The Polynomial Method in Finite Geometry

Simeon Ball, Aart Blokhuis

May 23-27th, 2016, Singapore

Designs and Additive Combinatorics

Fully reducible lacunary polynomials

Notation: $\mathbb{F}$ without index is $\mathbb{F}_q = GF(q)$, the finite field of order $q = p^h$, where p is a prime, (but sometimes p is a point). $(g, h) = \gcd(g, h)$, the greatest common divisor of the polynomials g and h.
$(x : y : z) = \langle (x, y, z) \rangle$ denotes a projective point in $PG_2(\mathbb{F})$.

LEMMA(essentially Rédei): Let $f = g(X)X^q + h(X) \in \mathbb{F}[X]$ be a polynomial which factorizes into linear factors in $\mathbb{F}[X]$.

If $\deg g, \deg h \leq \frac{1}{2}(q-1)$ then either

$$f(X) = g(X)(X^q - X)$$

or

$$f(X) = (g, h)e(X^p) \ .$$

PROOF

Write $f = s \cdot r$, where $s = (X^q - X, f)$ has the same roots as f, but simple.

$$s \mid f - g(X^q - X) = gX + h \ .$$

$$r \mid f' \text{ and } f \quad \text{so} \quad r \mid gf' - g'f = gh' - g'h.$$

$$f \mid (Xg + h)(gh' - g'h) \ .$$

Comparing degrees gives $(Xg + h)(gh' - g'h) = 0$ and now $h = -Xg$ or (after removing the gcd) $g' = h' = 0$.

Examples showing the degree bound is sharp

In both examples q is odd.

(i) $g(X) = 1$, $h(X) = -X^{(q+1)/2}$,

$$f(X) = X^q - X^{(q+1)/2} = X^{(q+1)/2}(X^{(q-1)/2} - 1)$$

factors into linear factors in $\mathbb{F}[X]$ (see below).

Examples showing the degree bound is sharp

In both examples q is odd.

(i) $g(X) = 1$, $h(X) = -X^{(q+1)/2}$,

$$f(X) = X^q - X^{(q+1)/2} = X^{(q+1)/2}(X^{(q-1)/2} - 1)$$

factors into linear factors in $\mathbb{F}[X]$ (see below).

(ii) $g(X) = X^{(q-1)/2} - 3$, $h(X) = 3X^{(q+1)/2} - X$,

$$f(X) = X(X^{(q-1)/2} - 1)^3 = X \prod_{s=\square} (X - s)^3 .$$

Here $\square$ denotes a nonzero square in $\mathbb{F}$.

THEOREM: Let S be a set of points of $PG_2(\mathbb{F})$ with the property that every line is incident with a point of S.
If $|S| < \frac{3}{2}(q+1)$ and q is prime then S contains a line.

PROOF: Choose coordinates (X_1, X_2, X_3) so that $X_3 = 0$ is a tangent and $p_\infty = p = (1:0:0)$ its point in S. With $S_0 = S \setminus \{p\}$ let

$$f(X,Y) = \prod_{(a:b:1)\in S_0} (X + bY + a) \ .$$

For $y, z \in \mathbb{F}$ the line $X_1 + yX_2 + zX_3 = 0$ is incident with a point of S_0.

Proof, continued

Proof: Choose coordinates (X_1, X_2, X_3) so that $X_3 = 0$ is a tangent and $p = (1:0:0)$ its point in S. Let $f(X, Y) = \prod_{(a:b:1)\in S_0}(X + bY + a)$. For $y, z \in \mathbb{F}$ the line $X_1 + yX_2 + zX_3 = 0$ is incident with a point of S_0.

So $\exists(a:b:1) \in S_0$: $a + yb + z = 0$ hence $f(X, Y)$ is zero for all pairs $(x, y) \in \mathbb{F}^2$ hence:

$$f(X, Y) = g_1(X, Y)(X^q - X) + h_1(X, Y)(Y^q - Y)$$

Restrict to the highest degree terms

$$f^*(X, Y) := \prod_{(a:b:1)\in S_0}(X + bY) = g_0X^q + h_0Y^q$$

put $Y = 1$: $f^*(X, 1) = \prod_{(a:b:1)}(X + b) = gX^q + h$.

So $\prod_{(a:b:1)}(X+b) = gX^q + h$ is fully reducible,
$\deg(h) \leq \deg(g) = m \leq (q-1)/2$ and the lemma applies:
$\deg(h) \leq \deg(g)$, so $Xg + h \neq 0$ and

$$f^*(X,1) = (g,h)e(X^p) \ .$$

But $q = p$ is prime so

$$e(X^q) = (X+c)^q \quad \text{for some} \quad c \in \mathbb{F} \ .$$

We see that S contains the line $X_3 = cX_2$. $\square$

EXAMPLE: (the bubble construction)

