A (LIGHT)WEIGHT TWIN PRIME CONJECTURE FOR POLYNOMIALS OVER FINITE FIELDS

PAUL POLLACK

Abstract. We consider the following conjecture for polynomials over a finite field $\mathbf{F}_q$: for each integer $s \geq 0$, there are infinitely many pairs of primes P_1, P_2 over $\mathbf{F}_q$ for which $P_2 - P_1$ has weight s, where s is assumed even in the case $q = 2$. (The *weight* $w(P)$ of a polynomial is the the number of nonzero terms of P.) Define

$$S_q = \{s : w(P_2 - P_1) = s \text{ for infinitely many prime pairs } P_1, P_2 \text{ over } \mathbf{F}_q\}.$$

In the direction of the conjecture, we show that any fixed integer $s \geq 0$ belongs to S_q once $\#\mathbf{F}_q > q_0(s)$. Moreover, we show that S_q has lower density $>$ 1/1200 for every $\mathbf{F}_q$.

1. Introduction

1.1. **Motivation.** In 1849, de Polignac asserted that every even integer could be written as a difference of primes in infinitely many ways ([dP49]). Notwithstanding 150 years of subsequent progress in analytic number theory, this problem remains very much open; the strongest result in this direction is Chen's theorem [Che73], according to which every even number can be written in infinitely many ways as the difference of a prime and a number with at most two prime factors.

One can consider the analogous problem when the ring $\mathbf{Z}$ of integers is replaced by the ring of polynomials over a finite field. To state the analogous conjecture in the most suggestive manner, we call an element of $\mathbf{F}_q[T]$ *even* if it is divisible by all primes of $\mathbf{F}_q[T]$ of norm 2: thus every polynomial over $\mathbf{F}_q[T]$ is even unless $q = 2$, in which case the even polynomials are exactly those divisible by $T(T + 1)$.

Conjecture 1.1 (a de Polignac Conjecture for $\mathbf{F}_q[T]$)**.** *Let D be an arbitrary even polynomial in $\mathbf{F}_q[T]$. Then there are infinitely many prime pairs $P, P + D$.*

This conjecture is alluded do in various degrees of detail by Webb [Web83] and Hsu [Hsu96] (who obtain upper bound results), Cherly [Che78] (who obtains "almost-prime" results by a lower-bound sieve), and by Effinger, Hicks & Mullen [EHM02] (who formulate a quantitative version of the conjecture in some special cases with accompanying computational evidence). (See also the expository paper [EHM05].) Hall proved Conjecture 1.1 in the case when $D = 1$ and $\#\mathbf{F}_q > 3$ (see [Hal06]); this was extended by the present author to all cases where D is constant [Pol]. Unfortunately, these ideas do not appear to shed any light on the nonconstant case; e.g., we still do not know if there are infinitely many prime pairs $P, P + (T^2 + T)$ in $\mathbf{F}_2[T]$.

2000 *Mathematics Subject Classification.* Primary: 11T55, Secondary: 11N32.
The author is supported by an NSF Graduate Research Fellowship.

In light of this, one can consider weakened twin prime conjectures. Instead of asking for prime pairs which differ by a fixed D, one can ask for prime pairs whose difference is small: for example, one might ask whether there are infinitely many pairs of prime polynomials P_1, P_2 over $\mathbf{F}_q$ whose difference has bounded positive degree. Of course if this is the case, then Conjecture 1.1 holds for some fixed nonconstant polynomial D, and even this weak claim seems difficult to establish for a single finite field $\mathbf{F}_q$.

A more workable variant, and one more amenable to the methods of [Hal06] and [Pol], is to ask that $P_2 - P_1$ be small in the sense of having low "weight." Here the *weight* of a polynomial A, denoted $w(A)$ in what follows, is the number of its nonzero coefficients. This leads us to formulate the following assertion:

Conjecture 1.2 (A (Light)weight Twin Prime Conjecture)**.** *Fix a finite field $\mathbf{F}_q$. For each integer $s \geq 0$, there are infinitely many pairs of primes P_1, P_2 over $\mathbf{F}_q$ for which $P_2 - P_1$ has weight s, where s is assumed even in the case $q = 2$.*

This conjecture lives up to its name; if we assume Conjecture 1.1, then Conjecture 1.2 follows immediately: If $\#\mathbf{F}_q > 2$, take $D := 1 + T + \cdots + T^{s-1}$ in Conjecture 1.1, and if $\#\mathbf{F}_q = 2$, take $D := (T^2+T)(1+T^2+\cdots+T^{s-2})$ (recall that we assume s is even in this last case).

1.2. **Results.** We prove two partial results in the direction of Conjecture 1.2. For each finite field $\mathbf{F}_q$, define

$$S_q = \{s : w(P_2 - P_1) = s \text{ for infinitely many prime pairs } P_1, P_2 \text{ over } \mathbf{F}_q\}.$$

Then Conjecture 1.2 asserts that S_q consists of all nonnegative integers in the case $q > 2$ and all nonnegative even integers in the case when $q = 2$.

