Polynomials over Finite Fields: When is there a polynomial of degree d vanishing on a given set of points?

Nathan Kaplan

Yale University

March 14, 2014

The Finite Field Kakeya Conjecture

Theorem (Dvir, Conjecture of Wolff)

Let $E \subset \mathbb{F}_q^n$ be a set containing a line in every direction. Then $|E| \geq c_n q^n$ where c_n is a constant independent of q.

The Finite Field Kakeya Conjecture

Theorem (Dvir, Conjecture of Wolff)

Let $E \subset \mathbb{F}_q^n$ be a set containing a line in every direction. Then $|E| \geq c_n q^n$ where c_n is a constant independent of q.

Idea: A set having this special structure can't be 'too small'.

The Polynomial Method

1. Start with a problem about points in a vector space.
2. Find the lowest degree polynomial vanishing on these points.
3. Use this polynomial to attack the problem.

The Polynomial Method

1. Start with a problem about points in a vector space.
2. Find the lowest degree polynomial vanishing on these points.
3. Use this polynomial to attack the problem.

1. If a set is 'small' we can find a low-degree polynomial vanishing on it.
2. If no polynomial vanishes on the set, then the set is 'large'.

Zero Sets of Polynomials

1. Given a set, when does a low-degree polynomial vanish on it? Equivalently, when is a set of points contained in a variety of low-degree?

Zero Sets of Polynomials

1. Given a set, when does a low-degree polynomial vanish on it? Equivalently, when is a set of points contained in a variety of low-degree?

2. Questions about zeros of polynomials and points on varieties tend to have nicer answers in projective space than in affine space. Even if you're only concerned about problems in $\mathbb{F}_q^n$, there is something to be gained by working projectively.

Interpolation and Schwartz-Zippel

Lemma

Let $d \geq 0$.

1. *If $P \in \mathbb{F}_q[X]$ is a nontrivial polynomial of degree at most d, then P vanishes on at most d points in $\mathbb{F}_q$.*
2. *If $E \subset \mathbb{F}_q$ is a set of size at most d, then there is a nontrivial polynomial of degree at most d vanishing on E.*

Interpolation and Schwartz-Zippel

Lemma

Let $d \geq 0$.

1. *If $P \in \mathbb{F}_q[X]$ is a nontrivial polynomial of degree at most d, then P vanishes on at most d points in $\mathbb{F}_q$.*
2. *If $E \subset \mathbb{F}_q$ is a set of size at most d, then there is a nontrivial polynomial of degree at most d vanishing on E.*

Idea of the proof: Let $P(X) = \prod_{p \in E}(X - p)$.
Alternatively, polynomials of degree at most d form a vector space of dimension $d + 1$ (spanned by $1, X, X^2, \ldots X^d$). The evaluation map,

$$f \to (f(p_1), \ldots, f(p_{|E|})),$$

is linear. We choose any polynomial in the kernel of this map.

Interpolation and Schwartz-Zippel

Lemma

1. *(Schwartz-Zippel) Let* $n \geq 1$ *and* $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ *of degree at most* d*. If* P *does not vanish entirely, then* P *vanishes on at most* dq^{n-1} *points.*
2. *If* $E \subseteq \mathbb{F}_q^n$ *with* $|E| < \binom{d+n}{d}$*, then there is a nonzero polynomial of degree at most* d *vanishing on* E*.*

Interpolation and Schwartz-Zippel

Lemma

1. *(Schwartz-Zippel) Let $n \geq 1$ and $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree at most d. If P does not vanish entirely, then P vanishes on at most dq^{n-1} points.*
2. *If $E \subseteq \mathbb{F}_q^n$ with $|E| < \binom{d+n}{d}$, then there is a nonzero polynomial of degree at most d vanishing on E.*

Idea of the proof: Polynomials of degree at most d form a vector space of dimension at most $\binom{d+n}{d}$. Evaluation again gives a linear map.

Interpolation and Schwartz-Zippel

Lemma

1. *(Schwartz-Zippel) Let $n \geq 1$ and $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree at most d. If P does not vanish entirely, then P vanishes on at most dq^{n-1} points.*
2. *If $E \subseteq \mathbb{F}_q^n$ with $|E| < \binom{d+n}{d}$, then there is a nonzero polynomial of degree at most d vanishing on E.*

Idea of the proof: Polynomials of degree at most d form a vector space of dimension at most $\binom{d+n}{d}$. Evaluation again gives a linear map.

This is not the whole story. If $n = 2$ and $d = 3$, when is there a cubic $F(X, Y)$ vanishing on a set of points?

Interpolation and Schwartz-Zippel

Lemma

1. *(Schwartz-Zippel) Let $n \geq 1$ and $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree at most d. If P does not vanish entirely, then P vanishes on at most dq^{n-1} points.*
2. *If $E \subseteq \mathbb{F}_q^n$ with $|E| < \binom{d+n}{d}$, then there is a nonzero polynomial of degree at most d vanishing on E.*

Idea of the proof: Polynomials of degree at most d form a vector space of dimension at most $\binom{d+n}{d}$. Evaluation again gives a linear map.

This is not the whole story. If $n = 2$ and $d = 3$, when is there a cubic $F(X, Y)$ vanishing on a set of points?
Yes, when $|E| \leq 9$, no when $|E| > 2q$.

Affine Varieties

Definition

An affine variety is the common zero set of a collection of polynomials. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. *Then* $V(f) = \{p \in \mathbb{F}_q^n \mid f(p) = 0\}$.

Affine Varieties

Definition

An affine variety is the common zero set of a collection of polynomials. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. *Then* $V(f) = \{p \in \mathbb{F}_q^n \mid f(p) = 0\}$.

Same idea with more polynomials: Given $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$$V(f_1, \ldots, f_m) = \{f_1(p) = \cdots = f_m(p) = 0\}.$$

Affine Varieties

Definition

An affine variety is the common zero set of a collection of polynomials. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. *Then* $V(f) = \{p \in \mathbb{F}_q^n \mid f(p) = 0\}$.

Same idea with more polynomials: Given $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$$V(f_1, \ldots, f_m) = \{f_1(p) = \cdots = f_m(p) = 0\}.$$

If $m = 1$, $V(f)$ is a hypersurface. Schwartz-Zippel says that an affine hypersurface of degree at most d contains at most dq^{n-1} points.

Affine Varieties

Definition

An affine variety is the common zero set of a collection of polynomials. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. *Then* $V(f) = \{p \in \mathbb{F}_q^n \mid f(p) = 0\}$.

Same idea with more polynomials: Given $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$$V(f_1, \ldots, f_m) = \{f_1(p) = \cdots = f_m(p) = 0\}.$$

If $m = 1$, $V(f)$ is a hypersurface. Schwartz-Zippel says that an affine hypersurface of degree at most d contains at most dq^{n-1} points. Interpolation says that every small set of points in contained in a low-degree hypersurface.

Projective Space

Definition

The projective space $\mathbb{P}^n(\mathbb{F}_q)$ *consists of all* $(x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1} \setminus (0, \ldots, 0)$ *where two elements are equivalent if one is a scalar multiple of the other, that is for any* $\alpha \in \mathbb{F}_q^*$,

$$[x_0 : x_1 : \cdots : x_n] \sim [\alpha x_0 : \alpha x_1 : \cdots : \alpha x_n].$$

Projective Space

Definition

The projective space $\mathbb{P}^n(\mathbb{F}_q)$ *consists of all* $(x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1} \setminus (0, \ldots, 0)$ *where two elements are equivalent if one is a scalar multiple of the other, that is for any* $\alpha \in \mathbb{F}_q^*$,

$$[x_0 : x_1 : \cdots : x_n] \sim [\alpha x_0 : \alpha x_1 : \cdots : \alpha x_n].$$

Example: $\mathbb{P}^1(\mathbb{F}_q)$: $[1 : 0] = (1, 0), (2, 0), \ldots, (a_{q-1}, 0)$,
$[1 : 1] = (1, 1), (2, 2), \ldots$.
This has $q + 1$ points, $[1 : a]$ for $a \in \mathbb{F}_q$ and $[0 : 1]$.

Projective Space

Definition

The projective space $\mathbb{P}^n(\mathbb{F}_q)$ *consists of all* $(x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1} \setminus (0, \ldots, 0)$ *where two elements are equivalent if one is a scalar multiple of the other, that is for any* $\alpha \in \mathbb{F}_q^*$,

$$[x_0 : x_1 : \cdots : x_n] \sim [\alpha x_0 : \alpha x_1 : \cdots : \alpha x_n].$$

Example: $\mathbb{P}^1(\mathbb{F}_q)$: $[1 : 0] = (1, 0), (2, 0), \ldots, (a_{q-1}, 0)$,
$[1 : 1] = (1, 1), (2, 2), \ldots$.
This has $q + 1$ points, $[1 : a]$ for $a \in \mathbb{F}_q$ and $[0 : 1]$.

Example: $\mathbb{P}^n(\mathbb{F}_q)$ has $\frac{q^{n+1}-1}{q-1}$ points

$$[1 : a_1 : \cdots : a_n], [0 : 1 : a_2 : \cdots : a_n], \ldots, [0 : \cdots : 0 : 1],$$

one for each one-dimensional subspace of $\mathbb{F}_q^{n+1}$.