Consider the identifications: (sub is subspace)

$$\begin{array}{ccccccc} PG_2(\mathbb{F}_{p^h}) & \leftrightarrow & V_3(\mathbb{F}_{p^h}) & \leftrightarrow & V_{3h}(\mathbb{F}_p) & \leftrightarrow & PG_{3h-1}(\mathbb{F}_p) \\ \text{point} & \leftrightarrow & 1\text{-dim sub} & \leftrightarrow & h\text{-dim sub} & \leftrightarrow & (h-1)\text{-dim sub} \\ \text{line} & \leftrightarrow & 2\text{-dim sub} & \leftrightarrow & 2h\text{-dim sub} & \leftrightarrow & (2h-1)\text{-dim sub} \end{array}$$

Let U be a h-dim sub of $PG_{3h-1}(\mathbb{F}_p)$, let

$$B(U) = \{x \text{ point of } PG_2(\mathbb{F}_{p^h}) \,|\, x \cap U \neq \emptyset\}\ .$$

For any line ℓ of $PG_2(\mathbb{F}_{p^h})$: $\ell \cap U \neq \emptyset$, so $\exists x \in B(U)$ incident with ℓ, and $B(U)$ is a blocking set of size at most
$(p^{h+1}-1)/(p-1) = q + q/p + \cdots + 1$.

The linearity conjecture

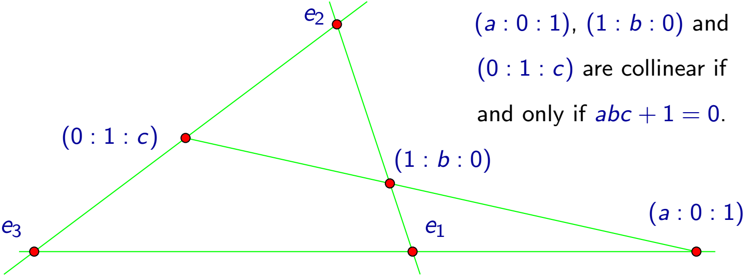
Let U be a h-dim subspace of $PG_{3h-1}(\mathbb{F}_p)$, let

$$B(U) = \{x \ \text{ point of } \ PG_2(\mathbb{F}_{p^h}) \,|\, x \cap U \neq \emptyset\} \ .$$

For any line ℓ of $PG_2(\mathbb{F}_{p^h})$: $\ell \cap U \neq \emptyset$, so $\exists x \in B(U)$ incident with ℓ, and $B(U)$ is a blocking set of size at most $(p^{h+1} - 1)/(p-1) = q + q/p + \cdots + 1$.

CONJECTURE: All minimal blocking sets of size $< \frac{3}{2}(q+1)$ arise from the bubble construction.

EXAMPLE: (the coset construction)



$(a:0:1)$, $(1:b:0)$ and $(0:1:c)$ are collinear if and only if $abc+1=0$.

$S = \{(a:0:1) \mid -a \in H\} \cup \{(1:b:0) \mid -b \notin H\} \cup$
$\cup \{(0:1:c) \mid -c \notin H\} \cup \{e_1, e_2, e_3\}$
is a blocking set for H subgroup of $\mathbb{F}^*$. If $|\mathbb{F}^* : H| = r$, then $|S| = 2q+1-\frac{q-1}{r}$. For $r=2$: $|S| = \frac{3}{2}(q+1)$.

Link to additive combinatorics

If is contained in the union of three lines (as above), one can use Kneser's theorem to show that H is the union of cosets. Also for 3 concurrent lines H is the union of cosets, but now of the additive group.

Functions that determine few directions

The function $\phi : \mathbb{F} \to \mathbb{F}$ determines the direction d if $\exists x \neq y \in \mathbb{F}$ s.t.

$$d = \frac{\phi(y) - \phi(x)}{y - x}.$$

d is not determined $\Leftrightarrow x \mapsto \phi(x) - dx$ is permutation of $\mathbb{F}$.

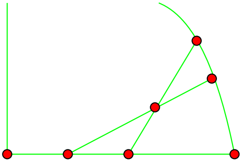
Functions that determine few directions

The function $\phi : \mathbb{F} \to \mathbb{F}$ determines the direction d if $\exists x \neq y \in \mathbb{F}$ s.t.

$$d = \frac{\phi(y) - \phi(x)}{y - x}.$$

d is not determined $\Leftrightarrow x \mapsto \phi(x) - dx$ is permutation of $\mathbb{F}$.

The graph of ϕ is $\{(x : \phi(x) : 1) \,|\, x \in \mathbb{F}\}$, a set of q affine points with $e_2 = (0 : 1 : 0)$ not determined.



Appending points $(1 : d : 0)$ where d is a direction determined by ϕ gives a blocking set of size $q + N(\phi)$, where $N(\phi)$ is the number of directions determined by ϕ.

Coset and bubble construction

To the blocking set coming from the coset construction corresponds a function ϕ with $N(\phi) = q + 1 - |H|$.

For q odd, $|H| = (q-1)/2$ we find $N(\phi) = \frac{1}{2}(q+3)$.

For a special choice of subspace U in the bubble construction we find a function ϕ determining between $q/s + 1$ and $\frac{q-1}{s-1}$ directions for some subfield $\mathbb{F}_s$ of $\mathbb{F}$.

For q even, $s = 2$ we find ϕ with $N(\phi) = \frac{1}{2}(q+2)$.

