Finite Fields and Their Applications 46 (2017) 247–254

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Short Communication

A note on character sums in finite fields

Abhishek Bhowmick [a], Thái Hoàng Lê [b,*], Yu-Ru Liu [c]

[a] *Department of Computer Science, The University of Texas at Austin, TX 78712, United States*
[b] *Department of Mathematics, The University of Mississippi, University, MS 38677, United States*
[c] *Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, ON, N2L 3G1, Canada*

ARTICLE INFO

Article history:
Received 7 November 2016
Received in revised form 10 March 2017
Accepted 17 March 2017
Available online 21 April 2017
Communicated by Stephen D. Cohen

MSC:
11L40
11T55

Keywords:
Character sums
Finite fields
L-functions
Function fields

ABSTRACT

We prove a character sum estimate in $\mathbb{F}_q[t]$ and answer a question of Shparlinski.

1. Introduction

Shparlinski [5] asks the following.

* Corresponding author.
E-mail addresses: bhowmick@cs.utexas.edu (A. Bhowmick), leth@olemiss.edu (T.H. Lê), yrliu@math.uwaterloo.ca (Y.-R. Liu).

http://dx.doi.org/10.1016/j.ffa.2017.03.010
1071-5797/

Problem 1. [5, Problem 14] Let $m \in \mathbb{Z}$ and χ be a non-principal character modulo m. Under the Generalized Riemann Hypothesis, obtain an estimate of the form

$$\sum_{k=1}^{N} \chi(k) \ll N^{1/2} m^{o(1)}$$

for any N, with an explicit expression for $m^{o(1)}$.

Though it has never been explicitly written down, such a bound is presumably well-known among analytic number theorists due to its connection with upper bounds for L-functions. Indeed, let $L(s,\chi)$ be the Dirichlet L-function associated with χ and $s = \sigma + it$. First we assume that χ is primitive. Then conditionally under GRH, we have the bound [3, Exercise 8, Section 13.2]

$$L(s,\chi) \ll \exp\left(C_1 \frac{\log m|t|}{\log\log m|t|}\right) \tag{1}$$

for some absolute constant $C_1 > 0$ and uniformly for $1/2 \le \sigma \le 3/2$ and $|t| \ge 2$. Using the bound (1) and a standard contour integral one can show that

$$\sum_{k=1}^{N} \chi(k) \ll N^{1/2} \exp\left(C_2 \frac{\log m}{\log\log m}\right) \tag{2}$$

for some absolute constant $C_2 > 0$, when χ is primitive. If χ is induced by a character χ_1 modulo r with $r|m$ then

$$\sum_{k=1}^{N} \chi(k) = \sum_{\substack{k=1 \\ (k,r)=1}}^{N} \chi_1(k) = \sum_{d|\frac{m}{r}} \mu(d)\chi_1(d) \sum_{k \le N/d} \chi_1(k).$$

Bounding this trivially, together with the fact that the number of prime factors of n is $O\left(\frac{\log n}{\log\log n}\right)$, it follows that we have a bound of type (2) as well when χ is not primitive.

The purpose of this note, however, is to obtain a bound similar to (2) in the polynomial ring $\mathbb{F}_q[t]$. Let $Q \in \mathbb{F}_q[t]$ be a polynomial of degree n. A (Dirichlet) character χ modulo Q is 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 and by setting $\chi(f) = 0$ for all $(f,Q) \neq 1$. If Q is irreducible then χ is a character on the field $\mathbb{F}_{q^n}$.

Shparlinski (private communication) also asks an $\mathbb{F}_q[t]$-analog of Problem 1:

Problem 2. Let $Q \in \mathbb{F}_q[t], \deg Q = n > 0$ and χ be a non-principal character modulo Q. Let A_d be the set of all monic polynomials of degree exactly d in $\mathbb{F}_q[t]$. Obtain an estimate of the form

$$\sum_{f\in A_d}\chi(f) \ll q^{\frac{d}{2}+o(n)}$$

for any d, with an explicit expression for $o(n)$.

We prove the following explicit estimate.

