On the Bombieri-Pila Method Over Function Fields

A. Sedunova

June 30, 2015

Abstract

In [1] E. Bombieri and J. Pila introduced a method for bounding the number of integral lattice points that belong to a given arc under several assumptions. In this paper we generalize the Bombieri-Pila method to the case of function fields of genus 0 in one variable. We then apply the result to counting the number of elliptic curves contain in an isomorphism class and with coefficients in a box.

1 Introduction

In [1] E. Bombieri and J. Pila proved that if \( \Gamma \) is a subset of an irreducible algebraic curve of degree \( d \) inside a square of side \( N \), then the number of lattice points on \( \Gamma \) is bounded by \( c(d, \varepsilon) N^{\frac{d}{2} + \varepsilon} \) for any \( \varepsilon > 0 \), where the constant \( c(d, \varepsilon) \) does not depend on \( \Gamma \). There are many analogues of this remarkable result. For example, one can be interested in finding a bound for a number of solutions of \( f(x, y) = 0 \mod p \) with \( x \in I, y \in J \), where \( I \) and \( J \) are short intervals in \( \mathbb{Z}/p\mathbb{Z} \) (see [2] and [3]). Such results are \( p \)-analogues of the Bombieri-Pila bound. (Here we should assume that the lengths of \( I \) and \( J \) are much shorter 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 \( F_q^n \) modelled as \( F_q[T]/f(T) \) where \( f \) is a fixed irreducible polynomial of degree \( n \) and \( T \) is a formal variable. Then an interval is the set of polynomials of the form \( X + Y = X(T) + Y(T) \), where \( X \in F_q[T] \) is a fixed polynomial and \( Y(T) \) runs through all polynomials of degree bounded by a given natural number. This point of view was used by J. Cilleruelo and I. Shparlinski in [4] for obtaining some bounds on the number of solutions of polynomial congruences modulo a prime with variables in short intervals. The same authors also formulated [4, Problem 9], which is solved here.

Our main goal is to prove

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

\[
|S| \ll_{d, \varepsilon} |I|^{\frac{d}{2} + \varepsilon}.
\]

One can pose a question: why can we not just follow the Bombieri-Pila approach in order to get Theorem 1? Unfortunately, in this case we will cross some difficulties in getting Lemma 2 of [1], since we do not have the necessary analogue of the mean value theorem in function fields (see [5], Lemma 1). There seem to be at least two plausible ways to avoid this difficulty. The first one consists in getting a function field variant of Theorem 4 in Heath-Brown’s article [6]. The second one, which we will follow here, is to adapt the method of Helfgott-Venkatesh [7].

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

After that we will use Theorem 1 to get some applications, such as a calculation of the number of isomorphism classes which are represented by elliptic curves \( E_{a,b} \) parametrized by coefficients \( a, b \in F_q[T] \) lying in a small box, say, \( I^2 \). Using this result one can calculate the number of elliptic curves lying in a given isomorphism class with coefficients lying in a small box. To proceed we will work with ideas proposed in [3].
2 Auxiliary statements

Let $X$ and $Y$ be variables with values in $\mathbb{F}_q[T]$, i.e. their values are of the form $X = X(T) = a_0 + a_1T + \ldots + a_nT^n$, $Y = Y(T) = b_0 + b_1T + \ldots + b_mT^m$, where $T$ is a placeholder, $a_i, b_j \in \mathbb{F}_q$, $i = 0, \ldots, \deg X = n$, $j = 0, \ldots, \deg Y = m$. For $X \in \mathbb{F}_q[T]$ we denote by $|X|$ its norm: $|X| = q^{\deg X}$.

Define "an interval" $I$ as the set of polynomials on a formal variable $T$ of the form $X(T) + Y(T)$, where $X(T)$ is a fixed polynomial and $Y(T)$ runs through all polynomials of degree less or equal than a given integer.

In what follows $C$ is an irreducible algebraic curve of degree $d$ over $\mathbb{F}_q[T]$, which is described by $F(X,Y) = 0$, $F(X,Y) \in (\mathbb{F}_q[T])[X,Y]$. Write $S$ for the set of points on $C$ inside $I^2$.

