On primitive elements in finite fields of low characteristic

Abhishek Bhowmick[*] Thái Hoàng Lê[†]

September 16, 2014

Abstract

We discuss the problem of constructing a small subset of a finite field containing primitive elements of the field. Given a finite field, $\mathbb{F}_{q^n}$, small q and large n, we show that the set of all low degree polynomials contains the expected number of primitive elements.

The main theorem we prove is a bound for character sums over short intervals in function fields. Our result is unconditional and slightly better than what is known (conditionally under GRH) in the integer case and might be of independent interest.

1 Introduction

1.1 Character sum estimates

Let $q > 1$ and χ be a non-principal character modulo q. It is desirable to have an estimate of the form

$$\sum_{1 \leq n \leq x} \chi(n) = o(x)$$

for x as small as possible (depending on q). Such an estimate would have immediate applications in finding the first non-quadratic residue modulo q, or the smallest primitive root modulo q (if, say, q is an odd prime power).

In [MV77], Montgomery and Vaughan had the idea of comparing the above character sum to the corresponding sum over *smooth numbers.* Given $x, y > 0$, a positive integer n is called y-smooth if none of its prime divisors are greater than y. Let $\mathcal{S}(x, y)$ be the set of all integers $1 \leq n \leq x$ that is y-smooth. For a function f, put $\Psi(x, y; f) = \sum_{n \in \mathcal{S}(x,y)} f(n)$. We also put $\Psi(x, y) = \Psi(x, y; 1) = |\mathcal{S}(x, y)|$.

Montgomery and Vaughan [MV77] proved the following estimate under the Generalized Riemann Hypothesis (GRH):

Theorem 1 ([MV77, Lemma 2])**.** *Let χ be a non-principal character modulo q. Then for all*

[*] Corresponding author. Email: bhowmick@cs.utexas.edu. Department of Computer Science, The University of Texas at Austin. Research supported in part by NSF Grants CCF-0916160 and CCF-1218723.

[†] Email: leth@math.utexas.edu. Department of Mathematics, The University of Texas at Austin.

$(\log q)^4 \le y \le x \le q$, *we have*

$$\sum_{1\le n\le x} \chi(n) = \sum_{n\in\mathcal{S}(x,y)} \chi(n) + O\left(xy^{-1/2}(\log q)^4\right).$$

Coupled with known estimates on $\Psi(x,y)$, any result of this kind will lead to an estimate for $\sum_{n\le x}\chi(n)$.

In [GS01], Granville and Soundararajan refined Montgomery-Vaughan's method and improved their result to a wider range of x and y. They proved the following, still under GRH:

Theorem 2 ([GS01, Theorem 2])**.** *Let χ be a non-principal character modulo q. Then for all $(\log q)^2(\log x)^2(\log\log x)^{12} \le y \le x \le q$, we have*

$$\sum_{1\le n\le x} \chi(n) = \sum_{n\in\mathcal{S}(x,y)} \chi(n) + O\left(\frac{\Psi(x,y)}{(\log\log q)^2}\right).$$

They also conjectured the following estimate for a wider range.

Conjecture 1. *There exists a constant $A > 0$ such that the following holds. Let χ be a non-principal character modulo q. Then for all $(\log q + (\log x)^2)(\log\log q)^A \le y \le x \le q$, we have*

$$\sum_{1\le n\le x} \chi(n) = \sum_{n\in\mathcal{S}(x,y)} \chi(n) + o\left(\Psi(x,y,\chi_0)\right).$$

Here χ_0 is the principal character modulo q.

In this paper, we will prove an analog of these estimates in function fields. Let $\mathbb{F}_q$ be the field over q elements and $\mathbb{F}_q[t]$ be the polynomial ring over $\mathbb{F}_q$. Let A_d denote the set of all polynomials of degree *exactly* d. Given $r\in\mathbb{Z}^+$, a polynomial $f\in\mathbb{F}_q[t]$ is called *r-smooth* if none of its irreducible factors have degree greater than r. Let $\mathcal{P}(d,r)$ denote the set of all r-smooth polynomials in A_d and $N(d,r) = |\mathcal{P}(d,r)|$.

