BOUNDED GAPS BETWEEN PRIME POLYNOMIALS WITH A GIVEN PRIMITIVE ROOT

LEE TROUPE

Abstract. A famous conjecture of Artin states that there are infinitely many prime numbers for which a fixed integer g is a primitive root, provided $g \neq -1$ and g is not a perfect square. Thanks to work of Hooley, we know that this conjecture is true, conditional on the truth of the Generalized Riemann Hypothesis. Using a combination of Hooley's analysis and the techniques of Maynard-Tao used to prove the existence of bounded gaps between primes, Pollack has shown that (conditional on GRH) there are bounded gaps between primes with a prescribed primitive root. In the present article, we provide an unconditional proof of the analogue of Pollack's work in the function field case; namely, that given a monic polynomial $g(t)$ which is not an vth power for any prime v dividing $q-1$, there are bounded gaps between monic irreducible polynomials $P(t)$ in $\mathbb{F}_q[t]$ for which $g(t)$ is a primitive root (which is to say that $g(t)$ generates the group of units modulo $P(t)$). In particular, we obtain bounded gaps between primitive polynomials, corresponding to the choice $g(t) = t$.

1. Introduction

Among the most prominent conjectures in number theory is the prime k-tuples conjecture of Hardy and Littlewood, the qualitative version of which states that for any admissible tuple of integers $\mathcal{H} = \{h_1, \ldots, h_k\}$, there are infinitely many natural numbers n such that the shifted tuple $n+\mathcal{H} = \{n+h_1, \ldots, n+h_k\}$ consists entirely of primes. To this day, we do not know of a single admissible tuple for which the above statement is true.

We can instead ask for something weaker: Can we show that infinitely many shifts of admissible k-tuples contain just two or more primes? In 2013, Yitang Zhang stunned the mathematical world by demonstrating that, for every sufficiently long tuple $\mathcal{H}$, there are infinitely many natural numbers n for which $n+\mathcal{H}$ contains at least two primes, thereby establishing the existence of infinitely many bounded gaps between consecutive primes [Zha14]. Zhang's breakthrough was soon followed by work of Maynard [May15] and Tao, who independently established that infinitely many shifts of admissible k-tuples contain m primes, for any $m \geq 2$, provided k is large enough with respect to m. As a consequence, we have not only bounded gaps between primes, but also that $\liminf_{n\to\infty} p_{n+m} - p_n < \infty$ (here p_n denotes the nth prime number).

The Maynard-Tao machinery can be utilized to probe questions concerning bounded gaps between primes in other contexts. Let q be a power of a prime and

---

The author was supported by NSF RTG Grant DMS-1344994.

2000 *Mathematics Subject Classification.* 11N36; 11T06.

Key words and phrases. bounded gaps between primes; polynomials; finite fields.

consider the ring $\mathbb{F}_q[t]$. We say that an element p of $\mathbb{F}_q[t]$ is *prime* if p is monic and irreducible. The following theorem, a bounded gaps result for $\mathbb{F}_q[t]$, is due to Castillo, Hall, Lemke Oliver, Pollack, and Thompson [CHL⁺15].

Theorem 1.1. *Let $m \geq 2$. There exists an integer k_0 depending on m but independent of q such that for any admissible k-tuple $\{h_1, \ldots, h_k\} \subset \mathbb{F}_q[t]$ with $k \geq k_0$, there are infinitely many $f \in \mathbb{F}_q[t]$ such that at least m of $f+h_1, \ldots, f+h_k$ are prime.*

In particular, if $\{h_1, \ldots, h_k\} \subset \mathbb{F}_q[t]$ is a long enough admissible tuple, the difference in norm between primes in $\mathbb{F}_q[t]$ is at most $\max_{1 \leq i \neq j \leq k} |h_i - h_j|$, infinitely often. (Here $|f| = q^{\deg f}$ for $f \in \mathbb{F}_q[t]$.)

Artin's famous primitive root conjecture states that for any integer $g \neq -1$ and not a square, there are infinitely many primes for which g is a primitive root; that is, there are infinitely many primes p for which g generates $(\mathbb{Z}/p\mathbb{Z})^*$. Work of Hooley [Hoo67] establishes the truth of Artin's conjecture, assuming GRH; the following result due to Pollack [Pol14] is a bounded gaps result in this setting.

Theorem 1.2 (conditional on GRH)**.** *Fix an integer $g \neq -1$ and not a square. Let $q_1 < q_2 < \ldots$ denote the sequence of primes for which g is a primitive root. Then for each m,*

$$\liminf_{n \to \infty} (q_{n+m-1} - q_n) \leq C_m,$$

where C_m is finite and depends on m but not on g.

Artin's conjecture can be formulated in the setting of polynomials over a finite field with q elements, where q is a prime power. Let $g \in \mathbb{F}_q[t]$ be monic and not an vth power, for any v dividing $q-1$; this is analogous to the requirement that g not be a square in the integer case. We say that g is a primitive root for a prime polynomial $p \in \mathbb{F}_q[t]$ if g generates the group $(\mathbb{F}_q[t]/p\mathbb{F}_q[t])^*$. In Bilharz's 1937 Ph.D. thesis [Bil37], he confirms Artin's conjecture that there are infinitely many such p for a given g satisfying the above requirements, conditional on the Riemann hypothesis for global function fields, a result proved by Weil in 1948.

