A new and improved version of the circle method over function fields

Matthew Hase-Liu

Abstract

The circle method is a classical technique in analytic number theory, originally developed to count solutions to polynomial equations: the general principle is to express the counts in terms of exponential sums that are parametrized by a "circle". In the function field setting, these exponential sums are complete and obtaining good estimates reduces to bounding certain auxiliary singular loci, which can be analyzed easily after applying a weighted degeneration technique from Gröbner bases. As an application, this gives the first subexponential bound on the number of variables required in Birch's theorem over $\mathbb{F}_q(t)$.

Rational points on hypersurfaces

Let F be a smooth homogeneous degree d equation over $\mathbb{Q}$ in n variables.

Question 1. *How many solutions does $F = 0$ have?*

Of course there could be infinitely many, and this doesn't make too much sense.

Write $\vec{x} = (x_1, \ldots, x_n)$ with $x_i \in \mathbb{Z}$. Define the counting function

$$N_B(F) = \#\{\vec{x} \in \mathbb{Z}^n : F(\vec{x}) = 0 \text{ and } |x_i| \leq B\}$$

for any integer B.

We have $F(\vec{x}) = O(B^d)$ and a natural guess is that the values are "randomly" distributed, i.e. the probability that $F(\vec{x}) = 0$ is approximately CB^{-d}.

Birch showed that

$$N_B(F) \sim \underbrace{B^n}_{\text{available variables}} \times \underbrace{CB^{-d}}_{\text{probability that } F(\vec{x})=0} = CB^{n-d} \text{ as } B \to \infty$$

for $n > (d-1)2^d$, which is a special case of *Manin's conjecture*.

Over function fields?

Suppose $\mathbb{F}_q$ is a finite field. Let F be a homogeneous degree d equation over $\mathbb{F}_q[t]$ in n variables.

Write $\vec{x} = (x_1, \ldots, x_n)$ with $x_i \in \mathbb{F}_q[t]$. Define the counting function

$$N_e(F) = \#\{\vec{x} \in \mathbb{F}_q[t]^n : F(\vec{x}) = 0 \text{ and } \deg x_i \leq e\}$$

for any integer e. Here, B from earlier should be thought of as q^e.

A geometric viewpoint

Let $X \subset \mathbb{P}^{n-1}_{\mathbb{F}_q}$ be a smooth hypersurface of degree d, say defined by $F(x_1, \ldots, x_n) = 0$.

Geometers like to study the space X by studying the space of curves on X: A map from $\mathbb{P}^1$ to X of degree e can be thought of as a map $\mathbb{P}^1$ to $\mathbb{P}^{n-1}$ of degree e that factors through X. Even more explicitly, this is a tuple up to scaling $(f_1(u,v) : \cdots : f_n(u,v))$ of homogeneous polynomials with no common roots, with each f_i of degree e, and such that $F(f_1, \ldots, f_n)$ vanishes identically.

This space is called

$$\mathrm{Mor}_e\left(\mathbb{P}^1, X\right).$$

Observe that $N_e(F)$ is almost $\#\,\mathrm{Mor}_e(\mathbb{P}^1, X)(\mathbb{F}_q)$.

Question 2. *What's the dimension of* $\mathrm{Mor}_e(\mathbb{P}^1, X)$*?*

Naively, we have $n(e+1)$ parameters to choose coefficients for the f_i's, minus the $de+1$ conditions defined by the vanishing, minus one more for scaling:

$$n(e+1) - (de+1) - 1 = e(n-d) + n - 2.$$

Assuming this is correct, the Lang-Weil bounds tell us that

$$\#\,\mathrm{Mor}_e\left(\mathbb{P}^1, X\right)(\mathbb{F}_q) \sim \#\text{components} \times q^{e(n-d)+n-2} \text{ as } q \to \infty.$$

Notice that this looks very similar to the asymptotic in Birch's theorem! The key difference is that here we want $q \to \infty$ instead of $e \to \infty$.

Some results from the last 20 years

Arithmetic:

- Birch's theorem over $\mathbb{F}_q(t)$: Lee showed that

  $$N_e(F) \sim Cq^{e(n-d)} \text{ as } e \to \infty$$

  for $n > (d-1)2^d$ (and $p > d$).
- Waring's problem over $\mathbb{F}_q(t)$: Sawin showed a similar asymptotic when F is diagonal and $n > 4d - 6$ (but with q superexponential in d). Recently I improved this to $n > 2d$ (with q polynomial in d).

