JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Mei-Chu CHANG, Bryce KERR, Igor E. SHPARLINSKI et Umberto ZANNIER

Elements of large order on varieties over prime finite fields

Tome 26, n° 3 (2014), p. 579-593.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_3_579_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 579–593

Elements of large order on varieties over prime finite fields

par Mei-Chu CHANG, Bryce KERR, Igor E. SHPARLINSKI
et Umberto ZANNIER

Résumé. Soit $\mathcal{V}$ une variété algébrique fixée définie par m polynomes en n variables à coefficients entiers. Nous montrons qu'il existe une constante $C(\mathcal{V})$ telle que pour presque tout nombre premier p, tous les points de la réduction de $\mathcal{V}$ modulo p, sauf peut-être $C(\mathcal{V})$ d'entre eux, possède une composante d'ordre multiplicatif grand. Ceci généralise plusieurs résultats précédents et constitue un pas en direction d'une conjecture de B. Poonen.

Abstract. Let $\mathcal{V}$ be a fixed algebraic variety defined by m polynomials in n variables with integer coefficients. We show that there exists a constant $C(\mathcal{V})$ such that for almost all primes p for all but at most $C(\mathcal{V})$ points on the reduction of $\mathcal{V}$ modulo p at least one of the components has a large multiplicative order. This generalises several previous results and is a step towards a conjecture of B. Poonen.

1. Introduction

One of the major problems of the theory of finite fields is, given a finite field $\mathbb{F}_q$ with q elements, find in polynomial time a generator of its multiplicative group $\mathbb{F}_q^*$. Even in the class of probabilistic algorithms, it seems that factoring $q-1$ is unavoidable and thus no polynomial-time algorithm is known nowadays.

One of the possible ways to circumvent the factorisation obstacle is to find some constructions of reasonably small subsets of finite fields, that are guaranteed to contain a generator, see [21, 22, 23] for some results of this type.

Another possible relaxation of the original problem is to construct elements x in a given field $\mathbb{F}_q$ or in its extension of large *order* $\operatorname{ord} x$, see [1, 6, 7, 8, 9, 15, 19, 20, 25, 26] and references therein. We recall that for a non-zero element $x \in \overline{\mathbb{F}}_q$ in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ the order $\operatorname{ord} x$ is the smallest positive integer t with $x^t = 1$.

Manuscrit reçu le 30 mai 2013, révisé le 21 novembre 2013, accepté le 15 mars 2014.

Voloch [25, 26] has considered the points (x, y) on an algebraic curve $f(x, y) = 0$, defined over the ground field $\mathbb{F}_q$ and such that x is of high degree $d = [\mathbb{F}_q(x) : \mathbb{F}_q]$ over $\mathbb{F}_q$. In particular, under some natural conditions, it is shown in [25] that if $f(X, Y) \in \mathbb{F}_q[X, Y]$ is absolutely irreducible, then for any $\varepsilon > 0$ there is some $\delta > 0$ such that either $\operatorname{ord} x > d^{2-\varepsilon}$ or $\operatorname{ord} y > \exp(\delta(\log d)^2)$.

More recently, it has been shown in [8] that if the zero set of a polynomial $f(X, Y) \in \mathbb{Z}[X, Y]$ has no common components with those of $X^r - Y^s$ and $X^r Y^s - 1$ for any $r, s \in \mathbb{Z}$, $r, s \geq 0$, then for any function $\varepsilon(z)$ with $\lim_{z\to\infty} \varepsilon(z) = 0$, there is a set of primes p of relative density 1 such that for all but at most $C(f)$ solutions of the equation

$$f(x, y) = 0, \qquad (x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p,$$

we have

$$\max\{\operatorname{ord} x, \operatorname{ord} y\} \geq p^{1/4+\varepsilon(p)},$$

see also [7].

We note that the results of Voloch [25, 26] (and thus those of [8]) are motivated by the following general conjecture due to Poonen (but are quantitatively much weaker):

Conjecture 1.1. *Let $\mathcal{A}$ be a semiabelian variety defined over $\mathbb{F}_q$ and let $\mathcal{X}$ be a closed subvariety of $\mathcal{A}$. Denote $\mathcal{Z}$ the union of all translates of positive-dimensional semiabelian varieties over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ contained in $\mathcal{X}$. Then, for every nonzero x in $(\mathcal{X} - \mathcal{Z})(\overline{\mathbb{F}}_q)$, the order of x in $\mathcal{A}(\overline{\mathbb{F}}_q)$ is at least q^{dc} for some constant $c > 0$, where d is the degree of x over $\mathbb{F}_q$.*

Here we extend the result of [8] to points on general algebraic varieties. Although our results and Conjecture 1.1 do not imply each other, our estimates may be considered as yet an indirect confirmation of this conjecture. We expand the method of [7, 8] by some new ideas including the use of Hilbert's *Nullstellensatz*.

We say that an absolutely irreducible variety $\mathcal{V} \subseteq \mathbb{C}^n$ does not contain a monomial curve, if it does not contain a curve parametrised by

$$X_1 = \rho_1 T^{k_1}, \ldots, X_n = \rho_n T^{k_n},$$

where $\rho_1, \ldots, \rho_n$ are roots of unity and $k_1, \ldots, k_n$ are integers, not all equal to zero.