Theorem 1. *Let $Q \in \mathbb{F}_q[t], \deg Q = n > 0$ and χ be a non-principal (not necessarily primitive) character modulo Q. If $n \geq 10^4$ and $\frac{\log\log n}{\log n} \geq \frac{1}{\log q}$, then we have*

$$\left|\sum_{f\in A_d}\chi(f)\right| \leq q^{\frac{d}{2}+\frac{d\log\log n}{\log n}} e^{\frac{8qn}{\log^2 n}}. \tag{3}$$

Note that we have the analogies $N \leftrightarrow q^d$ and $m \leftrightarrow q^n$ between $\mathbb{Z}$ and $\mathbb{F}_q[t]$. The bound (2) corresponds to $q^{\frac{d}{2}}\exp\left(\frac{Cn}{\log n}\right)$ in $\mathbb{F}_q[t]$. Thus (3) is stronger than (2) when d is small (e.g., when $d \ll \frac{n}{\log n}$) but weaker than (2) when d is large (e.g., when $d \gg n$). It is an interesting problem to see if in $\mathbb{F}_q[t]$ we can achieve, or even beat (2) for all d. Nevertheless, our proof of (3) is much simpler than the proof in the integers and is potentially still useful in applications. The constants 8 and 10^4 in (3) can certainly be improved, but we do not attempt to do so to keep our estimates clean.

We also record another similar character sum estimate, which might be of interest.

Theorem 2. *Let $Q \in \mathbb{F}_q[t], \deg Q = n > 0$ and χ be a non-principal (not necessarily primitive) character modulo Q. Under the hypotheses of Theorem 1, we have*

$$\left|\sum_{f\in A_d}\mu(f)\chi(f)\right| \leq q^{\frac{d}{2}+\frac{d\log\log n}{\log n}} e^{\frac{8qn}{\log^2 n}}.$$

Here μ is the Möbius function on $\mathbb{F}_q[t]$ defined by

$$\mu(f) = \begin{cases} (-1)^k, & \text{where } k \text{ is the number of monic irreducible factors of } f, \\ & \text{if } f \text{ is square-free,} \\ 0, & \text{otherwise.} \end{cases}$$

The difference between Theorem 1 and Theorem 2 is that, while the former is trivial when $d \geq n$, the latter is non-trivial for all d.

It is useful to compare (3) with other character sum estimates in $\mathbb{F}_q[t]$. In [1], the first two authors proved that for any $2\log_q n \leq r \leq d \leq n$, we have

$$\left|\sum_{f\in A_d}\chi(f)\right| \leq q^d \cdot \rho\left(\frac{d}{r}\right) q^{O\left(\frac{d\log d}{r^2}\right)} + O\left(nq^{d-r/2}\right). \tag{4}$$

Here $\rho(u)$ is the Dickman function, i.e., 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 $0 \leq u \leq 1$. We have the asymptotic estimate $\rho(u) = u^{-u(1+o(1))}$ as $u \to \infty$.

The difference between the inequalities (4) and (3) is that while (4) is non-trivial in a wider range of d, (3) provides a better saving when d is large. Indeed, if one wants to match the bound in (3), the second term in RHS of (4) requires one to choose r close to d. But then the contribution of the first term in RHS of (4) becomes significant. Hence (3) does not follow from (4).

One can also compare (3) with the analog of the Pólya–Vinogradov inequality in $\mathbb{F}_q[t]$ [2, Proposition 2.1], which states that for any d,

$$\left| \sum_{f \in A_d} \chi(f) \right| \leq 2q^{\frac{n-1}{2}}.$$

2. Proofs of Theorems 1 and 2

Similar to the integers, we deduce Theorems 1 and 2 from a bound for L-functions near the critical line (Proposition 3). We begin with some facts about L-functions in $\mathbb{F}_q[t]$. Throughout this paper, f will stand for a monic polynomial and P will stand for a monic, irreducible polynomial. Fix Q of degree n and a non-principal character χ modulo Q. Put $A(d, \chi) = \sum_{f \in A_d} \chi(f)$. Then the L-function (assuming $\mathrm{Re}(s) > 1$) associated with χ is

$$L(s, \chi) = \sum_{f} \frac{\chi(f)}{q^{s \deg f}} = \sum_{d=0}^{\infty} A(d, \chi) q^{-ds}.$$

