On the elliptic curve analogue of the sum-product problem

Igor Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

Received 25 September 2007; revised 11 December 2007
Available online 10 January 2008
Communicated by Gary L. Mullen

Abstract

Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ of $q$ elements and $x(P)$ to denote the $x$-coordinate of a point $P = (x(P), y(P)) \in E$. Let $\oplus$ denote the group operation in the Abelian group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on $E$. We show that for any sets $R, S \subseteq E(\mathbb{F}_q)$ at least one of the sets

$$\{x(R) + x(S) : R \in R, S \in S\} \quad \text{and} \quad \{x(R \oplus S) : R \in R, S \in S\}$$

is large. This question is motivated by a series of recent results on the sum-product problem over $\mathbb{F}_q$.

© 2008 Elsevier Inc. All rights reserved.

Keywords: Sum-product problem; Elliptic curves; Character sums

1. Introduction

We fix a finite field $\mathbb{F}_q$ of $q$ elements and an elliptic curve $E$ over $\mathbb{F}_q$ given by an affine Weierstraß equation

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

with some $a_1, \ldots, a_6 \in \mathbb{F}_q$, see [11].
We recall that the set of all points on \( E \) forms an Abelian group, with the point at infinity \( O \) as the neutral element, and we use \( \oplus \) to denote the group operation (we also use \( \ominus \) in its natural meaning). As usual, we write every point \( P \neq O \) on \( E \) as \( P = (x(P), y(P)) \).

Let \( E(\mathbb{F}_q) \) denote the set of \( \mathbb{F}_q \)-rational points on \( E \).

We show that for any sets \( R, S \subseteq E \), at least one of the sets

\[
U = \{ x(R) + x(S) : R \in \mathcal{R}, \ S \in \mathcal{S} \},
V = \{ x(R \oplus S) : R \in \mathcal{R}, \ S \in \mathcal{S} \},
\]

is large.

This question is motivated by a series of recent results on the sum-product problem over \( \mathbb{F}_q \) which assert that for any sets \( A, B \subseteq \mathbb{F}_q \), at least one of the sets

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

is large, see [1–8] for the background and further references.

In fact, our approach is a combination of the argument of M. Garaev [4] and an estimate of [10] of certain bilinear character sums over points of \( E(\mathbb{F}_q) \). We recall the idea of [4] (extended to the case of two distinct sets instead of just \( A = B \) as in [4]) to obtain upper and lower bounds on the number of solutions \( (a_1, a_2, g, h) \) to the equation

\[
a_1 a_2^{-1} + a_2 = g, \quad a_1, a_2 \in \mathcal{A}, \ g \in \mathcal{G}, \ h \in \mathcal{H}.
\]

This equation obviously has at least \((\#\mathcal{A})^2 \#\mathcal{B}\) as the solutions of the form \( (a_1, a_2, a_2 + b, a_1 b) \), \( a_1, a_2 \in \mathcal{A}, \ b \in \mathcal{B} \). There are now several ways to get the upper bound \((\#\mathcal{A})^2 \#\mathcal{G}\#\mathcal{H}/q + O(q^{1/2}\#\mathcal{A}(\#\mathcal{G}\#\mathcal{H})^{1/2})\) on the number of solutions. For example, one can simply use the result of A. Sárközy [9] (see also [4]).

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

2. Sum-product estimate for elliptic curves

**Theorem 1.** Let \( \mathcal{R} \) and \( \mathcal{S} \) be arbitrary sets of \( E(\mathbb{F}_q) \). Then for the sets \( \mathcal{U} \) and \( \mathcal{V} \), given by (1), we have

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

**Proof.** Let

\[
\mathcal{W} = \{ R \oplus S : R \in \mathcal{R}, \ S \in \mathcal{S} \}.
\]

Following the idea of M. Garaev [4], we now denote by \( J \) the number of solutions \( (S_1, S_2, W, u) \) to the equation

\[
x(W \ominus S_1) + x(S_2) = u, \quad S_1, S_2 \in \mathcal{S}, \ W \in \mathcal{W}, \ u \in \mathcal{U}.
\]
Since obviously the vectors
\[(S_1, S_2, W, u) = (S_1, S_2, R \oplus S_1, x(R) + x(S_2)), \quad R \in \mathcal{R}, \ S_1, S_2 \in \mathcal{S},\]
are all pairwise distinct solutions to (3), we obtain
\[J \geq \#\mathcal{R}(\#\mathcal{S})^2.\]  
(4)

