APPLICATION OF LINEAR ALGEBRA IN COMBINATORICS

Xilogiannis Evangelos
Advisor : Mihalis Kolountzakis
University of Crete
Department of mathematics

May 2010

Acknowledgements

I would like to thank my adviser professor Prof. Mihalis Kolountzakis for the assistance he has provided me and also thank the other two members of my committee Profs Theodoulos Garefalakis and Eleni Tzanaki.

Contents

Chapter 1

Introduction

In the following pages we will examine the use of linear algebra in combinatorics. More precisely we will look at some theorems from the area of discrete geometry,extremal combinatorics and finite fields constructions. The dates of the results span from the beginning of the 20^{th} century (the Dehn theorem) to recent years (the Dvir theorem) . The tools used although may appear elementary they give powerful and interesting results .

Chapter 2

Useful Lemmas

First we will prove some theorems that we will make frequent use of.

Note In the following pages F will denote a finite field.

Definition Let U be a $m \times m$ matrix over R. If for all nonzero vectors x it is true that $xUx^T > 0$ we say that the matrix is positive definite. If it is true that $xUx^T \geq 0$ we say that the matrix is positive semidefinite.

Definition Let V be a linear space over Q. A linear function is a map

$$f : V \to Q$$

with the property that for all $a, b \in V$ we have

$$f(a + b) = f(a) + f(b)$$

We also know that if two elements $a, b \in V$ are linearly independent there is a linear function that $f(a) = 0$ and $f(b) = 1$.

Definition A symmetric $m \times m$ matrix B with real entries is positive semidefinite if for any $x \in R^m$ the quadratic form xB^Tx is nonnegative. If in addition the only case the quadratic form xB^Tx vanishes is only when x is itself zero then B is positive definite.

Theorem 1. ***(Schwartz 1980)*** *Let $f \in F[x_1, .., x_n]$ be a non zero polynomial with degree d and $\Omega \subseteq F$ be a set with $|\Omega| = N$. Let $Z(f, \Omega)$ denote the set of roots from Ω^n. Then*

$$|Z(f, \Omega)| \leq dN^{n-1}$$

Proof. By induction on n, the number of variables.
For $n = 1$ the number of roots cannot exceed the degree thus $|Z(f, \Omega)| \leq d$.
For $n \geq 2$ we write f in terms of the powers of x_n

$$f(x_1, ..., x_n) = g_0 + g_1 x_n + g_2 x_n^2 + ... + g_k x_n^k \tag{2.1}$$

where $g_i \in F[x_1, ..x_{n-1}]$, deg $g_i \leq d - i$ and g_k is not the zero polynomial. We choose an element $(a_1, ..., a_n)$ of $Z(f, \Omega)$ at random. There are two possible cases :

1) $g_k(a_1, ..a_{n-1}) = 0$
As $deg(g_k) \leq d - k$ by the inductive hypothesis the number of roots of g_k in the subset Ω^{n-1} is at most $(d-k)N^{n-2}$. Thus the possible maximal number of those tuples is $\leq (d-k)N^{n-1}$.

2) $g_k(a_1, ..a_{n-1}) \neq 0$
In this case we bound the number of tuples simply by N^{n-1}. Since a_n must now be a root of the non zero polynomial f of degree k, the number of possible choices for a_n is at most k. Hence this case results in at most kN^{n-1} roots of *f*.

The two upper bounds add to total of dN^{n-1} completing the proof.

□

The following lemma is an immediate consequence of the above.

Lemma 1. ***Small degree lemma*** *A polynomial in F^d of degree less than $q = |F|$ cannot vanish everywhere unless it is the zero polynomial*

Proof. Let P be a non zero polynomial. Since $deg(P) \leq |F| - 1$ by the Schwartz theorem the number of its roots cannot exceed the number $(|F| - 1)|F|^{n-1}$. By assumption this is a contradiction thus P must be identically zero. □

We will now establish some criteria regarding the linear independence of polynomials.

Lemma 2. ***(Diagonal Criterion)*** *For $i = 1, .., m$ let $f_i : \Omega \longrightarrow F$ be a function and $a_i \in \Omega$ elements such*

$$f_i(a_j) \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i \neq j. \end{cases}$$

then $f_1, ...f_m$ are linearly independent members of the space F^Ω

Proof. Let

$$\sum_{i=1}^{m} \lambda_i f_i(x) = 0$$

be a linear relation between the f_i. We substitute a_j for the variable x and what remains is $\lambda_j f_j(a_j) = 0$ which implies that $\lambda_j = 0$ for every j.

Thus the linear relation under consideration is the trivial one.

□

Lemma 3. ***(Triangular Criterion)*** *For $i = 1, ...m$ let $f_i : \Omega \longrightarrow F$ be a function and $a_i \in \Omega$ elements such*

$$f_i(a_j) \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i < j. \end{cases}$$

then $f_1, ...f_m$ are linearly independent members of the space F^{Ω}.

Proof. For a contradiction we assume there exists a nontrivial linear relation $\sum_{i=1}^{m} \lambda_i f_i = 0$ between the f_i. Let i_0 be the greater i such that $\lambda_i \neq 0$. We substitute a_{i_0} for the variable on each side. By the above condition for the $f_i(a_j)$ all but one terms vanish and what remains is

$$\lambda_{i_0} f_{i_0}(a_{i_0}) = 0$$

. Which implies that $\lambda_{i_0} = 0$. Which is a contradiction.

