Arnold Mathematical Journal (2019) 5:105–121
https://doi.org/10.1007/s40598-019-00112-z

RESEARCH CONTRIBUTION

Solutions of Polynomial Equations in Subgroups of $\mathbb{F}_p^*$

Sergei Makarychev[1] · **Ilya Vyugin**[2]

Received: 4 December 2018 / Revised: 16 April 2019 / Accepted: 20 May 2019 / Published online: 5 June 2019
© Institute for Mathematical Sciences (IMS), Stony Brook University, NY 2019

Abstract
We present an upper bound on the number of solutions of an algebraic equation $P(x, y) = 0$ where x and y belong to the union of cosets of some subgroup of the multiplicative group κ^* of some field of positive characteristic. This bound generalizes the bound of Corvaja and Zannier (J Eur Math Soc 15(5):1927–1942, 2013) to the case of union of cosets. We also obtain the upper bounds on the generalization of additive energy.

Keywords Polynomial · Algebraic equation · Field of positive characteristic · Subgroup

1 Introduction

1.1 Background

Let κ be a field of characteristic p, $\overline{\kappa}$ be its algebraic closure, κ^* be the multiplicative group of κ, and G be a subgroup of multiplicative group κ^*. For example $\kappa = \mathbb{F}_p$.

Garcia and Voloch constructed estimates on the number of solutions of the linear equations on subgroups. They considered the equation

---

Dedicated to the 70th anniversary of Rafail Kalmanovich Gordin.

The work of I.V. Vyugin is supported by the Russian Science Foundation grant RSF 19-11-00001 and performed in Steklov Mathematical Institute of Russian Academy of Sciences.

✉ Ilya Vyugin
vyugin@gmail.com

Sergei Makarychev
svmakarychev@yandex.ru

1 Skolkovo Institute of Science and Technology, National Research University Higher School of Economics, Moscow, Russia

2 Institute for Information Transmission Problems RAS, National Research University Higher School of Economics, Steklov Mathematical Institute RAS, Moscow, Russia

$$y = x + \mu, \quad \mu \neq 0. \tag{1}$$

They proved that for an arbitrary subgroup $G \in \mathbb{F}_p^*$, such that

$$|G| < (p-1)/((p-1)^{1/4}+1),$$

the number of solutions $(x, y) \in G \times G$ of the Eq. (1) is less than or equal to $4|G|^{2/3}$.

Heath-Brown and Konyagin (see Heath-Brown and Konyagin 2000; Stepanov 1969) generalized the Garcia–Voloch result using Stepanov method. They have obtained that the number of solutions $(x, y) \in \cup_{i=1}^{h} G_i^1 \times G_i^2$ of the Eq. (1) is less than or equal to $C(h|G|)^{2/3}$, where $|G| < (p-1)/((p-1)^{1/4}+1)$, $G_i^1 = g_i' G$, $G_i^2 = g_i'' G$ are cosets of G, such that $G_i^k \neq G_j^k$ if $i \neq j$, $i = 1, \ldots, h$, $k = 1, 2$, C is a constant. The case of systems of linear equations has been studied in Vyugin and Shkredov (2012) and Shkredov et al. (2015).

The Garcia–Voloch result has been generalized to the case of algebraic curves by Corvaja and Zannier (2013).

Theorem 1 (Corvaja and Zannier) *Let X be a smooth projective absolutely irreducible curve over a field κ of characteristic p. Let $u, v \in \kappa(X)$ be rational functions, multiplicatively independent modulo κ^*, and with non-zero differentials; let S be the set of their zeros and poles; and let $\chi = |S| + 2g - 2$ be the Euler characteristic of $X \backslash S$. Then*

$$\sum_{\nu \in X(\overline{\kappa}) \backslash S} \min\{\nu(1-u), \nu(1-v)\} \leqslant \left(3\sqrt[3]{2}(\deg u \deg v \chi)^{1/3}, 12\frac{\deg u \deg v}{p}\right), \tag{2}$$

where $\nu(f)$ denotes the multiplicity of the vanishing of f at the point ν.

It follows from Corollary 2 of Corvaja and Zannier (2013) that

$$\#\{(x, y) \mid (x, y) \in X, x, y \in G\} \leqslant \max\left(3\sqrt[3]{2}\chi^{1/3}|G|^{2/3}, 12\frac{|G|^2}{p}\right).$$

The estimates on the number of solutions of polynomial equations have found wide applications in related areas of mathematics. In particular, some specific case of the theory that was developed by the authors of this article, recently has been applied to improve the bounds of Bourgain et al. (2016) on the possible number of nodes outside the "giant component" and on the size of individual connected components in the suitably defined functional graph of Markoff triples modulo p. The results can be found in the joint work of Konyagin et al. "On the new bound for the number of solutions of polynomial equations in subgroups and the structure of graphs of Markoff triples" (see Konyagin et al. 2017).

1.2 Notation

Let us consider an algebraic equation

$$P(x, y) = 0, \quad P \in \overline{\kappa}[x, y], \tag{3}$$

where

$$P(x, y) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x^i y^j. \tag{4}$$

Let us introduce the set of polynomials $\mathcal{P}$:

$$\mathcal{P} = \{P_{q',q''}(x, y) \mid P_{q',q''} = P(q'x, q''y),\ q', q'' \in \kappa^*\}$$

and the subset

$$P_k(x, y) = P(q'_k x, q''_k y), \quad k = 1, \dots, h.$$

We call these polynomials G-independent if for any integers $1 \leqslant i < j \leqslant h$ ratios q'_i/q'_j and q''_i/q''_j do not belong to G simultaneously.

Let us put by definition

$$\mathcal{N}_h = \bigcup_{k=1}^{h} \{(x, y) \in G \times G \mid P_k(x, y) = 0\}. \tag{5}$$

In other words, $\mathcal{N}_h$ is the set of solutions $(x, y) \in \bigcup_{k=1}^{h} G_k^1 \times G_k^2$ of the Eq. (3), where $G_k^1 = q'_k G$, $G_k^2 = q''_k G$.

