Distribution of Points on Varieties over Finite Fields

Igor Shparlinski

University of New South Wales

Introduction

Set-up and motivation

Let $\mathbb{F}_p$ be a finite field of p elements, where p is prime.

Given m polynomials $f_j \in \mathbb{F}_p[X_1, \ldots, X_n]$ in n variables we are interested in the distribution of

1. points on the variety

$$f_j(x_1, \ldots, x_n) = 0, \quad j = 1, \ldots, m;$$

2. points of polynomial values

$$(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) .$$

Question 2 is a special case of Question 1 if one considers the $(m+n)$-dimensional variety

$$f_j(x_1, \ldots, x_n) - y_j = 0, \quad j = 1, \ldots, m.$$

We represent $\mathbb{F}_p$ by the set $\{0, \ldots, p-1\}$.

So we can investigate the distribution of points in boxes

$$\mathfrak{B} = [u_1 + 1, u_1 + h_1] \times \ldots \times [u_s + 1, u_s + h_s]$$

and cubes

$$\mathfrak{C} = [u_1 + 1, u_1 + h] \times \ldots \times [u_s + 1, u_s + h],$$

where

- $s = n$ for the boxes containing the values of variables: (Q.1);
- $s = m$ or $s = m + n$ for the boxes containing the values of polynomials and also of variables (Q.2).

The classical approach is via algebraic geometry methods of *Weil* and *Deligne*:

Fouvry, Fouvry & Katz, Luo, Shparlinski & Skorobogatov

A natural threshold is $h_i \geq p^{1/2}$.

In almost all known results the threshold is substantially higher, e.g. $h_i \geq p^{3/4}$ or even higher.

Here we concentrate on some interesting special cases when one can go beyond the $p^{1/2}$-threshold.

Why is this possible?

There are tools and methods that go beyond the algebraic geometry threshold of $\sqrt{p}$:

- The bound of *Burgess* (1962) of character sums and its recent generalisation to mixed character sums due to *Chang* (2010)
- The bound of *Ayyad, Cochrane & Zheng* (1996) on the 4th moment of short character sums
- The bound of *Vinogradov* of exponential sums with polynomials and its recent improvement due to *Wooley* (2012)
- Methods of additive combinatorics usually apply to very thin sets
- Since we work over $\mathbb{F}_p$ whose elements can be lifted to $\mathbb{Z}$, we can sometimes switch from congruences to equations.

Sacrifices we are willing to make

We consider only some special varieties, usually with some multiplicative structure to enable us to use multiplicative character sums.

In many cases we

- obtain results only for cubes $\mathfrak{C}$
  - this is enough for many applications and also for studying the distribution of solutions in arbitrary convex domains: *Kerr* (2012) combined such results with some ideas of *Schmidt* (1975)
- obtain upper bounds instead of asymptotic formulas

Additional gains

- Using multiplicative characters enables us to use the large sieve and obtain stronger results for *almost all* primes.

  For example, sometimes one can use the bound of *Heath-Brown* (1995) on the mean value of real character sums

- Bounds of exponential sums rapidly lose their strength when one consider composite moduli, while bounds of character sums very often remain the same:

  Burgess (1962) bound (for cube-free moduli)
  Pólya–Vinogradov (1916) bound
  Ayyad, Cochrane & Zheng (1996) is replaced by the bound of *Friedlander & Iwaniec* (1985)

Examples

Hyperbolas:

$$x_1 \ldots x_n \equiv \lambda \pmod p$$

Links to numerous number theoretic problems.

Markoff-Hurwitz hypersurface:

$$x_1^2 + \ldots + x_n^2 \equiv x_1 \ldots x_n \pmod p$$

Dwork hypersurface:

$$x_1^n + \ldots + x_n^n \equiv x_1 \ldots x_n \pmod p$$

which is an example of a *Calabi-Yau variety*.

Both can be generalised as

$$f_1(x_1) + \ldots + f_n(x_n) \equiv x_1^{k_1} \ldots x_n^{k_n} \pmod p$$

with some polynomials $f_i \in \mathbb{F}_p[X]$ and integers k_i, $i = 1, \ldots, n$.

Erdős-Graham equation:

$$\frac{1}{x_1} + \ldots + \frac{1}{x_n} \equiv \lambda \pmod{p}$$

Plane curves:

$$f(x, y) \equiv 0 \pmod{p}$$

and in particular values of univariate polynomials:

$$f(x) \equiv y \pmod{p}$$

Weierstraß equations of isomorphic elliptic curves

$$(ax^4, bx^6)$$

A similar question can be, and has been, also asked for *hyperelliptic curves*.