□

We will now present some classic and useful results in enumerate combinatorics.

Lemma 4. *The number of integer solutions to the equation*

$$x_1 + ... + x_n = r$$

under the condition that $x_i > 0$ for all $i = 1, ..., n$ is $\binom{r-1}{n-1}$

Proof. A typical solution to the above equation looks like this

$$(\bullet \bullet \bullet | \bullet | ... | \bullet \bullet)$$

that is the number of points $\bullet$ denote the size of x_i and the $|$ separate consecutive t x_i's. There are $r - 1$ possible places to put the $|$ and the cardinality of the $|$ is $n - 1$. Thus the number of possible configurations is $\binom{r-1}{n-1}$, and our proof is complete. □

Lemma 5. *The number of integer solutions to the equation*

$$x_1 + ... + x_n = r$$

under the condition that $x_i \geq 0$ for all $i = 1, ..., n$ is $\binom{n+r-1}{r}$

Proof. The proof is almost the same as the previous lemma the trick is to add n 'dummy' $\bullet$ in the initial configuration thus having $n+r-1$ possible places to put the $|$. (which will lead us to a number of $\binom{n+r-1}{r}$ possible solutions). For every configuration once me put the $|$ in place we remove the 'ghost' $\bullet$ and completing the proof. □

Lemma 6. *The number of monomials*

$$x_1^{a_1}x_2^{a_2}...x_n^{a_n}$$

with

$$a_1 + a_2 + ... + a_n \leq d$$

is $\binom{n+d}{d}$.

Proof. We can rewrite the above elements as $x^{a_1}x^{a_2}...x^{a_n}1^{a_{n+1}}$, we see that their cardinality is the number of possible integer solutions of the equation $a_1 + a_2 + ... + a_n + a_{n+1}$ under the condition $x_i \geq 0$. From the previous lemma this number is $\binom{n+d-1+1}{d+1-1}$ and the proof is complete.

□

Lemma 7. ***(Degree lemma)*** *Let $E \subseteq F^n$ be a set of cardinality less than $\binom{d+n}{n}$ for some $d \geq 0$. Then there exists a non zero polynomial $P \in F[x_1, ...x_n]$ on n varaibles of degree at most d which vanishes on E.*

Proof. Let V be the vector space of polynomials in $F[x_1, ...x_n]$ of degree at most d. The set of monomials

$$x^{a_1}x^{a_2}...x^{a_n}$$

with

$$a_1 + a_2 + ... + a_n \leq d$$

forms a basis for V. Thus V has dimension $\binom{n+d}{d}$. On the other hand the vector space F^E of F-valued functions on E has dimension

$$|E| \leq \binom{n+d}{d}$$

. Hence the evaluation map

$$P \mapsto (P(x))_{x \in E}$$

from V to F^E is non injective,and the claim follows.

□

Chapter 3

The Kakeya Problem

We will examine the Kakeya problem in which we had recently a breakthrough in Finite geometries thanks to Dvir, Tao, Sharir and other researchers.

A Besicovitch set is a subset of R^n which contains a unit line segment in each direction. Besicovitch sets are also known as Kakeya sets. The following is believed to be true .

Conjecture. A Besicovitch set in R^n must have Hausdorff dimension n.

The problem above looks like geometric measure theory. The motivation for studying it comes from harmonic analysis, analytic number theory, and PDE. And the techniques used to prove some (partial) results are mostly geometrical and combinatorial, additive number theory being the latest addition. It is generally expected that ideas from other, seemingly unrelated, fields of mathematics will be needed to finally resolve the problem. More information of the problem can be found in [6].

In 1999, Wolff posed the finite field analogue to the Kakeya problem, in hopes that the techniques for solving this simpler conjecture could be carried over to the Euclidean case.

Finite Field Kakeya Conjecture: Let F be a finite field, let $K \subseteq F^n$ be a Kakeya set, i.e. for each vector $y \in F^n$ K contains a line $\{x + ty : t \in F\}$ for some x ∈ F. Then the set K has size at least $c_n F^n$ where $c_n \to 0$ is a constant that only depends on n.

The above hypothesis was proved in 2008 from Zeev Dvir,his proof we are going to present in the following pages.

Definition 1. *A **Kakeya** set in F^n is a set $K \subset F^n$ that contains a line in every direction. More formally K is a Kakeya set if for every $x \in F$ there is a $y \in F$ such the line*

$$L_{x,y} = \{y + ax | a \in F\}$$

is contained in K

Theorem 2. ***(Dvir 2008)***
Let $K \subset F^n$ be a Kakeya set and $|F| = q$ then

$$|K| \geq C_n q^n$$

.

Proof. It is sufficient to show that all the Kakeya sets have size at least

$$\binom{q+n-1}{n}$$

since it is true that

$$\binom{q+n-1}{n} \geq \frac{(q+n-1)(q+n-2)...(q)}{n!} \geq \frac{q^n}{n!}$$

We will suppose there exists a kakeya set $K \subset F^n$ of size less than $\binom{q+n-1}{n}$. which will lead us to contradiction.

We make use of the degree lemma.

Thus there exists a polynomial $P \in F[x_1, ...x_n]$ of degree at most $q-1$ so that for every $x \in K$ is a root of P.

We can write

$$P = \sum_{i=0}^{q-1} P_i$$

where P_i denotes the homogeneous part of P of degree i.

