Solutions of polynomial equation over F_p and new bounds of energy of multiplicative subgroups

I. V. Vyugin

Institute for Information Transmission Problems
Russian Academy of Sciences

CANT 2016, Graz 4-8 January 2016

iitp-g

Linear equations: Garcia and Voloch's bound

Let G be a subgroup of F_p^*, p is prime.

Theorem (Garcia-Voloch)

Let $G \subset F_p^*$ be a subgroup, such that $|G| < (p-1)/((p-1)^{1/4}+1)$. Then the number of solutions of the equation

$$y = x + q, \quad q \neq 0,$$

such that $x, y \in G$ does not exceed $4|G|^{2/3}$.

Heath-Brown and Konyagin have proved this result by Stepanov method.

The problem's statement

Let G be a subgroup of F_p^*, p is prime.
The bound of the number of solutions of equation

$$P(x, y) = 0, \qquad P \in F_p[x, y],$$

such that $x \in g_1 G$, $y \in g_2 G$, where $g_1 G$, $g_2 G$ are cosets by subgroup G, was obtained by Corvaja and Zannier.

P. Corvaja, U. Zannier, Greatest Common Divisor $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields, J. of Eur. Math. Soc., V. 15, I. 5, pp. 1927-1942, 2013.

Corvaja and Zannier's bound

Theorem (Corvaja-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 $X \setminus S$. Then*

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

where $v(f)$ denotes the multiplicity of vanishing of f at the point v.

Corvaja and Zannier's bound was obtained by hyperwronskian method.
Let us denote the set

$$\Omega = \{(x, y) \mid x \in g_1 G, y \in g_2 G, P(x, y) = 0\}.$$

Makarychev and Vyugin have obtained the upper bound

$$\#\Omega < 16mn^2(m+n)|G|^{2/3}.$$

by Stepanov method.

Bound in average

Let us suppose that $P(x,y)$ is a homogeneous of degree n, $l_1,\dots,l_h$ belongs to different cosets by subgroup G of F_p^*.

Theorem (Makarychev, I.V.)

Let us consider a homogeneous polynomial $P(x,y)$ of degree n, such that $\deg P(x,0) \geqslant 1$. *Then the set of equations*

$$P(x,y) = l_i, \quad i = 1,\dots,h,$$

$h < \min(\frac{1}{81}|G|^{4/3}, \frac{1}{3}pt^{-4/3})$ *the sum N_h of numbers of solutions of the set of equations does not exceed*

$$N_h \leqslant 32h^{3/4}n^5|G|^{2/3}.$$

Additive energy and its generalizations

Let A be a subset of F_p
Additive energy

$$E_k(A) = \#\{(x_1, \dots, x_{2n}) \mid x_1 + x_2 = \cdots = x_{2n-1} + x_{2n},\ x_i \in A,\ i = 1, \dots, 2n\}$$

Theorem

Let G be a subgroup of F_p^*, and $|G| \leqslant p^{2/3}$. Then

$$E_2(G) = O(|G|^{5/2}) \quad \textit{(Konyagin)}; \tag{1}$$

$$E_3(G) = O(|G|^3 \log |G|)) \quad \textit{(Shkredov)}; \tag{2}$$

$$E_k(G) = |G|^k + O(|G|^{\frac{2l+3}{3}})) \quad \textit{(Shkredov)},\ k \geqslant 4. \tag{3}$$

Polynomial energy

Let A be a subset of F_p, $P(x,y)$ be a polynomial. Polynomial energy

$$E_k^P(A) = \#\{(x_1,\dots,x_{2n}) \mid P(x_1,x_2) = \dots = P(x_{2n-1},x_{2n}),\ x_i \in A,\ i = 1,\dots$$

Theorem (Makarychev, I.V.)

Let G be a subgroup of F_p^*, $P \in F_p[x,y]$ is a homogeneous and $100(mn)^{3/2} < |G| < \left(\frac{p}{3}\right)^{\frac{12}{17}}$. Then the following holds: if $q \leqslant 3$ then

$$E_P^q(G) \leqslant C(n,q)|G|^{\frac{7q+16}{12}};$$

if $q = 4$ then

$$E_P^4 \leqslant C(n,q)|G|^{1+\frac{2q}{3}} \ln|G|;$$

if $q \geqslant 5$ then

$$E_P^q(G) \leqslant C(n,q)|G|^{1+\frac{2q}{3}},$$

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

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

Corollary

Let G be a subgroup of F_p^*, and $f,g \in F_p[x]$, $\deg f = m$, $\deg g = n$ and $100(mn)^{3/2} < |G| < \frac{1}{3}p^{3/4}$. Then

$$E(f(G),g(G)) < 16mn^2(m+n)|G|^{8/3}.$$

The sketch of 2-dimensional of Stepanov's method.