Hyperbolas

Large boxes

Let $J_n(\lambda; \mathfrak{B})$ be the number of solutions of the congruence

$$x_1 \ldots x_n \equiv \lambda \pmod p, \qquad (x_1, \ldots, x_n) \in \mathfrak{B}$$

We always assume $\lambda \not\equiv 0 \pmod p$.

Bounds of multidimensional Kloosterman sums:

$$J_n(\lambda; \mathfrak{B}) = \frac{h_1 \ldots h_n}{p} + O(p^{n/2+o(1)})$$

Fouvry & Katz (2001) if $\mathfrak{B} = \mathfrak{C}$ then

$$J_n(\lambda; \mathfrak{C}) = \frac{h^n}{p} + O(p^{(n-1)/2+o(1)} + h^{n-1}p^{-1/2+o(1)})$$

This is *nontrivial* for $h \geq p^{1/2+1/2n+o(1)}$.

Shparlinski (2007): with multiplicative characters we can do better.

Theorem 1 *For $n = 3$,*

$$J_3(\lambda; \mathfrak{B}) = \frac{h_1 h_2 h_3}{p} + O\left((h_1 h_2 h_3)^{\alpha_\nu} p^{\beta_\nu + o(1)}\right)$$

holds with $\nu = 1, 2, \ldots$, where

$$\alpha_\nu = \frac{2\nu - 1}{3\nu} \qquad \textit{and} \qquad \beta_r = \frac{\nu + 1}{4\nu^2}.$$

Theorem 2 *For* $n \geq 4$,

$$J_n(\lambda; \mathfrak{B}) = \frac{h_1 \dots h_n}{p} + O\left((h_1 \dots h_n)^{\alpha_{n,\nu}} p^{\beta_{n,\nu} + o(1)}\right)$$

holds with $\nu = 1, 2, \dots$, *where*

$$\alpha_{n,\nu} = 1 - \frac{n + 2\nu - 4}{n\nu} \quad \text{and} \quad \beta_{n,\nu} = \frac{(n-4)(\nu+1)}{4\nu^2}.$$

If $\mathfrak{B} = \mathfrak{C}$ then taking $\nu = \lceil n^{1/2} \rceil$ this is *nontrivial* for $h \geq p^{1/4+\varepsilon}$ provided that n is large enough.

Sketch of the proof

Express $J_n(\lambda;\mathfrak{B})$ via sums of multiplicative characters χ modulo p

$$J_n(\lambda;\mathfrak{B}) = \sum_{x_i=u_i+1}^{u_i+h_i} \frac{1}{p-1}\sum_{\chi}\chi\left(\lambda^{-1}\prod_{i=1}^{n} x_i\right)$$
$$= \frac{1}{p-1}\sum_{\chi}\prod_{i=1}^{n}\sum_{x_i=u_i+1}^{u_i+h_i}\chi(x_i).$$

- The main term comes from the principal character χ_0 and is equal to $M = h_1 \ldots h_n/(p-1)$.
- The error term, after the change of summation becomes

$$E \le \frac{1}{p-1}\sum_{\chi\neq\chi_0}\prod_{i=1}^{n}\left|\sum_{x_i=u_i+1}^{u_i+h_i}\chi(x_i)\right|$$
$$\le \frac{1}{p-1}\left(\prod_{i=1}^{n}\sum_{\chi\neq\chi_0}\left|\sum_{x_i=u_i+1}^{u_i+h_i}\chi(x_i)\right|^{n}\right)^{1/n}.$$

For sums

$$\sum_{\chi \neq \chi_0} \left| \sum_{x=u+1}^{u+h} \chi(x_i) \right|^n$$

use the Burgess bound

$$\left| \sum_{x=u+1}^{u+h} \chi(x_i) \right| \le h^{1-1/\nu} p^{(\nu+1)/4\nu^2 + o(1)}$$

for $(n-4)$ times and then the bound of *Ayyad, Cochrane & Zheng* (1996) on the 4th moment

$$\sum_{\chi \neq \chi_0} \left| \sum_{x=u+1}^{u+h} \chi(x_i) \right|^4 \le h^2 p^{1+o(1)}.$$

Applications

Smooth values of shifted monomial products:

Fouvry & Shparlinski (2011):

For positive integers $a_1, \ldots, a_n$ and any $\varepsilon > 0$ there is a positive proportion of vectors $(m_1, \ldots m_n)$ so that

$$F = m_1^{a_1} \ldots m_n^{a_n} - 1$$

is $F^{1-n/2d+\varepsilon}$-smooth.

