THE POLYNOMIAL METHOD IN FINITE GEOMETRY

SIMEON BALL AND AART BLOKHUIS

Abstract. We will consider a finite set embedded in some geometry, which has a geometrical property. For example, a set S of points in a finite projective plane, with the property that every line is incident with a point of S. The polynomial method involves defining a polynomial f, or a set of polynomials, which translates to geometric property of S to an algebraic property of f. The hope is that one can gain information from the algebraic property of f. This information is then translated back to the geometrical setting to obtain information about S. For example, suppose that we have constructed a polynomial f of degree $|S|$ and that the geometrical property of S implies some algebraic property of f. If the algebraic property of f implies a lower bound on the degree of f then we obtain a lower bound for $|S|$.

The geometric objects we will consider will, for the most part, be embedded in projective and affine spaces over finite fields and will often have some link to error-correcting codes. In some examples, we will also consider finite sets of points and lines embedded in projective and affine spaces over other fields, the reals for example.

The algebraic methods we shall use include applications of Bezout's theorem, the resultant method, Hasse derivatives, combinatorial nullstellensatz, group characters, interpolation.

1. Basic objects and definitions

Let $\mathbb{K}$ denote an arbitrary field.

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is the power of a prime p.

Let $\mathrm{V}_k(\mathbb{K})$ denote the k-dimensional vector space over $\mathbb{K}$.

Let $\mathrm{PG}_{k-1}(\mathbb{K})$ denote the $(k-1)$-dimensional projective space over $\mathbb{K}$.

Let $\mathrm{AG}_k(\mathbb{K})$ denote the k-dimensional affine space over $\mathbb{K}$.

An affine point of $\mathrm{AG}_k(\mathbb{K})$ is simply of vector of $\mathrm{V}_k(\mathbb{K})$ which, with respect to a basis, has coordinates $(x_1, \ldots, x_k)$. A projective point of $\mathrm{PG}_{k-1}(\mathbb{K})$ is a one-dimensional subspace of $\mathrm{V}_k(\mathbb{K})$ which, with respect to a basis, is $\langle (x_1, \ldots, x_k) \rangle$, where $\langle u_1, \ldots, u_r \rangle$ denotes the subspace spanned by the vectors $u_1, \ldots, u_r$.

Date: 22 May 2016.

The *weight* of a vector is the number of non-zero coordinates it has with respect to a fixed canonical basis.

A k-dimensional *linear code* of length n and minimum distance d is a k-dimensional subspace of $\mathrm{V}_n(\mathbb{F}_q)$ in which every non-zero vector has weight at least d.

The greatest common divisor of two polynomials f and g is denoted by (f, g).

2. Lacunary polynomials

A *lacunary polynomial* is a polynomial that in the sequence of its coefficients has a run of zeros. If a lacunary polynomial in $\mathbb{K}[X]$ factorises into linear factors in $\mathbb{K}[X]$, then one can usually say something further about the polynomial.

Lemma 1. *Let*

$$f(X) = g(X)X^q + h(X)$$

be a polynomial in $\mathbb{F}_q[X]$ *which factorises into linear factors in* $\mathbb{F}_q[X]$.

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

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

or

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

for some polynomial $e \in \mathbb{F}_q[X]$.

Example 2. (q odd). $g(X) = 1$, $h(X) = X^{(q+1)/2}$. Then

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

factorises into linear factors.

Example 3. (q odd). $g(X) = X^{(q-1)/2} - 3$, $h(X) = 3X^{(q+1)/2} - X$. Then

$$f(X) = X(X^{(q-1)/2} - 1)^3,$$

factorises into linear factors.

Theorem 4. *Let* S *be a set of points of* $\mathrm{PG}_2(\mathbb{F}_q)$ *with the property that every line is incident with at least one point of* S. *If* $|S| < 3(q+1)/2$ *and* q *is prime then* S *contains all the points of a line.*

A *blocking set* B is a set of points of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ in which every hyperplane is incident with at least a point of B. More generally a *t-fold blocking set* B is a set of points of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ in which every hyperplane is incident with at least t points of B.

A blocking set is called trivial if it contains a line.

A spread of $\mathrm{V}_{2k}(\mathbb{F}_q)$ is a set of k-dimensional subspaces which partition the non-zero vectors. From a spread one can make projective planes amongst other things. A partial spread of $\mathrm{V}_4(\mathbb{F}_q)$ gives rise to a blocking set of $\mathrm{PG}_2(\mathbb{F}_q)$ which is trivial if and only if the partial spread is not maximal.

Many of the results for blocking sets in $\mathrm{PG}_2(\mathbb{F}_q)$ are easily extendable to $\mathrm{PG}_{k-1}(\mathbb{F}_q)$.

