Proceedings of the Edinburgh Mathematical Society (2010) **53**, 1–12 ©
DOI:10.1017/S0013091508000771 Printed in the United Kingdom

BILINEAR CHARACTER SUMS AND SUM–PRODUCT PROBLEMS ON ELLIPTIC CURVES

OMRAN AHMADI[1*] AND IGOR SHPARLINSKI[2]

[1] *Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[2] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia* (igor@comp.mq.edu.au)

(Received 30 July 2008)

Abstract Let $\boldsymbol{E}$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ of q elements. We improve a bound on bilinear additive character sums over points on $\boldsymbol{E}$, and obtain its analogue for bilinear multiplicative character sums. We apply these bounds to some variants of the sum–product problem on $\boldsymbol{E}$.

Keywords: sum–product problem; elliptic curves; character sums

2000 *Mathematics subject classification:* Primary 11G05; 11L07; 11T23

1. Introduction

We fix an ordinary elliptic curve $\boldsymbol{E}$ over a finite field $\mathbb{F}_q$ of q elements.

We assume that $\boldsymbol{E}$ is given by an affine Weierstrass equation

$$\boldsymbol{E} : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6,$$

with some $a_1, \ldots, a_6 \in \mathbb{F}_q$ [**20**].

We recall that the set of all points on $\boldsymbol{E}$ forms an abelian group, with the point at infinity $\mathcal{O}$ as the neutral element. As usual, we write every point $Q \neq \mathcal{O}$ on $\boldsymbol{E}$ as $Q = (x(Q), y(Q))$.

Let $\boldsymbol{E}(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on $\boldsymbol{E}$ and let $P \in \boldsymbol{E}(\mathbb{F}_q)$ be a fixed point of order T.

Let $\mathbb{Z}_T$ denote the residue ring modulo T and let $\mathbb{Z}_T^*$ be its unit group.

We use the ideas of Garaev and Karatsuba [**8**] to improve the bound of [**1**] on bilinear sums of additive characters with $x(kmP)$ as argument, where k and m run through arbitrary sets $\mathcal{K}, \mathcal{M} \subseteq \mathbb{Z}_T^*$. We also use a result of Chen [**4**], which in turn is based on a result of Perret [**16**], to estimate similar bilinear sums of multiplicative characters.

* Present address: Claude Shannon Institute, University College Dublin, Dublin 4, Ireland (omran.ahmadi@ucd.ie).

We combine this bound with an argument of Garaev [**7**] to study two versions of the sum–product problem on $\boldsymbol{E}$. We show that, for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$, at least one of the sets

$$\left.\begin{aligned} \mathcal{S} &= \{x(aP) + x(bP) : a \in \mathcal{A},\ b \in \mathcal{B}\},\\ \mathcal{T} &= \{x(abP) : a \in \mathcal{A},\ b \in \mathcal{B}\} \end{aligned}\right\} \tag{1.1}$$

is large. Furthermore, in some ranges of $\#\mathcal{A}$, $\#\mathcal{B}$ and T we obtain a matching lower bound.

Finally, we also show that at least one of the sets

$$\left.\begin{aligned} \mathcal{X} &= \{x(aP)x(bP) : a \in \mathcal{A},\ b \in \mathcal{B}\},\\ \mathcal{Y} &= \{x(abP) : a \in \mathcal{A},\ b \in \mathcal{B}\} \end{aligned}\right\} \tag{1.2}$$

is large.

These problems are motivated by a series of recent results on the sum–product problem over $\mathbb{F}_q$, which assert that, for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$, at least one of the sets

$$\mathcal{G} = \{a + b : a \in \mathcal{A},\ b \in \mathcal{B}\} \quad \text{and} \quad \mathcal{H} = \{ab : a \in \mathcal{A},\ b \in \mathcal{B}\}$$

is large (see [**2**,**3**,**6**,**7**,**10**–**13**,**19**] for the background, various modifications of the original problem and further references).

We note that yet another variant of the sum–product problem for elliptic curves has recently been considered in [**18**] (which in turn is based on the estimate of some other bilinear character sums given in [**17**]). It is shown in [**18**] that, for sets $\mathcal{P}, \mathcal{Q} \subseteq \boldsymbol{E}(\mathbb{F}_q)$, at least one of the sets

$$\{x(P) + x(Q) : P \in \mathcal{P},\ Q \in \mathcal{Q}\} \quad \text{and} \quad \{x(P \oplus Q) : P \in \mathcal{P},\ Q \in \mathcal{Q}\} \tag{1.3}$$

is large, where $\oplus$ denotes the group operation on the points of $\boldsymbol{E}$.

Throughout the paper, the implied constants in the symbols 'O' and '$\ll$' may depend on an integer parameter $\nu \geqslant 1$. We recall that $X \ll Y$ and $X = O(Y)$ are both equivalent to the inequality $|X| \leqslant cY$ with some constant $c > 0$.

