Value sets of sparse polynomials

Felipe Voloch

Number Theory Web Seminar

June 2020

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Abstract

We obtain a lower bound on the size of the value set $f(\mathbb{F}_p)$ of a sparse polynomial $f(x) \in \mathbb{F}_p[x]$ over a finite field of p elements when p is prime. This bound is uniform with respect to the degree and depends on the number of terms of f.

Joint work with I. Shparlinski

Value sets

If $f \in \mathbb{F}_q[x]$ has degree n, then $V(f) := \#f(\mathbb{F}_q) \geq \lceil q/n \rceil$ since each element of $\mathbb{F}_q$ has at most n preimages under f.

Bound attained if $n|(q-1), f(x) = x^n$. For q prime and $\geq \lceil q/n \rceil \geq 3$, these (up to obvious transformations) are the only examples where the equality is attained. If $q = p^2, p^3, p$ prime these "minimal value polynomials" are also classified.

Carlitz, Lewis, Mills, Strauss; Borges, Reis

We study the question of bounding $V(f) := \#f(\mathbb{F}_q)$ from below as a function of the number of terms in f, rather than its degree. Specifically, if $f(x) = a_0 + \sum_{i=1}^{t} a_i x^{n_i}$, we want to estimate $V(f)$ in terms of t and q.

Main result

Theorem 1

For prime $p \geq 5$ and integers $1 \leq n_1, \ldots, n_t < p-1$ such that

(i) $\max_{1\leq j<i\leq t} \gcd(n_j - n_i, p-1) \leq 2^{-t^2}(p-1)$,

(ii) $\gcd(n_1, \ldots, n_t, p-1) = 1$,

If $f(x) = \sum_{i=1}^{t} a_i x^{n_i} \in \mathbb{F}_p[x], a_i \neq 0,\ i = 1, \ldots, t,$ then

$$V(f) \geq \min\{(\frac{3p}{t})^{2/3}, \frac{1}{12} p^{4/(3t+4)}\}.$$

For $t = 2, n_1 = 1$ we get $V(f) \geq \sqrt{p}$.

Counterexamples

Hypotheses (i) and (ii) necessary: If $n|(p-1), n|n_i, \forall i$, then $V(f) \leq p/n$.

Prime field is necessary: $x + x^p + \cdots + x^{p^{t-1}}$ maps $\mathbb{F}_{p^t}$ to $\mathbb{F}_p$.

Ideas of proof - I

First, reduce the degree of $f(x)$. Replace x by $x^m, (m, p-1) = 1$ (bijection on $\mathbb{F}_p$).

This replaces n_i by $mn_i \pmod{p-1}$ and, by (i) and (ii), can be made simultaneously small for some choice of m.

This alone already gives a bound for the number of solutions of $f(x) = a$ which gives a lower bound for $\# f(\mathbb{F}_p)$ (about $p^{1/t}$). But we will do better.

Canetti, Friedlander, Konyagin, Larsen, Lieman, Shparlinski

Ideas of proof - II

If $\#f(\mathbb{F}_p)$ is small then the number of solutions of $f(x) = f(y)$ is large. We want to bound the number of irreducible factors of $f(x) - f(y)$ and their degrees.

For each irreducible factor $g(x, y)$ we use known bounds for the number of points on curves over finite fields to estimate the number of solutions of $g(x, y) = 0$

Hasse, Weil; Stöhr, V.

Ideas of proof - III

Let K be the function field of the curve $g(x,y)=0$. The equation

$$\sum_{i=1}^{t} a_i x^{n_i} - \sum_{i=1}^{t} a_i y^{n_i} = 0$$

is an S-unit equation on K where S is the set of zeros and poles of x and y. Use generalized abc bounds.

Zannier; Brownawell, Masser; V.

Ideas of proof - IV

K/F function field of genus g and characteristic $p > 0$ and S finite set of places of K. If $u_1, \dots, u_m$ are S-units of K, linearly independent over F, with $\deg(u_1 : \cdots : u_m) < p$ and

$$u_1 + \cdots + u_m = 1$$

then

$$\max\{\deg u_i\} \leq \frac{m(m-1)}{2}(2g - 2 + \#S)$$

Exponential sums - I

We also bound some exponential sums. E.g. p prime, $n|(p-1)$,

$|\sum_{x=0}^{p-1} \exp(2\pi i(ax + bx^n)/p| \ll p^{4/5}$

Averaging reduces to estimate number of solutions of

$x^n + y^n - (x + y - 1)^n = 1.$

Same ideas as before then handles the number of factors and the number of solutions for each factor.

Exponential sums - II

Conjecture

$x^n + y^n - (x+y-1)^n - 1 \in \bar{\mathbb{F}}_p[x,y]$ *has unique irreducible factor besides* $x-1, y-1, x+y$ *if* $2 \le n < p, n \neq (p+1)/2$.

True for $p < 200$ or $n = (p-1)/2$.

For $n = (p+1)/2$ it is a product of linear and quadratics.

Popovych; Borges, Cook, Coutinho

THANK YOU