Theorem 1.1. *Assume that an algebraic variety $\mathcal{V} \subseteq \mathbb{C}^n$ is defined over $\mathbb{Q}$. Also assume that $\mathcal{V}$ does not contain a monomial curve. Then there is a constant $C(\mathcal{V})$, depending only on $\mathcal{V}$ such that for any function $\varepsilon(z)$ with*

$$\lim_{z\to\infty} \varepsilon(z) = 0,$$

there is a set of primes p of relative density 1 such that for all but at most $C(\mathcal{V})$ points $(x_1, \ldots, x_n) \in \mathcal{V}_p$ with components from $\overline{\mathbb{F}}_p$, on the reduction $\mathcal{V}_p \subseteq \overline{\mathbb{F}}_p^n$ of $\mathcal{V}$ modulo p, we have

$$\max\{\operatorname{ord} x_1, \ldots, \operatorname{ord} x_n\} \ge \varepsilon(p) p^{1/2n}.$$

For the case of a single plane curve of degree d, we can get a weaker bound, although the set of primes removed depends only on d.

Theorem 1.2. *Fix an integer $d \ge 2$ and a function $\varepsilon(z)$ with*

$$\lim_{z \to \infty} \varepsilon(z) = 0.$$

Then for a set of primes p, depending only on d and $\varepsilon(z)$, of relative density 1, for any polynomial $f(X, Y) \in \mathbb{F}_p[X, Y]$ of degree d that is not divisible by any polynomial of the form

$$\rho X^\alpha Y^\beta - 1 \quad \text{or} \quad \rho Y^\beta - X^\alpha$$

for any $\rho \in \overline{\mathbb{F}}_p$ and integers $\alpha, \beta \ge 0$, all solutions $(x, y) \in (\overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p)^*$ of $f(x, y) = 0$ satisfy

$$\operatorname{ord} x + \operatorname{ord} y \ge \varepsilon(p) p^{2/(89d^2+3d+12)}$$

except for at most $11d^2 + 1$ of them.

As in [8], we note that the main result of [24], combined with [14, Theorem 7] implies that for any fixed $\varepsilon > 0$ and a positive proportion of primes, the curve

$$XY - X^2 - 1 = 0$$

contains at least $p^{1/2}$ points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ such that x and y are both of multiplicative order at most $p^{3/4+\varepsilon}$. This result can easily be extended to other curves, see [24] for details. However, it seems very likely that neither this upper bound nor our lower bounds are tight.

2. Preparations

We recall that the logarithmic height of a nonzero polynomial $F \in \mathbb{Z}[Z_1, \ldots, Z_n]$ is defined as the logarithm of the maximum of the absolute values of the coefficients of F.

We need the following quantitative version of the Bézout theorem, that follows from a result of D'Andrea, Krick and Sombra [11], which in turn improves a series of previous estimates such as those of Krick, Pardo and Sombra [16]. Namely, by [11, Theorem 2] we have the following result (which improves [5, Lemma 23]):

Lemma 2.1. *Let $F_1, \ldots, F_N, \in \mathbb{Z}[X_1, \ldots, X_n]$ be $N + 1 \ge 2$ polynomials in n variables of degree at most $D \ge 3$ and of logarithmic height at most H*

and let $G \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial in n variables of degree at most $d \geq 3$ and of logarithmic height at most h vanishes on the variety

$$F_1(X_1, \ldots, X_n) = \ldots = F_N(X_1, \ldots, X_n) = 0.$$

There are positive integers b and r with

$$\log b \leq C(n, N) \left(D^{n+1} h + dD^n H + dD^{n+1} \right)$$

and polynomials $Q_1, \ldots, Q_N \in \mathbb{Z}[X_1, \ldots, X_n]$ such that

$$F_1 Q_1 + \ldots + F_N Q_N = bG^r,$$

where $C(n, N)$ depends only on n and N.

As usual, we use $\mathbb{G}_{\mathrm{m}}^n$ to denote the complex algebraic torus, that is, the n-fold Cartesian product of the multiplicative group $\mathbb{G}_{\mathrm{m}} = \mathbb{C}^*$ of the complex numbers, see [4, 27, 28]. Let $\mathcal{U}$ be the group of all roots of unity. The elements of $\mathcal{U}^n$ are the torsion points of $\mathbb{G}_{\mathrm{m}}^n$ with respect to the natural group structure.

We call the elements of $\mathcal{U}^n$ the *torsion points* of $\mathbb{G}_{\mathrm{m}}^n$.

For a complex variety $\mathcal{V}$ in $\mathbb{G}_{\mathrm{m}}^n$ we denote by $N(\mathcal{V})$ the number of torsion points on $\mathcal{V}$. We need the following result about the finiteness of $N(\mathcal{V})$, which is due to Laurent [17].

Lemma 2.2. *If an algebraic variety $\mathcal{V}$ in $\mathbb{G}_{\mathrm{m}}^n$ does not contain a monomial curve, then $N(\mathcal{V})$ is finite.*

We refer to the work of Aliev and Smyth [2, Theorem 1.2] for an explicit version of Lemma 2.2.

We also note the work of [18] is related to some algorithmic aspects of finding torsion points. We also use the following result of Beukers and Smyth [3, Section 4.1].