If $Q\in\mathbb{F}_q[t]$, then a character χ modulo Q is simply a character on the multiplicative group $(\mathbb{F}_q[t]/(Q))^\times$, which can be extended to a function on all of $\mathbb{F}_q[t]$ by periodicity. If Q is irreducible of degree n, then χ can be naturally regarded as a character on the field $\mathbb{F}_{q^n}$.

Thoughout this paper, f will stand for a *monic* polynomial and P for a *monic, irreducible* polynomial in $\mathbb{F}_q[t]$.

We will prove the following:

Theorem 3. *Let Q be a polynomial of degree n in $\mathbb{F}_q[t]$ and χ be a non-principal character modulo Q. For any $2\log_q n \le r \le d \le n$, we have*

$$\sum_{f\in A_d} \chi(f) = \sum_{f\in\mathcal{P}(d,r)} \chi(f) + O\left(nq^{-r/2}q^d\right).$$

Notice that the implicit constant in $O(\cdot)$ is independent of q. The range of applicability of our estimate is better than that of Granville-Soundararajan, which corresponds to

$$2\log_q n + 2\log_q d + O(\log_q \log_q d) \le r \le d \le n.$$

Our error term is also better than that of Montgomery-Vaughan, which corresponds to

$$O\left(n^4 q^{-r/2} q^d\right).$$

However, our range is still far weaker than the conjectured range of Granville-Soundararajan.

Our method follows Montgomery-Vaughan closely. The sources of our improvements are a character sum estimate not available in the integers (Theorem 8), and the use of Cauchy's integral formula instead of Perron's formula.

From Theorem 3 we deduce the following:

Corollary 4. *Let Q be a polynomial of degree n in $\mathbb{F}_q[t]$ and χ be a non-principal character modulo Q. For any $2\log_q n \leq r \leq d \leq n$, we have*

$$\frac{1}{q^d}\left|\sum_{f\in A_d}\chi(f)\right| \leq \varepsilon_{q,d,r,n},$$

where $\varepsilon_{q,d,r,n} = \rho\left(\frac{d}{r}\right) q^{O\left(\frac{d\log d}{r^2}\right)} + O\left(nq^{-r/2}\right)$ and $\rho(\cdot)$ is the Dickman function.

Like Theorem 3, this inequality is uniform in q. The function ρ will be defined later in Section 2.2, but for now we note that ρ decays extremely rapidly to 0: $\rho(u) = u^{-u(1+o(1))}$ as $u \to \infty$.

1.2 Finding primitive roots in $\mathbb{F}_{q^n}$

The problem of deterministically outputting a primitive element of a finite field is a notoriously hard problem. However, a relaxation of this problem is well studied. The goal is to output a small subset of the field guaranteed to contain primitive elements (even one primitive element). This has applications in coding theory, cryptography and combinatorial designs. For details, see the wonderful survey of Shparlinski (Research problem AP5, [Shp90a]). We mention the relevant literature now.

Let $\mathbb{F}_{q^n}$ be the finite field in consideration. We consider the setting of small q and growing n. Shoup [Sho92] and Shparlinski [Shp90] independently gave efficient algorithms to construct a set $M \subset \mathbb{F}_{q^n}$ when q is prime[1] of size $\mathrm{poly}(n, q)$ that contains a primitive element. Shparlinski's set is of size $O(n^{10})$. Shoup uses a stronger sieve and gets a set of smaller size (In fact, as noted in [Shp90a], using the stronger sieve, Shparlinksi also obtains a similar bound). However, Shoup outputs the set of low degree polynomials that are irreducible and guarantees a lower bound on the density of the primitive elements, say μ (where the density is taken over the set of irreducible polynomials). However, the enumeration step requires outputting all degree d polynomials and therefore the density suffers a loss ($o(\mu)$).