Denote by g the greatest common divisor of the following set of differences:

$$g = g(P) = \gcd\{j_1 - j_2 \mid \exists i_1, i_2 \,:\, a_{i_1 j_1} a_{i_2 j_2} \neq 0\}. \tag{6}$$

It is obvious, that $g \leqslant n$.

2 Results

Theorem 2 *Consider the following assumptions:*

- $P(x, y) \in \overline{\mathbb{F}}_p[x, y]$ *is an irreducible polynomial* (4) *having bidegree* (m, n) *such that* $P(0, 0) \neq 0$ *and* $\deg_x P(x, 0) \geqslant 1$, $n \geqslant 1$;
- *polynomials* $P_1, \dots, P_h \in \mathcal{P}$ *are* G*-independent;*
- G *is a subgroup of* $\mathbb{F}_p^*$ *such that* $10^3 < |G| < \frac{1}{3} p^{3/4} h^{-1/4}$, *where* $h < (40mn^2)^{-3} |G|^2$.

Then the following bound

$$\#\mathcal{N}_h \leqslant 12mng(m+n)h^{2/3}|G|^{2/3} \tag{7}$$

holds.

Let A, B be subsets of the field $\mathbb{F}_p$. The *additive energy* is defined by

$$E(A, B) = \#\{(x_1, y_1, x_2, y_2) \in (A \times B)^2 \mid x_1 + y_1 = x_2 + y_2\},$$

and we denote $E(A, A)$ by $E(A)$. The additive energy plays an important role in many problems of additive combinatorics as well as in number theory (see Tao and Vu 2006; Schoen and Shkredov 2013).

We introduce some generalizations of the additive energy which we call the *polynomial energy*. Let $P(x, y)$ be a polynomial and q be a positive integer. We define two types of *polynomial q-energy* $E_P^q(A)$ with respect to polynomial P by

$$E_P^q(A) = \#\{(x_1, y_1, \dots, x_q, y_q) \in A^{2q} \mid P(x_1, y_1) = \dots = P(x_q, y_q)\}$$

and by

$$\hat{E}_P^q(A) = \#\{(x_1, y_1, \dots, x_q, y_q) \in A^{2q} \mid P(x_1, y_1) = \dots = P(x_q, y_q) \neq 0\}.$$

We will consider polynomials $P(x, y)$ of bidegree (m, n) such that $\deg P(x, 0) \geqslant 1$.

Theorem 3 *Suppose that the polynomial* $P(x, y) \in \overline{\mathbb{F}}_p[x, y]$ *is homogeneous of degree* n, $\deg P(x, 0) \neq 0$, $\deg_y P(x, y) \geqslant 1$ *and the polynomial* $f(x, y) = P(x, y) - 1$ *is irreducible over* $\overline{\mathbb{F}}_p$. *Let* G *be a subgroup of* $\mathbb{F}_p^*$ *such that* $10^3 < |G| < \frac{1}{3}p^{1/2}$. *Then the following holds:*
if $q = 2$, *then*

$$\hat{E}_P^2(G) \leqslant 10^3 n^8 |G|^{5/2};$$

if $q = 3$, *then*

$$\hat{E}_P^3(G) \leqslant 17^3 n^{12}(n)|G|^3 \ln |G|;$$

if $q \geqslant 4$, *then*

$$\hat{E}_P^q(G) \leqslant 17^q 3n^{4q}|G|^{1+\frac{2q}{3}},$$

and for all q *holds*

$$E_P^q(G) \leqslant \hat{E}_P^q(G) + |G|^q n^q.$$

3 Stepanov's Method with Polynomials of Two Variables

Let us consider a polynomial $\Phi \in \overline{\kappa}[x, y, z]$ such that

$$\deg_x \Phi(x, y, z) < A, \quad \deg_y \Phi(x, y, z) < B, \quad \deg_z \Phi(x, y, z) < C,$$

or in other words

$$\Phi(x, y, z) = \sum_{a,b,c} \lambda_{a,b,c} x^a y^b z^c, \quad a \in \mathbf{A}, \quad b \in \mathbf{B}, \quad c \in \mathbf{C}, \quad \lambda_{a,b,c} \in \overline{\mathbb{F}}_p \tag{8}$$

$$\mathbf{A} = \{0, \ldots, A-1\}, \quad \mathbf{B} = \{0, \ldots, B-1\}, \quad \mathbf{C} = \{0, \ldots, C-1\}. \tag{9}$$

Consider the following polynomial

$$\Psi(x, y) = \Phi(x, x^t, y^t). \tag{10}$$

Then let us require that the polynomial Ψ, defined by (10) satisfies the following conditions:

1. all pairs $(x, y) \in \mathcal{N}_h \backslash \mathcal{N}_{sing}$ are zeros of order at least D of the function $\Psi(x, y)$ on the curve $P(x, y) = 0$.
2. the polynomials $\Psi(x, y)$ and $P(x, y)$ are relatively prime.

Let us define coefficients $\lambda_{a,b,c}$ such that the elements of the set

$$\mathcal{N}_h' = \mathcal{N}_h \backslash \mathcal{N}_{sing}, \quad \mathcal{N}_{sing} = \left\{(x, y) \mid P(x, y) = 0 \wedge \left(x = 0 \vee y = 0 \vee \frac{\partial P}{\partial y}(x, y) = 0\right)\right\}$$

be zeros of the system

$$\begin{cases} \Psi(x, y) = 0 \\ P(x, y) = 0 \end{cases} \tag{11}$$

of orders at least D. Lemma 5 gives us the bound

$$\mathcal{N}_{sing} \leqslant (m+n)^2.$$

If polynomials $\Psi(x, y)$ and $P(x, y)$ are relatively prime, then the generalized Bézout theorem (see Shafarevich 2013, Chapter 4, §2.1) gives us the upper bound (12) for $\#\mathcal{N}_h$. An upper bound for D is given by the number of coefficients $\lambda_{a,b,c}$. The main difficulty in the application of Stepanov's method is proving that the polynomials $\Psi(x, y)$ and $P(x, y)$ are relatively prime. We prove that the polynomial (10) is nonzero using Lemmas 1 and 3.