Let us consider a polynomial $\Phi \in \mathbb{F}_p[X, Y, Z]$ such that

$$\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C,$$

or in the other words

$$\Phi(X, Y, Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a Y^b Z^c, \qquad a \in [A], \quad b \in [B], \quad c \in [C]. \quad (4)$$

Consider the following polynomial

$$\Psi(x, y) = \Phi(x, x^t, y^t), \quad (5)$$

which satisfies to the following conditions:
1) all roots (x, y) of the equation $P(x, y) = 0$, such that $x \in g_1 G, y \in g_2 G$, are zeros of system

$$\begin{cases} \Psi(x, y) = 0 \\ P(x, y) = 0 \end{cases} \quad (6)$$

of the an order at least D.

2) the greatest common divisor of polynomials $\Psi(x,y)$ and $P(x,y)$ is a nonzero constant.
If these conditions are satisfied then the generalized Bézout's theorem gives us the upper bound of the number N of roots (x,y) such that $x \in g_1 G$, $y \in g_2 G$:

$$N \leqslant \frac{\deg \Psi(x,y) \cdot \deg P(x,y)}{D} \leqslant \frac{(A-1+(B-1)t+(C-1)t)(m+n)}{D}. \quad ($$

A pair (x,y) is the solution of the system (6) of the order at least D, if $P(x,y)=0$ and $\Psi(x,y)=0$ and derivatives

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

vanishes on the curve $P(x,y)=0$.
To test the second condition $P(x,y) \not| \Psi(x,y)$.

Lemma

Let

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

be a polynomial, $nAB \leqslant t$, coefficients $\lambda_{a,b,c}$ do not vanish simultaneously, $P(x,y)$ be an irreducible polynomial and $\deg_y P(x,y) = n$, $P(0,0) \neq 0$. Then $P(x,y)$ does not divide $\Psi(x,y)$.

Polynomial maps and multiplicative subgroups.

Linear maps

Theorem (Shkredov, I.V.)

Let G be a subgroup of F_p^*, such that $|G| > 32n2^{20n\log(n+1)}$, $p > 4n|G|(|G|^{\frac{1}{2n+1}} + 1)$, $q_0, \dots, q_n$ be different residues. Then the number of such $x \in F_p$ that

$$x + q_i \in G, \qquad i = 0, 1, \dots, n$$

does not exceed $4n(n+1)(|G|^{\frac{1}{2n+1}} + 1)^{n+1}$.

Asymptotic form of the previous theorem.

If $C_1(n) < |G| < C_2(n)p^{1-\alpha_n}$, then

$$\#\{x \in F_p \mid x + q_i \in G, i = 0, \ldots, n\} < C_3(n)t^{1/2+\beta_n},$$

where $\alpha_n, \beta_n \to 0$, $n \to \infty$, $C_1(n), C_2(n), C_3(n)$ are some constants.

Polynomial generalization

Let $f_1, \ldots, f_n \in F_p[x]$ be polynomials of degrees

$$\deg f_i(x) = m_i,$$

and $G \subset F_p^*$ be a multiplicative subgroup.
Let us consider the map

$$x \to (f_1(x), \ldots, f_n(x))$$

and the set

$$L = \{x \mid f_i(x) \in G, i = 1, \ldots, n\}.$$

$$\deg f_i(x) = m_i,$$

$$L = \{x \mid f_i(x) \in G, i = 1, \ldots, n\}.$$

Theorem (I.V.)

If $C_1(m) < |G| < C_2(m)p^{1-\frac{1}{2n-1}}$, $m = (m_1, \ldots, m_n)$, $f_i(0)$ *are pairwice distinct and there exists such* $\mu_1, \ldots, \mu_n$ *that* $f_i(\mu_i) = 0$, *and* $f_j(\mu_i) \neq 0$ *for all* $j \neq i$. *Then*

$$\#L < C_3(m)|G|^{\frac{1}{2}+\frac{1}{2n}},$$

for some constants $C_1(m), C_2(m), C_3(m)$.

Application

Let G be a subgroup of F_p^*.
Suppose that

$$G = P(A, B) = \{P(a, b) \mid a \in A, b \in B\},$$

where A, B are some subsets of F_p, $P \in F_p[x, y]$ such that $\deg P(x, 0) \geqslant 1$, $\deg P(0, y) \geqslant 0$. Then $|A|$ and $|B|$ are around of $\sqrt{G}$.

Idea of proof.

Let us suppose that $G = P(A, B)$, and let B be a set $B = \{b_j\}_{j=1}^{j=k}$.
Let us denote a touple of polynomials $f_i(x) = P(x, b_i)$.

For any $x \in A$, and $i = 1, \ldots, k$: $f_i(x) = P(x, b_j) \in G$.
Consequently, the number of such x does not exceed $C_3(m)|G|^{\frac{1}{2}+\frac{1}{2k}}$.

$$|A| < C_3(m)|G|^{\frac{1}{2}+\frac{1}{2k}}.$$

For B all is symmetric.

Application

Thank you for your attention!!!