It is even more convenient to put

$$\mathcal{L}(z, \chi) = \sum_{d=0}^{\infty} A(d, \chi) z^d. \tag{5}$$

Clearly $L(s, \chi) = \mathcal{L}(q^{-s}, \chi)$ for any $\mathrm{Re}(s) > 1$. Since $A(d, \chi) = 0$ whenever $d \geq n$ [4, 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

$$\mathcal{L}(z, \chi) = \prod_{P} \left(1 - \chi(P) z^{\deg P}\right)^{-1} \tag{6}$$

whenever $|z| < 1/q$. In the same range of z, we also have

$$\frac{1}{\mathcal{L}(z,\chi)} = \prod_P \left(1 - \chi(P) z^{\deg P}\right) = \sum_f \mu(f)\chi(f) z^{\deg f}. \tag{7}$$

The *Generalized Riemann Hypothesis* states that all roots of $\mathcal{L}(z,\chi)$ have modulus $q^{-1/2}$ or 1. In other words, we can write

$$\mathcal{L}(z,\chi) = \prod_{i=1}^{D} (1 - \alpha_i z) \tag{8}$$

where $|\alpha_i| = q^{1/2}$ or 1 for any q, for some $D \leq n-1$. In particular, (7) remains valid when $|z| < q^{-1/2}$.

Our results are deduced from the following bound for $\mathcal{L}(z,\chi)$ near the circle $|z| = q^{-1/2}$.

Proposition 3. *Let χ be a (not necessarily primitive) character modulo Q with $\deg Q = n$. Let $q^{-3/4} \leq R < q^{-1/2}$. For any $|w| = R$, we have*

$$|\mathcal{L}(w,\chi)| \leq \exp\left(n^2 R^L q \left(7 + \frac{1}{L(1 - q^{1/2}R)}\right)\right), \tag{9}$$

$$\left|\frac{1}{\mathcal{L}(w,\chi)}\right| \leq \exp\left(n^2 R^L q \left(7 + \frac{1}{L(1 - q^{1/2}R)}\right)\right), \tag{10}$$

where $L = \lceil 2\log_q n \rceil$.

The "correct" choice of R will be made later in applications.

Proof. By taking the logarithmic derivatives of (6) and (8), we have two different expressions for $\frac{\mathcal{L}'(z,\chi)}{\mathcal{L}(z,\chi)}$. Namely, we have

$$\frac{\mathcal{L}'(z,\chi)}{\mathcal{L}(z,\chi)} = \sum_{l=1}^{\infty} a_l z^{l-1}$$

where

$$a_l = -\sum_{i=1}^{D} \alpha_i^l \tag{11}$$

according to (8), while

$$a_l = \sum_{\deg f = l} \Lambda(f)\chi(f) \tag{12}$$

according to (6). Here Λ is the von Mangoldt function on $\mathbb{F}_q[t]$ defined by

$$\Lambda(f) = \begin{cases} \deg P, & \text{if } f = P^k \text{ for some monic irreducible } P \text{ and } k \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

From (11) we have

$$|a_l| \leq nq^{l/2} \tag{13}$$

and from (12) we have

$$|a_l| \leq \sum_{\deg f = l} \Lambda(f) = q^l. \tag{14}$$

Recall that $L = \lceil 2\log_q n \rceil$. For $l \geq L$ we use the bound (13) and $l < L$ we use the bound (14). Therefore, for any z, we have

$$\left| \frac{\mathcal{L}'(z,\chi)}{\mathcal{L}(z,\chi)} \right| \leq \sum_{l=1}^{L-1} q^l |z|^{l-1} + \sum_{l=L}^{\infty} nq^{l/2} |z|^{l-1}. \tag{15}$$

Since $\mathcal{L}(0,\chi) = 1$, by integrating (15) along the line from 0 to w, we have

$$|\log \mathcal{L}(w,\chi)| \leq \sum_{l=1}^{L-1} \frac{(Rq)^l}{l} + \sum_{l=L}^{\infty} n \frac{(Rq^{1/2})^l}{l}. \tag{16}$$

