark. We may recover Theorem 1.1 of [16] by taking u/z to be fixed, $D = 5q^z$, and allowing z to go to infinity.

We also prove the existence of irregularities in the distribution of primes in arithmetic progressions to large moduli, improving upon the previously mentioned work of Udovina.

Theorem 1.4. *Assume that* z*,* D*, and* u *are positive integers satisfying* $z \ge z_0$*,* $D \ge 5q^z$*, and* $B < u/z \ll e^{2z/3}/z$ *for certain absolute constants* z_0 *and* B*. If* $q = 2$*, further assume* $u < 2^{2z/3}/z$*. If* l *is any monic polynomial of degree* D*, then for some* $u_\pm \in (u, u(1 + 3A/\log(u/z)))$ *there exist arithmetic progressions* $(D + u_+; l, a_+)$ *and* $(D + u_-; l, a_-)$ *with* $(l, a_\pm) = 1$ *satisfying*

$$\pi(D + u_+; l, a_+) \ge \frac{q^{D+u_+}}{\phi(l)(D+u_+)}\left[1 + \exp\left(-\frac{u}{z}\left(\log\left(\frac{u}{z}\right) + \log\log\left(\frac{u}{z}\right) + O(1)\right)\right)\right],$$

$$\pi(D + u_-; l, a_-) \le \frac{q^{D+u_-}}{\phi(l)(D+u_-)}\left[1 - \exp\left(-\frac{u}{z}\left(\log\left(\frac{u}{z}\right) + \log\log\left(\frac{u}{z}\right) + O(1)\right)\right)\right].$$

Remark. We may easily modify the proof and instead obtain, for any fixed degree $D' \ge 5q^z$, irregular progressions $(D'; l_+, a_+)$ and $(D'; l_-, a_-)$ such that $\pi(D'; l_\pm, a_\pm)$ satisfies the analogous inequalities, and $D - \deg l_\pm$ satisfies the bounds stated for $u_\pm$.

We could give many more examples following [8]; essentially, the present work suggests that all of the examples appearing in [8] could likely be translated into $\mathbb{F}_q[t]$. We will give a brief discussion of some examples and applications in Section 6.

The outline of the paper is as follows: In Section 2 we will describe our setup and notation and introduce some needed facts about $\mathbb{F}_q[t]$. In Section 3 we will state and prove the $\mathbb{F}_q[t]$ version of the general framework, involving several results on the oscillation of mean values of certain arithmetic functions. In Section 4 we will apply this framework to the primes and prove Theorems 1.3 and 1.4. In Section 5 we will then present the proofs of Theorems 1.1 and 1.2. We will conclude in Section 6 with several additional examples.

Acknowledgements

To be entered later (after the referee report is received).

2. Notation and General Considerations

Let x denote a variable element of $\mathbb{F}_q[t]$, and let $a(x) : \mathbb{F}_q[t] \to \mathbb{R}$ denote an arithmetic function taking nonnegative values. Typically we think of $a(x)$ as the characteristic function of a subset $\mathcal{A}$ of $\mathbb{F}_q[t]$, but this is not required. We will, however, make several assumptions about the function $a(x)$, which we describe in this section.

We introduce the following notation:

$$\mathcal{A}(n) := \sum_{\deg x = n} a(x), \tag{2.1}$$

$$\mathcal{A}(n; m, a) := \sum_{\substack{\deg x = n \\ x \equiv a \pmod m}} a(x). \tag{2.2}$$

For a fixed monic polynomial x and an integer $i < \deg x$, we will also write

$$\mathcal{A}(x, i) := \sum_{\deg s \leq i} a(x + s), \tag{2.3}$$

where s ranges over all (not necessarily monic) polynomials of $\mathbb{F}_q[t]$.

When $a(x)$ is the characteristic function of the primes we also write $\pi(n), \pi(n; m, a), \pi(x, i)$ for the above. Moreover, when $a(x)$ is the characteristic function of any set $\mathcal{A}$, we write $(n; m, a)$ and (x, i) to denote the sets of those polynomials ("arithmetic progressions" and "intervals", respectively) counted in the sums above.

We will now make the following assumption:

Assumption 2.1. *For each monic m which is coprime to a 'bad' modulus $\mathcal{S}$, we have*

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|} \mathcal{A}(n), \tag{2.4}$$

for a multiplicative arithmetic function $h(m)$ which takes values in $[0, 1]$.

Our results will then take the shape of limitations on naive estimates predicted by (2.4).

Our assumption that h is multiplicative may be thought of as an assertion that the 'probabilities' that a 'random' polynomial x is divisible by two coprime polynomials m_1 and m_2 should be independent. Our assumption that $h(m) \leq 1$ for all m will be true for the examples we have in mind. Moreover, if instead $h(m)$ is much larger than 1 for any m, it is quite easy to prove the existence of irregular behavior. (See Proposition 2.1 of [8].)

We now assume further that the asymptotic behavior of $\mathcal{A}(n; m, a)/\mathcal{A}(n)$ should depend only on the gcd of a and m, and again our main results take the shape of limitations on the extent to which

this assumption can hold. With this assumption, we arrive at the prediction (exactly following Section 2 of [8], where further details and motivation can be found) that

$$\mathcal{A}(n;m,a) \sim \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n),$$

where

$$\gamma_m := \prod_{p|m}\Big(\frac{1-h(p)/|p|}{1-1/|p|}\Big)^{-1} = \prod_{p}\Big(1-\frac{1}{|p|}\Big)\Big(1+\frac{f_m(p)}{|p|}+\frac{f_m(p^2)}{|p|^2}+\cdots\Big). \tag{2.5}$$

Here $f_m(a)$ is a multiplicative function which is periodic with period m and satisfies $f_m(a) = f_m((a,m))$, and also $f_m(ca) = f_m(a)$ for any nonzero constant $c \in \mathbb{F}_q$. If $p \nmid m$, then $f_m(p^k) = 1$ for any $k \geq 1$. Otherwise, we have

$$f_m(p^k) := \begin{cases} \Big(h(p^k) - \frac{h(p^{k+1})}{|p|}\Big)\Big(1-\frac{h(p)}{|p|}\Big)^{-1} & \text{if } k < e, \\ h(p^e)\Big(1-\frac{1}{|p|}\Big)\Big(1-\frac{h(p)}{|p|}\Big)^{-1} & \text{if } k \geq e. \end{cases} \tag{2.6}$$

Here p^e is the highest power of p dividing m. If m is squarefree then we will have $f_m(r) \leq 1$ for all r. (We remark that our main results assume that $f_m(r) \leq 1$ for all r, and that m will be squarefree in all of our examples.)

Basic facts about $\mathbb{F}_q[t]$. Here we review some standard facts and notation concerning $\mathbb{F}_q[t]$ which will be used later.

The prime number theorem for arithmetic progressions (see Chapter 4 of [14]) states that

$$\pi(n;m,a) = \frac{1}{\phi(m)}\frac{q^n}{n} + O_m\Big(\frac{q^{n/2}}{n}\Big), \tag{2.7}$$

whenever $(a,m) = 1$. Here the Euler ϕ-function is defined by $\phi(m) = |(\mathbb{F}_q[t]/m\mathbb{F}_q[t])^\times|$.

In the special case of counting primes, we in fact have the exact formula (again, see [14])

$$\pi(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}, \tag{2.8}$$

where $\pi(n)$ denotes the number of primes of degree n. This in particular implies that $\pi(n) \leq q^n/n$, a fact we will use later.

We will in fact use an improved version of (2.7) due to Rhin [13], which makes the dependence on m explicit and simultaneously allows us to restrict to intervals of the type (x,i), when i is at least $(\deg x)^{1/2+\epsilon}$.

To state Rhin's result, we write $\pi(x,n;m,a)$ for the number of primes p which are congruent to a modulo m and which are also in the interval (x,n) (i.e., which satisfy $\deg(f-p) \leq n$). We will also write $(x,n;m,a)$ for the set of monic polynomials meeting these conditions. Then whenever $(a,m) = 1$ and $n \geq \deg m$, Rhin's result is that

$$\pi(x,n;m,a) = \frac{1}{\phi(m)}\frac{q^{n+1}}{\deg x} + O((\deg x)q^{(\deg x)/2}). \tag{2.9}$$

The implied constant is absolute, and it is bounded explicitly in [13].

Periodically, we will use 'absolute value' notation: that is, for a monic polynomial $x \in \mathbb{F}_q[t]$, then $|x|$ is defined to be $q^{\deg x} = |\mathbb{F}_q[t]/(x)|$.

Throughout, we will use the notation $f(t) \gg g(t)$ to mean that $f(t) > Cg(t)$ for some constant C and for sufficiently large t. Unless explicitly stated to the contrary, the constant C and the minimum allowable t will be absolute. In particular (and in contrast to the author's previous paper [16]), any dependence of our constants or inequalities on q will be explicitly noted.

3. The Framework

As in [8], our results boil down to proving the existence of oscillations in mean values of arithmetic functions. For the most part our methods and results closely follow [8], and some repetition will be unavoidable. There are several differences occurring in our arguments, however, which we summarize here.