Lemma 2.3. *Let $f \in \mathbb{C}[X, Y]$ be of degree d and let $\mathcal{V}$ be the variety defined by the equation*

$$f(X, Y) = 0.$$

Then either

$$N(\mathcal{V}) \leq 11d^2$$

or $\mathcal{V}$ contains infinitely many points which are roots of unity. In this case f has a factor of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ for some nonnegative integers i, j not both zero and some root of unity ρ.

3. Proof of Theorem 1.1

We notice that without loss of generality we can assume that the function $\varepsilon(z)z^{1/2n}$ is monotonically increasing and tends to infinity as $z \to \infty$.

Let us fix a sufficiently large real number z and set

$$T = \varepsilon(z)z^{1/2n}.$$

We see from Lemma 2.2 that there is some constant $T_0(\mathcal{V})$ depending only on $\mathcal{V}$ such that the components of any points in $\mathcal{V} \cap \mathbb{U}^n$ are roots of unity of order at most $T_0(\mathcal{V})$.

Assume that z is large enough so that $T > T_0(\mathcal{V})$.

We now fix some positive integers $t_1, \dots, t_n$ with

$$T \geq \max\{t_1, \dots, t_n\} > T_0(\mathcal{V}). \tag{3.1}$$

Assume that $\mathcal{V}$ is the zero set of the polynomials

$$f_i(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n], \qquad i = 1, \dots, m.$$

Let

$$\Phi_t(X) = \prod_{\substack{s=1 \\ \gcd(s,t)=1}}^{t} (X - \exp(2\pi i s/t)) \tag{3.2}$$

be the t-th cyclotomic polynomial. Suppose the numbers $\gamma_1, \dots, \gamma_n$ satisfy $\Phi_{t_i}(\gamma_i) = 0$, $i = 1, \dots, n$. Consider the products

$$b(t_1, \dots, t_n; \gamma_1, \dots, \gamma_n) = \prod_{j=1}^{m} \max\{1, |\operatorname{Nm} f_j(\gamma_1, \dots, \gamma_n)|\}, \tag{3.3}$$

where $\operatorname{Nm} \vartheta$ denotes the norm to $\mathbb{Q}$ of an algebraic integer ϑ.

Note that

$$b(t_1, \dots, t_n; \gamma_1, \dots, \gamma_n) \mid B(t_1, \dots, t_n), \tag{3.4}$$

where

$$B(t_1, \dots, t_n) = \prod_{j=1}^{m} \max\left\{1, \prod_{\vartheta_1:\ \Phi_{t_1}(\vartheta_1)=0} \cdots \prod_{\vartheta_n:\ \Phi_{t_n}(\vartheta_n)=0} |f_j(\vartheta_1, \dots, \vartheta_n)|\right\}.$$

It is easy to see that

$$\log B(t_1, \dots, t_n) = O(T^n) \tag{3.5}$$

where, here and after, the implied constants depend only on $\mathcal{V}$. Thus, the bound (3.5) implies that there are

$$O\left(\frac{\log B(t_1, \dots, t_n)}{\log(\log B(t_1, \dots, t_n) + 2)}\right) = O(T^n / \log T)$$

primes $p \mid B(t_1, \dots, t_n)$. Therefore, there are at most $O(T^{2n}/\log T) = o(z/\log z)$ primes $p \le z$ which satisfy this divisibility condition for at least one choice of $t_1, \dots, t_n$ with (3.1).

For each remaining prime p the variety $\mathcal{V}_p$ does not contain a point $(x_1, \dots, x_n) \in \mathcal{V}_p$ with

$$\operatorname{ord} x_1 = t_1, \dots, \operatorname{ord} x_n = t_n \tag{3.6}$$

for any choice of positive integers $t_1, \dots, t_n$ satisfying (3.1). Thus for these primes, for every point $(x_1, \dots, x_n) \in \mathcal{V}_p$ with

$$\max\{\operatorname{ord} x_1, \dots, \operatorname{ord} x_n\} > T_0(\mathcal{V})$$

we have

$$\max\{\operatorname{ord} x_1, \dots, \operatorname{ord} x_n\} \ge T = \varepsilon(z) z^{1/2n}. \tag{3.7}$$

Indeed, let $(x_1, \dots, x_n) \in \mathcal{V}_p$ satisfy (3.6). Choose α such that

$$\mathbb{F}_p(x_1, \dots x_n) = \mathbb{F}_p(\alpha)$$

where α is a root of $f \in \mathbb{Z}[X]$ irreducible over $\mathbb{F}_p$ of degree r. For each x_i we have

$$x_i = \sum_{j=0}^{r-1} \beta_{i,j} \alpha^j, \quad \beta_{i,j} \in \{0, 1, \dots, p-1\}.$$

Let ρ be a root of f over $\mathbb{C}$ and consider $z_i \in \mathbb{Q}(\rho)$ defined by

$$z_i = \sum_{j=0}^{r-1} \beta_{i,j} \rho^j.$$

Then for some choice of ρ there exists a prime ideal $\mathfrak{p}$ dividing p such that

$$x_j \equiv z_j \pmod{\mathfrak{p}}, \tag{3.8}$$

and

$$f_i(z_1, \dots, z_n) \equiv \Phi_{t_j}(z_j) \equiv 0 \pmod{\mathfrak{p}}, \tag{3.9}$$

where $i = 1, \dots, m$ and $j = 1, \dots, n$.

