Exponential Sums over Points of Elliptic Curves

Omran Ahmadi
School of Mathematics
Institute for Research in Fundamental Sciences
P.O. Box: 19395-5746, Tehran, Iran
omran.ahmadi@ucd.ie

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

Abstract

We derive a new bound for some bilinear sums over points of an elliptic curve over a finite field. We use this bound to improve a series of previous results on various exponential sums and some arithmetic problems involving points on elliptic curves.

Subject Classification (2010) Primary 11L07, 11T23 Secondary 11G20

1 Introduction

Let q be a prime power and let $\mathcal{E}$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ of q elements of characteristic $p \geq 5$ given by an affine Weierstraß equation

$$\mathcal{E} : \quad Y^2 = X^3 + AX + B$$

with some $A, B \in \mathbb{F}_q$, see [2, 4, 25].

We recall that the set of all points on $\mathcal{E}$ forms an abelian group, with the "point at infinity" $\mathcal{O}$ as the neutral element, and we use $\oplus$ to denote the group operation. In particular, we sometimes work with group characters associated with this group.

As usual, we write every point $P \neq \mathcal{O}$ on $\mathcal{E}$ as $P = (\mathbf{x}(P), \mathbf{y}(P))$. Let $\mathcal{E}(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on $\mathcal{E}$. We recall that the celebrated result of Bombieri [5] implies, in particular, an estimate of order $q^{1/2}$ for exponential sums with functions from the function field of $\mathcal{E}$ taken over all points of $\mathcal{E}(\mathbb{F}_q)$. More recently, various character sums over points of elliptic curves have been considered in a number of papers, see [1, 3, 7, 9, 10, 15, 16, 17, 18, 19, 21, 23] and references therein; many of these estimates are motivated by applications to pseudorandom number generators on elliptic curves [24].

We fix a nonprincipal additive character ψ of $\mathbb{F}_q$. All our estimates are uniform with respect to the additive character ψ.

Let $G \in \mathcal{E}(\mathbb{F}_q)$ be a point of order T, in other words, T is the cardinality of the cyclic group $\langle G \rangle$ generated by G in $\mathcal{E}(\mathbb{F}_q)$.

Given two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$, in the unit group of residue ring $\mathbb{Z}_T$ modulo T, and arbitrary complex functions α and β supported on $\mathcal{A}$ and $\mathcal{B}$ with

$$|\alpha_a| \le 1,\ a \in \mathcal{A}, \qquad \text{and} \qquad |\beta_b| \le 1,\ b \in \mathcal{B},$$

we consider the bilinear sums of *multiplicative type*:

$$U_{\alpha,\beta}(\psi, \mathcal{A}, \mathcal{B}; G) = \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \alpha_a \beta_b \psi(x(abG)). \qquad (1)$$

Furthermore, given two sets $\mathcal{P}, \mathcal{Q} \subseteq \mathcal{E}(\mathbb{F}_q)$ and arbitrary complex functions $\rho(P)$ and $\vartheta(Q)$ supported on $\mathcal{P}$ and $\mathcal{Q}$ we consider the bilinear sums of *additive type*:

$$V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{P \in \mathcal{P}} \sum_{Q \in \mathcal{Q}} \rho(P)\vartheta(Q)\psi(x(P \oplus Q)). \qquad (2)$$

Bounds of the sums $U_{\alpha,\beta}(\psi, \mathcal{A}, \mathcal{B}; G)$ and $V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q})$ are proved in [1, 3] and [21], respectively, where several applications of these bounds have been shown.

Here we improve the bound of [21] and use it with the bound of [1], and also with some additional arguments, to refine a series of previous results. In particular, we give improvements:

- of the elliptic curve version of the sum-product theorem of [22];
- of the bound of character sums from [17] with a sequences of points of cryptographic significance;
- of the bound of character sums from [23] with linear combinations of $x(P)$ and $x(nP)$ for $P \in \mathcal{E}(\mathbb{F}_q)$;

Throughout the paper, any implied constants in the symbols O and $\ll$ may occasionally depend, where obvious, on the integer parameter $\nu \geq 1$ and real parameter $\varepsilon > 0$, but are absolute otherwise. We recall that the notations $A \ll B$ and $A = O(B)$ are both equivalent to the statement that the inequality $|A| \leq c\,B$ holds with some constant $c > 0$.