For our purposes, the most significant difference between $\mathbb{Z}$ and $\mathbb{F}_q[t]$ is that the primes of $\mathbb{F}_q[t]$ are 'clumped' into degrees. In particular, if $f : \mathbb{F}_q[t] \to \mathbb{C}$ is an arithmetic function, then the Dirichlet series $\sum_{x \in \mathbb{F}_q[t]} f_Q(x)|x|^{-s}$ does not distinguish between primes of the same degree. Accordingly we expect to prove statements concerning entire degrees of polynomials, and this will indeed be the case.

We will fix an integer z, which we assume is larger than an implied absolute constant z_0. (We remark in particular that z_0 does not depend on q.) Let Q be an element of $\mathbb{F}_q[t]$ whose prime factors are all of degree $\leq z$, and (as in Section 2) let $f_Q(x)$ be a multiplicative function with $f_Q(p^k) = 1$ whenever $p \nmid Q$, such that $0 \leq f_Q(x) \leq 1$ for all x.

We associate to $f(x)$ the Dirichlet series

$$F_Q(s) := \sum_{x \in \mathbb{F}_q[t]} f_Q(x)|x|^{-s}, \tag{3.1}$$

and define a further Dirichlet series $G_Q(s) = \sum_n g_Q(x)|x|^{-s}$ by the equation

$$F_Q(s) = \zeta(s)G_Q(s). \tag{3.2}$$

In other words, for $\Re s > 1$, $G_Q(s)$ is defined by the Euler product

$$G_Q(s) := \sum_{x \in \mathbb{F}_q[t]} g_Q(x)|x|^{-s} = \prod_{p|Q} \left(1 - \frac{1}{|p|^s}\right)\left(1 + \frac{f_Q(p)}{|p|^s} + \frac{f_Q(p^2)}{|p|^{2s}} + \dots\right). \tag{3.3}$$

The equation (3.3) also furnishes an analytic continuation of $G_Q(s)$ to $\Re s > 0$. We note the relations

$$G_Q(1) = \gamma_Q, \tag{3.4}$$

where γ_Q was defined in (2.5), as well as

$$f_Q(x) = \sum_{d|x} g_Q(d) \tag{3.5}$$

which follows immediately from (3.2). We note furthermore that g_Q is multiplicative, $g_Q(x) = 0$ for any $x \nmid Q$, and $|g_Q(x)| \leq 1$ for any x.

We expect from (3.1) that $G_Q(1) = \gamma_Q$ should be the mean value of $f_Q(x)$, and define an error term $E(u)$ measuring the average deviation of f_Q from the mean:

$$E(u) := \frac{1}{q^u} \sum_{\deg x = u} (f_Q(x) - G_Q(1)). \tag{3.6}$$

Remark. Our definition of $E(u)$ differs somewhat from the analogous definition in [8]. To follow [8] most closely we would sum over $\deg n \leq uz$ instead, but this definition works nicely in $\mathbb{F}_q[t]$.

We introduce a variable $\xi \in (0, \frac{2}{3})$; we will later make further explicit restrictions on ξ in terms of z and q. We also introduce the following quantities, following [8], which will be used in the formulation of our results:

$$H_j(\xi) := \sum_{p|Q} \frac{1 - f_Q(p)}{|p|} |p|^{\xi} \left(1 - \frac{\deg p}{z}\right)^j,$$

$$H(\xi) = H_0(\xi) := \sum_{p|Q} \frac{1 - f_Q(p)}{|p|} |p|^{\xi},$$

$$J(\xi) := \sum_{p|Q} \frac{1}{|p|^2} |p|^{2\xi}.$$

Our main result is the following analogue of Theorem 3.1 of [8]. It establishes that under some reasonable technical hypotheses, the function $f_Q(n)$ exhibits oscillations when averaged over single degrees.

Theorem 3.1. *Assume that ξ satisfies*

$$\frac{6}{z \log q} < \xi < \min\left(\frac{2}{3}, \frac{2}{3 \log q}\right). \tag{3.7}$$

Suppose further that $H(\xi) \geq 20H_2(\xi) + 76J(\xi) + 20$, so that

$$\tau := \sqrt{(5H_2(\xi) + 19J(\xi) + 5)/H(\xi)} \leq 1/2. \tag{3.8}$$

Then there exist integers $u_{\pm} \in (zH(\xi)(1 - 2\tau), zH(\xi)(1 + 2\tau))$ satisfying

$$E(u_+) \geq \frac{1}{12\xi z \log q H(\xi)} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi)\Big) q^{-\xi u_+},$$

$$E(u_-) \leq -\frac{1}{12\xi z \log q H(\xi)} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi)\Big) q^{-\xi u_-}.$$

We will prove Theorem 3.1 after first proving several preliminary technical results. In [8] Granville and Soundararajan prove several bounds for different integrals of the functions $q^{\xi u}E(u)$ and $q^{\xi u}|E(u)|$, and for $\mathbb{F}_q[t]$ we will prove similar results with the integrals replaced with sums.

Proposition 3.2. *In the range $0 < \xi < 0.67$, we have*

$$\sum_{u=0}^{\infty} q^{\xi u} |E(u)| \leq \frac{1}{\xi \log q} \exp(H(\xi) + 5J(\xi)).$$

Proof. Using (3.5) we see that

$$E(u) = -G_Q(1) + \sum_{\substack{d \in \mathbb{F}_q[t] \\ \deg d \leq u}} \frac{g_Q(d)}{|d|} = \sum_{\substack{d \in \mathbb{F}_q[t] \\ \deg d > u}} \frac{g_Q(d)}{|d|}.$$

Therefore, it follows that

$$\begin{aligned}\sum_{u=0}^{\infty} q^{\xi u}|E(u)| &\le \sum_{u=0}^{\infty} q^{\xi u}\Big(\sum_{\deg d>u} \frac{|g_Q(d)|}{|d|}\Big)\\ &= \sum_{d\in\mathbb{F}_q[t]} \frac{|g_Q(d)|}{|d|} \sum_{u<\deg d} q^{\xi u}\\ &< \sum_{d\in\mathbb{F}_q[t]} \frac{|g_Q(d)|}{|d|} \frac{q^{\xi(\deg d)}}{\xi\log q}\\ &= \frac{1}{\xi\log q}\sum_{d\in\mathbb{F}_q[t]} \frac{|g_Q(d)|}{|d|^{1-\xi}}.\end{aligned}$$

Exactly as in [8], we have $|p|\ge 2$ for any prime p, and the bound $\xi<0.67$ implies that

$$\sum_{d\in\mathbb{F}_q[t]} \frac{|g_Q(d)|}{|d|^{1-\xi}} \le \prod_{p|Q}\Big(1+\frac{1-f_Q(p)}{|p|^{1-\xi}}\Big)\Big(1+\frac{5}{|p|^{2(1-\xi)}}\Big).$$

The proposition then follows by taking logarithms. □

For a complex variable s, we introduce a function

$$I(s) := \sum_{u=0}^{\infty} q^{-su}E(u). \tag{3.9}$$

By Proposition 3.2, the sum converges absolutely for $\Re s > -\frac{2}{3}$. Then we have for $\Re s>0$

$$\begin{aligned}I(s) &= \sum_{x\in\mathbb{F}_q[t]}\Big(f_Q(x)-G_Q(1)\Big)q^{(-\deg x)(s+1)}\\ &= F_Q(1+s)-G_Q(1)\zeta(1+s),\end{aligned}$$

which gives the identity

$$I(s) = \zeta(1+s)\Big(G_Q(1+s)-G_Q(1)\Big). \tag{3.10}$$

By analytic continuation this identity holds for $\Re s > -\frac{2}{3}$.

Proposition 3.3. *If* $\frac{6}{z\log q} < \xi < \min(\frac{2}{3}, \frac{2}{3\log q})$, *then*

$$\sum_{u=0}^{\infty} q^{\xi u}|E(u)| \ge \frac{1}{2\xi\log q}\Big(\exp[H(\xi)-5H_2(\xi)-5J(\xi)]-1\Big).$$

Remark. This result should be compared to Proposition 3.7 of [8].