THEOREM: Any function determining at most $\frac{1}{2}(q+1)$ directions comes from the bubble construction.

Hasse derivatives

The k-th Hasse-derivative $\dfrac{\partial^k}{\partial X}$ of a polynomial $\sum c_i X^i$ is

$$\frac{\partial^k}{\partial X}\left(\sum c_i X^i\right) = \partial^k\left(\sum\right) = \sum \binom{i}{k} c_i X^{i-k} .$$

EXERCISE: $\partial^k(fg) = \sum_{i=0}^{k} \partial^i f \cdot \partial^{k-i} g$.

EXERCISE: if a is zero of f of multiplicity m, then a is zero of $\partial^i f$ of multiplicity $\geq m - i$.

An important exercise

EXERCISE: if $X^q + h$ is fully reducible and $2 \leq \deg h \leq \frac{1}{2}(q-1)$ then $X^q + h = e(X^s)$, for some (maximal) $s = p^\sigma$, $\sigma > 0$.

Prove that $\deg(h) \geq \dfrac{q+s}{s+1}$, for this s where $\mathbb{F}_s$ is subfield of $\mathbb{F}$.

An important exercise

EXERCISE: if $X^q + h$ is fully reducible and $2 \le \deg h \le \frac{1}{2}(q-1)$ then $X^q + h = e(X^s)$, for some (maximal) $s = p^\sigma$, $\sigma > 0$.

Prove that $\deg(h) \ge \dfrac{q+s}{s+1}$, for this s where $\mathbb{F}_s$ is subfield of $\mathbb{F}$.

$$X^{q/s} + h^{1/s} \mid (X+h)\left(h^{1/s}\right)', \quad \left(h^{1/s}\right)' \neq 0, \quad s \neq q, \quad h \neq -X$$

Conclusion: $q/s \le (1 + 1/s)\deg h - 1$.

The Rédei polynomial

Let $f(X,Y)=\prod_{x\in F}(X+xY-\phi(x))=\sum_{j=0}^{q}\sigma_j(Y)X^{q-j}$.

If d is not determined by ϕ then $f(X,d)=X^q-X$ which implies $\sigma_j(d)=0$ for $j=1,\ldots,q-2$. Since $\deg(\sigma_j)\leq j-1$ for $j=1,\ldots,q-2$, $\sigma_j\equiv 0$ for $j=1,\ldots,q-N(\phi)$.

If d *is* determined by ϕ, then let s be the maximal power of p s.t. $f(X,d)=e(X^s)$, i.e. $\sigma_j(d)=0$ if $s\not| j$.

Hence $f(X,Y)=X^q+\sum_{j=0}^{N_0/s}\sigma_{q-js}(Y)X^{js}+\sigma_{q-1}(Y)X$,

where for some $N_0\leq N(\phi)-1$, $\sigma_{q-N_0}\not\equiv 0$.

If d *is* determined by ϕ, then let s be the maximal power of p s.t. $f(X,d) = e(X^s)$, i.e. $\sigma_j(d) = 0$ if $s \not| j$.

Hence $f(X,Y) = X^q + \sum_{j=0}^{N_0/s} \sigma_{q-js}(Y) X^{js} + \sigma_{q-1}(Y) X$,

where for some $N_0 \leq N(\phi) - 1$, $\sigma_{q-N_0} \not\equiv 0$.

The exercise implies $N_0 \geq \frac{q+s}{s+1}$, examples all give $N_0 \geq \frac{q}{s} + 1$.

Any factor of $f(X,d)$ is factor of $X + \sum_{j=0}^{N_0} \sigma_{q-j}(Y) X^j$.

Proof that $N(\phi) \geq q/s + 1$

In what follows y is a direction determined by ϕ.

$$\frac{\partial^k f}{\partial Y}(y) = \left(\sum \frac{x_1 \cdots x_k}{\prod (X + x_i Y - f(x_i))} \right) f(X, y) .$$

Multiplying both sides by $\left(X + \sum_{j=0}^{N_0} \sigma_{q-j} X^j \right)^k$ gives a polynomial identity so

$$f(X, y) \mid \left(X + \sum_{j=0}^{N_0} \sigma_{q-j} X^j \right)^k \frac{\partial^k f}{\partial Y}(y) .$$

If $N \leq q/s$ then $N_0 \leq q/s - 1$, so $q - 1 \geq kN_0 + N_0 \Rightarrow \frac{\partial^k f}{\partial Y}(y) = 0$, for $k = 1, \ldots, s-1$.

In particular $\dfrac{\partial^k \sigma_{q-N_0}(y)}{\partial Y}(y) = 0$.

In particular $\dfrac{\partial^k \sigma_{q-N_0}(y)}{\partial Y}(y) = 0$.

$\dfrac{\partial^{s-1} \sigma_{q-N_0}(y)}{\partial Y}(y) = 0$ is an s-th power. It has $\geq sN_0$ zeros, but its degree is $\leq q - N_0 - 1$. If it's not zero then $sN_0 \leq q - N_0 - 1$, contradicting exercise.