Theorem 1. *For each fixed integer $s \geq 0$, there is a constant $q_0(s)$ such that $s \in S_q$ whenever $\#\mathbf{F}_q > q_0(s)$.*

Theorem 2. *Fix a finite field $\mathbf{F}_q$. As $x \to \infty$, we have*

$$\liminf_{x\to\infty} \frac{\#S_q \cap [0,x]}{x} > \frac{1}{1200}.$$

Theorem 1 is proved by combining an algebraic result of Serret & Dickson with an elementary method of Hayes ([Hay63b], [Hay63a]). The proof of Theorem 2 is more difficult: the inspiration comes from Prachar's proof [Pra52] that the set of (rational) prime differences $p_2 - p_1$ has positive lower density. However, the proof also requires results on the multiplicative structure of polynomials with a given weight, which we derive from the work of Mauduit and Sárközy [MS97] on the structure of integers with prescribed digit sum.

Notation and Conventions. Throughout we use $\mathbf{F}_q, \mathbf{F}_q[T]$, and $\mathbf{F}_q(T)$ with their usual meanings. We write $\mathbf{F}_q(T)_\infty$ for the completion of $\mathbf{F}_q(T)$ at the prime associated to the $(1/T)$-adic valuation, so that

$$\mathbf{F}_q(T)_\infty = \mathbf{F}_q((1/T)) = \left\{ \sum_{i=-\infty}^{n} a_i T^i : a_i \in \mathbf{F}_q \right\}.$$

We define an absolute value $|\cdot|$ on $\mathbf{F}_q(T)_\infty$ by

$$\left| \sum_{i=-\infty}^{n} a_i T^i \right| = q^n \quad \text{if } a_n \neq 0.$$

We define the *fractional part* of an element of $\mathbf{F}_q(T)_\infty$ by

$$\left\{\sum_{i=-\infty}^{n} a_i T^i\right\} = \sum_{i<0} a_i T^i.$$

We write $e\colon \mathbf{F}_q(T)_\infty \to S^1$ for the map defined by

$$e\left(\sum_{i=-\infty}^{n} a_i T^i\right) = \exp\left(\frac{2\pi i}{p}\mathrm{Tr}(a_{-1})\right).$$

Note that $e(\gamma)$ depends only on the fractional part of γ. We use the same symbol for the function from $\mathbf{R}$ to S^1 with $e(\eta) = \exp(2\pi i\eta)$; no confusion should arise between these two uses.

For polynomials over $\mathbf{F}_q$ we use the terms "irreducible" and "prime" interchangeably; both refer only to monic polynomials unless otherwise stated. The capital roman letter P always stands for a prime polynomial. We use d, ϕ and Ω for the polynomial analogues of the cognate number-theoretic functions: $d(A)$ is the number of monic divisors of A, $\phi(A)$ the number of units modulo A in a complete residue system, and $\Omega(A)$ the number of monic prime divisors of A, counted with multiplicity.

We use $P^+(n)$ to denote the largest prime factor of the integer $n \geq 2$. We write $\#S$ for the size of a finite set S. Finally, we use the notation $\mathbf{P}(E)$ for the probability of an event E.

2. Proof of Theorem 1

The following lemma is due to Serret in the case of prime fields [Ser66, Théorème I, p. 656] and Dickson in the general case ([Dic97, p. 382]; see also [Dic58, §34]).

Lemma 3. *Let f be an irreducible polynomial over $\mathbf{F}_q$ of degree d, and fix a root α of f from $\mathbf{F}_{q^d}$. Suppose l is an odd prime for which α is not an lth power in $\mathbf{F}_{q^d}$. Then the substitution $T \mapsto T^{l^k}$ leaves f irreducible for every $k = 1, 2, 3, \dots$.*

In particular, suppose that P_1 and P_2 are two irreducibles of $\mathbf{F}_q[T]$ for which the hypotheses of Lemma 3 are satisfied for the same prime l. Since

$$w(P_1(T) - P_2(T)) = w(P_1(T^l) - P_2(T^l)) = w(P_1(T^{l^2}) - P_2(T^{l^2})) = \dots,$$

we find that $w(P_1(T) - P_2(T)) \in S_q$. So to prove Theorem 1, it suffices to show that for each fixed $s \geq 0$, we can find such a a pair of irreducibles whose difference has weight s once q is large enough (depending on s).

This follows immediately from the following lemma, which is perhaps of independent interest:

Lemma 4. *Fix an integer $d \geq 2$, and let D be a polynomial of degree $d-1$ over $\mathbf{F}_q$. Then as $\#\mathbf{F}_q \to \infty$,*

$$\#\{(P_1, P_2) : P_1, P_2 \text{ degree } d \text{ primes}, P_1 - P_2 = cD \text{ for some } c \in \mathbf{F}_q^*\} \geq (1 + o(1))\frac{q^{d+1}}{d^2},$$

uniformly in D. The same is true even with P_1 and P_2 restricted to irreducible polynomials which satisfy the hypotheses of Lemma 3 with $l = P^+(q^d - 1)$.

Remark. This should be compared to a theorem of Hayes ([Hay63b], [Hay63a]). Hayes shows that every polynomial of degree $d-1$ can be represented the difference of two (not necessarily monic) irreducibles of degree d provided q is large enough compared to d, and he establishes an asymptotic formula for the number of such representations under certain additional constraints.