Proof. We take $s=-(\xi+i\pi/(z\log q))$ in (3.10), and see that

$$\sum_{u=0}^{\infty} q^{\xi u}|E(u)| \ge |I(s)| \ge |\zeta(1+s)|\Big(|G_Q(1+s)|-1\Big). \tag{3.11}$$

We have

$$\zeta(1+s) = 1/(1-q^{-s}) = \frac{1}{s\log q - \frac{1}{2}(s\log q)^2 + \frac{1}{6}(s\log q)^3 + \dots}. \tag{3.12}$$

If $\xi \log q < 2/3$, then $|s \log q| \le 1$ for large z, and we then have

$$|\zeta(1+s)| \ge \frac{1}{(e-1)|s\log q|} \ge \frac{1}{(e-1)|s/\xi|(\xi \log q)}.$$

We compute that with $\xi > 6/(z\log q)$ we have $(e-1)|s/\xi| < 2$, and so we have

$$|\zeta(1+s)| \ge \frac{1}{2\xi \log q}. \tag{3.13}$$

For the quantity $|G_Q(1+s)|$, we have the inequality

$$\log |G_Q(1+s)| \ge H(\xi) - 5H_2(\xi) - 5J(\xi). \tag{3.14}$$

The proof of (3.14) proceeds exactly as in [8], and so we omit the details here. Upon exponentiating and plugging everything into (3.11) we obtain our result. □

Proposition 3.4. *For $0 < \xi < \frac{2}{3}$, we have the upper bound*

$$\left|\sum_{u=0}^{\infty} q^{\xi u} E(u)\right| \le \frac{2}{\xi \log q}. \tag{3.15}$$

Proof. Using (3.10) with $s = -\xi$, we have

$$\sum_{u=0}^{\infty} q^{\xi u} E(u) = \zeta(1-\xi)\Big(G_Q(1-\xi) - G_Q(1)\Big). \tag{3.16}$$

The definition of G_Q implies that $|G_Q(t)| \le 1$ for any real $t > 0$, and we have

$$\zeta(1-\xi) = \frac{-1}{\xi \log q + \frac{1}{2}(\xi \log q)^2 + \frac{1}{6}(\xi \log q)^3 + \cdots}$$

which implies in particular that

$$|\zeta(1-\xi)| \le \frac{1}{\xi \log q}. \tag{3.17}$$

The result follows immediately from (3.16) and (3.17). □

Proof of Theorem 3.1. Let I_+ (and I_-) denote the set of u where $E(u) \ge 0$ (respectively $E(u) < 0$). Combining Propositions 3.3 and 3.4, we see that

$$\sum_{u \in I^{\pm}} q^{\xi u} |E(u)| \ge \frac{1}{4\xi \log q}\left(\exp[H(\xi) - 5H_2(\xi) - 5J(\xi)] - 1\right) - \frac{1}{\xi \log q}. \tag{3.18}$$

Using the fact that $H(\xi) - 5H_2(\xi) - 5J(\xi) \ge 20$, this implies that

$$\sum_{u \in I^{\pm}} q^{\xi u} |E(u)| \ge \frac{1}{5\xi \log q} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi)\Big). \tag{3.19}$$

Write $u_1 = \lfloor zH(\xi)(1+2\tau)\rfloor$. Then Proposition 3.2 implies that for $z > 150/\ln 2$,

$$\begin{aligned}\sum_{u \ge u_1} q^{\xi u}|E(u)| &\le q^{-\tau u_1/(z\log q)} \sum_{u=0}^{\infty} q^{(\xi + \tau/(z\log q))u}|E(u)| \\ &\le \frac{1}{\xi \log q} \exp\left(-\frac{\tau u_1}{z} + H\Big(\xi + \frac{\tau}{z\log q}\Big) + 5J\Big(\xi + \frac{\tau}{z\log q}\Big)\right).\end{aligned}$$

We will have $H\big(\xi + \frac{\tau}{z\log q}\big) \le e^{\tau} H(\xi) < (1+\tau+\tau^2)H(\xi)$ and $J\big(\xi + \frac{\tau}{z\log q}\big) \le e^{2\tau} J(\xi) < 2.8 J(\xi)$, so we conclude that

$$\sum_{u \ge u_1} q^{\xi u} |E(u)| \le \frac{1}{\xi \log q} \exp\Big(-\frac{\tau u_1}{z} + (1+\tau+\tau^2)H(\xi) + 14 J(\xi) \Big).$$

Plugging in the definition of u_1, we obtain

$$\sum_{u \ge u_1} q^{\xi u} |E(u)| \le \frac{1}{\xi \log q} \exp\Big(H(\xi) - \tau^2 H(\xi) + 14 J(\xi) + \frac{\tau}{z} \Big),$$

and substituting the definition of τ we see that

$$\sum_{u \ge u_1} q^{\xi u} |E(u)| \le \frac{2}{e^5 \xi \log q} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi) \Big). \tag{3.20}$$

We similarly write $u_0 = \lceil z H(\xi)(1-2\tau) \rceil$, and we have

$$\begin{aligned} \sum_{u \le u_0} q^{\xi u} |E(u)| &\le q^{\tau u_0/(z \log q)} \sum_{u=0}^{\infty} q^{(\xi - \tau/(z\log q))u} |E(u)| \\ &\le \frac{1}{\xi \log q - \tau/z} \exp\bigg(\frac{\tau u_0}{z} + H\Big(\xi - \frac{\tau}{z\log q}\Big) + 5J\Big(\xi - \frac{\tau}{z \log q}\Big) \bigg). \end{aligned}$$

We have $J\big(\xi - \frac{\tau}{z\log q}\big) \le J(\xi)$, and

$$\begin{aligned} H\Big(\xi - \frac{\tau}{z\log q}\Big) &\le \sum_{p \mid Q} \frac{1 - f_Q(p)}{|p|} |p|^{\xi} \Big(1 - \tau \frac{\deg p}{z} + \frac{\tau^2}{2} \Big) \\ &= H(\xi)(1 - \tau + \tau^2/2) + \tau H_1(\xi) \le H(\xi)(1 - \tau + \tau^2/2) + \tau \sqrt{H(\xi) H_2(\xi)}. \end{aligned}$$

Thus, we conclude that

$$\sum_{u \le u_0} q^{\xi u} |E(u)| \le \frac{1}{\xi \log q - \tau/z} \exp\bigg(\frac{\tau u_0}{z} + H(\xi)(1 - \tau + \tau^2/2) + \tau \sqrt{H(\xi) H_2(\xi)} + 5J(\xi) \bigg).$$

Substituting the definition of u_0, we see that

$$\sum_{u \le u_0} q^{\xi u} |E(u)| \le \frac{1}{\xi \log q - \tau/z} \exp\bigg(H(\xi) - \frac{3}{2}\tau^2 H(\xi) + \tau \sqrt{H(\xi) H_2(\xi)} + 5J(\xi) + \frac{\tau}{z} \bigg).$$

A routine calculation establishes that

$$-\frac{3}{2}\tau^2 H(\xi) + \tau \sqrt{H(\xi) H_2(\xi)} + 5J(\xi) \le -5H_2(\xi) - 5J(\xi) - 5,$$

and we conclude that

$$\sum_{u \le u_0} q^{\xi u} |E(u)| \le \frac{2}{e^5 (\xi \log q - \tau/z)} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi) \Big).$$

Since $\xi z \log q > 6$, we see that

$$\sum_{u \le u_0} q^{\xi u} |E(u)| \le \frac{2.5}{e^5 \xi \log q} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi) \Big). \tag{3.21}$$

Combining (3.19), (3.20), and (3.21) we see that

$$\sum_{u \in I_{\pm} \cap (u_0, u_1)} q^{\xi u} |E(u)| \ge \frac{1}{6 \xi \log q} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi) \Big). \tag{3.22}$$

As $u_1 - u_0 \le 2zH(\xi)$, we have for some $u_\pm \in I_\pm \cap (u_0, u_1)$ that

$$|E(u_\pm)| \ge \frac{1}{12\xi z \log qH(\xi)} \exp\Big(H(\xi) - 5H_2(\xi) - 5J(\xi)\Big) q^{-\xi u_\pm},$$

which is the desired result. □

We now derive several corollaries of Theorem 3.1, still following [8]. Our first such is the analogue of Corollary 3.2 of [8].

Corollary 3.5. *Let $e^{-z/13} \le \eta \le 1/100$ and suppose that Q is composed only of primes of degrees in $[(1-\eta)z, z]$. Suppose further that*

$$\sum_{p|Q} \frac{1 - f_Q(p)}{|p|} \ge \eta^2.$$

Then for $e^{z/2} \ge u \ge 5z/\eta^2$ (if $q = 2$, for $e^{z/5} \ge u \ge 5z/\eta^2$) there exist points $u_\pm \in [u, u(1+23\eta)]$ such that

$$E(u_+) \ge \exp\bigg(-\frac{u}{z}(1+25\eta) \log\bigg(\frac{2u}{z\eta^2}\bigg)\bigg), \tag{3.23}$$

$$E(u_-) \le -\exp\bigg(-\frac{u}{z}(1+25\eta) \log\bigg(\frac{2u}{z\eta^2}\bigg)\bigg). \tag{3.24}$$

Proof. We observe that for $q \ne 2$ and $\xi < \frac{2}{3\log q}$, or for $q = 2$ and $\xi < \frac{53}{100}$, we have the inequalities

$$H(\xi) \ge \eta^2 q^{(1-\eta)\xi z}, \quad H_2(\xi) \le \eta^2 H(\xi), \quad J(\xi) \le \eta^2 H(\xi). \tag{3.25}$$

The first two relations are clear. To show the last, it suffices to show that

$$q^{2\xi z} \sum_{p|Q} \frac{1}{|p|^2} \le \eta^4 q^{(1-\eta)\xi z}.$$

Clearly $\sum_{p|Q} |p|^{-2} \le q^{(-1+\eta)z}$ for large z, and collecting terms we see that it is enough to show that

$$q^{z(\xi - 1 + \eta + \eta\xi)} \le \eta^4.$$

We then check that this follows from our upper bound on ξ and our upper and lower bounds on η.