So $\dfrac{\partial^{s-1} \sigma_{q-N_0}(y)}{\partial Y} \equiv 0$. Similarly $\dfrac{\partial^{j} \sigma_{q-N_0}(y)}{\partial Y} \equiv 0$ for $j = 1, \ldots, s-1$.
Therefore σ_{q-N_0} is an s-th power.
But $\sigma_{q-N_0}(Y)$ is zero for all directions not determined by ϕ since $s(q-N) >> q - N_0$ implies $\sigma_{q-N_0} \equiv 0$ (Contradiction).

Further reading

Analysis of $f(X, Y)$ proves the Bubble-conjecture for functions determining few directions, or blocking sets of size $q + m$ with an m-secant.

Using Newton's identities $\sigma_j \equiv 0$, for $j = 1, \ldots, q - N(\phi)$ implies

$$\sum_{x \in \mathbb{F}} (xY - \phi(x))^j \equiv 0, \text{ for } j = 1, \ldots, q - N(\phi),$$

from which we deduce that

$$\phi(X)^j \mod (X^q - X)$$

has no X^{q-1-i} term if $\binom{i+j}{j} \neq 0$ and $i + j \leq n - N(\phi)$.

The coset construction

Careful analysis of linear maps between polynomial spaces

$$(F_1, \dots, F_j) \mapsto F_1 f + \cdots + F_j f^j$$

allows one to prove:

THEOREM: (q prime). Any function determining at most $(2q+1)/3$ directions comes from the coset construction.

CONJECTURE: (q prime). If $N(\phi) < p - p/t - t$ then the graph of ϕ is contained in an algebraic curve of degree $\leq t-1$.

Applications of projective blocking sets

(i) A *spread* of $V_k(\mathbb{F})$ is a partition of the non-zero vectors into k-dim subspaces. A large partial spread gives rise to a proj. blocking set.

(ii) A *k-dimensional linear code* C of length n and minimum distance d is a k-dim subspace of $\mathbb{F}^n$ in which every non-zero vector has at least d non-zero coordinates.
Let G be a $k \times n$ matrix with rowspace C.
Let S be the set of columns of G, viewed as points of $PG_{k-1}(\mathbb{F})$.
Every hyperplane is incident with at most $n - d$ point of the (multi-)set S.

If the code is *projective*, that is S is a set, then its complement B is a t-fold blocking set (with respect to hyperplanes).

Complex characters

Let $w \in \mathbb{F}_p^k = G$, viewed as elementary abelian group.

Define $\chi_w : G \to \mathbb{C}$ by $\chi_w(x) = \exp(\frac{2\pi i}{p}(w \cdot x))$.

LEMMA: If $g(x) = \sum_{w \in G} c_w \chi_w(x)$, $c_w \in \mathbb{Z}$ satisfies $g(x) = 0$, $\forall x \neq 0$, then $|G| = p^k$ divides $g(0)$.

PROOF: $g(0) = \sum_{x \in G} g(x) = \sum_x \sum_w c_w \chi_w(x) =$

$$= \sum_w c_w \sum_x \chi_w(x) = c_0 \sum_x \chi_0(x) = c_0 |G|.$$

Affine sets with bounded hyperplane intersections

THEOREM: Let S be a set of n points in $AG_k(\mathbb{F}_p)$, such that any hyperplane is incident with at most t points of S.

Then $n \leq (t-e)p+e$, where $e \in \{0,\dots,k-1\}$ is maximal such that $\binom{t}{e} \not\equiv 0 \mod p^{k-e}$.

LEMMA: If S is as above, then the coefficient of $X^{tp-n+\epsilon}$ in $(X-1)^{-n}(X^p-1)^t$ is zero mod p^k for all $\epsilon \geq 1$.

PROOF of the LEMMA

LEMMA: The coefficient of $X^{tp-n+\epsilon}$ in $(X-1)^{-n}(X^p-1)^t$ is zero mod p^{k-2} for all $\epsilon \geq 1$.

PROOF: Let $f(X,x) = \prod_{u \in S}(1 - \exp(\frac{2\pi i}{p}(u \cdot x))X) = \sum_{j=0}^{n} \sigma_j(x)X^j$,

where $\sigma_j(x)$ is an integer combination of characters.

Let $g(X,x) = \sum_{j=0}^{\infty} \rho_j(x)X^j$ be the inverse: $g(X,x)f(X,x) = 1$.

Then $\rho_j(x)$ also is an integer combination of characters.

Proof continued

By hypothesis, for $x \neq 0$, $u \cdot x = a \in \mathbb{F}_p$ for at most t elements $u \in S$, so $f(X,x) \mid (X^p - 1)^t \quad$ for $x \neq 0$.
Let $h(X,x) = (X^p - 1)^t g(X,x)$, then

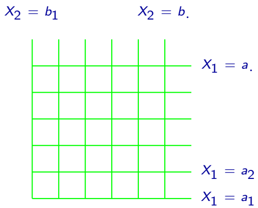
$$f(X,x)h(X,x) = (X^p - 1)^t \ ,$$

so h is a polynomial in X of degree $tp - n$.
The coefficient of $X^{tp-n+\epsilon}$ in $h(X,x)$ is an integer combination of characters, which is zero $\forall x \neq 0$:

$$f(X,0) = (X-1)^n \Rightarrow h(X,0) = (X-1)^{-n}(X^p - 1)^t \ .$$

Now apply the previous lemma. □

Combinatorial Nullstellensatz



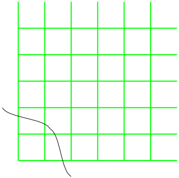
Let $\mathbb{K}$ be any field,

S_i finite subset of $\mathbb{K}$,

let $g_i(X_i) = \prod_{a \in S_i} (X_i - a)$.