Projective Varieties

Definition

A projective variety is the common zero set of a collection of homogeneous polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$. *We let*

$$V(f_1, \ldots, f_m) = \{p \in \mathbb{P}^n(\mathbb{F}_q) \mid f_1(p) = \cdots = f_m(p) = 0\}.$$

Projective Varieties

Definition

A projective variety is the common zero set of a collection of homogeneous polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$. *We let*

$$V(f_1, \ldots, f_m) = \{p \in \mathbb{P}^n(\mathbb{F}_q) \mid f_1(p) = \cdots = f_m(p) = 0\}.$$

Why homogenous? Example: $\mathbb{P}^1(\mathbb{F}_3)$, $f = x + 1$. Then
$f(2, 0) = 0$, $f(1, 0) \neq 0$ but $[1 : 0] = [2 : 0]$.
If a homogeneous polynomial vanishes at $(x_0, \ldots, x_n)$ then it vanishes at $(\alpha x_0, \ldots, \alpha x_n)$ for any $\alpha \in \mathbb{F}_q^*$.

Projective Varieties

Definition

A projective variety is the common zero set of a collection of homogeneous polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$. *We let*

$$V(f_1, \ldots, f_m) = \{p \in \mathbb{P}^n(\mathbb{F}_q) \mid f_1(p) = \cdots = f_m(p) = 0\}.$$

Why homogenous? Example: $\mathbb{P}^1(\mathbb{F}_3)$, $f = x + 1$. Then
$f(2, 0) = 0$, $f(1, 0) \neq 0$ but $[1 : 0] = [2 : 0]$.
If a homogeneous polynomial vanishes at $(x_0, \ldots, x_n)$ then it vanishes at $(\alpha x_0, \ldots, \alpha x_n)$ for any $\alpha \in \mathbb{F}_q^*$.

Theorem (Serre, Tsfasman)

Let $F \in \mathbb{F}_q[x_0, \ldots, x_n]$ *be homogeneous of degree* d. *Then* $|V(F)| \leq dq^{n-1} + \frac{q^{n-1}-1}{q-1}$, *where equality holds if and only if* F *factors as a product of linear forms that intersect in a common* $\mathbb{P}^{n-2}$.

Example: $n = d = 2$, then $|V(F)| \leq 2q + 1$.

Projective Varieties

We have seen that $\mathbb{P}^2(\mathbb{F}_q)$ has points $[1 : a : b]$, $[0 : 1 : a]$: $[0 : 0 : 1]$. It has lines $\{\alpha x + \beta y + \gamma z = 0\}$. This is the line defined by $[\alpha : \beta : \gamma]$, since (α, β, γ) and $(2\alpha, 2\beta, 2\gamma)$ define the same line.

Projective Varieties

We have seen that $\mathbb{P}^2(\mathbb{F}_q)$ has points $[1 : a : b]$, $[0 : 1 : a]$: $[0 : 0 : 1]$. It has lines $\{\alpha x + \beta y + \gamma z = 0\}$. This is the line defined by $[\alpha : \beta : \gamma]$, since (α, β, γ) and $(2\alpha, 2\beta, 2\gamma)$ define the same line.

Any two distinct lines in $\mathbb{P}^2(\mathbb{F}_q)$ intersect at a unique point. This is not true in $\mathbb{F}_q^2$ since we have the 'parallel lines' $x + y = 1$ and $x + y = 2$. These 'intersect at infinity'.

Projective Varieties

We have seen that $\mathbb{P}^2(\mathbb{F}_q)$ has points $[1 : a : b]$, $[0 : 1 : a]$: $[0 : 0 : 1]$.
It has lines $\{\alpha x + \beta y + \gamma z = 0\}$. This is the line defined by $[\alpha : \beta : \gamma]$, since (α, β, γ) and $(2\alpha, 2\beta, 2\gamma)$ define the same line.

Any two distinct lines in $\mathbb{P}^2(\mathbb{F}_q)$ intersect at a unique point. This is not true in $\mathbb{F}_q^2$ since we have the 'parallel lines' $x + y = 1$ and $x + y = 2$.
These 'intersect at infinity'.
In general, finding the intersection comes down to solving the matrix equation:

$$\begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Projective Varieties

We have seen that $\mathbb{P}^2(\mathbb{F}_q)$ has points $[1 : a : b]$, $[0 : 1 : a]$: $[0 : 0 : 1]$.
It has lines $\{\alpha x + \beta y + \gamma z = 0\}$. This is the line defined by $[\alpha : \beta : \gamma]$, since (α, β, γ) and $(2\alpha, 2\beta, 2\gamma)$ define the same line.

Any two distinct lines in $\mathbb{P}^2(\mathbb{F}_q)$ intersect at a unique point. This is not true in $\mathbb{F}_q^2$ since we have the 'parallel lines' $x + y = 1$ and $x + y = 2$. These 'intersect at infinity'.
In general, finding the intersection comes down to solving the matrix equation:

$$\begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

The dual projective plane comes from exchanging points and lines. More generally, we can exchange points and hypersurfaces in $\mathbb{P}^n(\mathbb{F}_q)$, and dimension k and $n - k$ subspaces of $\mathbb{F}_q^{n+1}$.

Automorphisms

The group $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$ acts on $\mathbb{P}^n(\mathbb{F}_q)$ by 'change of basis':

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which sends $[1:0:0]$ to $[a_1 : b_1 : c_1]$, $[0:1:0]$ to $[a_2 : b_2 : c_2]$, $[0:0:1]$ to $[a_3 : b_3 : c_3]$.

Automorphisms

The group $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$ acts on $\mathbb{P}^n(\mathbb{F}_q)$ by 'change of basis':

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which sends $[1:0:0]$ to $[a_1 : b_1 : c_1]$, $[0:1:0]$ to $[a_2 : b_2 : c_2]$, $[0:0:1]$ to $[a_3 : b_3 : c_3]$.
This is a bijection on points and is invertible, and therefore is an automorphism. In fact, every automorphism arises in this way.

Automorphisms

The group $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$ acts on $\mathbb{P}^n(\mathbb{F}_q)$ by 'change of basis':

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which sends $[1:0:0]$ to $[a_1 : b_1 : c_1]$, $[0:1:0]$ to $[a_2 : b_2 : c_2]$, $[0:0:1]$ to $[a_3 : b_3 : c_3]$.
This is a bijection on points and is invertible, and therefore is an automorphism. In fact, every automorphism arises in this way.
There exists an automorphism of $\mathbb{P}^1$ that sends any three points to $[1:0]$, $[0:1]$, $[1:1]$. This involves solving

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Automorphisms

Automorphisms act on varieties and the corresponding polynomials as well.

Automorphisms

Automorphisms act on varieties and the corresponding polynomials as well. Let $p \equiv 3 \pmod 4$. Every quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_p)$ is equivalent to either:

1. x^2 (double root),
2. $x^2 - y^2$ (two rational roots),
3. $x^2 + y^2$ (two Galois-conjugate roots in $\{\mathbb{F}_{p^2} \setminus \mathbb{F}_p\}$, $[1 : \pm i]$).

Automorphisms

Automorphisms act on varieties and the corresponding polynomials as well. Let $p \equiv 3 \pmod 4$. Every quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_p)$ is equivalent to either:

1. x^2 (double root),
2. $x^2 - y^2$ (two rational roots),
3. $x^2 + y^2$ (two Galois-conjugate roots in $\{\mathbb{F}_{p^2} \setminus \mathbb{F}_p\}$, $[1 : \pm i]$).

In $\mathbb{P}^2(\mathbb{F}_q)$ every conic is either:

1. A double line ($q + 1$ points)
2. The product of two rational lines ($2q + 1$ points)
3. The product of two Galois-conjugate lines (1 point)
4. A smooth conic ($q + 1$ points).

Automorphisms

Automorphisms act on varieties and the corresponding polynomials as well. Let $p \equiv 3 \pmod 4$. Every quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_p)$ is equivalent to either:

1. x^2 (double root),
2. $x^2 - y^2$ (two rational roots),
3. $x^2 + y^2$ (two Galois-conjugate roots in $\{\mathbb{F}_{p^2} \setminus \mathbb{F}_p\}$, $[1 : \pm i]$).

In $\mathbb{P}^2(\mathbb{F}_q)$ every conic is either:

1. A double line ($q + 1$ points)
2. The product of two rational lines ($2q + 1$ points)
3. The product of two Galois-conjugate lines (1 point)
4. A smooth conic ($q + 1$ points).

Note that $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + |\mathbb{P}^{n-1}(\mathbb{F}_q)|$.
The first term comes from points $[1 : a_1 : \cdots : a_n]$ and the second is the 'hyperplane at infinity', $\{x_0 = 0\}$.

Automorphisms

Automorphisms act on varieties and the corresponding polynomials as well.
Let $p \equiv 3 \pmod 4$. Every quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_p)$ is equivalent to either:

1. x^2 (double root),
2. $x^2 - y^2$ (two rational roots),
3. $x^2 + y^2$ (two Galois-conjugate roots in $\{\mathbb{F}_{p^2} \setminus \mathbb{F}_p\}$, $[1 : \pm i]$).