Assume that ξ has been chosen so that $H(\xi) \ge 5/\eta^2$. Then we will prove the conclusion of the corollary when $u = zH(\xi)(1-10\eta)$. We will then prove that we thus obtain all u in the range claimed, for appropriate choices of ξ permitted by the hypotheses of Theorem 3.1.

If $H(\xi) \ge 5/\eta^2$, the latter two inequalities in (3.25) imply that $\tau \le 5\eta$. Using Theorem 3.1, we conclude that for those ξ satisfying (3.7) there exist integers $u_\pm$ in $(zH(\xi)(1-10\eta), zH(\xi)(1+10\eta))$ such that

$$E(u_+) \ge \frac{1}{12\xi z \log qH(\xi)} \exp\Big((1-10\eta^2)H(\xi)\Big) q^{-\xi u_+},$$

with an analogous bound for $E(u_-)$. We claim that $E(u_+) \ge q^{-\xi u_+}$. We will justify this by showing that in fact

$$\exp(.9H(\xi)) \ge 12\xi z \log qH(\xi). \tag{3.26}$$

We know that $H(\xi) \ge \eta^2 q^{(1-\eta)\xi z}$, and this implies that

$$\xi z \log q \le \frac{1}{1-\eta} \log\bigg(\frac{H(\xi)}{\eta^2}\bigg) \le \frac{102}{100} \log\bigg(\frac{H(\xi)}{\eta^2}\bigg).$$

Therefore, (3.26) follows if

$$\exp(.9H(\xi)) \geq 13 \log\Big(\frac{H(\xi)}{\eta^2}\Big) H(\xi),$$

which follows in turn from our lower bound on $H(\xi)$.

At this point write $u = zH(\xi)(1-10\eta)$ so that $u_+ \in [u, (1+23\eta)u]$. The bound on $H(\xi)$ in (3.25) implies that

$$\xi \leq \frac{1}{(1-\eta)z \log q} \log\Big(\frac{2u}{z\eta^2}\Big),$$

and substituting this into the inequality $E(u_+) \geq q^{-\xi u_+}$ we see that

$$E(u_+) \geq q^{-\xi u(1+23\eta)} \geq \exp\bigg(-u \frac{1}{(1-\eta)z} \log\Big(\frac{2u}{z\eta^2}\Big)(1+23\eta)\bigg),$$

which yields the inequality (3.23). A similar analysis yields (3.24).

We must now argue that for arbitrary u in the range claimed we may choose ξ so that $u = zH(\xi)(1-10\eta)$. Since $H(\xi)$ is an increasing, continuous function of ξ, and the range of ξ allowed by Theorem 3.1 is an interval, it suffices to show that some $u < 5z/\eta^2$ and some $u > e^{z/2}$ (or, if $q = 2$, $u > e^{z/5}$) can be achieved. We will do this by estimating $H(\xi)$ when ξ is at the endpoints of the range allowed. Note that our assumption that $H(\xi) \geq 5/\eta^2$ is automatically satisfied if $u \geq 5z/\eta^2$.

For the lower bound, write $\xi_0 = z/(6 \log q)$, and we see that

$$zH(\xi_0) \leq z \sum_{p|Q} |p|^{-1+6/(z \log q)} \leq z \sum_{\deg p \in [(1-\eta)z, z]} |p|^{-1+6/(z \log q)}.$$

By the prime number theorem, this is

$$\leq z \sum_{i \in [(1-\eta)z, z]} \frac{1}{i} e^{6i/z} \leq e^6 \frac{\eta z + 1}{(1-\eta)}, \tag{3.27}$$

and for large z this latter quantity is less than $5z/\eta^2$, as desired.

For the upper bound, if $q \neq 2$ then choose $\xi_0 = \frac{2}{3 \log q}$ and the first inequality in (3.25) implies that $H(\xi_0) \geq e^{-2z/13} q^{(1-\eta)\xi_0} > e^{z/2}$ (so that we obtain a value of $u > .9ze^{z/2} > e^{z/2}$). If $q = 2$, then choose $\xi_0 = \frac{53}{100}$ and similarly $H(\xi_0) > e^{z/5}$.

□

Corollary 3.6. *Suppose that Q is divisible only by primes of degrees in $[z/2, z]$. Assume further that C is a positive constant such that for ξ satisfying (3.7) we have $H(\xi) \geq \frac{Cq^{\xi z}}{\xi z \log q}$. Then, if $q \neq 2$, there exists a positive constant A depending only on C such that for any u satisfying*

$$A < u/z < Ce^{2z/3}/z, \tag{3.28}$$

there are integers $u_\pm \in [u(1 - \frac{A}{\log(u/z)}), u(1 + \frac{A}{\log(u/z)})]$ satisfying

$$E(u_+) \geq \exp\bigg(-\frac{u_+}{z}\Big(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O(1)\Big)\bigg).$$

$$E(u_-) \leq -\exp\bigg(-\frac{u_-}{z}\Big(\log\Big(\frac{u_-}{z}\Big) + \log\log\Big(\frac{u_-}{z}\Big) + O(1)\Big)\bigg).$$

If $q = 2$, then the same conclusion holds if in place of (3.28) u satisfies $A < u/z < C2^{2z/3}/z$.

Proof. This will follow from Theorem 3.1. We begin by bounding the quantities $H_2(\xi)$ and $J(\xi)$ from above. We first claim that $H_2(\xi) \ll \frac{q^{z\xi}}{(\xi z \log q)^3}$. To see this, observe that

$$H_2(\xi) = \sum_{p|Q} \frac{1 - f_Q(p)}{|p|} |p|^{\xi} \Big(1 - \frac{\deg p}{z}\Big)^2 \le \sum_{i=\lceil z/2 \rceil}^{z} \frac{1}{i} q^{i\xi} \Big(1 - \frac{i}{z}\Big)^2.$$

The sum over i is

$$\ll \frac{q^{z\xi}}{z^3} \Big(q^{-\xi} + \sum_{i=2}^{\lfloor z/2 \rfloor} q^{-i\xi} i^2\Big) \ \le \ \frac{q^{z\xi}}{z^3} \Big(q^{-\xi} + \int_{t=1}^{z/2} q^{-t\xi} (t+1)^2 dt\Big),$$

and in the integral we observe that $(t+1)^2 \ll t^2$, expand the bounds to $(0, \infty)$, and integrate by parts to deduce our claim.

We also claim that $J(\xi) \ll \frac{q^{z\xi}}{(\xi z \log q)^3}$. We have

$$J(\xi) = \sum_{p|Q} \frac{1}{|p|^2} |p|^{2\xi} \ll \frac{1}{z} \int_{t=(z/2)-1}^{z+1} q^{(-1+2\xi)t} dt \ll \max(1, q^{(-1+2\xi)(z+1)}),$$

which we readily check is $\ll \frac{q^{z\xi}}{(\xi z \log q)^3}$.

For $\xi z \log q > 6$ and z large, it then follows that

$$5H_2(\xi) + 19J(\xi) + 5 \le C_1 \frac{q^{z\xi}}{(\xi z \log q)^3}$$

for an absolute constant C_1. Therefore, our lower bound on $H(\xi)$ implies that τ (see (3.8)) satisfies

$$\tau \le \frac{\sqrt{C_1/C}}{\xi z \log q}. \tag{3.29}$$

We now write $u = zH(\xi)$. We have $\frac{Cq^{\xi z}}{\xi z \log q} \le H(\xi) \ll \frac{q^{\xi z}}{\xi z \log q}$, where the lower bound is true by hypothesis, and the upper bound will be proved later in Lemma 4.1. These bounds imply that

$$\xi z \log q = \log(u/z) + \log\log(u/z) + O_C(1). \tag{3.30}$$

We also have

$$H(\xi) - 5H_2(\xi) - 5J(\xi) = O_C\Big(\frac{u}{z}\Big),$$

so that if the hypotheses of Theorem 3.1 are met, we have for some $u_+ \in [u(1-2\tau), u(1+2\tau)]$ that

$$E(u_+) \ge \frac{1}{12\xi z \log q H(\xi)} \exp\Big(- \xi u_+ \log q + O_C\Big(\frac{u}{z}\Big)\Big).$$

We observe that

$$12\xi z \log q H(\xi) \ll_C \frac{u}{z} \log\Big(\frac{u}{z}\Big) = \exp\Big(O_C\Big(\frac{u}{z}\Big)\Big),$$

and, assuming that τ is bounded away from $1/2$ (to be proved shortly),

$$\log(u_+) = \log(u) + O(1), \tag{3.31}$$

so that putting these estimates together we obtain

$$E(u_+) \ge \exp\Big(- \frac{u_+}{z} \Big(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O_C(1)\Big)\Big). \tag{3.32}$$

The same argument proves the analogous bound for $E(u_-)$.