THEOREM: Let $f \in \mathbb{K}[X_1, \ldots, X_n]$. If f is zero on the grid $S_1 \times \cdots \times S_k$, then $f = \sum_{i=1}^{k} g_i(X_i) h_i(X_1, \ldots, X_k)$ for some polynomials $h_1, \ldots, h_k$, where $\deg h_i \leq \deg f - |S_i|$.

Combinatorial Nullstellensatz, continued



Let $D_i \subset S_i$, $D_i \neq \emptyset$.

Let $\ell_i(X_i) = \prod_{a \in D_i} (X_i - a)$

THEOREM: If f is zero on $S_1 \times \cdots \times S_k \setminus (D_1 \times \cdots \times D_k)$ and non zero in at least one point of $D_1 \times \cdots \times D_k$, then

$$f = \sum g_i(X_i)h_i + u(X_1, \ldots, X_k) \prod \frac{g_i(X_i)}{\ell_i(X_i)}, \text{ for some } u \neq 0.$$

It follows that $\deg(f) \geq \sum_{i=1}^{k} (|S_i| - |D_i|)$.

Proof

We can write $f = \sum g_i(X_i)h_i + r(X_1, \ldots, X_n)$, where the degree in X_i of r is at most $|S_i| - 1$. $\ell_i(X_i)f$ is zero at all points of $S_1 \times \cdots \times S_k$, so

$\ell_i(X_i)r$ is zero at all points $S_1 \times \cdots \times S_k$.

Nullstellensatz, together with degree of X_i in r is at most $|S_i| - 1$ implies $l_i(X_i)r = g_i(X_i)h_i$,

so $\frac{g_i}{l_i}$ divides r, for each $i = 1, \ldots, k$. $\square$

Affine sets with bounded hyperplane intersections

THEOREM: Let S be a set of n points in $AG_{k-1}(\mathbb{F})$, such that any hyperplane is incident with at least t points of S.

Then $|S| \geq (t+k-2)(q-1)+1$.

PROOF: $(t=1)$ Let $f(X_1,\ldots,X_k) = \prod_{u \in S}(u_1X_1 + \cdots + u_{k-1}X_{k-1}+1)$.

Then f is zero in $\mathbb{F}^k \setminus (0,\ldots,0)$ so apply previous theorem.

One can prove more for larger t since the theorem implies $f(X,0,\ldots,0) = (X^t v(X) + u(X))(X^{q-1}-1)^t$ where $\deg u \leq |S| - (t+k-2)(q-1) - 1$ and $X^t v(X) + u(X)$ factors into linear factors.

Extension fields as vector spaces

$\mathbb{F}_{q^k}$ is a vector space over $\mathbb{F} = \mathbb{F}_q$ of dimension k.

We can view elements of $\mathbb{F}_{q^k}$ as vectors of $AG_k(\mathbb{F})$.

Hyperplanes have equation $\mathrm{Tr}(aX) = b$, $a \in \mathbb{F}_{q^k}$, $b \in \mathbb{F}$.

More generally an r-dimensional subspace has equation $f(X) = b$ where f is a q-linearized polynomial
$f(X) = a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots + X^{q^r}$.

In particular x, y, z are collinear iff $\begin{vmatrix} 1 & x & x^q \\ 1 & y & y^q \\ 1 & z & z^q \end{vmatrix} = 0$ iff

$(x-y)(x-z)\begin{vmatrix} 1 & x & x^q \\ 0 & 1 & (x-y)^{q-1} \\ 0 & 1 & (x-z)^{q-1} \end{vmatrix} = 0$ if and only if
$(x-y)^{q-1} = (x-z)^{q-1}$.

A $(q-1)$-st power u^{q-1} in $\mathbb{F}_{q^k}$ is a $\left(\dfrac{q^k-1}{q-1}\right)$-st root of unity.

Nuclei

THEOREM: Let S be a set of $q+m$ points of $AG_2(\mathbb{F})$ and let N be a disjoint set of points such that every line with a point of N is incident with a point of S. Then $|N| \leq m(q-1)$.

PROOF: Consider S as a subset of $\mathbb{F}_{q^2}$ and let

$$f(T,X) = \prod_{y \in S} (T - (X-y)^{q-1}) = \sum_{j=0}^{|S|} \sigma_j(X) T^{|S|-j} .$$

where $\sigma_j(X)$ is of degree $\leq j(q-1)$.
If $x \in N$ then $f(T,x) = (T^{q+1}-1)$(poly of degree $m-1$). Hence $\sigma_m(x) = 0$. The coefficient of $T^{|S|-m}$ in $(T - X^{q-1})^{|S|}$ is $X^{m(q-1)}$ so σ_m has degree $m(q-1)$ which implies the bound.