2. Bilinear sums over elliptic curves

Let ψ and φ be a non-trivial additive character and a non-trivial multiplicative character of $\mathbb{F}_q$, respectively.

We consider the bilinear sums

$$T_{\rho,\vartheta}(\psi, \mathcal{K}, \mathcal{M}) = \sum_{k \in \mathcal{K}} \left| \sum_{m \in \mathcal{M}} \rho(k)\vartheta(m)\psi(x(kmP)) \right|,$$

$$W_{\rho,\vartheta}(\varphi, \mathcal{K}, \mathcal{M}) = \sum_{k \in \mathcal{K}} \left| \sum_{m \in \mathcal{M}} \rho(k)\vartheta(m)\varphi(x(kmP)) \right|,$$

where $\mathcal{K}, \mathcal{M} \subseteq \mathbb{Z}_T^*$, $\rho(k)$ and $\vartheta(m)$ are arbitrary complex functions supported on $\mathcal{K}$ and $\mathcal{M}$ with

$$|\rho(k)| \leqslant 1,\ k \in \mathcal{K}, \quad \text{and} \quad |\vartheta(m)| \leqslant 1,\ m \in \mathcal{M}.$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

The sums $T_{\rho,\vartheta}(\psi,\mathcal{K},\mathcal{M})$ were introduced and estimated in [**1**]. Here we obtain a stronger result by using the approach to sums of this type given in [**8**].

Theorem 2.1. *Let $\boldsymbol{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$, and let $P \in \boldsymbol{E}(\mathbb{F}_q)$ be a point of order T. Then, for any fixed integer $\nu \geqslant 1$, for all subsets $\mathcal{K}, \mathcal{M} \subseteq \mathbb{Z}_T^*$ and complex functions $\rho(k)$ and $\vartheta(m)$ supported on $\mathcal{K}$ and $\mathcal{M}$ with*

$$|\rho(k)| \leqslant 1, \ k \in \mathcal{K}, \quad \text{and} \quad |\vartheta(m)| \leqslant 1, \ m \in \mathcal{M},$$

uniformly over all non-trivial additive characters ψ of $\mathbb{F}_q$ we have

$$T_{\rho,\vartheta}(\psi,\mathcal{K},\mathcal{M}) \ll (\#\mathcal{K})^{1-1/2\nu}(\#\mathcal{M})^{(\nu+1)/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}.$$

Proof. We follow the scheme of the proof of [**8**, Lemma 4] in the special case when $d = 1$ (and also $\mathbb{Z}_T$ plays the role of $\mathbb{Z}_{p-1}$). Furthermore, in our proof $\mathcal{K}$, $\mathcal{M}$ and $\mathbb{Z}_T^*$ play the roles of $\mathcal{X}$, $\mathcal{L}_d$ and $\mathcal{U}_d$ in the proof of [**8**, Lemma 4], respectively. In particular, for some integer parameter L with

$$1 \leqslant L \leqslant T(\log q)^{-2} \tag{2.1}$$

we define $\mathcal{V}$ as the set of the first L prime numbers which do not divide $\#\boldsymbol{E}(\mathbb{F}_q)$ (clearly we can assume that, say, $T \geqslant (\log q)^3$, since otherwise the bound is trivial). We also note that in this case

$$\max_{v\in\mathcal{V}} v = O(\#\mathcal{V}\log q). \tag{2.2}$$

Then we arrive at the following analogue of [**8**, Bound (4)]:

$$T_{\rho,\vartheta}(\psi,\mathcal{K},\mathcal{M}) \leqslant \frac{(\#\mathcal{K})^{1-1/2\nu}}{\#\mathcal{V}} \sum_{t\in\mathbb{Z}_T^*} M_t^{1/(2\nu)},$$

where

$$M_t = \sum_{z\in\mathbb{Z}_T} \left| \sum_{v\in\mathcal{V}} \vartheta(vt)\chi_{\mathcal{M}}(vt)\psi(x(zvP)) \right|^{2\nu}$$

and $\chi_{\mathcal{M}}$ is the characteristic function of the set $\mathcal{M}$. We only deviate from that proof at the point where the Weil bound is applied to the sums

$$\sum_{z\in\mathcal{H}} \exp\left(\frac{2\pi \mathrm{i} a}{p}\left(\sum_{j=1}^{\nu} z^{tv_j} - \sum_{j=\nu+1}^{2\nu} z^{tv_j}\right)\right) \ll \max_{1\leqslant j\leqslant 2\nu} v_j q^{1/2},$$

where $\mathcal{H}$ is an arbitrary subgroup of $\mathbb{F}_q^*$ and $v_1, \ldots, v_{2\nu}$ are positive integers (such that $(v_{\nu+1}, \ldots, v_{2\nu})$ is not a permutation of $(v_1, \ldots, v_\nu)$). Here, as in [**1**], we use instead the following bound from [**15**]:

$$\sum_{\substack{Q\in\mathcal{H},\\ Q\neq\mathcal{O}}} \psi\left(\sum_{j=1}^{\nu} x(v_jQ) - \sum_{j=\nu+1}^{2\nu} x(v_jQ)\right) \ll \max_{1\leqslant j\leqslant 2\nu} v_j^2 q^{1/2}, \tag{2.3}$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

where $\mathcal{H}$ is a subgroup of $\boldsymbol{E}(\mathbb{F}_p)$ (in our particular case $\mathcal{H} = \langle P\rangle$ is generated by P) and $v_1, \ldots, v_{2\nu}$ are the same as in the above, that is, such that $(v_{\nu+1}, \ldots, v_{2\nu})$ is not a permutation of $(v_1, \ldots, v_\nu)$.