Our result differs from this in the following sense. Firstly, we show that the simple set of all monic polynomials of degree $d \sim C\log_q n$ is guaranteed to contain a primitive element. This statement as it is, is not new because of the above result of Shoup. However, we also show that the density of primitive elements is μ, that is we do not suffer any density loss. We also give another density argument which basically states for d as above the density of primitive elements in the

[1] Shoup's result on character sums also works for q non prime though the result is stated for prime q.

set of monic degree d polynomials is close to $\phi(q^n-1)/(q^n-1)$ (where $\phi(\cdot)$ is the Euler totient function) when q^n-1 does not have too many distinct prime divisors. We state our application in more detail next.

From our character sum estimates, we derive the following. Let $N = q^n$. Note that for an irreducible polynomial Q of degree n, $\mathbb{F}_{q^n} \equiv \mathbb{F}_q[x]/(Q(x))$. Let $\omega(N-1)$ be the number of distinct prime factors of $N-1$. Let $\mathcal{Q}(d)$ be the set of monic polynomials of degree d that are primitive in $\mathbb{F}_{q^n}$. We prove the following:

Theorem 5. *Let $d = \left(2\log_q n + 2\log_q(1/\varepsilon)\right)\frac{C\log 1/\varepsilon}{\log\log 1/\varepsilon}$, for some absolute constant C. Then,*

$$\left|\frac{|\mathcal{Q}(d)|}{q^d} - \frac{\phi(N-1)}{N-1}\right| = 2^{\omega(N-1)}O_q(\varepsilon).$$

Another way of looking at this theorem is to see that we have a probabilistic algorithm to output a primitive element that improves on the naive algorithm of outputting a random element in the following ways and gives similar success probability.

- Uses nearly logarithmic (in n) randomness as opposed to linear.
- Runs in logarithmic time as opposed to linear.

Note that if $N-1$ is prime, then $\omega(N-1) = 1$. However, if $\omega(N-1)$ is large, then our bound becomes trivial due to the exponential dependence on $\omega(N-1)$. That is, we require $\varepsilon \ll 2^{-\omega(N-1)}$. In such cases, we prove a stronger lower bound on the density of primitive elements using Iwaniec's shifted sieve (as used in [Sho92]). As one can observe, we need a much weaker dependence on ε now, that is $\varepsilon \ll \omega(N-1)^{-2}$. However, we no longer have a pseudorandomness statement as we have a one sided guarantee which is needed in most applications. We state it next.

Theorem 6. *There is a universal constant c such that the following is true. Let $\varepsilon = \varepsilon_{q,d,r,n}$ from Corollary 4. Let $N = q^n$. Then, if $\varepsilon < \frac{c}{\omega(N-1)^2(\log\omega(N-1)+1)^2}$, then*

$$\frac{|\mathcal{Q}(d)|}{q^d} \geq \frac{c}{(\log\omega(N-1)+1)^2}.$$

2 Preliminaries

2.1 L-functions in $\mathbb{F}_q[t]$

Recall that A_k is the set of all monic polynomials of degree exactly k in $\mathbb{F}_q[t]$. Let I_k be the subset of A_k consisting of irreducible polynomials and $\pi_k = |I_k|$. It is well known that

$$\pi_k \leq \frac{q^k}{k}. \tag{1}$$

Following Montgomery-Vaughan, we will work with L-functions in $\mathbb{F}_q[t]$. Fix Q of degree n and a non-principal character χ modulo Q. Define