In $\mathbb{P}^2(\mathbb{F}_q)$ every conic is either:

1. A double line ($q + 1$ points)
2. The product of two rational lines ($2q + 1$ points)
3. The product of two Galois-conjugate lines (1 point)
4. A smooth conic ($q + 1$ points).

Note that $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + |\mathbb{P}^{n-1}(\mathbb{F}_q)|$.
The first term comes from points $[1 : a_1 : \cdots : a_n]$ and the second is the 'hyperplane at infinity', $\{x_0 = 0\}$.
$\mathbb{P}^n$ is covered by 'affine pieces' $\{x_0 = 1\}, \{x_1 = 1\}, \ldots, \{x_n = 1\}$.

Segre's Theorem

What is the maximum number of points in $\mathbb{F}_q^2$, no three on a line?

Segre's Theorem

What is the maximum number of points in $\mathbb{F}_q^2$, no three on a line?

Theorem (Segre)

Suppose q is odd. The maximum number of points in $\mathbb{F}_q^2$ no three on a line is $q+1$. In fact, the maximum number of points in $\mathbb{P}^2(\mathbb{F}_q)$ no three on a line is $q+1$, where equality holds if and only if the points are the rational points of a smooth conic.

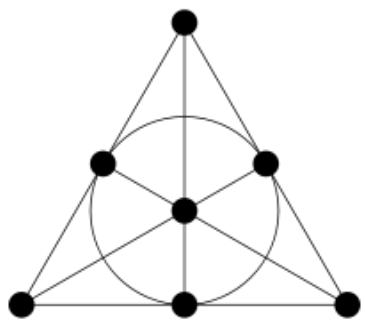
Segre's Theorem

What is the maximum number of points in $\mathbb{F}_q^2$, no three on a line?

Theorem (Segre)

Suppose q is odd. The maximum number of points in $\mathbb{F}_q^2$ no three on a line is $q+1$. In fact, the maximum number of points in $\mathbb{P}^2(\mathbb{F}_q)$ no three on a line is $q+1$, where equality holds if and only if the points are the rational points of a smooth conic.

This is false in characteristic 2:



The complement of a line gives $4 = q+2$ points, no three on a line, 'hyperoval'. Classifying hyperovals in $\mathbb{P}^2(\mathbb{F}_{2^m})$ is an active area of research.

Conics

Let us use this projective result to understand the affine case. Choose a smooth conic in $\mathbb{P}^2$, $f(x, y, z)$ such that $f(x, y, z)$ has no $\mathbb{F}_q$-rational points on the line at infinity $[0 : 1 : a]$.

Conics

Let us use this projective result to understand the affine case. Choose a smooth conic in $\mathbb{P}^2$, $f(x, y, z)$ such that $f(x, y, z)$ has no $\mathbb{F}_q$-rational points on the line at infinity $[0 : 1 : a]$.

This implies $f(0, y, z)$ is irreducible on $\mathbb{P}^1(\mathbb{F}_q)$. This gives $q + 1$ points, all in $\mathbb{F}_q^2 \subset \mathbb{P}^2(\mathbb{F}_q)$, no three on a line.

Conics

Let us use this projective result to understand the affine case. Choose a smooth conic in $\mathbb{P}^2$, $f(x, y, z)$ such that $f(x, y, z)$ has no $\mathbb{F}_q$-rational points on the line at infinity $[0 : 1 : a]$.

This implies $f(0, y, z)$ is irreducible on $\mathbb{P}^1(\mathbb{F}_q)$. This gives $q + 1$ points, all in $\mathbb{F}_q^2 \subset \mathbb{P}^2(\mathbb{F}_q)$, no three on a line.

For example, let us choose 4 points, no three on a line, in $\mathbb{F}_q^2$: $(0, 0), (1, 0), (0, 1), (1, 1)$. In fact, there is an automorphism of $\mathbb{P}^2(\mathbb{F}_q)$ taking any four such points to these four (exercise).

Conics

Let us use this projective result to understand the affine case. Choose a smooth conic in $\mathbb{P}^2$, $f(x, y, z)$ such that $f(x, y, z)$ has no $\mathbb{F}_q$-rational points on the line at infinity $[0 : 1 : a]$.

This implies $f(0, y, z)$ is irreducible on $\mathbb{P}^1(\mathbb{F}_q)$. This gives $q + 1$ points, all in $\mathbb{F}_q^2 \subset \mathbb{P}^2(\mathbb{F}_q)$, no three on a line.

For example, let us choose 4 points, no three on a line, in $\mathbb{F}_q^2$: $(0, 0), (1, 0), (0, 1), (1, 1)$. In fact, there is an automorphism of $\mathbb{P}^2(\mathbb{F}_q)$ taking any four such points to these four (exercise).

This gives projective points $[1 : 0 : 0], [1 : 1 : 0], [1 : 0 : 1], [1 : 1 : 1]$. Let us try to write down a smooth conic vanishing on these points. The conic is given by

$$f(x, y, z) = a_0x^2 + a_1xy + a_2y^2 + a_3xz + a_4yz + a_5z^2.$$

Conics

The condition that f vanishes on these projective points implies that $a_0 = a_1 + a_2 = a_3 + a_5 = a_1 + a_2 + a_3 + a_4 + a_5 = 0$, so $a_4 = 0$. This gives

$$f(x, y, z) = axy - ay^2 + bxz - bz^2.$$

Definition

A singular point of a curve $\{F(x, y, z) = 0\} \subset \mathbb{P}^2$ *is a point* P *where* $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$.

These are exactly the points without a unique tangent line.

Conics

The condition that f vanishes on these projective points implies that $a_0 = a_1 + a_2 = a_3 + a_5 = a_1 + a_2 + a_3 + a_4 + a_5 = 0$, so $a_4 = 0$. This gives

$$f(x, y, z) = axy - ay^2 + bxz - bz^2.$$

Definition

A singular point of a curve $\{F(x, y, z) = 0\} \subset \mathbb{P}^2$ *is a point* P *where* $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$.

These are exactly the points without a unique tangent line.
We have

$$\begin{aligned} \frac{\partial F}{\partial x} &= ay + bz \\ \frac{\partial F}{\partial y} &= ax - 2ay \\ \frac{\partial F}{\partial z} &= bx - 2bz \end{aligned}$$

Conics

These are three lines. When do they intersect at a common point? We want to find solutions to

$$\begin{pmatrix} 0 & a & b \\ a & -2a & 0 \\ b & 0 & -2b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Conics

These are three lines. When do they intersect at a common point? We want to find solutions to

$$\begin{pmatrix} 0 & a & b \\ a & -2a & 0 \\ b & 0 & -2b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

The determinant of this matrix is $2ab(a+b)$. Choose $a = b = 1$. This gives a smooth conic which passes through $q+1$ points in the affine plane $x = 1$, no three of which lie on a line, and including our four chosen points:

$$f(x, y, z) = x(y+z) - (y^2 + z^2).$$

Points on a line

How do we know when three points lie on a line?

$$\begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Do there exist α, β, γ such that these points lie on $\alpha x + \beta y + \gamma z = 0$?
Is this determinant zero?

Points on a line

How do we know when three points lie on a line?

$$\begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Do there exist α, β, γ such that these points lie on $\alpha x + \beta y + \gamma z = 0$?
Is this determinant zero?

Any five points lie on a conic. How do we know if 6 points do?

Points on a line

How do we know when three points lie on a line?

$$\begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Do there exist α, β, γ such that these points lie on $\alpha x + \beta y + \gamma z = 0$? Is this determinant zero?

Any five points lie on a conic. How do we know if 6 points do? Form the 6×6 matrix where each point $[a : b : c]$ gives a column with entries $a^2, ab, b^2, ac, bc, c^2$. Is the determinant zero?

Quadric Hypersurfaces

In $\mathbb{P}^3(\mathbb{F}_q)$ there are two non-isomorphic quadric hypersurfaces:

1. Plus Quadric: Isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ given by $XY = ZW$.

Quadric Hypersurfaces

In $\mathbb{P}^3(\mathbb{F}_q)$ there are two non-isomorphic quadric hypersurfaces:

1. Plus Quadric: Isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ given by $XY = ZW$. Idea: Let $[x_0 : x_1]$ be the coordinates of the first $\mathbb{P}^1$ and $[y_0 : y_1]$ be the coordinates of the second.

Quadric Hypersurfaces

In $\mathbb{P}^3(\mathbb{F}_q)$ there are two non-isomorphic quadric hypersurfaces:

1. Plus Quadric: Isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ given by $XY = ZW$. Idea: Let $[x_0 : x_1]$ be the coordinates of the first $\mathbb{P}^1$ and $[y_0 : y_1]$ be the coordinates of the second. Now let

$$X = x_0y_0, \ Y = x_1y_1, \ Z = x_0y_1, \ W = x_1y_1$$

and note that $XY = ZW$. This has $(q+1)^2$ points.