Since K is a kakeya set for every $y \in F^n$ there exists $x \in F^n$ so that for every $a \in F$ we have $P(x+ay) = 0$. For a fixed pair of x and y $P(x+ay)$ is a polynomial on a of degree $d \leq q-1$.

Thus we can see that his polynomial vanishes in q different points. So by the Small degree lemma it must be identically zero and hence all its coefficients are zero. In particular the coefficient of a^{q-1} is zero (which can be seen to be exactly $P_{q-1}(y)$).

Since y was arbitrary by Schwartz lemma it follows that the polynomial P_{q-1} is identically zero.

Therefore

$$P = \sum_{i=0}^{q-2} P_i$$

and repeating this argument we conclude that the polynomials $P_{q-2}.P_{q-3}, ..., P_1$ are all identically zero.

Thus P is a constant $P_0 = 0$ as it vanishes at K.

A contradiction .

□

Note The original proof of the theorem can be found in [4]

Remark 1. *It is easy to see that $c_n = 1/n!$ above; this was recently improved to*

$$c_n = (1/2 + o(1))^n$$

which is best possible except for possible refinements of the $o(1)$ error.

The above proof can be found in [7].

Remark 2. *It is also possible, following **exactly** the same steps, to prove a weaker form of the theorem about (δ, γ)-kakeya sets.*

(A set $K \subset F^n$ is a (δ, γ)-kakeya set if there exists a set $L \subset F^n$ of size at least δq^n that for every $x \in L$ there is a line in the direction x that intersects K in at least γq points.)

Lemma 8. *Let $K \subset F^n$ be a (δ, γ)-kakeya set. Then :*

$$|K| \geq \binom{d+n-1}{n-1}$$

where

$$d = \lfloor q \min\{\delta, \gamma\} \rfloor - 2.$$

Remark 3. *Using the same machinery we can construct bounds on the size of Nikodym sets.*

A set B in F_q^n is Nikodym if for each $x \in B^c$ there exists a line L such that

$$L \cap B^c = \{x\}$$

In other worlds any point $x \in B^c$ belongs to a line that lies entirely in B (except for the point x itself).

Theorem 3. *Let F be a finite field with $|F| = q$ any Nikodym set $B \subset F^n$ satisfies*

$$|B| \geq \binom{q+n-2}{n}$$

Proof. We suppose that exists a Nikodym set $B \subset F^n$ of size less than $\binom{q+n-2}{n}$
By degree lemma there exists a non zero polynomial $P \in F[x_1, ..., x_n]$ on n variables of degree at most $d-2$ that vanishes on B.
By our initial assumption we have $B^c \neq \varnothing$ and in fact

$$|B^c| \geq q^n - \binom{q+n-2}{n}$$

.

Since B is a Nikodym set for every $x \in B^c$ there exist a line L_x such for every $y \in L_x \backslash \{x\}$ it is true $y \in B$, (and so $P(y) = 0$)
The restriction of P on the line L_x is a polynomial of degree at most $q-2$, and since it has $q-1$ roots (the points y) by Schwarz Lemma P is the zero polynomial.

As a result P is takes the value zero also on the point x. Since x was an arbitrary point of B^c and P is also identically zero in B it follows that P is identically zero in F^n. Thus by the Small degree lemma P is the zero

□

Note Unfortunately the above it is not a good bound. For example for the case $n = 2$ the bound will be

$$\binom{q+2-2}{2} = \frac{q(q-1)}{2} = \frac{q^2}{2} + O(q)$$

but us we see in the following theorem this bound can be improved to $2q^2/3 + O(q) > q^2/2 + O(q)$ for big enough q :

Theorem 4. ***(Liangpan Li 2008)*** *Any Nikodym set $B \subset F_q^2$ satisfies*

$$|B| \geq 2q^2/3 + O(q) \ (q \to \infty)$$

Proof. We set $s = \lfloor q/3 \rfloor$. First we assume that

$$|B^c| \geq s(q-1) + 2q$$

Since B is a Nikodym set, for each $x \in B^c$ there exists a line L_x such that

$$L_x \cap B^c = \{x\}$$

Obviously , all of these lines are distinct from each other since their points (except one) belong to B.
We know that the cardinality of the directions of lines laying in in F_q^2 is $\frac{q^2-1}{q-1} = q + 1$
We partition $\{L_x\}_{x \in B^c}$ into classes $\{G_i\}_{i=0}^q$ according to their directions. Without loss of generality we may assume that

$$|G_0| \geq |G_1| \geq |G_2| \geq ... \geq |G_q|$$

Thus

$$q + q + |G_2| \cdot (q-1) \geq \sum_{i=0}^{q} |G_i| = |B^c| \geq s(q-1) + 2q$$

from which yields

$$|G_2| \geq s$$

Since $|G_0| \geq |G_1| \geq |G_2|$ we can choose s parallel lines from each class G_0, G_1, G_2. We denote the new classes W_0, W_1, W_2, where $W_i \subset G_i$ and $|W_i| = s$.
Each line of class W_0 will have exactly $q-1$ points in B, and all those lines are parallel (they have no point in common). Thus

$$|B| \geq |B \cap W_0| = s(q-1)$$

We now check what the lines in class W_1. Each line of this class has exactly $q-1$ points in B, two (different) lines of W_1 have no point in common, and since we are on the plane each line of the class W_0 intersects with all the lines of the class W_1.

