DOUBLE CHARACTER SUMS OVER SUBGROUPS AND INTERVALS

MEI-CHU CHANG AND IGOR E. SHPARLINSKI

Abstract. We estimate double sums

$$S_\chi(a, \mathcal{I}, \mathcal{G}) = \sum_{x \in \mathcal{I}} \sum_{\lambda \in \mathcal{G}} \chi(x + a\lambda), \qquad 1 \le a < p-1,$$

with a multiplicative character χ modulo p where $\mathcal{I} = \{1, \ldots, H\}$ and $\mathcal{G}$ is a subgroup of order T of the multiplicative group of the finite field of p elements. A nontrivial upper bound on $S_\chi(a, \mathcal{I}, \mathcal{G})$ can be derived from the Burgess bound if $H \ge p^{1/4+\varepsilon}$ and from some standard elementary arguments if $T \ge p^{1/2+\varepsilon}$, where $\varepsilon > 0$ is arbitrary. We obtain a nontrivial estimate in a wider range of parameters H and T. We also estimate double sums

$$T_\chi(a, \mathcal{G}) = \sum_{\lambda, \mu \in \mathcal{G}} \chi(a + \lambda + \mu), \qquad 1 \le a < p-1,$$

and give an application to primitive roots modulo p with 3 non-zero binary digits.

1. Introduction

1.1. **Background and motivation.** For a prime p, we use $\mathbb{F}_p$ to denote the finite field of p elements, which we always assume to be represented by the set $\{0, \ldots, p-1\}$.

Since the spectacular results of Bourgain, Glibichuk & Konyagin [8], Heath-Brown & Konyagin [19] and Konyagin [25] on bounds of exponential sums

$$\sum_{\lambda \in \mathcal{G}} \exp(2\pi i a\lambda/p), \qquad a \in \mathbb{F}_p^*, \tag{1}$$

over small multiplicative subgroups $\mathcal{G}$ of $\mathbb{F}_p^*$, there has been a remarkable progress in this direction, also involving sums over consecutive powers g^i, $i = 1, \ldots, N$, of elements $g \in \mathbb{F}_p^*$, see the survey [17] and

Date: February 23, 2014.

2010 *Mathematics Subject Classification.* 11L40.

Key words and phrases. character sums, intervals, multiplicative subgroups of finite fields.

also very recent results of Bourgain [4, 5] and Shkredov [28, 29]. Exponential sums over short segments of consecutive powers $g, \ldots, g^N$ of a fixed element $g \in \mathbb{F}_p^*$, have also been studied, see [24, 26] and references therein. However the multiplicative analogues of the sums (1), that is, the sums

$$\sum_{\lambda \in \mathcal{G}} \chi(a+\lambda), \qquad a \in \mathbb{F}_p^*,$$

with a nonprincipal multiplicative character χ of $\mathbb{F}_p$ have been resisting all attempts to improve the classical bound

$$\left| \sum_{\lambda \in \mathcal{G}} \chi(a+\lambda) \right| \le \sqrt{p}. \tag{2}$$

Note that (2) is instant from the Weil bound, see [20, Theorem 11.23], if one notices that

$$\sum_{\lambda \in \mathcal{G}} \chi(a+\lambda) = \frac{T}{p-1} \sum_{\mu \in \mathbb{F}_p^*} \chi(a+\mu^{(p-1)/T}),$$

where $T = \#\mathcal{G}$ (but can also be obtained via elementary arguments).

We now recall that Bourgain [3, Section 4] has shown that double sums over short intervals and short segments of consecutive powers

$$\sum_{x=1}^{H} \sum_{n=1}^{N} \exp(2\pi i a x g^n/p), \qquad 1 \le a < p-1,$$

can be estimated for much smaller values of N than for single sums over consecutive powers. Here we show that similar mixing can also be applied to the sums of multiplicative characters and thus lead to nontrivial estimates of the sums

$$S_\chi(a, \mathcal{I}, \mathcal{G}) = \sum_{x \in \mathcal{I}} \sum_{\lambda \in \mathcal{G}} \chi(x + a\lambda), \qquad 1 \le a < p-1,$$

where $\mathcal{I} = \{1, \ldots, H\}$ is an interval of H consecutive integers and $\mathcal{G} \subseteq \mathbb{F}_p^*$ is a multiplicative subgroup of order T for the values of H and T to which previous bounds do not apply. More precisely, one can immediately estimate the sums $S_\chi(a, \mathcal{I}, \mathcal{G})$ nontrivially if for some fixed $\varepsilon > 0$ we have $H \ge p^{1/4+\varepsilon}$, by using the Burgess bound, see [20, Theorem 12.6], or $T \ge p^{1/2+\varepsilon}$, by using (2).

1.2. **Main results.** Here we obtain a nontrivial estimate in a wider range of parameters H and T.

Theorem 1. *For every fixed real $\varepsilon > 0$ there are some $\delta > 0$ and $\eta > 0$ such that if $H > p^{\varepsilon}$ and $T > p^{1/2-\delta}$ then for the interval $\mathcal{I} = \{1, \ldots, H\}$ and the multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order T, we have*

$$S_\chi(a, \mathcal{I}, \mathcal{G}) = O(HTp^{-\eta})$$

uniformly over $a \in \mathbb{F}_p^*$ and nonprincipal multiplicative characters χ of $\mathbb{F}_p$.