$$L(s,\chi) = \sum_{f \text{ monic}} \frac{\chi(f)}{|f|^s} \tag{2}$$

for $|s| > 1$. Put $A(d,\chi) = \sum_{f \in A_d} \chi(f)$. Then we can write

$$L(s,\chi) = \sum_{m=0}^{\infty} A(m,\chi) q^{-ms}.$$

Actually, it is even more convenient to put

$$\mathcal{L}(z,\chi) = \sum_{m=0}^{\infty} A(m,\chi) z^{m}.$$

Clearly $L(s,\chi) = \mathcal{L}(q^{-s},\chi)$ for any $\mathrm{Re}(s) > 1$. Since $A(m,\chi) = 0$ whenever $m \geq n$ [Ros02, Proposition 4.3], $\mathcal{L}(z,\chi)$ is a polynomial of degree at most $n-1$, and in particular an entire function. We have the Euler product formula

$$\mathcal{L}(z,\chi) = \prod_{P} \left(1 - \chi(P) z^{\deg(P)}\right)^{-1} \tag{3}$$

whenever $|z| < 1/q$.

The *Generalized Riemann Hypothesis in function fields*, proved by Weil, states that all roots of $\mathcal{L}$ have modulus equal to either 1 or $q^{-1/2}$. Thus we have yet another representation

$$\mathcal{L}(z,\chi) = \prod_{i=1}^{m} (1 - \alpha_i z) \tag{4}$$

where $1 \leq m \leq n-1$ and $|\alpha_i| = 1$ or $q^{1/2}$ for any $i = 1, \ldots, m$.

We recall the following results in $\mathbb{F}_q[t]$ which we will need.

Lemma 7 (Mertens' estimate [Ros99])**.** *For any $k > 0$, we have*

$$\prod_{\deg P \leq k} \left(1 - q^{-\deg P}\right)^{-1} = e^{\gamma} k (1 + o_k(1))$$

where γ is Euler's constant.

The next result is a character sum estimate which is not available in the integers.

Theorem 8 ([Hsu98, Theorem 2.1])**.** *For any polynomial Q of degree n in $\mathbb{F}_q[t]$, any non-trivial character χ modulo Q and $k > 0$, we have*

$$\left| \sum_{P \in I_k} \chi(P) \right| \leq (n+1) \frac{q^{k/2}}{k}.$$

Hsu [Hsu98] attributed this result to Effinger and Hayes [EH91]. When χ is quadratic, a more general result was proved by Car [Car02, Proposition II.2]. For completeness, we include a quick proof of Theorem 8.

Proof. From (3) and (4), by taking logarithmic derivatives, we have

$$\sum_{f\in\mathbb{F}_q[t]}\Lambda(f)\chi(f)z^{\deg f}=\sum_{l=1}^{\infty}\left(-\sum_{i=1}^{m}\alpha_i^l\right)z^l$$

for $|z|<1/q$, where $\Lambda(f)$ is the von Mangoldt function

$$\Lambda(f)=\begin{cases}\deg(P), & \text{if } P=P^k \text{ for some monic, irreducible } P;\\ 0, & \text{otherwise.}\end{cases}$$

By comparing the coefficients of z^k, and using the fact that $|\alpha_i|\le q^{1/2}$ for each i, we have

$$\left|\sum_{f\in A_k}\Lambda(f)\chi(f)\right|\le(n-1)q^{k/2}.$$

Therefore,

$$\left|\sum_{l|k}l\sum_{P\in I_l}\chi(P^{k/l})\right|\le(n-1)q^{k/2}.$$

Consequently, in view of (1)

$$\begin{aligned}\left|k\sum_{P\in I_k}\chi(P)\right| &\le (n-1)q^{k/2}+\sum_{l|k,l<k}l\pi_l\\ &\le (n-1)q^{k/2}+\sum_{l|k,l<k}q^l\\ &\le nq^{k/2}+\sum_{l=1}^{[k/2]-1}q^l\\ &\le (n+1)\,q^{k/2}\end{aligned}$$

as desired. □

2.2 Smooth polynomials

We recall some facts about the function $N(r,d)$. Just as its integer counterpart $\Psi(x,y)$, $N(d,r)$ is closely related to the *Dickman function.* Recall that the Dickman function $\rho(u)$ is the unique continuous function satisfying