If these conditions are satisfied, then the generalized Bézout's theorem gives us an upper bound of the number $\#\mathcal{N}_h$:

$$\begin{aligned}\#\mathcal{N}_h &\leqslant \#\mathcal{N}_{sing} + \frac{\deg \Psi(x, y) \cdot \deg P(x, y)}{D} \\ &\leqslant (m+n)^2 + \frac{(A-1+(B-1)t+(C-1)t)(m+n)}{D}.\end{aligned} \tag{12}$$

A pair (x, y) is a root of $\Psi(x, y)$ order at least D on the curve $P(x, y) = 0$, if $P(x, y) = 0$ and $\Psi(x, y) = 0$ and if the derivatives

$$\frac{d^k}{dx^k}\Psi(x, y) = 0, \quad k = 1, \dots, D-1$$

vanish on the curve $P(x, y) = 0$ (see 4.1).

Let us apply the Lemma 3 to test the second condition. If $P(x, y)$ is irreducible, then $P(x, y)$ and $\Psi(x, y)$ are relatively prime if $P(x, y) \nmid \Psi(x, y)$.

4 Lemmas

Lemma 1 *Let $Q(x, y) \in \overline{\kappa}[x, y]$ be a polynomial and let*

$$P(x, y) = f_n(x)y^n + \cdots + f_1(x)y + f_0(x),$$

be an irreducible polynomial of bidegree (m, n). If $P(x, y) \mid Q(x, y^t)$ and $t = |G| < p$ is the order of subgroup $G \subset \kappa^*$, then $P(x, 0)^{[t/g]} \mid Q(x, 0)$,[1] *where g defined in* (6).

Proof We have $P(x, y) \mid Q(x, y^t)$ by assumption. Let us substitute $y = q\tilde{y}$ in the polynomial $P(x, y) \longmapsto P_q(x, \tilde{y}) = P(x, q\tilde{y})$, where $q \in G$. Actually,

$$P_q(x, y) \mid Q(x, y^t),$$

because $q^t = 1$ and $P_q(x, y) \mid Q(x, (qy)^t) = Q(x, y^t)$. For any $q \in G$ polynomials $P_q(x, y)$ are irreducible, because $P(x, y)$ is irreducible by assumption. The leading coefficient of the polynomial $P_q(x, y)$ is $f_n(x)q^n$. There exist at least $[t/n]$ elements $q_1, \dots, q_{[t/g]} \in G$ such that $q_1^n, \dots, q_{[t/g]}^n$ are pairwise distinct. Note that the following polynomials

$$P_{q_1}(x, 0) = \cdots = P_{q_{[t/g]}}(x, 0) = f_0(x)$$

are the same and $f_0(x) \not\equiv 0$ (if $f_0(x) \equiv 0$, then $y \mid P(x, y)$), but the leading terms $f_n(x)q^{gn}y^n$ of polynomials $P_q(x, y)$, $q = q_1, \dots, q_{[t/g]}$ are distinct. Consequently, the polynomials $P_{q_1}(x, y), \dots, P_{q_{[t/g]}}(x, y)$ are distinct. These polynomials are relatively prime, because they are distinct and irreducible. Further, we have

$$(P_{q_1}(x, y) \cdot \cdots \cdot P_{q_{[t/g]}}(x, y)) \mid Q(x, y^t),$$

[1] $[x]$—the integer part of x.

and

$$(P_{q_1}(x,0)\cdot\dots\cdot P_{q_{[t/g]}}(x,0)) \mid Q(x,0).$$

Note that $P(x,0) = P_q(x,0)$ for any $q \in G$ and we obtain the statement of the Lemma

$$P(x,0)^{[t/g]} \mid Q(x,0).$$

□

We present Lemma 6 of Heath-Brown and Konyagin (2000) with minimal corrections (in Heath-Brown and Konyagin (2000) polynomial $f(x)$ belongs to $\mathbb{F}_p[x]$).

Lemma 2 *Let $f(x) \in \overline{\kappa}[x]$ be a sum of $N \geqslant 1$ distinct monomials. Suppose further that* $\deg f(x) < p$. *Then $(x-\alpha)^N$, $\alpha \in \overline{\kappa}^*$ cannot divide $f(x)$.*

Proof Let us consider an arbitrary polynomial $g(x)$ in the following form

$$g(x) = \sum_{j=1}^{s} C_j x^{i_j}, \quad i_1 > \dots > i_s.$$

Let us define the operator $D : \overline{\kappa}[x] \to \overline{\kappa}[x]$ such that

$$Dg(x) = \frac{d}{dx}\left(\frac{g(x)}{x^{i_s}}\right).$$

The operator D satisfies to the following conditions:

1. D maps polynomials with s monomials to polynomials with $s-1$ monomials;
2. if $\alpha \neq 0$ is a root of $g(x)$ of order l, then α is a root of $Dg(x)$ of order $l-1$.
   Let us apply the operator D^{N-1} to the polynomial $f(x)$. The polynomial $D^{N-1}f(x)$ is a monomial, consequently, it has the only zero root. Hence we obtain that the order of root α is less than or equal to $N-1$.

