ACTA ARITHMETICA
181.4 (2017)

On the Bombieri–Pila method over function fields

by

Alisa Sedunova (Göttingen and Bonn)

1. Introduction. E. Bombieri and J. Pila [1] proved that if Γ is a subset of an irreducible algebraic curve of degree d inside a square of side N, then the number of lattice points on Γ is bounded by $c(d,\varepsilon)N^{1/d+\varepsilon}$ for any $\varepsilon > 0$, where the constant $c(d,\varepsilon)$ does not depend on Γ. There are many analogues of this remarkable result. For example, one can be interested in finding a bound for the number of solutions of $f(x,y) = 0 \bmod p$ with $x \in I$ and $y \in J$, where I and J are short intervals in $\mathbb{Z}/p\mathbb{Z}$ (see [2] and [4]). Such results are p-analogues of the Bombieri–Pila bound. (Here we should assume that the lengths of I and J are much smaller than p, so that the Weil bound and other standard methods cannot be applied.)

One can go further and look for a function field analogue. Here we work in a finite field $\mathbb{F}_{q^n}$ modelled as $\mathbb{F}_q[T]/f(T)$ where f is a fixed irreducible polynomial of degree n and T is a formal variable. Then one can define an "interval" as a set of polynomials of the form $X + Y = X(T) + Y(T)$, where $X \in \mathbb{F}_q[T]$ is a fixed polynomial and $Y(T) \in \mathbb{F}_q[T]$ runs through all polynomials of degree bounded by a given natural number. This point of view was used by J. Cilleruelo and I. Shparlinski [3] to obtain some bounds on the number of solutions of polynomial congruences modulo a prime with variables in short intervals. The same authors also formulated [3, Problem 9] that is solved here.

Our main goal is to prove

Theorem 1. *Let $\mathcal{C}$ be an irreducible algebraic curve of degree d over $\mathbb{F}_q[T]$, q is a prime power. Define S as the set of points on $\mathcal{C}$ inside I^2, where I is a set of polynomials $X \in \mathbb{F}_q[T]$ with $\deg X \le n$ and $|I| = q^{n+1}$. Then*

$$|S| \ll_{d,\varepsilon} |I|^{1/d+\varepsilon}.$$

2010 *Mathematics Subject Classification*: Primary 11P21; Secondary 14H05.
Key words and phrases: integral points, function fields, diophantine equations.
Received 19 September 2016; revised 3 August 2017.
Published online 4 December 2017.

DOI: 10.4064/aa8613-8-2017

One can ask: why cannot we just follow the Bombieri–Pila approach in order to get Theorem 1? Unfortunately, in this case we will come across some difficulties in getting [1, Lemma 2], since we do not have the mean value analogue for function fields (see [8, Lemma 1]). There seem to be at least two plausible ways to avoid this difficulty. The first one consists of getting a function field variant of Heath-Brown's [6, Theorem 14]. The second one is to adapt the method of Helfgott–Venkatesh [7]. Since the first one appears to require some long and technical computations, we follow the second approach here. Another result of this type is given in [5, Theorem 5.6.3].

We need analogues of [7, Propositions 3.1 and 3.2]. Combining and developing the original ideas of [1] together with an adaptation of some results of [7] will lead to our main result.

We use Theorem 1 to get some applications. We prove bounds on the number of isomorphism classes which are represented by elliptic curves $E_{a,b}$ parametrized by coefficients $a, b \in \mathbb{F}_q[T]$ lying in a small box, say, I^2. Results of that type can be found in [4, Lemma 5.1], where a similar estimate is proven over $\mathbb{F}_p$. We follow [2] and use this result to estimate the number of elliptic curves in a given isomorphism class with coefficients lying in a small box. We use some ideas of [4].

2. Auxiliary statements. Let q be a prime power, and let X and Y be variables with values in $\mathbb{F}_q[T]$, i.e. $X = X(T) = a_0 + a_1T + \cdots + a_nT^n$, $Y = Y(T) = b_0 + b_1T + \cdots + b_mT^m$, where T is a place holder, $a_i, b_j \in \mathbb{F}_q$, $i = 0, \dots, \deg X = n$ and $j = 0, \dots, \deg Y = m$. For $X \in \mathbb{F}_q[T]$, let $|X| = q^{\deg X}$.