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 a polynomial $F$ 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 $W$ be a set consisting of finitely many linearly independent polynomials $F \in (\mathbb{F}_q[T])[X,Y]$ including the constant polynomial $1$. Write $d_W$ for the total degree of all elements of $W$. Assume that the elements of $W$ separate, meaning that $\forall (X_1,Y_1), (X_2,Y_2) \in (\mathbb{F}_q[T])^2$ there is an $F \in W$ such that $F(X_1,Y_1) \neq F(X_2,Y_2)$. We define a $W$-curve to be an affine algebraic curve described by an equation $G(X,Y) = 0$, where all the monomials of $G$ belong to $W$.

During the proof of Theorem 1 we will use the following choice of $W$:

**Example 1** Define $W = W_{d,M}$ as

$$W = \{X^iY^j\mid i \leq d, j \leq M\},$$

where $d$ and $M$ are given numbers. Then $|W| = (d+1)(M+1)$, $d_W = (d+1)(M+1)^{d+M+1}$. The $W$-curves are plane curves of degree less or equal than $d$ and $M$ in $X$ and $Y$ respectively.

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

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

$$|S| \ll_W |I|^{\frac{2\alpha d}{\log q} + \alpha + O(C)}$$

where $\omega = |W|$.

**Proof.** We are going to prove it 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 $F_1,F_2,\ldots,F_\omega$ for the elements of $W$, we define a function

$$W : (\mathbb{F}_q[T])^2^\omega \rightarrow \mathbb{F}_q[T]$$

by

$$W(P_1,\ldots,P_\omega) = \det(F_i(P_j))_{1 \leq i,j \leq \omega}.$$  

Let $P$ denote an ensemble of points in $S$: $P = (P_1,\ldots,P_\omega)$, $P_i = (X_i,Y_i) \in S$. We say that $P$ is admissible if $W(P) = W(P_1,\ldots,P_\omega) \neq 0$ (where $0$ stands for zero polynomial in $\mathbb{F}_q[T]$). Define

$$\Delta = \prod_P |W(P)|,$$

where $*$ means that we take the operation over all admissible $P$.

By the definition of $d_W$ we have

$$|W(P)| \ll_W |I|^{d_W}$$

for every $P \in S^\omega$. Taking $\log \Delta$ and applying the expression above gives

$$\frac{\log \Delta}{|S|^\omega} = \sum_P \frac{\log |W(P)|}{|S|^\omega} \leq d_W \log |I| + O_W(1).$$

(2.1)
Fix any irreducible polynomial $f$ with $|f| \leq N$, where $N$ is to be set at the end. Then for every point $P \in (\mathbb{F}_q[T])^2$ let $\rho_P$ be the fraction of points in $S$ that reduce to $P \mod f$. For each $P$ let $\kappa(P) \in \{0, 1, \ldots, \omega - 1\}$ be defined in a way that $\omega - \kappa(P)$ is the number of distinct points among the points $P_i \mod f$. Then one can state

$$\text{ord}_f \Delta \geq \sum_{P}^* \kappa(P) = \sum_{P} \kappa(P) - \sum_{P} \kappa(P),$$

where the first sum on the right hand side is taken over all $P$ and the second one is the sum over all inadmissible ensembles $P$.

We are going to proceed in two steps. First, we will calculate the sum over all $P$ as a random variable with uniform distribution.

Then the expected value of the number of distinct points among the $P \mod f$ is equal to