2 Preparations

2.1 Single sums

We recall the following special case of the bound of [15, Corollary 1]:

Lemma 1. *Let $\mathcal{E}$ be an ordinary curve defined over $\mathbb{F}_q$ and let $G \in \mathcal{E}(\mathbb{F}_q)$ be a point of order T. Then for any group character χ on $\mathcal{E}(\mathbb{F}_q)$.*

$$\sum_{n\in\mathbb{Z}_T} \psi\left(x\left(nG\right)\right)\chi(G) \ll q^{1/2},$$

2.2 Bilinear sums of multiplicative type

We recall the bound of [1, Theorem 2.1] on the sums (1):

Lemma 2. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$, and let $G \in \mathcal{E}(\mathbb{F}_q)$ be a point of order T. Then, for any fixed integer $\nu \geq 1$, uniformly over all nontrivial additive characters ψ of $\mathbb{F}_q$, we have*

$$U_{\alpha,\beta}(\psi, \mathcal{A},\mathcal{B}; G) \\ \ll (\#\mathcal{A})^{1-1/2\nu}(\#\mathcal{B})^{1-1/(\nu+2)}T^{(\nu+1)/\nu(\nu+2)}q^{1/4(\nu+2)}(\log q)^{1/(\nu+2)}.$$

2.3 Bilinear sums of additive type

For the sum (2) it is shown in [21] that if

$$\max_{P\in\mathcal{P}} |\rho(P)| \le 1 \qquad \text{and} \qquad \max_{Q\in\mathcal{Q}} |\vartheta(Q)| \le 1$$

then for any fixed integer $\nu \ge 1$ we have

$$V_{\rho,\vartheta}(\psi,\mathcal{P},\mathcal{Q}) \ll (\#\mathcal{P})^{1-1/2\nu}(\#\mathcal{Q})^{1/2}q^{1/2\nu} + (\#\mathcal{P})^{1-1/2\nu}\#\mathcal{Q}q^{1/4\nu}. \qquad (3)$$

Here we obtain a different bound which is stronger than (3) in several cases (for example, when $\#\mathcal{P} = \#\mathcal{Q}$).

Theorem 3. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let*

$$\sum_{P\in\mathcal{P}} |\rho(P)|^2 \le R \qquad \textit{and} \qquad \sum_{Q\in\mathcal{Q}} |\vartheta(Q)|^2 \le T.$$

Then, uniformly over all nontrivial additive characters ψ of $\mathbb{F}_q$

$$|V_{\rho,\vartheta}(\psi,\mathcal{P},\mathcal{Q})| \ll \sqrt{qRT}.$$

Proof. Let $\mathcal{X}$ be the set of group characters on $\mathcal{E}(\mathbb{F}_q)$. We collect the points P and Q with a given sum $S = P \oplus Q$ and identify this condition via the character sum over $\mathcal{X}$. This gives

$$V_{\rho,\vartheta}(\psi,\mathcal{P},\mathcal{Q}) = \sum_{S\in\mathcal{E}(\mathbb{F}_q)} \psi(x(S)) \sum_{P\in\mathcal{P}}\sum_{Q\in\mathcal{Q}} \rho(P)\vartheta(Q)\frac{1}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\chi\in\mathcal{X}} \chi(P\oplus Q\ominus S).$$

Therefore

$$V_{\rho,\vartheta}(\psi,\mathcal{P},\mathcal{Q}) = \frac{1}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\chi\in\mathcal{X}}\sum_{S\in\mathcal{E}(\mathbb{F}_q)} \psi(x(S))\overline{\chi(S)} \sum_{P\in\mathcal{P}}\rho(P)\chi(P)\sum_{Q\in\mathcal{Q}}\vartheta(Q)\chi(Q).$$

The sums over S is $O(q^{1/2})$ by Lemma 1, so

$$V_{\rho,\vartheta}(\psi,\mathcal{P},\mathcal{Q}) \ll \frac{q^{1/2}}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\chi\in\mathcal{X}}\left|\sum_{P\in\mathcal{P}}\rho(P)\chi(P)\right|\left|\sum_{Q\in\mathcal{Q}}\vartheta(Q)\chi(Q)\right|.$$

We now use the Cauchy inequality, getting

$$\begin{aligned}
&\left(\sum_{\chi\in\mathcal{X}}\left|\sum_{P\in\mathcal{P}}\rho(P)\chi(P)\right|\left|\sum_{Q\in\mathcal{Q}}\vartheta(Q)\chi(Q)\right|\right)^2\\
&\qquad\le \sum_{\chi\in\mathcal{X}}\left|\sum_{P\in\mathcal{P}}\rho(P)\chi(P)\right|^2 \sum_{\chi\in\mathcal{X}}\left|\sum_{Q\in\mathcal{Q}}\vartheta(Q)\chi(Q)\right|^2\\
&\qquad\ll \#\mathcal{E}(\mathbb{F}_q)^2RT,
\end{aligned}$$

since

$$\begin{aligned}
\sum_{\chi\in\mathcal{X}}\left|\sum_{P\in\mathcal{P}}\rho(P)\chi(P)\right|^2 &= \sum_{P_1,P_2\in\mathcal{P}}\rho(P_1)\overline{\rho(P_2)}\sum_{\chi\in\mathcal{X}}\chi(P_1\ominus P_2)\\
&= \#\mathcal{E}(\mathbb{F}_q)\sum_{P\in\mathcal{P}}|\rho(P)|^2 \le \#\mathcal{E}(\mathbb{F}_q)R
\end{aligned}$$