Let G be a matrix whose rows form a basis for a k-dimensional linear code of length n and minimum distance d. Then the columns of G are a set T of vectors of $\mathrm{V}_k(\mathbb{F}_q)$ with the property that any hyperplane contains at most $n-d$ vectors of T. Considering the set as points in the corresponding projective space $\mathrm{PG}_{k-1}(\mathbb{F}_q)$, this gives a set S of n points with the property that any hyperplane contains at most $n-d$ points of S. If S contains no multiple points, which is equivalent to the dual code having minimum distance at least three, then the complement of S is a $((q^{k-1}-1)/(q-1)-n+d)$-fold blocking set of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$. Thus any constructions or bounds on such t-fold blocking sets is in one to one correspondence with linear codes whose dual has minimum distance at least three.

Example 5. (The bubble construction) Let $\mathbb{F}_s$ be a subfield of $\mathbb{F}_q$, where $q = s^t$. The vector space $\mathrm{V}_3(\mathbb{F}_q)$ is also a vector space over $\mathbb{F}_s$, isomorphic to $\mathrm{V}_{3t}(\mathbb{F}_s)$. The one-dimensional subspaces of $\mathrm{V}_3(\mathbb{F}_q)$ become a spread of t-dimensional subspaces of $\mathrm{V}_{3t}(\mathbb{F}_s)$ and the two-dimensional subspaces of $\mathrm{V}_3(\mathbb{F}_q)$ become a spread of $2t$-dimensional subspaces of $\mathrm{V}_{3t}(\mathbb{F}_s)$. Let U be a $(t+1)$-dimensional subspace of $\mathrm{V}_{3t}(\mathbb{F}_s)$. A point of $\mathrm{PG}_2(\mathbb{F}_q)$ is a one-dimensional subspaces of $\mathrm{V}_3(\mathbb{F}_q)$ and therefore a t-dimensional subspaces of $\mathrm{V}_{3t}(\mathbb{F}_s)$. Let B be the set of points of $\mathrm{PG}_2(\mathbb{F}_q)$ which intersect U non-trivially, under this identification. Then B is a blocking set, since any line of $\mathrm{PG}_2(\mathbb{F}_q)$ corresponds to a $2t$-dimenisonal subspace of $\mathrm{V}_{3t}(\mathbb{F}_s)$ and therefore intersect U non-trivially.

Conjecture 6. *All minimal blocking set of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *with less than* $3(q+1)/2$ *points come from the bubble construction (Example 5).*

Example 7. (The coset construction) Let H be a multiplicative subgroup of $\mathbb{F}_q$. The set

$$\{\langle(a,0,1)\rangle \mid a \in H\} \cup \{\langle(0,b,1)\rangle \mid b \notin H\} \cup \{\langle(1,d,0)\rangle \mid d \notin H\}$$

is a blocking set of $\mathrm{PG}_2(\mathbb{F}_q)$ of size $2q+1-(q-1)/r$, where $|H| = (q-1)/r$. Observe that if $r = 2$ then this blocking set has size $3(q+1)/2$.

3. Functions which determine few directions

Let ϕ be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Let

$$D(\phi) = \{d \in \mathbb{F}_q \mid \text{there exist } x, y \in \mathbb{F}_q \text{ such that } \ d = \frac{\phi(y)-\phi(x)}{y-x}\},$$

denote the set of directions determined by ϕ.

Observe that for $d \in \mathbb{F}_q$, the function $\phi(x) + dx$ is a permutation if and only if $-d$ is not a direction determined by ϕ.

The graph of the function ϕ is a set of q affine points in $\mathrm{AG}_2(\mathbb{F}_q)$. This set of points we can consider as a set of points in the affine part of the projective plane $\mathrm{PG}_2(\mathbb{F}_q)$, where the infinte point $\langle(0,1,0)\rangle$ is not determined. Thus, by changing basis, or applying symmetry, the graph of a function is equivalent to a set of q affine points for which at least one direction is not determined. We have the following examples.

Example 8. (The bubble construction). By choosing the subspace U in Example 5 carefully, we can construct a function ϕ which determines between $q/r+1$ and $(q-1)/(r-1)$ directions, where $\mathbb{F}_r$ is a subfield of $\mathbb{F}_q$.

Example 9. (The coset construction). Considering only the affine points of Example 7 we obtain a function ϕ which determines $q+1-|H|$ directions.