We also obtain a similar estimate at the other end of region of H and T, namely for a very small T and H that is still below the reach of the Burgess bound (see [20, Theorem 12.6]). In fact in this case we are able to estimate a more general sums

$$\mathfrak{S}_\chi(f, \mathcal{I}, \mathcal{G}) = \sum_{x \in \mathcal{I}} \sum_{\lambda \in \mathcal{G}} \chi(x + f(\lambda)),$$

with a non-constant polynomial $f \in \mathbb{F}_p[X]$.

Theorem 2. *For every fixed real $\varepsilon > 0$ and integer $d \geq 1$ there are some $\delta > 0$ and $\eta > 0$ such that if $T > p^{\varepsilon}$ and $H > p^{1/4-\delta}$ then for the interval $\mathcal{I} = \{1, \ldots, H\}$, the multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order T, we have*

$$\mathfrak{S}_\chi(f, \mathcal{I}, \mathcal{G}) = O(HTp^{-\eta})$$

uniformly over polynomials $f \in \mathbb{F}_p[X]$ of degree d and nonprincipal multiplicative characters χ of $\mathbb{F}_p$.

We also give an explicit version of Theorem 1 in the case when $H = p^{1/4+o(1)}$ and $T = p^{1/2+o(1)}$, that is, when other methods just start to fail.

Theorem 3. *Let $H = p^{1/4+o(1)}$ and $T = p^{1/2+o(1)}$. Then for the interval $\mathcal{I} = \{1, \ldots, H\}$ and the multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order T, we have*

$$|S_\chi(a, \mathcal{I}, \mathcal{G})| \leq HTp^{-5/48+o(1)}$$

uniformly over $a \in \mathbb{F}_p^*$ and nonprincipal multiplicative characters χ of $\mathbb{F}_p$.

Furthermore, we also consider double sums

$$T_\chi(a, \mathcal{G}) = \sum_{\lambda, \mu \in \mathcal{G}} \chi(a + \lambda + \mu), \qquad 1 \leq a < p - 1,$$

where both variables run over a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$.

Using recent estimates of Shkredov [28] on the so-called *additive energy* of multiplicative subgroups we also estimate them below the obvious range $T \geq p^{1/2}$, where $T = \#\mathcal{G}$, given by the estimate

$$|T_\chi(a, \mathcal{G})| \leq Tp^{1/2},$$

which follows from (2).

Theorem 4. *Let $T \le p^{2/3}$. Then for the multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order T, we have*

$$|T_\chi(a,\mathcal{G})| \le \begin{cases} T^{19/26}p^{1/2+o(1)}, & \text{if } T \le p^{1/2}, \\ T^{9/13}p^{27/52+o(1)}, & \text{if } p^{1/2} < T \le p^{29/48}, \\ Tp^{1/3+o(1)}, & \text{if } p^{29/48} < T \le p^{2/3}, \end{cases}$$

uniformly over $a \in \mathbb{F}_p^*$ and nonprincipal multiplicative characters χ of $\mathbb{F}_p$.

Note that Theorem 4 nontrivial provided that $T \ge p^{13/33+\varepsilon}$ for some fixed $\varepsilon > 0$.

We also give an application of Theorem 4 to primitive roots modulo p with few non-zero binary digits. More precisely, let u_p denote the smallest u such that there exists a primitive root modulo p with u_p non-zero binary digits. It is shows in [16, Theorem 5] that $u_p \le 2$ for all but $o(Q/\log Q)$ primes $p \le Q$, as $Q \to \infty$ (note that in [16] the result is formulated only for quadratic non-residues but it is easy to see that the argument also holds for primitive roots). Instead of $o(Q/\log Q)$, can obtain a slightly more explicit but still rather weak bound on the size of the exceptional set. Here we show that Theorem 4 implies a rather strong bound on the set of primes $p \le Q$ for which $u_p \le 3$ does not hold.

Theorem 5. *For all but at most $Q^{26/33+o(1)}$ primes $p \le Q$, we have $u_p \le 3$ as $Q \to \infty$.*

We also note that one may attempt to treat the sums $S_\chi(a,\mathcal{I},\mathcal{G})$ and $T_\chi(a,\mathcal{G})$ within the general theory of double sums of multiplicative characters, see [6, 7, 11, 12, 15, 21, 22, 23] and references therein. However it seems that none of the presently known results implies a nontrivial estimate in the range of Theorems 1 and 4.

2. Preparations

2.1. **Notation and general conventions.** Throughout the paper, p always denotes a sufficiently large prime number and χ denotes an non-principal multiplicative character modulo p. We assume that $\mathbb{F}_p$ is represented by the set $\{0,\ldots,p-1\}$.

Furthermore, $\mathcal{G}$ always denotes a multiplicative subgroup of $\mathbb{F}_p^*$ of order $\#\mathcal{G} = T$ and $\mathcal{I}$ always denotes the set $\mathcal{I} = \{1,\ldots,H\}$.

We also assume that $f \in \mathbb{F}_p[X]$ is a of degree $d \ge 1$. In particular, f is not a constant.

The notations $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \le cV$ with some constant $c > 0$ that may depend on the real parameter $\varepsilon > 0$ and the integer parameters $d \ge 1$ and $\nu \ge 1$ and is absolute otherwise.

In particular, all our estimates are uniform with respect to the polynomial f and the character χ.