Similarly,

$$\sum_{\chi\in\mathcal{X}}\left|\sum_{Q\in\mathcal{Q}}\vartheta(Q)\chi(Q)\right|^2 \le \#\mathcal{E}(\mathbb{F}_q)T,$$

and the desired result now follows. □

3 Combinatorial Problems

3.1 Sum-product problem for elliptic curves

In [22], for any sets $\mathcal{R},\mathcal{S}\subseteq\mathcal{E}$ it is shown that

$$\#\mathcal{U}\#\mathcal{V} \gg \min\{q\#\mathcal{R}, (\#\mathcal{R})^2\#\mathcal{S}q^{-1/2}\} \tag{4}$$

where

$$\begin{aligned}
\mathcal{U} &= \{x(R)+x(S)\ :\ R\in\mathcal{R},\ S\in\mathcal{S}\},\\
\mathcal{V} &= \{x(R\oplus S)\ :\ R\in\mathcal{R},\ S\in\mathcal{S}\}.
\end{aligned} \tag{5}$$

Clearly (4) implies that at least one of the sets $\mathcal{U}$ and $\mathcal{V}$ is large.

The main ingredient of the proof of (4) in [22] is (3). Using Theorem 3 in the argument of [22] one immediately derives the following improvement on (4):

Theorem 4. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $\mathcal{R}$ and $\mathcal{S}$ be arbitrary subsets of $\mathcal{E}(\mathbb{F}_q)$. Then for the sets $\mathcal{U}$ and $\mathcal{V}$, given by* (5), *we have*

$$\#\mathcal{U}\#\mathcal{V} \gg \min\{q\#\mathcal{R}, (\#\mathcal{R}\#\mathcal{S})^2 q^{-1}\}.$$

3.2 Sárközy problem for elliptic curves

In [21], the number of solutions $M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V})$ of the equation

$$x(S) + x(T) = x(U \oplus V), \qquad S \in \mathcal{S},\ T \in \mathcal{T},\ U \in \mathcal{U},\ V \in \mathcal{V},$$

for any sets $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V} \subseteq \mathcal{E}(\mathbb{F}_q)$ is estimated. It is shown that if

$$\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V} \geq q^{7/2+\varepsilon}, \qquad \varepsilon > 0,$$

then

$$M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}) = \left(1 + O(q^{-\varepsilon/2})\right) \frac{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}{q}. \tag{6}$$

The result above is the elliptic curve analogue of a result of A. Sárközy [20] regarding the number of solutions $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ of the equation

$$a + b = cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D},$$

for sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$.

In [21], the asymptotic formula (6) is proved using (3). Now, using Theorem 3, the following improvement on (6) is immediate. The proof is omitted as it is completely similar to the proof given in [21].

Theorem 5. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$. Then for every $\varepsilon > 0$ and arbitrary sets $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V} \subseteq \mathcal{E}(\mathbb{F}_q)$ with*

$$\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V} \geq q^{3+\varepsilon}, \qquad \varepsilon > 0$$

we have

$$M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}) = \left(1 + O(q^{-\varepsilon/2})\right) \frac{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}{q}.$$

3.3 Distribution of subset sums

Let $P \in \mathcal{E}(\mathbb{F}_q)$ be an $\mathbb{F}_q$-rational point on an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$, and σ be an endomorphism on $\mathcal{E}$. Also, let $\mathcal{M}_k$ be the set of k-dimensional vectors with coordinates $0, \pm 1$ which do not have two consecutive nonzero components, that is,

$$\mu_j \mu_{j+1} = 0, \text{ for all } j = 0, \ldots, k-2. \tag{7}$$

Motivated by applications to pseudo-random number generation, the set of points

$$P_{\sigma,\mathbf{m}} = \sum_{j=0}^{k-1} \mu_j \sigma^j(P), \qquad \mathbf{m} = (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k, \tag{8}$$

where σ is an endomorphism of the elliptic curve $\mathcal{E}$ have been considered in [17].

In [17], three specific endomorphisms are considered. The first endomorphism considered in [17] is the *doubling* endomorphism $\delta(P) = 2P$ which is defined for any elliptic curve over any finite field.

