

ELEMENTS OF HIGH ORDER ON FINITE FIELDS FROM ELLIPTIC CURVES

JOSÉ FELIPE VOLOCH

ABSTRACT. We discuss the problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field. We prove that the values on points of order small with respect to their degree of rational functions on an elliptic curve have high order. We discuss several special cases, including an old construction of Wiedemann, giving the first non-trivial estimate for the order of the elements in this construction.

1. INTRODUCTION

We discuss the problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field. We prove that the values on points of order small with respect to their degree of rational functions on an elliptic curve have high order.

We prove a theorem which gives information on the orders of the coordinates of points on a curve in $E \times \mathbf{G}_m$, where E is an elliptic curve defined over a finite field and \mathbf{G}_m is the multiplicative group. This is analogous to the main theorem of [4] which concerns curves in $\mathbf{G}_m \times \mathbf{G}_m$ and some of our arguments extend those of that paper. Our result can also be viewed as a weak form of a conjecture of Poonen which is discussed in [4].

Throughout this paper \mathbf{F}_q is a field of q elements where q is a power of the prime p . Our main result is as follows:

Theorem 1.1. *Let X be an absolutely irreducible curve in $E \times \mathbf{G}_m$, where E is an elliptic curve, with both X and E defined over \mathbf{F}_q . Assume that the projection of X to both factors is non-constant. Given $\epsilon > 0$, there exists $\delta > 0$ such that, for d sufficiently large given $(P, b) \in X$ with $d = [\mathbf{F}_q(P) : \mathbf{F}_q]$, such that the group generated by P is invariant under the \mathbf{F}_q -Frobenius and such that r , the order of P , satisfies $r < d^{3/2-\epsilon}$ then b has multiplicative order at least $\exp(\delta(\log d)^2)$.*

We also obtain a much better lower bound for the multiplicative order of b when X is contained in the graph of a function $E \rightarrow \mathbf{P}^1$. (see Section 4). Note that our result applies only certain finite fields,

namely those generated (as a field) by a point on E of small order. On the positive side, given that we have the flexibility of choosing E , this expands the scope of applicability beyond the results of [4]. A result of Gao ([3]), using a different construction, produces elements of order at least $\exp(\delta(\log d)^2/\log \log d)$ in \mathbf{F}_{q^d} for many (conjecturally all) values of d .

2. PRELIMINARIES

We will use the following lemma from [4].

Lemma 2.1. *For fixed integers $m, a \geq 2$ and real $\epsilon > 0$. If $r \geq 2$, $(r, ma) = 1$ is an integer and d is the order of $a \pmod r$, then, given $N < d$, there is a coset Γ of $\langle a \rangle \subset (\mathbf{Z}/r)^*$ with*

$$\#\{n \mid 1 \leq n \leq N, (n, m) = 1, n \pmod r \in \Gamma\} \gg Nd^{1-\epsilon}/r - r^\epsilon$$

The following construction is going to be very similar one in [4] but, unlike that paper, it will be useful to take a more geometric approach. We begin by replacing X by its closure in $E \times \mathbf{P}^1$ and all curves considered below will be projective.

We have the projection $X \rightarrow E$ and we denote by D its degree. Also, for any positive integer n , we have the map $[n] : E \rightarrow E$ given by multiplication by n . We consider the curve X_n obtained by taking the fiber product of these two maps (for any given n). Composing the map $X_n \rightarrow X$ with the second projection $X \rightarrow \mathbf{P}^1$, gives a map $X_n \rightarrow \mathbf{P}^1$ and this yields an element y_n of the function field of X_n .

If $(n, Dp) = 1$ then the map $X_n \rightarrow X$ is separable of degree n^2 and X_n is absolutely irreducible. For those values of n , the divisor of zeros of y_n is supported at the points of X_n above the points R on E with $nR = Q$, where Q runs through the points on E below the zeros of y_1 on X . We can view the functions y_n as elements of a fixed algebraic closure of the function field of X .