Let as before γ_j be a root of Φ_{t_j} over $\mathbb{C}$, $j = 1, \dots, n$, so that from (3.1) we have $\operatorname{Nm} f_i(\gamma_1, \dots, \gamma_n) \ne 0$ for at least one $i = 1, \dots, m$. On the other hand, from (3.9),

$$\operatorname{Nm} f_i(\gamma_1, \dots, \gamma_n) \equiv \operatorname{Nm} f_i(z_1, \dots, z_n) \equiv 0 \pmod{p},$$

for every $i = 1, \dots, m$. Hence from (3.3) we obtain

$$b(t_1, \dots, t_n; \gamma_1, \dots, \gamma_n) \equiv 0 \pmod{p}.$$

Thus we see from (3.4) that $p \mid B(t_1, \dots, t_n)$ which contradicts the choice of p.

This implies that for all but $o(z/\log z)$ primes $p \le z$ we have (3.7).

Clearly there are at most

$$\left(\sum_{1\le t\le T_0(\mathcal{V})} t\right)^n \le T_0(\mathcal{V})^{2n}$$

points $(x_1,\dots,x_n)\in\mathcal{V}_p$ with

$$\max\{\operatorname{ord} x_1,\dots,\operatorname{ord} x_n\}\le T_0(\mathcal{V}).$$

Since we have assumed that the function $\varepsilon(z)z^{1/2n}$ is monotonically increasing, we see that (3.7) concludes the proof with $C(\mathcal{V})=T_0(\mathcal{V})^{2n}$.

4. Proof of Theorem 1.2

As before we notice again that without loss of generality we can assume that the function $\varepsilon(z)z^{2/(89d^2+3d+12)}$ is monotonically increasing and tends to infinity as $z\to\infty$.

First we need to introduce some notation and constructions which will be used throughout the proof. For $\varepsilon(z)=o(1)$, let

$$T=\varepsilon(z)z^{2/(89d^2+3d+12)}. \tag{4.1}$$

Given polynomials $f_1,\dots,f_s\in\mathbb{K}[Z_1,\dots,Z_N]$ over a field $\mathbb{K}$, we write $V(f_1,\dots,f_s)$ for the variety defined by the system of equations

$$f_1(Z_1,\dots,Z_N)=\dots=f_s(Z_1,\dots,Z_N)=0.$$

Let $\mathbf{A}=\{A_{i,j}\}_{0\le i+j\le d}$ and consider the polynomial

$$f(\mathbf{A},X,Y)=\sum_{0\le i+j\le d} A_{i,j}X^iY^j\in\mathbb{Z}[\mathbf{A},X,Y].$$

Note that we consider the vector of coefficients $\mathbf{A}$ as a vector of $(d+1)(d+2)/2$ variables. Let

$$\Phi^0_{\alpha,\beta}(X,Y,\rho)=\rho X^\alpha Y^\beta-1\in\mathbb{Z}[X,Y,\rho]$$

and

$$\Phi^1_{\alpha,\beta}(X,Y,\rho)=\rho Y^\beta-X^\alpha\in\mathbb{Z}[X,Y,\rho].$$

Writing

$$f(\mathbf{A},X,Y)=\sum_{i=0}^{d} f_i(\mathbf{A},X)Y^i,\qquad f_i(\mathbf{A},X)\in\mathbb{Z}[\mathbf{A},X],$$

and

$$\Phi^\nu_{\alpha,\beta}=\sum_{i=0}^{\beta}\Phi^\nu_{i,\alpha,\beta}(X,\rho)Y^i,\qquad \Phi^\nu_{i,\alpha,\beta}(X,\rho)\in\mathbb{Z}[X,\rho],$$

we consider the resultant $\mathrm{Res}_Y(f(\mathbf{A}, X, Y), \Phi^\nu_{\alpha,\beta}(X, Y, \rho))$ of the polynomials f and $\Phi^\nu_{\alpha,\beta}$ with respect to the variable Y. Expanding the Sylvester determinant, we see that

$$\mathrm{Res}_Y(f(\mathbf{A}, X, Y), \Phi^\nu_{\alpha,\beta}(X, Y, \rho)) = \sum_{r=0}^{R} \widetilde{g}^\nu_{r,\alpha,\beta} X^r, \qquad \widetilde{g}^\nu_{r,\alpha,\beta} \in \mathbb{Z}[\mathbf{A}, \rho],$$

for some integer R. Let $\widetilde{V}^\nu_{\alpha,\beta}$ be the variety defined by the equations

$$\widetilde{V}^\nu_{\alpha,\beta} = V(\widetilde{g}^\nu_{r,\alpha,\beta},\ r = 1, \dots, R). \tag{4.2}$$