This improves on $F^{1-2/d+2/d(n+1)+\varepsilon}$–smoothness of *Fouvry* (2010).

Small boxes

The following result of *Bourgain, Garaev, Konyagin & Shparlinski* (2012):

Theorem 3 *Let $n \ge 2$ be a fixed integer, $\lambda \not\equiv 0 \pmod p$. Assume that for some sufficiently large positive integer h and prime p we have*

$$h < p^{1/(n^2-1)}.$$

Then

$$J_n(\lambda;\mathfrak{C}) = \exp\left(O\left(\frac{\log h}{\log\log h}\right)\right).$$

In the case $nu = 4$ this solves an open problem of *Cilleruelo & Garaev* (2010).

Sketch of the proof

Express $J_n(\lambda; \mathfrak{C})$ via characters as before and use the Hölder inequality to reduce everything to $u_1 = \ldots = u_n = u$.

If

$$(u+x_1)\ldots(u+x_n) \equiv \lambda \pmod p, \quad 1 \le x_1, \ldots, x_n \le h$$

has many solutions then there are many polynomials with not so large coefficients with a common root u modulo p.

Use the Dirichlet principle to conclude that there are two pairs of such polynomials

$$(U+y_{j,1})\dots(U+y_{j,n}) \qquad \text{and} \qquad (U+z_{j,1})\dots(U+z_{j,n}),$$

for which

$$P_j(U) = (U+y_{j,1})\dots(U+y_{j,n}) - (U+z_{j,1})\dots(U+z_{j,n}),$$

where $j = 1, 2$

- are nonzero co-prime polynomials over $\mathbb{Z}$
- have small coefficients.

Estimate [very carefully!] the resultant $R = \mathrm{Res}(P_1, P_2)$ which satisfies

$$R \neq 0 \qquad \text{and} \qquad R \equiv 0 \pmod{p}$$

and obtain a contradiction.

Warning: The argument is actually more subtle.

Modifications

- In the symmetric case with $n \ge 3$

  $$x_1 \dots x_n \equiv y_1 \dots y_n \pmod p,$$

  with $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathfrak{C}$ one can take

  $$h < p^{1/e_n}$$

  with

  $$e_n = \max\{n^2 - 2n - 2, n^2 - 3n + 4\}.$$

  If $n = 2$, *Ayyad, Cochrane & Zheng* (1996) give an optimal result.

- For almost all primes p one can get a *nontrivial* bound for any h

Applications

Points on exponential curves: Improvements of bounds of *Chan & Shparlinski* (2010) and *Cilleruelo & Garaev* (2011) for

$$x \equiv ag^z \pmod{p}, \quad 1 \le x \le h,\ 1 \le z \le H.$$

Double character sum estimates: Improvements of bounds of *Friedlander & Iwaniec* on sums

$$\sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(a+b)$$

E.g. if $\mathcal{A} \subseteq [M, M+A]$, $A \le p^{1/2}$ and $\#\mathcal{A} > p^{9/20+\varepsilon}$ for some $\varepsilon > 0$, then for some $\delta > 0$ we have

$$\sum_{a_1,a_2\in\mathcal{A}} \chi(a_1+a_2) \ll (\#\mathcal{A})^2 p^{-\delta}.$$

Character sums with the divisor function: Improvements of bounds of *Karatsuba* (2000) on sums

$$S_a(N) = \sum_{1 \le n \le N} \tau(n)\chi(a+n).$$

Shifted power testing: Given $t \in \mathbb{F}_p$ and a black-box that for every $x \in \mathbb{F}_p$ outputs $(x+s)^e$ for some **hidden** $s \in \mathbb{F}_p$ and **known** $e \mid p-1$ decide whether $s = t$.

Weierstraß equations

Preliminaries

Let

$$E_{a,b}: \quad Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p,\ 4a^3 + 27b^2 \neq 0.$$

Two curves $E_{a,b}$ and $E_{r,s}$ are isomorphic *iff*

$$ax^4 \equiv r \pmod p \qquad \text{and} \qquad bx^6 \equiv s \pmod p$$

for some $x \in \mathbb{F}_p^*$.