2.2. **Bounds of some exponential and character sums.** First we recall the classical result of Davenport and Erdős [13], which follows from the Weil bound of multiplicative character sums, see [20, Theorem 11.23].

Lemma 6. *For a fixed integer $\nu \ge 1$ and an integer $R < p$, we have*

$$\sum_{v \in \mathbb{F}_p} \left| \sum_{r=1}^{R} \chi\left(v + r\right) \right|^{2\nu} \ll R^{2\nu} p^{1/2} + R^{\nu} p.$$

The following result is a version of Lemma 6 with $\nu = 1$ which is slightly more precise in this case.

Lemma 7. *For any set $\mathcal{V} \subseteq \mathbb{F}_p$ and complex numbers α_v of such that $|\alpha_v| \le 1$ for $v \in \mathcal{V}$, we have*

$$\sum_{u \in \mathbb{F}_p} \left| \sum_{v \in \mathcal{V}} \chi(u + v) \right|^2 \ll \#\mathcal{V} p.$$

Proof. Denoting by $\overline{\chi}$ the conjugate character and recalling that $\overline{\chi}(w) = \chi(w^{-1})$ for $w \in \mathbb{F}_p^*$, we obtain

$$\sum_{u \in \mathbb{F}_p} \left| \sum_{v \in \mathcal{V}} \chi(u + v) \right|^2 = \sum_{v,w \in \mathcal{V}} \alpha_v \overline{\alpha}_w \sum_{u \in \mathbb{F}_p} \chi(u + v)\overline{\chi}(u + w).$$

If $v = w$ the inner sum is equal to $p - 1$. So the total contribution from such terms is $O(Mp)$. Otherwise, we derive

$$\begin{aligned} \sum_{u \in \mathbb{F}_p} \chi(u + v)\overline{\chi}(u + w) &= \sum_{u \in \mathbb{F}_p} \chi(u + v - w)\overline{\chi}(u) \\ &= \sum_{u \in \mathbb{F}_p^*} \chi(u + v - w)\overline{\chi}(u) = \sum_{u \in \mathbb{F}_p^*} \chi\left(1 + (v - w)u^{-1}\right) \\ &= \sum_{u \in \mathbb{F}_p^*} \chi\left(1 + u\right) = \sum_{u \in \mathbb{F}_p} \chi\left(1 + u\right) - \chi(1) = -\chi(1). \end{aligned}$$

So the total contribution from such terms is $O(M^2) = O(Mp)$ and the result follows. □

We also need the following bound of Bourgain [2, Theorem 1].

Lemma 8. *For every fixed real $\varepsilon > 0$ and integer $r \ge 1$ there is some $\xi > 0$ such that for any integers $k_1, \ldots, k_r \ge 1$ with*

$$\gcd(k_i, p-1) < p^{1-\varepsilon}, \qquad \text{and} \qquad \gcd(k_i - k_j, p-1) < p^{1-\varepsilon},$$

for $i, j = 1, \ldots, r$, $i \ne j$, uniformly over the coefficients $a_1, \ldots, a_r \in \mathbb{F}_p$, not all equal to zero, we have

$$\sum_{x=1}^{p-1} \exp\left(\frac{2\pi i}{p}\left(a_1 x^{k_1} + \ldots + a_r x^{k_r}\right)\right) \ll p^{1-\xi}.$$

Clearly for any $F \in \mathbb{F}_p[X]$ and a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $\#\mathcal{G} = T$ we have

$$\frac{1}{\#\mathcal{G}} \sum_{\lambda \in \mathcal{G}} \exp\left(\frac{2\pi i}{p} F(\lambda)\right) = \frac{1}{p-1} \sum_{x=1}^{p-1} \exp\left(\frac{2\pi i}{p} F(x^{(p-1)/T})\right) \ll p^{-\xi}.$$

so we derive from Lemma 8:

Corollary 9. *For every fixed real $\varepsilon > 0$ and integer $d \ge 1$ there is some $\xi > 0$ such that for $T \ge p^{\varepsilon}$, uniformly over $a \in \mathbb{F}_p^*$, we have*

$$\sum_{\lambda \in \mathcal{G}} \exp\left(\frac{2\pi i}{p} a f(\lambda)\right) \ll T p^{-\xi}.$$

2.3. **Bound on the number of solutions to some congruences.** First we note that combining Corollary 9 with the *Erdős-Turán inequality* (see, for example, [14, Theorem 1.21]) that relates the uniformity of distribution to exponential sums, we immediately obtain:

Lemma 10. *For every fixed real $\varepsilon > 0$ and integer $r \ge 1$ there is some $\kappa > 0$ such that for $T \ge p^{\varepsilon}$, we have*

$$\#\{\lambda \in \mathcal{G} \ : \ f(\lambda) \equiv b + x \pmod p, \ \text{where } x \in \mathcal{I}\} = \frac{HT}{p} + O\left(T^{1-\kappa}\right),$$

uniformly over $b \in \mathbb{F}_p$.

Let $N(\mathcal{I}, \mathcal{G})$ be the number of solutions to the congruence

$$\lambda x \equiv y \pmod p, \qquad x, y \in \mathcal{I}, \ \lambda \in \mathcal{G}.$$

Some of our results rely on an upper bound on $N(\mathcal{I}, \mathcal{G})$ which is given in [9, Theorem 1], see also [10] for some other bounds.