Motivated by the results catalogued above, we presently establish an unconditional result which can be viewed as a synthesis of Theorems 1.1 and 1.2.

Theorem 1.3. *Let g be a monic polynomial in $\mathbb{F}_q[t]$ such that g is not a vth power for any prime v dividing $q-1$, and let $\mathbb{P}_g$ denote the set of prime polynomials in $\mathbb{F}_q[t]$ for which g is a primitive root. For any $m \geq 2$, there exists an admissible k-tuple $\{h_1, \ldots, h_k\}$ such that there are infinitely many $f \in \mathbb{F}_q[t]$ with at least m of $f+h_1, \ldots, f+h_k$ belonging to $\mathbb{P}_g$.*

Remark 1.4. A prime polynomial $a \in \mathbb{F}_q[t]$ is called *primitive* if t is a primitive root for a; see [LN97] for an overview of primitive polynomials. Taking $g = t$, we obtain as an immediate corollary the existence of bounded gaps between primitive polynomials.

Notation. In what follows, q is an arbitrary but fixed prime power and $\mathbb{F}_q$ is the finite field with q elements. The Greek letter Φ will denote the Euler phi function for $\mathbb{F}_q[t]$; that is, $\Phi(f) = \#(\mathbb{F}_q[t]/f\mathbb{F}_q[t])^*$. The symbols $\ll, \gg$, and the O and o-notations have their usual meanings; constants implied by this notation may implicitly depend on q. Other notation will be defined as necessary.

2. The necessary tools

For a monic polynomial a and a prime polynomial P not dividing a in $\mathbb{F}_q[t]$, define the d-th power residue symbol $(a/P)_d$ to be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}.$$

Let $b \in \mathbb{F}_q[t]$ be monic, and write $b = P_1^{e_1} \cdots P_s^{e_s}$. Define

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s} \left(\frac{a}{P_j}\right)_d^{e_j}.$$

We will make use of a number of properties of the d-th power residue symbol. The following is taken from Propositions 3.1 and 3.4 of [Ros02].

Proposition 2.1. *The d-th power residue symbol has the following properties.*

(a) $\left(\frac{a_1}{b}\right)_d = \left(\frac{a_2}{b}\right)_d$ *if* $a_1 \equiv a_2 \pmod{b}$.

(b) *Let $\zeta \in \mathbb{F}_q^*$ be an element of order dividing d. Then, for any prime $P \in \mathbb{F}_q[t]$ with $P \nmid a$, there exists $a \in \mathbb{F}_q[t]$ such that* $\left(\frac{a}{P}\right)_d = \zeta$.

We now state a special case of the general reciprocity law for d-th power residue symbols in $\mathbb{F}_q[t]$, Theorem 3.5 in [Ros02]:

Theorem 2.2. *Let $a, b \in \mathbb{F}_q[t]$ be monic, nonzero and relatively prime. Then*

$$\left(\frac{a}{b}\right)_d = \left(\frac{b}{a}\right)_d (-1)^{\frac{q-1}{d}\deg(a)\deg(b)}.$$

Another essential tool in our analysis is the Chebotarev density theorem. The following is a restatement of Proposition 6.4.8 in [FJ08].

Theorem 2.3. *Write $K = \mathbb{F}_q(t)$ and let L be a finite Galois extension of K, and let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(L/K)$. Let $\mathbb{F}_{q^n}$ be the constant field of L/K. For each $\tau \in \mathcal{C}$, suppose $\mathrm{res}_{\mathbb{F}_{q^n}} \tau = \mathrm{res}_{\mathbb{F}_{q^n}} \mathrm{Frob}_q^k$, where $k \in \mathbb{N}$. The number of unramified primes P of degree k whose Artin symbol $\left(\frac{L/K}{P}\right)$ is $\mathcal{C}$ is given by*

$$\frac{\#\mathcal{C}}{m}\frac{q^k}{k} + O\left(\frac{\#\mathcal{C}}{m}\frac{q^{k/2}}{k}(m + g_L)\right),$$

where $m = [L : K\mathbb{F}_{q^n}]$, g_L is the genus of L/K, and the constant implied by the big-O is absolute.

In our application, the extension L/K will be the compositum of a Kummer extension and a cyclotomic extension of $K = \mathbb{F}_q(t)$. The next three results will help us estimate g_L.

We say that an element $a \in K^*$ is *geometric* at a prime $r \neq q$ if $K(\sqrt[r]{a})$ is a geometric field extension of K (that is, the constant field of $K(\sqrt[r]{a})$ is the same as the constant field of K). Proposition 10.4 in [Ros02] concerns the genus of such extensions; we state it below.

Proposition 2.4. *Suppose $r \neq \operatorname{char} \mathbb{F}_q$ is a prime and $K' = K(\sqrt[r]{a})$, $a \in K$ nonzero. Assume that a is geometric at r and that a is not an rth power in K^*. With $g_{K'}$ denoting the genus of K'/K,*

$$2g_{K'} - 2 = -2r + R_a(r-1),$$

where R_a is the sum of the degrees of the finitely many primes $P \in K$ where the order of P in a is not divisible by r.