In what follows, $\mathcal{C}$ is an irreducible algebraic curve of degree d over $\mathbb{F}_q[T]$, which is described by $F(X, Y) = 0$, where $F(X, Y) \in (\mathbb{F}_q[T])[X, Y]$. Write S for the set of points on $\mathcal{C}$ inside I^2, where I is an interval in $\mathbb{F}_q[T]$ defined before (we consider intervals I centered at 0, i.e. of the form $I = \{Y(T) \in \mathbb{F}_q[T] \mid \deg Y \le n\}$).

For any $F(X, Y) \in (\mathbb{F}_q[T])[X, Y]$ we write $\deg_X F$ and $\deg_T F$ to denote the degree of F with respect to X and T respectively. We also use the standard notation $\deg F(X, Y)$ for the degree of $F(X, Y)$ as a polynomial in X and Y.

Let $\mathcal{W}$ be a set of finitely many linearly independent polynomials $F \in (\mathbb{F}_q[T])[X, Y]$ including the constant polynomial $\mathbf{1}$. Write $d_{\mathcal{W}}$ for the sum of the degrees of all elements in $\mathcal{W}$ and define $\omega = |\mathcal{W}|$. Assume that the elements of $\mathcal{W}$ separate points, meaning that for any two distinct $(X_1, Y_1), (X_2, Y_2) \in (\mathbb{F}_q[T])^2$ there is an $F \in \mathcal{W}$ such that $F(X_1, Y_1) \ne F(X_2, Y_2)$. We define a $\mathcal{W}$-*curve* to be an affine algebraic curve described by an equation $G(X, Y) = 0$, where all the monomials of G belong to $\mathcal{W}$.

In the proof of Theorem 1 we will use the following choice of $\mathcal{W}$:

EXAMPLE 1. Define $\mathcal{W} = \mathcal{W}_{d,M}$ as

$$\mathcal{W} = \{X^i Y^j \mid i \le d,\ j \le M\},$$

where d and M are given natural numbers. Then

$$\omega = (d+1)(M+1), \qquad d_{\mathcal{W}} = (d+1)(M+1)\frac{d+M}{2}.$$

The $\mathcal{W}$-curves are plane curves of degree $\le d$ and $\le M$ in X and Y respectively.

This choice is taken from the work of Bombieri and Pila [1].

LEMMA 1. *Let $\mathcal{C}$ be an irreducible algebraic curve of degree d defined over $\mathbb{F}_q[T]$ and let S be the set of points on $\mathcal{C}$ inside I^2. Suppose that the number of residues $\{(X,Y) \bmod f \mid X, Y \in S\}$ is at most $\alpha|f|$ for some fixed $\alpha > 0$ and for every irreducible polynomial $f \in \mathbb{F}_q[T]$. Assume that $\mathcal{W}$ is chosen so that any $\mathcal{W}$-curve contains at most a constant number C of elements of S. Then as $|I| \to \infty$,*

$$|S| \ll_{\mathcal{W}} |I|^{\frac{2\alpha d_{\mathcal{W}}}{\omega(\omega-1)} + \psi(\omega, C, \alpha)}, \quad \textit{where} \quad \psi(\omega, C, \alpha) \le \frac{2\alpha d_{\mathcal{W}} C}{\omega^2(\omega-1)^2}.$$

Proof. The proof is in the spirit of [7, Proposition 3.1]. Write $P = (X, Y)$ for a point in $(\mathbb{F}_q[T])^2$ with coordinates $X, Y \in \mathbb{F}_q[T]$. Fixing an arbitrary ordering $F_1, \dots, F_\omega$ of the elements of $\mathcal{W}$, we define

$$W : ((\mathbb{F}_q[T])^2)^\omega \to \mathbb{F}_q[T] \quad \text{by} \quad W(P_1, \dots, P_\omega) = \det\left(F_i(P_j)\right)_{1 \le i,j \le \omega}.$$

Fix any irreducible polynomial f with $\deg f \,|\, \operatorname{ord}_q N$, where N is a natural number to be set at the end, and $\operatorname{ord}_q N$ is the maximal power of q that divides N, $q^{\operatorname{ord}_q N} \,\|\, N$. (Keep in mind that this means that $|f| = q^{\deg f} \le q^{\operatorname{ord}_q N} \le N$.) Notice that if the number of distinct points among $P_i \bmod f$ is less than or equal to some k, then

$$\operatorname{ord}_f W(P_1, \dots, P_\omega) \ge \omega - k.$$

Let $\mathbf{P}$ denote an ensemble of points in S,

$$\mathbf{P} = (P_1, \dots, P_\omega), \qquad P_i = (X_i, Y_i) \in S.$$

We say that $\mathbf{P}$ is *admissible* if $W(\mathbf{P}) = W(P_1, \dots, P_\omega) \ne \mathbf{0}$ (where $\mathbf{0}$ stands for the zero polynomial in $\mathbb{F}_q[T]$). Recall that $|X| = q^{\deg X}$ for $X \in \mathbb{F}_q[T]$ and define