Now, since $\#\boldsymbol{E}(\mathbb{F}_q) = O(q)$, using an argument similar to that given in [**8**] and recalling (2.2), we obtain

$$M_t \ll \sum_{v_1\in\mathcal{V}} \cdots \sum_{v_\nu\in\mathcal{V}} \left(\prod_{j=1}^{\nu} \chi_{\mathcal{M}}(v_j t)\right) T + \sum_{v_1\in\mathcal{V}} \cdots \sum_{v_{2\nu}\in\mathcal{V}} \left(\prod_{j=1}^{2\nu} \chi_{\mathcal{M}}(v_j t)\right) q^{1/2}(\#\mathcal{V}\log q)^2.$$

Therefore,

$$M_t \ll \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right)^{\nu} T + \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right)^{2\nu} q^{1/2}(\#\mathcal{V}\log q)^2.$$

This leads to

$$\begin{aligned} T_{\rho,\vartheta}(\psi,\mathcal{K},\mathcal{M}) \ll{}& \frac{(\#\mathcal{K})^{1-1/2\nu}}{\#\mathcal{V}} T^{1/2\nu} \sum_{t\in\mathbb{Z}_T^*} \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right)^{1/2} \\ &+ \frac{(\#\mathcal{K})^{1-1/2\nu}}{\#\mathcal{V}} (\#\mathcal{V}\log q)^{1/\nu} q^{1/4\nu} \sum_{t\in\mathbb{Z}_T^*} \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right). \end{aligned}$$

On the other hand, we have

$$\sum_{t\in\mathbb{Z}_T^*} \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right) = \#\mathcal{M}\#\mathcal{V},$$

and by the Cauchy inequality we get

$$\begin{aligned} \sum_{t\in\mathbb{Z}_T^*} \left(\sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right)^{1/2} &\leqslant (\#Z_T^*)^{1/2} \left(\sum_{t\in\mathbb{Z}_T^*} \sum_{v\in\mathcal{V}} \chi_{\mathcal{M}}(vt)\right)^{1/2} \\ &\leqslant T^{1/2}(\#\mathcal{M}\#\mathcal{V})^{1/2}. \end{aligned}$$

Thus,

$$T_{\rho,\vartheta}(\psi,\mathcal{K},\mathcal{M}) \ll \frac{(\#\mathcal{K})^{1-1/2\nu}}{(\#\mathcal{V})^{1/2}} T^{1/2\nu+1/2}(\#\mathcal{M})^{1/2} + (\#\mathcal{K})^{1-1/2\nu}(\#\mathcal{V}\log q)^{1/\nu} q^{1/4\nu}\#\mathcal{M}. \tag{2.4}$$

Let

$$L = \left\lfloor \frac{T^{(v+1)/(v+2)}}{q^{1/(2v+4)}(\log q)^{2/(v+2)}(\#\mathcal{M})^{v/(v+2)}} \right\rfloor.$$

We note that if $L = 0$, then

$$\begin{aligned} T^{(v+1)/(v+2)} &\leqslant q^{1/(2v+4)}(\log q)^{2/(v+2)}(\#\mathcal{M})^{v/(v+2)} \\ &\leqslant q^{1/(2v+4)}(\log q)^{2/(v+2)} T^{v/(v+2)} \end{aligned}$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

and thus

$$T \leqslant q^{1/2}(\log q)^2.$$

It is easy to check that in this case

$$\begin{aligned}\frac{(\#\mathcal{K})^{1-1/2\nu}(\#\mathcal{M})^{(\nu+1)/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}}{\#\mathcal{K}\#\mathcal{M}}&\\ \geqslant (\#\mathcal{K})^{-1/2\nu}(\#\mathcal{M})^{-1/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}&\\ \geqslant T^{-1/2\nu}T^{-1/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}&\\ = T^{-1/2(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)} \geqslant 1,&\end{aligned}$$

and thus the result is trivial.

We now assume that $L \geqslant 1$ and choose $\mathcal{V}$ to be of cardinality $\#\mathcal{V} = L$. Then we have

$$\frac{T^{(v+1)/(v+2)}}{q^{1/(2v+4)}(\log q)^{2/(v+2)}(\#\mathcal{M})^{v/(v+2)}} \geqslant \#\mathcal{V} \geqslant \frac{T^{(v+1)/(v+2)}}{2q^{1/(2v+4)}(\log q)^{2/(v+2)}(\#\mathcal{M})^{v/(v+2)}},$$

and $L \leqslant T(\log q)^{-2}$ provided that q is large enough. Now the result follows from (2.4). □

We also have the same result for sums of multiplicative characters.