Quadric Hypersurfaces

In $\mathbb{P}^3(\mathbb{F}_q)$ there are two non-isomorphic quadric hypersurfaces:

1. Plus Quadric: Isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ given by $XY = ZW$. Idea: Let $[x_0 : x_1]$ be the coordinates of the first $\mathbb{P}^1$ and $[y_0 : y_1]$ be the coordinates of the second. Now let

$$X = x_0y_0, \ Y = x_1y_1, \ Z = x_0y_1, \ W = x_1y_1$$

   and note that $XY = ZW$. This has $(q+1)^2$ points.
2. Minus Quadric: Example $XY = f_2(Z, W)$, where $f_2(Z, W)$ is an irreducible quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_q)$. This has $q^2 + 1$ points.

Quadric Hypersurfaces

In $\mathbb{P}^3(\mathbb{F}_q)$ there are two non-isomorphic quadric hypersurfaces:

1. Plus Quadric: Isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ given by $XY = ZW$. Idea: Let $[x_0 : x_1]$ be the coordinates of the first $\mathbb{P}^1$ and $[y_0 : y_1]$ be the coordinates of the second. Now let

$$X = x_0y_0, \ Y = x_1y_1, \ Z = x_0y_1, \ W = x_1y_1$$

   and note that $XY = ZW$. This has $(q+1)^2$ points.
2. Minus Quadric: Example $XY = f_2(Z, W)$, where $f_2(Z, W)$ is an irreducible quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_q)$. This has $q^2 + 1$ points.

Understanding quadric hypersurfaces is equivalent to understanding quadratic forms over finite fields.

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.
2. Plane Cubic Curves and Inflection Points.

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.
2. Plane Cubic Curves and Inflection Points.
3. Rational Points on Smooth Varieties: Hasse, Hasse-Weil, Fixed Points of Frobenius.

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.
2. Plane Cubic Curves and Inflection Points.
3. Rational Points on Smooth Varieties: Hasse, Hasse-Weil, Fixed Points of Frobenius.
4. Size of the Zero Set- Chevalley-Warning, Ax-Katz...

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.
2. Plane Cubic Curves and Inflection Points.
3. Rational Points on Smooth Varieties: Hasse, Hasse-Weil, Fixed Points of Frobenius.
4. Size of the Zero Set- Chevalley-Warning, Ax-Katz...
5. Proof of Finite Field Kakeya. Subsequent Improvements: The Method of Multiplicities. Constructions of Kakeya Sets.

What's next?

1. Bezout's Theorem for Curves in $\mathbb{P}^2$.
2. Plane Cubic Curves and Inflection Points.
3. Rational Points on Smooth Varieties: Hasse, Hasse-Weil, Fixed Points of Frobenius.
4. Size of the Zero Set- Chevalley-Warning, Ax-Katz...
5. Proof of Finite Field Kakeya. Subsequent Improvements: The Method of Multiplicities. Constructions of Kakeya Sets.
6. 'Flexy' varieties.

PART TWO

Bezout's Theorem for Plane Curves

Theorem

Let C and D be curves of degree m and n that do not contain a common component. Then C and D intersect in exactly mn points counted with multiplicity.

This implies that two curves that intersect in more than mn points must share a component.

Note that affine curves intersect in at most mn points, often fewer due to intersections on the line at infinity.

Bezout's Theorem for Plane Curves

Theorem

Let C and D be curves of degree m and n that do not contain a common component. Then C and D intersect in exactly mn points counted with multiplicity.

This implies that two curves that intersect in more than mn points must share a component.

Note that affine curves intersect in at most mn points, often fewer due to intersections on the line at infinity.

There is also a version of Bezout's theorem for intersections of hypersurfaces. If hypersurfaces $V(F_1), \ldots, V(F_m)$ intersect in a finite number of points, then this number is at most the product of the degrees.

Bezout's Theorem for Plane Curves

Example: A line intersects a degree d curve in exactly d points. A line intersecting in more than d points must be contained in that curve. More generally, a line that intersects a degree d hypersurface in more than d points must be contained in that hypersurface.

Bezout's Theorem for Plane Curves

Example: A line intersects a degree d curve in exactly d points. A line intersecting in more than d points must be contained in that curve. More generally, a line that intersects a degree d hypersurface in more than d points must be contained in that hypersurface.

Intersection multiplicity for lines: The line through $p = [x_0 : y_0 : z_0]$ is given by

$$\ell : \ \{p + t[v_0 : v_1 : v_2] \mid t \in \mathbb{F}_q\} \cup \{[v_0 : v_1 : v_2]\}.$$

Suppose C is defined by $\{F = 0\}$ with

$$F(X, Y, Z) = a_1 X^d + a_2 X^{d-1} Y + \cdots + a_{\binom{d+2}{2}} Z^d.$$

We consider $F(X + tv_0, Y + tv_1, Z + tv_2)$ as a polynomial in t. The intersection number $(C \cdot \ell)_p$ is the exponent of the lowest degree nonzero term.

Computing the Intersection Multiplicity

Example: Let

$$C: \ \{X^2 + Y^2 + Z^2 = 0\} \subseteq \mathbb{P}^2, \quad \ell: \ \{X - Y = 0\}.$$

At $p = [1 : 1 : 0]$ we expand

$$F(1, 1, t) = 1^2 - 1^2 + t^2 = t^2,$$

so the intersection multiplicity is 2. This is the tangent line to C at p.

Computing the Intersection Multiplicity

Example: Let

$$C: \{X^2 + Y^2 + Z^2 = 0\} \subseteq \mathbb{P}^2, \quad \ell: \{X - Y = 0\}.$$

At $p = [1 : 1 : 0]$ we expand

$$F(1, 1, t) = 1^2 - 1^2 + t^2 = t^2,$$

so the intersection multiplicity is 2. This is the tangent line to C at p.

Let

$$C: \{Y^2 Z = X^3 + Z^3\} \subseteq \mathbb{P}^2, \quad \ell: \{Z = 0\}.$$

At $p = [0 : 1 : 0]$ we expand $F(t, 1, 0) = -t^3$, so the intersection multiplicity is 3.

Computing the Intersection Multiplicity

Example: Let

$$C: \{X^2 + Y^2 + Z^2 = 0\} \subseteq \mathbb{P}^2, \quad \ell: \{X - Y = 0\}.$$

At $p = [1 : 1 : 0]$ we expand

$$F(1, 1, t) = 1^2 - 1^2 + t^2 = t^2,$$

so the intersection multiplicity is 2. This is the tangent line to C at p.

Let

$$C: \{Y^2 Z = X^3 + Z^3\} \subseteq \mathbb{P}^2, \quad \ell: \{Z = 0\}.$$

At $p = [0 : 1 : 0]$ we expand $F(t, 1, 0) = -t^3$, so the intersection multiplicity is 3.

This is an important example. If we dehomogenize, setting $Z = 1$, $x = \frac{X}{Z}$, and $y = \frac{Y}{Z}$, this gives $y^2 = x^3 + 1$, the equation of an elliptic curve in Weierstrass form.

Inflection Points

1. If $p \in C \cap D$ then $(C \cdot D)_p \geq 1$ with equality if and only if the curves meet transversally at P, that is, p is a smooth point of both curves and the two curves have distinct tangent lines at p.
2. A line that intersects a smooth point of a curve with multiplicity at least two is a tangent line to the curve at that point. If the multiplicity is at least three then the point is an inflection point and the line is called a line of inflection.
3. Any line through a singular point meets the curve with multiplicity at least two.
4. Bezout's theorem says that $\sum_{p \in C \cap D} (C \cdot D)_p = mn$.

Inflection Points

1. If $p \in C \cap D$ then $(C \cdot D)_p \geq 1$ with equality if and only if the curves meet transversally at P, that is, p is a smooth point of both curves and the two curves have distinct tangent lines at p.
2. A line that intersects a smooth point of a curve with multiplicity at least two is a tangent line to the curve at that point. If the multiplicity is at least three then the point is an inflection point and the line is called a line of inflection.
3. Any line through a singular point meets the curve with multiplicity at least two.
4. Bezout's theorem says that $\sum_{p \in C \cap D}(C \cdot D)_p = mn$.

Corollary

An irreducible plane cubic has at most one singular point.

Proof: Suppose not. The line connecting two singular points intersects the curve with multiplicity at least 4, contradicting Bezout.

Inflection Points

Definition

The Hessian of a plane curve $\{F = 0\}$ *is the plane curve of degree* $3(d-2)$ *given by the determinant of the* 3×3 *matrix of second partial derivatives of* F*.*

Inflection Points

Definition

The Hessian of a plane curve $\{F = 0\}$ *is the plane curve of degree* $3(d-2)$ *given by the determinant of the* 3×3 *matrix of second partial derivatives of* F*.*

Example: If $F(X, Y, Z) = X^3 + Y^3 + Z^3$, then the Hessian is

$$\det \begin{pmatrix} 6X & 0 & 0 \\ 0 & 6Y & 0 \\ 0 & 0 & 6Z \end{pmatrix} = 216XYZ.$$

Inflection Points

Definition

The Hessian of a plane curve $\{F = 0\}$ *is the plane curve of degree* $3(d-2)$ *given by the determinant of the* 3×3 *matrix of second partial derivatives of* F*.*

Example: If $F(X, Y, Z) = X^3 + Y^3 + Z^3$, then the Hessian is

$$\det \begin{pmatrix} 6X & 0 & 0 \\ 0 & 6Y & 0 \\ 0 & 0 & 6Z \end{pmatrix} = 216XYZ.$$

Proposition

Suppose the characteristic of $\mathbb{F}_q$ *does not divide* $2(d-1)$*. The inflection points of the curve* $\{F = 0\}$ *are the intersection points of the curve with its Hessian.*

Inflection Points of Cubics

Corollary

A smooth plane cubic has 9 inflection points, counted with multiplicity.

