Linear Algebra methods in Combinatorics

Daniël Kroes
dkroes@ucsd.edu

Jacob Naranjo
janaranj@ucsd.edu

Jiaxi Nie
jin019@ucsd.edu

Jason O'Neill
jmoneill@ucsd.edu

Nicholas Sieger
nsieger@ucsd.edu

Sam Sprio
sspiro@ucsd.edu

Emily Zhu
e9zhu@ucsd.edu

Fall 2019 Quarter

Abstract

Linear algebra tools have been used to solve many problems in extremal combinatorics. The far reaching nature of the subject matter has resulted in a book [4] written by Babai and Frankl. Many of the proofs in the area are short, elegant and straightforward and as a result fit perfectly in a graduate student seminar. We will start with a few results which are fundamental in extremal set theory including the oddtown/eventown problem and the Frankl-Wilson Theorem. The seminar will culminate with some big results in the past few years including the method of slice rank to solve capset problem and the recently solved sensitivity conjecture.

1 Introduction

These notes are comprised from an eight lecture series for graduate students in combinatorics at UCSD during the Fall 2019 Quarter. The organization of these expository notes is as follows. Each section corresponds to a fifty minute lecture given as part of the seminar. We shall first establish some common notation.

1.1 Notation

Throughout these notes, we let $[n] := \{1, 2, \ldots, n\}$ and consider

$$2^{[n]} := \{A \subset [n]\}.$$

Moreover, we are interested in the collection of size k subsets of an n-element set which we denote as $\binom{[n]}{k} := \{A \subset [n] : |A| = k\}$.

We denote subfamilies of $\binom{[n]}{k}$ and $2^{[n]}$ by calligraphic letters, sets by capital letters and elements by lower case letters. When the ground set is clear, we will use $\overline{X}$ to denote the complement of X.

Contents

2 Oddtown/Eventown [5, 20]

The first problem we will investigate considers a town of n people which we may think of as $[n]$ and a collection of clubs within this town which we may view as subsets of $[n]$. By insisting that the clubs have a particular size modulo 2 and that distinct pairs of clubs intersect at a particular size modulo 2, we then want to maximize the number of clubs one can have in this situation. We thus get a collection of four possible problems.

Definition 2.1. Let n be a positive integer, and let $\mathcal{F}$ be a collection of subsets of $[n]$ such that

1. $|F|$ is even (odd) for any $F \in \mathcal{F}$;
2. $|F \cap F'|$ is even (odd) for any distinct $F, F' \in \mathcal{F}$.

Then $\mathcal{F} \subset 2^{[n]}$ is said to follow *eventown eventown rules* (analogously for the other possibilities.)

Frankl and Tokushige [16] treat the even/even and odd/even case of this problem. They are interested in

$$f_{e,e}(n) := \max_{\mathcal{F} \subset 2^{[n]}} \{|\mathcal{F}| : \mathcal{F} \text{ follows eventown/eventown rules.}\}$$

Moreover, we define $f_{e,o}(n), f_{o,o}(n), f_{o,e}(n)$ analogously.

Theorem 2.2. *For all $n \geq 1$, $f_{e,e}(n) = 2^{\lfloor n/2 \rfloor}$.*

Theorem 2.3. *For all $n \geq 1$, $f_{o,e}(n) = n$.*

For the construction for Theorem 2.3, one can simply take $\mathcal{F} = \{\{i\} \ : \ i \in [n]\}$. For Theorem 2.2, one may take

$$\mathcal{F} = \left\{ \bigcup_{i \in S} \{2i-1, 2i\} \ : \ S \subseteq [\lfloor n/2 \rfloor] \right\}.$$

Given a subset $F \subset [n]$, we can form its characteristic vector $x_F \in \{0,1\}^n$ where we let

$$(x_F)_i = 1 \iff i \in F.$$

Proof of Theorem 2. Let x_F be the characteristic vectors of $F \in \mathcal{F}$. Then

$$\langle x_F, x_{F'} \rangle = |F \cap F'| = 1 \pmod 2 \iff F = F'.$$

Therefore, given a linear combination $0 = \alpha_1 x_{F_1} + \cdots + \alpha_m x_{F_m}$, one gets

$$0 = \langle \alpha_1 x_{F_1} + \cdots + \alpha_m x_{F_m}, x_{F_i} \rangle = \alpha_i$$

for all $i \in [m]$ and hence $\{x_{F_1}, \ldots, x_{F_m}\}$ is linearly independent and hence $m \leq n$ as desired.