Theorem 2.2. *Let $\boldsymbol{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$, and let $P \in \boldsymbol{E}(\mathbb{F}_q)$ be a point of order T. Then, for any fixed integer $\nu \geqslant 1$, for all subsets $\mathcal{K}, \mathcal{M} \subseteq \mathbb{Z}_T^*$ and complex functions $\rho(k)$ and $\vartheta(m)$ supported on $\mathcal{K}$ and $\mathcal{M}$ with*

$$|\rho(k)| \leqslant 1, \ k \in \mathcal{K}, \quad \text{and} \quad |\vartheta(m)| \leqslant 1, \ m \in \mathcal{M},$$

uniformly over all non-trivial additive characters ψ of $\mathbb{F}_q$:

$$W_{\rho,\vartheta}(\varphi, \mathcal{K}, \mathcal{M}) \ll (\#\mathcal{K})^{1-1/2\nu}(\#\mathcal{M})^{(\nu+1)/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}.$$

Proof. The proof is fully analogous to that of Theorem 2.1 and so we only briefly indicate a few changes.

First of all we notice that the proof of [**15**, Lemma 3], which implies that the sums

$$\sum_{j=1}^{\nu} x(v_jQ) - \sum_{j=\nu+1}^{2\nu} x(v_jQ), \quad v_1, \ldots, v_{2\nu},$$

are non-constant rational functions of components $x(Q)$ and $y(Q)$ of Q of degree $O(\max_{1\leqslant j\leqslant 2\nu} v_j^2)$ (unless $(v_{\nu+1}, \ldots, v_{2\nu})$ is a permutation of $(v_1, \ldots, v_\nu)$), extends to the products

$$\prod_{j=1}^{\nu} x(v_jQ) \prod_{j=\nu+1}^{2\nu} x(v_jQ)^{-1}, \quad v_1, \ldots, v_{2\nu},$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

at the cost of only minor changes. Furthermore, using the bound of Chen [**4**, Proposition 1] instead of the bound of [**14**] used in [**15**], we obtain the following analogue of (2.3):

$$\sum_{\substack{Q\in\mathcal{H},\\ Q\neq\mathcal{O}}} \varphi\Bigg(\prod_{j=1}^{\nu} x(v_jQ)\Bigg)\bar{\varphi}\Bigg(\prod_{j=\nu+1}^{2\nu} x(v_jQ)\Bigg) \ll \max_{1\leqslant j\leqslant 2\nu} v_j^2 q^{1/2},$$

where $\bar{\varphi}$ is the complex conjugate character (we also recall that $\varphi(z^{-1}) = \bar{\varphi}(z)$ for any $z \in \mathbb{F}_q^*$). The rest of the proof follows that of Theorem 2.1 without any changes. □

3. Lower bounds for sum–product problems on elliptic curves

Theorem 3.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be arbitrary subsets of $\mathbb{Z}_T^*$. Then for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1.1), we have*

$$\#\mathcal{S}\#\mathcal{T} \gg \min\{q\#\mathcal{A}, (\#\mathcal{A})^2(\#\mathcal{B})^{5/3}q^{-1/6}T^{-4/3}(\log q)^{-2/3}\}.$$

Proof. Let

$$\mathcal{H} = \{ab : a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

Following the ideas in [**7**], we now denote by J the number of solutions (b_1, b_2, h, u) to the equation

$$x(hb_1^{-1}P) + x(b_2P) = u, \quad b_1, b_2 \in \mathcal{B},\ h \in \mathcal{H},\ u \in \mathcal{S}. \tag{3.1}$$

Since the vectors

$$(b_1, b_2, h, u) = (b_1, b_2, ab_1, x(aP) + x(b_2P)), \quad a \in \mathcal{A},\ b_1, b_2 \in \mathcal{B},$$

are obviously all pairwise distinct solutions to (3.1), we obtain

$$J \geqslant \#\mathcal{A}(\#\mathcal{B})^2. \tag{3.2}$$

To obtain an upper bound on J we use Ψ to denote the set of all q additive characters of $\mathbb{F}_q$ and write Ψ^* for the set of non-trivial characters. Using the identity

$$\frac{1}{q}\sum_{\psi\in\Psi}\psi(z) = \begin{cases} 1 & \text{if } z = 0,\\ 0 & \text{otherwise,}\end{cases} \tag{3.3}$$