□

Lemma 3 *Let*

$$\Psi(x,y) = \sum_{a,b,c} \lambda_{a,b,c} x^a x^{bt} y^{ct}, \quad a \in \mathbf{A}, \quad b \in \mathbf{B}, \quad c \in \mathbf{C}$$

be a polynomial such that $nAB \leqslant t$, coefficients $\lambda_{a,b,c} \in \overline{\kappa}$ do not vanish simultaneously, $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *are sets defined at (9). Further, let $P \in \overline{\kappa}[x,y]$ be an irreducible polynomial and assume that* $\deg_y P(x,y) = n \geqslant 1$, $P(0,0) \neq 0$. *Then $P(x,y)$ does not divide $\Psi(x,y)$.*

Proof Put $c_{min} = \min\{c \in \mathbf{C} \mid \exists a, b : \lambda_{a,b,c} \neq 0, \ a \in \mathbf{A}, \ b \in \mathbf{B}\}$ (such c exists because all $\lambda_{a,b,c}$ do not vanish simultaneously). Let us represent the polynomial $\Psi(x, y)$ in the form

$$\Psi(x, y) = y^{c_{min}t}\tilde{\Psi}(x, y).$$

Now, let us rewrite the polynomial $\tilde{\Psi}(x, y)$ in the form

$$\tilde{\Psi}(x, y) = \sum_{a,b,c: c>c_{min}} \lambda_{a,b,c} x^a x^{bt} y^{(c-c_{min})t} + \sum_{a,b} \lambda_{a,b,c_{min}} x^a x^{bt}, \\ a \in \mathbf{A}, \quad b \in \mathbf{B}, \quad c \in \mathbf{C}. \tag{13}$$

So, if $P(x, y) \mid \Psi(x, y)$, then $P(x, y) \mid \tilde{\Psi}(x, y)$. By Lemma 1 with $Q(x, y^t) = \tilde{\Psi}(x, y)$ we obtain

$$P(x, 0)^{[t/n]} \mid \tilde{\Psi}(x, 0). \tag{14}$$

$\tilde{\Psi}(x, 0)$ is a nonzero polynomial, because coefficients $\lambda_{a,b,c_{min}}$, $a \in \mathbf{A}$, $b \in \mathbf{B}$ in (13) do not vanish simultaneously. Consider the roots $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{F}}_p$ of polynomial $P(x, 0)$, $k = \deg P(x, 0)$. Then $\prod_{i=1}^{k} \alpha_i = P(0, 0) \neq 0$, and consequently $\alpha_i \neq 0$, $i = 1, \ldots, k$. If (14) holds, then

$$(x - \alpha_1)^{[t/n]} \mid \tilde{\Psi}(x, 0).$$

Now we use Lemma 2. But since the number of nonzero terms of polynomial $\tilde{\Psi}(x, 0)$ is less than or equal to t/n ($t \geqslant nAB$), Lemma 2 gives us that

$$(x - \alpha_1)^{[t/n]} \nmid \tilde{\Psi}(x, 0),$$

a contradiction. $\square$

Lemma 4 *Let $Q \in \overline{\kappa}[x, y]$ be a polynomial such that*

$$\deg_x Q(x, y) \leqslant \mu, \quad \deg_y Q(x, y) \leqslant \nu \tag{15}$$

and $P \in \overline{\kappa}[x, y]$ be a polynomial such that

$$\deg_x P(x, y) \leqslant m, \quad \deg_y P(x, y) \leqslant n. \tag{16}$$

Then the condition

$$P(x, y) \mid Q(x, y) \tag{17}$$

can be given by $n((\nu - n + 2)m + \mu)$ homogeneous linear equations on coefficients of the polynomial $Q(x, y)$.

Proof The dimension of the vector space $\mathcal{L}$ of polynomials $Q(x, y)$ that satisfy (16) is equal to $(\mu+1)(\nu+1)$. Let us call the vector subspace of polynomials $Q(x, y)$ that satisfy (15) and (17) by $\mathcal{L}'$. As well as $Q(x, y) = P(x, y)R(x, y)$ where polynomial $R(x, y)$ such that

$$\deg_X R(X, Y) \le \mu - m, \quad \deg_Y R(X, Y) \le \nu - n,$$

than the vector space $\mathcal{L}'$ isomorphic to the vector space of polynomials $R(x, y)$. The dimension of the vector space $\mathcal{L}'$ is equal to $(\mu - m + 1)(\nu - n + 1)$. It means that the subspace $\mathcal{L}'$ of the space $\mathcal{L}$ is given by a system of

$$(\mu+1)(\nu+1) - (\mu - m + 1)(\nu - n + 1) = \mu n + \nu m - mn + m + n + 1 \le \\ \le (\mu + \nu + 1)mn$$

homogeneous linear equations. □

4.1 Orders of Roots of the Polynomial $\Psi(x, y)$ on a Curve $P(x, y) = 0$

In this section we present bounds on the number of equations that we have to set for existence of a polynomial $\Psi(x, y)$ such that all points of set M_1 without maybe $(m+n)^2$ points would be roots of $\Psi(x, y)$ of orders at least D on a given curve $P(x, y) = 0$.

Let us find an inductive formula for the derivatives $\frac{d^k}{dx^k} y$ of the function $y(x)$ defined by $P(x, y) = 0$. Consider the polynomials $q_k(x, y)$ and $r_k(x, y)$, $k \in \mathbb{N}$, which are defined inductively as

$$q_1(x, y) = -\frac{\partial}{\partial x} P(x, y), \quad r_1(x, y) = \frac{\partial}{\partial y} P(x, y),$$

and

$$\begin{aligned} q_{k+1}(x, y) &= \frac{\partial q_k}{\partial x}\left(\frac{\partial P}{\partial y}\right)^2 - \frac{\partial q_k}{\partial y}\frac{\partial P}{\partial x}\frac{\partial P}{\partial y} - (2k-1)q_k(x, y)\frac{\partial^2 P}{\partial x \partial y}\frac{\partial P}{\partial y} \\ &\quad +(2k-1)q_k(x, y)\frac{\partial^2 P}{\partial y^2}\frac{\partial P}{\partial x}, \\ r_{k+1}(x, y) &= r_k(x, y)\left(\frac{\partial P}{\partial y}\right)^2 = \left(\frac{\partial P}{\partial y}\right)^{2k+1}. \end{aligned}$$