For p prime we let $\widetilde{V}^\nu_{\alpha,\beta,p}$ denote the variety over $\overline{\mathbb{F}}_p$ defined by the equations

$$\widetilde{g}^\nu_{r,\alpha,\beta} = 0, \qquad r = 1, \dots, R.$$

Let the polynomials $(g^\nu_{s,\alpha,\beta},\ s = 1, \dots, S)$ generate the elimination ideal of $(\widetilde{g}^\nu_{r,\alpha,\beta},\ r = 1, \dots, R)$ with respect to the variable ρ, that is, we have the following relation between the corresponding ideals

$$(g^\nu_{s,\alpha,\beta},\ s = 1, \dots, S) = (\widetilde{g}^\nu_{r,\alpha,\beta},\ r = 1, \dots, R) \cap \mathbb{C}[\mathbf{A}] \tag{4.3}$$

and let

$$V^\nu_{\alpha,\beta} = V(g^\nu_{s,\alpha,\beta},\ s = 1, \dots, S).$$

Consider the projection

$$\pi : \mathbb{C}^{(d+1)(d+2)/2+1} \to \mathbb{C}^{(d+1)(d+2)/2}$$

$$(\mathbf{A}, \rho) \mapsto \mathbf{A}$$

so that from [10, Chapter 3.2, Lemma 1]

$$\pi(\widetilde{V}^\nu_{\alpha,\beta}) \subseteq V^\nu_{\alpha,\beta}. \tag{4.4}$$

Let $V^\nu_{\alpha,\beta,p}$ denote the variety over $\overline{\mathbb{F}}_p$ defined by the equations

$$g^\nu_{s,\alpha,\beta} = 0, \qquad s = 1, \dots, S.$$

Let $K = 11d^2 + 1$ and for K-tuples

$$\mathbf{m} = (m_1, \dots, m_K) \qquad \text{and} \qquad \mathbf{n} = (n_1, \dots, n_K)$$

with integer coordinates let $W_{\mathbf{m},\mathbf{n}}$ be the variety defined by the equations

$$\sum_{0 \le i+j \le d} A_{i,j} X_k^i Y_k^j = \Phi_{m_k}(Y_k) = \Phi_{n_k}(X_k) = 0, \qquad k = 1, \dots, K,$$

in variables $(\{A_{i,j}\}_{0 \le i+j \le d}, (X_k, Y_k)_{1 \le k \le K})$ and Φ_t is defined as in (3.2). Then we have

$$W_{\mathbf{m},\mathbf{n}} \subseteq U \bigcup \left(\bigcup_{0 \le \alpha,\beta \le d} \left(V^0_{\alpha,\beta} \cup V^1_{\alpha,\beta} \right) \right),$$

where

$$U = \bigcup_{1 \le k_1 < k_2 \le K} V\left(X_{k_1} - X_{k_2}, Y_{k_1} - Y_{k_2}\right).$$

This may be seen by taking

$$P = (\{a_{i,j}\}_{0 \le i+j \le d}, (x_k, y_k)_{1 \le k \le K}) \in W_{\mathbf{m},\mathbf{n}}$$

and considering the curve

$$f(X,Y) = \sum_{0 \le i+j \le d} a_{i,j} X^i Y^j.$$

If f vanishes on a monomial curve, then for some integers $0 \le \overline{\alpha}, \overline{\beta} \le d$ not both zero and some root of unity $\overline{\rho}$, f has a factor of the form

$$\Phi^0_{\overline{\alpha},\overline{\beta}}(X,Y,\overline{\rho}) \quad \text{or} \quad \Phi^1_{\overline{\alpha},\overline{\beta}}(X,Y,\overline{\rho})$$

so that

$$\mathrm{Res}_Y(f(X,Y), \Phi^0_{\overline{\alpha},\overline{\beta}}(X,Y,\overline{\rho})) = 0$$

or

$$\mathrm{Res}_Y(f(X,Y), \Phi^1_{\overline{\alpha},\overline{\beta}}(X,Y,\overline{\rho})) = 0.$$

Using (4.4) this gives

$$P \in \bigcup_{0 \le \alpha,\beta \le d} \left(V^0_{\alpha,\beta} \cup V^1_{\alpha,\beta}\right).$$

If f does not vanish on a monomial curve, then by Lemma 2.3 f has at most $11d^2 = K - 1$ solutions in roots of unity. Since the numbers $(x_k, y_k)_{1 \le k \le K}$ satisfy

$$\sum_{0 \le i+j \le d} a_{i,j} x_k^i y_k^j = \Phi_{m_k}(x_k) = \Phi_{n_k}(y_k) = 0, \qquad k = 1, \dots K,$$

we see that for some $j_1 \ne j_2$ we have $(x_{j_1}, y_{j_1}) = (x_{j_2}, y_{j_2})$ so that

$$P \in U.$$

We may choose an integer H bounded in terms of d and polynomials $(G_h,$ $h = 1, \dots, H)$ with degree and height bounded in terms of d such that

$$\bigcup_{0 \le \alpha,\beta \le d} \left(V^0_{\alpha,\beta} \cup V^1_{\alpha,\beta}\right) = V(G_h,\ h = 1, \dots, H). \tag{4.5}$$

Consider the set

$$\mathcal{K} = \{(k_1, k_2)\ :\ 1 \le k_1 < k_2 \le K\}$$

and for each of the $2^{K(K+1)/2}$ partitions $\mathcal{P} = (\mathcal{I}, \mathcal{J})$

$$\mathcal{I} \cup \mathcal{J} = \mathcal{K} \qquad \text{and} \qquad \mathcal{I} \cap \mathcal{J} = \emptyset$$

of $\mathcal{K}$ into subsets $\mathcal{I}, \mathcal{J} \subseteq \mathcal{K}$ and $h = 1, \dots, H$ we define the polynomial

$$G_{h,\mathcal{P}} = G_h \prod_{(k_1,k_2)\in\mathcal{I}} (X_{k_1} - X_{k_2}) \prod_{(k_1,k_2)\in\mathcal{J}} (Y_{k_1} - Y_{k_2}) \in \mathbb{Z}[\mathbf{A}, (X_k, Y_k)_{1\le k\le K}]$$

so that for each $\mathbf{m}, \mathbf{n}$, h and $\mathcal{P}$ the polynomial $G_{h,\mathcal{P}}$ vanishes on $W_{\mathbf{m},\mathbf{n}}$.