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

Further,

$$\mathbb{E} \left( \sum_P Y_P \right) = \sum_P \mathbb{E}(Y_P) = \sum_P \mathbb{P}(\exists P_i | P_i \equiv P \mod f) = \sum_P (1 - \mathbb{P}(\forall P_i | P_i \equiv P \mod f))$$

$$= \sum_P (1 - \mathbb{P}(\forall P_i | P_i \not\equiv P \mod f)) = \sum_P \left( 1 - \prod_i \mathbb{P}(P_i \not\equiv P \mod f) \right) = \sum_P \left( 1 - \prod_i (1 - \rho_P) \right)$$

$$= \sum_P (1 - (1 - \rho_P)^\omega).$$

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

$$\det(F(P_i))_{1 \leq i, j \leq l} \neq 0$$

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

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

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

Further,

$$\mathbb{E} \left( \sum_P Y_P \right) = \sum_P \mathbb{E}(Y_P) = \sum_P \mathbb{P}(\exists P_i | P_i \equiv P \mod f) = \sum_P (1 - \mathbb{P}(\forall P_i | P_i \equiv P \mod f))$$

$$= \sum_P (1 - \mathbb{P}(\forall P_i | P_i \not\equiv P \mod f)) = \sum_P \left( 1 - \prod_i \mathbb{P}(P_i \not\equiv P \mod f) \right) = \sum_P \left( 1 - \prod_i (1 - \rho_P) \right)$$

$$= \sum_P (1 - (1 - \rho_P)^\omega).$$

We then have

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

Next

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

Since

$$(1 - \rho_P)^\omega + \omega \rho_P - 1 = 1 - \omega \rho_P + \left( \frac{\omega}{2} \right) \rho_P^2 + \ldots + (-1)^\omega \left( \frac{\omega}{\omega} \right) \rho_P^\omega + \omega \rho_P - 1 = \rho_P^\omega \left( \left( \frac{\omega}{2} \right) - o_{C, \omega}(1) \right),$$

then

$$\frac{\sum_P \kappa(P)}{|S|^\omega} = \frac{\omega (\omega - 1)}{2} \sum_P \rho_P^\omega - o_{C, \omega} \left( \sum_P \rho_P^\omega \right).$$

Now let us bound the sum over all inadmissible $P$. Consider the set of such $P$ with $\kappa(P) > 0$. Then one of the followings is true:
1. There exist $i$ and $j$, such that $P_i = P_j$;

2. There exist $i$ and $j$, such that $P_i \equiv P_j \pmod{f}$, but $P_i \neq P_j$.

The total number of inadmissible $P$, such that the first condition above holds is equal to $O(\lvert S \rvert^{\omega-1})$. Let us estimate this number for the second case. Permute the entries in such a way that $i = 1$, $j = 2$ and $F_1 = 1$, $F_2(P_1) \neq F_2(P_1)$ (this is possible since we have assumed that the elements of $W$ separate points and $W$ contains $1$). Then for $l = 2$

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

Choose the maximal $l$, such that the above statement still holds. Then $P_{l+1}$ lies on a $W$ curve determined by $P_1$, $P_2$, \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 $P$, such that the second case takes place is equal to

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

where $\delta$ is the number of pairs $(Q_1, Q_2) \in S^2$ that reduce to the same point mod $f$. By the definition of $\rho_P$ we have

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

Summing two results we see that there are at most

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

(2.4)

inadmissible $P$ with $\kappa(P) > 0$. Putting (2.3) and (2.4) into (2.2) we have

$$\frac{\text{ord}_f \Delta}{|S|^{\omega}} \geq \sum_P \frac{\kappa(P) - \sum_P \kappa(P)}{|S|^{\omega}} \geq \left(\frac{\omega(\omega - 1)}{2} - o_{C,\omega}(1)\right) \sum_P \rho_P^2 - O_\omega\left(|S|^{-1}\left(1 + \sum_P \rho_P^2\right)\right).$$

Using Cauchy’s inequality

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

one can state

$$\frac{\text{ord}_f \Delta}{|S|^{\omega}} \geq \left(\frac{\omega(\omega - 1)}{2} - o_{C,\omega}(1)\right) \frac{1}{\alpha|f|} - O_{\omega,\alpha,|f|}\left(|S|^{-1}\right).$$

Multiply the equation above by $\log |f|$ and sum over all $|f| \leq N$:

$$\sum_{|f| \leq N} \log |f| \left(\frac{\omega(\omega - 1)}{2} - o_{C,\omega}(1)\right) \frac{1}{\alpha|f|} + O_{\omega,\alpha} \left(|S|^{-1} \sum_{|f| \leq N} \log |f|\right) \leq \frac{\log \Delta}{|S|^{\omega}}.$$ (2.5)