The second endomorphism considered in [17] is the *Frobenius endomorphism* of the so called *Koblitz curves.* A Koblitz curve, $\mathcal{E}_a$, $a \in \mathbb{F}_2$, is given by the Weierstraß equation

$$\mathcal{E}_a : \ Y^2 + XY = X^3 + aX^2 + 1,$$

(see [14]) and its Frobenius endomorphism φ, which acts on a $\mathbb{F}_{2^n}$-rational point $P = (x, y) \in \mathcal{E}_a(\mathbb{F}_{2^n})$ is given by

$$\varphi(P) = (x^2, y^2).$$

Clearly $\varphi(P) \in \mathcal{E}_a(\mathbb{F}_{2^n})$.

Finally authors in [17] considered one of the GLV curves introduced by Gallant, Lambert and Vanstone [11], and detailed below.

Let the characteristic of $\mathbb{F}_q$ be a prime $p \geq 3$ such that -7 is a quadratic residue modulo p (that is, $p \equiv 1, 2, 4 \pmod 7$). Define an elliptic curve $\mathcal{E}_{GLV}$ over $\mathbb{F}_p$ by

$$\mathcal{E}_{GLV} : Y^2 = X^3 - \frac{3}{4}X^2 - 2X - 1.$$

Let $\xi \in \mathbb{F}_p$ be a square root of -7. If $b = (1 + \xi)/2$ and $c = (b - 3)/4$, then the map ψ, defined in the affine plane by

$$\psi(P) = \left(\frac{x^2 - b}{b^2(x - c)}, \frac{y(x^2 - 2cx + b)}{b^3(x - c)^2} \right)$$

for $P = (x, y) \in \mathcal{E}_{GLV}$, is an endomorphism of $\mathcal{E}_{GLV}$.

In [17], it has been shown that under mild conditions, the points (8) possess some uniformity of distribution properties, where σ is one of the following endomorphisms:

$$\sigma = \begin{cases} \delta, & \text{for an arbitrary curve } \mathcal{E}, \\ \varphi, & \text{for a Koblitz curve } \mathcal{E} = \mathcal{E}_a,\ a = 0, 1 \\ \psi, & \text{for the GLV curve } \mathcal{E} = \mathcal{E}_{GLV}. \end{cases} \qquad (9)$$

Here, using Theorem 3 we improve the result of [17] in some ranges of parameters.

First we need the following estimate on $\#\mathcal{M}_k$ given by Bosma [6, Proposition 4].

Lemma 6. *For any $k \geq 2$, we have:*

$$\#\mathcal{M}_k = \frac{4}{3}2^k + O(1).$$

For an endomorphism σ of an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ and a nonprincipal additive character ψ of $\mathbb{F}_q$, we define the exponential sum

$$S_{\sigma,k}(\chi) = \sum_{\mathbf{m} \in \mathcal{M}_k} \chi\left(x(P_{\sigma,\mathbf{m}})\right),$$

where we always assume that the value of the character is defined as zero if the expression in the argument is not defined (for example, if $P_{\sigma,\mathbf{m}} = \mathcal{O}$ in the above sum).

It is shown in [17, Lemma 2.1] that if $P \in \mathcal{E}(\mathbb{F}_q)$ is of prime order ℓ then for any integer $k \geq 1$ the bound

$$|S_{\sigma,k}(\chi)| \ll \#\mathcal{M}_k \left(q^{1/4\nu}\ell^{-1/2\nu} + 2^{-k/2\nu}q^{(\nu+1)/4\nu^2}\right) \qquad (10)$$

holds with any fixed integer

$$\nu \geq \frac{\log q}{2k \log 2},$$

where σ is one of the endomorphisms (9).

Given an endomorphism σ of an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$, and an integer $k \geq 1$, we denote by $N_{\sigma,k}(Q)$ the number of representations

$$P_{\sigma,\mathbf{m}} = Q, \qquad \mathbf{m} = (m_0, \ldots, m_{k-1}) \in \mathcal{M}_k.$$

We recall [17, Lemma 2.1]:

Lemma 7. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $P \in \mathcal{E}(\mathbb{F}_q)$ be of prime order ℓ. Then for any positive integer k and for every point $Q \in \mathcal{E}(\mathbb{F}_q)$ the bound*

$$N_{\sigma,k}(Q) \ll 2^k \ell^{-1} + 1$$

holds, where σ is one of the endomorphisms (9).

We now obtain a bound that improves (10) for some values of parameters (namely for large k and ℓ).

Theorem 8. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $P \in \mathcal{E}(\mathbb{F}_q)$ be of prime order ℓ. Then for any integer $k \geq 1$ the bound*

$$|S_{\sigma,k}(\chi)| \ll \#\mathcal{M}_k q^{1/2} \ell^{-1} + (\#\mathcal{M}_k)^{1/2} q^{1/2}$$

holds where σ is one of the endomorphisms (9).