we obtain

$$\begin{aligned} J &= \sum_{b_1\in\mathcal{B}}\sum_{b_2\in\mathcal{B}}\sum_{h\in\mathcal{H}}\sum_{u\in\mathcal{S}}\frac{1}{q}\sum_{\psi\in\Psi}\psi(x(hb_1^{-1}P) + x(b_2P) - u)\\ &= \frac{1}{q}\sum_{\psi\in\Psi}\sum_{b_1\in\mathcal{B}}\sum_{h\in\mathcal{H}}\psi(x(hb_1^{-1}P))\sum_{b_2\in\mathcal{B}}\psi(x(b_2P))\sum_{u\in\mathcal{S}}\psi(-u)\\ &= \frac{(\#\mathcal{B})^2\#\mathcal{S}\#\mathcal{H}}{q} + \frac{1}{q}\sum_{\psi\in\Psi^*}\sum_{b_1\in\mathcal{B}}\sum_{h\in\mathcal{H}}\psi(x(hb_1^{-1}P))\sum_{b_2\in\mathcal{B}}\psi(x(b_2P))\sum_{u\in\mathcal{S}}\psi(-u). \end{aligned}$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

Applying Theorem 2.1 with $\rho(k) = \vartheta(m) = 1$, $\mathcal{K} = \mathcal{H}$ and $\mathcal{M} = \{b^{-1} : b \in \mathcal{B}\}$ and also taking $\nu = 1$, we obtain

$$\left| \sum_{b_1 \in \mathcal{B}} \sum_{h \in \mathcal{H}} \psi(x(hb_1^{-1}P)) \right| \ll \Delta,$$

where

$$\Delta = (\#\mathcal{H})^{1/2} (\#\mathcal{B})^{2/3} T^{2/3} q^{1/12} (\log q)^{1/3}.$$

Therefore,

$$J \ll \frac{(\#\mathcal{B})^2 \#\mathcal{S} \#\mathcal{H}}{q} + \frac{1}{q} \Delta \sum_{\psi \in \Psi^*} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \left| \sum_{u \in \mathcal{S}} \psi(-u) \right|. \tag{3.4}$$

Extending the summation over ψ to the full set Ψ and using the Cauchy inequality, we obtain

$$\sum_{\psi \in \Psi *} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \left| \sum_{u \in \mathcal{S}} \psi(u) \right| \leqslant \sqrt{\sum_{\psi \in \Psi} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right|^2} \sqrt{\sum_{\psi \in \Psi} \left| \sum_{u \in \mathcal{S}} \psi(u) \right|^2}. \tag{3.5}$$

Recalling the orthogonality property (3.3), we derive

$$\sum_{\psi \in \Psi} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right|^2 = q \#\{(b_1, b_2) \in \mathcal{B}^2 : b_1 \equiv \pm b_2 \pmod T\} \ll q \#\mathcal{B}.$$

Notice that $b_1 \equiv -b_2 \pmod T$ has been included, since $x(P) = x(-P)$ for $P \in \boldsymbol{E}(\mathbb{F}_q)$.

Similarly,

$$\sum_{\psi \in \Psi} \left| \sum_{u \in \mathcal{S}} \psi(u) \right|^2 \leqslant q \#\mathcal{S}.$$

Substituting these bounds in (3.5), we obtain

$$\sum_{\psi \in \Psi *} \left| \sum_{b \in \mathcal{B}} \psi(x(bP)) \right| \left| \sum_{u \in \mathcal{S}} \psi(u) \right| \ll q \sqrt{\#\mathcal{B} \#\mathcal{S}},$$

which, after substitution in (3.4), yields

$$J \ll \frac{(\#\mathcal{B})^2 \#\mathcal{S} \#\mathcal{H}}{q} + \Delta (\#\mathcal{S})^{1/2} (\#\mathcal{B})^{1/2}. \tag{3.6}$$

Thus, comparing (3.2) and (3.6), we derive

$$\frac{(\#\mathcal{B})^2 \#\mathcal{S} \#\mathcal{H}}{q} + \Delta (\#\mathcal{S})^{1/2} (\#\mathcal{B})^{1/2} \gg \#\mathcal{A} (\#\mathcal{B})^2.$$

Thus, either

$$\frac{(\#\mathcal{B})^2 \#\mathcal{S} \#\mathcal{H}}{q} \gg \#\mathcal{A} (\#\mathcal{B})^2 \tag{3.7}$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

or

$$\Delta(\#\mathcal{S})^{1/2}(\#\mathcal{B})^{1/2} \gg \#\mathcal{A}(\#\mathcal{B})^2. \tag{3.8}$$

If (3.7) holds, then we have

$$\#\mathcal{S}\#\mathcal{H} \gg q\#\mathcal{A}.$$

If (3.8) holds, then, recalling the definition of Δ, we derive

$$(\#\mathcal{S})^{1/2}(\#\mathcal{H})^{1/2}(\#\mathcal{B})^{5/3}T^{2/3}q^{1/12}(\log q)^{1/3} \gg \#\mathcal{A}(\#\mathcal{B})^2.$$

It only remains to note that $\#\mathcal{T} \geqslant 0.5\#\mathcal{H}$ to conclude the proof. □

We now consider several special cases.