Lemma 11. *Let $\nu \ge 1$ be a fixed integer. Then*

$$N(\mathcal{I}, \mathcal{G}) \le H t^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + H^2 t^{1/\nu} p^{-1/\nu+o(1)},$$

as $p \to \infty$, *where*

$$t = \max\{T, p^{1/2}\}.$$

We also use the following bound which is due to Ayyad, Cochrane and Zheng [1, Theorem 1].

Lemma 12. *Let* $\mathcal{J}_i = \{b_i+1, \ldots, b_i+h_i\}$ *for some integers* $p > h_i+b_i > b_i \geq 1$, $i = 1, 2, 3, 4$. *Then*

$$\#\{(x_1, x_2, x_3, x_4) \in \mathcal{J}_1 \times \mathcal{J}_2 \times \mathcal{J}_3 \times \mathcal{J}_4 \ : \ x_1x_2 \equiv x_3x_4 \pmod p\} = \frac{1}{p} h_1h_2h_3h_4 + O\left((h_1h_2h_3h_4)^{1/2} (\log p)^2\right).$$

We now fix some real $L > 1$ and denote by $\mathcal{L}$ the set of primes of the interval $[L, 2L]$. We need an upper bound on the quantity

$$W = \#\Big\{(u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \mathcal{I}^2 \times \mathcal{L}^2 \times \mathcal{S}^2 \ : \ \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p\Big\} \tag{3}$$

for some special class of sets.

We say that a set $\mathcal{S} \subseteq \mathbb{F}_p$ is h-spaced if no elements $s_1, s_2 \in \mathcal{S}$ and positive integer $k \leq h$ satisfy the equality $s_1 + k = s_2$.

The following result is given in [11] and is based on some ideas of Shao [27].

Lemma 13. *If* $L < H$ *and* $2HL < p$ *then for any* H*-spaced set* $\mathcal{S}$ *for* W, *given by* (3) *we have*

$$W \ll \frac{(\#\mathcal{S}HL)^2}{p} + \#\mathcal{S}HLp^{o(1)}.$$

We also define

$$U = \sum_{v \in \mathbb{F}_p} U(v)^2, \tag{4}$$

where

$$U(v) = \#\left\{(u, \ell, \lambda) \in \mathcal{I} \times \mathcal{L} \times \mathcal{G} \ : \ \frac{u + f(\lambda)}{\ell} \equiv v \pmod p\right\}. \tag{5}$$

Lemma 14. *For every fixed real* $\varepsilon > 0$ *and integer* $d \geq 1$ *there are some* $\delta >$ *and* $\eta > 0$ *such that if*

$$T > p^{\varepsilon} \qquad \text{and} \qquad p^{1/2-\varepsilon} \geq H \geq L$$

then for U, *given by* (4) *we have*

$$U \ll HLT^2p^{-\eta}.$$

Proof. Let $\mathcal{S}_1$ be the largest H-separated subset of $\mathcal{F}_0 = \{f(\lambda) \ : \ \lambda \in \mathcal{G}\}$. By Lemma 10 we have $\#\mathcal{S}_1 \gg p^{\kappa}$ for some fixed $\kappa > 0$.

Inductively, we define $\mathcal{S}_{k+1}$ as the largest H-separated subset of

$$\mathcal{F}_k = \mathcal{F}_{k-1} \setminus \bigcup_{j=1}^{k} \mathcal{S}_j, \qquad k = 1, 2, \ldots.$$

Clearly for some $b \in \mathbb{F}_p$ and a set $\mathcal{J} = \{b+1, \ldots, b+H\}$ we have

$$\#\left(\mathcal{F}_k \cap \mathcal{J}\right) \geq \frac{\#\mathcal{F}_k}{\#\mathcal{F}_{k+1}}.$$

On the other hand, by Lemma 10

$$\#\left(\mathcal{F}_k \cap \mathcal{J}\right) \leq \#\left(\mathcal{F}_1 \cap \mathcal{J}\right) \ll Tp^{-\kappa}.$$

Hence there is a partition

$$\mathcal{F}_0 = \bigcup_{k=0}^{K} \mathcal{S}_k$$

into disjoined sets with $K \leq Tp^{-\kappa/2}$ such that

- $\#\mathcal{S}_0 \leq Tp^{-\kappa/2}$,
- $\mathcal{S}_k$ is H-separated with $\#\mathcal{S}_k \geq p^{\kappa/2}$, $k = 1, \ldots, K$.

For $k = 0, \ldots, K$ we define

$$U_k(v) = \# \left\{ (u, \ell, s) \in \mathcal{I} \times \mathcal{L} \times \mathcal{S}_k \ : \ \frac{u+s}{\ell} \equiv v \pmod p \right\}.$$

We have

$$U(v) = \sum_{k=0}^{K} U_k(v) = U_0(v) + \sum_{k=1}^{K} U_k(v).$$

So, squaring out and summing over all $v \in \mathbb{F}_p$, we obtain

$$\begin{aligned} U &\ll \sum_{v \in \mathbb{F}_p} U_0(v)^2 + \sum_{v \in \mathbb{F}_p} \left(\sum_{k=1}^{K} U_k(v) \right)^2 \\ &= \sum_{v \in \mathbb{F}_p} U_0(v)^2 + \sum_{v \in \mathbb{F}_p} \sum_{k,m=1}^{K} U_k(v) U_m(v). \end{aligned}$$