As we know from (2.1)

$$\frac{\log \Delta}{|S|^{\omega}} \leq d_W \log |f| + O_W(1).$$

Applying this estimate to (2.5) gives

$$\frac{\omega(\omega - 1)}{2\alpha} \sum_{|f| \leq N} \frac{\log |f|}{|f|} + O_{\omega,\alpha} \left(|S|^{-1} \sum_{|f| \leq N} \log |f|\right) - o_{C,\omega,\alpha} \left(\sum_{|f| \leq N} \frac{\log |f|}{|f|}\right) \leq d_W \log |f| + O_W(1).$$

Taking $N = |S|$ we end with

$$|S| \ll_{\omega, W} \left|f\right|^{\frac{2d_W}{2\omega}} + o_{\omega, C}(1).$$

$\square$
Lemma 2 Let $C$ be an irreducible algebraic curve of degree $d$ over $\mathbb{F}_q[T]$ which is defined by $F(X, Y) = 0$. There exists a linear transformation $$(X, Y) \rightarrow (X', Y')$$ such that $\deg_X F(X', Y') = d$.

**Proof.** We can assume $\deg_X F(X, Y) < d$, otherwise we are done. Any polynomial of the form $F(X, Y) \in (\mathbb{F}_q[T])[X, Y]$ can be written as $$F(X, Y) = \sum_{i \in J_1, j \in J_2} F_{ij} X^i Y^j,$$ where $J_1, J_2 \subset \{0, 1, \ldots, d\}$, $F_{ij} \in \mathbb{F}_q$ and $$\max_{i \in J_1} (i + j) = \deg F = d, \quad \max_{i \in J_1} i = \deg_X F < d.$$ Consider a linear transformation $$(X, Y) \rightarrow (X', Y')$$ such that $(X, Y) = (AX' + BY', CX' + DY')$, where $A, B, C, D \in \mathbb{F}_q[T]$ with $AD - BC \neq 0$. Changing the variables $(X, Y) \rightarrow (X', Y')$ we obtain $$F(X, Y) = \sum_{i \in J_1, j \in J_2} F_{ij} (AX' + BY')^i (CX' + DY')^j.$$ In new variables $(X', Y')$ we have $$\deg_{X'} F = \max_{i \in J_1, j \in J_2} (i + j),$$ which is equal to $d$, since $\max_{i \in J_1, j \in J_2} (i + j) = \deg F = d$. \hfill \Box

3 Proof of the theorem

We start with an interpolation argument, which is used for a similar goal in [5]. Let again $F \in (\mathbb{F}_q[T])[X, Y]$ be written in a form $$F(X, Y) = \sum_{i \in J_1, j \in J_2} F_{ij} X^i Y^j,$$ where $J_1, J_2 \subset \{0, 1, \ldots, d\}$, $F_{ij} \in \mathbb{F}_q$. We are counting the number of distinct lattice points $P = (X, Y) \in I^2 \cap C$. If we have less than $r(d) = d^2 + 1$ such points, then we are done. Suppose that we have at least $r(d)$ points: $P_i = (X_i, Y_i) \in C \cap F^1, i = 1, \ldots, r(d)$ with $F(P_i) = 0$. Denote by $n(d) = \frac{1}{2}(d + 1)(d + 2)$ the number of monomials of degree less or equal than $d$. Consider $n(d) \times r(d)$ matrix $A$, whose $i$-th row consists of the monomials of degree $d$ in the variables $X_i, Y_i$. Let $\vec{b} \in \mathbb{F}_q^{n(d)}$ be a vector, whose entries are the corresponding coefficients $F_{ij}$ of $F(X, Y)$. For such a vector $\vec{b}$ we have an equation $$A \vec{b} = \vec{0}.$$ Since $\vec{b} \neq \vec{0}$, then the matrix $A$ has a rank less than or equal to $n(d) - 1$. Thus there is a solution $\vec{g} \neq \vec{0}$, where $\vec{g}$ is constructed out of the minors of $A$ with $|\vec{g}| \ll_d |I|^{dn(d)}$. 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 (points $P_i$).