Fix an algebraic closure $\overline{K}$ of K. One can define an analogue of exponentiation in $\mathbb{F}_q[t]$; that is, for $M \in \mathbb{F}_q[t]$ and $u \in \overline{K}$, the symbol u^M is again an element of $\overline{K}$. In particular, we have an analogue of cyclotomic field extensions. Define $\Lambda_M = \{u \in \overline{K} \mid u^M = 0\}$; then $K(\Lambda_M)/K$ is a *cyclotomic* extension of K, and many properties of cyclotomic extensions of $\mathbb{Q}$ carry over (at least formally) to this setting. See Chapter 12 of [Sal07] for details of this construction and for properties of these extensions. The following proposition, a formula for the genus of cyclotomic extensions of $\mathbb{F}_q(t)$, is taken from Theorem 12.7.2.

Proposition 2.5. *Let $M \in \mathbb{F}_q[t]$ be monic of the form $M = \prod_{i=1}^r P_i^{\alpha_i}$, where the P_i are distinct irreducible polynomials. Then*

$$2g_M - 2 = -2\Phi(M) + \sum_{i=1}^r d_i s_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2)\frac{\Phi(M)}{q-1},$$

where g_M is the genus of $K(\Lambda_M)/K$, $d_i = \deg P_i$, and $s_i = \alpha_i \Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i - 1)}$.

Finally, if a function field L/k with constant field k is the compositum of two subfields K_1/k and K_2/k, we can estimate the genus of L given the genera of K_1 and K_2 using Castelnuovo's inequality (Theorem 3.11.3 in [Sti09]), stated below.

Proposition 2.6. *Let K_1/k and K_2/k be subfields of L/k satisfying*

- *$L = K_1K_2$ is the compositum of K_1 and K_2, and*
- *$[L : K_i] = n_i$ and K_i/K has genus g_i, $i = 1, 2$.*

Then the genus g_L of L/K is bounded by

$$g_L \leq n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1).$$

3. Maynard-Tao over $\mathbb{F}_q(t)$

We now briefly recall the Maynard-Tao method as adapted for the function field setting in [CHL+15]. Fix an integer $k \geq 2$, and let $\mathcal{H} = \{h_1, \ldots, h_k\}$ be an admissible k-tuple of elements of $\mathbb{F}_q[t]$ (that is, for each prime $p \in \mathbb{F}_q[t]$, the set $\{h_i \pmod{p} : 1 \leq i \leq k\}$ is not a complete set of residues modulo p). Let $W = \prod_{|p|<\log\log\log(q^\ell)} p$. Define sums S_1 and S_2 as follows:

$$S_1 = \sum_{\substack{n \in A(q^\ell) \\ n \equiv \beta \pmod{W}}} \omega(n)$$

and

$$S_2 = \sum_{\substack{n \in A(q^\ell) \\ n \equiv \beta \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i) \right) \omega(n),$$

where $A(q^\ell)$ is the set of all monic polynomials in $\mathbb{F}_q[t]$ of norm q^ℓ (i.e., degree ℓ), $\mathbb{P}$ is the set of monic irreducible elements of $\mathbb{F}_q[t]$, $\beta \in \mathbb{F}_q[t]$ is chosen so that $(\beta + h_i, W) = 1$ for all $1 \leq i \leq k$ (such a β exists by the admissibility of $\mathcal{H}$), and

$$\omega(n) = \left(\sum_{\substack{d_1, \ldots, d_k \\ d_i | (n+h_i) \forall i}} \lambda_{d_1 \ldots, d_k} \right)^2$$

for suitably chosen weights $\lambda_{d_1 \ldots, d_k}$. Suppose $S_2 > (m-1)S_1$, for some integer $m \geq 2$ and some choice of weights; then there exists $n_0 \in A(q^\ell)$ such that at least m of the $n_0 + h_1, \ldots, n_0 + h_k$ are prime. The goal is to find a sequence of such $n_0 \in A(q^\ell)$ as $\ell \to \infty$. If this can be done, then infinitely often we obtain gaps between primes of size at most $\max_{1 \leq i,j \leq k : i \neq j} |h_i - h_j|$.

For the choice of suitable weights and the subsequent asymptotic formulas for S_1 and S_2, we refer to Proposition 2.3 of [CHL+15], which we restate here for convenience:

Proposition 3.1. *Let $0 < \theta < \frac{1}{4}$ be a real number and set $R = |A(q^\ell)|^\theta$. Let F be a piecewise differentiable real-valued function supported on the simplex $\mathcal{R}_k := \{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \leq 1\}$, and let*

$$F_{\max} := \sup_{(t_1, \ldots, t_k) \in [0,1]^k} |F(t_1, \ldots, t_k)| + \sum_{i=1}^{k} |\frac{\partial F}{\partial x_i}(t_1, \ldots, t_k)|.$$