We now assume that

$$\max\{m_1, n_1, \dots, m_K, n_K\} \le T.$$

Since $G_{h,\mathcal{P}}$ has degree and height bounded in terms of d and the polynomials defining the variety $W_{\mathbf{m},\mathbf{n}}$ have the degree and height bounded by $O(T)$, by Lemma 2.1 there exist $A_{h,\mathcal{P},\mathbf{m},\mathbf{n}}, \gamma_{h,\mathcal{P},\mathbf{m},\mathbf{n}} \in \mathbb{Z}$ and polynomials $F_k, Q_k, R_k \in \mathbb{Z}[\mathbf{A}, (X_k, Y_k)_{1\le k\le K}]$, $1 \le k \le K$, such that

$$A_{h,\mathcal{P},\mathbf{m},\mathbf{n}} G_{h,\mathcal{P}}^{\gamma_{h,\mathcal{P},\mathbf{m},\mathbf{n}}} = \sum_{1\le k\le K} \left(F_k \sum_{0\le i+j\le d} A_{i,j} X_k^i Y_k^j + Q_k \Phi_{m_k}(X_k) + R_k \Phi_{n_k}(Y_k) \right) \tag{4.6}$$

and

$$\log A_{h,\mathcal{P},\mathbf{m},\mathbf{n}} = O\left(T^{(45d^2+3d+8)/2}\right) \tag{4.7}$$

since the total number of variables $(\mathbf{A}, (X_k, Y_k)_{1\le k\le K})$ is

$$(d+1)(d+2)/2 + 2K = (45d^2 + 3d + 6)/2.$$

Let

$$\mathfrak{A} = \prod_{h,\mathcal{P},\mathbf{m},\mathbf{n}} A_{h,\mathcal{P},\mathbf{m},\mathbf{n}},$$

where the product is taken over the all $O(T^{2K})$ K-tuples $\mathbf{m}, \mathbf{n}$ with coordinates less than T, all integers h with $1 \le h \le H$ and all $2^{K(K+1)/2}$ partitions $\mathcal{P}$ of $\mathcal{K}$. As in the proof of Theorem 1.1, by (4.1) and (4.7) the number of prime factors of $\mathfrak{A}$ satisfies the bound

$$O\left(\frac{T^{(45d^2+3d+8)/2} T^{2K}}{\log T}\right) = O\left(\frac{T^{(89d^2+3d+12)/2}}{\log T}\right) = o\left(\frac{z}{\log z}\right)$$

since H and K are bounded in terms of d. Suppose $\{a_{i,j}\}_{0\le i+j\le d}$ has integer coordinates and let

$$f(X, Y) = \sum_{0\le i+j\le d} a_{i,j} X^i Y^j \in \mathbb{Z}[X, Y].$$

Take a prime p not dividing $\mathfrak{A}$ and take any polynomial $f \in \mathbb{F}_p[X, Y]$. We first suppose that f is not divisible by Y. Suppose f has at least K distinct solutions

$$(x_k, y_k) \in \overline{\mathbb{F}}_p, \qquad 1 \le k \le K,$$

such that for each k

$$\operatorname{ord} x_k = m_k \le T, \qquad \operatorname{ord} y_k = n_k \le T.$$

Clearly there a partition $\mathcal{P} = (\mathcal{I}, \mathcal{J})$ of $\mathcal{K}$ such that

$$\prod_{(k_1,k_2)\in\mathcal{I}} (x_{k_1} - x_{k_2}) \prod_{(k_1,k_2)\in\mathcal{J}} (y_{k_1} - y_{k_2}) \ne 0$$

Hence, considering (4.6), since p does not divide $\mathfrak{A}$, we see that for each $h = 1, \dots, H$

$$G_h(\{a_{i,j}\}_{0\le i+j\le d}) \equiv 0 \pmod{p}.$$

Hence by (4.5) for some integers $\overline{\alpha}, \overline{\beta}$ and some $\nu = 0, 1$ we have

$$\{a_{i,j}\}_{0\le i+j\le d} \in V^{\nu}_{\overline{\alpha},\overline{\beta},p}.$$