$$\Delta = \prod_{\mathbf{P}}^{*} W(\mathbf{P});$$

here and below, $*$ means that we take an operation over all admissible $\mathbf{P}$'s. By the definition of $d_{\mathcal{W}}$ we have

$$|W(\mathbf{P})| \ll_{\mathcal{W}} |I|^{d_{\mathcal{W}}}$$

for every $\mathbf{P} \in S^\omega$. Taking $\log_q |\Delta|$ and applying the expression above gives

$$\frac{\log_q |\Delta|}{|S|^\omega} = \frac{\sum_{\mathbf{P}}^* \log_q |W(\mathbf{P})|}{|S|^\omega} \le d_{\mathcal{W}} \log_q |I| + O_{\mathcal{W}}(1). \tag{2.1}$$

For every $P \in (\mathbb{F}_q[T])^2$ let ρ_P be the fraction of points in S that reduce to $P \bmod f$. For each $\mathbf{P}$ let $\kappa(\mathbf{P}) \in \{0, \dots, \omega - 1\}$ be such that $\omega - \kappa(\mathbf{P})$ is the number of distinct points among the $P_i \bmod f$. Then

$$\operatorname{ord}_f W(\mathbf{P}) \ge \omega - (\omega - k(\mathbf{P})) = k(\mathbf{P}),$$

which brings us to

$$\sum_{\mathbf{P}}^* \operatorname{ord}_f W(\mathbf{P}) \ge \sum_{\mathbf{P}}^* \kappa(\mathbf{P}) = \sum_{\mathbf{P}} \kappa(\mathbf{P}) - \sum_{\mathbf{P}}^{\mathrm{na}} \kappa(\mathbf{P}), \tag{2.2}$$

where the first sum on the right hand side is over all $\mathbf{P}$ and the second is over all inadmissible $\mathbf{P}$.

We proceed in two steps. First, we will calculate the sum over all $\mathbf{P} \in S^\omega$ by probabilistic methods. Here we see $P_1, \dots, P_\omega$ as ω independent random variables with values in $(\mathbb{F}_q[T])^2$ and use

$$Y_P = \begin{cases} 1 & \text{if at least one of } P_i \ne P \text{ in } S \text{ is equal to } P \bmod f, \\ 0 & \text{otherwise.} \end{cases}$$

In the case of $\mathbf{P}$ inadmissible, we have either at least two points $P_i = P_j$ among the entries of $\mathbf{P}$, or at least two points $P_i = P_j \bmod f$, $P_i, P_j \in \mathbf{P}$, $P_i \ne P_j$. The number of pairs P_i, P_j that satisfy the first possibility can be easily bounded by $O(|S|^{\omega-1})$, and in the latter case we permute the entries of our matrix so as to have

$$\det (F_i(P_j))_{1 \le i,j \le l} \ne 0$$

with maximal possible l and then apply the fact that any $\mathcal{W}$-curve contains at most a constant number of elements of S.

Let us start with the sum over all $\mathbf{P} \in S^\omega$. Consider $\mathbf{P}$ as a random variable with uniform distribution. Then the expected value of the number of distinct points among the $P_i \bmod f$ is equal to

$$\frac{\sum_{\mathbf{P}} (\omega - \kappa(\mathbf{P}))}{|S|^\omega} = \mathbb{E}\Big(\sum_P Y_P\Big).$$

Further,

$$\begin{aligned} \mathbb{E}\Big(\sum_P Y_P\Big) &= \sum_P \mathbb{E}(Y_P) = \sum_P \operatorname{Prob}(\exists P_i \ne P \mid P_i \equiv P \bmod f) \\ &= \sum_P \big(1 - \operatorname{Prob}(\nexists P_i \ne P \mid P_i \equiv P \bmod f)\big) \end{aligned}$$

$$= \sum_P \big(1 - \mathrm{Prob}(\forall P_i \neq P \mid P_i \not\equiv P \bmod f)\big)$$
$$= \sum_P \Big(1 - \prod_i \mathrm{Prob}(P_i \not\equiv P \bmod f,\, P_i \neq P)\Big)$$
$$= \sum_P \Big(1 - \prod_i (1-\rho_P)\Big) = \sum_P (1-(1-\rho_P)^\omega).$$