Set

$$\lambda_{d_1, \ldots, d_k} := \left(\prod_{i=1}^{k} \mu(d_i)|d_i| \right) \sum_{\substack{r_1, \ldots, r_k \\ d_i | r_i \forall i \\ (r_i, W) = 1 \, \forall i}} \frac{\mu(r_1, \ldots, r_k)^2}{\prod_{i=1}^k \Phi(r_i)} F \left(\frac{\log |r_1|}{\log R}, \ldots, \frac{\log |r_k|}{\log R} \right)$$

whenever $|d_1 \cdots d_k| < R$ and $(d_1 \cdots d_k, W) = 1$, and $\lambda_{d_1, \ldots, d_k} = 0$ otherwise. Then the following asymptotic formulas hold:

$$S_1 = \frac{(1 + o(1)) \Phi(W)^k |A(q^\ell)| (\frac{1}{\log q} \log R)^k}{|W|^{k+1}} I_k(F)$$

and

$$S_2 = \frac{(1+o(1))\Phi(W)^k|A(q^\ell)|(\frac{1}{\log q}\log R)^{k+1}}{\big(\log|A(q^\ell)|\big)|W|^{k+1}}\sum_{m=1}^{k} J_k^{(m)}(F),$$

where

$$I_k(F) := \int\cdots\int_{\mathcal{R}_k} F(x_1,\ldots,x_k)^2 dx_1\ldots dx_k,$$

and

$$J_k^{(m)}(F) := \int\cdots\int_{[0,1]^{k-1}}\left(\int_0^1 F(x_1,\ldots,x_k)dx_m\right)^2 dx_1\ldots dx_{m-1}dx_{m+1}\ldots dx_k.$$

By the above proposition, as $\ell\to\infty$, $S_2/S_1 \to \theta\frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)}$. Set

$$M_k := \sup_F \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)},$$

where the supremum is taken over all F satisfying the conditions of the Proposition 3.1. Following Proposition 4.13 of [May15], we have $M_k > \log k - 2\log\log k - 2$ for all large enough k. In particular, $M_k\to\infty$, so upon choosing k large enough depending on m (and choosing F and θ appropriately), we obtain the desired result for any admissible k-tuple $\mathcal{H}$.

For the present article, we fix g satisfying the conditions of Theorem 1.3 and modify the above argument as necessary; our modifications are somewhat similar to those in [Pol14]. Given an admissible k-tuple $\mathcal{H}=\{h_1,\ldots,h_k\}$, the set $g\mathcal{H}=\{gh_1,\ldots,gh_k\}$ is again admissible. We work from now on with admissible k-tuples $\mathcal{H}$ such that every element of $\mathcal{H}$ is divisible by g. Set

$$W := \operatorname{lcm}\left(g, \prod_{|p|<\log_3(q^\ell)} p\right).$$

With $A(q^\ell)$ defined as above, we will insist that ℓ is prime; this will be advantageous in what follows. We again search among $n\in A(q^\ell)$ belonging to a certain residue class modulo W, but we must choose this residue class more carefully than in the original Maynard-Tao argument; that is, we choose this residue class so that primes detected by the sieve will have g as a primitive root.

Lemma 3.2. *We can choose $\alpha\in\mathbb{F}_q[t]$ such that, for any $1\le i\le k$ and for any $n\equiv\alpha \pmod W$ with $\deg(n)$ odd,*

- *$n+h_i$ is coprime to W, and*
- *$\left(\frac{g}{n+h_i}\right)_{q-1}$ generates $\mathbb{F}_q^*$.*

Proof. Fix a generator $\omega\in\mathbb{F}_q^*$. Suppose $\deg(g)$ is even. Write $g=p_1^{f_1}\cdots p_r^{f_r}$ with p_i irreducible for each i. Since g is not an vth power for any $v\mid q-1$, the numbers $f_1,\ldots,f_r,q-1$ have greatest common divisor equal to one. Hence, we may write

$$1 = b_1f_1+\ldots+b_rf_r+b_{r+1}(q-1)$$

for some integers b_i not all zero. Thus

$$\omega = \omega^{b_1 f_1 + \ldots + b_r f_r + b_{r+1}(q-1)} = \omega^{b_1 f_1 + \ldots + b_r f_r}.$$

Now, for each $1 \leq i \leq r$, ω^{b_i} is an element of $\mathbb{F}_q^*$ of order dividing $q-1$. By Proposition 2.1b, for each such i there exists $a_i \in \mathbb{F}_q[t]$ with $(a_i/p_i)_{q-1} = \omega^{b_i}$; and by the Chinese remainder theorem, we can replace each a_i in the system of congruences above by a single element $a \in \mathbb{F}_q[t]$. So, by definition,

$$\left(\frac{a}{g}\right)_{q-1} = \prod_{i=1}^{r} \left(\frac{a_i}{p_i}\right)_{q-1}^{f_i} = \prod_{i=1}^{r} \omega^{b_i f_i} = \omega.$$

(note that all polynomials here are monic). Choose α so that $\alpha \equiv a \pmod g$ and $(\alpha + h_i, W/g) = 1$ for all $h_i \in \mathcal{H}$; such an α can be chosen by the admissibility of $\mathcal{H}$. Then by Proposition 2.1a, for all $n \equiv \alpha \pmod W$, we have

$$\left(\frac{a}{g}\right)_{q-1} = \left(\frac{\alpha + h_i}{g}\right)_{q-1} = \left(\frac{n + h_i}{g}\right)_{q-1},$$

recalling that all $h_i \in \mathcal{H}$ are divisible by g. According to Theorem 2.2,

$$\left(\frac{n + h_i}{g}\right)_{q-1} = (-1)^{\deg(n+h_i)\deg(g)} \left(\frac{g}{n + h_i}\right)_{q-1} = \left(\frac{g}{n + h_i}\right)_{q-1},$$

so that $(\frac{g}{n+h_i})_{q-1}$ generates $\mathbb{F}_q^*$ as desired. If $\deg(g)$ is odd, so that the factor of -1 remains on the right-hand side of the above equation, repeat the argument with $-\omega$ in place of ω. $\square$

Let $\alpha \in \mathbb{F}_q[t]$ be suitably chosen according to Lemma 3.2. Define

$$\tilde{S}_1 := S_1$$

and

$$\tilde{S}_2 := \sum_{\substack{n \in A(q^\ell) \\ n \equiv \alpha \pmod W}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}_g}(n + h_i) \right) \omega(n).$$

(So $\tilde{S}_2$ is just S_2 with $\mathbb{P}$ replaced with $\mathbb{P}_g$.) Our theorem follows immediately from the following proposition.