Proof. Let us choose $r = \lceil k/2 \rceil$. For $j = 0, 1$ we define $\mathcal{U}_j$ to be the subset of $\mathbf{u} = (u_1, \ldots, u_r) \in \mathcal{M}_r$ with $u_r = \pm j$. To form a vector in $\mathcal{M}_k$, a vector from $\mathcal{U}_0$ can be appended by any vector in $\mathcal{V}_0 = \mathcal{M}_{k-r}$ while one from $\mathcal{U}_1$ requires the following digit to be zero. Hence, we put

$$\mathcal{V}_1 = \{(0, \mathbf{w}) \ : \ \mathbf{w} \in \mathcal{M}_{k-r-1}\}.$$

We have

$$S_{\sigma,k}(\chi) = R_{\sigma,0} + R_{\sigma,1},$$

where

$$R_{\sigma,j} = \sum_{\mathbf{u} \in \mathcal{U}_j} \sum_{\mathbf{v} \in \mathcal{V}_j} \chi\left(x\left(P_{\sigma,\mathbf{u}} + \sigma^r(P_{\sigma,\mathbf{v}})\right)\right), \qquad j = 0, 1.$$

We now consider the sets

$$\mathcal{X}_j = \{P_{\sigma,\mathbf{u}} \ : \ \mathbf{u} \in \mathcal{U}_j\} \qquad \text{and} \qquad \mathcal{Y}_j = \{\sigma^r(P_{\sigma,\mathbf{v}}) \ : \ \mathbf{v} \in \mathcal{V}_j\}.$$

Using Lemma 7, we see that we can write

$$R_{\sigma,j} = \sum_{X \in \mathcal{X}_j} \sum_{Y \in \mathcal{Y}_j} M(X) N(Y) \chi\left(x\left(S + T\right)\right), \qquad j = 0, 1.$$

with some positive coefficients $M(X)$ and $N(Y)$ such that

$$M(X) \ll 2^r \ell^{-1} + 1 \qquad \text{and} \qquad N(Y) \ll 2^{k-r} \ell^{-1} + 1.$$

We also trivially have

$$\sum_{X\in\mathcal{X}_j} M(X) = \#\mathcal{U}_j \qquad \text{and} \qquad \sum_{Y\in\mathcal{Y}_j} N(Y) = \#\mathcal{V}_j.$$

Therefore

$$\sum_{X\in\mathcal{X}_j} M(X)^2 \le \#\mathcal{U}_j \left(2^r\ell^{-1}+1\right) \quad \text{and} \quad \sum_{Y\in\mathcal{Y}_j} N(Y)^2 = \#\mathcal{V}_j \left(2^{k-r}\ell^{-1}+1\right).$$

Therefore, by Theorem 3, we derive

$$R_{\sigma,0} \ll \sqrt{q(2^r\ell^{-1}+1)(2^{k-r}\ell^{-1}+1)\#\mathcal{U}_j\#\mathcal{V}_j}, \qquad j=0,1.$$

Clearly $\#\mathcal{U}_j\#\mathcal{V}_j \le \#\mathcal{M}_k \ll 2^k$. Furthermore, by the choice of r

$$(2^r\ell^{-1}+1)(2^{k-r}\ell^{-1}+1) \ll (2^{k/2}\ell^{-1}+1)^2 \ll 2^k\ell^{-2}+1.$$

And thus

$$|R_{\sigma,j}| \ll q^{1/2}2^k\ell^{-1} + q^{1/2}2^{k/2}, \qquad j=0,1,$$

which concludes the proof. □

Clearly, if for some fixed $\varepsilon > 0$ we have $\ell > q^{1/2+\varepsilon}$ and $2^k \ge q^{1+\varepsilon}$, then the bound of Theorem 8 is nontrivial. As in [17, Section 4], we can now use this bound in various questions about the distribution of $x(P_{\sigma,\mathbf{m}})$ for $\mathbf{m} \in \mathcal{M}_k$.

4 Sums Over Consecutive Intervals

4.1 Stationary phase sums

For an integer n and $a, b \in \mathbb{F}_q$, we now consider the sums

$$S_n(\psi; a, b) = \sum_{P\in\mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P) + bx(nP)\right).$$

As it has been mentioned in [23], it follows from a much more general result of [16, Corollary 5] that if at least one of a and b is a non-zero element of $\mathbb{F}_q$ and $n > 0$, then

$$S_n(\psi; a, b) = O(n^2q^{1/2}). \tag{11}$$

Furthermore, in [23], the following two bounds are given:

$$S_n(\psi; a, b) \ll q^{3/2}/d, \tag{12}$$

and

$$S_n(\psi; a, b) \ll qd^{-1/2} + q^{3/4}, \tag{13}$$

where $d = \gcd(n, \#\mathcal{E}(\mathbb{F}_q))$. The above bounds improve on (11) when d is not very small. The bound (12) is nontrivial whenever $d/q^{1/2} \to \infty$ as $q \to \infty$. The bound (13) is nontrivial for $d \to \infty$ as $q \to \infty$, however it is weaker than the first bound for $d > q^{3/4}$.