To obtain an upper bound on \(J\) we use \(\Psi\) to denote the set of all \(q\) additive characters of \(\mathbb{F}_q\) and write \(\Psi^*\) for the set of nontrivial characters. Using the identity
\[1_q \sum_{\psi \in \Psi} \psi(z) = \begin{cases} 0, & \text{if } z \in \mathbb{F}_q^*, \\ 1, & \text{if } z = 0, \end{cases}\]  
(5)
we obtain
\[J = \sum_{S_1 \in \mathcal{S}} \sum_{S_2 \in \mathcal{S}} \sum_{W \in \mathcal{W}} \sum_{u \in \mathcal{U}} \frac{1}{q} \sum_{\psi \in \Psi} \psi\left(x(W \ominus S_1) + x(S_2) - u\right)\]
\[= \frac{1}{q} \sum_{\psi \in \Psi} \sum_{S_1 \in \mathcal{S}} \sum_{W \in \mathcal{W}} \psi\left(x(W \ominus S_1)\right) \sum_{S_2 \in \mathcal{S}} \psi\left(x(S_2)\right) \sum_{u \in \mathcal{U}} \psi\left(-u\right)\]
\[= \frac{(\#\mathcal{S})^2 \#\mathcal{U} \#\mathcal{W}}{q} + \frac{1}{q} \sum_{\psi \in \Psi^*} \sum_{S_1 \in \mathcal{S}} \sum_{W \in \mathcal{W}} \psi\left(x(W \ominus S_1)\right) \sum_{S_2 \in \mathcal{S}} \psi\left(x(S_2)\right) \sum_{u \in \mathcal{U}} \psi\left(-u\right).\]

We now recall the main result of [10]. Let
\[T_{\rho, \vartheta}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{P \in \mathcal{P}} \sum_{Q \in \mathcal{Q}} \rho(P) \vartheta(Q) \psi\left(x(P \oplus Q)\right),\]  
(6)
where \(\mathcal{P}, \mathcal{Q} \subseteq \mathbb{E}(\mathbb{F}_q)\), \(\rho(P)\) and \(\vartheta(Q)\) are arbitrary complex functions supported on \(\mathcal{P}\) and \(\mathcal{Q}\) with
\[|\rho(P)| \leq 1, \quad P \in \mathcal{P}, \quad \text{and} \quad |\vartheta(Q)| \leq 1, \quad Q \in \mathcal{Q},\]
and \(\psi\) is a nontrivial additive character of \(\mathbb{F}_q\). Note that we always assume that the values for which the corresponding summation term is not defined (that is, the terms with \(P = -Q\)) are excluded from the summation.

For the sum \(T_{\rho, \vartheta}(\psi, \mathcal{P}, \mathcal{Q})\) given by (6) it is shown in [10] that for any fixed integer \(\nu \geq 1\) we have
\[T_{\rho, \vartheta}(\psi, \mathcal{P}, \mathcal{Q}) \ll (\#\mathcal{P})^{1-1/2^\nu}(\#\mathcal{Q})^{1/2}q^{(1/2^\nu)+1/2} + (\#\mathcal{P})^{1-1/2^\nu}(\#\mathcal{W})^{1/2}q^{1/(4^\nu)}.\]  
(7)
In our case (taking this bound with \(\nu = 1\), \(\rho(P) = \vartheta(Q) = 1\), \(\mathcal{P} = \mathcal{W}\), \(\mathcal{Q} = \mathcal{S}\)) it implies that
\[\sum_{S_1 \in \mathcal{S}} \sum_{W \in \mathcal{W}} \psi\left(x(W \ominus S_1)\right) \ll (\#\mathcal{W})^{1/2}(\#\mathcal{S})^{1/2}q^{1/2} + (\#\mathcal{W})^{1/2}\#\mathcal{S}q^{1/4}.\]
Therefore,

\[ J \sim \frac{(\#S)^2 \#U \#V}{q} \ll \left( (\#V)^{1/2} (\#S)^{1/2} q^{1/2} + (\#W)^{1/2} \#S q^{1/4} \right) \frac{1}{q} \sum_{\psi \in \Psi^*} \left| \sum_{S \in S} \psi(x(S)) \right| \left| \sum_{u \in U} \psi(u) \right|. \]  

(8)

Extending the summation over \( \psi \) to the full set \( \Psi \) and using the Cauchy inequality, we obtain

\[ \sum_{\psi \in \Psi^*} \left| \sum_{S \in S} \psi(x(S)) \right| \left| \sum_{u \in U} \psi(u) \right| \leq \sqrt{\sum_{\psi \in \Psi} \left| \sum_{S \in S} \psi(x(S)) \right|^2 \sum_{\psi \in \Psi} \left| \sum_{u \in U} \psi(u) \right|^2}. \]  