Then $\frac{d^k}{dx^k} y = \frac{q_k(x,y)}{r_k(x,y)}$, $k \in \mathbb{N}$. Indeed, by the implicit function theorem we have

$$\frac{d}{dx} y = -\frac{\frac{\partial}{\partial x} P(x, y)}{\frac{\partial}{\partial y} P(x, y)} = \frac{q_1(x, y)}{r_1(x, y)}.$$

Then

$$\begin{aligned}
\frac{d^{k+1}}{dx^{k+1}}y &= \frac{d}{dx}\left(\frac{q_k(x,y)}{r_k(x,y)}\right)\\
&= \frac{\left(\frac{\partial q_k}{\partial x}+\frac{\partial q_k}{\partial y}\frac{d}{dx}y\right)r_k(x,y)-\left(\frac{\partial r_k}{\partial x}+\frac{\partial r_k}{\partial y}\frac{d}{dx}y\right)q_k(x,y)}{r_k(x,y)^2}\\
&= \frac{\left(\frac{\partial q_k}{\partial x}+\frac{\partial q_k}{\partial y}\frac{\frac{-\partial P}{\partial x}}{\frac{\partial P}{\partial y}}\right)\left(\frac{\partial P}{\partial y}\right)^{2k-1}-\left((2k-1)\left(\frac{\partial P}{\partial y}\right)^{2k-2}\frac{\partial^2 P}{\partial y\partial x}+(2k-1)\frac{\partial^2 P}{\partial y^2}\left(\frac{\partial P}{\partial y}\right)^{2k-2}\frac{\frac{-\partial P}{\partial x}}{\frac{\partial P}{\partial y}}\right)q_k(x,y)}{\left(\frac{\partial P}{\partial y}\right)^{2(2k-1)}}\\
&= \frac{\frac{\partial q_k}{\partial x}\left(\frac{\partial P}{\partial y}\right)^2-\frac{\partial q_k}{\partial y}\frac{\partial P}{\partial x}\frac{\partial P}{\partial y}-\left((2k-1)\left(\frac{\partial P}{\partial y}\right)\frac{\partial^2 P}{\partial y\partial x}-(2k-1)\frac{\partial^2 P}{\partial y^2}\frac{\partial P}{\partial x}\right)q_k(x,y)}{\left(\frac{\partial P}{\partial y}\right)^2\left(\frac{\partial P}{\partial y}\right)^{2k-1}} = \frac{q_{k+1}(x,y)}{r_{k+1}(x,y)}
\end{aligned}$$

The implicit function theorem gives us the derivatives $\frac{d^{k+1}}{dx^{k+1}}y$ in a point (x, y) on the algebraic curve (3) if the denominator $r_k(x, y)$ is not equal to zero. Otherwise $r_k(x, y) = 0$ if and only if the following system holds

$$\begin{cases} P(x,y)=0\\ \dfrac{\partial P}{\partial y}(x,y)=0. \end{cases} \tag{18}$$

If the polynomial $P(x, y)$ is irreducible, then the polynomials $P(x, y)$ and $\frac{\partial P}{\partial y}(x, y)$ are relatively prime. Thus Bézout's theorem gives us the bound $L \leqslant (m+n)(m+n-1)$, where L is the number of roots of the system (18) (see Shafarevich 2013, Chapter 4, §2.1).

Define the differential operators D_k on the algebraic curve (3). Let D_0 be identity operator and

$$D_k = \left(\frac{\partial P}{\partial y}\right)^{2k-1} x^k y^k \frac{d^k}{dx^k}, \quad k \in \mathbb{N}. \tag{19}$$

Let $\Psi(x, y)$ be the polynomial (10). Let us obtain the following relations

$$\begin{aligned}
D_k x^a x^{bt} y^{ct} &= R_{k,a,b,c}(x,y) x^a x^{bt} y^{ct},\\
D_k \Psi(x,y)|_{x\in q_l' G, y\in q_l'' G} &= R_{k,l}(x,y)|_{x\in q_l' G, y\in q_l'' G}, \quad l=1,\ldots,h
\end{aligned} \tag{20}$$

for some polynomials $R_{k,a,b,c}(x, y)$ and $R_{k,l}(x, y)$, $l = 1, \ldots, h$ using formulas of derivatives on the algebraic curve $P(x, y) = 0$.

Let us obtain the following lemma.

Lemma 5 *If $P(x, y) \mid \Psi(x, y)$ and $P(x, y) \mid D_j\Psi(x, y) = 0$, $j = 1, \ldots, k-1$, then at least one of the following alternatives holds: either*

- *(x, y) is a root of order at least k of $\Psi(x, y)$ on the algebraic curve $P(x, y) = 0$; or*
- *$x = 0$ or $y = 0$ or $\frac{\partial P}{\partial y}(x, y) = 0$ on the algebraic curve $P(x, y) = 0$.*

Proof If $D_l\Psi(x, y)$ is equal to zero on the curve $P(x, y)$, then $\frac{d^l}{dx^l}\Psi(x, y) = 0$ or $x = 0$ or $y = 0$ or $\frac{\partial P}{\partial y}(x, y) = 0$ on the curve $P(x, y)$. If $\Psi(x, y) = 0$ and $\frac{d^l}{dx^l}\Psi(x, y) = 0$ for $l = 1, \dots, k-1$, then the pair (x, y) satisfies the first case of conditions of Lemma 5. If $x = 0$ or $y = 0$ or $\frac{\partial P}{\partial y}(x, y) = 0$ on the curve $P(x, y)$, then the pair (x, y) satisfies the second case of conditions of Lemma 5. $\square$

Let us count the number of pairs (x, y) that satisfy to the second case of conditions of Lemma 5. Actually, the number of pairs $(x, 0)$ on the curve (3) is less than or equal to $\deg_x P(x, y) = m$, the number of pairs $(0, y)$ on the curve (3) is less than or equal to $\deg_y P(x, y) = n$, the number of pairs (x, y) such that $\frac{\partial P}{\partial y}(x, y) = 0$ on the curve (3) is less than or equal to $(m+n)(m+n-1)$. The sum of numbers of such pairs is less than or equal to $(m+n)^2$.

