Uniform Distribution Theory **9** (2014), no.2, 59–65

uniform
distribution
theory

ON THE ELLIPTIC CURVE POWER GENERATOR

László Mérai

ABSTRACT. For a given elliptic curve $\mathcal{E}$ we obtain an upper bound on a character sum formed by linear combination of $f(kQ)$ where Q runs on the curve and f arbitrary rational function.

We apply the result to study the elliptic curve analogue of the power generator.

Communicated by W.G. Nowak

1. Introduction

Let $p > 3$ be a prime number and $\gamma \geq 1$ be a positive integer. Let $\mathbb{F}_q$ denote the finite field of $q = p^\gamma$ elements.

Let $e, m \geq 2$ and ϑ be positive integers such that $(m, \vartheta) = 1$. The *power generator* defines the sequence u_n by the rule

$$u_n \equiv u_{n-1}^e \pmod{m}, \quad 0 \leq u_n < m, \qquad n = 1, 2, \ldots \tag{1}$$

with the initial value $u_0 = \vartheta$. The power generator has many application see [2].

Let $\mathcal{E}$ be an elliptic curve defined by the short Weierstrass equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_q$$

with non-zero discriminant (see [7]). We recall that the $\mathbb{F}_q$-rational points $\mathcal{E}(\mathbb{F}_q)$ of the curve $\mathcal{E}$ with the usual addition $\oplus$ form an Abelian group with the point in infinity $\mathcal{O}$ as a neutral element. Let $\mathbb{F}_q(\mathcal{E})$ denote the function field of the curve $\mathcal{E}$ over $\mathbb{F}_q$, and let $x(\cdot)$ and $y(\cdot)$ be the coordinate functions. We denote by $\deg(f)$ the degree of the pole divisor of f. In particular, $\deg(x) = 2$ and $deg(y) = 3$.

Recall that the torsion group $\mathcal{E}[m]$ of the curve is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_m$ if $p \nmid m$. If m has the form $m = p^r m'$, where $r \geq 1$ and $p \nmid m'$, then $\mathcal{E}[m]$ is

2010 Mathematics Subject Classification: 11L07, 11T23, 14H52, 11K45.
Keywords: elliptic curves, power generator, exponential sums, discrepancy.
Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. K100291 and by the Momentum (Lendület) fund of the Hungarian Academy of Sciences.

isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_{m'}$ or $\mathbb{Z}_{m'} \times \mathbb{Z}_{m'}$. Specially, $\mathcal{E}[p]$ is isomorphic to $\mathbb{Z}_p$ when the curve is said to be *ordinary* or $\mathcal{E}[p] = \{\mathcal{O}\}$ when the curve is *supersingular*.

In 2005, Lange and Shparlinski [6] defined the elliptic curve analogue of the generator (1). Let $P \in \mathcal{E}(\mathbb{F}_p)$ be a point of order T and e be an integer such that $(T, e) = 1$. The *elliptic curve power generator* builds a sequence by the rule

$$U_n = eU_{n-1} \quad n = 1, 2, \dots \tag{2}$$

with the initial value $U_0 = P$. If the order of e is t modulo T, then clearly the sequence U_n is a purely periodic sequence with period length t.

An obvious way to compute the elements of the sequence is to compute e which would be the solution of the discrete logarithm problem on this curve. On the other hand to compute an element from the previous part of the sequence one may need to solve the computational Diffie-Hellman problem. Since in general both of these problems are assumed to be hard, the elliptic curve power generator is thought to have good pseudorandom properties.

The distribution of the coordinate sequence $\big(x(U_n)\big)$ have been widely studied. For example Lange and Shparlinski [6] showed that this sequence has large linear complexity and is uniformly distributed (see also [1]). Their proof is based on the following character sum estimate: if $\mathcal{E}$ is an ordinary curve, $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$, ψ is a non-principal additive character of $\mathbb{F}_q$, then for integers $1 \le k_1 < \dots < k_s \le K$ we have

$$\sum_{P \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i x(k_i P)\right) \ll sK^2 q^{1/2}$$

for all all integers $c_1, \dots, c_s$ such that not all of them are zeros.