Proposition 3.3. *We have the same asymptotic formulas for $\tilde{S}_1$ and $\tilde{S}_2$ as we do for S_1 and S_2 in Proposition 3.1.*

If we can establish Proposition 3.3, Maynard's argument to establish the existence of bounded rational prime gaps can be used to obtain Theorem 1.3.

4. Proof of Proposition 3.3

This proof follows essentially the same strategy as Section 3.3 of [Pol14]. Since $\tilde{S}_1 = S_1$, we need only concern ourselves with $\tilde{S}_2$. We can write $\tilde{S}_2 = \sum_{m=1}^{k} \tilde{S}_2^{(m)}$, where

$$\tilde{S}_2^{(m)} := \sum_{\substack{n \in A(q^\ell) \\ n \equiv \alpha \pmod W}} \chi_{\mathbb{P}_g}(n + h_m)\omega(n).$$

The proof of Proposition 3.1 (which refers to Maynard's analysis) shows that, for any m,

$$S_2^{(m)} \sim \frac{\varphi(W)^k |A(q^\ell)| (\frac{1}{\log q} \log R)^{k+1}}{|W|^{k+1} \log q^\ell} \cdot J_k^{(m)}(F).$$

To establish Proposition 3.3, it would certainly suffice to prove that the difference between $S_2^{(m)}$ and $\tilde{S}_2^{(m)}$ is asymptotically negligible, i.e., that as $\ell \to \infty$ through prime values,

$$S_2^{(m)} - \tilde{S}_2^{(m)} = o\left(\frac{\varphi(W)^k |A(q^\ell)| (\log q^\ell)^k}{|W|^{k+1}}\right). \tag{1}$$

We now focus on establishing (1) for each fixed m.

For prime r dividing $q^\ell - 1$, let $\mathcal{P}_r$ denote the set of all irreducible polynomials $p \in A(q^\ell)$ satisfying

$$g^{\frac{q^\ell - 1}{r}} \equiv 1 \pmod p.$$

We have the inequality

$$0 \le \chi_{\mathbb{P}} - \chi_{\mathbb{P}_g} \le \sum_{r \mid q^\ell - 1} \chi_{\mathcal{P}_r}$$

for any argument which is not an irreducible polynomial dividing g, and it follows that

$$0 \le S_2^{(m)} - \tilde{S}_2^{(m)} \le \sum_{r \mid q^\ell - 1} \sum_{\substack{n \in A(q^\ell) \\ n \equiv \alpha \pmod W}} \chi_{\mathcal{P}_r}(n + h_m)\omega(n). \tag{2}$$

We will show that this double sum satisfies the asymptotic estimate in (1).

First note that primes r dividing $q - 1$ make no contribution to the sum. Indeed, suppose $r \mid q - 1$ and $p := n + h_m$ is detected by the sum. Then

$$1 \equiv g^{\frac{q^\ell - 1}{r}} \equiv \left(\frac{g}{p}\right)_r = \left(\frac{g}{p}\right)_{q-1}^{\frac{q-1}{r}}.$$

So $(g/p)_{q-1}$ does not generate $\mathbb{F}_q^*$, and this contradicts the choice of the residue class $\alpha \pmod W$.

Upon expanding the weights and reversing the order of summation, the right-hand side of (2) becomes

$$\sum_{\substack{r\mid q^\ell-1\\ r\nmid q-1}}\sum_{\substack{d_1,\ldots,d_k\\ e_1,\ldots,e_k}}\lambda_{d_1\ldots,d_k}\lambda_{e_1\ldots,e_k}\sum_{\substack{n\in A(q^\ell)\\ n\equiv\alpha \pmod W\\ [d_i,e_i]\mid n+h_i\forall i}}\chi_{\mathcal{P}_r}(n+h_m). \tag{3}$$

By definition of the λ terms, the $\{d_i\}$ and $\{e_i\}$ that contribute to the sum are precisely those such that $W,[d_1,e_1],\ldots,[d_k,e_k]$ are pairwise coprime. Thus, the inner sum can be written as a sum over a single residue class modulo $M := W\prod_{i=1}^k[d_i,e_i]$. We will also require that $n+h_m$ is coprime to M (otherwise, it will not contribute to the inner sum), which occurs when $d_m=e_m=1$.