Exercise 1. *Prove directly that the function $\phi(x) = x^{(q+1)/2}$ determines $(q+3)/2$ directions when q is odd.*

The *k-th Hasse derivative* of a polynomial

$$f(X) = \sum c_i X^i,$$

is

$$\frac{\partial^k f}{\partial X} = \sum \binom{i}{k} c_i X^{i-k}.$$

Exercise 2. Prove that

$$\frac{\partial^k (fg)}{\partial X} = \sum_{i=0}^{k} \frac{\partial^i f}{\partial X} \frac{\partial^{k-i} g}{\partial X}.$$

Exercise 3. Prove that if a is a zero of f of multiplicity m then a is a zero of $\frac{\partial^k f}{\partial X}$ of multiplicity at least $m-k$.

Exercise 4. By Lemma 1, if $X^q + h(X)$ factorises into linear factors and $2 \leqslant \deg h \leqslant \frac{1}{2}(q-1)$ then $h = e(X^p)$ for some polynomial e. Prove that

$$\deg h \geqslant \frac{q+s}{s+1},$$

for some s dividing q.

Theorem 10. *A function ϕ that determines at most $(q+1)/2$ directions comes from the bubble construction.*

More can be said in the case that q is prime. Suppose ϕ determines N directions. Then the function $x \to \phi(x)^i$ (the i-th power of $\phi(x)$), when considered as a polynomial, has degree bounded by approx. $N+i$. This property can be used to prove the following theorem.

Theorem 11. (q prime) *A function f which determines less than $(2q+1)/3$ directions comes from the coset construction, Example 9.*

4. Complex characters

Let $w \in G = \mathbb{F}_p^k$.

Define a *character* χ_w as a map from G to $\mathbb{C}$ by

$$\chi_w(x) = e^{(2\pi i/p)(w \cdot x)},$$

where $\cdot$ is the standard scalar product.

Lemma 12. *If $g(x)$ is an integer combination of characters and has the property that $g(x) = 0$ for all $x \neq 0$, then $|G|$ divides $g(0)$.*

Exercise 5. Let S be a set of n points in $\mathrm{AG}_2(\mathbb{F}_q)$ with the property that any line is incident with at most t points of S. Prove that $n \leqslant (t-1)q + t$ and that if $n = (t-1)q + t$ then every line is incident with either 0 or t points of S and t divides q.

Exercise 6. *Let S be a set of n points in $\mathrm{AG}_k(\mathbb{F}_q)$ with the property that any hyperplane is incident with at most t points of S. Prove that $n \leqslant \max(tq, (t-k+2)q + t)$.*

Define

$$f(X,x)=\prod_{u\in S}(X-\chi_u(x)),$$

so that it is a polynomial whose coefficients are integer combinations of complex characters, and for every $x\in G$ this defines a polynomial $f(X,x)\in\mathbb{C}[X]$.

Using the fact that $f(X,x)$ divides $(X^p-1)^t$ and its coefficients are integer combinations of complex characters one can prove the following theorem.

Theorem 13. *Let S be a set of n points in $\mathrm{AG}_k(\mathbb{F}_p)$ with the property that any hyperplane is incident with at most t points of S. Then the coefficient of $X^{tp-n+\epsilon}$ in*

$$(X-1)^{-n}(X^p-1)^t$$

is divisible by p^k, for all $\epsilon\geqslant 1$.

The previous theorem allows one to prove the following theorem.

Theorem 14. *Let S be a set of n points in $\mathrm{AG}_k(\mathbb{F}_p)$ with the property that any hyperplane is incident with at most t points of S. Then*

$$n\leqslant(t-e)p+e,$$

where $e\in\{0,1,\ldots,k-1\}$ is maximal with the property that

$$\binom{t}{e}\neq 0 \pmod{p^{k-e}}.$$

Exercise 7. *Let S be a set of n points in $\mathrm{AG}_k(\mathbb{F}_p)$ with the property that any r-dimensional subspace is incident with at most t points of S. Then the coefficient of $X^{tp^{n-r}-n+\epsilon}$ in*

$$(X-1)^{-n}(X^{p^{n-r}}-1)^t$$

is divisible by p^k, for all $\epsilon\geqslant 1$.

5. Combinatorial Nullstellensatz

Let S_i be a finite subset of $\mathbb{K}$, for $i=1,\ldots,k$. Let

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

Theorem 15. *Let $f\in\mathbb{K}[X_1,\ldots,X_k]$. If f is zero on $S_1\times\cdots\times S_k$ then*

$$f=\sum_{i=1}^{k}g_i(X_i)h_i(X_1,\ldots,X_k),$$

for some polynomials h_i, where $\deg h_i \leqslant \deg f - |S_i|$.