$$\rho(u)=\frac{1}{u}\int_{u-1}^{u}\rho(t)dt$$

for all $u>1$, with initial condition $\rho(u)=1$ for $0\le u\le 1$. We have $\rho(u)=1-\log u$ for $1\le u\le 2$, and the following asymptotic formula [HT93, Corollary2.3]

$$\rho(u)=\exp\left(-u\left(\log u+\log\log(u+2)-1+O\left(\frac{\log\log(u+2)}{\log(u+2)}\right)\right)\right)$$

for all $u \geq 1$. In particular, we have

$$\rho(u) \leq \exp\left(-u \log u\right) \tag{5}$$

for u sufficiently large.

We have the following estimate for $N(d,r)$ due to Soundararajan.

Theorem 9 ([Sou, Theorem 1.1])**.** *For any $\log_q d \log^2 d \leq r \leq d$, we have, uniformly in q,*

$$N(d,r) = q^d \rho\left(\frac{d}{r}\right) q^{O\left(\frac{d\log d}{r^2}\right)}.$$

In particular, we have $N(d,r) \sim q^d \rho(d/r)$ as $d \to \infty$ and $\frac{r}{\sqrt{d\log d}} \to \infty$.

3 Proof of Theorem 3 and Corollary 4

Let us introduce auxiliary functions

$$\mathcal{M}(z,\chi) = \prod_{\deg(P)\leq r} \left(1 - \chi(P) z^{\deg(P)}\right)^{-1}$$

and

$$\mathcal{N}(z,\chi) = \mathcal{L}(z,\chi)/\mathcal{M}(z,\chi).$$

Note that for $|z| < 1/q$, we have

$$\mathcal{M}(z,\chi) = 1 + \sum_{k=1}^{\infty} \left(\sum_{f\in\mathcal{P}(k,r)} \chi(f) \right) z^k.$$

Also, by the Euler product formula we have

$$\mathcal{N}(z,\chi) = \prod_{\deg(P)>r} \left(1 - \chi(P) z^{\deg(P)}\right)^{-1}.$$

Let $0 < R < 1/q$ be arbitrary, and C_R be the circle centered at 0 with radius R. By the Cauchy integral formula, we have

$$\begin{aligned} A(d,\chi) - \sum_{f\in\mathcal{P}(d,r)} \chi(f) &= \frac{1}{2\pi i}\int_{C_R} \left(\mathcal{L}(z,\chi) - \mathcal{M}(z,\chi)\right) z^{-d-1} dz \\ &= \frac{1}{2\pi i}\int_{C_R} \mathcal{M}(z,\chi)\left(\mathcal{N}(z,\chi) - 1\right) z^{-d-1} dz \end{aligned} \tag{6}$$

Therefore, it suffices to bound $\mathcal{M}(z,\chi)$ and $\mathcal{N}(z,\chi) - 1$ on C_R.

By Lemma 7, we have $\mathcal{M}(z,\chi) = O(r)$ on C_R.

On C_R, we have

$$\begin{aligned}
|\log N(z,\chi)| &= \left| \sum_{\deg(P)>r} -\log\left(1-\chi(P)z^{\deg(P)}\right) \right| \\
&= \left| \sum_{\deg(P)>r} \sum_{m=1}^{\infty} \frac{1}{m}\chi(P^m) z^{m\deg(P)} \right| \\
&= \left| \sum_{m=1}^{\infty} \sum_{k=r+1}^{\infty} \frac{z^{mk}}{m} \sum_{P\in I_k} \chi(P^m) \right|. \qquad (7)
\end{aligned}$$

We break the above sum into two parts, $m=1$ and $m\geq 2$. By Theorem 8, the contribution of $m=1$ in (7) is

$$\begin{aligned}
\left| \sum_{k=r+1}^{\infty} z^k \sum_{P\in I_k} \chi(P) \right| &\ll n \sum_{k=r+1}^{\infty} \frac{q^{k/2}R^k}{k} \\
&\ll \frac{n}{r}(Rq^{1/2})^r \qquad (8)
\end{aligned}$$

since $Rq^{1/2} < q^{-1/2} \leq 2^{-1/2}$.