Now, changing the order of summation in the second term in the above and then using the Cauchy inequality, yields

$$U \ll V_1 + V_2^2, \tag{6}$$

where

$$V_1 = \sum_{v \in \mathbb{F}_p} U_0(v)^2 \qquad \text{and} \qquad V_2 = \sum_{k=1}^{K} \left(\sum_{v \in \mathbb{F}_p} U_k(v)^2 \right)^{1/2}.$$

We have,

$$\begin{aligned} V_1 &= \#\Big\{(u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \mathcal{I}^2 \times \mathcal{L}^2 \times \mathcal{S}_0^2 \ : \\ &\qquad\qquad \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p \Big\} \\ &\le \max_{s_1, s_2 \in \mathbb{F}_p} \#\Big\{(u_1, u_2, \ell_1, \ell_2) \in \mathcal{I}^2 \times \mathcal{L}^2 \ : \\ &\qquad\qquad \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p \Big\}. \end{aligned}$$

Since $L \le H \le p^{1/2-\varepsilon}$, by Lemma 12 we obtain

$$V_1 \ll (\#\mathcal{S}_0)^2 HL(\log p)^2 \ll HLT^2 p^{-\varepsilon} (\log p)^2. \tag{7}$$

Furthermore, Lemma 13 implies that for $k = 1, \ldots, K$ we have

$$\sum_{v \in \mathbb{F}_p} U_k(v)^2 \ll (\#\mathcal{S}_k HL)^2 p^{-1} + \#\mathcal{S}_k HL p^{o(1)}.$$

Hence, applying the Cauchy inequality, we derive

$$\begin{aligned} V_2 &\ll \sum_{k=1}^{K} \left(\#\mathcal{S}_k HL p^{-1/2} + (\#\mathcal{S}_k)^{1/2} H^{1/2} L^{1/2} p^{o(1)} \right) \\ &\le HLTp^{-1/2} + H^{1/2} L^{1/2} p^{o(1)} \sum_{k=1}^{K} (\#\mathcal{S}_k)^{1/2} \\ &\le HLTp^{-1/2} + H^{1/2} L^{1/2} p^{o(1)} \left(K \sum_{k=1}^{K} \#\mathcal{S}_k \right)^{1/2} \\ &\le HLTp^{-1/2} + H^{1/2} K^{1/2} L^{1/2} T^{1/2} p^{o(1)}. \end{aligned}$$

Since $K \le Tp^{-\kappa/2}$ and $L \le H \le p^{1/3}$, we see that

$$V_2 \ll HLTp^{-1/2} + H^{1/2} L^{1/2} T p^{-\kappa/2 + o(1)} \le H^{1/2} L^{1/2} T p^{-\kappa/2 + o(1)} \tag{8}$$

(assuming that κ is small enough). Substituting (7) and (8) in (6), leads us to the bound

$$U \ll HLT^2 p^{-\varepsilon} \log p + HLT^2 p^{-\kappa + o(1)}$$

and the result follows. □

Let $E(\mathcal{G})$ be the additive energy of a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, that is

$$E(\mathcal{G}) = \#\{(\lambda_1, \mu_1, \lambda_2, \mu_2) \in \mathcal{G}^4 \ : \ \lambda_1 + \mu_1 = \lambda_2 + \mu_2\}.$$

By a result of Heath-Brown and Konyagin [19], if $\#\mathcal{G} = T \le p^{2/3}$ we have

$$E(\mathcal{G}) \ll T^{5/2}.$$

Recently, Shkredov [28] has given an improvement which we present in the following slightly less precise form (which supreses logarithmic factors in $p^{o(1)}$).

Lemma 15. *For $T \le p^{2/3}$ we have*

$$E(\mathcal{G}) \le \begin{cases} T^{32/13}p^{o(1)}, & \text{if } T \le p^{1/2}, \\ T^{31/13}p^{1/26+o(1)}, & \text{if } p^{1/2} < T \le p^{29/48}, \\ T^3p^{-1/3+o(1)}, & \text{if } p^{29/48} < T \le p^{2/3}. \end{cases}$$

.

3. Proofs of main results

3.1. **Proof of Theorem 1.** We have

$$S_\chi(a, \mathcal{I}, \mathcal{G}) = \frac{1}{T}W, \tag{9}$$

where

$$W = \sum_{x \in \mathcal{I}} \sum_{\lambda, \mu \in \mathcal{G}} \overline{\chi}(\mu)\chi(\mu x + a\lambda).$$

(since $\overline{\chi}(\mu) = \chi(\mu^{-1})$ for $\mu \in \mathbb{F}_p^*$). Hence

$$|W| \le \sum_{x \in \mathcal{I}} \sum_{\lambda, \mu \in \mathcal{G}} \left| \sum_{\lambda \in \mathcal{G}} \chi(x\mu + a\lambda) \right|.$$

Collecting the products μx with the same value $u \in \mathbb{F}_p$, we obtain

$$|W| \le \sum_{u \in \mathbb{F}_p} R(u) \left| \sum_{\lambda \in \mathcal{G}} \chi(u + a\lambda) \right|,$$

where

$$R(u) = \#\{(x, \mu) \in \mathcal{I} \times \mathcal{G} \ : \ \mu x = u\}.$$

So, by the Cauchy inequality,

$$|W|^2 \le \sum_{u \in \mathbb{F}_p} R(u)^2 \sum_{u \in \mathbb{F}_p} \left| \sum_{\lambda \in \mathcal{G}} \chi(u + a\lambda) \right|^2.$$