Geometry:

Let X be a hypersurface in $\mathbb{P}^{n-1}$ of degree d.

- Irreducibility and dimension of $\mathrm{Mor}_e(\mathbb{P}^1, X)$ for general X: Riedl–Yang for $n > d+2$.
- Singularities of $\mathrm{Mor}_e(\mathbb{P}^1, X)$ for arbitrary smooth X: Glas–HL for n exponential in d.
- Irreducibility and dimension of $\mathrm{Mor}_e(\mathbb{P}^2, X)$ for arbitrary smooth X: Browning–Yamagishi for $n > 2^d(d-1)(de+1)$.

Almost all of these use the circle method over $\mathbb{F}_q(t)$. I want to discuss an improved refinement that lets you improve upon a lot of the results above. I'll just describe two of them:

Theorem 3 ("Better Birch", HL)**.** *Suppose F cuts out a smooth hypersurface in $\mathbb{P}^{n-1}_{\mathbb{F}_q(t)}$. Let $p > d$, $q > (d-1)^{2n/(n-2d(d-1))}$, and $n > 2d(d-1)$. Then,*

$$N_e(F) \sim Cq^{e(n-d)} \text{ as } e \to \infty$$

for some explicit $C > 0$ that is a product of local densities.

Remark 4. For reference, by the Lang–Tsen theorem, $X(\mathbb{F}_q(t)) \neq \varnothing$ for $n > d^2$. However, there are smooth degree d hypersurfaces $X \subset \mathbb{P}^{d^2-1}_{\mathbb{F}_q(t)}$ with no $\mathbb{F}_q(t)$-point!

Theorem 5 ("Higher-dimensional circle method", Glas–HL)**.** *For any smooth hypersurface $X \subset \mathbb{P}^{n-1}_{\mathbb{C}}$ of degree d, the space $\mathrm{Mor}_e(\mathbb{P}^m, X)$ is irreducible and has the expected dimension for all $e \geq 1$, provided that $n > 4^{m+1}d^{2m}$.*

Overview of strategy

I'll focus on Birch's theorem.

(i) (Circle method) Express point-counts as a sum of exponential sums indexed by a "circle".

(ii) (Katz's complete sum estimates) Each $\alpha \in$"circle" gives an exponential sum that is complete, so (an improved version of) Katz gives us strong estimates in terms of the codimension of some auxiliary singular locus.

(iii) (Multiplication rank) Define a new invariant $r(\alpha)$ stratifying the circle. This is relatively natural to consider but doesn't seem to have appeared before.

(iv) (Weighted degeneration) Bound the exponential sums in terms of $r(\alpha)$ using an idea from computational algebraic geometry.

Point-counts as exponential sums

For simplicity, let's just assume F is defined over $\mathbb{F}_q$, i.e. is some homogeneous equation in n variables of degree d with coefficients in $\mathbb{F}_q$.

Let Poly_e denote the vector space of homogeneous polynomials in $\mathbb{F}_q[u, v]$ of degree e. The "circle" is defined as the space of linear functionals $\mathrm{Poly}^\vee_{de}$ (linear maps $\mathrm{Poly}_{de} \to \mathbb{F}_q$). For $\alpha \in \mathrm{Poly}^\vee_{de}$, we define the exponential sum associated to α as follows:

$$S(\alpha) \coloneqq \sum_{\vec{g} \in \mathrm{Poly}_e^n} \psi\left(\alpha\left(F\left(\vec{g}\right)\right)\right),$$

where ψ is a non-trivial additive character $\mathbb{F}_q \to \mathbb{C}^\times$.