Inflection Points of Cubics

Corollary

A smooth plane cubic has 9 inflection points, counted with multiplicity.

Example: Consider $X^3 + Y^3 + Z^3 = 0$ intersected with $216XYZ = 0$. We have 9 inflection points:

$$\begin{array}{lll} [1:-1:0] & [1:e^{\pi i/3}:0] & [1:e^{-\pi i/3}:0] \\ [1:0:-1] & [1:0:e^{\pi i/3}] & [1:0:e^{-\pi i/3}] \\ [0:1:-1] & [0:1:e^{\pi i/3}] & [0:1:e^{-\pi i/3}] \end{array}$$

This construction works over any field with three cube roots of -1, for example in $\mathbb{F}_{13}$, $4^3 = 10^3 = -1$.

Inflection Points of Cubics

Corollary

A smooth plane cubic has 9 inflection points, counted with multiplicity.

Example: Consider $X^3 + Y^3 + Z^3 = 0$ intersected with $216XYZ = 0$. We have 9 inflection points:

$$\begin{array}{lll} [1:-1:0] & [1:e^{\pi i/3}:0] & [1:e^{-\pi i/3}:0] \\ [1:0:-1] & [1:0:e^{\pi i/3}] & [1:0:e^{-\pi i/3}] \\ [0:1:-1] & [0:1:e^{\pi i/3}] & [0:1:e^{-\pi i/3}] \end{array}$$

This construction works over any field with three cube roots of -1, for example in $\mathbb{F}_{13}$, $4^3 = 10^3 = -1$.
Check that this gives 9 points in $\mathbb{P}^2(\mathbb{C})$ where the line between any two contains a third. Take any line not passing through any of these points, such as $2X + Y - Z = 0$, and get 9 points in the affine $\mathbb{C}^2$, $(2X + Y - Z = 1)$, with this property.

The Sylvester-Gallai Theorem

Theorem

Given a collection of n points in $\mathbb{R}^2$ that do not all lie on a line there exists a line containing exactly two of them.

The Sylvester-Gallai Theorem

Theorem

Given a collection of n points in $\mathbb{R}^2$ that do not all lie on a line there exists a line containing exactly two of them.

The previous construction shows that this theorem is false over $\mathbb{C}^2$! We note that by starting from inflection points of higher degree Fermat curves, $\{X^d + Y^d + Z^d = 0\}$, a slight adjustment gives a collections of $3d$ points with this property for any $d \geq 3$.

The Sylvester-Gallai Theorem

Theorem

Given a collection of n points in $\mathbb{R}^2$ that do not all lie on a line there exists a line containing exactly two of them.

The previous construction shows that this theorem is false over $\mathbb{C}^2$! We note that by starting from inflection points of higher degree Fermat curves, $\{X^d + Y^d + Z^d = 0\}$, a slight adjustment gives a collections of $3d$ points with this property for any $d \geq 3$.

A recent paper of Green and Tao makes use of the geometry of cubic curves to construct large sets with few of these 'ordinary lines', lines through exactly two points.

The Sylvester-Gallai Theorem

Theorem

Given a collection of n points in $\mathbb{R}^2$ that do not all lie on a line there exists a line containing exactly two of them.

The previous construction shows that this theorem is false over $\mathbb{C}^2$! We note that by starting from inflection points of higher degree Fermat curves, $\{X^d + Y^d + Z^d = 0\}$, a slight adjustment gives a collections of $3d$ points with this property for any $d \geq 3$.

A recent paper of Green and Tao makes use of the geometry of cubic curves to construct large sets with few of these 'ordinary lines', lines through exactly two points.

Theorem (Kelly)

Any Sylvester-Gallai configuration in $\mathbb{C}^n$ is contained in a $\mathbb{C}^2 \subseteq \mathbb{C}^n$.

Geometry of Cubic Curves

Theorem (Chasles)

Suppose $\{F = 0\}$ *and* $\{G = 0\}$ *are two cubics that meet in* 9 *distinct points* $p_1, \ldots, p_9 \subset \mathbb{P}^2$. *Then if* $X \subset \mathbb{P}^2$ *is any cubic containing* $p_1, \ldots, p_8$, *then* X *also contains* p_9.

Geometry of Cubic Curves

Theorem (Chasles)

Suppose $\{F = 0\}$ *and* $\{G = 0\}$ *are two cubics that meet in* 9 *distinct points* $p_1, \ldots, p_9 \subset \mathbb{P}^2$. *Then if* $X \subset \mathbb{P}^2$ *is any cubic containing* $p_1, \ldots, p_8$, *then* X *also contains* p_9.

This is an early case of the Cayley-Bacharach theorem. Roughly, the theorem concerns the following question.

What is the dimension of the space of degree d polynomials vanishing on a distinct set of points? Usually adding another point causes the dimension to go down by one. When this is the case we say that these point impose independent conditions on these polynomials. We note that when we go from $p_1, \ldots, p_8$ to this collection together with p_9, the space of cubics vanishing on these points does not change.

Geometry of Cubic Curves

Theorem (Chasles)

Suppose $\{F = 0\}$ *and* $\{G = 0\}$ *are two cubics that meet in* 9 *distinct points* $p_1, \ldots, p_9 \subset \mathbb{P}^2$. *Then if* $X \subset \mathbb{P}^2$ *is any cubic containing* $p_1, \ldots, p_8$, *then* X *also contains* p_9.

This is an early case of the Cayley-Bacharach theorem. Roughly, the theorem concerns the following question.

What is the dimension of the space of degree d polynomials vanishing on a distinct set of points? Usually adding another point causes the dimension to go down by one. When this is the case we say that these point impose independent conditions on these polynomials. We note that when we go from $p_1, \ldots, p_8$ to this collection together with p_9, the space of cubics vanishing on these points does not change.

Interpolation problems in algebraic geometry are concerned with understanding when collections of points impose independent conditions on polynomials of a fixed degree.

The Size of the Zero Set of a Polynomial

The maximum number of zeros of a affine/projective variety of degree d is given by Scwartz-Zippel/Serre-Tsfasman. When we restrict to smooth varieties things become much more complicated.

The Size of the Zero Set of a Polynomial

The maximum number of zeros of a affine/projective variety of degree d is given by Scwartz-Zippel/Serre-Tsfasman. When we restrict to smooth varieties things become much more complicated.

Theorem (Hasse)

Let $C: \{F = 0\} \subset \mathbb{P}^2$ *be a smooth cubic. Then*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

The Size of the Zero Set of a Polynomial

The maximum number of zeros of a affine/projective variety of degree d is given by Scwartz-Zippel/Serre-Tsfasman. When we restrict to smooth varieties things become much more complicated.

Theorem (Hasse)

Let $C: \{F = 0\} \subset \mathbb{P}^2$ *be a smooth cubic. Then*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Theorem (Hasse-Weil Bound)

Let $C: \{F = 0\} \subset \mathbb{P}^2$ *be a smooth degree* d *curve. We define the genus of* C *by* $g(C) = \frac{(d-1)(d-2)}{2}$. *Then*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

The genus of C is related to the genus of the Riemann surface given by the zero set of a curve in $\mathbb{C}^2$.

Riemann-Hypothesis for Curves over Finite Fields

This result is closely related to the Riemann Hypothesis for curves over finite fields. There is a notion of the zeta function of a variety over $\mathbb{F}_q$, a generating function that keeps track of the number of points of C over $\mathbb{F}_q$ and over all finite extensions of $\mathbb{F}_q$. For such zeta functions we know that all the roots lie on the critical line.

Riemann-Hypothesis for Curves over Finite Fields

This result is closely related to the Riemann Hypothesis for curves over finite fields. There is a notion of the zeta function of a variety over $\mathbb{F}_q$, a generating function that keeps track of the number of points of C over $\mathbb{F}_q$ and over all finite extensions of $\mathbb{F}_q$. For such zeta functions we know that all the roots lie on the critical line.

We also note that there is a much more difficult version of this result for higher dimensional varieties, Deligne's solution to the Weil Conjectures.

The Frobenius Map

The main idea used to count points on varieties over finite fields is to understand the number of fixed points of a special map.
We define the Frobenius map,

$$\begin{aligned} \varphi : \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) &\to \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) \\ [x_0 : \cdots : x_n] &\to \quad [x_0^q : \cdots : x_n^q]. \end{aligned}$$

The Frobenius Map

The main idea used to count points on varieties over finite fields is to understand the number of fixed points of a special map.
We define the Frobenius map,

$$\begin{aligned} \varphi : \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) &\to \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) \\ [x_0 : \cdots : x_n] &\to \quad [x_0^q : \cdots : x_n^q]. \end{aligned}$$

The points 'defined over $\mathbb{F}_q$', those which are fixed by the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, are exactly the fixed points of this map.