This approach doesn't work in the even/even case. The reason is that in this case, $x_F \cdot x_F = 0$ too, and so the linear independence argument doesn't hold true anymore. And in fact, this observation is the key to the proof of the first theorem.

Proof of Theorem 1. Let V be the subspace spanned by the x_F, then $|\mathcal{F}| \leq 2^{\dim V}$. Recall that

$$\begin{aligned} V^\perp &= \{u \in \mathbb{F}_2^n \ : \ u \cdot v = 0 \text{ for all } v \in V\} \\ &= \{u \in \mathbb{F}_2^n \ : \ u \cdot c_F = 0 \text{ for all } F \in \mathcal{F}\}. \end{aligned}$$

is a subspace satisfying $\dim V + \dim V^\perp = n$. By the above observations, $x_F \in V^\perp$ for all $F \in \mathcal{F}$, hence $V \subseteq V^\perp$, so $n = \dim V + \dim V^\perp \geq 2 \dim V$, proving $\dim V \leq \lfloor n/2 \rfloor$. □

Theorem 2.4. *For all $n \geq 1$, $f_{e,o}(n) \leq n$.*

Proof. Assume that $|\mathcal{F}| = n + 1$. There must exist $\alpha_F \in \mathbb{F}_2$ not all zero with

$$\sum_F \alpha_F x_F = 0.$$

In this case $x_F \cdot x_{F'} = 1$ if $F \neq F'$ and 0 if $F = F'$, so taking the inner product with x_G we find

$$0 = \sum_{F \neq G} \alpha_F$$

which holds for any $G \in \mathcal{F}$. This shows that $\alpha_F = 1$ for all $F \in \mathcal{F}$.

In particular, $0 = \sum_{F \neq G} 1 = |\mathcal{F}| - 1 = n$, hence $|\mathcal{F}|$ is odd and n is even. But now, by duality, $\overline{\mathcal{F}} = \{\overline{F} \ : \ F \in \mathcal{F}\}$ is also a set satisfying the desired conditions. Therefore,

$$0 + 0 = \sum_{F \in \mathcal{F}} c_F + \sum_{F \in \mathcal{F}} c_{\overline{F}} = |\mathcal{F}| \cdot \mathbf{1},$$

contradicting the fact that $|\mathcal{F}|$ is odd. To achieve $|\mathcal{F}| = n - 1$, take $\mathcal{F} = \{\{i, n\} \ : \ i \in [n-1]\}$. In fact, if n is odd one can add $\{1, 2, 3, \ldots, n-1\}$ to achieve the upper bound of n. □

2.1 Fischer's inequality

Another problem is if one considers the case where we impose that all intersections have size $k < n$.

Theorem 2.5. *Let $\mathcal{F} \subseteq 2^{[n]}$ be so that such that $|F \cap F'| = k$ for any $F \neq F' \in \mathcal{F}$. Then $|\mathcal{F}| \leq n$.*

Proof. Again let x_F be the characteristic vectors, but this time over $\mathbb{R}$. Then $x_F \cdot x_{F'} = k$ for all $F \neq F'$. Assume $|\mathcal{F}| = n + 1$, then we have a non-trivial linear combination $0 = \sum_{F \in \mathcal{F}} \alpha_F x_F$. Taking the squared norm of this we find

$$0 = \sum_{F \in \mathcal{F}} \alpha_F^2 |F| + \sum_{F \neq F'} \alpha_F \alpha_{F'} k = k \left(\sum_{F \in \mathcal{F}} \alpha_F \right)^2 + \sum_{F \in \mathcal{F}} \alpha_F^2 (|F| - k).$$

But we note that $|F| - k \geq 0$, with equality holding at most once, so at most all but one of the α_F must be 0. But then all α_F are zero, contradicting that our linear combination was non-trivial. □

This theorem has a nice application to a problem made famous by Erdős [13].

Theorem 2.6. *Consider a set of n points in the plane. Then either they are all collinear, or there exist at least n lines containing at least 2 of these points.*

One can prove this theorem by induction, by first proving that if the points are not all collinear there exists some line containing exactly 2 of the points. However, there also is a proof using Fischer's inequality.