The proof of Lemma 4 requires a few preliminary results. The first of these is a result of Siegel [Sie21]:

Lemma 5. *Let $f(T)$ be a nonzero polynomial over $\mathbf{Z}[T]$ with at least two distinct roots. Then $P^+(f(n)) \to \infty$ as $n \to \infty$.*

Lemma 6. *Fix a finite field $\mathbf{F}_q$. Let d be a positive integer, and let l be the largest prime factor of $q^d - 1$. The number of irreducible polynomials of degree d over $\mathbf{F}_q$ which fail to satisfy the hypothesis of Lemma 3 for the prime l is bounded by*

$$\frac{1}{l}\frac{q^d}{d}. \tag{1}$$

Moreover, $l \to \infty$ in either of the following two situations:

(i) *$\mathbf{F}_q$ is fixed and $d \to \infty$,*
(ii) *$d \geq 2$ is fixed and $\#\mathbf{F}_q \to \infty$.*

Proof. The number of nonzero lth powers in $\mathbf{F}_{q^d}$ is $(q^d-1)/l$. Each irreducible polynomial of degree d over $\mathbf{F}_q$ violating the hypothesis of Lemma 3 has d distinct roots which are nonzero lth powers. Since distinct irreducible polynomials have distinct roots, the number of such polynomials is at most q^d/dl, which is (1).

Suppose first that q is fixed and $d \to \infty$. By Lemma 5, the largest prime factor of $n(n+1)$ tends to infinity with N; setting $n = q^d - 1$ then gives the result.

Contrariwise, if d is fixed and $\#\mathbf{F}_q \to \infty$, then the result follows immediately upon applying Lemma 5 to the polynomial $T^d - 1$, which has d distinct roots. □

Proof of Lemma 4. It suffices to prove the final claim. Let D be a polynomial of degree $d-1$. If P_1 and P_2 are two irreducibles of degree d, then $P_1 - P_2$ is an $\mathbf{F}_q$-multiple of D precisely when $P_1 \equiv P_2 \pmod{D}$. For each congruence class $A \bmod D$, let N_A denote the number of primes P satisfying the hypothesis of Lemma 3 with l the largest prime factor of $q^d - 1$. Then as $q \to \infty$, Lemma 6 (in the case of fixed d) together with the classical formula for the number of irreducibles of a given degree shows that

$$\sum_{A \bmod D} N_A \geq (1+o(1))q^d/d,$$

$$\text{so by Cauchy-Schwarz,} \qquad \sum_{A \bmod D} N_A^2 \geq (1+o(1))q^{d+1}/d^2.$$

This latter sum counts the number of pairs P_1, P_2 with $P_1 \equiv P_2 \pmod{D}$. To complete the proof, we have to eliminate the trivial pairs with $P_1 = P_2$; but there are just $(1+o(1))q^d/d = o(q^{d+1}/d^2)$ of these. □

3. Proof of Theorem 2

3.1. **Outline.** For the rest of this article we assume $\mathbf{F}_q$ is fixed; in particular, implied constants may always depend on q.

As in the proof of Theorem 1, we produce elements of S_q by taking the weight of the difference of two irreducible polynomials which satisfy the hypotheses of Lemma 3 for the same prime l. By (i) of Lemma 6, one knows that as d tends to infinity, there are $(1+o(1))q^d/d$ such irreducibles of degree d for the prime $l = P^+(q^d-1)$. Call a degree d prime of this type a *good prime*.

Now suppose d is a large positive integer. For each k, define

$$N_k = \{(P_1, P_2) : P_1, P_2 \text{ good primes of degree } d, w(P_1 - P_2) = k\}.$$

Then

$$k \in S_q \quad \text{whenever} \quad N_k \neq 0.$$

Moreover,

$$\sum_{k=1}^{d} N_k \geq (1+o(1))q^{2d}/d^2 \qquad (\text{as } d \to \infty). \tag{2}$$

Define W_k to be the number of polynomials of degree $< d$ of weight k, so that

$$W_k = \binom{d}{k}(q-1)^k.$$

The W_k form a unimodal sequence which attains a maximum at $k = \lfloor (1-1/q)d \rfloor$, where Stirling's formula shows $W_k \asymp q^d/\sqrt{d}$. We might therefore expect that the bulk of the contribution to (2) should come from those indices i close to $(1-1/q)d$.

To quantify this, we model the weight distribution of a random polynomial of degree $< d$ over $\mathbf{F}_q$ as the sum of d independent random variables $X_1, \ldots, X_d$, each binomially distributed with parameter $1/q$. Note that $W = X_1 + \cdots + X_d$ is a random variable with expectation $(1-1/q)d$ and variance

$$\sigma^2 := d(1/q)(1-1/q).$$

We now prove that the contribution from those k with $|k - d(q-1)/q| > \sigma\sqrt{3 \log\log d}$ is negligible.

This requires two tools; the first is Bernstein's inequality (see, e.g., [Rén70, Chapter VII]):

Lemma 7 (Bernstein's Inequality)**.** *Let X be a bounded random variable with vanishing expectation and $|X| \leq M$. Let $X_1, X_2, X_3, \ldots$ be independent copies of X, and let $\sigma^2 = n\mathrm{Var}(X)^2$ be the variance of $\sum_{i=1}^n X_i$. Then*

$$\mathbf{P}\left(\left|\sum_{i=1}^{n} X_i\right| \geq t\sigma\right) < \exp\left(-\frac{t^2}{2 + \frac{2}{3}\frac{M}{\sigma}t}\right).$$

The second result we need is an upper bound on twin prime pairs, whose proof we defer to §3.2.