Using the character sum estimate a non-trivial upper bound was proved to the discrepancy of $\big(x(U_n)\big)_{n=1}^{t}$.

As it was pointed out in [6] similar result can be proven for sums with $y(k_iP)$ or linear combinations $ax(k_iP) + by(k_iP)$. In this paper we prove a result about sums with $f(k_iP)$, where $f \in \mathbb{F}_q(\mathcal{E})$ is arbitrary non-constant function

$$\sum_{P \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i f(k_i P)\right). \tag{3}$$

In Section 2 we prove a non-trivial bound to (3). When the curve is defined over a prime field $\mathbb{F}_p$, by using the same argument than [1], the result immediately gives a bound on the sum

$$\sum_{n=1}^{N} \mathbf{e}_p\big(f(U_n)\big),$$

where $\mathbf{e}_p(\alpha) = \exp(2\pi i\alpha/p)$.

In Section 3 we obtain a discrepancy bound of $\big(f(U_n)\big)$ by the Erdős-Turán-Koksma inequality. We state the result in a general form, namely we state a result about the discrepancy of the s-tuples $\big(f(U_n),\dots,f(U_{n+s-1})\big)$, however the bound will only be non-trivial if $s=1$ or e is small.

2. A character sum

We will need the following result about character sums over elliptic curves proved by Kohel and Shparlinski [5].

Lemma 1. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$. Let $f\in\mathbb{F}_q(\mathcal{E})$ be a non-constant function and ψ a non-trivial additive character of $\mathbb{F}_q$. Then the bound*

$$\left|\sum_{\substack{Q\in\mathcal{H}\\ f(Q)\neq\infty}} \psi\big(f(Q)\big)\right| \le 2q^{1/2}\deg f$$

holds, where $\mathcal{H}$ is an arbitrary subgroup of $\mathcal{E}(\mathbb{F}_q)$.

Theorem 2. *Let $1\le k_1<\dots<k_s\le K$ be fixed integers, $c_1,\dots,c_s\in\mathbb{F}_q$ such that $c_s\neq 0$. Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_q$. Let $f\in\mathbb{F}_q(\mathcal{E})$ be a non-constant function, and ψ a non-trivial additive character of $\mathbb{F}_q$. Then the bound*

$$\sum_{\substack{Q\in\mathcal{H}\\ f(Q)\neq\infty}} \psi\left(\sum_{i=1}^{s} c_i f(k_iQ)\right) \ll q^{1/2}sK^2\deg f$$

holds, where $\mathcal{H}$ is a subgroup of $\mathcal{E}(\mathbb{F}_q)$ such that $(|\mathcal{H}|,k_1\cdots k_s)=1$. The implied constant does not depend on $k_1,\dots,k_s$.

Proof. First we show that the function $F(P)=\sum_{i=1}^{s}c_if(k_iP)\in\mathbb{F}_q(\mathcal{E})$ is not a constant function. Let Q be a pole of f with maximal order d. Now we have $Q\in\mathcal{E}[d]\subset\mathcal{E}[dk_s]$. Write $d=p^\alpha d'$ and $k_s=p^\beta k_s'$ with $\alpha,\beta\ge 0$ and $p\nmid d',k_s'$. Let Q_1,Q_2 be points of order dk_s and $d'k_s'$ which generate $\mathcal{E}[kd_s]$:

$$\mathcal{E}[kd_s]=\{a_1Q_1\oplus a_2Q_2:\ 0\le a_1<dk_s, 0\le a_2<d'k_s'\}.$$

Write $Q=a_1Q_1\oplus a_2Q_2$. Since

$$da_1Q_1\oplus da_2Q_2=dQ=\mathcal{O},$$

we have

$$da_1Q_1=da_2Q_2=\mathcal{O}$$

thus

$$dk_s \mid da_1, \quad d'k'_s \mid da_2. \tag{4}$$

From the first relation we have $k_s \mid a_1$. Let

$$a_1^* = \frac{a_1}{k_s} \in \mathbb{N}.$$

On the other hand from the second relation of (4) we have $k'_s \mid a_2$ which means that the congruence

$$k_s a_2^* \equiv a_2 \mod d'k'_s$$

has a solution in a_2^*. Let $Q^* = a_1^* Q_1 \oplus a_2^* Q_2$, where now $k_s Q^* = Q$.