Lemma 2.2. *The algebraic functions $y_n, (n, Dp) = 1$, are multiplicatively independent.*

Proof. It is enough to show that, if L is a function field containing the $y_n, n \leq N, (n, Dp) = 1$, then the divisors of the y_n in L are \mathbf{Z} -linearly independent. We prove this by induction on N . Let k be the largest order (in the group law of E) among the points of E below the zeros of y_1 on X . Among the points of E below the zeros of y_N there is a point of order kN , which cannot be below a zero of $y_n, n < N$. \square

For a function field L/\mathbf{F}_q and an element z of L , denote by $\deg_L z$ the degree of the divisor of zeros of z in L , which is also $[L : \mathbf{F}_q(z)]$ if z is non-constant. We have that $\deg_{K_n} y_n \ll n^2$, where $K_n = \mathbf{F}_q(X_n)$.

3. PROOF OF THE MAIN THEOREM

Let F denote the \mathbf{F}_q -Frobenius map on all varieties over \mathbf{F}_q appearing in what follows. With notation as in the statement of the theorem, let $F(P) = aP, a \in \mathbf{Z}, (a, r) = 1, N = [d^{1/2-\epsilon}]$ and $\Gamma = \gamma\langle a \rangle$ be the coset given by lemma 2.1. Choose a point $C \in E$ of order r such that $P = \gamma C$. If $n \leq N, (n, q) = 1, n \bmod r \in \Gamma$ then $n \equiv \gamma a^j \pmod{r}$ for some j and let J be the set of all such j . Thus, for $j \in J$,

$$F^j(P, b) = (F^j(P), b^{q^j}) = (a^j P, b^{q^j})$$

and $a^j P = n_j C$, where $n_j \leq N, (n_j, q) = 1, n_j \bmod r \in \Gamma$ gives rise to j . It follows that there is a point of X_{n_j} above $C \in E$ where y_{n_j} takes the value b^{q^j} . Let $T = [\eta \log d]$, where $\eta > 0$ will be chosen later. If $I \subset J$, let $b_I = \prod_{j \in I} b^{q^j}$.

We now claim that the b_I are distinct for distinct $I \subset J, |I| \leq T$. If $b_I = b_{I'}$ for two distinct such subsets I, I' , then the algebraic function $z = (\prod_{j \in I} y_{n_j} / \prod_{j \in I'} y_{n_j}) - 1$ vanishes at a place of the field L , compositum of the $K_{n_j}, j \in I \cup I'$ above $C \in E$.

$$\deg_L z \leq \sum_{j \in I \cup I'} \deg_L y_{n_j} = \sum_{j \in I \cup I'} [L : K_{n_j}] \deg_{K_{n_j}} y_{n_j} \ll TD^{2T} N^2$$

which is smaller than $d = [\mathbf{F}_q(C) : \mathbf{F}_q]$ for a suitably small choice of η and all d sufficiently large and that is not possible, unless $z = 0$ and therefore the $y_{n_j}, j \in I \cup I'$ are multiplicatively dependent. This contradicts lemma 2.2. It follows that there are at least $\binom{|J|}{T}$ distinct powers of b . Now lemma 2.1 (with $\epsilon/3$ instead of ϵ) gives that

$$|J| \gg d^{3/2-\epsilon/3}/r - r^{\epsilon/3} \gg d^{2\epsilon/3} - (d^{3/2-\epsilon})^{\epsilon/3} \gg d^{2\epsilon/3},$$

hence $\binom{|J|}{T} \geq (|J|/T - 1)^T \gg \exp(\delta(\log d)^2)$, for some suitably small $\delta > 0$, proving the theorem.

4. RATIONAL MAPS

In this section we discuss the special case where our curve X is an open subset of the graph of $y : E \rightarrow \mathbf{P}^1$. In this case, we can obtain much better bounds. Indeed, following the proof of the theorem, we have that $y_n = y \circ [n]$ so $K_n = \mathbf{F}_q(E)$ and we get the much smaller estimate $\deg_L z \ll TDN^2$. We can, therefore choose a much larger

value of T , say $T = [d^\eta]$ for some small $\eta > 0$ and the proof of the theorem yields that b has multiplicative order at least $\exp(d^\delta)$ with the same notation and assumptions. More precisely, we have:

Theorem 4.1. *Let E be an elliptic curve and y a non-constant function on E , with both y and E defined over \mathbf{F}_q . Given $\epsilon > 0$, there exists $\delta > 0$ such that, for d sufficiently large, given $P \in E$ with $d = [\mathbf{F}_q(P) : \mathbf{F}_q]$, such that the group generated by P is invariant under the \mathbf{F}_q -Frobenius and such that r , the multiplicative order of P , satisfies $r < d^{3/2-\epsilon}$ then $y(P)$ has multiplicative order at least $\exp(d^\delta)$.*

We now explore a couple of special cases of Theorem 2. We begin with E a supersingular elliptic curve such that F acts by multiplication by a on E , where $a = \pm\sqrt{q}$, for q a square. Under these assumptions, the condition that the group generated by P is invariant under F is automatic and the only condition to be checked is $r < d^{3/2-\epsilon}$. Note that $E(\mathbf{F}_{q^d}) \cong (\mathbf{Z}/(\sqrt{q}^d \pm 1))^2$.