The Frobenius Map

The main idea used to count points on varieties over finite fields is to understand the number of fixed points of a special map.
We define the Frobenius map,

$$\begin{aligned} \varphi : \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) &\to \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) \\ [x_0 : \cdots : x_n] &\to \quad [x_0^q : \cdots : x_n^q]. \end{aligned}$$

The points 'defined over $\mathbb{F}_q$', those which are fixed by the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, are exactly the fixed points of this map.

For a curve $C : \{F = 0\}$, $F(X, Y, Z) = a_0 X^d + \cdots + a_{\binom{d+2}{2}} Z^d$,

$$\varphi : \ C \to C^{(q)}, \quad \text{where } C^{(q)} \text{ is cut out by}$$
$$F^{(q)}(X, Y, Z) = a_0^q X^d + \cdots + a_{\binom{d+2}{2}}^q Z^d.$$

The Frobenius Map

The main idea used to count points on varieties over finite fields is to understand the number of fixed points of a special map.
We define the Frobenius map,

$$\begin{aligned} \varphi : \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) &\to \quad \mathbb{P}^n(\overline{\mathbb{F}_q}) \\ [x_0 : \cdots : x_n] &\to \quad [x_0^q : \cdots : x_n^q]. \end{aligned}$$

The points 'defined over $\mathbb{F}_q$', those which are fixed by the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, are exactly the fixed points of this map.

For a curve $C : \{F = 0\}$, $F(X, Y, Z) = a_0 X^d + \cdots + a_{\binom{d+2}{2}} Z^d$,

$$\varphi : \ C \to C^{(q)}, \quad \text{where } C^{(q)} \text{ is cut out by}$$
$$F^{(q)}(X, Y, Z) = a_0^q X^d + \cdots + a_{\binom{d+2}{2}}^q Z^d.$$

If each $a_i \in \mathbb{F}_q$ then $C^{(q)} = C$ and $C(\mathbb{F}_q)$ is the set of fixed points of φ.

The Frobenius Map

This allows us to use fixed-point theorems inspired by algebraic toplogy to count the number of fixed points of the Frobenius map. These include results like the Lefschetz fixed point theorem, and the more difficult Grothendieck fixed point theorem. The number of fixed points is calculated in terms of the trace of the map induced by Frobenius on a certain cohomology group. In more complicated cases the right setting is to define étale cohomology groups.

The Frobenius Map

This allows us to use fixed-point theorems inspired by algebraic toplogy to count the number of fixed points of the Frobenius map. These include results like the Lefschetz fixed point theorem, and the more difficult Grothendieck fixed point theorem. The number of fixed points is calculated in terms of the trace of the map induced by Frobenius on a certain cohomology group. In more complicated cases the right setting is to define étale cohomology groups.

For smooth curves the number of $\mathbb{F}_q$ points $q+1$ minus the trace of Frobenius acting on a certain cohomology group, and the Hasse-Weil bound says that this trace is not too large.

Chevalley-Warning

Theorem (Chevalley-Warning)

1. *Let p be the characteristic of $\mathbb{F}_q$ and $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ satisfy $\sum_i \deg(f_i) < n$. Then*

$$|V(f_1, \ldots, f_m)| \equiv 0 \pmod{p}.$$

2. *Suppose that each f_i is homogeneous of degree $d \geq 1$. Then $|V(f_1, \ldots, f_m)| \geq p$.*

Chevalley-Warning

Theorem (Chevalley-Warning)

1. *Let p be the characteristic of $\mathbb{F}_q$ and $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ satisfy $\sum_i \deg(f_i) < n$. Then*

$$|V(f_1, \ldots, f_m)| \equiv 0 \pmod{p}.$$

2. *Suppose that each f_i is homogeneous of degree $d \geq 1$. Then $|V(f_1, \ldots, f_m)| \geq p$.*

Theorem (Ax-Katz)

Suppose that each f_i has degree d_i. Then $|V(f_1, \ldots, f_m)|$ is divisible by $q^{\max\left\{0, \lceil \frac{n - \sum d_i}{\max d_i} \rceil\right\}}$.

Chevalley-Warning

Theorem (Chevalley-Warning)

1. *Let p be the characteristic of $\mathbb{F}_q$ and $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ satisfy $\sum_i \deg(f_i) < n$. Then*

$$|V(f_1, \ldots, f_m)| \equiv 0 \pmod{p}.$$

2. *Suppose that each f_i is homogeneous of degree $d \geq 1$. Then $|V(f_1, \ldots, f_m)| \geq p$.*

Theorem (Ax-Katz)

Suppose that each f_i has degree d_i. Then $|V(f_1, \ldots, f_m)|$ is divisible by $q^{\max\left\{0, \lceil \frac{n - \sum d_i}{\max d_i} \rceil\right\}}$.

Chevalley-Warning can be very useful for applications. For example, this shows that no hypersurface in $\mathbb{F}_q^n$ of degree less than n vanishes at a single point.

Surfaces

Example: A smooth cubic surfaces S in $\mathbb{P}^3(\mathbb{F}_q)$ has $|S(\mathbb{F}_q)| = q^2 + q + 1 + tq$ where $t \in [-3, 6] \setminus \{-2, 5\}$. Such a surface contains exactly 27 lines.

Surfaces

Example: A smooth cubic surfaces S in $\mathbb{P}^3(\mathbb{F}_q)$ has $|S(\mathbb{F}_q)| = q^2 + q + 1 + tq$ where $t \in [-3, 6] \setminus \{-2, 5\}$. Such a surface contains exactly 27 lines.

What sorts of surfaces contain many lines?

Definition

A doubly-ruled surface (regulus) in $\mathbb{R}^3$ is a surface such that every point has two lines passing through it.

Two non-equivalent examples:

$$\{(x, y, xy) \mid x, y \in \mathbb{R}\} \text{ and } \{(x, y, z) \mid x^2 + y^2 - z^2 = 1\}.$$

Surfaces

Example: A smooth cubic surfaces S in $\mathbb{P}^3(\mathbb{F}_q)$ has $|S(\mathbb{F}_q)| = q^2 + q + 1 + tq$ where $t \in [-3, 6] \setminus \{-2, 5\}$. Such a surface contains exactly 27 lines.

What sorts of surfaces contain many lines?

Definition

A doubly-ruled surface (regulus) in $\mathbb{R}^3$ is a surface such that every point has two lines passing through it.

Two non-equivalent examples:

$$\{(x, y, xy) \mid x, y \in \mathbb{R}\} \text{ and } \{(x, y, z) \mid x^2 + y^2 - z^2 = 1\}.$$

Theorem (Guth-Katz)

Let L be a set of N lines in $\mathbb{R}^3$ such that no more than $\sqrt{N}$ lines intersect in a single point and no plane or doubly ruled surface contains more than $\sqrt{N}$ lines. Then the number of incidences of lines in L is as most a constant times $N^{\frac{3}{2}} \log(N)$.

Finite Field Kakeya

Definition

A set $E \subseteq \mathbb{F}_q^n$ *is called a Kakeya set if for every* $v \in \mathbb{F}_q^n \setminus (0, \ldots, 0)$ *there exists a* $y \in \mathbb{F}_q^n$ *such that*

$$\ell_{v_0,y} = \{tv + y \mid t \in \mathbb{F}_q\} \subseteq E.$$

Finite Field Kakeya

Definition

A set $E \subseteq \mathbb{F}_q^n$ is called a Kakeya set if for every $v \in \mathbb{F}_q^n \setminus (0, \ldots, 0)$ there exists a $y \in \mathbb{F}_q^n$ such that

$$\ell_{v_0,y} = \{tv + y \mid t \in \mathbb{F}_q\} \subseteq E.$$

Recall: If a set $E \subseteq \mathbb{F}_q^n$ satisfies $|E| < \binom{d+n}{n}$ then there is a nonzero polynomial of degree d vanishing on E.

Finite Field Kakeya

Definition

A set $E \subseteq \mathbb{F}_q^n$ is called a Kakeya set if for every $v \in \mathbb{F}_q^n \setminus (0, \ldots, 0)$ there exists a $y \in \mathbb{F}_q^n$ such that

$$\ell_{v_0,y} = \{tv + y \mid t \in \mathbb{F}_q\} \subseteq E.$$

Recall: If a set $E \subseteq \mathbb{F}_q^n$ satisfies $|E| < \binom{d+n}{n}$ then there is a nonzero polynomial of degree d vanishing on E.

Theorem (Dvir)

Any Kakeya set $E \subset \mathbb{F}_q^n$ satisfies $|E| \geq \frac{q^n}{n!}$.

Finite Field Kakeya

Definition

A set $E \subseteq \mathbb{F}_q^n$ is called a Kakeya set if for every $v \in \mathbb{F}_q^n \setminus (0, \ldots, 0)$ there exists a $y \in \mathbb{F}_q^n$ such that

$$\ell_{v_0,y} = \{tv + y \mid t \in \mathbb{F}_q\} \subseteq E.$$

Recall: If a set $E \subseteq \mathbb{F}_q^n$ satisfies $|E| < \binom{d+n}{n}$ then there is a nonzero polynomial of degree d vanishing on E.

Theorem (Dvir)

Any Kakeya set $E \subset \mathbb{F}_q^n$ satisfies $|E| \geq \frac{q^n}{n!}$.

