GENERATORS OF ELLIPTIC CURVES OVER FINITE FIELDS

IGOR E. SHPARLINSKI AND JOSÉ FELIPE VOLOCH

Abstract. We prove estimates on character sums on the subset of points of an elliptic curve over $\mathbb{F}_{q^n}$ with x-coordinate of the form $\alpha + t$ where $t \in \mathbb{F}_q$ varies and fixed α is such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. We deduce that, for a suitable choice of α, this subset has a point of maximal order in $E(\mathbb{F}_{q^n})$. This provides a deterministic algorithm for finding a point of maximal order which for a very wide class of finite fields is faster than other available algorithms.

1. Introduction

As usual, for a prime power q we use $\mathbb{F}_q$ to denote the finite field of q elements. We study elliptic curves over extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$.

Let E be an elliptic curve give by given by an affine Weierstraß equation

$$y^2 = x^3 + ax^2 + bx + c$$

with some $a, b, c \in \mathbb{F}_{q^n}$ where q is assumed odd. We recall that the set of all points on E forms an abelian group with the "point at infinity" $\mathcal{O}$ as the neutral element, see [19] for background. Denoting by $E(\mathbb{F}_{q^n})$ the set of $\mathbb{F}_{q^n}$-rational points on E, we have

$$\#E(\mathbb{F}_q) = \mathbb{Z}/M \times \mathbb{Z}/L$$

for for unique integers M and L with $L \mid M$ and $\#E(\mathbb{F}_{q^n}) = ML$. The number M is called the *exponent* of $E(\mathbb{F}_{q^n})$. Points $P \in E(\mathbb{F}_{q^n})$ of order M are called *points of maximum order*.

We recall, that the celebrated work of Schoof [14] provides an algorithm that computes $\#E(\mathbb{F}_q)$ in deterministic polynomial time, see also [1] for more recent improvements (both theoretic and practical). Computing the group structure, that is, the numbers, M and L has also

Date: April 6, 2011.

2010 *Mathematics Subject Classification.* Primary 11G20,11Y16 ; Secondary 11T23.

Key words and phrases. Elliptic curves, generators, finite fields.

been considered in the literature and has turned out to be more difficult. In particular, a probabilistic algorithm of Miller [12] runs in expected polynomial time plus the time needed to factor $\gcd(\#E(\mathbb{F}_q), q-1)$, see also [2]. Furthermore, Friedlander, Pomerance and Shparlinski [7] have shown that for a sufficiently large prime p and for almost all elliptic curves E over $\mathbb{F}_p$, the factorisation part of the algorithm is in fact less time consuming than the rest of the computation (since $\gcd(\#E(\mathbb{F}_q), p-1)$ tends to be rather small). On the other hand, in some case this greatest common divisor is large and is difficult to factor.

The deterministic algorithm of [10] computes the group structure of any elliptic curve over $\mathbb{F}_q$ (and if fact produces two generators of the group of points) in exponential time $O(q^{1/2+o(1)})$ which is too slow for practical applications.

Here we show that, for high degree extensions $\mathbb{F}_{q^n}$ of finite fields $\mathbb{F}_q$, one can design a deterministic polynomial time algorithm, which generates a small set $\mathcal{G}$ of points on $E(\mathbb{F}_{q^n})$ such that at least one point $P \in \mathcal{G}$ is of maximum order. We remark that this is an elliptic curve analogue of the results of [5, 15, 17] (see also [18, Theorem 8]).