Consequently,

$$\frac{\sum_{\mathbf{P}} (\omega - \kappa(\mathbf{P}))}{|S|^\omega} = \sum_P \left(1-(1-\rho_P)^\omega\right).$$

Next

$$\frac{\sum_{\mathbf{P}} \kappa(\mathbf{P})}{|S|^\omega} = \frac{\sum_{\mathbf{P}} \omega}{|S|^\omega} - \sum_P (1-(1-\rho_P)^\omega) = \sum_P \big((1-\rho_P)^\omega + \omega\rho_P - 1\big). \tag{2.3}$$

Now let us bound the sum over all inadmissible $\mathbf{P}$'s. Consider the set of such $\mathbf{P}$'s with $\kappa(\mathbf{P}) > 0$. Then one of the following is true:

(1) There exist i and j such that $P_i = P_j$.
(2) There exist i and j such that $P_i \equiv P_j \bmod f$, but $P_i \neq P_j$.

The total number of inadmissible $\mathbf{P}$ such that (1) holds is $O(|S|^{\omega-1})$. For (2), permute the entries in such a way that $i = 1$, $j = 2$ and $F_1 = \mathbf{1}$, $F_2(P_i) \neq F_2(P_j)$ (this is possible since we have assumed that the elements of $\mathcal{W}$ separate points and $\mathcal{W}$ contains $\mathbf{1}$). Then for $l = 2$,

$$\det\left(F_i(P_j)\right)_{1\le i,j\le l} \neq 0.$$

Take the maximal l such that the above statement still holds. Then P_{l+1} lies on a $\mathcal{W}$ curve determined by $P_1, \ldots, P_l$. As we demanded, the number of possible values for P_{l+1} is bounded above by a constant. Then the number of inadmissible $\mathbf{P}$ such that (2) holds is

$$O_\omega(|S|^{\omega-3}\delta),$$

where δ is the number of pairs $(Q_1, Q_2) \in S^2$ that reduce to the same point mod f. Since ρ_P is defined as a fraction of points in S that reduce to P mod f, one can write

$$\delta = |S|^2 \sum_P \rho_P^2.$$

Summing the two results we see that there are at most

$$O_\omega(|S|^{\omega-1} + |S|^{\omega-3}\delta) = O_\omega\Big(|S|^{\omega-1}\Big(1 + \sum_P \rho_P^2\Big)\Big) \tag{2.4}$$
$$= |S|^\omega O_\omega\Big(|S|^{-1}\Big(1 + \sum_P \rho_P^2\Big)\Big)$$

inadmissible $\mathbf{P}$ with $\kappa(\mathbf{P}) > 0$.

We divide (2.2) by $|S|^\omega$ and insert (2.3) and (2.4) divided by $|S|^\omega$ into (2.2) to see that

$$\sum_{\mathbf{P}}{}^{*}\frac{\operatorname{ord}_f W(\mathbf{P})}{|S|^\omega} \geq \sum_P\big((1-\rho_P)^\omega+\omega\rho_P-1\big)+O_\omega\Big(|S|^{-1}\Big(1+\sum_P\rho_P^2\Big)\Big). \tag{2.5}$$

Now we have to give an upper bound for the first term on the right hand side of (2.5), that is, for (2.3). In order to do that we consider two cases.

(1) If for any point P we have $\rho_P < C/\omega^4$, then

$$\begin{aligned}(1-\rho_P)^\omega+\omega\rho_P-1&=1-\omega\rho_P+\binom{\omega}{2}\rho_P^2+\cdots+(-1)^\omega\binom{\omega}{\omega}\rho_P^\omega+\omega\rho_P-1\\&\geq\rho_P^2\bigg(\binom{\omega}{2}-\rho_P\binom{\omega}{3}+\cdots+(-1)^\omega\rho_P^{\omega-2}\binom{\omega}{\omega}\bigg)\\&\geq\rho_P^2\bigg(\binom{\omega}{2}\bigg)-\varphi(\omega,C)\bigg),\end{aligned}$$

where $\varphi(\omega,C)$ is quite small,

$$\varphi(\omega,C)\leq\frac{C}{\omega}+O_C\bigg(\frac{1}{\omega^2}\bigg).$$

Hence (2.3) becomes

$$\frac{\sum_{\mathbf{P}}\kappa(\mathbf{P})}{|S|^\omega}\geq\frac{\omega(\omega-1)}{2}\sum_P\rho_P^2-\varphi(\omega,C)\Big(\sum_P\rho_P^2\Big). \tag{2.6}$$