Proof: We claim that no polynomial of degree less than q vanishes on E. Then,

$$|E| \geq \binom{n + (q-1)}{n} = \frac{(q + (n-1)) \cdots q}{n!} \geq \frac{q^n}{n!}.$$

Proof of Finite Field Kakeya

1. Suppose $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ has degree $d < q$ and vanishes on E. We consider the homogenized polynomial $\overline{P}(x_1, \ldots, x_n) = x_0^d P(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$. Now each term has degree exactly d and $V(\overline{P})$ is a projective variety in $\mathbb{P}^n$.

Proof of Finite Field Kakeya

1. Suppose $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ has degree $d < q$ and vanishes on E. We consider the homogenized polynomial $\overline{P}(x_1, \ldots, x_n) = x_0^d P(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$. Now each term has degree exactly d and $V(\overline{P})$ is a projective variety in $\mathbb{P}^n$.

2. The affine points $[1 : x_1 : \cdots : x_n]$ of $V(\overline{P})$ correspond exactly to zeros of P. However, there are also points of $V(\overline{P})$ on the hyperplane at infinity $[0 : x_1 : \cdots : x_n]$. We claim that $\overline{P}$ vanishes at every such point.

Proof of Finite Field Kakeya

1. Suppose $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ has degree $d < q$ and vanishes on E. We consider the homogenized polynomial $\overline{P}(x_1, \ldots, x_n) = x_0^d P(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$. Now each term has degree exactly d and $V(\overline{P})$ is a projective variety in $\mathbb{P}^n$.

2. The affine points $[1 : x_1 : \cdots : x_n]$ of $V(\overline{P})$ correspond exactly to zeros of P. However, there are also points of $V(\overline{P})$ on the hyperplane at infinity $[0 : x_1 : \cdots : x_n]$. We claim that $\overline{P}$ vanishes at every such point.

3. Note that $\overline{P}(0, x_1, \ldots, x_n) = P^d(x_1, \ldots, x_n)$, where P^d denotes the highest degree part of P. This is a polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ of degree $d < q$. Since $\overline{P}$ vanishes on every $[0 : x_1 : \cdots : x_n]$, we see that $P^d(x_1, \ldots, x_n) = 0$ for $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ and $P^d(0, \ldots, 0) = 0$ since $d > 0$. Therefore, P^d vanishes on $q^n > dq^{n-1}$ points, so by Schwartz-Zippel it is zero. This contradicts the statement that P had degree d.

Proof of Finite Field Kakeya

1. We now show that $\overline{P}(0, x_1, \ldots, x_n) = 0$ for all nonzero $v = (x_1, \ldots, x_n)$. Consider the line $\ell_{v,y} = \{tv + y\}$ in the direction of v that is contained in E. This line together with the point $[0 : v]$ determines a projective line in $\mathbb{P}^n$.

Proof of Finite Field Kakeya

1. We now show that $\overline{P}(0, x_1, \ldots, x_n) = 0$ for all nonzero $v = (x_1, \ldots, x_n)$. Consider the line $\ell_{v,y} = \{tv + y\}$ in the direction of v that is contained in E. This line together with the point $[0 : v]$ determines a projective line in $\mathbb{P}^n$.

2. Since P vanishes on this line, $\overline{P}(1, tv + y) = 0$ for all $t \in \mathbb{F}_q$. Since $V(\overline{P})$ contains q points of this line, and $q > d$, it contains the last point $[0 : v]$ also. Since v was chosen arbitrarily $\overline{P}(0, v) = 0$ for all nonzero $v \in \mathbb{F}_q^n$, completing the proof.

Proof of Finite Field Kakeya

1. We now show that $\overline{P}(0, x_1, \ldots, x_n) = 0$ for all nonzero $v = (x_1, \ldots, x_n)$. Consider the line $\ell_{v,y} = \{tv + y\}$ in the direction of v that is contained in E. This line together with the point $[0 : v]$ determines a projective line in $\mathbb{P}^n$.

2. Since P vanishes on this line, $\overline{P}(1, tv + y) = 0$ for all $t \in \mathbb{F}_q$. Since $V(\overline{P})$ contains q points of this line, and $q > d$, it contains the last point $[0 : v]$ also. Since v was chosen arbitrarily $\overline{P}(0, v) = 0$ for all nonzero $v \in \mathbb{F}_q^n$, completing the proof.

A major step in this proof is that $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ gives rise to a projective variety of degree $d < q$ which vanishes on an entire hyperplane but is not the zero polynomial on it, which is impossible.

The Method of Multiplicities

Theorem (Dvir, Kopparty, Saraf, Sudan)

Any Kakeya set $E \subset \mathbb{F}_q^n$ *satisfies* $|E| \geq \frac{q^n}{2^n}$.

The Method of Multiplicities

Theorem (Dvir, Kopparty, Saraf, Sudan)

Any Kakeya set $E \subset \mathbb{F}_q^n$ satisfies $|E| \geq \frac{q^n}{2^n}$.

The main idea comes from the 'method of multiplicities'. Instead of showing that no polynomial of degree $d < q$ vanishes on E, we show that no polynomial of low-degree 'vanishes to high order' at every point of E.

The Method of Multiplicities

Theorem (Dvir, Kopparty, Saraf, Sudan)

Any Kakeya set $E \subset \mathbb{F}_q^n$ satisfies $|E| \geq \frac{q^n}{2^n}$.

The main idea comes from the 'method of multiplicities'. Instead of showing that no polynomial of degree $d < q$ vanishes on E, we show that no polynomial of low-degree 'vanishes to high order' at every point of E.

Example: We say that $P(x_1, \ldots, x_n)$ vanishes to order m at $(0, \ldots, 0)$ if m is the exponent of the lowest-degree term of P.

The Method of Multiplicities

A more formal definition is given in terms of Hasse derivatives. Let

$$P(x) = \sum_{j=1}^{d} c_j x^j, \text{ and define } D^i(P(x)) = \sum_{j=1}^{d} \binom{j}{i} c_j x^{j-i}.$$

The Method of Multiplicities

A more formal definition is given in terms of Hasse derivatives. Let

$$P(x) = \sum_{j=1}^{d} c_j x^j, \text{ and define } D^i(P(x)) = \sum_{j=1}^{d} \binom{j}{i} c_j x^{j-i}.$$

This gives a positive characteristic analogue of Taylor series. There is an extra factor of $\frac{1}{i!}$ here in order to avoid multiplying or dividing by the characteristic.

The Method of Multiplicities

A more formal definition is given in terms of Hasse derivatives. Let

$$P(x) = \sum_{j=1}^{d} c_j x^j, \text{ and define } D^i(P(x)) = \sum_{j=1}^{d} \binom{j}{i} c_j x^{j-i}.$$

This gives a positive characteristic analogue of Taylor series. There is an extra factor of $\frac{1}{i!}$ here in order to avoid multiplying or dividing by the characteristic.

Example: Over $\mathbb{F}_3$, $D^3(x^3) = 1$, not $3 \cdot 2 \cdot x^0 = 0$.

The Method of Multiplicities

Proposition

For $P \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$$P(y_1, \ldots, y_n) = \sum D^{i_1,\ldots,i_n} \left(P(y_1, \ldots, y_n)\right) (x_1 - y_1)^{i_1} \cdots (x_n - y_n)^{i_n},$$

where

$$D^{i_1,\ldots,i_n} \left(\sum c_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n} \right) = \sum c_{j_1,\ldots,j_n} \binom{j_1}{i_1} \cdots \binom{j_n}{i_n} x_1^{j_1 - i_1} \cdots x_n^{j_n - i_n}.$$

The Method of Multiplicities

Proposition

For $P \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$$P(y_1, \ldots, y_n) = \sum D^{i_1,\ldots,i_n}\left(P(y_1, \ldots, y_n)\right)(x_1 - y_1)^{i_1} \cdots (x_n - y_n)^{i_n},$$

where

$$D^{i_1,\ldots,i_n}\left(\sum c_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n}\right) = \sum c_{j_1,\ldots,j_n} \binom{j_1}{i_1} \cdots \binom{j_n}{i_n} x_1^{j_1 - i_1} \cdots x_n^{j_n - i_n}.$$

Definition

We say that P *vanishes to order at least* m *at* $p = (p_1, \ldots, p_n)$ *if all* $D^{i_1,\ldots,i_n}\left(P(p_1, \ldots, p_n)\right) = 0$ *for* $i_1 + \cdots + i_n < m$.

The Method of Multiplicities

Lemma

Fix $d \geq 0$. If $p_1, \ldots, p_k$ are points in $\mathbb{F}_q^n$ and $c_1, \ldots, c_k$ are nonnegative integers, then

$$\sum_{j=1}^{k} \binom{c_j + n - 1}{n} < \binom{d+n}{n}$$

implies that there exists a polynomial of degree at most d vanishing to order at least c_j at each p_j.

The Method of Multiplicities

Lemma

Fix $d \geq 0$. If $p_1, \ldots, p_k$ are points in $\mathbb{F}_q^n$ and $c_1, \ldots, c_k$ are nonnegative integers, then

$$\sum_{j=1}^{k} \binom{c_j + n - 1}{n} < \binom{d+n}{n}$$

implies that there exists a polynomial of degree at most d vanishing to order at least c_j at each p_j.