The idea is to show that if $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ for some root α of an irreducible polynomial of degree n over $\mathbb{F}_q$, then one can find a point $P \in E(\mathbb{F}_{q^n})$ of maximum order with $x(P) = \alpha + t$ for some $t \in \mathbb{F}_q$, where as usual, we write every point $P \neq \mathcal{O}$ on E as $P = (x(P), y(P))$. In turn, this result is based on a new estimate of character sums over points P of an elliptic curve with x coordinates of the form $x(P) = \alpha + t$. These estimates are analogues of those of Carlitz [3] and Katz [9]. We note that if a finite field $\mathbb{F}_r$ is of the form $r = q^n$ with appropriate q and n, then the above argument immediately gives an explicit construction of small set of points on $E(\mathbb{F}_r)$ which contains a point of an appropriate order. In the case that r is not of a suitable form (and thus $\mathbb{F}_r$ does not have a desired subfield), we use the same approach as in [17]. More precisely, we first build an extension $\mathbb{F}_{r^m}$ which has a necessary subfield, apply our construction construction to $E(\mathbb{F}_{r^m})$ and then use the trace map to come back to points on $E(\mathbb{F}_r)$.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' are absolute (we recall that the notation $U \ll V$ is equivalent to $U = O(V)$).

2. Character Sum Bound

Let α be such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

First, $t \mapsto \alpha + t$ extends to a map

$$\psi_\alpha : \ \mathbb{P}^1 \to R_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{P}^1 \simeq (\mathbb{P}^1)^n,$$

where $R_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ stands for the Weil restriction of scalars functor (see, for example, [6]). We denote $A = R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ and let $\pi : A \to (\mathbb{P}^1)^n$ be the map induced from $x : E \to \mathbb{P}^1$. Let also $C_\alpha \subseteq A$ be the curve

$$C_\alpha = \pi^{-1}(\psi_\alpha(\mathbb{P}^1)). \tag{1}$$

Over $\mathbb{F}_{q^n}$ the cover $C_\alpha \to \mathbb{P}^1$ is given by the system of equations

$$y_i^2 = h_i(t), \qquad i = 1, \ldots, n,$$

where

$$h_i(T) = (T+\alpha^{(i)})^3 + a^{(i)}(T+\alpha^{(i)})^2 + b^{(i)}(T+\alpha^{(i)}) + c^{(i)} \in \mathbb{F}_{q^n}[T], \tag{2}$$

and we denote by $\gamma^{(i)}$, $i = 1, \ldots, n$, the conjugates of $\gamma \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, $\gamma^{(i)} = \gamma^{q^i}$. We also use $A(\mathbb{F}_q)$ and $C_\alpha(\mathbb{F}_q)$ to denote the set of $\mathbb{F}_q$-rational points on A and C_α respectively.

Theorem 1. *If the polynomials $h_1, \ldots, h_n$ given by (2) are pairwise relatively prime then, for any non-trivial character χ of $A(\mathbb{F}_q)$, we have*

$$\sum_{P \in C_\alpha(\mathbb{F}_q)} \chi(P) \ll n2^n q^{1/2}.$$

Proof. If $h_1, \ldots, h_n$ are pairwise relatively prime, then the cover $C \to \mathbb{P}^1$ has geometric Galois group $(\mathbb{Z}/2)^n$, as the polynomials $h_1, \ldots, h_n$ are independent modulo squares. It follows that C_α is absolutely irreducible under these conditions. Furthermore, the zeros of each h_i and the point at infinity have 2^{n-1} pre-images in C_α all with ramification index 2. It follows from the Hurwitz formula that the genus of C_α is $2^{n-1}3(n-1)+1$.

We now show that C_α generates A as an algebraic group. Let J be the Jacobian of C_α. We need to show that the map $J \to A$ obtained by functoriality is surjective. It is enough to show that the map on the tangent spaces at the origin is surjective or, equivalently, that the dual map is injective. Over $\mathbb{F}_{q^n}$, owing to the description of C_α, this latter map is the natural map sending a n-dimensional vector space to the space generated by the differential forms dx/y_i, $i = 1, \dots, n$, inside the space of holomorphic differentials on C_α. Assume that

$$\sum_{i=1}^{n} c_i dx/y_i = 0. \tag{3}$$

By the Hurwitz formula, dx/y_i vanishes exactly at the ramification points of the map $C_\alpha \to E_i$, where $E_i : y^2 = h_i(t)$. As the map $t : E_i \to \mathbb{P}^1$ ramifies at the zeros of h_i and infinity, the map $C_\alpha \to E_i$ ramifies at the points above the zeros of h_j, $j \neq i$ but not at the points above the zeros of h_i. So, evaluating the sum on the left hand side of (3) at a point above a zero of h_i yields $c_i = 0$, showing the injectivity of our map, as desired.