To conclude our proof, we first prove the upper bound on τ required by (3.8) and (3.31). In particular, (3.29) and (3.30) imply that there exist constants A_1, A_2 depending only on C so that whenever $u/z \geq A_1$ we have

$$\tau < \frac{A_2}{\log(u/z)} < \frac{1}{4}. \tag{3.33}$$

We must also argue, as in Corollary 3.5, that we may obtain any u in the range (3.28) by choosing an appropriate ξ satisfying the hypotheses of Theorem 3.1. Again it suffices to check the endpoints. For the lower endpoint $\xi_0 = \frac{6}{z \log q}$, we have

$$H\Big(\frac{6}{z\log q}\Big) \leq \sum_{\deg p \in [z/2,z]} \frac{1}{|p|}|p|^{\xi} \leq \frac{2}{z} \sum_{i \in [z/2,z]} e^{6i/z} \leq \frac{2}{z} e^6 \Big(\frac{z}{2}+1\Big) \leq e^6 + 1.$$

(The last step assumes $z \geq 2e^6 + 1$.) Thus, $u/z = H(\xi)$ may be chosen as small as $\max(A_1, e^6+1)$. Conversely, we obtain the upper bound on u/z by choosing $\xi_0 = \min\big(\frac{2}{3}, \frac{2}{3\log q}\big)$ and applying the lower bound we have assumed on $H(\xi)$. The theorem therefore follows with $A := \max(A_1, 2A_2, e^6 + 1)$. □

4. Limitations on the Equidistribution of Primes

In this section we will prove Theorems 1.3 and 1.4, which guarantee the existence of irregularities in the distribution of primes in short intervals and in arithmetic progressions with large moduli. We begin with a lemma which allows us to estimate $H(\xi)$ in the relevant cases.

Lemma 4.1. *Assume that α, β, and ξ are given with $0 < \alpha < \beta \leq 1$ and $6/z < \xi \log q < 1$. Then for sufficiently large z we have*

$$\sum_{\deg p \in [\alpha z, \beta z]} |p|^{-1+\xi} \asymp \frac{q^{\xi\beta z}}{\xi z \log q}. \tag{4.1}$$

Remark. The constants implied by $\gg$ and "sufficiently large" in the lemma above depend on α and β but not ξ or q. We will apply this lemma with fixed values of α and β, so that in these applications the implied constants may be taken to be absolute.

Proof. We first observe that

$$\sum_{\deg p \in [\alpha z, \beta z]} |p|^{-1+\xi} \gg \frac{1}{z} \sum_{i \in [\alpha z, \beta z]} q^{\xi i}.$$

To prove the lower bound in (4.1) we use (3.12) to see that

$$\sum_{i \in [\alpha z, \beta z]} q^{\xi i} \geq \frac{q^{\xi(\beta z - 1)} - q^{\xi \alpha z}}{1 - q^{-\xi}} \geq \frac{q^{\xi\beta z}}{\xi \log q} q^{-\xi} \Big(1 - q^{\xi[(\alpha-\beta)z+1]}\Big).$$

When $z \geq \frac{6}{\beta - \alpha}$, the bounds on $\xi \log q$ imply that

$$\sum_{i \in [\alpha z, \beta z]} q^{\xi i} > \frac{q^{\xi\beta z}}{\xi \log q} \left(\frac{1}{e}\Big(1 - e^{5(\alpha-\beta)}\Big)\right),$$

as desired. To prove the upper bound in (4.1), we observe (again using (3.12)) that

$$\sum_{i \in [\alpha z, \beta z]} q^{\xi i} \leq \frac{q^{\xi\beta z}}{1 - q^{-\xi}} \leq \frac{2q^{\xi\beta z}}{\xi \log q}.$$

□

Proof of Theorem 1.3. The proof largely follows Maier's original proof [9]. We construct a polynomial Q and find integers $u_\pm$ so that the number of polynomials of degree $u_\pm$ which are coprime to Q differs from the expected number. We then use a Maier matrix construction and the prime number theorem for arithmetic progressions to find short intervals which contain more or fewer primes than expected.

We prove the result only for f_+, the f_- case being exactly similar. Define

$$Q := \prod_{z/2 \le \deg p \le z} p,$$

and observe that

$$\deg Q < \frac{q^{z+1}}{q-1}, \tag{4.2}$$

which in turn implies that

$$\phi(Q) < q^{\deg Q} < q^{2q^z} < q^{2D/5}. \tag{4.3}$$

We now use Corollary 3.6 to find u_+ as mentioned earlier. In the notation of Section 3, we take $f_Q(x)$ to be the characteristic function of those x coprime to Q. Lemma 4.1 implies (with $\alpha = 1/2$ and $\beta = 1$) that the condition on $H(\xi)$ in the corollary is satisfied, with the constant A absolute. We write

$$u' := u\Big(1 - \frac{A}{\log(u/z)}\Big)^{-1},$$

and for any $B > A$, the condition $B < u/z \ll e^{2z/3}$ implies that $A < u'/z \ll e^{2z/3}$. Moreover, if B is sufficiently large, then we will have $u'(1 + A/\log(u'/z)) < u(1 + 3A/\log(u/z))$. Hence, Corollary 3.6 implies that there exists $u_+ \in (u, u(1 + 3A/\log(u/z)))$ such that the number of polynomials of degree u_+ coprime to Q is

$$\ge q^{u_+}\left[\frac{\phi(Q)}{q^{\deg Q}} + \exp\Big(-\frac{u_+}{z}\Big(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O(1)\Big)\Big)\right]. \tag{4.4}$$

We now define a Maier matrix M, with (r, s) entry $rQ + s$, where r ranges over all monic polynomials of degree $D - \deg Q$, and s ranges over all monic polynomials of degree u_+. The columns are arithmetic progressions of the form $(D; Q, s)$, and the rows are short intervals of the form $(rQ + q^{u_+}, u_+ - 1)$.

The prime number theorem for arithmetic progressions, in the form (2.9), together with (4.3), imply that each column with $(s, Q) = 1$ contains

$$\frac{1}{\phi(Q)}\frac{q^D}{D} + O(Dq^{D/2}) = \frac{1}{\phi(Q)}\frac{q^D}{D}\Big(1 + O(q^{-D/11})\Big) \tag{4.5}$$

primes. It follows from our lower bound on D and our upper bound on u/z that $D/20 \ge u_+/z$, so that $q^{-D/11} \le \exp(-u_+/z)$. Multiplying (4.4) and (4.5), we see that the total number of primes in M is therefore

$$\ge \frac{q^D}{D\phi(Q)} q^{u_+}\left[\frac{\phi(Q)}{q^{\deg Q}} + \exp\Big(-\frac{u_+}{z}\Big(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O(1)\Big)\Big)\right].$$

There are $q^{D-\deg Q}$ rows, so upon simplifying, we see that at least one row of M is an interval of the form $(f, u_+ - 1)$ with $\deg f = D$ containing

$$\ge \frac{q^{u_+}}{D}\left[1 + \exp\Big(-\frac{u_+}{z}\Big(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O(1)\Big)\Big)\right]$$

primes. By subdividing the interval appropriately, we obtain an interval (f, u) with $\geq \frac{q^{u+1}}{D}[1 + \cdots]$ primes. We also use the estimates $\log(u_+/z) = \log(u/z) + O(1)$ and $u_+ = u + O(1/\log(u/z))$ to see that our interval (f, u) contains

$$\geq \frac{q^{u+1}}{D}\left[1 + \exp\left(-\frac{u}{z}\left(\log\left(\frac{u}{z}\right) + \log\log\left(\frac{u}{z}\right) + O(1)\right)\right)\right]$$

primes, as desired. □

To prove Theorem 1.4, we first need to prove the existence of a modulus Q which satisfies certain technical constraints.

Lemma 4.2. *If l is a polynomial of degree at most $e^{2z/3}$ (at most $2^{2z/3}$ if $q = 2$), then there exists a polynomial Q which is coprime to l, whose prime factors all have degrees in $[z/2, z]$, and which satisfies*

$$\sum_{p|Q} |p|^{-1+\xi} \gg \frac{q^{\xi z}}{\xi z \log q}. \tag{4.6}$$

We observe that if $f_Q(n)$ is the characteristic function of those n coprime to Q, (4.6) provides the lower bound on $H(\xi)$ required by Corollary 3.6.

Proof. We will prove that we may in fact take

$$Q = Q(l) := \prod_{\substack{\deg p \in [z/2, z] \\ (p,l)=1}} p. \tag{4.7}$$

Define a polynomial l_0 by

$$l_0 := \prod_{\deg p \in [z/2, 3z/4]} p, \tag{4.8}$$

which we will think of as the "worst possible" l. Lemma 4.1 implies that $Q(l_0)$ satisfies (4.6), and we have

$$\deg l_0 = (1 + o_z(1)) \sum_{i \in [z/2, 3z/4]} q^i \geq (1 + o_z(1)) q^{3z/4 - 1},$$

which is greater than $e^{2z/3}$ if $q \neq 2$, and greater than $2^{2z/3}$ if $q = 2$.

If l has degree at most $e^{2z/3}$ (or $2^{2z/3}$), then it must have fewer prime divisors of degrees in $[z/2, z]$ than l_0. We may therefore define a polynomial l' by replacing those prime divisors of l with degrees in $(3z/4, z]$ with an equal number of primes with degrees in $[z/2, 3z/4]$ which are not already divisors of l. We see immediately that $Q(l_0) \mid Q(l')$, and if $h(Q)$ denotes the sum on the left of (4.6), we have $h(Q(l_0)) < h(Q(l')) < h(Q(l))$, so that $Q(l)$ also satisfies (4.6) as desired. □

Proof of Theorem 1.4. Again, we will prove only the u_+ result, the u_- result being exactly similar. We use Lemma 4.2 to choose Q coprime to l so that the conditions on Q and $H(\xi)$ of Corollary 3.6 are satisfied, and we define u_+ as in the proof of Theorem 1.3, so that the number of polynomials of degree u_+ which are coprime to Q is given by (4.4).