We now apply this lemma, showing that no low-degree polynomial of low-degree vanishes to order m at each point in E, where m is a parameter we can choose.

Construction of 'Small' Kakeya Sets

Proposition (Tao-Mockenhaupt/Dvir)

Given $n \geq 1$ there exists a Kakeya set of size at least

$$|E| \leq \begin{cases} q\left(\frac{q+1}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is odd.} \\ (q-1)\left(\frac{q}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is even.} \end{cases}$$

Construction of 'Small' Kakeya Sets

Proposition (Tao-Mockenhaupt/Dvir)

Given $n \geq 1$ there exists a Kakeya set of size at least

$$|E| \leq \begin{cases} q\left(\frac{q+1}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is odd.} \\ (q-1)\left(\frac{q}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is even.} \end{cases}$$

The previous bound cannot be improved by more than a factor of $\frac{1}{2}$.

Construction of 'Small' Kakeya Sets

Proposition (Tao-Mockenhaupt/Dvir)

Given $n \geq 1$ there exists a Kakeya set of size at least

$$|E| \leq \begin{cases} q\left(\frac{q+1}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is odd.} \\ (q-1)\left(\frac{q}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is even.} \end{cases}$$

The previous bound cannot be improved by more than a factor of $\frac{1}{2}$.

We start with the set

$$\left\{(v_1^2/4 + v_1 t, \ldots, v_{n-1}^2/4 + v_{n-1} t, t) \,|v_i, t \in \mathbb{F}_q\right\},$$

and use the structure of the set of squares in $\mathbb{F}_q$.
This set is not too large and is close to being a Kakeya set.

Construction of 'Small' Kakeya Sets

Proposition (Tao-Mockenhaupt/Dvir)

Given $n \geq 1$ there exists a Kakeya set of size at least

$$|E| \leq \begin{cases} q\left(\frac{q+1}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is odd.} \\ (q-1)\left(\frac{q}{2}\right)^{n-1} + q^{n-1} & \text{if } q \text{ is even.} \end{cases}$$

The previous bound cannot be improved by more than a factor of $\frac{1}{2}$.

We start with the set

$$\left\{(v_1^2/4 + v_1 t, \ldots, v_{n-1}^2/4 + v_{n-1} t, t) \,|v_i, t \in \mathbb{F}_q\right\},$$

and use the structure of the set of squares in $\mathbb{F}_q$.
This set is not too large and is close to being a Kakeya set.

In $\mathbb{F}_q^2$ for q odd, Blokhuis and Mazzocca have shown that every Kakeya set has size at least $\frac{q(q+1)}{2} + \frac{q-1}{2}$ with equality if and only if the set is of 'oval type'. This is related to Segre's theorem stated above.

The Kakeya Maximal Conjecture

Let $\ell_{v,y}$ denote the line through y in the direction v. For any function $f : \mathbb{F}_q^n \to \mathbb{R}$, define the Kakeya maximal function

$$f^* : \mathbb{P}^{n-1}(\mathbb{F}_q) \to \mathbb{R}, \quad f^*(w) = \max_{a \in \mathbb{F}_q^n} \sum_{x \in \ell_{w,a}} |f(x)|.$$

The Kakeya Maximal Conjecture

Let $\ell_{v,y}$ denote the line through y in the direction v. For any function $f : \mathbb{F}_q^n \to \mathbb{R}$, define the Kakeya maximal function

$$f^* : \mathbb{P}^{n-1}(\mathbb{F}_q) \to \mathbb{R}, \quad f^*(w) = \max_{a \in \mathbb{F}_q^n} \sum_{x \in \ell_{w,a}} |f(x)|.$$

Theorem (Ellenberg, Oberlin, Tao)

$$\sum_{w \in \mathbb{P}^{n-1}(\mathbb{F}_q)} |f^*(w)|^n \leq c_n q^{n-1} \sum_{x \in \mathbb{F}_q^n} |f(x)|^n.$$

The Kakeya Maximal Conjecture

Let $\ell_{v,y}$ denote the line through y in the direction v. For any function $f : \mathbb{F}_q^n \to \mathbb{R}$, define the Kakeya maximal function

$$f^* : \mathbb{P}^{n-1}(\mathbb{F}_q) \to \mathbb{R}, \quad f^*(w) = \max_{a \in \mathbb{F}_q^n} \sum_{x \in \ell_{w,a}} |f(x)|.$$

Theorem (Ellenberg, Oberlin, Tao)

$$\sum_{w \in \mathbb{P}^{n-1}(\mathbb{F}_q)} |f^*(w)|^n \leq c_n q^{n-1} \sum_{x \in \mathbb{F}_q^n} |f(x)|^n.$$

Taking f to be the indicator function of a Kakeya set, then $|f^*(w)| = q$ for every w. This recovers the finite field Kakeya conjecture.

The Kakeya Maximal Conjecture

Let $\ell_{v,y}$ denote the line through y in the direction v. For any function $f : \mathbb{F}_q^n \to \mathbb{R}$, define the Kakeya maximal function

$$f^* : \mathbb{P}^{n-1}(\mathbb{F}_q) \to \mathbb{R}, \quad f^*(w) = \max_{a \in \mathbb{F}_q^n} \sum_{x \in \ell_{w,a}} |f(x)|.$$

Theorem (Ellenberg, Oberlin, Tao)

$$\sum_{w \in \mathbb{P}^{n-1}(\mathbb{F}_q)} |f^*(w)|^n \leq c_n q^{n-1} \sum_{x \in \mathbb{F}_q^n} |f(x)|^n.$$

Taking f to be the indicator function of a Kakeya set, then $|f^*(w)| = q$ for every w. This recovers the finite field Kakeya conjecture.

There is also a version of this theorem that applies when we define $f^*(w)$ in terms of curves of bounded degree, not necessarily lines. This requires more algebraic geometry- the 'method of random rotations'.

Flexy Varieties

Some strange things can happen in algebraic geometry in characteristic p that you might not be aware of if you have not thought much about finite fields.

Theorem (Guth-Katz)

Let K be a field of characteristic 0 and L a set of N^2 lines in K^3 such that no more that $2N$ lines lie in any plane.
Let S be a set of points such that each line in L contains at least N points of S. Then $|S| > cN^3$ for some constant c.

Flexy Varieties

Some strange things can happen in algebraic geometry in characteristic p that you might not be aware of if you have not thought much about finite fields.

Theorem (Guth-Katz)

Let K be a field of characteristic 0 and L a set of N^2 lines in K^3 such that no more that $2N$ lines lie in any plane.
Let S be a set of points such that each line in L contains at least N points of S. Then $|S| > cN^3$ for some constant c.

This theorem is false over $\mathbb{F}_{p^2}$. Let $X \subset \mathbb{F}_{p^2}^3$ be the surface defined by

$$x - x^p + yz^p - zy^p = 0.$$

Consider the p^4 lines given by

$$\{(a, b, 0) + t(b^p, v, 1) \mid t \in \mathbb{F}_{p^2}\} \text{ where } a, v \in \mathbb{F}_p, \ b \in \mathbb{F}_{p^2}.$$

Let S be the set of $\mathbb{F}_{p^2}$ points of X and $N = p^2$. Then $|S| \approx N^{\frac{5}{2}}$ and S contains all of the N points on each line L. This is a contradiction.

Flexy Varieties

The surface X is very special- every smooth point is an inflection point. Ellenberg and Hablicsek call this a 'flexy surface'

Something similar can happen for curves. Consider $x^3y + y^3z + z^3x = 0 \subset \mathbb{P}^2(\mathbb{F}_3)$. Every rational point of this curve is an inflection point. This is famously called 'the funny curve' by Hartshorne. It is an example of a Hermitian curve. These play a big role in the study of curves with many points over finite fields and connections to coding theory.

Flexy Varieties

The surface X is very special- every smooth point is an inflection point. Ellenberg and Hablicsek call this a 'flexy surface'

Something similar can happen for curves. Consider $x^3y + y^3z + z^3x = 0 \subset \mathbb{P}^2(\mathbb{F}_3)$. Every rational point of this curve is an inflection point. This is famously called 'the funny curve' by Hartshorne. It is an example of a Hermitian curve. These play a big role in the study of curves with many points over finite fields and connections to coding theory.

Over $\mathbb{R}^2$ every flexy curve is a line and in $\mathbb{R}^3$ every flexy surface is a plane.

Flexy Varieties

The surface X is very special- every smooth point is an inflection point. Ellenberg and Hablicsek call this a 'flexy surface'

Something similar can happen for curves. Consider $x^3y + y^3z + z^3x = 0 \subset \mathbb{P}^2(\mathbb{F}_3)$. Every rational point of this curve is an inflection point. This is famously called 'the funny curve' by Hartshorne. It is an example of a Hermitian curve. These play a big role in the study of curves with many points over finite fields and connections to coding theory.

Over $\mathbb{R}^2$ every flexy curve is a line and in $\mathbb{R}^3$ every flexy surface is a plane.

Theorem (Ellenberg, Hablicsek)

If you add the additional assumption that no more than $2Nd$ lines lie in any flexy surface of degree d, then the result from the previous slide is true in characteristic p.