Using Cauchy's inequality for the inner sum in $O(\cdot)$ yields

$$\sum_P\rho_P^2\geq\frac{1}{\alpha|f|}\Big(\sum_P\rho_P\Big)^2=\frac{1}{\alpha|f|}.$$

Inserting this into (2.5) we get

$$\frac{1}{|S|^\omega}\sum_{\mathbf{P}}{}^{*}\operatorname{ord}_f W(\mathbf{P})\geq\bigg(\frac{\omega(\omega-1)}{2\alpha}-\frac{\varphi(\omega,C)}{\alpha}\bigg)\frac{1}{|f|}+O_{\omega,\alpha,|f|}(|S|^{-1}). \tag{2.7}$$

(2) Suppose now that there is a point P such that $\rho_P\geq C/\omega^4$. Using the fact that

$$\frac{\partial}{\partial x}((1-x)^\omega+\omega x-1)=\omega(1-(1-x)^{\omega-1})\geq\omega(1-(1-x))=\omega x$$

we get

$$(1-\rho_P)^\omega+\omega\rho_P-1\geq\frac{1}{2}\omega\rho_P^2\geq\frac{1}{2}\,\frac{C^2}{\omega^7}.$$

Since for $P' \neq P$ we have $(1-\rho_{P'})^\omega + \omega\rho_{P'} - 1 \geq 0$ and $\sum_P \rho_P^2 \leq 1$, we obtain

$$\frac{\operatorname{ord}_f W(\mathbf{P})}{|S|^\omega} \geq \frac{C^2}{2\omega^7} - O_\omega(|S|^{-1}).$$

For f with $|f| > c_{\omega,\alpha}$ depending only on ω the bound above implies (2.7) again.

Multiply (2.7) by $\log_q |f|$ and sum over all f such that $\deg f \,|\, \operatorname{ord}_q N$ and $\deg f > c_{\omega,q}$ (which expresses the fact that $|f| > c_{\omega,\alpha}$, denoted below by $**$):

$$\left(\frac{\omega(\omega-1)}{2\alpha} - \frac{\varphi(\omega,C)}{\alpha}\right) S_1 + O_{\omega,\alpha,|f|}\left(\frac{S_2}{|S|}\right) \leq \sum_{\deg f \mid \operatorname{ord}_q N}^{**} \sum_{\mathbf{P}}^{*} \frac{\log_q |f| \operatorname{ord}_f W(\mathbf{P})}{|S|^\omega},$$

where

$$S_1 = \sum_{\deg f \mid \operatorname{ord}_q N}^{**} \frac{\log_q |f|}{|f|} \quad \text{and} \quad S_2 = \sum_{\deg f \mid \operatorname{ord}_q N}^{**} \log_q |f|.$$

Since $\operatorname{ord}_f W(\mathbf{P}) \leq \log_{|f|} |W(\mathbf{P})|$, we have $\log_q |f| \operatorname{ord}_f W(\mathbf{P}) \leq \log_q |W(\mathbf{P})|$. Thus after applying (2.1) the expression above becomes

$$S_1\left(\frac{\omega(\omega-1)}{2\alpha} - \frac{\varphi(\omega,C)}{\alpha}\right) + O_{\omega,\alpha,|f|}(S_2|S|^{-1}) \leq d_{\mathcal{W}} \log_q |I| + O_{\mathcal{W}}(1). \tag{2.8}$$

Further,

$$S_2 = \sum_{f:\deg f \mid \operatorname{ord}_q N} \deg f = \sum_{i \mid \operatorname{ord}_q N} i M_i(q) = q^{\operatorname{ord}_q N} \leq N,$$

where $M_i(q)$ counts the number of irreducible polynomials of degree i and has the property $\sum_{i|n} i M_i(q) = q^n$. Similarly, $S_1 \geq \log_q N$. Inserting the estimates for S_1 and S_2 in (2.8) and taking $N = |S|$ we get

$$\log_q |S|\left(\frac{\omega(\omega-1)}{2\alpha} - \frac{\varphi(\omega,C)}{\alpha}\right) + O_{\omega,\alpha,|f|}(1) \leq d_{\mathcal{W}} \log_q |I| + O_{\mathcal{W}}(1).$$