Let D_i be a non-empty subset of S_i. Let

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

Theorem 16. *Let $f \in \mathbb{K}[X_1, \ldots, X_k]$. If f is zero on $S_1 \times \cdots \times S_k \setminus (D_1 \times \cdots \times D_k)$ and non-zero at at least one point of $D_1 \times \cdots \times D_k$ then*

$$f = \sum_{i=1}^{k} g_i(X_i) h_i(X_1, \ldots, X_k) + u(X_1, \ldots, u_k) \prod_{i=1}^{k} \frac{g_i(X_i)}{\ell_i(X_i)},$$

for some polynomials $u \neq 0$ and h_i, where $\deg h_i \leqslant \deg f - |S_i|$. *This implies*

$$\deg f \geqslant \sum_{i=1}^{k} (|S_i| - |D_i|).$$

An *affine blocking set* B is a set of points of $\mathrm{AG}_k(\mathbb{F}_q)$ in which every hyperplane is incident with at least a point of B. More generally a *t-fold affine blocking set* B is a set of points of $\mathrm{AG}_k(\mathbb{F}_q)$ in which every hyperplane is incident with at least t points of B.

Let m be the maximum weight of a linear code. Then by shortening the code by $n - m$ which may reduce the minimum distance by $n - m$, one obtains a code which contains the all-1 vector. As before, we consider the set of columns of a generator matrix for this code and observe now that this is a set S of points of $\mathrm{AG}_{k-1}(\mathbb{F}_q)$. The complement of S is t-fold blocking set of $\mathrm{AG}_{k-1}(\mathbb{F}_q)$. In difference to the projective case, if there are mutliple points occurring in the set of points obtained from the the set of columns of the generator matrix we take the complement with respect to w copies of the points, where w is the maximum multiplicity occurring. The reason for this is that allowing multiple points in an affine blocking set does not affect any of the proofs we shall consider, so we shall also allow multiple points in constructions, although this does not appear to help.

The following example is for $t < q$.

Example 17. *The set B of $(t + k - 1)(q - 1) + 1$ points on $t + k - 1$ concurrent lines of $\mathrm{AG}_k(\mathbb{F}_q)$ is a t-fold blocking set of $\mathrm{AG}_k(\mathbb{F}_q)$, provided that the directions of the lines, when viewed as a set S of points of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ form an arc, i.e. any k points of S span the whole space.*

Exercise 8. *Let B be a set of n points of $\mathrm{AG}_k(\mathbb{F}_q)$ with the property that every hyperplane is incident with at least t points of B. Prove that $n \geqslant \max(tq, (t + k - 2 - q^{k-2})q + t)$.*

By applying the Combinatorial nullstellensatz (generalised to zeros of multipicity and then punctured) one can improve on the trivial bound for $t \leqslant (k-1)(q-1)$.

Theorem 18. *Let B be a set of n points of $\mathrm{AG}_k(\mathbb{F}_q)$ with the property that every hyperplane is incident with at least t points of B. Then $n \geqslant (t+k-1)(q-1)+1$.*

Using Theorem 14 one obtains the following theorem in the case q is prime.

Theorem 19. *Let B be a set of n points of $\mathrm{AG}_k(\mathbb{F}_q)$ with the property that every hyperplane is incident with at least t points of B. If q is prime, then*

$$|B| \geqslant tq + e(q-1),$$

where $e \in \{0, 1, \ldots, k-1\}$ is maximal with the property that

$$\binom{-t}{e} \not\equiv 0 \pmod{q^{k-e}}.$$

One can improve on these bounds in the case that q is not a prime by using p-adic lifting, see Theorem 21.

6. The p-adic numbers

Let $\mathbb{Z}_p$ denote the p-adic integers. Let $f \in \mathbb{Z}_p[X]$ be a polynomial of degree h whose reduction modulo p is irreducible. Then f itself is irreducible, since any factorization would give a factorization modulo p. Let $\mathcal{R} = \mathbb{Z}_p[X]/(f)$ be the quotient ring of $\mathbb{Z}_p[X]$ by the ideal (f). Let

$$\mathfrak{p} = \mathcal{R}p = \{x \in \mathcal{R} \mid x = 0 \pmod{p}\}.$$

The ideal $\mathfrak{p}$ is the maximal ideal of $\mathcal{R}$ and $\mathcal{R}/\mathfrak{p}$ is isomorphic to the finite field $\mathbb{F}_q$.