By Bézout’s theorem it is possible only if $G$ is a multiple of $F$. Since $F$ is irreducible, then $G$ is also irreducible and defines the same curve $C$. Let us work with $G$ instead of $F$.

We are going to 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 proceed to the next step.

2. Using Weil bounds we obtain
\[
| \{(X, Y) \in (\mathbb{F}_q[T])^2 : G(X, Y) = 0 \mod f \}| = |f| + O_d(\sqrt{|f|}).
\]

Further, for every \( \varepsilon > 0 \) and for every irreducible polynomial \( f \in \mathbb{F}_q[T] \) with the condition \( |f| \geq c(\varepsilon) \) the set \( S \) intersects at most \( (1 + \frac{\varepsilon}{2}) |f| \) residue classes \( \mod f \) (here \( c(\varepsilon) \) is a constant that depends only on \( \varepsilon \)). Applying Lemma 1 with \( \alpha = 1 + \frac{\varepsilon}{2} \) and \( \mathcal{W} \) from Example 1 we obtain
\[
|S| \ll_{\varepsilon, \mathcal{W}} |I|^{\frac{1}{2} \left(1+\frac{\varepsilon}{2}\right) + o_{\varepsilon, c}(1)} + o_{\varepsilon, c}(1).
\]

We choose \( M \) to be large enough and end with
\[
|S| \ll_{\varepsilon, \mathcal{W}} |I|^{\frac{1}{2} + \frac{2\varepsilon}{3} + o_{\varepsilon, c}(1)}.
\]

4 An application to counting elliptic curves

In this section we are going to proceed with counting the number of elliptic curves \( E_{a,b} \) with coefficients \( a, b \) in a small box that lie in the same isomorphic classes. This is basically the generalization of several statements presented in [3]. Doing this we have an opportunity to apply Theorem 1 and also to show that some results for number fields can be also 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 a fixed polynomial and \( Y(T) \in \mathbb{F}_q[T] \) runs through all polynomials of degree less or equal than \( d \). The coefficients of \( X \) and \( Y \) belong to \( \mathbb{F}_q \) just as in section 2.

For a prime power \( q \) we consider a family of elliptic curves \( E_{a,b} \)
\[ E_{a,b} : Y^2 = X^3 + aX + b, \]
where \( X \) and \( Y \) belong to \( \mathbb{F}_q[T] \) as before and \( a, b \) are some coefficients from \( \mathbb{F}_q[T] \) with the property that \( 4a^3 + 27b^2 \neq 0 \). As in the number field case we say that two curves \( E_{a,b} \) and \( E_{c,d} \) are isomorphic if
\[ at^4 \equiv c(\mod f) \quad \text{and} \quad bt^6 \equiv d \ (\mod f). \]

The existence of an isomorphism between \( E_{a,b} \) and \( E_{c,d} \) implies that
\[ a^3d^2 \equiv b^3c^2 \ (\mod f) \quad (4.1) \]
for some \( f \in \mathbb{F}_q[T] \). We denote by \( N(I^2) \) the number of solutions to (4.1) with \( (a, b), (c, d) \in I^2 \). Then for \( \lambda \in \mathbb{F}_q[T] \) we write \( N_\lambda(I^2) \) for the number of solutions to the congruence
\[ a^3 \equiv \lambda b^2 \ (\mod f), \quad (a, b) \in I^2. \]

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

For a polynomial \( X \in \mathbb{F}_q[T] \) and an irreducible polynomial \( f \in \mathbb{F}_q[T] \) we use \( \{X\}_f \) to denote
\[ \{X\}_f = \min_{Y \in \mathbb{F}_q[T]} |X - fY| = \min_{Y \in \mathbb{F}_q[T]} q^{\deg(X-Y)}. \]