With this in mind, we claim

$$\sum_{\substack{n\in A(q^\ell)\\ n\equiv\alpha \pmod W\\ [d_i,e_i]\mid n+h_i\forall i}}\chi_{\mathcal{P}_r}(n+h_m)=\frac{1}{r\Phi(M)}\frac{q^\ell}{\ell}+O(q^{\ell/2}). \tag{4}$$

Indeed, suppose $p := n+h_m$ is detected by $\chi_{\mathcal{P}_r}$. Then p belongs to a certain residue class modulo M, and g is an rth power modulo p. Write $K=\mathbb{F}_q(t)$. The former condition forces Frob_p to be a certain element of $\mathrm{Gal}(K(\Lambda_M)/K)$, and the latter condition is equivalent to p splitting completely in the field $K(\zeta_r,\sqrt[r]{g})$, where ζ_r is a primitive rth root of unity. Let $L := K(\zeta_r,\Lambda_M,\sqrt[r]{g})$. If $K(\Lambda_M)/K$ and $K(\zeta_r,\sqrt[r]{g})/K$ are linearly disjoint extensions of K, then the above conditions on p amount to placing Frob_p in a uniquely determined conjugacy class $\mathcal{C}$ of size 1 in $\mathrm{Gal}(L/K)$.

To see that $K(\Lambda_M)/K$ and $K(\zeta_r,\sqrt[r]{g})/K$ are linearly disjoint extensions of K, first note that since ℓ is prime, our conditions on r imply that the order of q modulo r is equal to ℓ. In particular, this means $r>\ell$. Then since g is fixed while ℓ (and thus r) can be taken arbitrarily large, we can say that g is not an rth power in K.

The extension $K(\sqrt[r]{g})/K$ is not Galois, since the roots of the minimal polynomial t^r-g of $\sqrt[r]{g}$ are $\{\zeta_r^s\sqrt[r]{g}\}_{s=1}^r$, where ζ_r is a primitive rth root of unity. If all of these roots are elements of K, then K must contain all rth roots of unity, implying that $r\mid q-1$, contradicting the conditions on the sum over values of r above. Thus $K(\sqrt[r]{g})\not\subset K(\Lambda_M)$, as $K(\Lambda_M)$ is an abelian extension of K, and hence any subfield, corresponding to a (normal) subgroup of $\mathrm{Gal}(K(\Lambda_M)/K)$, is Galois. By a theorem of Capelli on irreducible binomials,

$$[K(\sqrt[r]{g},\Lambda_M):K]=[K(\sqrt[r]{g},\Lambda_M):K(\Lambda_M)][K(\Lambda_M):K]=r\Phi(M).$$

So we see that $K(\sqrt[r]{g})$ and $K(\Lambda_M)$ are linearly disjoint extensions of K.

For what follows, we need that $K(\sqrt[r]{g},\Lambda_M)/K$ is a geometric extension of K (i.e., that $\mathbb{F}_q$ is the full constant field of $K(\sqrt[r]{g},\Lambda_M)$). By Corollary 12.3.7 of [Sal07], $K(\Lambda_M)/K$ is a geometric extension of K, so it is enough to show that the extension $K(\sqrt[r]{g},\Lambda_M)/K(\Lambda_M)$ is also geometric. This follows from Proposition 3.6.6 of [Sti09], provided we have that t^r-g is irreducible in $K\bar{\mathbb{F}}_q(\Lambda_M)$. The previous paragraph shows that g is not an rth power in $K(\Lambda_M)$, so Capelli's theorem tells us t^r-g is irreducible in $K(\Lambda_M)$. Now, $K\bar{\mathbb{F}}_q(\Lambda_M)$ is a constant field extension of $K(\Lambda_M)$, the compositum of $K(\Lambda_M)$ and $\mathbb{F}_{q^b}$, say. Thus, $K\bar{\mathbb{F}}_q(\Lambda_M)/K$ is an abelian extension of K, as it is the compositum of two abelian extensions of K. If $t^r - g$ factors in this extension, then once again by Capelli, $K\bar{\mathbb{F}}_q(\Lambda_M)/K$ must contain an rth root of g; but this is impossible, by the argument of the previous paragraph. This establishes the claim.

Let K' denote the constant field extension $K(\zeta_r)$ of K; then according to Proposition 3.6.1 of [Sti09], we have $[K'(\Lambda_M, \sqrt[r]{g}) : K'] = r\Phi(M)$, and hence

$$[L : K] = [L : K'][K' : K] = [K'(\Lambda_M, \sqrt[r]{g}) : K'][K' : K] = r\Phi(M)\ell,$$

using Proposition 10.2 of [Ros02] to determine $[K' : K] = \mathrm{ord}_q(r) = \ell$ (here $\mathrm{ord}_q(r)$ denotes the multiplicative order of q modulo r). Thus $K(\zeta_r, \sqrt[r]{g})$ and $K(\Lambda_M)$ are linearly disjoint Galois extensions of K with compositum L, as desired.