In [23], the bound (3) is used to obtain (13). Here we use Theorem 3, to improve on the bounds (12) and (13). Although the proof of the new bound is quite similar to the proof given in [23], here, for the sake of completeness, instead of referring for details to [23] we give a complete proof of this bound.

Theorem 9. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $n > 0$ be an arbitrary integer. Then for any $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, we have*

$$S_n(\psi; a, b) \ll qd^{-1/2}$$

where $d = \gcd(n, \#\mathcal{E}(\mathbb{F}_q))$.

Proof. Let $\mathcal{H}_d \subseteq \mathcal{E}(\mathbb{F}_q)$ be the subgroup of $\mathcal{E}(\mathbb{F}_q)$ consisting of the d-torsion points $Q \in \mathcal{E}(\mathbb{F}_q)$, that is, of points Q with $dQ = \mathcal{O}$.

It is well-known, see [2, 4, 25], that the group $\mathcal{E}(\mathbb{F}_q)$ is isomorphic to

$$\mathcal{E}(\mathbb{F}_q) \cong \mathbb{Z}_M \times \mathbb{Z}_L \tag{14}$$

for some unique integers M and L with

$$L \mid M, \qquad LM = \mathcal{E}(\mathbb{F}_q), \qquad L \mid q - 1. \tag{15}$$

Since $d \mid \#\mathcal{E}(\mathbb{F}_q)$ we see from (14) and (15) that we can write $d = d_1 d_2$ where $d_1 = \gcd(d, M)$ and $d_2 \mid d_1$. It is now easy to see that

$$\#\mathcal{H}_d \geq d, \tag{16}$$

(clearly $\mathcal{H}_d$ is a subgroup of the group $\mathcal{E}[d]$ of d-torsion points on $\mathcal{E}$, thus we also have $\#\mathcal{H}_d \leq d^2$, see [2, 4, 25]).

For any point $Q \in \mathcal{E}(\mathbb{F}_q)$ we have

$$S_n(\psi; a, b) = \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P \oplus Q) + bx(n(P \oplus Q))\right).$$

Therefore, we obtain

$$\begin{aligned} S_n(\psi; a, b) &= \frac{1}{\#\mathcal{H}_d} \sum_{Q \in \mathcal{H}_d} \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P \oplus Q) + bx(n(P \oplus Q))\right) \\ &= \frac{1}{\#\mathcal{H}_d} \sum_{Q \in \mathcal{H}_d} \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P \oplus Q) + bx(nP)\right) \\ &= \frac{1}{\#\mathcal{H}_d} \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \sum_{Q \in \mathcal{H}_d} \psi\left(bx(nP)\right) \psi\left(ax(P \oplus Q)\right). \end{aligned}$$

Now applying Theorem 3 with $\mathcal{P} = \mathcal{E}(\mathbb{F}_q)$ and $\mathcal{Q} = \mathcal{H}_d$, we have

$$|S_n(\psi; a, b)| \ll \frac{1}{\#\mathcal{H}_d} \left(q^2 \#\mathcal{H}_d\right)^{1/2} \ll \frac{q}{d^{1/2}}$$

which concludes the proof. $\square$

Note that for $d \le q$, Theorem 9 is an improvement on (12) and (13). If $d > q$, then from the fact that $\#\mathcal{E}(\mathbb{F}_q) \le q + 1 + 2\sqrt{q}$, see [25, Chapter 5, Theorem 1.1], it follows that $d = \#\mathcal{E}(\mathbb{F}_q)$ and hence in this case from (12) and Theorem 9 we have

$$S_n(\psi; a, b) = \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P) + bx(nP)\right) = \sum_{P \in \mathcal{E}(\mathbb{F}_q)} \psi\left(ax(P)\right) \ll \sqrt{q}.$$

4.2 Sum with the elliptic curve power generator

We now improve the results of [3, 9] on the distribution of the *power generator* on elliptic curves. Namely, given a point $G \in \mathcal{E}(\mathbb{F}_q)$ of order t, we fix an integer e with $\gcd(e, t) = 1$, put $W_0 = G$ and consider the sequence

$$W_n = eW_{n-1}, \qquad n = 1, 2, \ldots. \tag{17}$$

In a more explicit form we have $W_n = e^n G$. Clearly, the sequence W_n is periodic with period T which is the multiplicative order of e modulo t.