That is each line of the class G_1 has exactly $q-1-s$ points in B **not** belonging in W_0. Thus

$$|B| \geq s(q-1) + s(q-1-s)$$

Following the same analysis for the class W_2 we reach the conclusion that

$$|B| \geq s(q-1) + s(q-1-s) + s(q-1-2s) = 3s(q-1-s)$$

$$\geq 3(q/3-1)(q-1-q/3) = (q-3)(2q/3-1) = 2q^3 - 3q + 3 = 2q^3 + O(q)$$

Now for the case

$$|B^c| < s(q-1) + 2q$$

the proof is straightforward .

$$|B| = |F^2| - |B^c| > q^2 - s(q-1) - 2q \geq q^2 - q(q-1)/3 - 2q$$

Thus $|B| \geq 2q^2/3 + O(p)$.
Comparing the two cases we reach the desired conclusion.

□

Note The original proof can be found in [5]

Chapter 4

The Joints Problem

Using the linear algebra method we can give a good bound about the possible number of joints in the Euclidean spaces.

Definition A joint in R^d is a point incident to at least d lines, not all in a common hyperplane.

Theorem 5. ***(Sharir, Kaplan, Shustin, 2009)***
The maximum possible number of joints is R^d of a set of n lines is $O(n^{d/(d-1)})$

Proof. Let $m = |J|$ and $n = |L|$

Step 1 A bipartite graph
We construct the digraph D with the vertex set (L,J) were L are the lines in some possible configuration in R^d. J is the set of joints and the set of edges $E(D)$ denotes the obvious relation between the lines and the joints (that is a line in L is incident only to those joints in J that are actually it's points in R^n.)

Step 2 Pruning
We construct the subgraph D' with the following process :

If a line $l \in L$ is incident to fewer than $m/(2n)$ joints then we remove it from L and also all its incidents points of J.
This process stops when it is not possible to remove any more points.

Its is easy to see that we will delete at most $m/2$ points.
Indeed let L_2 be the set of deleted points, $\mu(l)$ denote the number of incident joints of an element $l \in L$ it is true that:

$$|L_2| \leq \sum_{l \in L : \mu(l) < \frac{m}{2n}} \mu(l) \leq \frac{|L|m}{2n} = \frac{m}{2}$$

Thus the vertex set of D' will be a (L', J') where

$$L' \subseteq L, J' \subseteq J$$

and every point of L' is incident to at least $m/(2n)$ surviving points. Of course since each joint belongs to at least d lines (and with the 'pruning' algorithm

is continuing to be true in the remaining sub-configuration) each point of J' is incident to at least d points of L' (not all in the same hyper plane).

Step 3 False assumption
We already know that $|J'| \leq m$ thus by the degree lemma there exists a d-variate polynomial P with degree at most b.
Where b is the smallest integer satisfying

$$m < \binom{b+d}{b}$$

which vanishes at all the points of J'.

We now search a bound of b. Since b is minimal it is true that:

$$Km > \binom{b+d}{b} \geq \frac{b^d}{d!}$$

for some large enough integer K. Thus

$$b < (Kmd!)^{1/d}$$

We will now assume that in some configuration of lines there are

$$m > An^{d/(d-1)}$$

joints. In order for our assumption to lead us a contradiction we must choose A big enough such that the number of surviving points (on each line) is greater than b (the degree of P).
In other worlds we must have

$$\frac{m}{2n} > b$$

Which will hold if

$$\frac{m}{2n} > (Kmd!)^{1/d} > b$$

That lead us to the relation

$$m > (2n)^{d/(d-1)}(Kd!)^{1/(d-1)}$$

And in order to be true we simply choose $A > (2)^{d/(d-1)}(Kd!)^{1/(d-1)}$

Now since the number of roots on each line (of the set L') of the polynomial P is greater than it's degree d by by the Schwartz lemma it vanishes identically on every line of L'.

Step 4 Differentiating
For every point $a \in J'$ we can parametrize all the points in it's incidence line L' as $a + tu$ $t \in R$, $u \in R^d$ with $||u|| = 1$ (Where $|| \bullet ||$ is the Euclidean norm).
For every neighborhood of a we have

$$P(a + tu) = P(a) + t\nabla P(a)u + O(t^2)$$

. (Always true since $P \in C^\infty$).
Since P is identically zero in each line l we have $\nabla P(a)u = 0$.

This holds for every (remaining) line incident to a. Since a is a joint we have seen that there are at least d lines in L'.

(Which lines actually span the entire R^d). So $\nabla P(a)$ being orthogonal to them all must be the zero vector.
Thus all the first-order derivatives of P vanish at a .

Step 5 Final Step
Lets us now consider the derivatives P_{x_i} the degree is at most $b-1$.Since:

a) Every line $l \in L'$ contains more than $b-1$ points of J'.

b) P_{x_i} vanishes at each and every point of those lines.

Then by Schwartz's lemma P_{x_i} must vanish identically on l.
That means all the first-order derivatives of P vanish on all the lines of L'.
We can repeat the above process to each of these derivatives and we can conclude that all partial derivatives of P vanish identically on of lines off L'.
This is **impossible** because eventually we must reach derivatives which are nonzero constants on R^d.

This is a contradiction.

□

Note. The original proof can be found in [4].

Chapter 5

Discrete geometry problems

In this chapter we will examine some problems of the field of discrete geometry and in particular the Distance problem (defined below)

The distance problem Let

$$U = a_1, a_2, ..., a_m$$

be a set of points in the euclidean space R^n. For the euclidean distance we make use of the euclidean norm L^2. Let $A \in R$ be the set of all possible distances between these points (the distance set). That is we have $||x_i - x_j|| \in A$,with $j \neq i$.