Let us prove the following lemma.

Lemma 6 *The degrees of the polynomials $q_k(x, y)$ and $r_k(x, y)$ satisfy the bounds:*

$$\begin{aligned} &\deg_x q_k(x, y) \leqslant (2k-1)m - k, \quad \deg_y q_k(x, y) \leqslant (2k-1)n - 2k + 2, \\ &\deg_x r_k(x, y) \leqslant (2k-1)m, \quad \deg_y r_k(x, y) \leqslant (2k-1)(n-1), \quad k \in \mathbb{N}. \end{aligned} \tag{21}$$

Proof For polynomials $r_k(x, y)$ the statement of Lemma 6 is obvious. Let us obtain bounds of degrees of polynomials $q_k(x.y)$. Direct calculations gives us that $\deg_x q_1(x, y) \leqslant m - 1$, $\deg_y q_1(x, y) \leqslant n$. To obtain bounds (21) let us apply the induction by k. The base of induction $k = 1$ is already obtained. The step of induction is here:

$$\begin{aligned} &\deg_x q_k(x, y) \leqslant \deg_x q_{k-1}(x, y) + 2m - 1 \leqslant (2k-1)m - k, \\ &\deg_y q_k(x, y) \leqslant \deg_y q_{k-1}(x, y) + 2n - 2 \leqslant (2k-1)n - 2k + 2. \end{aligned}$$

$\square$

Lemma 7 *Degrees of the polynomials $R_{k,a,b,c}(x, y)$ and $R_{k,l}(x, y)$, $l = 1, \dots, h$, $k \in \mathbb{N}$ satisfy to the bounds*

$$\begin{aligned} \deg_x R_{k,a,b,c}(x, y) &\leqslant 2(2k-1)m \leqslant 4km, \\ \deg_y R_{k,a,b,c}(x, y) &\leqslant (2k-1)(2n-1) - k + 2 \leqslant 4kn, \\ \deg_x R_{k,l}(x, y) \leqslant A + 4km, &\qquad \deg_y R_{k,l}(x, y) \leqslant 4kn. \end{aligned} \tag{22}$$

Proof Consider the operator (19):

$$D_k x^{a+bt} y^{ct} = \left(\frac{\partial P}{\partial y}\right)^{2k-1} x^k y^k \frac{d^k}{dx^k} x^{a+bt} y^{ct} = R_{k,a,b,c}(x, y) x^a x^{bt} y^{ct}. \tag{23}$$

Let us represent the derivative $\frac{d^k}{dx^k}x^{a+bt}y^{ct}$ in the form:

$$\frac{d^k}{dx^k}x^{a+bt}y^{ct} = \sum_{(l_1,\dots,l_s)} C_{l_1,\dots,l_s} x^{a+bt-k+\sum_{i=1}^{s} l_i} y^{ct-s}\left(\frac{d^{l_1}y}{dx^{l_1}}\right)\cdots\left(\frac{d^{l_s}y}{dx^{l_s}}\right), \quad (24)$$

where $(l_1,\dots,l_s)$ are all tuples such that $l_i > 0$, $i = 1,\dots,s$, $l_1+\dots+l_s \leqslant k$, $s = 0,\dots,k$, $C_{l_1,\dots,l_s}$ are some constant coefficients. Lemma 6 gives us that

$$\prod_{i=1}^{s}\frac{d^{l_i}y}{dx^{l_i}} = \prod_{i=1}^{s}\frac{q_{l_i}(x,y)}{r_{l_i}(x,y)}.$$

$$D_k x^{a+bt}y^{ct} = \left(\frac{\partial P}{\partial y}\right)^{2k-1} x^k y^k \frac{d^k}{dx^k}x^{a+bt}y^{ct}$$

$$= \left(\frac{\partial P}{\partial y}\right)^{2k-1} x^k y^k \prod_{i=1}^{s}\frac{q_{l_i}(x,y)}{r_{l_i}(x,y)} = R_{k,a,b,c}(x,y)x^a x^{bt} y^{ct}.$$

Bounds of Lemma 6 and direct calculation gives us the bounds (22).

Let us obtain formulas (22). Degrees of polynomials $R_{k,a,b,c}(x,y)$ and $R_{k,l}(x,y)$ can be calculated by the formulas (23) and (24).

The result follows from Lemma 6 and formulas (19), (20). □

4.2 Proof of Theorem 2

Put the following parameters:

$$A = \left\lceil \frac{h^{-1/3}t^{2/3}}{g} \right\rceil, \quad B = C = [h^{1/3}t^{1/3}],$$

$$D = \left\lceil \frac{h^{-1/3}t^{2/3}}{4mng} \right\rceil. \quad (25)$$

Let $\Psi(x,y)$ be the polynomial (10). Condition

$$D_k\Psi(x,y) = 0 \quad \text{if } P(x,y) = 0 \text{ and } (x,y) \in \bigcup_{i=1}^{h} q_i'G \times q_i''G, \;\; k = 0,\dots,D-1 \quad (26)$$

holds if polynomials $R_{k,l}(x,y)$, $k = 0,\dots,D-1$, $l = 1,\dots,h$ vanish on the curve (3), it means that

$$P(x,y) \mid R_{k,l}(x,y), \quad k = 0,\dots,D-1, \quad l = 1,\dots,h. \quad (27)$$

Degrees of polynomials $R_{k,l}(x, y)$ are calculated in Lemma 7. Lemma 4 gives us that the condition (27) is equivalent to a system of

$$hmn \sum_{k=0}^{D-1} (4km + 4kn + A + 1) = h((A+1)Dmn + 2mn(m+n)D(D-1))$$
$$\leqslant h(ADmn + 2mn(m+n)D^2)$$

homogeneous linear equations on variables $\lambda_{a,b,c}$ (we use Lemma 4 and inequality $n((\nu - n + 2)m + \mu) \leqslant (\mu + \nu + 1)mn$).