Exercise

a) If $S, N \subset AG(2, \mathbb{F})$, $|S| = t(q+1) + (m-1)$ and every line incident with a point of N is incident with at least t points of S, then

$$\binom{t+m-1}{m} \neq 0 \quad \Rightarrow \quad |N| \leq m(q-1) \ .$$

b) If $S \subset AG(2, \mathbb{F})$ and every line is incident with at least t points of $|S|$ then $|S| \geq (t+1)q - p^e$ where e is maximal such that $p^e \mid t$.

Maximal arcs

THEOREM: Let $S \neq \emptyset$ be a set of points in $AG_2(\mathbb{F}_q)$, q odd, such that every line intersects S in 0 or in some constant number r of points. Then either S is a single point, or S contains all points of the plane.

PROOF: $|S| = 1 + (q+1)(r-1) = qr - q + r$ and $r \mid q$. We use the same polynomial as before:

$$f(T, X) = \prod_{y \in S} \left(T - (X-y)^{q-1}\right) = \sum_{j=0}^{|S|} \sigma_j(X) T^{|S|-j} \ .$$

For $X = x \in S$ we see every direction $r-1$ times:

$$f(T, x) = \prod_{y \in S} \left(T - (x-y)^{q-1}\right) = T(T^{q+1} - 1)^{r-1} \ ,$$

For $X = x \notin S$ we see every direction 0 or r (a power of p) times:

$$f(T, x) = \sum_{i=0}^{|S|/r} \sigma_{ir}(X) T^{|S|-ir} \ ,$$

rest of the proof

$$x \in S : f(T,x) = T(T^{q+1}-1)^{r-1}, x \notin S : f(T,x) = \sum_{i=0}^{|S|/r} \sigma_{ir}(X) T^{|S|-ir},$$

In both cases: $\sigma_j(x)$ (of degree $\leq j(q-1)$) is zero for $j = 1, \ldots, r-1$.
Moreover: $S(X) := \prod_{y \in S}(X-y) \mid \sigma_r(X)$.

Next step: input secret ingredient and conclude $(S(x)\sigma_r(x))' = 0$, but this implies that not only $S \mid \sigma_r$, but in fact S^{p-1} does, contradiction. $\square$

Lifting to the p-adic integers

Let $\mathbb{Z}_p$ denote the ring of p-adic integers.
Let $f(X)$ be a (monic) polynomial in $\mathbb{Z}_p[X]$ of degree h whose reduction modulo p also has degree h and is irreducible. Then f is irreducible.

Let $R = \mathbb{Z}_p[X]/(f)$ be the quotient ring of $\mathbb{Z}_p[X]$ by the ideal (f) and let $\mathfrak{p} = \{x \in R \mid x = 0 \mod (p)\}$.

Then $\mathfrak{p}$ is the maximal ideal of R and $R/\mathfrak{p} \simeq \mathbb{F}$.
Recall, $\mathbb{F} = \mathbb{F}_q$ and $q = p^h$.

Let T be the set of roots of $X^q - X$ in R

For $S \subset T$ define $g_S(X) = g(X) = \prod_{u \in S}(X - u)$.

Affine sets with bounded hyperplane intersections

LEMMA: If $f \in R[X]$ is the product of linear factors such that for each $u \in S$, there are at least t factors $X - a$ of f for which $a = u \mod p$, then

$$f(X) = \sum_{j=0}^{t} g(X)^{t-j} p^j h_j(X) \ ,$$

for some polynomials h_j, where $\deg h_j \leq \deg f - (t-j)|S|$.

PROOF: $f(X) = h(X) \prod_{i=1}^{t} (g(X) + pc_i(X))$,

for some $c_1, \ldots, c_t, h \in R[X]$. $\square$

Let $B \subset AG_k(\mathbb{F})$ such that every hyperplane is incident with at least t points of B. Lift each coordinate to the ring R. Let

$f(X, x_1, \dots, x_k) = \prod_{u \in B}(X + u_1 x_1 + \dots + u_{k-1} x_k + 1)$.

Let $y \in R^k$, $y \neq (0, \dots, 0)$.

From the lemma: $f(X, y) = \displaystyle\sum_{j=0}^{t} p^j h_j(X)(X^q - X)^{t-j}$,

so $f(X, y)$ modulo p^e is divisible by $(X^q - X)^{t-e+1}$.

Hence $(X^q - X)^{e-t-1} f(X, x_1, \dots, x_k)$ is a polynomial in X whenever we evaluate $(x_1, \dots, x_k) \neq (0, \dots, 0)$ modulo p^e.

Hence $(X^q - X)^{e-t-1} f(X, x_1, \ldots, x_k)$ is a polynomial in X whenever we evaluate $(x_1, \ldots, x_{k-1}) \neq (0, \ldots, 0)$ modulo p^e.

