AN ELEMENTARY APPROACH TO CHARACTER SUMS OVER MULTIPLICATIVE SUBGROUPS

Ke Gong[1]
Department of Mathematics, Henan University, Kaifeng, P. R. China
kg@henu.edu.cn

Received: 7/20/15, Accepted: 1/31/16, Published: 2/29/16

Abstract

Let p be an odd prime. Using I. M. Vinogradov's bilinear estimate, we present an elementary approach to estimate character sums

$$\sum_{x\in H}\chi(x+a), \qquad a\in\mathbb{F}_p^*,$$

where H is a multiplicative subgroup in the finite prime field $\mathbb{F}_p$. Two interesting mean-value estimates are also provided.

1. Introduction

Let p be an odd prime and $H < \mathbb{F}_p^*$ be a multiplicative subgroup in the finite prime field $\mathbb{F}_p$. After the opening work of Bourgain, Glibichuk, and Konyagin [1] on *extremely short* exponential sums $\sum_{x\in H}\psi(ax)$ with $a\in\mathbb{F}_p^*$ and ψ being the canonical additive character of $\mathbb{F}_p$, J. Bourgain posed the following problem concerning multiplicative character sum over a shifted subgroup [2, Problem 5].

Problem 1 (J. Bourgain). Obtain a nontrivial bound on $\sum_{x\in H}\chi(x+a)$ for $H<\mathbb{F}_p^*$, $|H|\sim\sqrt{p}$, and $a\in\mathbb{F}_p^*$.

Using I. M. Vinogradov's bilinear estimate for character sums, we shall present an elementary approach to Bourgain's character sum.

Theorem 1. *For any $H<\mathbb{F}_p^*$, we have*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H}\chi(x+a)\right| < p^{1/2}.$$

[1] This work was supported by NNSFC grant 11201117.

Thus, for any $\varepsilon > 0$ and $H < \mathbb{F}_p^*$ with $|H| > p^{1/2+\varepsilon}$, we have

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} \chi(x+a) \right| < p^{-\varepsilon}|H|.$$

Although we cannot break the square-root barrier, the result is nontrivial and has attained the same strength as the consequence of A. Weil's estimate for character sums, which is based on his deep work on the analogue of the Riemann hypothesis for the zeta-function of an algebraic function field over a finite field.

2. Vinogradov's Lemma

We recall that, first in 1940s [6] (up to a $\sqrt{2}$–factor in the upper bound) and then in his famous textbook [7], I. M. Vinogradov obtained the following bilinear estimate for character sums, which played a fundamental role in his studies of character sums over shifted primes.

Lemma 1 (I. M. Vinogradov). *Let p be an odd prime,* $\gcd(a,p) = 1$*, $\chi \neq \chi_0 \pmod{p}$,*

$$S = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(xy+a),$$

$$S' = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(xy(xy+a)).$$

For any complex-valued functions ξ and η with

$$\sum_{x=0}^{p-1} |\xi(x)|^2 \leq X, \qquad \sum_{y=0}^{p-1} |\eta(y)|^2 \leq Y,$$

we have

$$|S| \leq \sqrt{pXY}, \qquad |S'| \leq \sqrt{pXY}.$$

The proof is mainly based on the using of Cauchy–Schwarz inequality and the properties of Dirichlet characters.

3. Proof of Theorem 1

Here and below, we denote $A(\cdot)$ the indicator function for a subset A of $\mathbb{F}_p$.

Recall that $a \in \mathbb{F}_p^*$. We first write

$$\sum_{x\in H} \chi(x+a) = \frac{1}{|H|} \sum_{x,y\in H} \chi(xy+a) = \frac{1}{|H|} \sum_x \sum_y H(x)H(y)\chi(xy+a),$$

then apply Lemma 1 we obtain

$$\left|\sum_{x\in H} \chi(x+a)\right| \leq \frac{1}{|H|}\sqrt{p|H|\cdot|H|} = \sqrt{p}.$$

Indeed, once taking $\xi = \eta$ in Lemma 1 to be the indicator function of multiplicative subgroup $H < \mathbb{F}_p^*$, the estimate

$$\left|\sum_x \sum_y H(x)H(y)\chi(xy+a)\right| \leq |H|^{\frac{1}{2}} \left(p|H| - \left|\sum_{x\in H} \chi(x)\right|^2\right)^{\frac{1}{2}}$$

is implied in the original proof of Vinogradov [7]. This gives a more precise upper bound

$$\left|\sum_{x\in H} \chi(x+a)\right| \leq \left(p - \frac{1}{|H|}\left|\sum_{x\in H} \chi(x)\right|^2\right)^{\frac{1}{2}}.$$

4. Mean-value Estimate, I

We find that the following identity could be obtained using the classical method in [7] and [3].

Theorem 2. *For any subset $D \subset \mathbb{F}_p^*$, we have the identity*

$$\sum_{a\in\mathbb{F}_p} \left|\sum_{x\in D} \chi(x+a)\right|^2 = p|D| - |D|^2.$$

Proof. Indeed,

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} \left|\sum_{x\in D} \chi(x+a)\right|^2 &= \sum_{a\in\mathbb{F}_p} \sum_{x,y\in D} \chi(x+a)\overline{\chi}(y+a) \\ &= \sum_{a\in\mathbb{F}_p} \sum_{x\in D} |\chi(x+a)|^2 + \sum_{\substack{x,y\in D\\ x\neq y}} \sum_{a\in\mathbb{F}_p} \chi(x+a)\overline{\chi}(y+a) \\ &= (p-1)|D| - |D|(|D|-1) \\ &= p|D| - |D|^2.\end{aligned}$$