Finally, it follows that χ is a non-trivial character on C_α with trivial conductor so the bound on the theorem follows from the Weil bound (see, for example, [10]). □

Remark 2. *The curve C_α is not always absolutely irreducible. Here is an example*

$$q = n = 3, \qquad E : y^2 = x^3 - x, \qquad \alpha^3 - \alpha = -1.$$

Then $h_1 = h_2$ and $C_\alpha(\mathbb{F}_3) = \{\mathcal{O}\}$, so some condition on α is needed.

Using an elliptic curve of the same equation but now $q = n = p > 3$, p prime, $\alpha^p - \alpha = c$, where c is a non-square in $\mathbb{F}_p$, we get an example where C_α is absolutely irreducible and, yet, we still have $C_\alpha(\mathbb{F}_p) = \{\mathcal{O}\}$. The reason this time is that $\mathrm{Norm}_{\mathbb{F}_{p^p}/\mathbb{F}_p}((t+\alpha)^3 - (t+\alpha)) = c^3, t \in \mathbb{F}_p$, so $E(\mathbb{F}_{p^p})$ has no point with x-coordinate $t + \alpha, t \in \mathbb{F}_p$.

3. Construction

We always assume that we are given an element $\vartheta \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n}$.

Theorem 3. *For any $\varepsilon > 0$, sufficiently large prime power q, and integer n with*

$$n \le \left(\frac{1}{2\log 2} - \varepsilon\right) \log q$$

and any set $\mathcal{R} \subset \mathbb{F}_q$ of size $\#\mathcal{R} = 9n + 1$ there is $r \in \mathcal{R}$ such that for $\alpha = r\vartheta$ there is $P \in C_\alpha(\mathbb{F}_q)$ of maximum order.

Proof. Let $\mathcal{X}_d$ be set of characters χ of $A(\mathbb{F}_q)$ of order d; that is, such that $\chi^d = \chi_0$, where χ_0 is the principal character. By the orthogonality property of characters,

$$\frac{1}{d}\sum_{\chi\in X_d}\chi(P)=\begin{cases}1, & \text{if } P=dQ \text{ for some } Q\in A(\mathbb{F}_q),\\ 0, & \text{otherwise.}\end{cases}$$

Therefore, if M is the exponent of $E(\mathbb{F}_{q^n})$, then using the standard inclusion exclusion principle, we derive

$$\sum_{d\mid M}\frac{\mu(d)}{d}\sum_{\chi\in\mathcal{X}_d}\chi(P)=\begin{cases}1, & \text{if } P \text{ is of maximum order,}\\ 0, & \text{otherwise,}\end{cases}$$

where $\mu(d)$ is the Möbius function.

For $\alpha\in\mathbb{F}_{q^n}$ we denote by N_α the number of points $P\in C_\alpha(\mathbb{F}_q)$ of maximum order. Then from the above, we see that

$$N_\alpha=\sum_{P\in C_\alpha(\mathbb{F}_q)}\sum_{d\mid M}\frac{\mu(d)}{d}\sum_{\chi\in\mathcal{X}_d}\chi(P)=\sum_{d\mid M}\frac{\mu(d)}{d}\sum_{\chi\in\mathcal{X}_d}\sum_{P\in C_\alpha(\mathbb{F}_q)}\chi(P).$$