Let S be a finite subset of $\mathcal{R}$ whose elements are distinct modulo p and define

$$g(X) = \prod_{u \in S} (X - u).$$

Lemma 20. *Let $f \in \mathcal{R}[X]$ be the product of linear factors. If, for each $u \in S$, there are at least t factors $X - a$ of f for which $a = u$ modulo p, then*

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

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

Theorem 21. *Let B be a set of n points of $\mathrm{AG}_k(\mathbb{F}_q)$ with the property that every hyperplane is incident with at least t points of B. If*

$$n \leqslant (t+k+1-e)q - k - 1 - \epsilon$$

for some $e \in \{1, \ldots, t-1\}$ and $\epsilon \geqslant 1$ then

$$\sum_{j=0}^{k-1} (-1)^j \binom{-t+e-1}{j} \binom{n}{(t-e+1)q - \epsilon + j(q-1)} = 0 \pmod{p^e}.$$

7. Extension fields as vector spaces

The field $\mathbb{F}_{q^k}$ is a k-dimensional vector space over $\mathbb{F}_q$. Hence, the points of $\mathrm{AG}_k(\mathbb{F}_q)$ can be considered as elements in $\mathbb{F}_{q^k}$. The hyperplanes of $\mathrm{AG}_k(\mathbb{F}_q)$ are the set of solutions of equations of the form

$$\mathrm{Tr}(aX) = b,$$

where

$$Tr(x) = x + x^q + \cdots + x^{q^{k-1}},$$

and $a \in \mathbb{F}_{q^k}$ and $b \in \mathbb{F}_q$.

Three points $x, y, z \in \mathbb{F}_{q^k}$ are collinear iff

$$0 = \begin{vmatrix} 1 & x & x^q \\ 1 & y & y^q \\ 1 & z & z^q \end{vmatrix} = (x-y)(x-z) \begin{vmatrix} 1 & x & x^q \\ 0 & 1 & (x-y)^{q-1} \\ 0 & 1 & (x-z)^{q-1} \end{vmatrix},$$

so if and only if $(x-y)^{q-1} = (x-z)^{q-1}$.

Theorem 22. *Let S be a set of $q+m$ points of $\mathrm{AG}_2(\mathbb{F}_q)$ and let N be the set of points with the property that every line incident with a point of N is incident with at least one point of S. Then $|N| \leqslant m(q-1)$.*

Exercise 9. *Let S be a set of $t(q+1)+m-1$ points of $\mathrm{AG}_2(\mathbb{F}_q)$ and let N be the set of points with the property that every line incident with a point of N is incident with at least t points of S. Prove that if*

$$\binom{t+m-1}{m} \neq 0,$$

then $|N| \leqslant m(q-1)$.

Exercise 10. *Let S be a set of points of $\mathrm{AG}_2(\mathbb{F}_q)$ with the property that every line incident is incident with at least t points of S. Prove that*

$$|S| \geqslant (t+1)q - p^e,$$

where e is maximal such that p^e divides t.

Exercise 11. *Let S be a set of points of $\mathrm{AG}_2(\mathbb{F}_q)$ with the property that every line incident is incident with at most t points of S. Prove that*

$$|S| \leqslant (t-1)q + p^e,$$

where e is maximal such that p^e divides t.

Theorem 23. *Suppose that S is a set of points of $\mathrm{AG}_2(\mathbb{F}_q)$ with the property that every line incident is incident with either zero or exactly t points of S. If q is odd then S is either a point or the whole plane.*

8. Sets of points as algebraic hypersurfaces

Lemma 24. *Let S be a set of points of $\mathrm{AG}_k(\mathbb{F}_q)$. If*

$$|S| < \binom{n+k}{k}$$

then there exists a polynomial f of degree at most n with the property that

$$S \subseteq V(f) = \{x \in \mathrm{AG}_k(\mathbb{F}_q) \mid f(x) = 0\}.$$

Let N be a positive integer.

Let L be a set of lines of $\mathrm{AG}_k(\mathbb{K})$, D be the set of directions of these lines and let S be a set of points in $\mathrm{AG}_k(\mathbb{K})$ in which every line of L is incident with at least N points of S.

Theorem 25. *If $(k!|S|) < N^k$ then D is contained in an algebraic hypersurface of degree at most $(k!|S|)^{1/k}$.*

We define a N^{k-1} *grid* in $\mathrm{PG}_{k-1}(\mathbb{K})$ as a point set, which with respect to a suitable basis, has the form

$$\{\langle (a_1, \ldots, a_{k-1}, 1)\rangle \mid a_i \in A_i\},$$

where A_i is a subset of $\mathbb{K}$ of size N for all $i = 1, \ldots, k-1$.

Corollary 26. *If D is an N^{k-1} grid then $|S| \geqslant N^k/k!$.*

Corollary 27. *If $\mathbb{K} = \mathbb{F}_q$ and D is the set of all directions (i.e. $\mathrm{PG}_{k-1}(\mathbb{F}_q)$) then $|S| \geqslant q^k/k!$.*

One can construct good examples for $n = o(N)$ using the following theorem.