Proof. Assume not all points lie on a line. Let L be the set of lines determined by these points. For each point p let $A_p \subseteq L$ be the set of lines containing p. Since not all points are collinear, $A_p \neq A_q$ for different points p and q. Finally, $|A_p \cap A_q| = 1$ for $p \neq q$, since there is a unique line passing through p and q. By the above theorem, the number of sets of the form A_p is at most $|L|$, i.e. $n \leq |L|$. □

3 The Graham-Pollak Theorem [19]

The motivation for this problem derives from a communication network consisting of one-way loops connected at various points and trying to decide how to get a sequence of loops to follow to get to the destination. Graham and Pollak [19] treated the loops as vertices which were labeled an element of $\{0, 1, \star\}$ in a manner so that the Hamming distance between the strings corresponds to the distance in the graph. We then can decide the sequence of loops by traveling in decreasing Hamming distance. This problem can also be viewed as embedding the graph into a *squashed* cube. The case where the graph is the complete graph K_n is the nature of the Graham-Pollak theorem.

Theorem 3.1. *For $n \geq 1$, K_n can be embedded into an $(n-1)$-dimensional squashed cube and this is best possible.*

Associating subgraphs with certain quadratic forms, it turns out this is equivalent to the following.

Theorem 3.2 (Graham-Pollak [19])**.** *If K_n is decomposed into m-edge disjoint complete bipartite subgraphs, then $m \geq n - 1$.*

We first note that $n - 1$ is best possible as K_n may be written as $(n - 1)$ edge disjoint stars. However, there are also many other constructions which achieve $(n - 1)$ complete bipartite graphs.

Alon [2] also explored the following generalization of the problem.

Definition 3.3. For a graph G, a collection of complete bipartite graphs is said to be a *bipartite covering of order k* of a graph G if every edge of G lies in at least 1 and at most k of them.

Theorem 3.4. [2] *If there exists m complete bipartite graphs which form a bipartite covering of order k for K_n, then $m \geq \theta(kn^{\frac{1}{k}})$.*

The first proof we will present in this seminar is a proof by Tverberg [32].

Proof. Let $V = [n]$ and let $\{G_1(A_1, B_1), \ldots, G_m(A_m, B_m)\}$ be edge disjoint bipartite graphs which cover K_n. For each vertex i, we consider the corresponding variable x_i and for each $i \in [m]$, let

$$L_i := \sum_{j \in A_i} x_j \quad \text{and} \quad M_i := \sum_{j \in B_i} x_j.$$

Since the complete bipartite graphs partition $E(K_n)$,

$$\sum_{1 \leq i < j \leq n} x_i x_j = L_1 M_1 + \cdots + L_m M_m$$

as we have that $x_i x_j$ appears in $L_k M_k$ if and only if $\{i, j\} \in E(G_k(A_k, B_k))$. Seeking a contradiction, suppose that $m \leq n-2$. Then the system $L_i = 0$ for $i \in [m]$ together with $x_1 + \cdots x_m = 0$ consists of at most $n-1$ solutions in n variables and hence there is a nontrivial solution $\vec{a} := (a_1, \ldots, a_n)$. This yields a contradiction as

$$0 < \sum_{i=1}^{n} a_i^2 = (\sum_{i=1}^{n} a_i)^2 - 2 \sum_{1 \leq i < j \leq n} a_i a_j = 0^2 - 2\Big[L_1 M_1(\vec{a}) + \cdots + L_m M_m(\vec{a})\Big] = 0.$$

□

Peck [27] also proved the Graham-Pollak Theorem using an upper-triangular notion of adjacency matrices and properties of sums of matrices.

Proof. Let $\{G_1, \ldots, G_m\}$ be a collection of bipartite graph which form a edge-disjoint union of the complete graph K_n. For each of these graphs, we consider the upper-triangular adjacency matrix M_i so that for $j < k$, we let $(M_i)_{j,k} = 1$ if and only if $\{i, j\} \in E(G_i)$ and otherwise we let $(M_i)_{j,k} = 0$. Letting J_n be the upper-triangular matrix which consist 0's on the diagonal and 1's elsewhere (the upper-triangular adjacency matrix of K_n),

$$J_n = \sum_{i=1}^{m} M_i.$$

Noting that $\text{rank}(M_i) = 1$ and that $\text{rank}(J_n) = n-1$ and using the subadditivity of $\text{rank}(\cdot)$,

$$n - 1 = \text{rank}(J_n) \leq \sum_{i=1}^{m} \text{rank}(M_i) = m.$$

□

3.1 Extensions of Graham-Pollak

Babai and Frankl [4] have a similar proof using the upper-triangular notion of adjacency matrices. More recently, Vishwanathan [33, 34] gave a polynomial space proof and a counting proof of the Graham-Pollak theorem. We refer the reader to these sources for further proofs. We finish by noting that there is a hypergraph variant of Graham-Pollak for which we wish to cover $K_n^{(r)}$ by complete r-partite r-uniform hypergraphs. Let $f_r(n)$ denote the minumum number of complete r-partite r-uniform hypergraphs needed to cover each edge of the complete r-uniform hypergraph exactly once. Then, letting $l := \lfloor \frac{r}{2} \rfloor$, Alon [1] proved that

$$2\binom{2l}{l}^{-1}(1+o(1))\binom{n}{l} \le f_r(n) \le (1-o(1))\binom{n}{l}.$$

4 Multilinear Polynomials [3, 30]

The main purpose of the talk is proving the nonmodular analog of the Frankl-Wilson theorem which we will prove in Section 6.