Fouvry & Murty (1996): What is the number $T_{a,b,p}(\mathfrak{B})$ of curves

$$E_{r,s}: \quad (r, s) \in \mathfrak{B} = [R+1, R+K] \times [S+1, S+L]$$

that are isomorphic to a given curve $E_{a,b}$? Motivation: Lang-Trotter conjecture

Banks & Shparlinski (2009): Same question "on average" over $(a, b) \in \mathbb{F}_p^2$ and primes $p \leq Q$. Motivation: Sato-Tate conjecture

Both questions are about the joint distribution of values of two very simple polynomials

$$aX^4 \qquad \text{and} \qquad bX^6$$

in boxes.

Large boxes

Fouvry & Murty (1996)— used exponential sums
Weil bound: for any $(a,b) \in \mathbb{F}_p^2$,

$$T_{a,b,p}(\mathfrak{B}) \sim \frac{KL}{p}, \quad \text{if } KL \geq p^{3/2+\varepsilon},\ \min\{K,L\} \geq p^{1/2+\varepsilon}.$$

Banks & Shparlinski (2009) — used character sums
Burgess bound: for almost all $(a,b) \in \mathbb{F}_p^2$,

$$T_{a,b,p}(\mathfrak{B}) \sim \frac{KL}{p}, \quad \text{if } KL \geq p^{1+\varepsilon},\ \min\{K,L\} \geq p^{1/4+\varepsilon}$$

and

$$T_{a,b,p}(\mathfrak{B}) \gg \frac{KL}{p}, \quad \text{if } KL \geq p^{1+\varepsilon},\ \min\{K,L\} \geq p^{1/4e^{1/2}+\varepsilon}.$$

Furthermore, together with Large Sieve, for almost all primes p and $(a,b) \in \mathbb{F}_p^2$,

$$T_{a,b,p}(\mathfrak{B}) \sim \frac{KL}{p}, \quad \text{if } KL \geq p^{1+\varepsilon},\ \min\{K,L\} \geq p^{\varepsilon}.$$

Small boxes

<u>Observation:</u> $E_{a,b} \cong E_{r,s} \Longrightarrow r^3 b^2 \equiv a^3 s^2 \pmod p$.
Let's estimate

$$N_{\lambda,p}(\mathfrak{B}) = \#\{r^3 \equiv \lambda s^2 \pmod p \ : \ (r,s) \in \mathfrak{B}\}.$$

For $f \in \mathbb{Z}[X]$ we define:

$$I_f(\mathfrak{B}) = \#\{f(r) \equiv s^2 \pmod p \ : \ (r,s) \in \mathfrak{B}\}.$$

Cilleruelo,Garaev, Ostafe & Shparlinski (2010);
Cilleruelo, Shparlinski & Zumalacárregui (2012);
Chang, Cilleruelo, Garaev, Hernández, Shparlinski & Zumalacárregui (2012): For

$$\mathfrak{C} = [R+1, R+M] \times [S+1, S+M] \qquad \text{and} \qquad \deg f = 3$$

we have

$$I_f(\mathfrak{C}) < M^{1+o(1)} \begin{cases} M^{-2/3} & \text{if } M < p^{1/8}, \\ (M^4/p)^{1/6} & \text{if } p^{1/8} \le M < p^{5/23}, \\ (M^3/p)^{1/16} & \text{if } p^{5/23} \le M < p^{1/3}. \end{cases}$$

The proof uses Bombieri-Pila bound and some ideas from additive combinatorics

For $M \geq p^{1/2}$ exponential sums give a *nontrivial* bound.

Unfortunately we have no *nontrivial* estimate for $p^{1/3} < M < p^{1/2}$

Warning: Splitting $\mathfrak{C}$ into smaller squares does not work as the number of squares grows quadratically.

Remarks:

- For higher degree polynomials other methods work, e.g. Vinogradov's Mean Value Theorem, *Wooley* (2012).

- Similar (and somewhat stronger) results also hold for

$$J_f(\mathfrak{C}) = \#\{f(r) \equiv s \pmod p \ : \ (r,s) \in \mathfrak{C}\}.$$

- Similar results also hold for Weierstraß equations of hyperelliptic curves.

Applications

Diameter of orbits of polynomial dynamical systems: Given a polynomial $f \in \mathbb{F}_p[X]$, show that a partial orbit $x_k = f(x_{k-1})$, $k = 1, \ldots, N$, starting from some $x_0 \in \mathbb{F}_p$, can not be contained inside of a short interval.