Theorem 28. *Suppose that L is a set of N lines of $\mathrm{AG}_2(\mathbb{K})$ and let S be a set of points with the property that every line of L is incident with N points of S. Suppose that there are N parallel lines m_i, which are incident with $\frac{1}{2}N - \epsilon_i$ points of S which themselves are incident with two lines of L, where $\epsilon_1, \ldots, \epsilon_N$ have the property that*

$$\sum_{i=1}^{N} \epsilon_i \leqslant dN,$$

for some constant d, not depending on N.

Then there is a set L' of N^{n-1} lines in $\mathrm{AG}_n(\mathbb{K})$, $n \leqslant \frac{1}{2}N + 1$, whose directions contain a N^{n-1} grid and a set of points S' with the property that every line of L' is incident with N points of S' and where S' has less than $2(\frac{1}{2}N)^n + c(n)N^{n-1}$ points.

Example 29. If $\mathbb{K} = \mathbb{F}_q$ and $N = q$ then we can take L to be the lines of a dual conic (or any oval), where one of the lines is taken to be the line at infinity π_2. The points of S will include the affine points incident with a line of L.

Let x be the point incident with π_2 and not incident with a line of L. The lines $m_1, \ldots, m_N$ will be the q affine lines incident with x. Suppose q is odd. Since each point not on the conic but incident with a tangent to the conic is incident with $(q-1)/2$ bisecants, we have $\epsilon = \frac{1}{2}$ for all $i = 1, \ldots, q$ before we add points to S. Adding N points to S does not affect the fact that the condition on the ϵ_i. If q is even then each point not on the conic but incident with a tangent to the conic is incident with $q/2$ bisecants, except one point which is incident with no bisecants. Therefore, $\epsilon_i = 0$ for $i = 1, \ldots, q-1$ and $\epsilon_q = \frac{1}{2}q$. Again, adding N points to S does not affect the condition on the ϵ_i.

Example 30. If $\mathbb{K} = \mathbb{R}$ then we can take L to be the set of lines dual to a regular N-gon. We dualise in such a way that the line at infinity becomes a point on the line at infinity. Let S be the set of affine points dual to the bisecants to the N-gon. This gives $N-1$ points on each line of L and we arbitrarily add an additional point to S incident with ℓ, for each line $\ell \in L$.

The line joining $(\cos(2\pi a/N), \sin(2\pi a/N), 1)$ and $(\cos(2\pi b/N), \sin(2\pi b/N), 1)$ meets the line at infinity in the point $(-\tan(\pi(a+b)/N), 1, 0)$, so there are precisely N points on the line at infinity where the bisecants meet.

Let $p_1, \ldots, p_N$ be the N points on the line at infinity where the bisecants meet. Let $m_1, \ldots, m_N$ be the N (parallel) lines dual to the points $p_1, \ldots, p_N$. Before we add points to S we have that if N is even then $\epsilon_i = 0$ for $i = 1, \ldots, \frac{1}{2}N$ and $\epsilon_i = 1$ for $i = \frac{1}{2}N+1, \ldots, N$ and if N is odd then $\epsilon_i = \frac{1}{2}$ for $i = 1, \ldots, N$, ordering the lines in a suitable way. Adding N points to S does not affect the condition on $\epsilon_1, \ldots, \epsilon_N$.

Theorem 31. *Suppose that L is a set of lines of $\mathrm{AG}_2(\mathbb{F}_q)$. If q is odd and L has a line for every direction then $|S| \geqslant q(q+1)/2 + (q-1)/2$. Moreover if $|S| = q(q+1)/2 + (q-1)/2$ then S comes from Example 29.*

9. Bezout's theorem

Theorem 32. *If $f, g \in \mathbb{K}[X, Y]$ have no common factor then $V(f) \cap V(g)$ contains at most $(\deg f)(\deg g)$ points.*

Theorem 33. *If $f, g \in \mathbb{K}[X, Y, Z]$ have no common factor then $V(f) \cap V(g)$ contains at most $(\deg f)(\deg g)$ lines.*

Example 34. *Let L' be the set of N^{1+2e} lines of $\mathrm{AG}_2(\mathbb{R})$,*

$$L' = \{y = mx + c \mid m \in \{1, \ldots, N^e\},\ c \in \{1, \ldots, N^{1+e}\}\},$$

and let S' be the of $2N^{2+e}$ points

$$S' = \{(x, y) \mid x \in \{1, \ldots, N\},\ y \in \{1, \ldots, 2N^{1+e}\}\}.$$

Every line of L' is incident with at least N points of S'.

By taking the union N^{1-2e} such planar examples one can obtain an example L of N^2 lines of $\mathrm{AG}_3(\mathbb{R})$ and a set S of $2N^{3-e}$ lines with the property that every line of L is incident with at least N points of S.