Considering (4.2), let L^{ν}_r denote the degree of each $g^{\nu}_{r,\overline{\alpha},\overline{\beta}}$ as a polynomial in ρ and writing

$$\widetilde{g}^{\nu}_{r,\overline{\alpha},\overline{\beta}} = \sum_{\ell=0}^{L^{\nu}_r} \widetilde{g}^{\nu}_{r,\ell}\rho^{\ell}, \qquad \widetilde{g}^{\nu}_{r,\ell} \in \mathbb{Z}[\{A_{i,j}\}_{0\le i+j\le d}],$$

by the Extension Theorem from Elimination Theory (see for example [10, Chapter 3.6, Exercise 14], if

$$\widetilde{g}^{\nu}_{r,L^{\nu}_r}(\{a_{i,j}\}_{0\le i+j\le d}) \not\equiv 0 \pmod{p} \tag{4.8}$$

for at least one $1 \le r \le R$, then there exists $\overline{\rho} \in \overline{\mathbb{F}}_p$ such that

$$(\{a_{i,j}\}_{0\le i+j\le d}, \overline{\rho}) \in \widetilde{V}^{\nu}_{\overline{\alpha},\overline{\beta},p}$$

which implies f vanishes on the curve $\Phi^{\nu}_{\overline{\alpha},\overline{\beta}}(X, Y, \overline{\rho})$. To complete the proof we need to show that if

$$f(X, Y) = \sum_{0\le i+j\le d} a_{i,j}X^iY^j \in \mathbb{Z}[X, Y]$$

is not divisible by Y, then we have (4.8) for some r. Since

$$f(X, Y) = \sum_{j=0}^{d} \left(\sum_{i\le d-j} a_{i,j}X^i \right) Y^j,$$

from the assumption that f is not divisible by Y we see that there exists some $i_0 \ge 0$ such that $a_{i_0,0} \not\equiv 0 \pmod{p}$.

Consider first when $\nu = 0$, then supposing i_0 is the largest integer such that $a_{i_0,0} \not\equiv 0 \pmod{p}$. Let

$$f_0(X) = \sum_{i\le i_0} a_{i,0}X^i. \tag{4.9}$$

Then we have

$$\mathrm{Res}_Y(f(X,Y),\Phi^0_{\overline{\alpha},\overline{\beta}}(X,Y,\rho))$$
$$= \det\begin{bmatrix} f_0(X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & f_0(X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & f_0(X) & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \rho X^{\overline{\alpha}} & 0 & \cdot & \cdot \\ 0 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \rho X^{\overline{\alpha}} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \rho X^{\overline{\alpha}} \end{bmatrix},$$

so that the highest power of ρ occuring in the above expression is ρ^d. Inductivley expanding the determinant along succesive bottom rows, we see that the only term involving ρ^d is

$$\rho^d X^{d\overline{\alpha}} \left(\sum_{i\le i_0} a_{i,0}X^i\right)^{\overline{\beta}}. \tag{4.10}$$

Considering the highest power of X in (4.10), if we assume that (4.8) is not satisfied for each $1 \le r \le R$ then we must have $a_{i_0,0} \equiv 0 \pmod p$, contradicting the choice of $a_{i_0,0}$.

For the case $\nu = 1$, with $f_0(X)$ defined as in (4.9), we have

$$\mathrm{Res}_Y(f(X,Y),\Phi^1_{\overline{\alpha},\overline{\beta}}(X,Y,\rho))$$
$$= \det\begin{bmatrix} f_0(X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & f_0(X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & f_0(X) & \cdot & \cdot & \cdot & \cdot \\ X^{\overline{\alpha}} & \cdot & \cdot & \cdot & \cdot & \cdot & \rho & 0 & \cdot & \cdot \\ 0 & X^{\overline{\alpha}} & \cdot & \cdot & \cdot & \cdot & \cdot & \rho & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & X^{\overline{\alpha}} & \cdot & \cdot & \cdot & \cdot & \cdot & \rho \end{bmatrix}$$

and the rest of the argument is similar to the case $\nu = 0$.

Finally, if our polynomial f is divisible by Y, then letting Y^{n_f} be the largest power of Y dividing f, we apply the above argument to the polynomial $f' = Y^{-n_f} f$.

5. Comments

We note that the argument of the proof of Theorem 1.1 shows that there is a constant $c(\mathcal{V})$, depending only on $\mathcal{V}$ such that if a prime $p \ge \exp(c(\mathcal{V})T^n)$ then for any positive integers $t_1, \ldots, t_n \le T$ we have $p \nmid b(t_1, \ldots, t_n)$, where $b(t_1, \ldots, t_n)$ is given by (3.3).

This implies that for any prime we have

$$\max\{\operatorname{ord} x_1, \ldots, \operatorname{ord} x_n\} > (\log p)^{1/n} \tag{5.1}$$

for every point $(x_1, \ldots, x_n) \in \mathcal{V}_p$.

We note that for $m = 1$ and $n = 2$, that is, for plane curves, the exponents in Theorem 1.1 and in (5.1) become $1/4$ and $1/2$, respectively, which are the same exponents as the ones obtained in [8] via resultants.

Finally, we remark that if we restrict ourselves to the points on $\mathcal{V}_p$ that are defined over the ground field then using a result of Erdős and Murty [12, Theorem 2] one can show that for any function $\varepsilon(z)$ with $\lim_{z\to\infty} \varepsilon(z) = 0$, there is a set of primes p of relative density 1 such that for all but at most $C(\mathcal{V})$ points $(x_1, \ldots, x_n) \in \mathcal{V}_p$ with components from $\mathbb{F}_p$, we have

$$\max\{\operatorname{ord} x_1, \ldots, \operatorname{ord} x_n\} > p^{1/2n+\varepsilon(p)}.$$

Finally, we note that our results is related to the problem of construction so called *variety evasive sets* considered by Dvir, Kollár and Lovett [13]. In particular, Theorem 1.1 shows that for a given variety over $\mathbb{Q}$, that does not contain a monomial curve, for almost all primes p, Cartesian products of small order subgroups of $\mathbb{F}_p^*$ give explicit examples of such sets.