Thus applying Lemma 7 we derive

$$W^2 \le pT \sum_{u \in \mathbb{F}_p} R(u)^2.$$

Clearly

$$\sum_{u \in \mathbb{F}_p} R(u)^2 = Q,$$

where

$$Q = \#\{(x, y, \lambda, \mu) \in \mathcal{I} \times \mathcal{I} \times \mathcal{G} \times \mathcal{G} \ : \ \lambda x = \mu y\}.$$

Furthermore, it is clear that $Q = TN(\mathcal{I}, \mathcal{G})$, where $N(\mathcal{I}, \mathcal{G})$ is as in Lemma 11. Putting everything together and using the bound of Lemma 11, we see that for any fixed $\nu \ge 1$ we have

$$W^2 \le pT^2 \left(Ht^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + H^2 t^{1/\nu} p^{-1/\nu+o(1)}\right), \tag{10}$$

where

$$t = \max\{T, p^{1/2}\}.$$

We can certainly assume that $T \le p^{1/2+\varepsilon}$ as otherwise the result follows from the bound (2). Thus $t \le p^{1/2+\varepsilon}$ and we obtain

$$W^2 \le pT^2 \left(Hp^{1/4\nu(\nu+1)+\varepsilon(2\nu+1)/2\nu(\nu+1)+o(1)} + H^2 p^{-1/2\nu+\varepsilon/\nu+o(1)}\right).$$

Since $H \ge p^{\varepsilon}$, taking a sufficiently large ν we can achieve the inequality

$$Hp^{1/4\nu(\nu+1)+\varepsilon(2\nu+1)/2\nu(\nu+1)} \le H^2 p^{-1/2\nu+\varepsilon/\nu}.$$

We can also assume that $\varepsilon < 1/3$ as otherwise the result follows from the Burgess bound, see [20, Theorem 12.6], so the bound becomes

$$W^2 \le H^2 T^2 p^{1-1/6\nu+o(1)} \ll H^2 T^2 p^{1-1/7\nu}.$$

Recalling (9), we obtain

$$S_\chi(a, \mathcal{I}, \mathcal{G}) \ll Hp^{1/2-1/7\nu} \le HTp^{-1/14\nu}$$

for $T \ge p^{1/2-1/14\nu}$.

3.2. **Proof of Theorem 2.** Clearly we can assume that $H < p^{1/3}$ as otherwise the Burgess bound, (see [20, Theorem 12.6]) implies the desired result. We can also assume that $\varepsilon > 0$ is small enough, thus the conditions of Lemma 14 are satisfied.

We set

$$\gamma = \eta/3,$$

where η is as in Lemma 14 (which we assume to e sufficiently small).

Let $L = Hp^{-2\gamma}$, $R = \lceil p^{\gamma} \rceil$,and let $\mathcal{L}$ be the set of primes of the interval $[L, 2L]$.

Clearly

$$\mathfrak{S}_\chi(f,\mathcal{I},\mathcal{G}) = \frac{1}{\#\mathcal{L}R}\Sigma + O(LRT) = \frac{1}{\#\mathcal{L}R}\Sigma + O(HTp^{-\gamma}), \tag{11}$$

where

$$\begin{aligned}\Sigma &= \sum_{\ell\in\mathcal{L}}\sum_{r=1}^{R}\sum_{x\in\mathcal{I}}\sum_{\lambda\in\mathcal{G}}\chi(x+f(\lambda)+\ell r)\\ &\le \sum_{\ell\in\mathcal{L}}\sum_{x\in\mathcal{I}}\sum_{\lambda\in\mathcal{G}}\left|\sum_{r=1}^{R}\chi\left(\frac{x+f(\lambda)}{\ell}+r\right)\right| = \sum_{v\in\mathbb{F}_p}U(v)\left|\sum_{r=1}^{R}\chi\left(v+r\right)\right|,\end{aligned}$$

where $U(v)$ is given by (5). We now fix some integer $\nu \ge 1$ Writing $U(v) = U(v)^{(\nu-1)/\nu}(U(v)^2)^{1/2\nu}$ and using the Hölder inequality, we derive

$$\Sigma^{2\nu} = \left(\sum_{v\in\mathbb{F}_p}U(v)\right)^{2\nu-2}\sum_{v\in\mathbb{F}_p}U(v)^2\sum_{v\in\mathbb{F}_p}\left|\sum_{r=1}^{R}\chi\left(v+r\right)\right|^{2\nu}.$$

We obviously have

$$\sum_{v\in\mathbb{F}_p}U(v) \le H\#\mathcal{L}T \ll HLT.$$

Hence, using Lemmas 6 and 14 we derive

$$\Sigma^{2\nu} \ll (HLT)^{2\nu-2}HLT^2\left(R^{2\nu}p^{1/2}+R^{\nu}p\right).$$

Taking ν sufficiently large (depending on γ), we arrive to the inequality

$$\Sigma^{2\nu} \ll (HL)^{2\nu-1}T^{2\nu}R^{2\nu}p^{1/2-\eta} = (HLRT)^{2\nu}(HL)^{-1}p^{1/2-\eta}. \tag{12}$$

So taking $\delta = \kappa/4$, we see that

$$(HL)^{-1}p^{1/2-\eta} = H^{-2}p^{1/2-2\eta/3} \le p^{-\eta/6}.$$

Hence we infer from (12) that $\Sigma \ll (HLRT)p^{-\eta/12\nu}$, which after substitution in (11) concludes the proof.