Lemma 8. *Fix a finite field $\mathbf{F}_q$. Let $d \geq 2$ be an integer, and let $D \neq 0$ be a polynomial of degree $< d$ over $\mathbf{F}_q$. Then*

$$\#\{(P, P+D) : P, P+D \text{ are both irreducible of degree } d\} \leq 16\frac{q^d}{d^2}\prod_{P|D}\left(1 + \frac{1}{|P|}\right).$$

Remark. For D of degree d, the product appearing in the upper estimate is small, specifically

$$\prod_{\substack{P\mid D\\ P\text{ prime}}}\left(1+\frac{1}{|P|}\right)\ll \log d. \tag{3}$$

To see this, choose $r\geq 1$ minimal with $q^r\geq d$. The product of all primes of degree $\leq r$ has degree at least $q^r\geq d$, since $T^{q^r}-T$ is the product of the primes of degree dividing r. It follows that the product appearing above is bounded above by the analogous product taken over the primes of degree $\leq r$. Since the number of irreducibles of degree i is bounded above by q^i/i, we obtain an upper estimate of

$$\prod_{i=1}^{r}\left(1+\frac{1}{q^i}\right)^{q^i/i}\leq \prod_{i=1}^{r} e^{1/i}\leq e^{\log r+1}\ll r.$$

Since $r\leq 1+\frac{\log d}{\log q}$, (3) follows.

By Lemmas 7 and 8, for large d and each $1\leq k\leq d$ we have

$$\sum_{\substack{\deg A<d\\ w(A)=k}}\prod_{P\mid A}\left(1+\frac{1}{|P|}\right)\ll \frac{q^d\log d}{d^2}W_k,$$

so that

$$\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|>\sigma\sqrt{3\log\log d}}} N_k\leq \frac{q^d\log d}{d^2}\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|>\sigma\sqrt{3\log\log d}}} W_k$$
$$\leq \frac{q^{2d}\log d}{d^2}\mathbf{P}\left(\left|\sum_{i=1}^{d}X_i-\frac{q-1}{q}d\right|>\sigma\sqrt{3\log\log d}\right).$$

By Bernstein's inequality, the probability appearing on the right hand side is bounded by $\exp(-(3/2+o(1))\log\log d)$, and we conclude that

$$\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|\geq\sigma\sqrt{3\log\log d}}} N_k\leq \frac{q^{2d}}{d^2\log^{3/2+o(1)}d}.$$

In particular, if we throw out such k, we are left with the estimate

$$\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|\leq\sigma\sqrt{3\log\log d}}} N_k\geq (1+o(1))\frac{q^{2d}}{d^2} \tag{4}$$

as $d\to\infty$. To proceed further, we need a finer upper bound on N_k than used before: this requires us to study the average value of $\prod_{P\mid D}(1+1/|P|)$ along polynomials D of weight k. We state the key result of these investigations here, deferring the proof to §3.3.

Lemma 9. *For large enough d, we have*

$$\sum_{\substack{\deg A<d\\ w(A)=k}}\prod_{P\mid A}\left(1+\frac{1}{|P|}\right)\leq 5W_k$$

uniformly for $|k - d(q-1)/q| \leq \sigma\sqrt{3\log\log d}$. *Hence for such* k, *Lemma 8 shows*

$$N_k \leq 80\frac{q^d}{d^2}W_k. \tag{5}$$

With this result in hand the proof of Theorem 2 is easily completed. Let C be a large positive constant to be chosen momentarily. By Lemma 9,

$$\sum_{\substack{1\leq i\leq d\\ C\sigma\leq|k-d(q-1)/q|\leq\sigma\sqrt{3\log\log d}}} N_k \leq 80\frac{q^d}{d^2}\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|\geq C\sigma}} W_k. \tag{6}$$

By the central limit theorem, the right hand side is asymptotically

$$\frac{160}{\sqrt{2\pi}}\frac{q^{2d}}{d^2}\int_C^\infty e^{-x^2/2}\,dx,$$

and this is smaller than $\frac{1}{2}q^{2d}/d^2$ if we choose $C = 3$. With this choice of C, (4) implies that

$$\sum_{\substack{1\leq k\leq d\\ |k-d(q-1)/q|\leq C\sigma}} N_k \geq \left(\frac{1}{2}+o(1)\right)\frac{q^{2d}}{d^2}. \tag{7}$$

But by Lemma 9 and Stirling's formula,

$$\max_{|k-d(q-1)/q|\leq C\sigma} N_k \leq 80\frac{q^d}{d^2}\max W_k \leq 80(1+o(1))\frac{q^d}{d^2}\frac{1}{\sqrt{2\pi}}\frac{q^d}{\sigma},$$

and so the sum (7) must contain

$$\geq (1+o(1))\frac{\frac{1}{2}q^{2d}/d^2}{(80/\sigma\sqrt{2\pi})q^{2d}/d^2} = (1+o(1))\frac{1}{160}\sigma\sqrt{2\pi}$$

nonzero terms. That is, for large d,

$$\#S_q\cap[d(q-1)/q-3\sigma, d(q-1)/q+3\sigma] \geq (1+o(1))\frac{1}{160}\sqrt{2\pi}\sqrt{(1/q)(1-1/q)}\sqrt{d}.$$

But we can fit

$$\geq (1+o(1))\frac{x/2}{6\sqrt{x}\sqrt{(1/q)(1-1/q)}} \geq (1+o(1))\frac{1}{12}\frac{1}{\sqrt{(1/q)(1-1/q)}}\sqrt{x}$$

disjoint intervals of this kind into $[x/2, x]$. It follows that

$$\begin{aligned}&\#S_q\cap[x/2,x]\\ &\quad\geq (1+o(1))\left(\frac{1}{12}\frac{1}{\sqrt{(1/q)(1-1/q)}}\sqrt{x}\right)\left(\frac{1}{160}\sqrt{2\pi}\sqrt{(1/q)(1-1/q)}\sqrt{x/2}\right)\\ &\qquad\qquad\geq \frac{1+o(1)}{1920}\sqrt{\pi}x,\end{aligned}$$

which implies Theorem 2 since $\sqrt{\pi} > 1920/1200$.