Clearly, each elements of $Q^* \oplus E[k_s]$ is a pole of $f(k_s P)$ and there are elements of order $d \cdot k_s$ among them. By the maximality of d and k_s these elements are not poles of the other terms $f(k_i P)$ $(i < s)$.

Finally, we remark that a point P is a pole of $f(kP)$ iff $P \in Q \oplus \mathcal{E}[k]$, where kQ is a pole of f. Therefore $\deg f(kP) \le k^2 \deg f(P)$.

□

Using Theorem 2 we can prove the following bound of double exponential sums in the same way as [1]:

Corollary 3. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$ and $G \in \mathcal{E}(\mathbb{F}_p)$ be a point with order T. Let $f \in \mathbb{F}_p(\mathcal{E})$ be a non-constant function. Then for all sets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_T$ and all $\varepsilon > 0$ the following bound holds*

$$\sum_{u\in\mathcal{U}} \sum_{v\in\mathcal{V}} \alpha_u \beta_v \mathbf{e}_p\big(f(uvG)\big) \ll ABT^{5/6}(|\mathcal{U}||\mathcal{V}|)^{1/2} p^{1/12+\varepsilon} \deg f,$$

where

$$A = \max_{u\in\mathcal{U}} |\alpha_u|, \quad B = \max_{v\in\mathcal{V}} |\beta_v|$$

and the implied constant depends only on ε.

We use Corollary 3 to derive a bound for incomplete exponential sums for the sequence (2).

Theorem 4. *Let $\mathcal{E}$ be an ordinary elliptic curve defined over $\mathbb{F}_p$ and $G \in \mathcal{E}(\mathbb{F}_p)$ be a point with order T. Let $f \in \mathbb{F}_p(\mathcal{E})$ be a non-constant function. If $e \ge 2$ is an integer such that $(e, T) = 1$, then for $1 \le N \le T$ and for all $\varepsilon > 0$ we have*

$$\sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{i=0}^{s-1} a_i f(e^{n+i} G) \right) \ll N^{1/3} T^{5/9} p^{1/18+\varepsilon} s e^{2(s-1)} \deg f.$$

Proof. Let $L = \lceil N^{1/3} T^{5/9} p^{1/18} \deg f \rceil$. Then

$$\begin{aligned}
&\sum_{l=0}^{L-1}\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^{n+l}e^i G)\right)\\
&= \sum_{m=0}^{L-2}(m+1)\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^m e^i G)\right) + L\sum_{m=L-1}^{N-1}\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^m e^i G)\right)\\
&\quad+\sum_{m=N}^{N+L-2}(N+L-1-m)\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^m e^i G)\right)\\
&= L\sum_{m=0}^{N-1}\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^m e^i G)\right) + O(L^2),
\end{aligned}$$

i.e.,

$$\sum_{m=0}^{N-1}\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^{m+i} G)\right) = \frac{1}{L}\sum_{l=0}^{L-1}\sum_{n=0}^{N-1}\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^n e^l e^i G)\right) + O(L).$$

Since the degree of $F(P) = \sum_{i=0}^{s-1} a_i f(e^i G)$ is $\deg F \leq s e^{2(s-1)} \deg f$, applying Corollary 3 we get

$$\sum_{m=0}^{N-1}\mathbf{e}_p\left(\sum_{i=0}^{s-1} a_i f(e^{m+i} G)\right) \ll \frac{1}{L} T^{5/6} (LN)^{1/2} p^{1/12+\varepsilon} s e^{2(s-1)} \deg f.$$

By the choice of L we get the result.

□

3. Discrepancy

Using the exponential sum estimate proved in Theorem 4, the Erdős-Turán-Koksma inequality gives a non-trivial bound on the discrepancy of the s-tuple $\big(f(U_n), \dots, f(U_{n+s-1})\big)$ if $s = 1$ or e is small.