Visible points on curves: Given a plane curve $f(x, y) \equiv 0 \pmod p$, count the number of **visible** points, that is, points with $\gcd(x, y) = 1$.

Erdős-Graham Equation

Initial interval

Erdős-Graham (1980): Is it true that for any $\varepsilon > 0$ there exists $k(\varepsilon)$ such that any λ can be represented as

$$\frac{1}{x_1} + \ldots + \frac{1}{x_{k(\varepsilon)}} \equiv \lambda \pmod p$$

with $1 \le x_1, \ldots, x_{k(\varepsilon)} \le p^{\varepsilon}$?

Shparlinski (2002): True with $k(\varepsilon) = O(\varepsilon^{-3})$; using bounds of bilinear sums with inverses $u^{-1}v^{-1}$.
Glibichuk (2006): True with $k(\varepsilon) = O(\varepsilon^{-2})$; using methods of additive combinatorics.
Croot (2004): Generalisation to $\sum 1/x_i^m$; using methods of additive combinatorics.
Bourgain (2007): Generalisation to simultaneous $\sum 1/x_i^m$; using methods of additive combinatorics.

Idea

Let us take two expressions

$$\sum_{i=1}^{k} 1/x_i^m \qquad \text{and} \qquad \sum_{j=1}^{\ell} 1/y_j^m$$

Their sum and product are of the same type.

$$\Downarrow$$

Using the Sum-Product Theorem of *Bourgain, Katz & Tao* (2004), one can create a large (of cardinality at least $p^{0.500001}$) set of such sums.

After this exponential sums finish the job.

Warning: The argument is actually more subtle as the size of the terms also grows, while they must be up to p^{ε}.

Arbitrary intervals

Bourgain & Garaev (2012):

A variety of bounds on the number of solutions to

$$\frac{1}{x_1} + \ldots + \frac{1}{x_n} \equiv \lambda \pmod p, \qquad (x_1, \ldots, x_n) \in \mathfrak{C},$$

and on the cardinality of

$$\left\{ \frac{1}{x_1} + \ldots + \frac{1}{x_n} \ : \ (x_1, \ldots, x_n) \in \mathfrak{C} \right\}$$

<u>Generalised Erdős-Graham Problem:</u>
Is it true that for any $\varepsilon > 0$ there exists $\ell(\varepsilon)$ such that for any u, an arbitrary λ can be represented as

$$\frac{1}{x_1} + \ldots + \frac{1}{x_{\ell(\varepsilon)}} \equiv \lambda \pmod p$$

with $u + 1 \le x_1, \ldots, x_{\ell(\varepsilon)} \le u + p^{\varepsilon}$?

The case of $\varepsilon = 1/2$ is already hard.

Multiplicative Analogue

Points in small subgroups

Instead of distribution of points with components in short intervals, one can consider points with components in small subgroups of $\mathbb{F}_q^*$.

Poonen's Conjecture, Informally

Conjecture 4 *Under certain natural conditions, any point* $(x_1, \ldots, x_n)$ *on a variety* $\mathcal{V}$ *over* $\mathbb{F}_q$ *contains a component of multiplicative order at least* q^c*, where* $c > 0$ *depends only on some invariants of* $\mathcal{V}$ *(e.g., the dimension).*

Voloch (2007, 2010): Some results for plane curves (quantitatively much weaker).

Chang, Kerr, Shparlinski, Zannier (2013)

Theorem 5 *Assume that an absolutely irreducible over* $\mathbb{C}$ *variety* $\mathcal{V} \subseteq \mathbb{C}^n$ *is defined over* $\mathbb{Q}$. *Also assume that* $\mathcal{V}$ *does not contain a monomial curve:*

$$X^r Y^s - 1 \qquad \text{and} \qquad X^r - Y^s$$

Then there is a constant $C(\mathcal{V})$, *depending only on* $\mathcal{V}$ *such that for any* $\varepsilon > 0$, *for almost all primes* p, *for all but at most* $C(\mathcal{V})$ *points* $(x_1, \ldots, x_n) \in \mathcal{V}_p$ *on the reduction* $\mathcal{V}_p \subseteq \overline{\mathbb{F}}_p^n$ *of* $\mathcal{V}$ *modulo* p, *we have*

$$\max\{\mathrm{ord}\, x_1, \ldots, \mathrm{ord}\, x_n\} \geq p^{1/2n - \varepsilon}.$$

Amongst other tools, the proof uses an effective form of Hilbert's Nullstellensatz