(9)

Recalling the orthogonality property (5), we derive

\[ \sum_{\psi \in \Psi^*} \left| \sum_{S \in S} \psi(x(S)) \right|^2 = q \#\{(S_1, S_2) \in S^2 : x(S_1) = x(S_2)\} \leq 2q \#S, \]

since as it immediately follows from the Weierstraß equations, the curve \( E \) contains at most 2 points with a given value of the \( x \)-coordinate. Similarly,

\[ \sum_{\psi \in \Psi} \left| \sum_{u \in U} \psi(u) \right| \leq q \#U. \]

Substituting these bounds in (9) we obtain

\[ \sum_{\psi \in \Psi^*} \left| \sum_{S \in S} \psi(x(S)) \right| \left| \sum_{u \in U} \psi(u) \right| \ll q \sqrt{\#S \#U}, \]

which after inserting in (8), yields

\[ J \sim \frac{(\#S)^2 \#U \#V}{q} \ll \left( \#V \#U \right)^{1/2} \left( \#S q^{1/2} + (\#S)^{3/2} q^{1/4} \right). \]  

(10)

Thus, comparing (4) and (10), we derive

\[ \frac{(\#S)^2 \#U \#V}{q} + \left( \#V \#U \right)^{1/2} \left( \#S q^{1/2} + (\#S)^{3/2} q^{1/4} \right) \gg \#R (\#S)^2. \]

Since there are at most two points \( P \in E(\mathbb{F}_q) \) with the same value of \( x(P) \), we see that \( \#V \geq 0.5 \#W \). Hence,

\[ \#U \#V \gg \min\{q \#R, (\#R \#S)^2 q^{-1}, (\#R)^2 \#S^{-1/2}\}. \]
It remains to remark that since we obviously have \( \min\{\#U, \#V\} \geq \#R \) the bound of the theorem is nontrivial only if \( \#S \geq q^{1/2} \), in which case
\[
(#R\#S)^2 q^{-1} \geq (#R)^2 S q^{-1/2},
\]
which concludes the proof. \( \square \)

**Corollary 2.** Let \( R \) and \( S \) be arbitrary sets of \( E(\mathbb{F}_q) \) with
\[
q^{1-\varepsilon} \geq \#R \geq \#S \geq q^{1/2+\varepsilon}.
\]
Then for the sets \( U \) and \( V \), given by (1), we have
\[
\#U\#V \gg (#R)^2 q^\varepsilon.
\]

**Corollary 3.** Let \( R = S \) be an arbitrary set of \( E(\mathbb{F}_q) \) with
\[
\#R \geq q^{3/4}.
\]
Then for the sets \( U \) and \( V \), given by (1), we have
\[
\#U\#V \gg q\#R.
\]

3. **Comments**

It seems that the bound (7) is useful for our purpose only when it is taken with \( \nu = 1 \). However, several other equations, besides (2), have been used to obtain various lower bounds in the sum-product problem over finite fields. One can certainly try to use their analogues for its elliptic curve version which we have considered in the present paper. Possibly for some of them one can make use of (7) in its full generality.

Finally, as in [4] we can justify that the quantity \( q\#R \) should be present in any lower bound on \( \#U\#V \). Indeed, let \( q = p \) be prime and let \( E \) be a curve over \( \mathbb{F}_p \) such that \( E(\mathbb{F}_p) \) is a cyclic group (see [12] on statistics of cyclic elliptic curves) and let \( G \) be a generator. Let \( N \leq \min\{\#E(\mathbb{F}_p), p\} \) be any positive integer. We now take \( M = \lceil (pN)^{1/2} \rceil \). Then the pigeonhole principle implies that for some integer \( L \) there is a set \( M \in \{1, \ldots, M\} \) of cardinality \( \#M \geq M^2 / p \geq N \) such that
\[
x(mG) \in \{L + 1 \mod p, \ldots, L + M \mod p\}, \quad m \in M.
\]
We not take any subset \( N \subseteq M \) of cardinality \( N \) and put \( R = S = nG, n \in N \). Clearly, for the sets \( U \) and \( V \), given by (1) we have
\[
\max\{\#U, \#V\} \leq M \ll (p\#R)^{1/2}.
\]

**Acknowledgment**

This work was supported in part by ARC grant DP0556431.
References