We define a Maier matrix M with (r, s) entry $rQ + sl$, where r ranges over all polynomials with arbitrary leading coefficient of degree at most $D - \deg Q$, and s ranges over all monic polynomials of degree u_+. The rows are arithmetic progressions $(D + u_+; l, rQ)$, and the columns are sets of the form $(sl, D; Q, sl)$.

We use Rhin's result (2.9) and argue as in the proof of Theorem 1.3 to see that each column with $(Q, sl) = 1$ contains

$$\frac{1}{\phi(Q)}\frac{q^{D+1}}{D+u_+} + O\big((D+u_+)q^{(D+u_+)/2}\big) = \frac{1}{\phi(Q)}\frac{q^{D+1}}{D+u_+}\Big(1+O(q^{-D/11})\Big)$$

primes.

Since $(Q, l) = 1$, we may compute the number of s with $(Q, sl) = 1$ as in Theorem 1.3. We conclude that the total number of primes in the matrix is

$$\geq \frac{1}{\phi(Q)}\frac{q^{D+1}}{D+u_+}q^{u_+}\left[\frac{\phi(Q)}{q^{\deg Q}} + \exp\left(-\frac{u_+}{z}\left(\log\Big(\frac{u_+}{z}\Big) + \log\log\Big(\frac{u_+}{z}\Big) + O(1)\right)\right)\right]. \tag{4.9}$$

Those rows for which r is coprime to l will contain primes, and we compute that there are

$$\frac{\phi(l)}{|l|}q^{D-\deg Q+1} + O(\tau(\mathrm{sf}(l))) \tag{4.10}$$

such r. Here $|l| = q^D$, and $\tau(\mathrm{sf}(l))$ is the number of divisors of the squarefree kernel of l. To bound the error term, we observe that l can have at most $2D/z$ distinct prime divisors: at most $(1+o(1))\frac{q^{z+1}}{(q-1)z} < \frac{D}{z}$ of degree $\leq z$, and at most $\frac{D}{z}$ of degree $> z$. Therefore, $\tau(\mathrm{sf}(l)) \leq 2^{2D/z}$. As $D > 2\deg Q$ we readily compute that the quantity in (4.10) is

$$\phi(l)q^{-\deg Q+1}(1+O(q^{-D/11})). \tag{4.11}$$

Dividing (4.9) by (4.11), simplifying, and approximating u_+/z by u/z as in Theorem 1.3, we conclude that at least one row is an arithmetic progression of the form $(D+u_+; l, a)$ with $(a, l) = 1$ containing

$$\geq \frac{q^{D+u_+}}{\phi(l)(D+u_+)}\left[1+\exp\left(-\frac{u}{z}\left(\log\Big(\frac{u}{z}\Big) + \log\log\Big(\frac{u}{z}\Big) + O(1)\right)\right)\right] \tag{4.12}$$

primes as desired. □

To justify the remark made after the theorem, we let $Q = \prod_{\deg p\in[z/2,z]} p$, determine $u_\pm$ as before, and let l be any prime of degree $D - u_\pm$. We allow r to range over polynomials of degree $\leq D - u_\pm - \deg Q$, and then the argument proceeds as before.

5. Maier Matrices and the Uncertainty Principle

In this section we will return to the general setting described in Section 2 and prove Theorems 1.1 and 1.2. We first need several preliminary results. We write

$$\Delta_m(n) := \max_{a \pmod m}\left|\mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n)\right| \Big/ \frac{\mathcal{A}(n)}{\phi(m)}, \tag{5.1}$$

which measures the failure of polynomials of degree n to be equidistributed modulo m.

Our first result, the analogue of Proposition 2.2 of [8], establishes that $\Delta_m(n)$ cannot always be close to zero if $f_m(x)$ exhibits oscillatory behavior of the sort described in Section 3.

Proposition 5.1. *Let n be large, and assume that coprime monic polynomials m and l are given with $\deg m \leq n/2$ and $n > \deg l \geq n/2$. Then we have*

$$\frac{|m|}{\phi(m)}\Delta_m(n) + \frac{|l|}{\phi(l)}\Delta_l(n) + O(q^{-n/8}/\gamma_l) \geq \left|\frac{1}{q^{n-\deg l}}\sum_{\deg x = n-\deg l}\frac{f_m(x)}{\gamma_m} - 1\right|. \tag{5.2}$$

Proof. We define integers $R := n - \deg m - 1$ and $S := n - \deg l$, and a Maier matrix M with (r, s) entry $rm + sl$, where s ranges over monic polynomials of degree exactly S, and r ranges over polynomials of degree at most R and arbitrary leading coefficient. Then the rows of M are arithmetic progressions of the form $(n; l, rm)$ and the columns are arithmetic progressions of the form $(n; m, sl)$.

Since $f_l(r) = f_l(rm)$, the definition (5.1) implies that

$$\mathcal{A}(n; l, rm) = \frac{f_l(r)}{|l|\gamma_l}\mathcal{A}(n) + \epsilon_1 \Delta_l(n)\frac{\mathcal{A}(n)}{\phi(l)},$$

where ϵ_1, ϵ_2, etc. will denote real numbers between -1 and 1. Summing over all rows in the matrix, the total is

$$\mathcal{A}(n)\sum_r \frac{f_l(r)}{|l|\gamma_l} + \epsilon_2 \Delta_l(n)\frac{\mathcal{A}(n)}{\phi(l)}q^{R+1}. \tag{5.3}$$

A column-by-column calculation establishes that the total is also

$$\mathcal{A}(n)\sum_s \frac{f_m(s)}{|m|\gamma_m} + \epsilon_3 \Delta_m(n)\frac{\mathcal{A}(n)}{\phi(m)}q^{S}, \tag{5.4}$$

and we equate (5.3) and (5.4) and multiply through by $q^{\deg(lm)-n} = \frac{|l|}{q^{R+1}} = \frac{|m|}{q^S}$ to conclude that

$$\frac{1}{q^{R+1}}\sum_r \frac{f_l(r)}{\gamma_l} + \epsilon_2 \frac{|l|}{\phi(l)}\Delta_l(n) = \frac{1}{q^S}\sum_s \frac{f_m(s)}{\gamma_m} + \epsilon_3 \frac{|m|}{\phi(m)}\Delta_m(n). \tag{5.5}$$

To evaluate $\sum_r f_l(r)$, we write $\sum_r f_l(r) = (q-1)\sum_r' f_l(r)$, where the second sum is over monic r. We write $f_l(r) = \sum_{d|r} g_l(d)$ as in (3.5), so that

$$\begin{aligned}\sum_r{}' f_l(r) = \sum_r{}' \sum_{d|r} g_l(d) = \sum_{\deg d \le R} g_l(d) \sum_{\substack{\deg r \le R \\ d|r}}{}' 1 &= \sum_{\deg d \le R} g_l(d)\Big(\frac{q^{R+1-\deg d}}{q-1} + O(1)\Big) \\ &= \frac{q^{R+1}}{q-1}\sum_{\deg d \le R}\frac{g_l(d)}{|d|} + O\Big(\sum_{\deg d \le R} g_l(d)\Big),\end{aligned}$$

so that

$$\sum_r f_l(r) = q^{R+1}\sum_{\deg d \le R}\frac{g_l(d)}{|d|} + O\Big((q-1)\sum_{\deg d \le R} g_l(d)\Big). \tag{5.6}$$

The first sum over d is approximately equal to γ_l, with an error of $\sum_{\deg d > R} g_l(d)/|d|$, and the combined error is, for large n and $C := \frac{1}{1-2^{-2/3}}$,

$$\ll q^{1+2R/3}\sum_d \frac{g_l(d)}{|d|^{2/3}} \le q^{1+2R/3}\exp\Big(C\sum_{p|l}\frac{1}{|p|^{2/3}}\Big) \le q^{3R/4-2}. \tag{5.7}$$

The second inequality in (5.7) follows by expanding the sum in an Euler product, using the fact that $g_l(d) = 0$ for any $d \nmid l$, using the bound $|g_l(d)| \le 1$ for all d, and then summing the resulting geometric series. The third inequality will follow if $\exp(C\sum_{p|l}\frac{1}{|p|^{2/3}}) \le q^{R/13}$. As $R \ge \frac{1}{2}\deg l$, it is enough to show that

$$\sum_{p|l} 1 \le \frac{\log q}{26C}\deg l. \tag{5.8}$$

For $\log q \ge 26C$ this is immediate. For $q < \exp(26C)$, we observe that only a uniformly bounded number of primes may have degree $< \frac{52C}{\log q}$, and then (5.8) follows for large l.