The contribution of $m\geq 2$ in (7) is

$$\begin{aligned}
\left| \sum_{m=2}^{\infty} \sum_{k=r+1}^{\infty} \frac{z^{mk}}{m} \sum_{P\in I_k} \chi(P^m) \right| &\leq \sum_{k=r+1}^{\infty} \sum_{m=2}^{\infty} \frac{1}{mq^{mk}} \cdot \frac{q^k}{k} \\
&\leq \sum_{k=r+1}^{\infty} \sum_{m=2}^{\infty} \frac{1}{q^{(m-1)k}} \\
&\ll \sum_{k=r+1}^{\infty} \frac{1}{q^k} \\
&\ll \frac{1}{q^r}. \qquad (9)
\end{aligned}$$

From (8) and (9), we have

$$|\log N(z,\chi)| \ll \frac{n}{r}(Rq^{1/2})^r + 1/q^r \ll \frac{n}{r}(Rq^{1/2})^r. \qquad (10)$$

We have $\frac{n}{r}(Rq^{1/2})^r \leq \frac{n}{r}q^{-r/2} \leq 1$ if $r \geq 2\log_q n$. Therefore, as long as $r\geq 2\log_q n$, we have $|\mathcal{N}(z,\chi)-1| = O\left(\frac{n}{r}(Rq^{1/2})^r\right)$ on C_R. Combining this with (6), we have

$$\begin{aligned}
A(d,\chi) - \sum_{f\in\mathcal{P}(d,r)} \chi(f) &= O\left(r\cdot \frac{n}{r}(Rq^{1/2})^r \cdot R^{-d}\right) \\
&= O(n(Rq^{1/2})^r R^{-d}). \qquad (11)
\end{aligned}$$

Now notice that all the above estimates are independent of $R < 1/q$. Hence, letting R tend to $1/q$, we obtain the bound

$$A(d,\chi) - \sum_{f\in\mathcal{P}(d,r)} \chi(f) = O\left(nq^{-r/2}q^d\right)$$

as desired.

Remark 1. *The estimate (11) remains valid in the wider range $r \geq 2\log_q n - O(\log_q \log_q n)$, and Theorem 3 could have been extended to this range. Unfortunately, when $r \leq 2\log_q n$, the error term $O\left(nq^{-r/2}q^d\right)$ becomes larger than trivial. The exponent of q in the error term, as well as the coefficient of $\log_q n$ in Theorem 3 are the best that can be achieved using our method, since it comes ultimately from Theorem 8.*

Corollary 4 follows immediately from Theorems 3 and 9, since clearly $2\log_q n \geq \log_q(d\log^2 d)$.

4 Proof of Theorem 5

Theorem 5 is proved in a straightforward manner from Corollary 4. The proof technique is credited to Burgess [Bur62] and has been used in the context of irreducible polynomials in [Hsu98].

Recall that $N = q^n$. Define $A(N-1) = \{m : m|N-1, m \text{ squarefree}\}$, so that $|A(N-1)| = 2^{\omega(N-1)}$. Let $\mathcal{Q} \subseteq A_d$ be the set of primitive elements of $\mathbb{F}$.

Set $r = 2\log_q n + 2\log_q 1/\varepsilon$ and $d = r\frac{C\log 1/\varepsilon}{\log\log 1/\varepsilon}$ for some C to be specified later.

First, we observe that the error term $\varepsilon_{q,d,r,n}$ provided by Corollary 4 is $O_q(\varepsilon)$.

Indeed, $nq^{-r/2} = \varepsilon$. By (5), there is a constant C_1 such that for all $u \geq C_1$, $\rho(u) \leq e^{-u\log u}$. Let C_2 be a constant such that the first error term in Corollary 4 is bounded by $q^{C_2\frac{d\log d}{r^2}}$.