Let

$$K(n, l)$$

denote the maximal number m that there exists a family m of points U $|U| = K(n, l)$ in R^n with distance set $|A| = l$ we search bounds of the number $K(n, l)$.

First we will see how the linear algebra method can be used to give bounds in some special cases.

Lemma 9. *K(n,1)*$= n + 1$

Proof. We simply use the $(n+1)$-simplex polytope in every space R^n. Which is a maximal configuration (we cannot add more points to make it a $(n+2)$-simplex) and has $(n + 1)$ vertices.

□

Theorem 6. ***(Larman-Rogers-Seidel 1977)***

$$K(n, 2) \leq \binom{n}{2} + 3n + 2$$

Proof. We use the classic notation

$$||x|| = (\sum_{i=1}^{n} x_i^2)^{1/2}$$

for the Euclidean norm in R^n . Let U be a possible configuration of points U in R^n.

This set $U = a_1, a_2, ..., a_m$ gives birth to the following family of polynomials F

$$f_i(x) = (||x - a_i||^2 - d_1^2)(||x - a_i||^2 - d_2^2)$$

where d_1, d_2 are the elements of the two-point set A (the two possible distances).
We can easily see that

$$f_i(a_j) = \begin{cases} (d_1 d_2)^2 \neq 0 & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases}$$

By the triangular criterion these polynomials are linearly independent.

We now search the cardinality of the basis of (some) linear space in which they reside. If we expand a polynomial f_i of this family we can see that it is in fact a linear combination of the following (linearly independent) polynomials

$$(\sum_{i=1}^{n} x_i^2)^2, (\sum_{i=1}^{n} x_i^2)x_j, x_i x_j, x_i, 1$$

Using simple combinatorics to count their number we can see that their cardinality is actually

$$1 + n + (\binom{n}{2} + n + 1) = \binom{n}{2} + 3n + 2$$

The above number is the cardinality of the linear basis in question.

Since f_i are linearly independent their number cannot exceed the cardinality of their linear base this completes the proof.

□

Note The original proof can be found in [1].

We now make use of the linear algebra method for the general case $K(n, s)$

Theorem 7. ***(s-distance sets)*** *Using the notation above for the number of points $K(n, s)$ we have*

$$\binom{n+1}{s} \leq K(n, s) \leq \binom{n+s+1}{s}$$

Proof. **The upper bound** Let $y_1, .., y_m$ be a configuration of points in R^n having the distance set $A = \{d_1, ..., d_s\}$.

We once again construct the family F of polynomials

$$f_i(x) = \prod_{k=1}^{s} (||x - y_i||^2 - d_k^2)$$

and once again the polynomials f_i are linearly independent. Let L be the linear space which they generate.

We now search the cardinality of a basis of L. To do this we can use following trick.

1) We expand the norm-square expression in each factor of f_i and collect the squares. Thus the f_i's can be written as the sum of

$$(\sum x_i^2)^{k_0} x_1^{k_1} ... x_n^{k_n} \text{ with } \sum_{i=0}^{n} k_i \leq s$$

2) We set $z = \sum_{i=1}^{n} x_i^2$

In this way the f_i's can be seen as polynomials of $n+1$ variables, with degree at most s. The dimension of the linear space in which they reside is the number of homogenous polynomials on $n+1$ variables and degree at most s. Since this number is $\binom{n+s+1}{s}$ we achieve the desired bound.

The Lower bound Let us consider the incidence vectors of all s-subsets of a $n+1$ set. Let us name this set of vectors as W. This set lies on the hyperplane defined by the equation

$$\sum_{i=1}^{n+1} x_i = s$$

and therefore can be viewed as a subset of R^n.

It is easy to see that the cardinality of the distance set of the points of W is actually s. (The number of all possible different elements between 2 sets is an integer $a \in [0, ..., s]$.) Since the number of all s-subsets of a $n+1$ set is actually

$$\binom{n+1}{s}$$

we have achieved the desired bound.

□

If the configuration of points is less general we can achieve tighter bounds. For example:

Theorem 8. ***(Spherical s-distance sets)***
The maximum cardinality $K_s(n,s)$ of points in $S^{n-1} \subset R^n$ having distance set of size s is

$$\binom{n+1}{s} \leq K_s(n,s) \leq \binom{n+s-1}{s} + \binom{n+s-2}{s-1}$$

Proof. (The radius of the sphere clearly does not matter.)

The lower bound We consider all the (1,-1)-vectors in R^{n+1} with exactly s negative entries. Using simple combinatorics we can see that their number is

$$\binom{n+1}{s}$$

Clearly all these points belong to a sphere

$$S^n \subset R^{n+1}$$

and they also belong to the hyperplane defined by the equation

$$\sum_{i=1}^{n+1} x_i = n + 1 - 2s$$

And since the intersection of a hyperplane and a sphere is actually a sphere of lower dimension they can be viewer as a subset of

$$S^{n-1} \subset R^n$$

And since their distance set is actually s (the number of all possible different coordinates between 2 points) we have achieved the lower bound.