The contribution from the principal character χ_0 is

$$\#C_\alpha(\mathbb{F}_q)\sum_{d\mid M}\frac{\mu(d)}{d}=\frac{\varphi(M)}{M}\#C_\alpha(\mathbb{F}_q),$$

where $\varphi(M)$ is the Euler function, see [8, Equation (16.3.1)]. Therefore

$$\left|N_\alpha-\frac{\varphi(M)}{M}\#C_\alpha(\mathbb{F}_q)\right|\le\sum_{d\mid M}\frac{1}{d}\sum_{\substack{\chi\in\mathcal{X}_d\\ \chi\ne\chi_0}}\left|\sum_{P\in C_\alpha(\mathbb{F}_q)}\chi(P)\right|. \tag{4}$$

To apply Theorem 1 to the character sums in (4) we need to find α such that the polynomials $h_1,\dots,h_n$ given by (2) are pairwise relatively prime. If $\beta_j, j=1,2,3$ are the roots of x^3+ax^2+bx+c, this leads us to the condition on α is that

$$\alpha^{(i)}-\alpha\ne\beta_j^{(i)}-\beta_k,\qquad 1\le i<n,\ j,k=1,2,3$$

(recall that $\alpha^{(n)}=\alpha^{q^n}=\alpha$).

Recall that $\mathbb{F}_q(\vartheta)=\mathbb{F}_{q^n}$, implies that $\vartheta^{(i)}-\vartheta\ne0$ for $1\le i<n$. Consider $\alpha=r\vartheta$ with $r\in\mathbb{F}_q^*$. Then $\alpha^{(i)}-\alpha=r(\vartheta^{(i)}-\vartheta)$. If $\#\mathcal{R}>9n$, by inspection of $9n+1$ values of $r\in\mathcal{R}$ we can find at least one with

$$r\ne(\beta_j^{(i)}-\beta_k)/(\vartheta^{(i)}-\vartheta),\qquad 1\le i<n,\ j,k=1,2,3.$$

With this r, for $\alpha = r\vartheta$ we apply Theorem 1 and derive from (4)

$$\left| N_\alpha - \frac{\varphi(M)}{M} \# C_\alpha(\mathbb{F}_q) \right| \ll n 2^n q^{1/2} \sum_{d|M} \frac{1}{d} \# \mathcal{X}_d \ll \tau(M) n 2^n q^{1/2}$$

where $\tau(M)$ is the number of integer positive divisors of M.

As we have seen in the proof of Theorem 1, C_α is an absolutely irreducible curve of genus $O(n2^n)$. So, from the Weil bound we derive

$$\# C_\alpha(\mathbb{F}_q) = q + O(n 2^n q^{1/2}).$$

Using this bound together the well-known estimates on the divisor and Euler functions

$$\tau(M) = M^{o(1)} \qquad \text{and} \qquad \varphi(M) = M^{1+o(1)}, \tag{5}$$

as $s \to \infty$, see [8, Theorems 317 and 328], we conclude that $N_\alpha > 0$ under the conditions of the theorem. □

In particular, we see that if $r = p^k$ for a prime $p \geq 3$ and the integer $k \to \infty$ then for an elliptic curve E over $\mathbb{F}_r$, in polynomial time, one can find a set of $r^{o(1)}$ points $P \in E(\mathbb{F}_r)$ such that at least one of them is of maximum order, provided that k contains a divisor n in an appropriate range.

We now show that in fact a similar set can be constructed over any finite field of small characteristic. First we need the following auxiliary statement.

Lemma 4. *The trace map* $\mathrm{Tr} : A(\mathbb{F}_{q^k}) \to A(\mathbb{F}_q)$ *sending a point to the sum of its* $\mathbb{F}_{q^k}/\mathbb{F}_q$*-conjugates, is surjective.*