Note that the second to last equality is due to the fact

$$\sum_{a\in\mathbb{F}_p} \chi(x+a)\overline{\chi}(y+a) = -1,$$

which is a consequence of the observation that the congruence

$$x+a \equiv z(y+a) \pmod{p}$$

establishes a one-to-one correspondence between all a with $a \not\equiv -y$ and all z with $z \not\equiv 1$. □

We remark that Theorem 2 could be compared with its counterpart for exponential sums due to Konyagin [4, Lemma 2]. That is, for any subset $D \subset \mathbb{Z}_q$ (q is a positive integer), there holds

$$\sum_{a\in\mathbb{Z}_q^*} \left| \sum_{x\in D} e_q(ax) \right|^2 = |D|(q-|D|).$$

5. Mean-value Estimate, II

In this section we present a different type mean-value estimate.

Theorem 3. *For $a \in \mathbb{F}_p^*$, we have*

$$\frac{1}{p-1} \sum_{\chi \bmod p} \left| \sum_{n\in H} \chi(n+a) \right| \leq \sqrt{|H|}.$$

Proof. Indeed,

$$\begin{aligned}\left(\sum_{\chi \bmod p} \left| \sum_{n\in H} \chi(n+a) \right| \right)^2 &\leq (p-1) \sum_{m\in H} \sum_{n\in H} \sum_{\chi \bmod p} \chi\left(\frac{m+a}{n+a}\right) \\ &\leq (p-1)(p-1)|H| \\ &= (p-1)^2|H|,\end{aligned}$$

which completes the proof. □

If $a=0$, we recall that Shkredov [5, p. 607] has obtained

$$\sum_{\chi \bmod p} \left| \sum_{n\in H} \chi(n) \right| \leq p.$$

In a private communication, A. Granville provided a proof for the identity

$$\sum_{\chi \bmod p} \Big| \sum_{n\in H} \chi(n) \Big| = p-1.$$

We include his proof as follows.

If H is the subgroup of order $(p-1)/k$, then

$$H(n) = \frac{1}{k} \sum_{\psi:\ \psi^k=\chi_0} \psi(n),$$

so that

$$\sum_n H(n)\chi(n) = \frac{1}{k} \sum_{\psi:\ \psi^k=\chi_0} \sum_n (\psi\chi)(n).$$

This equals $\frac{p-1}{k}$ if $\chi = \overline{\psi}$ for some ψ satisfying $\psi^k = \chi_0$, and equals 0 otherwise. Thus we have

$$\sum_{\chi \bmod p} \Big| \sum_{n\in H} \chi(n) \Big| = \sum_{\chi \bmod p} \Big| \sum_n H(n)\chi(n) \Big| = \sum_{\psi:\ \psi^k=\chi_0} \frac{p-1}{k} = p-1.$$

6. Final Remarks

Using the estimate for S' in Lemma 1, we have for $a \in \mathbb{F}_p^*$

$$\Big| \sum_{x\in H} \chi(x(x+a)) \Big| = \frac{1}{|H|} \Big| \sum_x \sum_y H(x)H(y)\chi(xy(xy+a)) \Big| \le \sqrt{p},$$

which provides the same upper bound as found in Theorem 1 for nonlinear character sums.

We remark that I. E. Shparlinski has posed the following problem, which has immediate implications to polynomial factorization over finite fields.

Problem 2 (I. E. Shparlinski). Estimate nontrivially

$$\sum_{x\in H} \chi((x+a)(x+b)), \qquad ab(a-b) \in \mathbb{F}_p^*$$

for $H < \mathbb{F}_p^*$ and $|H| \sim \sqrt{p}$.

Finally, we would like to pose the following problems, which could also be dealt directly by Weil's estimates for character sums with rational functions argument. But no elementary approach is known.

Problem 3. Estimate nontrivially the sums

$$\sum_{x\in H} e\left(\frac{kx+\ell x^{-1}}{p}\right), \qquad \sum_{x\in H\setminus\{-a\}} e\left(\frac{k(x+a)^{-1}}{p}\right)$$

for $H < \mathbb{F}_p^*$ with $|H| \sim \sqrt{p}$, and $k, \ell, a \in \mathbb{F}_p^*$.

Acknowledgements. I would like to thank Professors Andrew Granville, Chaohua Jia, and Igor Shparlinski for their interests and comments on this work. I am grateful to Professor Sergei Konyagin for sending his Russian paper. I am also grateful to the anonymous referee for his/her helpful suggestions.

References

[1] J. Bourgain, A.A. Glibichuk and S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc.* **73** (2006), 380–398.

[2] M.-C. Chang, Character sums in finite fields. *Finite Fields: Theory and Applications*, 83–98, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, 2010.

[3] H. Davenport and P. Erdős, The distribution of quadratic and higher residues. *Publ. Math. Debrecen* **2** (1952), 252–265.

[4] S.V. Konyagin, Estimates for trigonometric sums over subgroups and for Gauss sums. *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems*, Part III (Tula, 2001), 86–114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002. (Russian)

[5] I.D. Shkredov, On monochromatic solutions of some nonlinear equations in $\mathbb{Z}/p\mathbb{Z}$. *Math. Notes* **88** (2010), 603–611.

[6] I.M. Vinogradov. An improvement of the estimation of sums with primes. *Izv. Akad. Nauk SSSR Ser. Mat.* **7** (1943), 17–34. (Russian)

[7] I.M. Vinogradov, *Foundations of the Theory of Numbers.* 7th ed., Nauka, Moscow, 1965. (Russian)