3.2. **An Upper Bound for Twin Prime Pairs in $\mathbf{F}_q[T]$.** We prove Lemma 8 using a polynomial analogue of Selberg's sieve given by Webb [Web83, Theorem 1]. The particular result of his we require is the following:

Lemma 10 (Selberg's Λ^2-sieve for $\mathbf{F}_q[T]$)**.** *Let $\mathcal{A}$ be a multiset of polynomials over $\mathbf{F}_q$, and let $\mathcal{P}$ be a finite set of $\mathbf{F}_q[T]$ primes. Suppose that f is a multiplicative function defined on the squarefree divisors of $\prod_{P\in\mathcal{P}} P$ with $1 < f(P) \leq |P| = q^{\deg P}$ for each $P \in \mathcal{P}$, and write*

$$\sum_{\substack{a\in\mathcal{A}\\ D\mid A}} 1 = \frac{\#\mathcal{A}}{f(D)} + R_D. \tag{8}$$

Let $\mathcal{D}$ be any divisor closed set consisting of monic divisors of $\prod_{P\in\mathcal{P}} P$. Then

$$\sum_{\substack{A\in\mathcal{A}\\ \gcd(A,\prod_{P\in\mathcal{P}} P)=1}} 1 \leq \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1}\prod_{P\mid D}\left(1-\frac{1}{f(P)}\right)^{-1}} + \sum_{D_1,D_2\in\mathcal{D}} |X_{D_1}X_{D_2}R_{[D_1,D_2]}|,$$

where

$$X_D = \mu(D)f(D)\frac{\sum_{C\in\mathcal{D},D\mid C} f(C)^{-1}\prod_{P\mid C}\left(1-\frac{1}{f(P)}\right)^{-1}}{\sum_{C\in\mathcal{D}} f(C)^{-1}\prod_{P\mid C}\left(1-\frac{1}{f(P)}\right)^{-1}}.$$

Proof of Lemma 8. We may assume that $d > 4$ since our bound is trivial otherwise. We may also assume that D is even (i.e., divisible by $T(T+1)$ in the case $q = 2$), since otherwise there are no prime pairs of this kind. We define the multiset

$$\mathcal{A} := \{A(A+D) : A \text{ monic}, \deg A = d\}.$$

Let $\mathcal{P}$ be the set of primes of degree $< d/2$ not dividing D. Then the number of prime pairs of the desired type is bounded by the number of elements of $\mathcal{A}$ coprime to $\prod_{P\in\mathcal{P}} P$, and this motivates an application of Lemma 10.

We take $\mathcal{D}$ to be the (divisor-closed) set of squarefree, monic polynomials of degree $< d/2$ supported on $\mathcal{P}$. We define the multiplicative function f appearing in Lemma 10 by setting $f(P) = |P|/2$ for $P \in \mathcal{P}$ and extending by multiplicativity. It is easy to check that if the squarefree polynomial D has degree $< d$ and is supported on $\mathcal{P}$, then (8) holds without any error term, i.e., with $R_D = 0$. Since the least common multiple of any pair $D_1, D_2 \in \mathcal{D}$ has degree $< d$, we obtain from Lemma 10 the following clean inequality:

$$\sum_{\substack{A\in\mathcal{A}\\ \gcd(A,\prod_{P\in\mathcal{P}} P)=1}} 1 \leq \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1}\prod_{P\mid D}\left(1-\frac{1}{f(P)}\right)^{-1}}. \tag{9}$$

To proceed we need a lower bound on the denominator in this expression. For each $D \in \mathcal{D}$, we have

$$f(D)^{-1}\prod_{P\mid D}\left(1-\frac{1}{f(P)}\right)^{-1} = \prod_{P\mid D}\frac{2}{|P|-2},$$

and so we have reduced the problem to obtaining a lower bound on

$$\sum_{D\in\mathcal{D}}\prod_{P|D}\frac{2}{|P|-2}=\sum_{D\in\mathcal{D}}\prod_{P|D}\left(\frac{2}{|P|}+\frac{4}{|P|^2}+\frac{8}{|P|^3}+\dots\right)$$
$$=\sum_{\substack{M\,\text{monic,}\\ \text{supported on }\mathcal{P}}}\frac{2^{\Omega(M)}}{|M|}\sum_{\substack{D\in\mathcal{D}\\ \operatorname{rad}(M)=D}}1.$$

The inner sum is positive whenever $\deg M<d/2$, and so we have a lower bound of

$$\sum_{\substack{M\ \text{monic,}\deg M<d/2\\ \gcd(M,D)=1}}\frac{2^{\Omega(M)}}{|M|}\geq\sum_{\substack{M\ \text{monic,}\deg M<d/2\\ \gcd(M,D)=1}}\frac{d(M)}{|M|}.$$