Proof. Consider first the map $A(\mathbb{F}_{q^k}) \to A(\mathbb{F}_{q^k})$ given by $P \mapsto \mathrm{Fr}(P) - P$, where Fr is the $\mathbb{F}_q$ Frobenius and let G denote its image. Since the kernel of this map is visibly $A(\mathbb{F}_q)$, we have $\#G = \#A(\mathbb{F}_{q^k})/\#A(\mathbb{F}_q)$. We now show that G is the kernel of Tr and cardinality considerations then implies the result. It is clear that G is contained in the kernel of Tr. Let now $P \in A(\mathbb{F}_{q^k}), \mathrm{Tr}(P) = \mathcal{O}$. By Lang's theorem [11], there exists $Q \in A(\bar{\mathbb{F}}_q)$, where $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$, with $\mathrm{Fr}(Q) - Q = P$. Now

$$\mathcal{O} = \mathrm{Tr}(P) = \mathrm{Tr}(\mathrm{Fr}(Q) - Q) = \mathrm{Fr}^k(Q) - Q,$$

therefore $Q \in A(\mathbb{F}_{q^k})$ and $P \in G$. □

Theorem 5. *For any fixed* $\varepsilon > 0$ *and sufficiently large prime power* $r = p^n$ *where* p *is prime and* $n \geq 1$ *is an integer for an elliptic curve* E

over $\mathbb{F}_r$, *in time* $O\left(p2^{(2+\varepsilon)n}\right)$, *one can find a set of* $O\left(p2^{(2+\varepsilon)n}\right)$ *points* $Q \in E\left(\mathbb{F}_r\right)$ *such that at least one of them is of maximum order.*

Proof. Fix some small $\varepsilon > 0$ and choose m as the smallest positive integer satisfying the inequlaity

$$n \le \left(\frac{1}{2\log 2} - \varepsilon\right) m \log p. \tag{6}$$

We now put $q = p^m$, and construct an irreducible polynomial of degree n over $\mathbb{F}_q$ (which can be done deterministically in time $p^{1/2}(mn)^{O(1)} = p^{1/2}n^{O(1)}$, see [15]). Thus for any root ϑ of the polynomial we have $\mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n} = \mathbb{F}_{p^{mn}}$. We now examine the set of points (where Tr is the $\mathbb{F}_q/\mathbb{F}_p$-trace)

$$\mathcal{Q}_\alpha = \{\operatorname{Tr} P \ : \ P \in C_\alpha(\mathbb{F}_q)\}.$$

Clearly $\mathcal{Q}_\alpha \subseteq A(\mathbb{F}_p) \simeq E\left(\mathbb{F}_r\right)$ and $\#\mathcal{Q}_\alpha = O\left(p2^{(2+\varepsilon)n}\right)$. So it remains to show that $\mathcal{Q}_\alpha$ contains a point of maximum order. First we notice that the exponent M of $E\left(\mathbb{F}_r\right)$ is a divisor of the exponent of $E\left(\mathbb{F}_{q^n}\right) = E\left(\mathbb{F}_{r^m}\right)$.

Furthermore, in the notation of the proof of Theorem 3, for any non-trivial character χ of $A(\mathbb{F}_p)$ we have

$$\sum_{P \in C_\alpha(\mathbb{F}_q)} \chi(\operatorname{Tr} P) \ll n2^n q^{1/2}. \tag{7}$$

Indeed we only need to notice that $P \mapsto \chi(\operatorname{Tr} P)$ is a non-trivial character of $A(\mathbb{F}_q)$. and this follows from Lemma 4.

Let N_α be the number of points $Q \in \mathcal{Q}_\alpha$ of maximum order.

So as in the proof of Theorem 3 we write

$$N_\alpha = \sum_{P \in C_\alpha(\mathbb{F}_q)} \sum_{d \mid M} \frac{\mu(d)}{d} \sum_{\chi \in \mathcal{X}_d} \chi(\operatorname{Tr} P)$$

and derive

$$N_\alpha = \frac{\varphi(M)}{M} \# C_\alpha(\mathbb{F}_q) + O\left(\tau(M) n 2^n q^{1/2}\right).$$

Since Equation (6) is equivalent to the condition of Theorem 3 on n and q, we see that $N_\alpha > 0$ provided that r is large enough. □

4. Comments

We note that the result of Theorem 5, in wide range of p and n gives a much faster deterministic algorithm and a much smaller set containing a point of maximum order on $E(\mathbb{F}_r)$ than that of [10].