Corollary 3.2. *For any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that if $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$ are arbitrary subsets with*

$$q^{1-\varepsilon} \geqslant \#\mathcal{A} \geqslant \#\mathcal{B} \geqslant T^{4/5+\varepsilon}q^{1/10},$$

then for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1.1), we have

$$\#\mathcal{S}\#\mathcal{T} \gg (\#\mathcal{A})^{2+\delta}.$$

In particular, if $T \geqslant q^{1/2+\varepsilon}$, then there is always some range of cardinalities $\#\mathcal{A}$ and $\#\mathcal{B}$ in which Corollary 3.2 applies non-trivially.

Corollary 3.3. *If $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$ are arbitrary subsets with*

$$\#\mathcal{A} = \#\mathcal{B} \geqslant T^{1/2}q^{7/16}(\log q)^{1/4},$$

then for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1.1), we have

$$\#\mathcal{S}\#\mathcal{T} \gg q\#\mathcal{A}.$$

We now obtain the multiplicative analogue of the above results for the sets $\mathcal{X}$ and $\mathcal{Y}$, given by (1.2).

Theorem 3.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be arbitrary subsets of $\mathbb{Z}_T^*$. Then for the sets $\mathcal{X}$ and $\mathcal{Y}$, given by (1.2), we have*

$$\#\mathcal{X}\#\mathcal{Y} \gg \min\{q\#\mathcal{A}, (\#\mathcal{A})^2(\#\mathcal{B})^{5/3}q^{-1/6}T^{-4/3}(\log q)^{-2/3}\}.$$

Proof. Let

$$\mathcal{G} = \{ab : a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

We remove, if necessary, at most two elements $a \in \mathcal{A}, b \in \mathcal{B}$ for which $x(aP) = x(bP) = 0$, and denote by I the number of solutions (b_1, b_2, g, w) to the equation

$$x(gb_1^{-1}P)x(b_2P) = w, \quad b_1, b_2 \in \mathcal{B},\ g \in \mathcal{G},\ w \in \mathcal{X}.$$

As before, we notice that

$$I \geqslant \#\mathcal{A}(\#\mathcal{B})^2.$$

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

To obtain an upper bound on I we use Φ to denote the set of all q multiplicative characters of $\mathbb{F}_q$ and write Φ^* for the set of non-trivial characters. Using the multiplicative analogue of (3.3):

$$\frac{1}{q-1}\sum_{\varphi\in\Phi}\varphi(z)=\begin{cases}1 & \text{if } z=1,\\ 0 & \text{otherwise,}\end{cases}$$

we obtain

$$\begin{aligned}I&=\sum_{b_1\in\mathcal{B}}\sum_{b_2\in\mathcal{B}}\sum_{g\in\mathcal{G}}\sum_{w\in\mathcal{X}}\frac{1}{q-1}\sum_{\varphi\in\Phi}\varphi(x(gb_1^{-1}P)x(b_2P)w^{-1})\\ &=\frac{1}{q-1}\sum_{\varphi\in\Phi}\sum_{b_1\in\mathcal{B}}\sum_{g\in\mathcal{G}}\varphi(x(gb_1^{-1}P))\sum_{b_2\in\mathcal{B}}\varphi(x(b_2P))\sum_{w\in\mathcal{X}}\bar{\varphi}(w)\\ &=\frac{(\#\mathcal{B})^2\#\mathcal{S}\#\mathcal{H}}{q-1}+\frac{1}{q-1}\sum_{\varphi\in\Phi^*}\sum_{b_1\in\mathcal{B}}\sum_{g\in\mathcal{G}}\varphi(x(gb_1^{-1}P))\sum_{b_2\in\mathcal{B}}\varphi(x(b_2P))\sum_{w\in\mathcal{X}}\bar{\varphi}(u).\end{aligned}$$

Applying Theorem 2.2 instead of Theorem 2.1, and proceeding as in the proof of Theorem 3.1, we derive the desired result. □

Accordingly, we also obtain the following result.

Corollary 3.5. *For any fixed $\varepsilon>0$ there exists $\delta>0$ such that if $\mathcal{A},\mathcal{B}\subseteq\mathbb{Z}_T^*$ are arbitrary subsets with*

$$q^{1-\varepsilon}\geqslant\#\mathcal{A}\geqslant\#\mathcal{B}\geqslant T^{4/5+\varepsilon}q^{1/10},$$

then for the sets $\mathcal{X}$ and $\mathcal{Y}$, given by (1.2), we have

$$\#\mathcal{X}\#\mathcal{Y}\gg(\#\mathcal{A})^{2+\delta}.$$

Corollary 3.6. *If $\mathcal{A},\mathcal{B}\subseteq\mathbb{Z}_T^*$ are arbitrary subsets with*

$$\#\mathcal{A}=\#\mathcal{B}\geqslant T^{1/2}q^{7/16}(\log q)^{1/4},$$

then for the sets $\mathcal{X}$ and $\mathcal{Y}$, given by (1.2), we have

$$\#\mathcal{X}\#\mathcal{Y}\gg q\#\mathcal{A}.$$

4. Upper bound for a sum–product problem on elliptic curves

We now show that in some cases the sets $\mathcal{S}$ and $\mathcal{T}$ are not very big.