3.3. **Proof of Theorem 3.** We proceed as before and use that $t, T = p^{1/2+o(1)}$, so (10) becomes

$$W^2 \le p^2\left(p^{1/4+1/4\nu(\nu+1)+o(1)}+p^{1/2-1/2\nu+o(1)}\right).$$

Taking $\nu = 2$ we obtain

$$W^2 \le p^2\left(p^{1/4+1/24+o(1)}+p^{1/4+o(1)}\right) = p^{55/24+o(1)},$$

which after substitution in (9) implies the result.

3.4. **Proof of Theorem 4.** As before, we have

$$T_\chi(a, \mathcal{G}) = \frac{1}{T} W, \tag{13}$$

where

$$W = \sum_{\lambda,\mu,\vartheta \in \mathcal{G}} \overline{\chi}(\vartheta)\chi(a\vartheta + \mu + \lambda).$$

Hence

$$|W| \le \sum_{\lambda,\mu \in \mathcal{G}} \left| \sum_{\vartheta \in \mathcal{G}} \overline{\chi}(\vartheta)\chi(a\vartheta + \lambda + \mu) \right|.$$

Collecting the sum $\lambda + \mu$ with the same value $u \in \mathbb{F}_p$, we obtain

$$|W| \le \sum_{u \in \mathbb{F}_p} F(u) \left| \sum_{\lambda \in \mathcal{G}} \chi(a\vartheta + \lambda + \mu) \right|,$$

where

$$F(u) = \#\{(\lambda, \mu) \in \mathcal{G}^2 \ : \ \lambda + \mu = u\}.$$

So, as in the proof of Theorem 1 we obtain

$$W^2 \le pT \sum_{u \in \mathbb{F}_p} R(u)^2 = pTE(\mathcal{G}).$$

Recalling Lemma 15 and using (13), we conclude the proof.

3.5. **Proof of Theorem 5.** Let us fix an arbitrary $\varepsilon > 0$. Let ℓ_p denote the multiplicative order of 2 modulo p. We see from Theorem 4 that if for a sufficiently large prime p we have $\ell_p \ge p^{13/33+\varepsilon}$ then

$$\sum_{1 \le k < m \le \ell_p} \chi(2^m + 2^k + 1) = \sum_{k,m=1}^{\ell_p} \chi(2^m + 2^k + 1) + O(\ell_p) = O(\ell_p^{2-\delta}).$$

Using a standard method of detecting primitive roots via multiplicative charactes, we conclude that if for a sufficiently large prime p we have $\ell_p \ge p^{13/33+\varepsilon}$ then $u_p \le 3$. It remains to estimate the number of primes $p \le Q$ with $\ell_p \ge p^{13/33+\varepsilon}$. Let $L = Q^{13/33+\varepsilon}$. Clearly for every such prime we have $p \mid W$ where

$$W = \prod_{\ell \le L} (2^\ell - 1) \le 2^{L(L+1)/2}.$$

Since W has $O(\log W) = O(L^2) = O(Q^{26/33+2\varepsilon})$ prime divisors and since ε is arbitrary, the result now follows.

4. Comments

It is easy to see that the full analogues of Theorems 1 and 2 can also be obtained for the sums

$$\sum_{x\in\mathcal{I}}\sum_{\lambda\in\mathcal{G}}\chi\left(\lambda x+a\right), \qquad 1\le a<p-1,$$

without any changes in the proof. Using a version of Lemma 11 given in [26, Lemma 9], one can also obtain analogues of our results for sums over the consecutive powers $g,\ldots,g^N$ of a fixed element $g\in\mathbb{F}_p^*$, provided that N is smaller than the multiplicative order of g modulo p and in the same ranges as T in Theorems 1 and 2.

Furthermore, without any changes in the proof, Theorem 2 can extended to the double sums

$$\sum_{x\in\mathcal{I}}\sum_{u\in\mathcal{U}}\chi\left(ax+u\right), \qquad 1\le a<p-1,$$

where $\mathcal{U}\subseteq\mathbb{F}_p$ is an arbitrary set of cardinality $U\ge p^{\varepsilon}$ and an interval $\mathcal{I}$ of length $H\le p^{1/3}$, such that for some $\kappa>0$ we have

$$\#\{u\in\mathcal{U}\ :\ u\equiv b+x \pmod p,\ \text{where } x\in\mathcal{I}\}\ll U^{1-\kappa}$$

(which replaces Lemma 10 in our argument).

It is also interesting to estimate sums

$$\sum_{x\in\mathcal{I}}\sum_{\lambda\in\mathcal{G}}\chi\left(f(x)+\lambda\right), \qquad 1\le a<p-1, \tag{14}$$

with a nontrivial polynomial $f(X)\in\mathbb{F}_p[X]$, for $H>p^{1/2-\eta}$ and $\#\mathcal{G}>p^{1/2-\eta}$ for some fixed $\eta>0$ (depending only on $\deg f$). To estimate these sums, one needs a nontrivial bound on the number of solutions to the congruence

$$\lambda f(x)\equiv f(y) \pmod p, \qquad x,y\in\mathcal{I},\ \lambda\in\mathcal{G},$$

which is better than H^2. In fact, using some ideas and results of [18, 30] one can get such a bound, but not in a range in which the sums (14) can be estimated nontrivially.