On the other hand, it has an exponential dependence on n, while its finite field analogues [16, 17, 18] depend on n polynomially. The reason is the exponential factor 2^n in the bound of Theorem 1, which in turn comes from the evaluation of the genus of C_α and seems to be unavoidable.

On the other hand, one can try to get an analogue of Theorem 1 for incomplete sums (in the style of [13]) and then reduce the dependence on p in Theorem 5 from linear to $p^{1/2}$ (as it is done in [18, Theorem 8] in the case of primitive roots of finite fields).

Finally, we notice that the actual identifying a point of maximum order in any set requires computing and factoring the cardinality $E(\mathbb{F}_r)$, we refer to [1] and [4] for a description of the state-of-art in both areas.

Acknowledgements

The first author was supported by ARC Grant DP1092835. The second author would like to thank Macquarie University and the University of Canterbury for their hospitality during the period in which this paper was written and the NSA for its support through Grant MDA904-H98230-09-1-0070.

References

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

[2] I. F. Blake, V. K. Murty and G. Xu, 'Refinements of Miller's algorithm for computing the Weil/Tate pairing', *J. Algorithms*, **58** (2006), 134–149.

[3] L. Carlitz, 'Distribution of primitive roots in a finite field', *Quart. J. Math. Oxford*, **4** (1953) 4–10.

[4] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, Springer-Verlag, Berlin, 2005.

[5] H. Davenport, 'On primitive roots in finite fields' *Quart. J. Math. (Oxford Ser.)* **8** (1937) 308–312.

[6] C Diem and N. Naumann, 'On the structure of the Weil restriction of Abelian varieties', *J. Ramanujan Math. Soc.*, **18** (2003) ,1–22.

[7] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Finding the group structure of elliptic curves over finite fields', *Bull. Aust. Math. Soc.*, **72** (2005), 251–263.

[8] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[9] N. M. Katz, ‘An estimate for character sums’, *J. Amer. Math. Soc.*, **2** (1989), 197–200.

[10] D. R. Kohel and I. E. Shparlinski, ‘Exponential sums and group generators for elliptic curves over finite fields’, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 395–404.

[11] S. Lang, ‘Algebraic groups over finite fields’, *Amer.J. Math.*, **78** (1956), 555–563.

[12] V. S. Miller, ‘The Weil pairing, and its efficient calculation’, *J. Cryptology*, **17** (2004), 235–261.

[13] G.I. Perel’muter and I. Shparlinski, ‘On the distribution of primitive roots in finite fields’, *Uspechi Matem. Nauk*, **45**, no.1 (1990), 185–186 (in Russian).

[14] R. Schoof, ‘Elliptic curves over finite fields and the computation of square roots mod p’, *Math. of Comp.*, bf 44 (1985), 483–494.

[15] V. Shoup, ‘New algorithms for finding irreducible polynomials over finite fields’, *Math. Comp.* **54** (1990), 435–447.

[16] V. Shoup, ‘Searching for primitive roots in finite fields’, *Math. Comp.* **58** (1992), 369–380.

[17] I. Shparlinski, ‘On primitive elements in finite fields and on elliptic curves’, *Matem. Sbornik*, **181** (1990), 1196–1206 (in Russian).

[18] I. Shparlinski, ‘Approximate constructions in finite fields’, *Proc. 3rd Conf. on Finite Fields and Appl., Glasgow, 1995*, London Math. Soc., Lect. Note Series, 1996, v.233, 313-332.

[19] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

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

E-mail address: igor.shparlinski@mq.edu.au

Department of Mathematics, University of Texas, Austin, TX 78712, USA

E-mail address: voloch@math.utexas.edu