Acknowledgement

The authors are very grateful to the referees for many very useful comments.

This research was supported by the NSF Grants DMS 1301608 and DMS 0932078000 (for M.-C. Chang), by the ARC Grant DP130100237 (for B. Kerr and I. E. Shparlinski) and by the ERC Grant "Diophantine Problems" (for U. Zannier).

M.-C. Chang is also very grateful to the Department of Mathematics of the University of California at Berkeley for hospitality.

References

[1] O. Ahmadi, I. E. Shparlinski and J. F. Voloch, *Multiplicative order of Gauss periods*, Intern. J. Number Theory, **6**, (2010), 877–882.

[2] I. Aliev and C. J. Smyth, *Solving algebraic equations in roots of unity*, Forum Math., **24**, (2012), 641–665.

[3] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number theory for the millenium (Urbana, Illinois, 2000), I, A.K. Peters, (2002), 67–85.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge Univ. Press, Cambridge, (2006).

[5] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, *On the hidden shifted power problem*, SIAM J. Comp., **41**, (2012), 1524–1557.
[6] J. F. Burkhart, N. J. Calkin, S. Gao, J. C. Hyde-Volpe, K. James, H. Maharaj, S. Manber, J. Ruiz and E. Smith, *Finite field elements of high order arising from modular curve*, Designs, Codes and Cryptography, **51**, (2009), 301–314.
[7] M.-C. Chang, *Order of Gauss periods in large characteristic*, Taiwanese J. Math., **17**, (2013), 621–628.
[8] M.-C. Chang, *Elements of large order in prime finite fields*, Bull. Aust. Math. Soc, **88**, (2013), 169–176.
[9] Q. Cheng, S. Gao and D. Wan, *Constructing high order elements through subspace polynomials*, Proc. 23rd ACM-SIAM Symposium on Discrete Algorithms, SIAM Press, (2012), 1457–1463.
[10] D. A. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, (1992).
[11] C. D'Andrea, T. Krick and M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze*, Annales Sci. de l'ENS, **46**, (2013), 549–627.
[12] P. Erdős and R. Murty, *On the order of a* (mod p), Proc. 5th Canadian Number Theory Association Conf., Amer. Math. Soc., Providence, RI, (1999), 87–97.
[13] Z. Dvir, J. Kollár and S. Lovett, *Variety evasive sets*, Comp. Complex., (to appear).
[14] K. Ford, *The distribution of integers with a divisor in a given interval*, Annals Math., **168**, (2008), 367–433.
[15] J. von zur Gathen and I. E. Shparlinski, *Gauss periods in finite fields*, Proc. 5th Conference of Finite Fields and their Applications, Augsburg, 1999, Springer-Verlag, Berlin, (2001), 162–177.
[16] T. Krick, L. M. Pardo and M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J., **109**, (2001), 521–598.
[17] M. Laurent, *Équations diophantiennes exponentielles*, Invent. Math., **78**, (1984), 299–327.
[18] L. Leroux, *Computing the torsion points of a variety defined by lacunary polynomials*, Math. Comp., **81**, (2012), 1587–1607.
[19] R. Popovych, *Elements of high order in finite fields of the form* $\mathbb{F}_q[x]/\Phi_r(x)$, Finite Fields Appl., **18**, (2012), 700–710.
[20] R. Popovych, *Elements of high order in finite fields of the form* $\mathbb{F}_q[x]/(x^m - a)$, Finite Fields Appl., **19**, (2013), 86–92.
[21] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp., **58**, (1992), 369–380.
[22] I. E. Shparlinski, *On primitive elements in finite fields and on elliptic curves*, Matem. Sbornik, **181**, (1990), 1196–1206 (in Russian).
[23] I. E. Shparlinski, *Approximate constructions in finite fields*, Proc. 3rd Conf. on Finite Fields and Appl., Glasgow, 1995, London Math. Soc., Lect. Note Series, **233**, (1996), 313–332.
[24] I. Shparlinski, *On the multiplicative orders of* γ *and* $\gamma + \gamma^{-1}$ *over finite fields*, Finite Fields Appl., **7**, (2001), 327–331.
[25] J. F. Voloch, *On the order of points on curves over finite fields*, Integers, **7**, (2007), Article A49, 4 pp.
[26] J. F. Voloch, *Elements of high order on finite fields from elliptic curves*, Bull. Aust. Math. Soc., **81**, (2010), 425–429.
[27] U. Zannier, *Lecture notes on Diophantine analysis*, Publ. Scuola Normale Superiore, Pisa, (2009).
[28] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Princeton Univ. Press, Princeton, (2012).

Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521, USA
E-mail: mcc@math.ucr.edu

Bryce Kerr
Department of Pure Mathematics
University of New South Wales
Sydney, NSW 2052, Australia
E-mail: b.kerr@student.unsw.edu.au

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor.shparlinski@unsw.edu.au

Umberto Zannier
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, Italy
E-mail: u.zannier@sns.it