Theorem 4.1 (Frankl-Wilson [17])**.** *Let p be prime and let $L \subset [0, p-1]$ and $k \notin L (mod\ p)$ with $|L| = s$. Suppose $\mathcal{F} \subset \binom{[n]}{k}$ is so that for all $F_1 \neq F_2 \in \mathcal{F}$, $|F_1 \cap F_2| \in L$. Then $|\mathcal{F}| \le \binom{n}{s}$.*

We will use the method of Multilinear polynomials, as was initially done by Alon, Babai and Suzuki [3], to prove the following Theorem.

Theorem 4.2 (Ray-Chaudhiri-Wilson [28])**.** *Let $L \subset [0, k-1]$ with $|L| = s$. Suppose $\mathcal{F} \subset \binom{[n]}{k}$ is so that for all $F_1 \neq F_2 \in \mathcal{F}$, $|F_1 \cap F_2| \in L$. Then $|\mathcal{F}| \le \binom{n}{s}$.*

As in section 2, for a set $I \subset [n]$, we consider its characteristic vector $x_I \in \{0,1\}^n$ where we set $(x_I)_j = 1 \iff j \in I$ and abusing notation we will also consider its corresponding multilinear polynomial $x_I := \prod_{i \in I} x_i$. For ease of notation, we will denote $f(I) := f(x_I)$ and observe that

$$x_I(J) = \delta_{I \subset J}.$$

In order to prove Theorem 4.2, we will need the following lemma:

Lemma 4.3. *Let $f : \{0,1\}^n \to \mathbb{R}$ be so that $f(I) \neq 0$ for all $I \subset [n]$ with $|I| \le r$. Then, the set $\{x_I f : |I| \le r\} \subset \mathbb{R}^{\{0,1\}^n}$ is linearly independent.*

Proof. Suppose there is a non-trivial linear combination

$$\sum_{|I| \le r} \lambda_I x_I f = 0. \tag{1}$$

Let I_0 be an inclusion-minimal subset so that $\lambda_{I_0} \neq 0$. Plugging in I_0 into Equation (1) yields that

$$0 = \sum_{|I| \le r} \lambda_I x_I f(I_0) = \lambda_{I_0} x_{I_0} f(I_0)$$

as if $I \subset I_0$, then we have that $\lambda_I = 0$ since I_0 is inclusion minimal and if I is not a subset of I_0, then we have that $x_I(I_0) = 0$. This then yields $\lambda_{I_0} = 0$; a contradiction. ☐

We will now consider the following space of multilinear polynomials

$$V := \text{span}\left\{ \prod_{i \in I} x_i : |I| \le s \right\}$$

and note that

$$\dim(V) = \sum_{i=0}^{s} \binom{n}{i}.$$

We are now ready to prove Theorem 4.2. Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ be such a set system and for each $F_i \in \mathcal{F}$, define the polynomial

$$f_i(x) := \prod_{l \in L} (x_{F_i} \cdot x - l).$$

Noting that $f_i(v_j) \neq 0 \iff i = j$ yields that these polynomials, after doing the standard multilinear polynomial reduction, are linearly independent and hence we get

$$m \leq \dim(V) = \sum_{i=0}^{s} \binom{n}{i}$$

which is not quite the desired upper-bound.

Consider the following polynomial $g := (\sum_{i=1}^{n} x_i) - k$ and note that $g(x_{F_i}) = 0$ for all $F_i \in \mathcal{F} \subset \binom{[n]}{k}$. Now, we claim that the following set is linearly independent

$$\{f_i : i \in [m]\} \bigsqcup \{x_I g : |I| \leq s-1\}.$$

Consider a linear combination

$$0 = \sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \leq s-1} \mu_I x_I g. \tag{2}$$

Plugging in x_{F_j} into Equation (2) yields that $\lambda_j = 0$ for all $j \in [m]$. Thus equation (2) becomes

$$0 = \sum_{|I| \leq s-1} \mu_I x_I g$$

and then Lemma 4.3 yields that $\mu_I = 0$ for all $|I| \leq s-1$. As a result

$$m + \sum_{i=0}^{s-1} \binom{n}{i} \leq \dim(V) = \sum_{i=0}^{s} \binom{n}{i}$$

and hence the result follows.