Now

$$\sum_{\substack{M\ \text{monic,}\deg M<d/2\\ \gcd(M,D)=1}}\frac{d(M)}{|M|}\prod_{P|D}\left(1+\frac{d(P)}{|P|}+\frac{d(P^2)}{|P|^3}+\dots\right)\geq\sum_{M\ \text{monic,}\deg M<d/2}\frac{d(M)}{|M|}.$$

Since

$$1+\frac{d(P)}{|P|}+\frac{d(P^2)}{|P|^3}+\dots=1+\frac{2}{|P|}+\frac{3}{|P|^2}+\dots=\frac{1}{(1-1/|P|)^2},$$

we find that

$$\sum_{\substack{M\ \text{monic,}\deg M<d/2\\ \gcd(M,D)=1}}\frac{d(M)}{|M|}\geq\left(\prod_{P|D}\left(1-\frac{1}{|P|}\right)^2\right)\sum_{M\ \text{monic,}\deg M<d/2}\frac{d(M)}{|M|}.$$

Carlitz has shown that $\sum_{\deg M=k}d(M)=(k+1)q^k$ ([Car31]; see also [Ros02, Proposition 2.5]), and this gives a lower bound of

$$\left(\prod_{P|D}\left(1-\frac{1}{|P|}\right)^2\right)\sum_{k<d/2}(k+1)\geq\frac{d^2}{8}\left(\prod_{P|D}\left(1-\frac{1}{|P|}\right)^2\right).$$

But

$$\#\mathcal{A}=\#\{A\text{ degree }d,\gcd(A,D)=1\}=q^d\frac{\phi(D)}{|D|}=q^d\prod_{P|D}\left(1-\frac{1}{|P|}\right),$$

and so (9) gives an upper bound for the number of $A\in\mathcal{A}$ prime to $\prod_{P\in\mathcal{P}}P$ of

$$\leq 8\frac{q^d}{d^2}\prod_{P|D}\left(1-\frac{1}{|P|}\right)^{-1}=\frac{q^d}{d^2}\prod_{P|D}\left(1+\frac{1}{|P|}\right)\prod_{P|D}\left(1-\frac{1}{|P|^2}\right)^{-1}.$$

Finally,

$$\prod_{P|D}\left(1-\frac{1}{|P|^2}\right)^{-1}\leq\sum_{A\ \text{monic}}\frac{1}{|A|^2}\leq\sum_{k=0}^{\infty}q^k\frac{1}{q^{2k}}\leq 2,$$

and the result follows. □

3.3. **Proof of Lemma 9.** Lemma 9 will be proved as a corollary of the following result, whose proof is based on a method of Mauduit & Sárközy [MS97, Theorem 2] (see also [MPS05, Theorem 2′]).

Lemma 11. *Let d be large, and suppose $1 \leq k \leq d$. Let M be a polynomial over $\mathbf{F}_q$ prime to T and satisfying $|M| \leq d^{3/4}$; moreover, suppose M is also prime to $T+1$ in the case $q=2$. Write*

$$\#\{A : A \text{ monic with } \deg A < d, w(A) = k, M \mid A\} = \frac{W_k}{|M|} + R(d, M).$$

Then

$$R(d, M) \leq q^d \exp(-cd^{1/4}),$$

where $c > 0$ is a constant depending only on q.

Proof. For z a complex number and $\gamma \in \mathbf{F}_q(T)_\infty$, define

$$G(z, \gamma) := \sum_{\deg A < d} z^{w(A)} e(A\gamma).$$

Then

$$\frac{1}{|M|} \sum_{B \bmod M} G\left(z, \frac{B}{M}\right) = \frac{1}{|M|} \sum_{B \bmod M} \sum_{\deg A < d} z^{w(A)} e\left(\frac{AB}{M}\right) = \sum_{\substack{\deg A < d \\ M \mid A}} z^{w(A)}.$$

As a consequence,

$$\begin{aligned} \#\{A : \deg A < d, M \mid A, w(A) = k\} &= \int_0^1 e(-k\beta) \sum_{\substack{\deg A < d \\ M \mid A}} e(\beta)^{w(A)}\, d\beta \\ &= \frac{1}{|M|} \sum_{B \bmod M} \int_0^1 e(-k\beta) G\left(e(\beta), \frac{B}{M}\right) d\beta. \end{aligned}$$

The contribution from the zero residue class mod M is

$$\begin{aligned} &\frac{1}{|M|} \int_0^1 e(-k\beta) G(e(\beta), 0)\, d\beta \\ &\qquad = \frac{1}{|M|} \int_0^1 e(-k\beta) \sum_{\deg A < d} e(\beta)^{w(A)}\, d\beta = \frac{1}{|M|} \sum_{\substack{\deg A < d \\ w(A) = k}} 1 = \frac{W_k}{|M|}. \end{aligned}$$

Hence

$$|R(d, M)| \leq \frac{1}{|M|} \sum_{\substack{B \bmod M \\ B \not\equiv 0 \pmod M}} \int_0^1 \left| G\left(e(\beta), \frac{B}{M}\right) \right| d\beta.$$