Using the fact that

$$\varphi(\omega,C) \leq \frac{C}{\omega} + O_C\left(\frac{1}{\omega^2}\right)$$

we end up with

$$|S| \ll_{\mathcal{W}} |I|^{\frac{2\alpha d_{\mathcal{W}}}{\omega(\omega-1)} + \psi(\omega,C,\alpha)},$$

where $\psi(\omega,C,\alpha)$ is as in the statement of the lemma. ∎

LEMMA 2. *Let $\mathcal{C}$ be an irreducible algebraic curve of degree d over $\mathbb{F}_q[T]$, defined by $F(X,Y) = 0$. There exists a linear transformation $(X,Y) \to (X',Y')$ such that $\deg_{X'} F(X',Y') = d$.*

Proof. We can assume $\deg_X F(X,Y) < d$, otherwise we are done. Any polynomial $F(X,Y) \in (\mathbb{F}_q[T])[X,Y]$ can be written as

$$F(X,Y) = \sum_{\substack{i\in J_1\\ j\in J_2}} F_{ij}X^iY^j,$$

where $J_1, J_2 \subset \{0,\dots,d\}$, $F_{ij} \in \mathbb{F}_q$ and

$$\max_{\substack{i\in J_1\\ j\in J_2}}(i+j) = \deg F = d, \qquad \max_{i\in J_1} i = \deg_X F < d.$$

Consider a linear transformation $(X,Y) \to (X',Y')$ such that

$$(X,Y) = (AX'+BY', CX'+DY'),$$

where $A,B,C,D \in \mathbb{F}_q[T]$ with $AD-BC \neq \mathbf{0}$. Changing the variables $(X,Y) \to (X',Y')$ we obtain

$$\begin{aligned} F(X,Y) &= \sum_{\substack{i\in J_1\\ j\in J_2}} F_{ij}(AX'+BY')^i(CX'+DY')^j \\ &= \sum_{\substack{i\in J_1\\ j\in J_2}} \sum_{k=0}^{i}\sum_{l=0}^{j} \binom{i}{k}\binom{j}{l} F_{ij}A^{i-k}B^kC^{j-l}D^l(X')^{i+j-k-l}(Y')^{k+l}. \end{aligned}$$

In the new variables (X',Y') we have

$$\deg_{X'} F = \max_{\substack{k\in\{0,\dots,i\},\, i\in J_1\\ l\in\{0,\dots,j\},\, l\in J_2}} (i+j-k-l),$$

which can be equal to d, since $\max_{i\in J_1,\, j\in J_2}(i+j) = \deg F = d$. ∎

3. Proof of Theorem 1. We start with an interpolation argument, which is used with a similar goal to [6]. Let again $F \in (\mathbb{F}_q[T])[X,Y]$ be written in the form

$$F(X,Y) = \sum_{\substack{i\in J_1\\ j\in J_2}} F_{ij}X^iY^j,$$

where $J_1, J_2 \subset \{0,\dots,d\}$, $F_{ij} \in \mathbb{F}_q$. We count the number of distinct lattice points $P = (X,Y) \in I^2 \cap \mathcal{C}$. If there are less than $r(d) = d^2+1$ such points, then we are done. Suppose that we have at least $r(d)$ points: $P_i = (X_i, Y_i) \in C \cap I^2$, $i = 1,\dots,r(d)$, with $F(P_i) = \mathbf{0}$. Denote by $n(d) = \frac{1}{2}(d+1)(d+2)$ the number of monomials of degree $\le d$. Consider the $n(d)\times r(d)$ matrix A whose ith row consists of the monomials of degree d in X_i, Y_i. Let $\vec{b} \in F_q^{n(d)}$ be the vector whose entries are the corresponding coefficients F_{ij} of $F(X,Y)$. Then

$$A\vec{b} = \vec{0}.$$

Since $\vec{b} \neq \vec{0}$, the matrix A has rank at most $n(d)-1$. Thus there is a so-

lution $\vec{g} \neq \vec{0}$, where $\vec{g}$ is constructed out of the polynomials $X_i, Y_i \in I$, so $|\vec{g}| \ll_d |I|^{dn(d)}$. Let $G \in (\mathbb{F}_q[T])[X,Y]$ be the form of degree d corresponding to the vector $\vec{g}$. Then $G(X,Y)$ and $F(X,Y)$ share $r(d)$ zeros (the points P_i). By Bézout's theorem this is possible only if G is a multiple of F. Since F is irreducible, G is also irreducible and defines the same curve $\mathcal{C}$. Let us work with G instead of F.

We proceed in two steps:

(1) If $\deg_X G < d$, then by Lemma 2 we can change variables so that $\deg_{X'} G = d$. If not, then go to the next step.