The coefficient of $X^{-\epsilon}$ is a polynomial in $x_1, \ldots, x_k$ of relatively small degree
its value at $(0, \ldots, 0)$ is the coefficient of $X^{-\epsilon}$ in

$$(X^q - X)^{e-t-1}(X+1)^{|B|} \ .$$

For ϵ small enough this coefficient must be zero modulo p^e.

Let S be a set of points of $AG_k(\mathbb{K})$.

LEMMA: If $|S| \leq \binom{n+k}{k}$ then there is an $f \in \mathbb{K}[X_1,\ldots,X_k]$ of degree at most n such that

$$S \subseteq V(f) = \{x \in AG_k(\mathbb{K}) \mid f(x) = 0\}.$$

PROOF: The dimension of the space of functions $S \to \mathbb{K}$ is $|S|$.
The dimension of the space of polynomials in $\mathbb{K}[X_1,\ldots,X_k]$ of degree at most n is $\binom{n+k}{k}$.
If $|S| < \binom{n+k}{k}$ then there are two polynomials g and h that agree on S. Let $f = g - h$. □

Kakeya type problems

Let L be a set of lines of $AG_k(\mathbb{K})$.
Let S be a set of points in $AG_k(\mathbb{K})$, such that every line of L is incident with at least N points of s.
Let D be a set of points of $PG_{k-1}(\mathbb{K})$ such that $d \in D$ iff L has a line with direction d.

THEOREM: With L, S, D and N as above: if $(k!|S|)^{1/k} < N$ then D is contained in an algebraic hypersurface of degree $\leq (k!|S|)^{1/k}$.

PROOF: By the lemma there is a poly f of degree $m \leq (k!|S|)^{1/k}$ with $S \subseteq V(f)$.
For each $d \in D$, $\exists x \in AG_k(\mathbb{K})$ such that $f(x + \lambda d) = 0$ for N values of λ.

PROOF: By the lemma there is a poly f of degree $m \leq (k!|S|)^{1/k}$ with $S \subseteq V(f)$.

For each $d \in D$, $\exists x \in AG_k(\mathbb{K})$ such that $f(x + \lambda d) = 0$ for N values of λ.

$$0 = f(x + \lambda d) = \sum_{j=0}^{m-1} \lambda^j f_j(x_1, \ldots, x_k, d_1, \ldots, d_k) + \lambda^m f_m(d_1, \ldots, d_k).$$

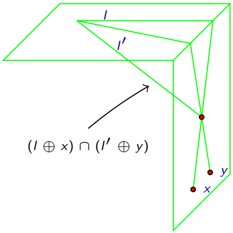
Since $m \leq N - 1$, each coeff of $\lambda^j \quad (j = 0, \ldots, m)$ is zero.

Hence $f_m(d) = 0$ and f_m is a hom. poly of degree m with $D \subseteq V(f_m)$.

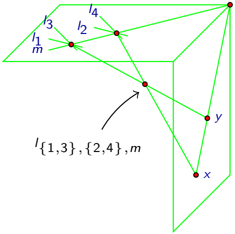
COROLLARY: If D is an N^{k-1} grid then $(k!|S|)^{1/k} \geq N$:

$$|S| \geq \frac{N^k}{k!} \ .$$

COROLLARY(Kakeya): If D is the set of all directions (i.e. $PG_{k-1}(\mathbb{F})$) then previous bound with $N = q$.



Starting with a set of N lines L in $AG_2(\mathbb{K})$ which has lines with different directions we can construct N^{k-1} lines in $AG_k(\mathbb{K})$



Starting with a set of $\frac{1}{2}N^2$ points S in $AG_2(\mathbb{K})$ we construct a set of $2(\frac{1}{2}N)^k$ points in $AG_k(\mathbb{K})$;

Suitable starting configurations exist for

$\mathbb{K} = \mathbb{F}$: L lines of a dual conic;

$\mathbb{K} = \mathbb{R}$: L lines of a dual regular N-gon.

Bezout's theorem

THEOREM: If f and $g \in \mathbb{K}[X_1, X_2]$ have no common factor, then $V(f,g)$ contains at most $(\deg f)(\deg g)$ points.

THEOREM: If $f, g \in \mathbb{K}[X_1, X_2, X_3]$ have no common factor, then $V(f,g)$ contains at most $(\deg f)(\deg g)$ lines.

Let L be a set of N^2 lines in $AG_3(\mathbb{K})$ and let S be a set of points with the property that every line of L is incident with at least N points of S. How small can $|S|$ be?

EXAMPLE:
$L' = \{Y = mX + c \,|\, m \in \{1, \ldots, N^e\}, c \in \{1, \ldots, N^{1+e}\}\}$;
$S' = \{(x, y) \,|\, x \in \{1, \ldots, N\}, \quad y \in \{1, \ldots, 2N^{1+e}\}\}$.

$|L'| = N^{1+2e}$ and $|S'| = cN^{2+e}$.

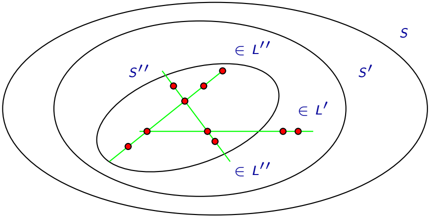
If L is the union of N^{1-2e} such sets L' then $|S| = cN^{3-e}$.