We are nearly in a position to use Theorem 2.3 to estimate the sum in (4). If $\tau \in \mathcal{C}$, the map τ fixes $K(\zeta_r, \sqrt[r]{g})/K$, and in particular restricts to the identity map on $\mathbb{F}_{q^\ell}$, the constant field of $K(\zeta_r, \sqrt[r]{g})$. Now for any $a \in \mathbb{F}_{q^\ell}$, we have

$$\mathrm{Frob}_q^\ell(a) = a^{q^\ell} = a(a^{q^\ell - 1}) = a,$$

and so the restriction condition of Theorem 2.3 is satisfied. The sum in question is therefore equal to

$$\frac{1}{r\Phi(M)}\frac{q^\ell}{\ell} + O\Big(\frac{1}{r\Phi(M)}\frac{q^{\ell/2}}{\ell}\big(r\Phi(M) + g_L\big)\Big). \tag{5}$$

Let g_1 and g_2 denote the genus of $K'(\sqrt[r]{g})/K'$ and $K'(\Lambda_M)/K'$, respectively. By Proposition 2.6,

$$g_L \le \Phi(M)g_1 + rg_2 + (\Phi(M) - 1)(r - 1).$$

Recalling that $K(\sqrt[r]{g})/K$ is a geometric extension, it follows from Proposition 2.4 that $g_1 \ll r$, with the implied constant depending on g. For g_2, we refer to Proposition 2.5, which states that

$$2g_2 - 2 = -2\Phi(M) + \sum_{i=1}^{v} d_i s_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2)\frac{\Phi(M)}{q-1},$$

where $M = \prod_{i=1}^{v} P_i^{\alpha_i}$ (with the P_i distinct irreducible polynomials), $d_i = \deg P_i$, and $s_i = \alpha_i\Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i - 1)}$. At any rate, the middle sum is

$$\le \Phi(M)\sum_{i=1}^{v} d_i\alpha_i = \Phi(M)\sum_{i=1}^{v} \alpha_i \deg(P_i) = \Phi(M)\deg(M).$$

The first and third terms are clearly $O(\Phi(M))$, and thus $g_L \ll r\Phi(M)\log|M|$. Inserting this estimate into (5), we obtain that the number of primes p detected by the sum in (4) is

$$\frac{1}{r\Phi(M)}\frac{q^\ell}{\ell} + O\Big(\frac{1}{r\Phi(M)}\frac{q^{\ell/2}}{\ell}\big(r\Phi(M) + r\Phi(M)\log|M|\big)\Big). \tag{6}$$

Recall that $M = W\prod_{i=1}^{k}[d_i, e_i]$. Owing to the support of the weights λ, we have $|\prod[d_i, e_i]| < R^2$, and hence

$$\begin{aligned}\log|M| = \log\left(|W|\prod_{i=1}^{k}|[d_i, e_i]|\right) &= \log|W| + \log(R^2)\\ &\ll \log|W| + \log(q^{2\theta\ell}) \ll \ell,\end{aligned}$$

recalling that $W = \prod_{|p|<\log\log\log(q^\ell)} p$. Therefore the error term in (6) is $O(q^{\ell/2})$, as claimed.

Inserting the above into (3), we produce an O-term of size

$$\begin{aligned}&\ll q^{\ell/2}\Bigg(\sum_{r|q^\ell-1} 1\Bigg)\Bigg(\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} |\lambda_{d_1\dots,d_k}||\lambda_{e_1\dots,e_k}|\Bigg)\\ &\qquad\ll q^{\ell/2}\log(q^\ell-1)\lambda_{\max}^2\Bigg(\sum_{s\,:\,|s|<R}\tau_k(s)\Bigg)^2\\ &\qquad\ll q^{\ell/2}\cdot\ell\cdot R^2(\log R)^{2k},\end{aligned}$$

and this is $o(q^\ell)$ since $R = q^{\theta\ell}$ where $0 < \theta < 1/4$.

We now focus on the main term:

$$\Bigg(\sum_{\substack{r|q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Bigg)\frac{q^\ell}{\ell\Phi(W)}\sideset{}{'}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}\frac{\lambda_{d_1\dots,d_k}\lambda_{e_1\dots,e_k}}{\prod_{i=1}^{k}\Phi([d_i, e_i])},\tag{7}$$

where the $'$ on the sum means that $[d_1, e_1], \dots, [d_k, e_k]$, and W are all pairwise coprime. Recalling the support of the weights λ, this is equivalent to requiring that $(d_i, e_j) = 1$ for all $1 \le i, j \le k$ with $i \ne j$. We account for this by inserting the quantity $\sum_{s_{i,j}|d_i,e_j}\mu(s_{i,j})$, which is 1 precisely when $(d_i, e_j) = 1$ and is 0 otherwise. Define a completely multiplicative function g such that $g(p) = |p| - 2$ on prime polynomials p; note that

$$\frac{1}{\Phi([d_i, e_i])} = \frac{1}{\Phi(d_i)\Phi(e_i)}\sum_{u_i|d_i,e_i} g(u_i).$$

Therefore, the primed sum above is equal to

$$\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k} g(u_i)\right)\sideset{}{''}\sum_{s_{1,2},\dots,s_{k-1,k}}\Bigg(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\mu(s_{i,j})\Bigg)\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots e_k\\ u_i|d_i,e_i\forall i\\ s_{i,j}|d_i,e_j\forall i\ne j\\ d_m=e_m=1}}\frac{\lambda_{d_1\dots,d_k}\lambda_{e_1\dots,e_k}}{\prod_{i=1}^{k}\Phi(d_i)\Phi(e_i)},\tag{8}$$

where the double-prime indicates that the sum is restricted to those $s_{i,j}$ which contribute to the sum, i.e. those coprime to $u_i, u_j, s_{i,a}$, and $s_{b,j}$ for all $a \ne j$ and $b \ne i$.