For a point $G \in \mathcal{E}(F_q)$, a nonprincipal additive character ψ of $\mathbb{F}_q$ and an integer N, we consider character sums

$$S(G, \psi, N)) = \sum_{n=0}^{N-1} \psi\left(x(W_n)\right)$$

with the sequence (17).

For $N = T$ the sum $S(G, \psi, T)$ is estimated in [16], where it is shown that for any fixed positive integer ν, we have

$$S(G, \psi, T) \ll T^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)}.$$

In [9], using two different approaches the above result is extended to incomplete sums $S(G, \psi, N)$ with $N \le T$. One of the approaches has led to

$$S(G, \psi, N) \ll N^{1-(3\nu+2)/2\nu(\nu+3)} t^{(\nu+1)/\nu(\nu+3)} q^{1/4(\nu+3)}. \qquad (18)$$

while the other one has yielded

$$S(G, \psi, N) \ll T^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} \log q. \qquad (19)$$

Notice that the bound (18) is stronger than (19) for short sums but for almost complete sums, the bound (19) is stronger.

Here using Lemma 2 and an inductive argument, we give a bound that improves both (18) and (19).

Theorem 10. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $N \le T$. Suppose that for some fixed $\varepsilon > 0$ we have $t \ge q^{1/2+\varepsilon}$. Then for any fixed integer $\nu \ge 1$ there exists $C(\nu, \varepsilon) \ge 1$ depending only on ν and ε such that*

$$S(G, \psi, N) \le C(\nu, \varepsilon) N^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)}.$$

Proof. Our proof is based on an induction.

Notice that if $N \le q^{1/2}$, then since $t \ge q^{1/2+\varepsilon}$ we have

$$N^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)} \ge N,$$

and thus the claim holds trivially.

Now suppose that the claim is true for all $k < N$, and hence there exists $C(\nu, \varepsilon)$, which is to be determined later, depending only on ν and ε, so that for all $k < N$, we have

$$S(G, \psi, k) \leq C(\nu, \varepsilon) k^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)}.$$

Let $\mathcal{M} = \{0, \dots, M-1\}$ where $M < N$. For every $m \in \mathcal{M}$, we have

$$S(G, \psi, N) = \sum_{n=0}^{N-1} \psi\left(x(e^{n+m}G)\right) + S(G, \psi, m) - S(H, \psi, m),$$

where $H = e^N G$, and hence

$$\sum_{m=0}^{M-1} S(G, \psi, N) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \psi\left(x(e^{n+m}G)\right) + \sum_{m=0}^{M-1} S(G, \psi, m) - \sum_{m=0}^{M-1} S(H, \psi, m).$$

Notice that our bounds hold for any point of order t, and thus using the fact that $\gcd(e, t) = 1$ we can apply the induction hypothesis to the point H too. Hence by the induction hypothesis we have

$$\begin{aligned} &M|S(G_0, \psi, N)| \\ &\qquad \leq W + 2MC(\nu, \varepsilon) M^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)}, \end{aligned}$$

where

$$W = \left| \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \psi\left(x(e^{n+m}G)\right) \right|.$$

Applying Lemma 2, we get

$$W \leq D(\nu, \varepsilon) (M)^{1-1/2\nu} (N)^{1-1/(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)}$$

for some $D(\nu, \varepsilon)$ depending only on ν and ε. From the two inequalities above, we have

$$\begin{aligned} &|S(G_0, \psi, N)| \\ &\quad \leq D(\nu, \varepsilon) M^{-1/2\nu} N^{1-1/(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)} \\ &\qquad + 2C(\nu, \varepsilon) M^{1-(3\nu+2)/2\nu(\nu+2)} t^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\log q)^{1/(\nu+2)}. \end{aligned}$$

We see that it suffices to take $M = \lceil N/2 \rceil$ and

$$C(\nu, \varepsilon) = \frac{2^{1/2\nu}}{1 - 2^{(3\nu+2)(2\nu(\nu+2)}} D(\nu, \varepsilon).$$

to conclude the proof. □

Notice that when $t = q^{1+o(1)}$ which is the most interesting case, taking ν to be a very large number shows that the bound in Theorem 10 is stronger than the bound (18) whenever $N \geq q^{5/6+\varepsilon}$ for some fixed $\varepsilon > 0$.