THEOREM: Let L be a set of N^2 lines in $AG_3(\mathbb{K})$, at most N in any plane. If $\mathrm{char}(\mathbb{K}) = 0$ or $\mathbb{K} = \mathbb{F}_p$ and S is a set of points such that every line of L is incident with at least N points of L, then $|S| > cN^3$ for some constant c.

PROOF: If $|S| < cN^3$ then there is a subset S' of S such that $S' \subset V(f)$ for some irreducible poly f of degree $d < \frac{1}{4}N$ (by the lemma).
L': lines of L incident with at least $4d$ points of S'.
S'': points of S' incident with at least 3 lines of L'.
L''': lines of L' incident with at least $4d$ points of S''.

By a dyadic pigeon-hole principle, one can show $|L''| > 4d^2$.

By a dyadic pigeon-hole principle, one can show $|L''| > 4d^2$.



A point of S'' is either a singular point or a flexy point of $V(f)$. Singular points are in $V(h)$, where h is the first partial derivative of f. Flexy points are in $V(g)$, where g is the Hessian of f ($\deg g < 3d$).

Bezout's theorem implies that $V(f, h)$ contains at most d^2 lines and $V(f, g)$ contains at most $3d^2$ lines.

The resultant of two polynomials

Let $f = \sum_{i=0}^{n} f_i X^i$ and $g(x) = \sum_{i=0}^{n-1} g_i X^i$ be polynomials in $\mathbb{K}[X]$.

Let $b = X^m + \sum_{i=0}^{m-1} X^i$ and $a = \sum_{i=0}^{m-1} a_i X^i$ be such that $af + bg = 0$.

Considering the coefficients of $X^{n+m-1}, \dots, X^{n-m-1}$ gives $2n$ linear equations which in matrix form are:

$(a_0, \dots, a_{m-1}, b_0, \dots, b_{m-1}) R_m = -(g_{n-1-2m}, \dots, g_{n-1})$.

Note that $\deg g \geq n - m$, so the right hand side is nonzero.

EXAMPLE $(m = 2)$:

$$(a_0, a_1, b_0, b_1) \begin{pmatrix} 0 & f_n & f_{n-1} & f_{n-2} \\ f_n & f_{n-1} & f_{n-2} & f_{n-3} \\ 0 & 0 & g_{n-1} & g_{n-2} \\ 0 & g_{n-1} & g_{n-2} & g_{n-3} \end{pmatrix} = -(g_{n-1}, g_{n-2}, g_{n-3}, g_{n-4}) .$$

Suppose $h = (f, g)$ has degree $n - k$.
If $m \geq k + 1$ there are multiple solutions (b can be a multiple of f/h and $a = -b(g/h)$. Hence $\det R_m = 0$.
If $m = k$ then there is a unique solution ($b = \gamma f/h$ and $a = -b(g/h)$, where γ is chosen so that b is monic). Hence $\det R_m \neq 0$.

Next suppose $f, g \in \mathbb{K}[X, Y]$.
By writing f and g as polynomials in X, whose coefficients are polynomials in Y, the determinant of R_m is a polynomial in Y.

Two variables

LEMMA: Suppose there is a $y_0 \in \mathbb{K}$ such that

$$\deg(f(X, y_0), g(X, y_0)) = n - m \ .$$

If there are n_h elements $y \in \mathbb{F}$ for which

$$\deg(f(X, y), g(X, y)) = n - (m - h) \ ,$$

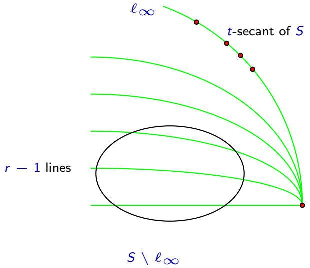
then $$\sum_{h=1}^{m-1} hn_h \leq \deg(\det \ R_m) \ .$$

PROOF: $(\det \ R_m)(y_0) \neq 0$.

If, for $y \in \mathbb{K}$, $\deg(f(X, y), g(X, y)) = n - (m - h)$, then y is a zero of multiplicity y. $\square$

THEOREM: Let S be a set of points of $PG_2(\mathbb{F})$ and suppose there is a point $p_\infty \notin S$, such that r lines incident with p_∞ contain all points of S. Then the number of lines incident with S is at most

$$1 + rq + (|S| - r)(q + 1 - r) \ .$$



(Case $|S \setminus \ell_\infty| > q$).

Let $f(X,Y) = \prod_{(a,b)\in S\setminus\ell_\infty}(X + aY + b)$ and $g(X,Y) = X^q - X$.

Let $p_\infty = (1 : y_0 : 0)$. Then $\deg(f(X, y_0, g(X, y_0)) = r - 1$.

$\#$ lines incident with S is at most

$$1 + tq + (q + 1 - t)(r - 1) + \sum_{h=1}^{r} hn_h.$$

By lemma,

$$\sum hn_h \le \deg(\det\ R_m) \le (|S| - (r-1) - m)(q - r + 1).$$

$(m = |S \setminus l_\infty| - r + 1)$