This system has a nonzero solution if the following inequality holds

$$h(ADmn + 2mn(m+n)D^2) < ABC, \tag{28}$$

because it means that the number of variables $\lambda_{a,b,c}$ is greater than the number of equations of the linear system. Let us substitute the numbers A, B and C (from (25)) to the inequality (28) and obtain the following inequality

$$DmnAh + 2D^2 mn(m+n)h < h\left[\frac{h^{-1/3}t^{2/3}}{g}\right]\left[\frac{h^{-1/3}t^{2/3}}{4mng}\right]mn$$
$$+2mnh(m+n)\left[\frac{h^{-1/3}t^{2/3}}{4mng}\right]^2 < ABC \tag{29}$$

for $h < C_1(m,n)t^2$, $t > C_2(m,n)$, where for example $C_1(m,n) = (40mn)^{-3}$ ($\frac{h^{-1/3}t^{2/3}}{4mn} > 10$) and $C_2(m,n) = 10^3$. The inequality

$$t \geqslant gAB = g\left[\frac{t^{2/3}}{g}\right][t^{1/3}],$$

gives us conditions of Lemma 3. The condition

$$\deg \Psi(x,y) < A + Bt + Ct < p, \quad \deg P(x,y) < m + n < p$$

on the characteristic of the field κ holds too.

Lemma 5 gives us the upper bound of $\#\mathcal{N}_h$. Let us obtain by (12) the upper bound on the number of elements of $\#\mathcal{N}_h$ that satisfy the first case of statement of Lemma 5. The upper bound of the number of elements of $\#\mathcal{N}_h$ that satisfy the second case of statement of Lemma 5 is less than or equal to $(m+n)^2$. Thus we obtain the following estimate

$$\#\mathcal{N}_h \leqslant h(m+n)^2 + \frac{(m+n)(A - 1 + (B-1)t + (C-1)t)}{D}$$
$$\leqslant 12mng(m+n)h^{2/3}t^{2/3}. \tag{30}$$

The inequality (30) holds if $\frac{h^{-1/3}t^{2/3}}{4mng} > 10$, (it is implied if $h < (40mng)^{-3}t^2$) and $h < C_2(m,n)t^2$. Now we obtain that the bound (30) is proved if $h < (40mng)^{-3}t^2$ and $t > 10^3$.

The proof of Theorem 2 is completed. □

5 Polynomial Energy for Homogeneous Polynomials

Let us consider a homogeneous polynomial

$$P(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i} \tag{31}$$

and a set of equations

$$P(x, y) = l_i, \quad l_i \in \mathbb{F}_p^*, \quad i = 1, \dots, h. \tag{32}$$

Lemma 8 *Let $P(x, y)$ be a homogeneous polynomial (31) and let $P(x, y) - 1$ be absolutely irreducible over κ. Then polynomials (32) are also absolutely irreducible over κ.*

Proof Let us consider the equation

$$P(x, y) = l. \tag{33}$$

We first prove that the polynomials $f_l(x, y) = P(x, y) - l$ are irreducible over $\overline{\kappa}$ for any $l \neq 0$. The polynomial $f(x, y) = P(x, y) - 1$ is irreducible by assumption. Since

$$f_l(x, y) = lf(\lambda^{-1}x, \lambda^{-1}y), \tag{34}$$

where $\lambda^n = l$, $\lambda \in \overline{\kappa}$, the polynomials $f_l(x, y)$ are irreducible for any $l \neq 0$. □

Let us estimate the number

$$N_h = \sum_{i=1}^{h} \#\{(x, y) \in G \times G \mid P(x, y) = l_i\}, \quad l_i \in \mathbb{F}_p^*, \quad i = 1, \dots, h.$$

Theorem 2 and Lemma 8 gives us the the following corollary.

Corollary 1 *Let us consider a homogeneous polynomial $P(x, y) \in \kappa[x, y]$ of degree n such that the polynomial $f(x, y) = P(x, y) - 1$ is irreducible over $\overline{\kappa}$,* deg $P(x, 0) \geqslant 1$, deg$_y$ $P(x, y) \geqslant 1$ *and a set of Eq. (32) such that $l_1, \dots, l_h$ belong to different cosets $g_i G$, $h < 40^3 n^6 |G|^2$ and $10^3 < |G| < \frac{1}{3} p^{3/4} h^{-1/4}$. Then the bound*

$$N_h < 24n^4 h^{2/3} |G|^{2/3}$$

holds.

6 Proof of Theorem 3

Let us consider the trivial relation

$$E_P^q(G) = \hat{E}_P^q(G) + (\#L)^q$$

where $L = \{(x, y) \mid P(x, y) = 0,\ x, y \in G\}$. We have the inequality

$$\#L \leqslant n|G|,$$

because for each $x \in G$ there are not grater than n different $y \in G$ such that $P(x, y) = 0$. Consequently, we have

$$E_P^q(G) \leqslant \hat{E}_P^q(G) + n^q |G|^q.$$

We will estimate $\hat{E}_P^q(G)$. Let us denote all non-zero elements of the set $\{P(x, y) \mid x, y \in G\}$ by α_i, $i = 1, \dots, N$ and consider such β_i that $\beta_i^n = \alpha_i$, $i = 1, \dots, N$.