Then the "igniting spark" of the circle method is the observation that

$$\begin{aligned}\sum_{\alpha \in \mathrm{Poly}_{de}^\vee} S(\alpha) &= \sum_{\vec{g} \in \mathrm{Poly}_e^n} \sum_{\alpha \in \mathrm{Poly}_{de}^\vee} \psi\left(\alpha\left(F\left(\vec{g}\right)\right)\right) = \sum_{\vec{g} \in \mathrm{Poly}_e^n} \begin{cases} 0 & \text{if } F\left(\vec{g}\right) \neq 0, \\ \#\,\mathrm{Poly}_{de}^\vee & \text{else} \end{cases} \\ &= \underbrace{\#\,\mathrm{Poly}_{de}^\vee}_{q^{de+1}} \#\left\{(g_1, \ldots, g_n) \in \mathrm{Poly}_e^n : F\left(g_1, \ldots, g_n\right) = 0\right\}.\end{aligned}$$

So

$$N_e(F) = q^{-de-1} \sum_{\alpha \in \mathrm{Poly}_{de}^\vee} S(\alpha).$$

Exponential sums via Katz

I will just state a general result by Katz (improved by combining some recent results by Wan and Zhang):

Theorem 6. *Let $N \geq 1$, ψ be a non-trivial additive character of $\mathbb{F}_q$, and $P \in \mathbb{F}_q[x_1, \ldots, x_N]$ have degree $d \geq 2$ with $p \nmid d$. Write P_d for the homogeneous part of P of degree d, and let $\mathrm{Sing}(P_d)$ denote the closed subscheme cut out by the first partial derivatives of P_d.*

Let $h = \mathrm{codim}_{\mathbb{A}^N} \mathrm{Sing}(P_d)$, $A_q = (1 - (d-1)/\sqrt{q})^{-1}$, and $\eta_q = 1/2 - \log_q(d-1)$.

If $q > (d-1)^2$, then

$$\left| \sum_{\vec{x} \in \mathbb{F}_q^N} \psi(P(\vec{x})) \right| \leq A_q q^{N - \eta_q h}.$$

In our case, we have $P_d = P = P_{\alpha,F}(\vec{g}) = \alpha(F(\vec{g}(t)))$, so

$$|S(\alpha)| \leq A_q q^{n(e+1) - \eta_q \,\mathrm{codim}_{\mathbb{A}^N} \mathrm{Sing}(P_{\alpha,F})}.$$

Multiplication rank

Definition 7. Let

$$C_\alpha : \mathrm{Poly}_e \to \mathrm{Poly}_{(d-1)e}^\vee$$

be the map $C_\alpha(h)(w) = \alpha(hw)$ and

$$r(\alpha) = \mathrm{rk}\, C_\alpha.$$

Remark 8. What does this mean? Here's a slogan:

$r(\alpha)$ **is the number of coefficients of each** g_i **that the phase** $\alpha(F(\vec{g}))$ **actually sees.**

Example 9. Consider $\alpha(f) = [t^e]f$, the coefficient of t^e with $t = v/u$. Take $d = 3$ and $e = 2$. In the monomial bases, the matrix of $C_\alpha : \mathrm{Poly}_2 \to \mathrm{Poly}_4^\vee$ has (i,j) entry $C_\alpha(t^i)(t^j) = \alpha(t^{i+j})$:

	1	t	t^2	t^3	t^4
1	$\alpha(1)$	$\alpha(t)$	$\alpha(t^2)$	$\alpha(t^3)$	$\alpha(t^4)$
t	$\alpha(t)$	$\alpha(t^2)$	$\alpha(t^3)$	$\alpha(t^4)$	$\alpha(t^5)$
t^2	$\alpha(t^2)$	$\alpha(t^3)$	$\alpha(t^4)$	$\alpha(t^5)$	$\alpha(t^6)$

Noting that $\alpha(t^m) = 1$ for $m = 2$ and 0 otherwise, this is

	1	t	t^2	t^3	t^4
1	0	0	1	0	0
t	0	1	0	0	0
t^2	1	0	0	0	0

and this has maximal rank $e + 1 = 3$.

The key observation is as follows:

Proposition 10.

$$\mathrm{codim}_{\mathbb{A}^N} \mathrm{Sing}(P_{\alpha,F}) \geq n \max\left(\left\lfloor \frac{r(\alpha)}{d-1} \right\rfloor - 1, 0\right).$$

Remark 11. Where does $r(\alpha)$ come from? Write $g_i = \sum_j a_{ij} t^j$. By the chain rule, we have

$$\frac{\partial P_{\alpha,F}}{\partial a_{ij}} = \alpha(t^j(\partial_i F)(\vec{g})) = C_\alpha(t^j)(\partial_i F(\vec{g})).$$

Then $\vec{g}$ is in the singular locus exactly when every functional in $\mathrm{im}\, C_\alpha$ kills $(\partial_i F)(\vec{g})$. This image has dimension $r(\alpha)$, so the singular locus is cut out by $r(\alpha)$ linear conditions on each $(\partial_i F)(\vec{g})$. If these were actually independent, we would get a codimension of $nr(\alpha)$. It turns out if you're careful you can actually get $nr(\alpha)/(d-1)$.