The upper bound To achieve the upper bound we proceed as in the linear case and construct a family D of linearly independent polynomials belonging to a linear space of the following base

$$(\sum_{i=1}^{n} x_i^2)^n, (\sum_{i=1}^{n} x_i^2)^a x_k ... x_l, x_i ... x_j, 1$$

For the next step we restrict the domain of the polynomials f_i in the unit sphere. The functions will remain independent (as members of the space of $S^{n-1} \to R$ functions), but now we see that they reside in a lower dimensional space than before.

That is we can drop $\sum_{i=1}^{2}$ from the list since it is a constant. We can also drop x_n^{2k} since

$$x_n^2 = 1 - \sum_{i=1}^{n-1} x_i^2$$

Thus the new base will have the following elements

$$x_1^{k_1} ... x_{n-1}^{k_{n-1}} \ , \ x_n (x_1^{b_1} ... x_{n-1}^{b_{n-1}})$$

$$\text{With } \sum_{i=1}^{n-1} k_i \leq s \text{ and } \sum_{i=1}^{n-1} b_i \leq s-1$$

The number of the above elements is

$$\binom{n+s-1}{s} + \binom{n+s-2}{s-1}$$

and the proof is complete.

□

More information about this family of problems can be found in [2]

Chapter 6

Extremal set theory

In this section we will use the polynomial technique to obtain some upper (and lower) bounds in the size of intersecting families.

Definition Let F be a family of subsets of some n-element set , and let

$$L \subseteq \{0, 1, ...\}$$

be a finite set of nonnegative integers .
We say that F is L-intersecting if

$$|A \cap B| \subseteq L$$

for every pair A, B of distinct members of F.

Theorem 9. ***(Frankl-Wilson 1981)*** *If F is an L-intersecting family of subsets of a set of n elements, then*

$$|F| \leq \sum_{i=0}^{|L|} \binom{n}{i}$$

Proof. (Due to Babai 1988. The original proof can be found in [2])

Let

$$F = \{A_1, ..., A_m\}$$

be the family in question. Without loss of generality we can assume that

$$|A_1| \leq |A_2| \leq .... \leq |A_m|$$

Let

$$L = \{l_1, ..., l_s\}$$

be the set of all intersection sizes. That is for every pair (i, j) with $i \neq j$ there is a k such that

$$|A_i \cap A_j| = l_k$$

We will now associate each set A_i with its incidence vector $u_i = (u_{i1}, .., u_{in})$, which we define as

$$u_{ij} = \begin{cases} 1 & \text{if } j \in A_i; \\ 0 & \text{if } j \notin A_i. \end{cases}$$

It is easy to see that

$$|A_i \cap A_j| = \langle u_i, u_j \rangle$$

where the form

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

is the standard inner product in R^n.

For our next step we construct the following family F of polynomials f_i for each $i = 1, ..., m$

$$f_i(x) = \prod_{k: l_k < |A_i|} (\langle u_i, x \rangle - l_k)$$

(We choose $x \in R^n$ so that the above polynomials f_i will be n-variable and well defined.)
We observe that

$$f_i(u_j) \begin{cases} \neq 0 & \text{for all } 1 \leq i \leq m, i = j \ ; \\ = 0 & \text{for all } 1 \leq j < i \leq m \ . \end{cases}$$

By the diagonal criterion the polynomials $f_1, f_2, ..f_m$ are linearly independent.

We now search for the cardinality of a basis of the linear space F. Because the domain (of the polynomials) is actually $\{0, 1\}$ we have $x_i^2 = x_i$ for each variable x_i.

Thus we see that all the $f_i's$ can be represented as sum of monomials . And we can see also that all the $f_i's$ have degree at most $s = |L|$ (due to the fact s is the number of all possible intersection sizes).

Thus the set of all monomials on (at most) n variables and degree (at most) s are a basis of the linear space F.

We can easily see that we have at most

$$\sum_{i=0}^{s} \binom{n}{i}$$

of them, so the proof is complete.

□

Using the same arguments we can prove the modular variation of the above theorem.

Theorem 10. ***(Deza-Frankl -Singhi 1983)***
Let $L \subseteq \{0, 1, .., p-1\}$ and p be a prime number. Assume that $F = \{A_1, .., A_m\}$ is a family of subsets of a set of n elements such that:

(a) *$|A_i| \notin L$ (mod p) when $(1 \leq i \leq m)$;*
(b) *$|A_i \cap A_j| \in L$ (mod p) when $1 \leq j < i \leq m$).*
Then

$$|F| \leq \sum_{i=0}^{|L|} \binom{n}{i}$$

Proof. We begin with a simple observation. Recall that a polynomial is multi-linear if it has degree ≤ 1 in each variable. Every multi-linear polynomial of degree $\leq s$ is a linear combination of monic multi-linear monomials (products of distinct variables) of degree $\leq s$.
We will also make use of the following lemma:

Lemma 10. ***(Multilinearization)*** *Let F be a field and $\Omega = \{0, 1\}^n \subseteq F^n$. If f is a polynomial of degree $\leq s$ in n variables over F then there exists (unique) multi-linear polynomial f' of degree $\leq s$ in the same variables such that*

$$f(x) = f'(x) \text{ for every } x \in \Omega$$

Proof. To prove this one can just expand f and use the identity $x_i^2 = x_i$, valid over Ω □

We once again introduce a polynomial $F(x, y)$ in $2n$ variables , this time $x, y \in F_p^n$,where F_p^n is the linear space of dimension n over F_p. We set

$$F(x, y) = \prod_{l \in L} (x \cdot y - l)$$

where

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

is the standard inner product in F_p^n. Now consider the n-variable polynomials

$$f_i(x) = F(x, u_i)$$

where

$$u_i \in F_p^n$$

is the incidence vector of the set

$$A_i \ (i = 1, ..., m)$$

. It is clear from the conditions that for $1 \leq i, j \leq m$

$$f_i(u_j) \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i \neq j. \end{cases}$$

These equations remain valid if we replace the f_i by the corresponding linear polynomials f_i'.
By the diagonal criterion these polynomials are linearly independent over F_p.