Let us re-denote elements β_i, $i = 1, \dots, N$ by β_{ij}, $i = 1, \dots, k$, $j = 1, \dots, s_i$ so that the following conditions are satisfied:

1. let β_{ij} be elements of the Young tableau, where i is the number of string ($i = 1, \dots, k$), j is the number of column ($j = 1, \dots, s_i$), $s_1 \geqslant \dots \geqslant s_k$ (s_i, $i = 1, \dots, k$, k are some numbers)
2. any elements $\beta_{i_1,j}$ and $\beta_{i_2,j}$ such that $\beta_{i_1,j}/\beta_{i_2,j} \notin G$ for each admissible $i_1 \neq i_2$, j.
3. $\varphi_{i,j} \geqslant \varphi_{i+1,j}$, $j = 1, \dots, s_1$, $i = 1, \dots, k_j - 1$.
   Where $\varphi_{ij} = \#\{(x, y) \mid P(x, y) = (\beta_{ij})^n,\ x, y \in G\}$ and let k_j be the number of the last element jth column, for $j = 1, \dots, s_1$. Obviously, the number of elements of any string of this tableau does not greater than $|G|$ ($s_1 \leqslant |G|$).
4. Corollary 1 and condition 2 gives us the following inequality

$$\begin{aligned}\sum_{i=1}^{h} \varphi_{ij} = \sum_{i=1}^{h} \#\{(x, y) \mid P(x, y) = \tilde{\beta}_{ij}^n,\ x, y \in G\} < 24 n^4 h^{2/3} |G|^{2/3},\\ h < 40^{-3} n^{-9} |G|^2. \end{aligned} \tag{35}$$

   for each $j = 1, \dots, s_1$ and $h = 1, \dots, \min(k_j, 40^{-3} n^{-9} |G|^2)$.
5. $\sum_{j=1}^{s_1} \sum_{i=1}^{k_j} \varphi_{ij} = |G|^2 - \#L$.
   The number $\hat{E}_P^q(G)$ has the form

$$\hat{E}_P^q(G) = \sum_{j=1}^{s_1} \sum_{i=1}^{k_j} (\varphi_{ij})^q. \tag{36}$$

We have to obtain the upper bound of the sum (36) where the set $\{\varphi_{ij}\}$ is satisfied the restrictions 1–5. Let us describe such set of numbers φ_{ij} that it satisfy to conditions 1–5 and the sum (36) is maximal.
It is easy to see that such $\tilde{\varphi}_{ij}$ have to be maximal. Such set satisfy to $|k_i - k_j| \leqslant 1$, $1 \leqslant i, j \leqslant |G|$. We have

$$\tilde{\varphi}_{ij} = \sum_{l=1}^{i} \tilde{\varphi}_{lj} - \sum_{l=1}^{i-1} \tilde{\varphi}_{lj} = 24n^4 i^{2/3}|G|^{2/3} - 24n^4(i-1)^{2/3}|G|^{2/3} + \varepsilon_{ij}$$
$$\leqslant 16n^4 i^{-1/3}|G|^{2/3} + 1 < 17n^4 i^{-1/3}|G|^{2/3},$$

where $\varepsilon_{ij} \in \{0, \pm 1\}$,

$$(\tilde{\varphi}_{ij})^q < (17n^4 i^{-1/3}|G|^{2/3})^q = 17^q n^{4q}|G|^{2q/3} i^{-q/3}$$

We have that $\sum_{j=1}^{s_1} \sum_{i=1}^{k_j} \varphi_{ij} \leqslant |G|^2$. We obtain that $\tilde{k}_j \leqslant \frac{|G|^{1/2}}{24^{3/2} n^6} + 1 < \left[\frac{|G|^{1/2}}{125n^6}\right] = \tilde{k}$.

Let us estimate the maximal value of the sum (36)

$$\hat{E}_P^q(G) \leqslant |G| \sum_{i=1}^{\tilde{k}} 17^q n^{4q}|G|^{2q/3} i^{-q/3}.$$

Let us consider case $q = 2$.

$$\hat{E}_P^2(G) \leqslant |G| \leqslant 17^2 3n^8|G|^{7/3}\tilde{k}^{1/3} < 10^3 n^8|G|^{5/2}.$$

In the case $q = 3$ we have

$$\hat{E}_P^3(G) \leqslant 17^3 n^{12}|G|^3 \ln |G|.$$

In the case $q > 3$ we have

$$\hat{E}_P^q(G) \leqslant 17^q 3n^{4q}|G|^{1+2q/3}.$$

$E_P^q(G)$ is less than or equal to $\hat{E}_P^q(G) + |G|^q n^q$.

□

Acknowledgements The authors are grateful to Sergei Konyagin, Ilya Shkredov and Ian Marshall for their attention and useful comments. The authors are particularly grateful to Igor Shparlinski and Umberto Zannier for their contribution to the formulation of the problem, which is considered in the paper.

References

Bourgain, J., Gamburd, A., Sarnak, P.: Markoff triples and strong approximation. C. R. Acad. Sci. Paris Ser. I **354**(2), 131–135 (2016)

Corvaja, P., Zannier, U.: Greatest common divisor of $u - 1$, $v - 1$ in positive characteristic and rational points on curves over finite fields. J. Eur. Math. Soc. **15**(5), 1927–1942 (2013)

Heath-Brown, R., Konyagin, S.: New bounds for gauss sums derived from k-th powers, and for heilbronn's exponential sum. Quart. J. Math. **51**, 221–235 (2000)

Konyagin, S.V., Makarychev, S.V., Shparlinski, I.E., Vyugin, I.V.: On the new bound for the number of solutions of polynomial equations in subgroups and the structure of graphs of markoff triples. arXiv preprint: arXiv:1711.05335 (2017)

Schoen, T., Shkredov, I.: Higher moments of convolutions. J. Number Theory **133**(5), 1693–1737 (2013)

Shafarevich, I.: Basic Algebraic Geometry I. Springer, Berlin (2013)

Shkredov, I.D., Solodkova, E.V., Vyugin, I.V.: Intersections of multiplicative subgroups and heilbronn's exponential sum. arXiv preprint: arXiv:1302.3839 (2015)

Stepanov, S.A.: On the number of points of a hyperelliptic curve over a finite prime field. Izv. Akad. Nauk. SSSR Ser. Mat. **33**(5), 1171–1181 (1969)

Tao, T., Vu, V.: Additive Combinatorics. Cambridge University Press, Cambridge (2006)

Vyugin, I.V., Shkredov, I.D.: On additive shifts of multiplicative subgroups. Sb. Math. **203**(6), 81–100 (2012)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.