For a given sequence Γ of N points

$$\Gamma = \{(\gamma_{n,1}, \dots, \gamma_{n,s}) : n = 1, \dots, N\} \tag{5}$$

in the s-dimensional unite cube $[0,1)^r$ the *discrepancy* $\Delta(\Gamma)$ of Γ is defined by

$$\Delta(\Gamma) \overset{\text{def}}{=} \sup_I \left| \frac{A_\Gamma(I)}{N} - |I| \right|,$$

where $I = \prod_{i=1}^{s}[u_i, v_i)$ is a sub-interval of $[0,1)^s$ and $A_\Gamma(I)$ is the number of points of Γ belonging to I.

We use the Erdős-Turán-Koksma inequality in the following form (see [3, Theorem 1.21]):

Lemma 5. *For any integer $H > 1$ and any sequence Γ of N points the discrepancy $\Delta(\Gamma)$ satisfies*

$$\Delta(\Gamma) \le \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \frac{1}{N}\sum_{\boldsymbol{h}}\prod_{j=1}^{s}\frac{1}{\max\{|h_j|,1\}}\left|\sum_{n=1}^{N} e\left(\sum_{l=1}^{s} h_l\gamma_{n,l}\right)\right|\right),$$

where the outer sum is taken over all vectors $\boldsymbol{h} = (h_1, \dots, h_s) \in \mathbb{Z}^r \setminus \boldsymbol{0}$ such that $|h_j| \le H$ for all $j = 1, \dots, s$.

Theorem 4 and the Erdős-Turán-Koksma bound implies a bound of the discrepancy of the sequence of points

$$\Gamma(N,s) = \left\{\left(\frac{f(U_nG)}{p}, \dots, \frac{f(U_{n+s-1}G)}{p}\right) : \ n = 1, \dots, N\right\}. \tag{6}$$

Corollary 6. *If $f \in \mathbb{F}_p(\mathcal{E})$ is a non-constant function and the sequence (U_n) is defined by (2), then*

$$\Delta\bigl(\Gamma(N,s)\bigr) \ll N^{-2/3}T^{5/9}p^{1/18+\varepsilon}s\left(\frac{3}{2}\right)^s e^{2(s-1)} \deg f.$$

4. Remarks

As we have remarked above the discrepancy bound of the s-tuples $(f(U_n), \dots, f(U_{n+s-1}))$ is non-trivial in the case when $s = 1$ or when e is small. However it is not known any non-trivial bound in this case even if the power generator is defined over residue rings (see [4]), or if the power generator is defined over elliptic curves but f is just a coordinate function (see [6]).

REFERENCES

[1] BANKS, W. D.—FRIEDLANDER, J. B.—GARAEV, M. Z.—SHPARLINSKI, I. E.: Double character sums over elliptic curves and finite fields. Pure and Appl. Math. Quart. **2** (2006), 179–197.

[2] MENEZES, A. J.—VAN OORSCHOT, P. C.—VANSTONE, S. A.: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997.

[3] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications*, Springer-Verlag, Berlin, 1997.

[4] FRIEDLANDER, J. B.—SHPARLINSKI, I. E.: *On the distribution of the power generator*, Math. Comp. **7**0 (2001), 1575–1589.

[5] KOHEL, D.—SHPARLINSKI, I. E.: *Exponential sums and group generators for elliptic curves over finite fields*, in: *Proc. Algorithmic Number Theory Symposium, Leiden, 2000*, Lect. Notes in Comp. Sci. **1838**, Springer-Verlag, Berlin, 2000, pp. 395–404.

[6] LANGE, T.—SHPARLISKI, I. E.: Certain exponential sums and random walks on elliptic curves, Canad. J. Math. **57** (2005), 338–350.

[7] SILVERMAN, J. H.: *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.

Received January 1, 2013
Accepted March 28, 2014

László Mérai
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sétány 1/C
H-1117 Budapest
HUNGARY
E-mail: merai@cs.elte.hu