We conclude from (5.6) and (5.7) that

$$\sum_r f_l(r) = q^{R+1}\Big(\gamma_l + O(q^{-n/8})\Big).$$

Substituting into (5.5) and rearranging terms, the proposition then follows. □

We now claim a similar result for short intervals. We define

$$\tilde{\Delta}(n,i) := \max_{\deg f = n} \left| \mathcal{A}(f,i) - \frac{\mathcal{A}(n)}{q^{n-(i+1)}} \right| \Big/ \frac{\mathcal{A}(n)}{q^{n-(i+1)}}, \tag{5.9}$$

as a measure of polynomials of degree n to be well-distributed in short intervals. The maximum is over all intervals (f,i), where f ranges over all polynomials of degree n.

Proposition 5.2. *Let n be large, let m be a polynomial with $\deg m \le n/2$, and suppose $i < n-1$. Then, we have*

$$\frac{|m|}{\phi(m)}\Delta_m(n) + \tilde{\Delta}(n,i) \ge \left| \frac{1}{q^{i+1}} \sum_{\deg x = i+1} \frac{f_m(x)}{\gamma_m} - 1 \right|. \tag{5.10}$$

Proof. The proof is similar to that of Proposition 5.1, but simpler. We construct a Maier matrix M, whose (r,s)-entry is the polynomial $rm+s$, where r ranges over all monics of degree $n - \deg m$ and s ranges over all monics of degree $i+1$. The rows are then short intervals of the form $(rm + q^{i+1}, i)$, and the columns are arithmetic progressions of the form $(n; m, s)$. Adding by rows and columns and equating, we conclude that

$$\frac{q^{n-\deg m}}{q^{n-(i+1)}}\big(1 + \epsilon_1 \tilde{\Delta}(n,i)\big) = \sum_{\deg s = i+1} \frac{f_m(s)}{|m|\gamma_m} + \epsilon_2 \Delta_m(n) \frac{q^{i+1}}{\phi(m)},$$

similarly to (5.5). (Here ϵ_1, ϵ_2 are quantities between -1 and 1.) The result then follows by multiplying through by $q^{\deg m - (i+1)}$ and rearranging terms. □

We are now ready to prove Theorems 1.1 and 1.2. In each case we will deduce the theorem from a similar but more technical proposition, along the lines of Theorems 2.4 and 2.5 of [8].

Proposition 5.3. *Let z be large, and assume that $n \ge 5q^z$. Let $\mathcal{S}$ be a set of 'bad' primes of degrees $< 99z/100$. Assume further that for some η satisfying $e^{-z/13} \le \eta \le 1/100$ we have*

$$\sum_{\deg p \in [(1-\eta)z, z]} \frac{1 - h(p)}{|p|} \ge \eta^2. \tag{5.11}$$

Then for all $5z/\eta^2 \le u \le e^{z/2}$ (for $q = 2$, for all $5z/\eta^2 \le u \le e^{z/5}$) we have

$$\max_{\deg l \le n-u; (l,\mathcal{S})=1} \Delta_l(n) \ge \frac{1}{3} \exp\left(-\frac{u}{z}(1+25\eta)\log\left(\frac{2u}{z\eta^2}\right)\right).$$

Proof. We write

$$Q := \prod_{\deg p \in [(1-\eta)z, z]} p, \tag{5.12}$$

so that we have

$$\deg Q < \frac{q^{z+1}}{q-1} \le 2q^z \le \frac{n}{2},$$

and we also check that $\frac{|Q|}{\phi(Q)} < \frac{5}{4}$. We recall the definition of $f_Q(x)$ in (2.6), and as Q is squarefree we have $f_Q(p) \le h(p)$. It therefore follows that

$$\sum_{\deg p \in [(1-\eta)z, z]} \frac{1 - f_Q(p)}{|p|} \ge \sum_{\deg p \in [(1-\eta)z, z]} \frac{1 - h(p)}{|p|} \ge \eta^2.$$

Corollary 3.5 then implies that if $e^{z/2} \ge u \ge 5z/\eta^2$ (for $q = 2$, if $e^{z/2} \ge u \ge 5z/\eta^2$) there exists an integer $\lambda \in [u, u(1+23\eta)]$ such that

$$\frac{1}{q^\lambda} \sum_{\deg x = \lambda} (f_Q(x) - G_Q(1)) \ge \exp\left(-\frac{u}{z}(1+25\eta) \log\left(\frac{2u}{z\eta^2}\right)\right).$$

We have that if $u \le e^{z/2}$, then $\lambda \le e^{z/2}(1+23\eta) \le \frac{n}{2}$ and so we may apply Proposition 5.1. We let l be any prime of degree $n - \lambda$, so that l, Q, and $\mathcal{S}$ are all coprime, and Proposition 5.1 implies that

$$\frac{|Q|}{\phi(Q)}\Delta_Q(n) + \frac{|l|}{\phi(l)}\Delta_l(n) + O(q^{-n/8}/\gamma_l) \ge \exp\left(-\frac{u}{z}(1+25\eta) \log\left(\frac{2u}{z\eta^2}\right)\right). \tag{5.13}$$

We observe that $|Q|/\phi(Q)$, $|l|/\phi(l)$, and $1/\gamma_l$ are each less than $5/4$, and that $q^{-n/8}$ is much smaller than the quantity at right, to conclude that for large n

$$\Delta_Q(n) + \Delta_l(n) \ge \frac{2}{3} \exp\left(-\frac{u}{z}(1+25\eta) \log\left(\frac{2u}{z\eta^2}\right)\right), \tag{5.14}$$

which immediately implies our result.

□

Proof of Theorem 1.1. We first observe that the prime number theorem (2.8) and (1.3) imply that

$$\sum_{\eta y \le \deg p \le y} \frac{1 - h(p)}{|p|} \deg p \ge \frac{2\alpha}{3} y. \tag{5.15}$$

We now claim that there is some $z \in [\eta y, y]$ satisfying the condition (5.11). For if not, we have for each $z \in [\eta y, y]$ that

$$\sum_{\deg p \in [(1-\eta)z, z]} \frac{1 - h(p)}{|p|} \deg p < \eta^2 z.$$

Summing over $z \in \{y, (1-\eta)y, (1-\eta)^2 y, \dots\}$, we obtain a series of intervals covering $[\eta y, y]$, and we conclude that

$$\sum_{\eta y \le \deg p \le y} \frac{1 - h(p)}{|p|} \deg p < \eta y,$$

contradicting (5.15).

We see that the condition $\eta \ge 13 \log y/y$ of Theorem 1.1 implies that $\eta \ge e^{-z/13}$ for any $z \ge \eta y$, by checking this for the minimum values $z = \eta y$ and $\eta = 13 \log y/y$. We also readily check that the condition on $\mathcal{S}$ in Theorem 1.1 implies the one in Proposition 5.3. Theorem 1.1 therefore follows from Proposition 5.3. □

Proposition 5.4. *Let z be large, and assume that $n \ge 5q^z$. Let $\mathcal{S}$ be a set of 'bad' primes of degrees $< 99z/100$. Assume further that for some η satisfying $e^{-z/13} \le \eta \le 1/100$ we have*

$$\sum_{\deg p \in [(1-\eta)z, z]} \frac{1 - h(p)}{|p|} \ge \eta^2. \tag{5.16}$$

Then for all $5z/\eta^2 \le u \le e^{z/2}$ (for $q = 2$, for all $5z/\eta^2 \le u \le e^{z/5}$), at least one of the following statements is true:

(i) For each m which is composed only of primes of degrees in $[(1-\eta)z, z]$ that satisfies

$$\sum_{p|m} \frac{1-h(p)}{|p|} \ge \eta^2, \tag{5.17}$$

we have $\Delta_m(n) \ge \frac{1}{2}\exp(-\frac{u}{z}(1+25\eta)\log(2u/z\eta^2))$.

(ii) We have $\tilde{\Delta}(n, u-1) \ge \frac{1}{2}\exp(-\frac{u}{z}(1+25\eta)\log(2u/z\eta^2))$.

Proof. The proof is essentially the same as the proof of Proposition 5.3. Define Q as in (5.12), and let m be any divisor of Q which satisfies (5.17). We use Corollary 3.5 as before with m in place of Q, and Proposition 5.2 then implies that for some $i \ge u$ we have

$$\Delta_m(n) + \tilde{\Delta}(n, i-1) \ge \exp\bigg(-\frac{u}{z}(1+25\eta)\log\bigg(\frac{2u}{z\eta^2}\bigg)\bigg). \tag{5.18}$$

We observe that $\tilde{\Delta}(n, i-1) \ge \tilde{\Delta}(n, u-1)$, as any irregular interval may be subdivided into subintervals, at least one of which will be irregular. The result then follows immediately. □

Proof of Theorem 1.2. The proof is very similar to that of Theorem 1.1. Again using (2.8), we have

$$\sum_{\eta y \le \deg p \le \lceil (1-\eta)y \rceil} \frac{1-h(p)}{|p|} \deg p \ge \frac{\alpha}{3} y. \tag{5.19}$$

If there is no $z \in [\eta y, \lceil (1-\eta)y \rceil]$ satisfying the condition (5.16), we obtain a geometric series as before and this time conclude that

$$\sum_{\eta y \le \deg p \le \lceil (1-\eta)y \rceil} \frac{1-h(p)}{|p|} \deg p \le \eta \lceil (1-\eta)y \rceil < \frac{\alpha}{3} y,$$

contradicting (5.19).