As usual, we use $\varphi(T)=\#\mathbb{Z}_T^*$ to denote the Euler function.

Theorem 4.1. *Let $q=p$ be prime and let $T\geqslant p^{3/4+\varepsilon}$. Then there are sets $\mathcal{A}=\mathcal{B}\subset\mathbb{Z}_T^*$ of cardinality*

$$\#\mathcal{A}=\#\mathcal{B}=(1+o(1))\frac{\varphi(T)^2}{2p}$$

such that for the sets $\mathcal{S}$ and $\mathcal{T}$, given by (1.1), we have

$$\max\{\#\mathcal{S},\#\mathcal{T}\}\leqslant(\sqrt{2}+o(1))\sqrt{p\#\mathcal{A}}$$

as $p\to\infty$.

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

Proof. We recall the bound from [**14**] of exponential sums over subgroups of the group of points on elliptic curves, which, in particular, implies that, for any subgroup $\mathcal{G}$ of $\boldsymbol{E}(\mathbb{F}_p)$, the bound

$$\sum_{G \in \mathcal{G}} \exp(2\pi \mathrm{i} \lambda x(G)/p) \ll p^{1/2} \tag{4.1}$$

holds uniformly over all integers λ with $\gcd(\lambda, p) = 1$.

Let $\mu(d)$ be the Möbius function, that is, $\mu(1) = 1$, $\mu(m) = 0$ if $m \geqslant 2$ is not square-free and $\mu(m) = (-1)^{\omega(m)}$ otherwise, where $\omega(d)$ is the number of distinct prime divisors of $d \geqslant 2$ [**9**, § 16.2].

Using the inclusion–exclusion principle, we obtain

$$\begin{aligned}\sum_{\substack{a=1,\\ \gcd(a,T)=1}}^{T} \exp(2\pi \mathrm{i} \lambda x(aP)/p) &= \sum_{d \mid T} \mu(d) \sum_{\substack{a=1,\\ d \mid a}}^{T} \exp(2\pi \mathrm{i} \lambda x(aP)/p) \\ &= \sum_{d \mid T} \mu(d) \sum_{b=1}^{T/d} \exp(2\pi \mathrm{i} \lambda x(bdP)/p).\end{aligned}$$

Using (4.1) and recalling that [**9**, Theorem 317]

$$\sum_{d \mid T} 1 = T^{o(1)},$$

we derive

$$\sum_{\substack{a=1,\\ \gcd(a,T)=1}}^{T} \exp(2\pi \mathrm{i} \lambda x(aP)/p) \ll p^{1/2+o(1)}.$$

Combining this with the Erdős–Turán inequality [**5**, Theorem 1.21], we see that, for any positive integer H, there are $H\varphi(T)/p + O(p^{1/2+o(1)})$ elements $a \in \mathbb{Z}_T^*$ with $x(aP) \in [0, H-1]$. Let $\mathcal{A} = \mathcal{B}$ be the set of these elements a. For the sets $\mathcal{S}$ and $\mathcal{T}$, we obviously have

$$\#\mathcal{S} \leqslant 2H \quad \text{and} \quad \#\mathcal{T} \leqslant \varphi(T).$$

We now choose $H = \varphi(T)/2$. Since $T \geqslant p^{3/4+\varepsilon}$ and also since [**9**, Theorem 328]

$$\varphi(T) \gg \frac{T}{\log\log T},$$

we have

$$\#\mathcal{A} = \#\mathcal{B} = \frac{\varphi(T)^2}{2p} + O(p^{1/2+o(1)}) = (1+o(1))\frac{\varphi(T)^2}{2p}$$

as $p \to \infty$. Therefore,

$$\max\{\#\mathcal{S}, \#\mathcal{T}\} \leqslant (\sqrt{2} + o(1))\sqrt{p\#\mathcal{A}},$$

which concludes the proof. □

https://doi.org/10.1017/S0013091508000771 Published online by Cambridge University Press

We note that if $T \geqslant p^{23/24+\varepsilon}$, then the cardinality of the sets $\mathcal{A}$ and $\mathcal{B}$ of Theorem 4.1 is

$$\#\mathcal{A} = \#\mathcal{B} = T^{2+o(1)}p^{-1} \geqslant T^{1/2}p^{7/16}(\log p)^{1/4},$$

and thus Corollary 3.3 also applies and we have

$$(\sqrt{2}+o(1))\sqrt{p\#\mathcal{A}} \geqslant \max\{\#\mathcal{S}, \#\mathcal{T}\} \geqslant \sqrt{\#\mathcal{S}\#\mathcal{T}} \gg \sqrt{p\#\mathcal{A}},$$

showing that both Corollary 3.3 and Theorem 4.1 are tight in this range.