Define new variables

$$y^{(m)}_{r_1,\dots,r_k} := \left(\prod_{i=1}^{k}\mu(r_i)g(r_i)\right)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\forall i\\ d_m=1}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}\Phi(d_i)}.$$

Then we can rewrite (8) as

$$\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^{k}g(u_i)\Big)\sideset{}{''}\sum_{s_{1,2},\dots,s_{k-1,k}}\Big(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\mu(s_{i,j})\Big)\times$$
$$\Big(\prod_{i=1}^{k}\frac{\mu(a_i)}{g(a_i)}\Big)\Big(\prod_{j=1}^{k}\frac{\mu(b_j)}{g(b_j)}\Big)y^{(m)}_{a_1,\dots,a_k}y^{(m)}_{b_1,\dots,b_k},$$

where $a_i = u_i\prod_{j\ne i}s_{i,j}$ and $b_j = u_j\prod_{i\ne j}s_{i,j}$. Recombining terms, we see that this is equal to

$$\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^{k}\frac{\mu(u_i)^2}{g(u_i)}\Big)\sideset{}{''}\sum_{s_{1,2},\dots,s_{k-1,k}}\Big(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\frac{\mu(s_{i,j})}{g(s_{i,j})^2}\Big)y^{(m)}_{a_1,\dots,a_k}y^{(m)}_{b_1,\dots,b_k}. \tag{9}$$

Let $y^{(m)}_{\max} := \max_{r_1,\dots,r_k}|y^{(m)}_{r_1,\dots,r_k}|$ and note that $y^{(m)}_{\max} \ll \frac{\Phi(W)}{W}\log R$; this follows from Lemma 2.6 of [CHL+15]. Using again the fact that $r \ge \ell$, we have

$$\sum_{\substack{r|q^\ell-1\\ r\nmid q-1}}\frac{1}{r} \le \frac{1}{\ell}\#\{\text{primes } p : p \mid q^\ell - 1\} = o(1),$$

using the standard result that the number of distinct prime divisors of a natural number n is $\ll \frac{\log n}{\log\log n}$.

Putting everything together, we see that (7) is

$$\ll \Bigg(\sum_{\substack{r|q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Bigg)\frac{q^\ell}{\ell\Phi(W)}\Bigg(\sum_{\substack{u<R\\ (u,W)=1}}\frac{\mu(u)^2}{g(u)}\Bigg)^{k-1}\Bigg(\sum_{s}\frac{\mu(s)^2}{g(s)^2}\Bigg)^{k(k-1)}\big(y^{(m)}_{\max}\big)^2$$
$$\ll \Bigg(\sum_{\substack{r|q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Bigg)\frac{q^\ell}{\ell\Phi(W)}\Big(\frac{\Phi(W)}{|W|}\Big)^{k+1}(\log R)^{k+1}$$
$$= o\Big(q^\ell\frac{\Phi(W)^k}{|W|^{k+1}}(\log q^\ell)^k\Big),$$

as desired.

5. An example: Primitive polynomials over $\mathbb{F}_2$

We conclude by calculating an explicit bound on small gaps between primitive polynomials over $\mathbb{F}_2$. Referring to the remark after Theorem 1.3 in [CHL$^+$15], any admissible 105-tuple $\mathcal{H}$ of polynomials in $\mathbb{F}_2[t]$ admits infinitely many shifts $f + \mathcal{H}$, $f \in \mathbb{F}_2[t]$, containing at least two primes. Let $\mathcal{H}$ be a collection of 105 prime polynomials in $\mathbb{F}_2[t]$ of norm greater than 105 (that is, of degree at least seven); it is easy to see that $\mathcal{H}$ is admissible. By Gauss's formula for the number of irreducible polynomials of a given degree over a finite field, there are 104 irreducible polynomials of degree seven, eight or nine over $\mathbb{F}_2$, so take $\mathcal{H}$ to be a 105-tuple of primes of degree at least seven and at most ten.

To apply our method, we require in general that each element of $\mathcal{H}$ be a multiple of the given primitive root g, and we may modify an admissible tuple $\mathcal{H}$ to obtain an appropriate admissible tuple by replacing each $h \in \mathcal{H}$ by gh. In the present case, with $g = t$ and $\mathcal{H}$ the 105-tuple described above, this operation results in an admissible 105-tuple $\mathcal{H}$ of polynomials of degree at least eight and at most eleven. Thus, with this choice of $\mathcal{H} = \{h_1, h_2, \ldots, h_{105}\}$, one finds that there are infinitely many gaps of norm at most N between primitive polynomials, where

$$N \leq \max_{1 \leq i \neq j \leq 105} |h_i - h_j| \leq 2^{11} = 2048.$$

For other choices of g and q, this construction produces a bound of the form $q^{\deg(g)+10}$.

Acknowledgements

The author thanks Paul Pollack for guidance during the course of this project and for many helpful comments during the editing of this manuscript.

References

[Bil37] H. Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), no. 1, 476–492.

[CHL$^+$15] A. Castillo, C. Hall, R.J. Lemke Oliver, P. Pollack, and L. Thompson, *Bounded gaps between primes in number fields and function fields*, Proc. Amer. Math. Soc. (2015).

[FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden.

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.

[May15] J. Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413.

[Pol14] P. Pollack, *Bounded gaps between primes with a given primitive root*, Algebra Number Theory **8** (2014), no. 7, 1769–1786.

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Sal07] G.D.V. Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser, 2007.

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[Zha14] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174.