5 Comments

Dvir [8] has considered the problem of constructing randomness extractors for algebraic varieties. In general terms the problem can be described as follows. Giving an algebraic variety $\mathcal{V}$ over $\mathbb{F}_q$ and one or several sources of random but not necessarily uniformly generated points on $\mathcal{V}$, design an algorithm to generate long string of random bits with a distribution that is close to uniform. The construction of [8] requires only one but rather uniform source of points on $\mathcal{V}$. In the case when $\mathcal{V} = \mathcal{E}$, the result of Theorem 3 has a natural interpretation as a two-source extractor from two biased sources of points P and Q, respectively. Say, if $q = p$, then one can use most significant bits of $x(P \oplus Q)$ (in some standard representation of the residues modulo p). The exact number of output bits depends on the bias of the sources of points P and Q.

We also remark that many of our results have direct analogues for sums with multiplicative characters.

6 Acknowledgements

During the preparation of this paper, O.A. was supported in part by a grant from IPM Grant 91050418 (Iran) and I. S. by ARC Grant DP1092835 (Australia) and by NRF Grant CRP2-2007-03 (Singapore).

A portion of this work was done when the authors were visiting the University of Waterloo; the support and hospitality of this institution are gratefully acknowledged.

References

[1] O. Ahmadi and I. E. Shparlinski, 'Bilinear character sums and the sum-product problem on elliptic curves', *Proc. Edinb. Math. Soc.*, **53** (2010), 1–12.

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and hyperelliptic curve cryptography: Theory and practice*, CRC Press, 2005.

[3] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Double character sums over elliptic curves and finite fields', *Pure and Appl. Math. Quart.*, **2** (2006), 179–197.

[4] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, **265**, Cambridge Univ. Press, 1999.

[5] E. Bombieri, 'On exponential sums in finite fields', *Amer. J. Math.*, **88** (1966), 71–105.

[6] W. Bosma, 'Signed bits and fast exponentiation', *J. Théorie des Nombres Bordeaux*, **13** (2001), 27–41.

[7] Z. Chen, 'Elliptic curve analogue of Legendre sequences', *Monatsh Math.*, **154** (2008), 1–10.

[8] Z. Dvir, 'Extractors for varieties', *Comput. Complex.*, **21** (2012), 515–572.

[9] E. El Mahassni and I. E. Shparlinski, 'On the distribution of the elliptic curve power generator', *Proc. 8th Conf. on Finite Fields and Appl.*, Contemporary Math., **461**, Amer. Math. Soc., 2008, 111–119.

[10] R. R. Farashahi and I. E. Shparlinski, 'Pseudorandom bits from points on elliptic curves', *Preprint*, 2009.

[11] R. P. Gallant, R. J. Lambert and S. A. Vanstone, 'Faster point multiplication on elliptic curves with efficient endomorphisms', *Proc Crypto 2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2139** (2001), 190–200.

[12] M. Z. Garaev, 'An estimate of Kloosterman sums with prime numbers and an application', *Matem. Zametki*, **88** (2010), 365–373 (in Russian).

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

[14] N. Koblitz, 'CM curves with good cryptographic properties', *Proc. Crypto 1991, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **576** (1992), 279–287.

[15] D. R. Kohel and I. E. Shparlinski, 'Exponential sums and group generators for elliptic curves over finite fields', *Proc. the 4th Algorithmic Number Theory Symp., Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 395–404.

[16] T. Lange and I. E. Shparlinski, 'Certain exponential sums and random walks on elliptic curves', *Canad. J. Math.*, **57** (2005), 338–350.

[17] T. Lange and I. E. Shparlinski, 'Distribution of some sequences of points on elliptic curves', *J. Math. Cryptology*, **1** (2007), 1–11.

[18] A. Ostafe and I. E. Shparlinski, 'Twisted exponential sums over points of elliptic curves', *Acta Arith.*, **148** (2011), 77–92.

[19] A. Ostafe and I. E. Shparlinski, 'Exponential sums over points of elliptic curves with reciprocals of primes', *Mathematika*, **58** (2012), 21–33.

[20] A. Sárközy, 'On sums and products of residues modulo p', *Acta Arith.*, **118** (2005), 403–409.

[21] I. E. Shparlinski, 'Bilinear character sums over elliptic curves', *Finite Fields and Their Appl.*, **14** (2008), 132–141.

[22] I. E. Shparlinski, 'On the elliptic curve analogue of the sum-product problem', *Finite Fields and Their Appl.*, **14** (2008), 721–726.

[23] I. E. Shparlinski, 'Some special character sums over elliptic curves', *Bol. Soc. Matem. Mexicana*, **15** (2009), 37–40.

[24] I. E. Shparlinski, 'Pseudorandom number generators from elliptic curves', Recent Trends in Cryptography, *Contemp. Math.*, vol. 477, Amer. Math. Soc., (2009), 121–141.

[25] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 2009.