Theorem 35. *Let N be a positive integer and let a, b be positive numbers.*

Let L be a set of aN^2 lines in $\mathrm{AG}_3(\mathbb{K})$ with the property that at most bN of the lines of L are contained in a plane. Let S be a set of points with the property that every line of L is incident with at least N points of S.

If $\mathrm{char}(\mathbb{K}) = 0$ or $\mathbb{K} = \mathbb{F}_p$ where p is prime, then there is a constant $c = c(a, b)$ such that $|S| > cN^3$.

The proof of Theorem 35 uses Lemma 36 and Bezout's theorem. The proof of Lemma 36 uses dyadic pigeon holing and Lemma 24.

Lemma 36. *There is a constant $c = c(a,b)$ such that if $|S| < cN^3$ then there is a hypersurface $V(f)$, where f is absolutely irreducible of degree $d < \frac{1}{4}N$, subsets $S'' \subseteq S' \subseteq S \cap V(f)$ and subsets $L'' \subseteq L' \subseteq L$, with the property that each line of L' is incident with at least $4d$ points of S', each point of S'' is incident with at least $2m/(aN^2)$ lines of L', and each line of L'' is incident with at least $4d$ points of S'' such that*

$$|L''| > bdm/N.$$

Example 37. *Using Example 29 and Example 30 lifted to three dimensions by Theorem 28, one can consruct examples of Bourgain sets for which $c(1,1) = \frac{1}{4}$.*

Theorem 35 does not hold if $\mathbb{K} = \mathbb{F}_q$ and q is not a prime. In the following example q is assumed to be a square.

Example 38. *The Hermitian polar space H_r defined, for example, by the equation*

$$x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} + x_3^{\sqrt{q}+1} = 1,$$

has q^2 lines and $q^{2.5}$ points (ignoring smaller order terms) and has the property that there are at most $\sqrt{q}$ of the lines contained in any plane

10. The resultant of two polynomials

Let

$$f(X) = \sum_{i=0}^{n} f_i X^i, \quad g(X) = \sum_{i=0}^{n-1} g_i X^i$$

be polynomials in $\mathbb{K}[X]$ where f has degree n.

Let

$$b = X^m + \sum_{i=0}^{m-1} b_i X^i, \quad a(X) = \sum_{i=0}^{m-1} a_i X^i,$$

be such that

$$af + bg = 0.$$

Considering the coefficients of $X^{n+m-1}, \ldots, X^{n+m-1}$ gives $2m$ lienar equations which in matrix form are given by the equation

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

Note that $\deg g \geqslant n - m$, so the right-hand side is not zero.

Let $h = (f, g)$.

If $m \geqslant k+1$ then 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 ($b = \gamma f/h$, γ is chosen so that b is monic and $a = -b(g/h)$). Hence $\det R_m \neq 0$.

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

Lemma 39. *Suppose that 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 $y \in \mathbb{K}$ for which

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

then

$$\sum_{i=1}^{h} h n_h \leqslant \deg(\det R_m).$$

Theorem 40. *Let S be a set of points of $\mathrm{PG}_2(\mathbb{F}_q)$ and suppose that there is a point $p_\infty \notin S$ such that r lines incident with p_∞ contain all the points of S. Then the number of lines incident with S is at most*

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

11. Arcs

An *arc* S is a set of vectors of $\mathrm{V}_k(\mathbb{F}_q)$ in which every subset of S of size k is a basis of the space, i.e. every k-subset is a set of linearly independent vectors. Equivalently, we define an arc of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ as a set of points in which every subset of size k spans the whole space.

Exercise 12. *Let S be an arc of size n of $\mathrm{V}_k(\mathbb{F}_q)$. Prove that if $k \geqslant q$ then $n \leqslant k + 1$ and give an example where $n = k + 1$.*

Exercise 13. *Prove that*

$$S = \{(1, x, \ldots, x^{k-1}) \mid x \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\},$$

is an arc of $\mathrm{V}_k(\mathbb{F}_q)$ of size $q + 1$.

Exercise 14. *Prove that if $q = 2^h$ and $(e, h) = 1$ then*

$$S = \{(1, x, x^{2^e}) \mid x \in \mathbb{F}_q\} \cup \{(0, 0, 1), (0, 1, 0)\},$$

is an arc of $\mathrm{V}_3(\mathbb{F}_q)$ of size $q + 2$.

Exercise 15. *Prove that if $\eta^4 = -1$ then*

$$S = \{(1, x, x^2 + \eta x^6, x^3, x^4) \mid x \in \mathbb{F}_q\} \cup \{(0, 0, 0, 0, 1)\},$$

is an arc of $\mathrm{V}_5(\mathbb{F}_9)$ of size 10.