(2) Using the Hasse–Weil bounds

$$|\#C(\mathbb{F}_q[T]) - (q+1)| \leq 2g\sqrt{q},$$

where $C(\mathbb{F}_q[T])$ is the set of rational points on a smooth absolutely irreducible projective curve C of genus g over a finite field $\mathbb{F}_q[T]$, we obtain

$$|\{(X,Y) \in (\mathbb{F}_q[T] \bmod f)^2 : G(X,Y) = 0 \bmod f\}| = |f| + O_d(\sqrt{|f|}).$$

Further, for every $\varepsilon > 0$ and every irreducible $f \in \mathbb{F}_q[T]$ with $|f| \geq c(\varepsilon)$ the set S intersects at most $(1+\varepsilon/2)|f|$ residue classes mod f (here $c(\varepsilon)$ is a constant that depends only on ε). Applying Lemma 1 with $\alpha = 1+\varepsilon/2$ and $\mathcal{W}$ from Example 1, $\mathcal{W} = \mathcal{W}_{d-1,M}$, we obtain

$$|S| \ll_{\varepsilon,\mathcal{W}} |I|^{(1+\varepsilon/2)(d+M-1)/(d(M+1)-1)+\psi(\omega,C,1+\varepsilon/2)}.$$

We choose M large enough and use $\omega = (d+1)(M+1)$ together with bounds for $\psi(\omega, C, 1+\varepsilon/2)$ in terms of ω to end up with

$$|S| \ll_{\varepsilon,\mathcal{W}} |I|^{1/d+3\varepsilon/4+o_{\varepsilon,C}(1)}.$$

4. An application to counting elliptic curves. In this section we count the number of elliptic curves $E_{a,b}$ with coefficients a, b in a small box that lie in the same isomorphism class. This is a generalization of the statements presented in [4]. We have an opportunity to apply Theorem 1 and to show that some results for number fields can be adapted to function fields.

Let I stand again for an interval of polynomials of the form $X(T)+Y(T)$, where $X(T) \in \mathbb{F}_q[T]$ is fixed and $Y(T) \in \mathbb{F}_q[T]$ runs through all polynomials of degree $\leq d$. The coefficients of X and Y belong to $\mathbb{F}_q$ just as in Section 2.

For a prime power q we consider the family of elliptic curves

$$E_{a,b} : Y^2 = X^3 + aX + b,$$

where X and Y belong to $\mathbb{F}_q[T]$ as before and a, b are some coefficients from $\mathbb{F}_q[T]$ with $4a^3 + 27b^2 \neq \mathbf{0}$. Let $f \in \mathbb{F}_q[T]$. As in the number field case, we say that two curves $E_{a,b}$ and $E_{c,d}$ are *isomorphic over* $\mathbb{F}_q[T]$ if

$$at^4 \equiv c \pmod f \quad \text{and} \quad bt^6 \equiv d \pmod f.$$

Such an isomorphism implies that

$$a^3d^2 \equiv c^3b^2 \pmod f. \tag{4.1}$$

For $\lambda \in \mathbb{F}_q[T]$ we write $N_\lambda(I^2)$ for the number of solutions to the congruence

$$a^3 \equiv \lambda b^2 \pmod f, \quad (a,b) \in I^2.$$

We are going to give an upper bound on $N_\lambda(I^2)$, which implies upper bounds for the number of elliptic curves $E_{a,b}$ with coefficients $a, b \in I$ that lie in the same isomorphism class.

For a polynomial $X \in \mathbb{F}_q[T]$ and an irreducible polynomial $f \in \mathbb{F}_q[T]$ we set

$$\{X\}_f = \min_{Y \in \mathbb{F}_q[T]} |X - fY| = \min_{Y \in \mathbb{F}_q[T]} q^{\deg(X-fY)}.$$

Similarly to [4, Lemma 3.2], from the Dirichlet pigeon-hole principle we obtain

LEMMA 3. *For real numbers $T_1, \dots, T_s$ which satisfy $1 \le T_1, \dots, T_s \le |f|$ and $T_1 \cdots T_s \ge |f|^{s-1}$, and any $X_1, \dots, X_s \in \mathbb{F}_q[T]$, there exists $t \in \mathbb{F}_q[T]$ such that t is not a multiple of f and*

$$\{X_i t\}_f \ll T_i, \quad i = 1, \dots, s.$$

Now we can give a good bound for $N_\lambda(I^2)$:

THEOREM 2. *Let I be an interval of polynomials of degree $\le d$ with coefficients in $\mathbb{F}_q$, and suppose the length of I is $|I| = q^d$. For any irreducible $f \in \mathbb{F}_q[T]$ such that $1 \le |I| \le |f|^{1/9}$ and for any $\lambda \in \mathbb{F}_q[T]$ we have*

$$N_\lambda(I^2) \le |I|^{1/3+o(1)}.$$

Proof. We have to estimate the number of solutions to

$$(X + X_0)^3 \equiv \lambda(X_0 + Y)^2 \pmod f.$$

This congruence is equivalent to

$$X^3 + 3XX_0^2 + 3X^2X_0 - \lambda Y^2 - 2\lambda X_0 Y \equiv \lambda X_0^2 - X_0^3 \pmod f. \tag{4.2}$$

For any $T \le |f|^{1/4}/|I|^{1/2}$ we can apply Lemma 3 to

$$X_1 = 1, \quad X_2 = 3X_0, \quad X_3 = 3X_0^2, \quad X_4 = -\lambda, \quad X_5 = -2\lambda X_0$$

and

$$T_1 = T^4|I|^2, \quad T_2 = T_4 = \frac{|f|}{T|I|}, \quad T_3 = T_5 = \frac{|f|}{T},$$

and find that there exists t with $|t| \le T^4|I|^2$ such that

$$\{3X_0t\}_f \le \frac{|f|}{T|I|}, \quad \{3X_0^2t\}_f \le \frac{|f|}{T}, \quad \{\lambda t\}_f \le \frac{|f|}{T|I|}, \quad \{2\lambda X_0 t\}_f \le \frac{|f|}{T}.$$

For $i = 1, \dots, 5$ define $f_i = X_i t$. Multiplying (4.2) by t leads to

$$f_1X^3 + f_2X^2 + f_3X + f_4Y^2 + f_5Y + f_6 = fZ, \tag{4.3}$$

where

$$|f_1| \le T^4|I|^2, \quad |f_2|, |f_4| \le \frac{|f|}{T|I|}, \quad |f_3|, |f_5| \le \frac{|f|}{T}, \quad |f_6| \le \frac{|f|}{2}.$$

Since for $X, Y \in I$ we have $|X|, |Y| \le |I|$, the left hand side of (4.3) is bounded above by $T^4|I|^5 + 4|f|\,|I|/T + |f|/2$. Thus by the strong triangle inequality,

$$|Z| \ll \frac{T^4|I|^5}{|f|} + \frac{|I|}{T} + 1.$$

Choosing $T \approx |f|^{1/5}/|I|^{4/5}$ and applying the condition $1 \le |I| \le |f|^{1/9}$ we end up with the bound $|Z| \ll |I|^{9/5}/q^{1/5} + 1 \ll 1$. ∎

Application of Theorem 2 to the family of curves E_{x^2,x^3} with $|x| \le |I|^{1/3}$ shows that the result of Theorem 2 cannot be improved. Thus in general we are not able to get any bound stronger than $N_\lambda(I^2) = O(|I|^{1/3})$.

References

[1] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. 59 (1989), 337–357.

[2] M. Chang, J. Cilleruelo, M. Garaev, J. Hernández, I. Shparlinski and A. Zumalácarregui, *Points on curves in small boxes and applications*, Michigan Math. J. 63 (2014), 503–534.

[3] J. Cilleruelo and I. Shparlinski, *Concentration of points on curves in finite fields*, Monatsh. Math. 171 (2013), 315–327.

[4] J. Cilleruelo, I. Shparlinski and A. Zumalácarregui, *Isomorphism classes of elliptic curves over a finite field in some thin families*, Math. Res. Lett. 19 (2012), 1–9.

[5] R. Cluckers, G. Comte and F. Loeser, *Non-Archimedean Yomdin–Gromov parametrizations and points of bounded height*, Forum Math. Pi 3 (2015), e5, 60 pp..

[6] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Ann. of Math. (2) 155 (2002), 553–598.

[7] H. A. Helfgott and A. Venkatesh, *How small must ill-distributed sets be?*, in: Analytic Number Theory. Essays in Honour of Klaus Roth, Cambridge Univ. Press, 2009, 224–234.

[8] H. P. F. Swinnerton-Dyer, *The number of lattice points on a convex curve*, J. Number Theory 6 (1974), 128–135.

Alisa Sedunova
Mathematisches Institut
Universität Göttingen
Bunsenstraße 3-5
D-37073 Göttingen, Germany
and
Max Planck Institute for Mathematics
Vivatsgasse 7
D-53111 Bonn, Germany
E-mail: alisa.sedunova@phystech.edu