On the other hand all the f_i' are multi-linear polynomials of degree $\leq s$ and therefore belong to a space of dimension

$$\sum_{k=0}^{|L|} \binom{n}{k}$$

□

Theorem 11. ***(Bollobas). The original proof can be found in [1].*** *Let $A_1, ..A_m$ be sets of size r and $B_1, ..B_m$ be sets of size s such that*
(a) *$A_i \cap B_i = \varnothing$ for $i = 1, .., m$*
(b) *$A_i \cap B_j \neq \varnothing$ whenever $i \neq j$*
then we have

$$m \leq \binom{r+s}{s}$$

Proof. **(Due to Frankl)**
Let X be the union of all sets $A_i \cup B_i$. Let $T(X)$ be an enumeration of the elements of X. We associate each $x \in X$ with a vector

$$F : x \to \langle 1, T(x), ..., T^r(x) \rangle$$

Every $r+1$ of these vectors are linearly independent, since $(1, T(x), ..., T^r(x))$ are points in the moment curve $(1, t, ..., t^r) \subseteq R^{r+1}$.

Now each subset $W \subset X$ we associate it with a polynomial $f_W(y)$ of $r+1$ variables in the following way:

$$f_W(y) = \prod_{u \in W} (y \cdot F(u))$$

It is easy to see that $f_{B_j}(x) = 0$ if and only if $F(u) \cdot x = 0$ for some $u \in B_j$.

The vectors corresponding to the elements of A_i generate a sub-space S_i of dimension r. Let a_i be a nonzero vector orthogonal to S_i.

From **b** follows that $f_{B_i}(a_j) = 0$ if $i \neq j$. Since every $r+1$ vectors $F(x), x \in X$ are linearly independent it follows from **a** and the fact that $dim(S_i) = r$ that

$$dim(\langle F(A_i) \cup F(B_i \rangle) = r + 1$$

From the above and since a_i is a non-zero vector orthogonal to S_i we conclude that $f_{B_i}(a_i) \neq 0$.

Thus by the diagonal Criterion the polynomials are linearly independent. And since they are homogenous of degree s in $r+1$ variables their number is at most

$$\binom{(r+1)+s-1}{s}$$

and the proof is complete.

□

Theorem 12. ***(Nonuniform Fisher Inequality)*** *Let $C_i, ..., C_m$ be distinct subsets of a set of n elements satisfying the following condition :*

$|C_i \cap C_j| = \lambda$ for some integer λ with $1 \leq \lambda < n$ and for every $i \neq j$ Then $m \leq n$

Proof. First we separate the case that one of the sets C_i has λ elements. Then all the others must contain this one and be disjoint otherwise. It follows that

$$m \leq n + 1 - \lambda \leq n$$

The second case will be that all the sets in question have more than λ elements that is that the numbers

$$\gamma_i = |C_i| - \lambda$$

are all positive.

We construct the incidence matrix M of the set system. (Where $\{M_{ij}\} = 1$ if the jth element belongs to the ith set, and zero otherwise). This condition can be summarized in the following matrix equation :

$$A = MM^T = \lambda J + C$$

where J is the all ones $m \times m$ matrix and C is the diagonal matrix

$$C = diag(\gamma_1, ..., \gamma_m)$$

We will now prove that A is of full rank. We will make use of the following lemma.

Lemma 11. *All positive definite matrices have full rank .*

In order to use the above lemma we will prove that λJ is positive semidefinite and C is positive definite. Indeed let

$$x = (x_1, ..., x_m) \in R^m$$

For a $m \times m$ matrix $U = (\mu_{ij})$ we have

$$xUx^T = \sum_{i=1}^{m} \sum_{i=1}^{m} \mu_{ij} x_i x_j$$

Thus

$$x\lambda Jx^T = \lambda(x_1 + ... + x_m)^2$$

And

$$xCx^T = \gamma_1 x_1^2 + ... + \gamma_m x_m^2$$

which justify both claims . Now it is obvious by the definition in chapter [2] that the sum of a positive definite and a positive semidefinite matrix is positive definite. Thus A is positive definite , thus it has full rank . Now we can see that

$$m = rk(A) \leq rk(MM^T) \leq rk(M) \leq n$$

and the proof is complete . □

Chapter 7

Hilbert's Third problem

The first of the famous Hilbert's problems that was solved was Problem 3. Although the first proof was complicated we will present a greatly simplified one in the spirit of the previous chapters.

First we will need some definitions.

Definition 2. *We call two polyhedra in R^3 equidissectible if one can dissect each of them by a finite number of plane cuts so that the resulting two sets of smaller polyhedra can be paired off into congruent pairs . In other words , one can cut up one of them and then reassemble the pieces to obtain the other*

Theorem 13. ***(M. Dehn, 1900)*** *There are two polyhedra in R^3 that are not equidissectable.*

Proof. In order to prove the above theorem we will need the following fact. Let

$$a = \arccos(1/3)$$

Then a/π is irrational.