From Dirichlet pigeon-hole principle we obtain

**Lemma 3** For real numbers \( T_1, \ldots, T_s \) with \( 1 \leq T_1, \ldots, T_s \leq |f|, T_1 \cdots T_s \geq |f|^{s-1} \) and any polynomials \( X_1, \ldots, X_s \in \mathbb{F}_q[T] \) there exists a polynomial \( t \in \mathbb{F}_q[T] \) such that \( t \) is not a multiple of \( f \) and
\[ \{X_i t\}_f \ll T_i, \quad i = 1, \ldots, s. \]

Now we can give a good bound for \( N_\lambda(I^2) \):
Theorem 2 Let I be an interval of polynomials of degree less or equal than d with coefficients in \( \mathbb{F}_q \) and the length of I is \( |I| = q^d \). For any irreducible polynomial \( f \in \mathbb{F}_q[T] \) such that \( 1 \leq |I| \leq |f|^{\frac{1}{2}} \) and for any \( \lambda \in \mathbb{F}_q[T] \) we have

\[ N_\lambda(I^2) \leq |I|^{\frac{1}{2}+o(1)}. \]

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

\[ X^3 + 3X^2X_0 + 3X_0^2X_0 - \lambda Y^2 - 2\lambda X_0 Y \equiv \lambda X_0^3 - X_0^3 \pmod{f}. \] (4.2)

For any \( T \leq q^{\frac{1}{2}}/|I|^{\frac{1}{2}} \) we can apply Lemma 3 to

\[ X_1 = 1, \ X_2 = 3X_0, \ X_3 = 3X_0^2, \ X_4 = -\lambda, \ X_5 = -2\lambda X_0 \]

and

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

and find that there exists \( t \) with \( |t| \leq T^4|I|^2 \) such that

\[ \{3X_0t\}_f \leq \frac{|f|}{T|I|}, \ \{3X_0^2t\}_f \leq \frac{|f|}{T}, \ \{\lambda t\}_f \leq \frac{q}{T|I|}, \ \{2\lambda X_0 t\}_f \leq \frac{|f|}{T}. \]

For \( i = 1, \ldots, 5 \) denote by \( f_i \) a polynomial which satisfies \( f_i = X_i t \). Then multiply (4.2) by \( t \) leads us to the equality

\[ f_1X^3 + f_2X^2 + f_3X + f_4Y^2 + f_5Y + f_6 = |f|Z, \] (4.3)

where

\[ |f_1| \leq T^4|I|^2, \ |f_2|, |f_4| \leq \frac{|f|}{T|I|}, \ |f_3|, |f_5| \leq \frac{|f|}{T}, \ |f_6| \leq \frac{|f|}{2}. \]

Since for \( X, Y \in I \) we have \( |X|, |Y| \leq |I| \), then the left hand side of (4.3) is bounded above by \( T^4|I|^5 + \frac{4|I||I|^3}{|I|^2} + \frac{|I|^3}{2}. \) Thus

\[ |Z| \ll \frac{T^4|I|^5}{|f|} + \frac{4|I|^3}{|f|} + 1. \]

Choosing \( T \approx \frac{|f|^{\frac{1}{2}}}{|I|^{\frac{1}{2}}} \) and applying the condition \( 1 \leq |I| \leq |f|^{\frac{1}{2}} \) we end with the bound

\[ |Z| \ll \frac{|f|^{\frac{1}{2}}}{q^{\frac{1}{2}}} + 1 \ll 1. \]

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

References

[1] E. Bombieri, J. Pila, The number of integral points on arcs and ovals, Duke Mathematical Journal 59 (1989), 2, 337–357.

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

[3] J. Cilleruelo, I. Shparlinski, A. Zumalácarregui, Isomorphism classes of elliptic curves over a finite field in some thin families, Math. Res. Lett. 19 (2012), 2, 1–9.
[4] J. Cilleruelo, I. Shparlinski, *Concentration of points on curves in finite fields*, Monatsh Math (2013), 171, 315–327.

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

[6] D.R. Heath-Brown, *The Density of rational points on curves and surfaces*, Ann. of Math. (2), Vol. 155 (2002), no. 2, 553–598.

[7] H.A. Helfgott, A. Venkatesh, *How small must ill-distributed sets be?*, Analytic number theory. Essays in honour of Klaus Roth. Cambridge University Press 2009, 224–234.