Finally, it is interesting to investigate whether one can estimate the sums

$$\sum_{\lambda_1,\ldots,\lambda_\nu\in\mathcal{G}}\chi(a+\lambda_1+\ldots+\lambda_\nu), \qquad 1\le a<p-1,$$

with $\nu\ge 3$ in a shorter range than that of Theorem 4 by using bounds on the higher order additive energy of multiplicative subgroups, see [28, 29] for such bounds. Clearly, for any $\varepsilon>0$ if $\#\mathcal{G}>p^{\varepsilon}$ then for a sufficiently large ν such a result follows instantly from [8], as if ν is large enough, the sums $\lambda_1+\ldots+\lambda_\nu$, $\lambda_1,\ldots,\lambda_\nu\in\mathcal{G}$, represent each

element of $\mathbb{F}_p$ with the asymptotically equal frequency. We however hope that the approach via the higher order additive energy can lead to better estimates for smaller values of ν and ε.

Acknowledgements

During the preparation of this paper, the first author was supported by the NSF Grants DMS 1301608 and by the NSF Grant 0932078000 while she was in residence at the Mathematical Science Research Institute in Berkeley, California, during the spring 2014 semester. This author would also like to thank the Mathematics Department of the University of California at Berkeley for its hospitality.

The second author was supported by the ARC Grant DP130100237. This author would also to thank the Max Planck Institute for Mathematics, Bonn, for support and hospitality during his work on this project.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums', *J. Number Theory*, **59** (1996), 398–413.

[2] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.*, **18** (2005), 477–499.

[3] J. Bourgain, 'On the distribution of the residues of small multiplicative subgroups of $\mathbb{F}_p$', *Israel J. Math.*, **172** (2009), 61–74.

[4] J. Bourgain, 'Sum-product theorems and applications', *Additive Number Theory*, Springer-Verlag, Berlin, 2010, 9–38.

[5] J. Bourgain, 'On exponential sums in finite fields', *An Irregular Mind*, Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest, 2010, 219–242.

[6] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comp.*, **41** (2012), 1524–1557.

[7] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Math. Inst.*, **280** (2013), 67–96.

[8] 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. Lond. Math. Soc.*, **73** (2006), 380–398.

[9] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Res. Notices*, **2008** (2008), Article rnn090, 1–29. (Corrigenda: *Intern. Math. Res. Notices*, **2009** (2009), 3146–3147).

[10] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Intern. Math. Res. Notices*, **2012** (2012), Article rnn097, 1968–2009.

[11] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Character sums and deterministic polynomial root finding in finite fields', *Preprint*, 2013 (available from `http://arxiv.org/abs/1308.4803`).

[12] M.-C. Chang, 'On a question of Davenport and Lewis and new character sum bounds in finite fields', *Duke Math. J.*, **145** (2008), 409–442.

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

[14] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[15] J. B. Friedlander and H. Iwaniec, 'Estimates for character sums', *Proc. Amer. Math. Soc.*, **119** (1993), 365–372.

[16] R. Dietmann, C. Elsholtz and I. E. Shparlinski, 'On gaps between quadratic non-residues in the Euclidean and Hamming metrics', *Indagationes Mathematicae*, **24** (2013), 930–938.

[17] M. Z. Garaev, 'Sums and products of sets and estimates of rational trigonometric sums in fields of prime order', *Russian Math. Surveys*, **65** (2010), 599–658 (Transl. from *Uspekhi Mat. Nauk*).

[18] D. Gómez-Pérez and I. E. Shparlinski, 'Subgroups generated by polynomials in finite fields', *Preprint*, 2013 (available from `http://arxiv.org/abs/1309.7378`).

[19] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Quart. J. Math.*, **51** (2000), 221–235.

[20] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[21] A. A. Karatsuba, 'The distribution of values of Dirichlet characters on additive sequences', *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).

[22] A. A. Karatsuba, 'Weighted character sums', *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izv. Math.)*, **64**(2) (2000), 29–42 (in Russian).

[23] A. A. Karatsuba, 'Arithmetic problems in the theory of Dirichlet characters', *Uspekhi Mat. Nauk. (Transl. as Russian Math. Surveys)*, **63**(4) (2008), 43–92 (in Russian).

[24] B. Kerr, 'Incomplete exponential sums over exponential functions', *Preprint*, 2013, (available from `http://arxiv.org/abs/1302.4170`).

[25] S. V. Konyagin, 'Bounds of exponential sums over subgroups and Gauss sums', *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).

[26] S. V. Konyagin and I. E. Shparlinski, 'On the consecutive powers of a primitive root: Gaps and exponential sums', *Mathematika*, **58** (2012), 11–20.

[27] X. Shao, 'Character sums over unions of intervals', *Preprint*, 2013 (available from `http://arxiv.org/abs/1302.0348`).

[28] I. D. Shkredov, 'Some new inequalities in additive combinatorics', *Moscow J. Comb. and Number Theory*, (to appear).

[29] I. D. Shkredov, 'On exponential sums over multiplicative subgroups of medium size', *Preprint*, 2013 (available from `http://arxiv.org/abs/1311.5726`).

[30] I. E. Shparlinski, 'Polynomial values in small subgroups of finite fields', *Preprint*, 2014 (available from `http://arxiv.org/abs/1401.0964`).

Department of Mathematics, University of California, Riverside, CA 92521, USA
E-mail address: mcc@math.ucr.edu

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au