Example 12. Let's see this in the previous example where $F = x_1^d + \cdots + x_n^d$ with $d = 3$, $e = 2$, and $\alpha(f) = [t^e]f$.

Write $g_i = a_{i0} + a_{i1}t + a_{i2}t^2$. Then,

$$\frac{\partial P_{\alpha,F}}{\partial a_{ij}} = 3\alpha(t^j g_i^2) = 3[t^{2-j}](g_i^2),$$

so $\vec{g}$ is singular exactly when $g_i^2 \equiv 0 \bmod t^3$ for all i. Note that $3/2 = (e+1)/(d-1) = r(\alpha)/(d-1)$, which is what appears in the proposition.

For α with $r(\alpha) \leq e$, we can actually compute the sums exactly! So the trickiest part of the argument is when $r(\alpha) = e + 1$ (note we always have $r(\alpha) \leq e + 1$), where we have the least control over α. However, the proposition gives us the best bounds on the exponential sum in this case! The main term is of the form $Cq^{e(n-d)}$, so we really want the part of

$$N_e(F) = q^{-de-1} \sum_{\alpha \in \mathrm{Poly}_{de}^\vee} S(\alpha)$$

where $r(\alpha) = e + 1$ to be $o(q^{e(n-d)})$. Indeed,

$$q^{-de-1} \sum_{r(\alpha)=e+1} |S(\alpha)| \le q^{-de-1} \cdot \underbrace{q^{de+1}}_{\text{trivial bound}} \cdot A_q q^{n(e+1)-\eta_q h}$$

with

$$h \ge n\left(\left\lfloor \frac{e+1}{d-1} \right\rfloor - 1\right).$$

Comparing the exponents of q, we want

$$\eta_q h - de \to \infty \text{ as } e \to \infty.$$

Since h is at worst approximately $n(e+1)/(d-1)$, this holds as soon as

$$\eta_q \frac{n}{d-1} > d,$$

which gives

$$n > 2d(d-1) \text{ with } q > (d-1)^{2n/(n-2d(d-1))}.$$

Weighted degeneration

How is the proposition proved? It turns out to use a nice trick from computational algebraic geometry. To demonstrate this, I'll just continue the example from earlier, where we got $g_i^2 \equiv 0 \bmod t^3$ (which gives $t^2 | g_i$, so the codimension is $2n$).

Let's compute it a different way:

Example 13. Since F is diagonal, the Jacobian ideal J is generated by the partials of $P_{\alpha,F}$:

$$[t^0](g_i^2) = a_{i0}^2, [t^1](g_i^2) = 2a_{i0}a_{i1}, [t^2](g_i^2) = 2a_{i0}a_{i2} + a_{i1}^2.$$

Step 1: Degenerate

Let's give a_{i1} weight 1 and a_{i0} and a_{i2} weight 0. Replacing each generator by its "initial form" (the sum of its terms of largest weight), we get

$$\operatorname{in}_w J \supset (a_{i0}^2, a_{i0}a_{i1}, a_{i1}^2)_{1 \le i \le n}.$$

Moreover, it is a standard fact that (since J is homogeneous)

$$\operatorname{ht} \operatorname{in}_w J = \operatorname{ht} J.$$

Step 2: Count

A monomial vanishes exactly when one of its variables does, so the zero set of a monomial ideal is a union of coordinate subspaces, and its codimension is the fewest variables meeting every

generator. For each i there are $3 = r(\alpha)$ monomials, and each variable lies in at most $2 = d - 1$ of them, so at least $3/2$ (rounded up to 2) variables are needed.

Observe that we have

$$\operatorname{codim} \operatorname{Sing}(P_{\alpha,F}) = \operatorname{ht} J = \operatorname{ht} \operatorname{in}_w J \geq \operatorname{ht}(a_{i0}^2, a_{i0}a_{i1}, a_{i1}^2)_{1 \leq i \leq n} = 2n.$$

Beyond this example, what happens in general? The equations are messier so we first have to make them look nicer (do some kind of row reduction), and choose a weight that works more generally and picks out a single monomial.