To proceed further, we note that

$$\begin{aligned}
G\left(e(\beta), \frac{B}{M}\right) &= \sum_{\deg A<d} e(\beta)^{w(A)} e\left(A\frac{B}{M}\right) \\
&= \sum_{a_0,\dots,a_{d-1}\in\mathbf{F}_q} \prod_{i=0}^{d-1} e(\beta)^{w(a_iT^i)} e\left(a_iT^i\frac{B}{M}\right) \\
&= \prod_{i=0}^{d-1}\left(1+e(\beta)\sum_{a\in\mathbf{F}_q^\times} e\left(aT^i\frac{B}{M}\right)\right).
\end{aligned}$$

Write

$$\left\{\frac{B}{M}\right\} = c_1T^{-1}+c_2T^{-2}+c_3T^{-3}+\dots.$$

Then for each $i \geq 0$,

$$\begin{aligned}
1+e(\beta)\sum_{a\in\mathbf{F}_q^\times} e\left(aT^i\frac{B}{M}\right) &= 1-e(\beta)+e(\beta)\sum_{a\in\mathbf{F}_q} e\left(aT^i\frac{B}{M}\right) \\
&= 1-e(\beta)+e(\beta)\sum_{a\in\mathbf{F}_q}\exp\left(2\pi i\frac{\mathrm{Tr}(ac_{i+1})}{p}\right).
\end{aligned}$$

The sum here takes the value q when $c_{i+1}=0$ and vanishes otherwise. To see this last claim, note that the sum is invariant under multiplication by every complex number of the form $\exp(2\pi i\mathrm{Tr}(a'c_{i+1})/p)$, with $a'\in\mathbf{F}_q$. But if $c_{i+1}\neq 0$, we can choose a' so $\mathrm{Tr}(a'c_{i+1})=1$ (by the surjectivity of the trace), so that $\exp(2\pi i\mathrm{Tr}(a'c_{i+1})/p)\neq 1$.

Consequently,

$$\left|G\left(e(\beta), \frac{B}{M}\right)\right| \leq |1+(q-1)e(\beta)|^{d-v}\,|1-e(\beta)|^{v}, \tag{10}$$

where v is the number of nonvanishing coefficients $c_1,c_2,\dots,c_d$. Since B/M does not belong to $\mathbf{F}_q[T]$, the sequence $\{c_i\}$ must contain nonzero terms; moreover, if e denotes the order of T modulo M, then the sequence of c_i is periodic with period e. Since $e\leq\phi(M)\leq|M|\leq d^{3/4}$ by hypothesis, for large d we must have

$$v \geq \frac{1}{2}d^{1/4}, \tag{11}$$

say. To complete the proof, we take two cases, according as whether $q>2$ or not. In the former case, we observe that (10) implies

$$\begin{aligned}
\left|G\left(e(\beta), \frac{B}{M}\right)\right| &\leq q^{d-v}2^v = q^d\left(\frac{2}{q}\right)^v \\
&\leq q^d\exp\left(v\log\frac{2}{q}\right) \leq q^d\exp\left(\left(\frac{1}{2}\log\frac{2}{q}\right)d^{1/4}\right).
\end{aligned}$$

Since this holds uniformly in B and β, (10) gives the lemma in this case (with $c=\frac{1}{2}\log(q/2)$).

Suppose now that $q=2$, and define v' to the number of vanishing coefficients among $c_1,\dots,c_D$, so that $v+v'=D$. If the sequence $\{c_i\}$ contains no vanishing coefficients, then

$$\left\{\frac{B}{M}\right\} = \frac{1}{T} + \frac{1}{T^2} + \frac{1}{T^3} + \cdots = \frac{1}{1+T},$$

contradicting that M is prime to $1+T$. As before, the periodicity of the c_i now implies that

$$v' \geq \frac{1}{2} d^{1/4} \tag{12}$$

for d sufficiently large. By (10),

$$\left| G\left(e(\beta), \frac{B}{M}\right) \right| \leq |1+e(\beta)|^{v'} |1-e(\beta)|^{v}.$$

Suppose now that $v' \geq v$. Then

$$\begin{aligned} |1+e(\beta)|^{v'}|1-e(\beta)|^{v} &= |1+e(\beta)|^{v'-v}|1+e(\beta)|^{v}|1-e(\beta)|^{v} \\ &= |1+e(\beta)|^{v'-v}|1-e(2\beta)|^{v} \leq 2^{v'-v}2^{v} \leq 2^{v'} = 2^{d-v}; \end{aligned}$$

since $v \geq \frac{1}{2}d^{1/4}$, the lemma follows with $c = \frac{1}{2}\log 2$. The case when $v \geq v'$ is similar, using (12) in place of (11). $\square$