Proof. Suppose the contrary. Then there exist positive integers k, l such that $a/\pi = k/l$. Thus

$$a = \frac{k}{l}\pi \Rightarrow e^{ai} = e^{\frac{k}{l}\pi i} \Rightarrow (e^{ai})^{2l} = e^{2k\pi 1} = 1$$

$$1 = (e^{ai})^{2l} = (\frac{1}{3} + \sqrt{1 - \frac{1}{3^2}}i)^{2l} = (\frac{1}{3} + \frac{\sqrt{8}}{3}i)^{2l}$$

Now we claim that

$$(\frac{1}{3} + \sqrt{1 - \frac{1}{3^2}}i)^n = \frac{a_n}{3^{n+1}} + \frac{\sqrt{2}b_n}{3^{n+1}}i$$

This is true for $n = 1$. Suppose it holds for $n - 1$. Then

$$(\frac{1}{3} + \sqrt{1 - \frac{1}{3^2}}i)^n = (\frac{a_{n-1}}{3^{n+1}} + \frac{\sqrt{2}b_{n-1}}{3^n})(\frac{1}{3} + \frac{\sqrt{8}}{3}i)$$

Multiplying out the right hand side, one arrives at the formulas $a_n = a_{n-1} - 4b_{n-1}$ and $b_n = b_{n-1} + 2a_{n-1}$.

Note that $a_1 = 1$ and $b_1 = 3 = -1\ mod(3)$. Plugging into the above recursions, we see that $a_2 = -1\ mod(3)$ and $b_2 = 1\ mod(3)$. Plugging in once more we get $a_3 = 1\ mod(3)$ and $b_3 = -1\ mod(3)$, whereupon the cycle repeats. In particular, b_n is never congruent to zero modulo three. which leads us to contradiction. Thus the proof is complete. □

A *dihedral angle* is the angle subtended by two half-planes with a common bounding line (the "spine"). Let as consider the following two polyhedra in R^3 :

a) The regular simplex.

b) The cube .

Using simple analytic geometry we see that all the dihedral angles at the edges of the cube are $\pi/2$ radians , and the for the angles of the regular simplex (at it's edges) are a radians.

We assume (for a contradiction) that the regular simplex and the cube are equidissectible. Let $b_1, ..., b_m$ be all the dihedral angles that occur at edges of the smaller polyhedra obtained in the course of dissection. Let V denote the set of all linear combinations of the b_i with rational coefficients. Then V is a (finite dimensional) linear space over Q. Therefore, it follows that there exists a linear function

$$f : V \to Q$$

such that $f(\pi) = 0$ and $f(a) = 1$. We also note that $f(\pi/2) = 0$ follows.

Let us now consider, for each polytope P arising in the dissection process the so-called *Dehn invariant* of P with respect to f:

$$W(P) = \sum |e_i| f(c_i)$$

where the summation extends over all edges e_i of P, $|e_i|$ denotes the length of e_i and c_i is the dihedral angle of P at e_i.

Lemma 12. *The Dehn invariant is additive.*

In other words if we cut a polyhedron to pieces, the W-values of the pieces add up to the W-value of the whole.

Proof. It suffices to prove this for a single cut

$$P = P_i \cup P_2$$

where the two pieces are cut apart along a plane S and have disjoint interiors. We will show that

$$W(P) = W(P_1) + W(P_2)$$

Let us expand each term above and examine what happens to the terms on the left hand side of the resulting equation.

The terms corresponding to edges not cut by S show up intact on the right hand size. If S cut across some edge e_i, it divides e_i , into two pieces both still attach to the same dihedral angle c_i, so the corresponding two terms on the right hand side add up to $|e_i|f(c_i)$. If cuts into the spine (the edge e_i lies in the hyperplane S) then S splits the dihedral angle c_i and leaves the e_i unaltered. The additivity of f guarantees the that the balances of the two sides is once again maintained.

Finally, we have to consider the contribution of the new edges arising along S but not appearing along P. Let e be such an edge (common in P_1 and P_2) and c_i the corresponding dihedral angle in P_i. It is obvious that

$$c_1 + c_2 = \pi$$

. Therefore the contribution of this edge is

$$|e|f(c_1) + |e|f(c_2) = |e|f(c_1 + c_2) = |e|f(\pi) = 0$$

This completes the proof of the additivity lemma .

□

The following corollary is immediate.

Corollary 1. *If two polyhedra are equidissectible then they have the same Dehn invariants*

For the final step we see that the Dehn invariant of the cube is 0 (since $f(\pi/2) = 0$) , while the Dehn invariant of the regular simplex is not (since $f(a) \neq 0$) The proof is complete .

□

Chapter 8

References

1. S. Jukna , Extremal Combinatorics , Springer-Verlag , 2001
2. L. Babai and P. Frankl , Linear Algebra Methods in Combinatorics , Preliminary Version , University of Chicago , 1992
3. R.A. Brualdi, Introductory Combinatorics , Fourth Edition , Prentice Hall , 2004
4. Z. Dvir , On the size of Kakeya sets in finite fields , arXiv:0803.2336v3
5. L. Li , On the size of Nikodym sets in finite fields , preprint
6. T. Wolff , Recent work connected with the Kakeya problem , Prospects in mathematics , 129 - 162 , Amer. Math . Soc. , Providence ,RI, 1999.
7. L. Guth , H. Katz , Algebraic Methods In Discrete Analogs Of The Kakeya Problem , arXiv:0812.1043v1