We may assume that ϵ is sufficiently small, so that

$$C_1 \leq \frac{C\log 1/\varepsilon}{\log\log 1/\varepsilon}.$$

Then,

$$\rho\left(\frac{d}{r}\right) q^{C_2\frac{d\log d}{r^2}} \leq \exp\left(-\frac{d}{r}\log\frac{d}{r} + C_2\frac{d\log d\log q}{r^2}\right).$$

We claim that the left hand side is $\leq \epsilon$, which is true if

$$\frac{d}{r}\log\frac{d}{r} \geq 2\log\frac{1}{\varepsilon} \tag{12}$$

and

$$C_2\frac{d\log d\log q}{r^2} \leq \frac{d}{2r}\log\frac{d}{r}. \tag{13}$$

Clearly, (12) holds for some absolute constant $C > 0$. Also, (13) holds for ε sufficiently small (depending on C_2). Thus,

$$\varepsilon_{q,d,r,n} = O_q(\varepsilon) \tag{14}$$

Let χ_0 be the principal character on $\mathbb{F}_{q^n}$. For any $m|N-1$, we have $\sum_{\chi:\chi^m=\chi_0}\chi(x) = m$ if x is an m-th power residue and zero otherwise. Using this, we build our indicator function for primitive elements in $\mathbb{F}_{q^n}$. Let $f(x)$ be the indicator function for primitive roots in $\mathbb{F}_{q^n}$. Then, it is easy to check that

$$f(x) = \sum_{m|N-1} \frac{\mu(m)}{m} \sum_{\chi:\chi^m=1} \chi(x)$$

Now,

$$\begin{aligned}
\sum_{x\in A_d} f(x) &= \sum_{x\in A_d}\sum_{m|N-1} \frac{\mu(m)}{m} \sum_{\chi:\chi^m=\chi_0} \chi(x) \\
&= \sum_{m|N-1} \frac{\mu(m)}{m} \sum_{\chi:\chi^m=\chi_0}\sum_{x\in A_d} \chi(x) \\
&= \sum_{m|N-1} \frac{\mu(m)}{m}\left(q^d\right) + \sum_{m|N-1} \frac{\mu(m)}{m} \sum_{\chi\neq\chi_0:\chi^m=1}\sum_{x\in A_d} \chi(x) \\
&= q^d\frac{\phi(N-1)}{N-1} + O\left(2^{\omega(N-1)}\varepsilon_{q,d,r,n}q^d\right) \quad \text{(by Corollary 4)}
\end{aligned}$$

Hence, by (14),

$$\left|\frac{|\mathcal{Q}(d)|}{q^d} - \frac{\phi(N-1)}{N-1}\right| = 2^{\omega(N-1)}O_q(\varepsilon).$$

5 Proof of Theorem 6

In this section, we shall see how to improve the probability of outputting a primitive element from the set of monic degree d polynomials. We shall use a generalization of Iwaniec's shifted sieve [Iwa78], proved by Shoup [Sho92]. We state it next.

Theorem 10 (Prop. 1 in [Sho92]). *Let Γ be a finite set. Let $U : \Gamma \to \mathbb{Z}$, $W : \Gamma \to \mathbb{R}_{\geq 0}$. Let $p_1, \ldots p_l$ be distinct primes with $\Pi = \prod_{i=1}^{l} p_i$. Define*

$$T = \sum_{\gamma\in\Gamma:\ \gcd(U(\gamma),\Pi)=1} W(\gamma)$$

and for $m|\Pi$,

$$S_m = \sum_{\gamma\in\Gamma:\ U(\gamma)=0 \pmod m} W(\gamma).$$

Suppose there are A, B such that for all $m|\Pi$,

$$|S_m - A/m| \leq B.$$

Then

$$T \geq c_1 A/(\log l + 1)^2 - c_2 l^2 B,$$

where c_1, c_2 are absolute positive constants.