Proof of Lemma 9. We have

$$\begin{aligned} \sum_{\substack{\deg A < d \\ w(A)=k}} \prod_{P \mid A} \left(1 + \frac{1}{|P|}\right) &\leq \frac{9}{4} \sum_{\substack{\deg A < d \\ w(A)=k}} \prod_{\substack{P \mid A \\ (P, T(T+1))=1}} \left(1 + \frac{1}{|P|}\right) \\ &= \frac{9}{4} \sideset{}{'}\sum_{M} \frac{1}{|M|} \sum_{\substack{\deg A < d \\ w(A)=k \\ M \mid A}} 1, \end{aligned}$$

where the $'$ indicates that the sum is restricted to squarefree monic polynomials M of degree $< d$, not divisible by either T or $T+1$. We break up the latter sum according as $|M| \geq d^{3/4}$ or not; the former values of M contribute at most

$$\ll \sideset{}{'}\sum_{q^d > |M| \geq d^{3/4}} \frac{1}{|M|} \sum_{\substack{\deg A < d \\ M \mid A}} 1 \ll q^d \sideset{}{'}\sum_{q^d > |M| \geq d^{3/4}} \frac{1}{|M|^2} \ll q^d \sum_{|M| \geq d^{3/4}} \frac{1}{|M|^2} \ll q^d / d^{3/4},$$

which is $o(W_k)$. Indeed, Stirling's formula yields that for $|k - d(q-1)/q| \leq \sigma\sqrt{3 \log\log d}$, we have

$$W_k = \frac{q^d}{\sqrt{d}} \exp(O(\log\log d)). \tag{13}$$

For the latter values of M, we write

$$\begin{aligned} \sideset{}{'}\sum_{|M| < d^{3/4}} \frac{1}{|M|} \sum_{\substack{\deg A < d \\ w(A)=k}} 1 &= \sideset{}{'}\sum_{|M| < d^{3/4}} \frac{1}{|M|} \left(\frac{W_k}{|M|} + R(d, M) \right) \\ &= W_k \sideset{}{'}\sum_{|M| < d^{3/4}} \frac{1}{|M|^2} + \sideset{}{'}\sum_{|M| < d^{3/4}} \frac{|R(d,M)|}{|M|}. \end{aligned}$$

The first term here is bounded by $2W_k$, and to complete the proof of the lemma (with a stronger bound of $(9/2+o(1))W_k$) it suffices to show that the second term is $o(W_k)$. By Lemma 11,

$$\begin{aligned}\sideset{}{'}\sum_{|M|<d^{3/4}} \frac{|R(d,M)|}{|M|} &\leq q^d \exp(-cd^{1/4}) \sum_{\substack{M \text{ monic} \\ |M|<d^{3/4}}} \frac{1}{|M|} \\ &\ll q^d \exp(-cd^{1/4}) \log d \ll q^d \exp\left(-\frac{c}{2} d^{1/4}\right),\end{aligned}$$

and this is certainly $o(W_k)$ by (13). □

References

[Car31] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Proc. Nat. Acad. Sci. U. S. A. **17** (1931), 120–122.

[Che73] J. R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176. MR 55 #7959

[Che78] J. Cherly, *A lower bound theorem in $F_q[x]$*, J. Reine Angew. Math. **303/304** (1978), 253–264. MR 80e:12022

[Dic97] L. E. Dickson, *Higher irreducible congruences*, Bull. Amer. Math. Soc. **3** (1897), 381–389.

[Dic58] ———, *Linear groups: with an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958. MR 21 #3488

[dP49] A. de Polignac, *Six propositions arithmologiques déduites du crible d'Ératosthène*, Nouv. Ann. Math. **8** (1849), 423–429.

[EHM02] G. Effinger, K. Hicks, and G. L. Mullen, *Twin irreducible polynomials over finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111. MR MR1995330 (2004h:11104)

[EHM05] ———, *Integers and polynomials: comparing the close cousins* $\mathbf{Z}$ *and* $\mathbf{F}_q[x]$, Math. Intelligencer **27** (2005), no. 2, 26–34. MR MR2156532

[Hal06] C. Hall, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128–147. MR MR2228953

[Hay63a] D. R. Hayes, *Correction to "A polynomial analog of the Goldbach conjecture"*, Bull. Amer. Math. Soc. **69** (1963), 493. MR 27 #135

[Hay63b] ———, *A polynomial analog of the Goldbach conjecture*, Bull. Amer. Math. Soc. **69** (1963), 115–116. MR 26 #109

[Hsu96] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory **58** (1996), no. 2, 267–287. MR MR1393616 (97e:11147)

[MPS05] C. Mauduit, C. Pomerance, and A. Sárközy, *On the distribution in residue classes of integers with a fixed sum of digits*, Ramanujan J. **9** (2005), no. 1-2, 45–62. MR MR2166377 (2006g:11198)

[MS97] C. Mauduit and A. Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. **81** (1997), no. 2, 145–173. MR MR1456239 (99a:11096)

[Pol] P. Pollack, *Irreducibility preserving substitutions for polynomials over a finite field*, in preparation.

[Pra52] K. Prachar, *Über Primzahldifferenzen*, Monatsh. Math. **56** (1952), 304–306. MR MR0053150 (14,727c)

[Rén70] A. Rényi, *Probability theory*, North-Holland Publishing Co., Amsterdam, 1970, Translated by László Vekerdi, North-Holland Series in Applied Mathematics and Mechanics, Vol. 10. MR MR0315747 (47 #4296)

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1 876 657

[Ser66] J.-A. Serret, *Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible*, Mémoires de l'Académie des sciences de l'Institut Impérial de France **35** (1866), 617–688.

[Sie21] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), no. 3-4, 173–213. MR MR1544471

[Web83] W. A. Webb, *Sieve methods for polynomial rings over finite fields*, J. Number Theory **16** (1983), no. 3, 343–355. MR 84j:12021

Department of Mathematics, Dartmouth College, Hanover, NH 03755
E-mail address: paul.pollack@dartmouth.edu