Now, consider the case of E an ordinary elliptic curve and $r = p^k$ and since $E[p^k]$ is cyclic, again the condition that the group generated by P is invariant under F is automatic and the only condition to be checked is $r < d^{3/2-\epsilon}$. Note that $d = sp^{k-k_0}$ for some fixed k_0, s and all k large. So the inequality $r < d^{3/2-\epsilon}$ is satisfied for large k and the conclusion of the theorem holds.

In [5], Wiedemann introduced the following elements of $\bar{\mathbf{F}}_2$, defined inductively as $a_0 = 1$, a_n a root of $x^2 + a_{n-1}x + 1, n > 0$. He showed that $\mathbf{F}_{2^{2^n}} = \mathbf{F}_2(a_n)$ and conjectured that a_n has order $2^{2^{n-1}} + 1$ for all n . Note that, as a_n has $\mathbf{F}_{2^{2^n}}/\mathbf{F}_{2^{2^{n-1}}}$ -norm 1, its order cannot be larger. Let E/\mathbf{F}_2 be the elliptic curve $y^2 + xy = x^3 + 1$. We will show how to obtain Wiedemann's elements from the construction of the preceding paragraph. We show that a_n is the x -coordinate of a point of order 2^n of E . It then follows that a_n has order at least $\exp(2^{\delta n})$, for some $\delta > 0$. Note that multiplication by 2 on E factors as FV , where V is the Verschiebung and a simple calculation shows that the x -coordinate of $V(x, y)$ is $(x^2 + 1)/x$. If P_n are defined inductively by $P_0 = (1, 0), V(P_{n+1}) = P_n$, then the x -coordinate of P_n is easily seen to satisfy the same equation as a_n , so we can take $a_n = x(P_n)$.

Wiedemann's construction is an example of an iterative construction of finite fields. Other examples can be found in [2] and references therein and also in [1], where the multiplicative order of elements thus obtained is estimated. Considering points of order s^n on an elliptic curve for fixed s and varying n , provides other examples of iterative constructions to which we can apply the theorems of this paper. We

thus obtain many examples of iterative construction of finite fields together with estimates for their multiplicative order which are much better than those previously obtained.

5. GENERALIZATIONS

It is possible to remove the condition that $\langle P \rangle$ is F -invariant from the statement of our theorems at the expense of a much weaker bound. It requires an analogue of Lemma 2.1 with $\mathbf{Z}[F]$ instead of \mathbf{Z} . It is also possible to state a similar theorem with the roles of E and \mathbf{G}_m reversed or with \mathbf{G}_m replaced by another elliptic curve and a proof along the lines of this paper will provide estimates. The scope of the technique seems to be to prove results about points on a curve inside $A \times B$ where A, B are semi-abelian varieties. The use of degrees prevents extending the argument from a curve to an arbitrary subvariety of $A \times B$. However, Poonen's conjecture (stated in [4]) would imply that the main hypothesis of such a theorem (namely that the order of one of the coordinates is small) could not be satisfied unless $\dim A = \dim B = 1$. Therefore we do not pursue such a generalization so as to avoid proving a potentially vacuous theorem.

REFERENCES

- [1] J. F. Burkhart et al., Finite field elements of high order arising from modular curves. *Des. Codes Cryptogr.* 51 (2009), no. 3, 301–314.
- [2] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields. *Des. Codes Cryptogr.* 2 (1992), no. 2, 169–174.
- [3] S. Gao, Elements of provable high orders in finite fields, *Proc. American Math. Soc.* 127 (1999), 1615–1623.
- [4] J. F. Voloch, On the order of points on curves over finite fields, *Integers*, 7 (2007) A49.
- [5] D. Wiedemann, An iterated quadratic extension of $\text{GF}(2)$, *Fibonacci Q.*, 26 (1988), 290–295.

(1) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TX 78712, USA

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