5. Comments

We note that, using Theorems 2.1 and 2.2 with other values of ν in the scheme of the proof of Theorems 3.1 and 3.4, respectively, one can obtain a series of other statements. However, they cannot be formulated as a lower bound on the products $\#\mathcal{S}\#\mathcal{T}$ and $\#\mathcal{X}\#\mathcal{Y}$. Rather, they only give a lower bound on $\max\{\#\mathcal{S}, \#\mathcal{T}\}$ and $\max\{\#\mathcal{X}, \#\mathcal{Y}\}$, which, however, may in some cases be more precise than those which follow from Theorems 3.1 and 3.4, respectively.

We note also that we do not have any upper bound for the sets $\mathcal{X}$ and $\mathcal{Y}$, given by (1.2). Some analogue of Theorem 4.1 can also be obtained for such sets, but only when $\mathbb{F}_q$ contains a subgroup of a desired size.

Certainly, extending the range in which the upper and lower bounds on $\#\mathcal{S}$ and $\#\mathcal{T}$ coincide is also a very important problem.

Finally, we note that, using the bound of [**16**] (see also [**4**]) on multiplicative character sums along an elliptic curve, one can obtain an analogue of the estimate of [**17**] for the bilinear multiplicative character sum with $x(P \oplus Q)$ over $P \in \mathcal{P}$, $Q \in \mathcal{Q}$ for two arbitrary sets $\mathcal{P}, \mathcal{Q} \subseteq \boldsymbol{E}(\mathbb{F}_q)$. In turn, this allows the derivation of an analogue of the results of [**18**], obtained for (1.3), and also for the sets

$$\{x(P)x(Q) : P \in \mathcal{P},\ Q \in \mathcal{Q}\} \quad \text{and} \quad \{x(P \oplus Q) : P \in \mathcal{P},\ Q \in \mathcal{Q}\}.$$

Acknowledgements. This paper was initiated during a very enjoyable visit by I.S. to the Department of Combinatorics and Optimization of the University of Waterloo, whose hospitality, support and stimulating research atmosphere are gratefully appreciated. The research of I.S. was supported by ARC Grant no. DP0556431.

References

1. W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, Double character sums over elliptic curves and finite fields, *Pure Appl. Math. Q.* **2** (2006), 179–197.
2. 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.
3. J. Bourgain, N. Katz and T. Tao, A sum product estimate in finite fields, and applications, *Geom. Funct. Analysis* **14** (2004), 27–57.
4. Z. Chen, Elliptic curve analogue of Legendre sequences, *Monatsh. Math.* **154** (2008), 1–10.

5. M. Drmota and R. Tichy, *Sequences, discrepancies and applications* (Springer, 1997).
6. M. Z. Garaev, An explicit sum–product estimate in $\mathbb{F}_p$, *Int. Math. Res. Not.* **2007** (2007), RNM035.
7. M. Z. Garaev, The sum–product estimate for large subsets of prime fields, *Proc. Am. Math. Soc.* **136** (2008), 2735–2739.
8. M. Z. Garaev and A. A. Karatsuba, New estimates of double trigonometric sums with exponential functions, *Arch. Math.* **87** (2006), 33–40.
9. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford University Press, 1979).
10. D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum–product theory in finite fields, and the Erdős–Falconer distance conjecture, *Trans. Am. Math. Soc.* (in press).
11. D. Hart, A. Iosevich and J. Solymosi, Sums and products in finite fields via Kloosterman sums, *Int. Math. Res. Not.* **2007** (2007), RNM007.
12. N. H. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *J. Analyt. Combinat.* **3** (2008), Article 3.
13. N. H. Katz and C.-Y. Shen, A slight improvement to Garaev's sum product estimate, *Proc. Am. Math. Soc.* **136** (2008), 2499–2504.
14. D. R. Kohel and I. E. Shparlinski, Exponential sums and group generators for elliptic curves over finite fields, in *Proc. 4th Algorithmic Number Theory Symp.*, Lecture Notes in Computer Science, Volume 1838, pp. 395–404 (Springer, 2000).
15. T. Lange and I. E. Shparlinski, Certain exponential sums and random walks on elliptic curves, *Can. J. Math.* **57** (2005), 338–350.
16. M. Perret, Multiplicative character sums and Kummer coverings, *Acta Arith.* **59** (1991), 279–290.
17. I. E. Shparlinski, Bilinear character sums over elliptic curves, *Finite Fields Applic.* **14** (2008), 132–141.
18. I. E. Shparlinski, On the elliptic curve analogue of the sum–product problem, *Finite Fields Applic.* **14** (2008), 721–726.
19. I. E. Shparlinski, On the exponential sum–product problem, *Indagationes Math.* **19** (2008), 325–331.
20. J. H. Silverman, *The arithmetic of elliptic curves* (Springer, 1995).