Let $\det(v_1, \ldots, v_k)$ denote the determinant of the matrix whose i-th row is v_i, a vector of $\mathrm{V}_k(\mathbb{F}_q)$, where we evaluate the determinant with respect to a fixed canonical basis.

If $C = \{p_1, \ldots, p_{k-1}\}$ is an ordered set of $k - 1$ vectors then we write

$$\det(u, C) = \det(u, p_1, \ldots, p_{k-1}).$$

Let A be a subset of S of size $k - 2$. Let $t = q + k - 1 - |S|$.

Lemma 41. *There are t hyperplanes of $\mathrm{V}_k(\mathbb{F}_q)$ which contain the vectors of A and no other vectors of S.*

Let $\alpha_1, \ldots, \alpha_t$ be pairwise linearly independent forms with the property that $\ker \alpha_i \cap S = A$. Define

$$f_A(x) = \prod_{i=1}^{t} \alpha_i(x),$$

a function from $\mathrm{V}_k(\mathbb{F}_q)$ to $\mathbb{F}_q$.

Lagrange interpolation gives the following lemma.

Lemma 42. *If E is a subset of S of size $t + k$ containing A then*

$$\sum_{e \in E \setminus A} f_A(e) \prod_{u \in E \setminus (A \cup \{e\})} \det(u, e, A)^{-1} = 0.$$

The lemma of tangents is the following.

Lemma 43. *For a subset D of S of size $k - 3$ and a subset $\{x, y, z\}$ of $S \setminus D$,*

$$f_{D \cup \{x\}}(y) f_{D \cup \{y\}}(z) f_{D \cup \{z\}}(x) = (-1)^{t+1} f_{D \cup \{x\}}(z) f_{D \cup \{y\}}(x) f_{D \cup \{z\}}(y).$$

Lemma 42 and Lemma 43 combine to imply that for any subset C of S of size $k - 1$ there is an $\alpha_C \in \mathbb{F}_q$ such that the following set of equations holds.

Lemma 44. *Let S be an arbitrarily ordered arc of size $q+k-1-t$ and let E be a subset of S of size $k+t$. For any subset A of E of size $k-2$,*

$$\sum \alpha_C \prod_{z\in E\setminus C} \det(z, C)^{-1} = 0,$$

where the sum runs over the subsets C of E of size $k-1$ containing A.

Lemma 44 is used to prove the following theorem. Recall that $q = p^h$, for some prime p.

Theorem 45. *Let S be an arc of $\mathrm{V}_k(\mathbb{F}_q)$. If $k \leqslant p$ then $|S| \leqslant q+1$. Moreover, if $k \leqslant p$ and $|S| = q+1$ and $k \neq (q+1)/2$ then S is a normal rational curve.*

For q even, define a polynomial in $k-1$ vector variables, so $k(k-1)$ indeterminates,

$$\phi_S(Y_1, \ldots, Y_{k-1}) = \sum_C \alpha_C \prod_{z\in E\setminus C} \frac{\det(z, Y_1, \ldots, Y_{k-1})}{\det(z, C)},$$

where the sum runs over all subsets C of size $k-1$ of E.

For q odd, define a polynomial in $k-1$ vector variables,

$$\phi_S(Y_1, \ldots, Y_{k-1}) = \sum_C \alpha_C^2 \prod_{z\in E\setminus C} \frac{\det(z, Y_1, \ldots, Y_{k-1})}{\det(z, C)},$$

where the sum runs over all subsets C of size $k-1$ of E.

Although ϕ_S is defined as a polynomial in $k-1$ vector variables, a simple change of variables shows that in fact it can be written as a polynomial in k indeterminates. Let

$$Z_i = (-1)^{i-1} \det(Y_1, \ldots, Y_{k-1}),$$

where the i-th coordinate of Y_j has been deleted, so the determinant is of a $(k-1)\times(k-1)$ matrix. Then

$$\phi_S = \phi_S(Z_1, \ldots, Z_k).$$

Theorem 46. *For any subset $A = \{a_1, \ldots, a_{k-2}\}$ of S of size $k-2$*

$$\phi_S(X, a_1, \ldots, a_{k-2}) = \alpha_A f_A(X),$$

if q is even and

$$\phi_S(X, a_1, \ldots, a_{k-2}) = \alpha_A^2 f_A(X)^2,$$

if q is odd.

Theorem 46 implies that the $\binom{|S|}{k-2}t$ points which are dual to the hyperplanes containing exactly $k-2$ points of S lie on the algebraic hypersurface $V(\phi_S)$.