Proof of Theorem 6. Let g be an arbitrary primitive element of $\mathbb{F}_{q^n}^\times$. Let $\Gamma = A_d$ and for every $f \in A_d$, let $U(f)$ denote the discrete logarithm of f with base g. Let $W(f) = 1$. Let $N - 1 = \prod_{i=1}^{l} p_i^{\alpha_i}$ be the prime factorization of $N - 1$. Set $\Pi = \prod_{i=1}^{l} p_i$. Let $m|\Pi$ and χ be a multiplicative character of $\mathbb{F}_{q^n}^\times$ of order m. We have

$$\begin{aligned} S_m &= \sum_{f \in A_d : U(f) = 0 \pmod{m}} 1 \\ &= \sum_{f \in A_d} \frac{1}{s} \sum_{i=0}^{m-1} \chi^i(f) \\ &= \frac{1}{m} \sum_{i=0}^{m-1} \sum_{f \in A_d} \chi^i(f) \end{aligned}$$

By Corollary 4, we have $|S_m - \frac{q^d}{m}| \le q^d \varepsilon$, where $\varepsilon = \varepsilon_{q,d,r,n}$. Thus, with $A = q^d$ and $B = q^d \varepsilon$, by Theorem 10, we have

$$T \ge c_1 q^d / (\log l + 1)^2 - c_2 l^2 q^d \varepsilon.$$

Also, note that by the way T is defined, T is also the cardinality of the primitive elements in A_d. Thus, we have

$$\frac{T}{q^d} \ge c / (\log l + 1)^2$$

as long as $\varepsilon < \frac{c}{l^2 (\log l + 1)^2}$, for a suitably chosen $c > 0$. □

6 Acknowledgement

We thank Ariel Gabizon, Felipe Voloch and David Zuckerman for helpful discussions, and Kannan Soundararajan for kindly sending us the unpublished manuscript [Sou]. The first author would also like to thank his advisor, David Zuckerman for his constant support and encouragement throughout the project.

References

[Car02] M. Car. Résidus quadratiques dans $\mathbb{F}_q[T]$. *Acta Arith.*, 104 (2002), 137–153.

[Bur62] D. A. Burgess. On Character Sums and Primitive Roots. Proceedings of the London Mathematical Society, s3-12(1):179–192, 1962.

[EH91] G.W. Effinger and D.R. Hayes. Additive number theory of polynomials over a finite field. Oxford University Press, 1991.

[Dav00] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[GS01] Andrew Granville and K. Soundararajan. Large character sums. *J. Amer. Math. Soc.*, 14(2):365–397, 2001.

[HT93] Adolf Hildebrand and Gérald Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2):411–484, 1993.

[Hsu98] Chih-Nung Hsu. On certain character sums over $\mathbb{F}_q[t]$. *Proceedings of the American Mathematical Society* 126.3 (1998): 647–652.

[Iwa78] H. Iwaniec On the problem of Jacobsthal. *Demonstratio Math.*, 11 (1978), no. 1, 225–231.

[MV77] H. L. Montgomery and R. C. Vaughan. Exponential sums with multiplicative coefficients. *Invent. Math.*, 43(1):69–82, 1977.

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

[Ros99] Michael Rosen. A generalization of Mertens' theorem. *J. Ramanujan Math. Soc.*, 14(1):1–19, 1999.

[Sho92] Victor Shoup. Searching for Primitive Roots in Finite Fields. *Math. Comp. 58 (1992)*, no. 197, 369–380.

[Shp90] Igor Shparlinski. On primitive elements in finite fields and on elliptic curves. *Matem. Sbornik*, 181(1990), 1196–1206 (in Russian).

[Shp90a] Igor Shparlinski. Approximate constructions in finite fields. FFA '95 Proceedings of the third international conference on Finite fields and applications.

[Sou] K. Soundararajan. Smooth polynomials: analogies and asymptotics. unpublished manuscript.