The second sum in (16) can be bounded by

$$\frac{n}{L} \sum_{l=L}^{\infty} (Rq^{1/2})^l \leq \frac{n}{L} R^L q^{\frac{L}{2}} \frac{1}{1 - Rq^{1/2}} \leq \frac{n^2 R^L q}{L} \frac{1}{1 - Rq^{1/2}} \tag{17}$$

since $q^{\frac{L-1}{2}} \leq n$. As for the first sum in (16), we bound it crudely by

$$\sum_{l=1}^{L-1} (Rq)^l \leq (Rq)^{L-1} \sum_{k=0}^{\infty} (Rq)^{-k} \leq \frac{n^2 R^{L-1}}{1 - (qR)^{-1}} \leq 7n^2 R^L q \tag{18}$$

since $qR \geq q^{1/4} \geq 2^{1/4}$. By combining (17) and (18), we have

$$|\log \mathcal{L}(w,\chi)| \leq 7n^2 R^L q + \frac{n^2 R^L q}{L} \frac{1}{1 - Rq^{1/2}},$$

from which both (9) and (10) follow. □

Our estimates above are crude. Even if we were more careful, this would result only in better constants, and the shape of the bounds would not be changed.

Proof of Theorems 1 and 2. In what follows, C_R denotes the circle centered at 0 with radius R. Put $R = q^{-1/2-\epsilon}$, for some $0 < \epsilon \leq \frac{1}{4}$ to be chosen later. We also make the additional assumption that $\epsilon \leq \frac{1}{\log q}$. From (9), for $z \in C_R$, we have

$$\begin{aligned} |\mathcal{L}(z,\chi)| &\leq \exp\left(qn^2R^L\left(7+\frac{1}{L(1-q^{1/2}R)}\right)\right) \\ &\leq \exp\left(\left(qn^{1-2\epsilon}\left(7+\frac{1}{L(1-q^{-\epsilon})}\right)\right)\right) \\ &\leq \exp\left(qn^{1-2\epsilon}\left(7+\frac{2}{L\epsilon\log q}\right)\right) \qquad (19) \\ &\leq \exp\left(qn^{1-2\epsilon}\left(7+\frac{1}{\epsilon\log n}\right)\right). \end{aligned}$$

The bound (19) follows from the fact that $\frac{\epsilon\log q}{1-e^{-\epsilon\log q}} \leq \frac{1}{1-e^{-1}} \leq 2$ if $\epsilon\log q \leq 1$, which is a consequence of the fact that the function $\frac{x}{1-e^{-x}}$ is increasing on $(0,\infty)$. From (5) we see that

$$\begin{aligned} |A(d,\chi)| &= \left|\frac{1}{2\pi i}\int_{C_R}\mathcal{L}(z,\chi)z^{-d-1}dz\right| \\ &\leq \max_{C_R}|\mathcal{L}(z,\chi)|\,R^{-d} \\ &\leq \exp\left(qn^{1-2\epsilon}\left(7+\frac{1}{\epsilon\log n}\right)\right)q^{(1/2+\epsilon)d}. \qquad (20) \end{aligned}$$

We now make the choice $\epsilon = \frac{\log\log n}{\log n}$, then $\epsilon \leq 1/4$ if $n \geq 10^4$. Also, by hypothesis $\epsilon \leq \frac{1}{\log q}$. We have $qn^{1-2\epsilon}\left(7+\frac{1}{\epsilon\log n}\right) = \frac{qn}{\log^2 n}\left(7+\frac{1}{\log\log n}\right) \leq \frac{8qn}{\log^2 n}$ if $n \geq 10^4$.

This implies Theorem 1.

Using (7) instead of (5), Theorem 2 follows in exactly the same way. □

Acknowledgments

The authors would like to thank Micah Milinovich and Igor Shparlinski for helpful discussions and the referees for useful and detailed comments which help to improve the presentation of the paper. Part of this work was done when the second author was supported by the Fondation Mathématique Jacques Hadamard and visiting the Taida Institute for Mathematical Sciences, and he gratefully acknowledges their support and hospitality.

References

[1] A. Bhowmick, T.H. Lê, On primitive elements in finite fields of low characteristic, Finite Fields Appl. 35 (2015) 64–77.
[2] C-N. Hsu, Estimates for coefficients of L-functions for function fields, Finite Fields Appl. 5 (1) (January 1999) 76–88.
[3] H.L. Montgomery, R.C. Vaughan, Multiplicative Number Theory I: Classical Theory, Cambridge University Press, 2007.
[4] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
[5] I. Shparlinski, Open problems on exponential and character sums, http://web.maths.unsw.edu.au/~igorshparlinski/CharSumProjects.pdf.