Thus, let z be such that (5.16) is satisfied, and let m be the product of all primes of degrees in $[(1-\eta)z, z]$. We have

$$\deg m \le \sum_{\deg p \le \lceil (1-\eta)y \rceil} \deg p \le 2q^{1+(1-\eta)y},$$

and the result now follows from Proposition 5.4. □

6. Further Examples and Applications

In this section we discuss several further examples and applications that are interesting and are simple to describe. Again we are closely following [8], and in the interest of brevity our discussion in this section will be less precise than before (or that in [8]). We reiterate that we expect that all of the examples in [8] should have analogies in $\mathbb{F}_q[t]$.

6.1. **Almost primes.** For a fixed r, we define a P_r polynomial to be a square-free polynomial with at most r distinct irreducible factors, and an E_r polynomial to be one with exactly r distinct irreducible factors. Letting $\pi_r(n)$ denote the number of (monic) E_r polynomials of degree n, Cohen [3] has proved the estimate

$$\pi_r(n) = \frac{q^n(\log n)^{r-1}}{(r-1)!n} + O\Big((\log n)^{r-2}\frac{q^n}{n}\Big). \tag{6.1}$$

In particular it follows that for each monic polynomial m, the proportion $h(m)$ of P_r and E_r polynomials divisible by m is zero. Therefore, these sets of polynomials (and arbitrary subsets thereof) constitute arithmetic sequences for each r, and Theorems 1.1 and 1.2 apply to these sequences.

6.2. **Norms from extensions of $\mathbb{F}_q(t)$.** Let K be a finite, geometric extension of $\mathbb{F}_q(t)$ (that is, one whose constant field is also $\mathbb{F}_q(t)$). In the notation of Section 2, We let $a(x)$ be the characteristic function of those polynomials that are norms of integral elements in K. As in $\mathbb{Z}$, a polynomial x is a norm from K if and only if p^e is whenever $p^e||x$. Therefore these polynomials form an arithmetic sequence, with $h(p) = 1$ for any prime p which is a norm from K, and $h(p) = O(1/|p|)$ for any prime which is not. The Chebotarev Density Theorem for function fields (see the work of Murty and Scherk [11] for an effective version) guarantees that both sets of primes have a positive density, so that the condition (1.4) is satisfied with a constant α depending on K. Accordingly the sequence of norms from K is irregularly distributed, as described by Theorems 1.1 and 1.2.

With some effort we expect to be able to prove additional similar results, along lines suggested by Examples 3, 7, and 8 of [8].

6.3. **Limitations on sieve estimates.** Let $\mathcal{A}$ be a set of monic polynomials in $\mathbb{F}_q[t]$, and let $\mathcal{P}$ be a set of primes. Define $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ to be the number of elements of $\mathcal{A}$ which have no prime factor $p \in \mathcal{P}$ with $\deg p \leq z$. Sieve theory (in $\mathbb{F}_q[t]$) is concerned with estimating $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ under certain natural hypotheses. For example, if $\mathcal{A}$ is the set of all monics up to a certain degree D, which is sufficiently large in relation to z, then it is possible to obtain good estimates for $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$.

The literature on sieve methods in $\mathbb{F}_q[t]$ is much less extensive than that for $\mathbb{Z}$. (But one may see, for example, the work of Car [2] adapting the Selberg sieve to $\mathbb{F}_q[t]$.) In this section we will show how our framework may be used to prove limitations on the quality of sieve estimates. This is in analogy to Corollaries 1.1, 1.2, and 6.1 of [8]; for simplicity we will formulate only the analogy of Corollary 6.1 and we will exclude the case $q = 2$ (for which a similar result could be obtained with additional effort).

Corollary 6.1. *Suppose that $q \neq 2$, and Q is a large squarefree polynomial which satisfies*

$$\sum_{p|Q} \frac{\deg p}{|p|} \geq 39 \log\log(\deg Q), \tag{6.2}$$

and define

$$\alpha := \frac{1}{\log(\deg Q)} \sum_{p|Q} \frac{\deg p}{|p|}, \tag{6.3}$$

and write $\eta := \min(1/100, \alpha/3)$. Then for $(\deg Q)^{\eta/2} \geq u \geq 5\log(\deg Q)/\eta^2$ and any $n \geq 2\deg Q$ there exist intervals $I_\pm$ of the form $(f_\pm, u)$ with $\deg f_\pm = n$, such that

$$\sum_{f \in I_+; (f,Q)=1} 1 \geq \frac{\phi(Q)}{|Q|} |I_+| \left(1 + \exp\left(-\frac{u}{\eta \log(\deg Q)}(1+25\eta)\log\left(\frac{2u}{\eta^3 \log(\deg Q)}\right)\right)\right), \tag{6.4}$$

$$\sum_{f \in I_-; (f,Q)=1} 1 \leq \frac{\phi(Q)}{|Q|} |I_-| \left(1 - \exp\left(-\frac{u}{\eta \log(\deg Q)}(1+25\eta)\log\left(\frac{2u}{\eta^3 \log(\deg Q)}\right)\right)\right). \tag{6.5}$$

Proof. As before we will argue only the I_+ case. Write $y = \log(\deg Q)$. We first claim that there exists some integer $z \in [\eta y, y - 3]$ such that

$$\sum_{\substack{\deg p \in [(1-\eta)z, z] \\ p|Q}} \frac{1}{|p|} \geq \eta^2. \tag{6.6}$$

To prove this, one argues by contradiction; if (6.6) fails, then the prime number theorem and the argument used in the proof of Theorem 1.1 provide a bound for $\sum_{p|Q} \deg p/|p|$ from above, which contradicts (6.2).

We may now apply Corollary 3.5. Let $a(x)$ be the characteristic polynomial of those polynomials coprime to Q and write

$$l := \prod_{\substack{\deg p \in [(1-\eta)z, z] \\ p|Q}} p. \tag{6.7}$$

Corollary 3.5 then implies that for $e^{z/2} \geq u \geq 5z/\eta^2$ there exists $u_+ \geq u$ satisfying

$$\sum_{\substack{\deg s = u_+ \\ (s,l)=1}} 1 \geq q^{u_+} \frac{\phi(l)}{|l|} \left(1 + \exp\left(-\frac{u}{z}(1+25\eta)\log\left(\frac{2u}{z\eta^2}\right)\right)\right). \tag{6.8}$$

We now construct a Maier matrix with entries $rl+s$, where s ranges over all monic polynomials of degree u_+, and r ranges over all monic polynomials of any fixed degree $R \geq \deg Q$. We compute that each column with $(s,l) = 1$ contains (exactly) $q^R\phi(Q/l)/|Q/l|$ elements coprime to Q, and multiplying this by (6.8) and dividing by the number of rows we obtain an interval $(rl + q^{u_+}, u_+)$ satisfying the inequality (6.4). Subdividing this into intervals of the form (f, u) we obtain the corollary. □

References

[1] A. Balog and T. Wooley, *Sums of two squares in short intervals*, Canad. J. Math. **52** (2000), 673-694.
[2] M. Car, *Le théorème de Chen pour* $\mathbf{F}_q[X]$, Dissertationes Math. **223** (1984), 54 pp.
[3] S. Cohen, *Further arithmetical functions in finite fields*, Proc. Edinburgh Math. Soc. (2) **16** (1968/1969), 349-363.
[4] B. Conrad, K. Conrad, and R. Gross, *Prime specialization in genus 0*, preprint.
[5] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.
[6] J. B. Friedlander and A. Granville, *Limitations to the equi-distribution of primes I*, Ann. of Math. **129** (1989), 363-382.
[7] A. Granville, *Unexpected irregularities in the distribution of prime numbers*, Proceedings of the International Congress of Mathematicians (Zürich, 1994), 388-399, Birkhäuser, Basel, 1995.
[8] A. Granville and K. Soundararajan, *An uncertainty principle for arithmetic sequences*, Ann. of Math. **165** (2007), no. 2, 593-635.
[9] H. Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), 221-225.
[10] E. Manstavičius and R. Skrabutėnas, *Summation of values of multiplicative functions on semigroups*, Lithuanian Math. J. **33** (1993), 255-264.
[11] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. (Paris), **319** (1994), 523-528.
[12] P. Pollack, *Simultaneous prime specializations of polynomials over finite fields*, preprint.
[13] G. Rhin, *Répartition modulo 1 dans un corps de séries formelles sur un corps fini*, Dissertationes Math. **95** (1972), 75 pp.
[14] M. Rosen, *Number theory in function fields*, GTM 210, Springer-Verlag, New York, 2002.
[15] K. Soundararajan, *The distribution of prime numbers*, Equidistribution in number theory, an introduction, 59-83, NATO Sci. Ser. II Math. Phys. Chem. **237**, Springer, Dordrecht, 2007.
[16] F. Thorne, *Irregularities in the distribution of primes in function fields*, J. Number Theory, accepted for publication.
[17] E. Udovina, unpublished manuscript.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: thorne@math.wisc.edu