4.1 Further applications

The method of multilinear polynomials also can be used the proof of the nonuniform variant of Frankl-Wilson.

Theorem 4.4 (Deza-Frankl-Singhi [11])**.** *Let p be prime and let $L \subset [0, p-1]$ be so that $|L| = s$ and $\mathcal{F} \subset 2^{[n]}$ such that for all $F_1 \neq F_2 \in \mathcal{F}$, $|F_1 \cap F_2| \in L$ and $|F_1| \notin L$, then $|\mathcal{F}| \leq \binom{n}{0} + \cdots + \binom{n}{s}$*

There is also the following nonmodular version of Theorem 4.4.

Theorem 4.5 (Snevily [30])**.** *Let $L \in \binom{[0,n-1]}{s}$ and $\mathcal{F} \subset 2^{[n]}$ so that for all $F_1 \neq F_2 \in \mathcal{F}$,*

$|F_1 \cap F_2| \in L$. *Then* $|\mathcal{F}| \leq \binom{n-1}{0} + \cdots + \binom{n-1}{s}$.

The above result may be seen as tight be taking

$$\mathcal{A} := \{A \subset [n] : 1 \in A; |A| \leq s+1\} \text{ or}$$

$$\mathcal{S}(2,3,7) = \{\{1,2,3\},\{3,4,5\},\{1,5,6\},\{1,4,7\},\{3,6,7\},\{2,5,7\},\{2,4,6\}\}.$$

5 The tensor product method and Exterior algebras [23]

Our main results for this section will be to establish some variants of the classical Bollobás set-pairs inequality, which we state below.

Theorem 5.1. [6] *Let* $A_1, \ldots, A_m \in \binom{[n]}{r}$ *and* $B_1, \ldots, B_m \in \binom{[n]}{s}$ *be such that* $|A_i \cap B_i| = 0$ *for all* $i \in [m]$ *and* $|A_i \cap B_j| > 0$ *for* $i \neq j$. *Then* $m \leq \binom{r+s}{r}$.

Note that this bound has no dependency on n, which is perhaps unexpected. Theorem 5.1 has a nice probabilistic proof. Here we'll give a linear algebra proof which will actually give us a stronger version of Theorem 5.1. The full proof will need some machinery, and we start by proving a weaker result to motivate our approach.

Proposition 5.2. *If* $A_1, \ldots, A_m$ *and* $B_1, \ldots, B_m$ *are as above, then* $m \leq (r+s)^r$.

Proof. Let $X = \bigcup A_i \cup B_i$. Let $W = \mathbb{R}^{r+s}$ and let $\{w_i : i \in X\} \subset W$ be a set of points in general position, i.e. any collection of $r+s$ of the w_i vectors are linearly independent. For each $I \subset X$, let $w_I = (w_{i_1}, \ldots, w_{i_l})$. If $A = \{a_1, \ldots, a_r\}$ and $B = \{b_1, \ldots, b_s\}$, define $f(w_A, w_B)$ to be the determinant of the matrix which has rows $w_{a_1}, \ldots, w_{a_r}, w_{b_1}, \ldots, w_{b_s}$ (in that order).
Because the w_i are in general position, it's not too difficult to see that $f(w_A, w_B) = 0$ if and only if $A \cap B \neq \emptyset$. In particular, $f(w_{A_i}, w_{B_j}) = 0$ if and only if $i \neq j$. We claim (and will prove later) that this implies the w_{A_i} vectors are linearly independent in $W' = (\mathbb{R}^{r+s})^r$. We conclude the result. □

Essentially, the proof gives a weak bound because we should really be modding W out by an appropriate equivalence relation. For example, we would like to say $w_A \sim w_{A'}$ if $f(w_A, w_B) = f(w_{A'}, w_B)$ for all B. Motivated by this, we wish to establish the following.

Theorem 5.3. *Let* W *be an* n*-dimensional* $\mathbb{F}$*-vector space. Then there exist maps* $f_k : W^k \to \mathbb{F}^{\binom{n}{k}}$ *and a pairing* $\beta_k : \mathbb{F}^{\binom{n}{k}} \times \mathbb{F}^{\binom{n}{n-k}} \to \mathbb{F}$ *such that*

$$\beta_k(f_k(w_1, \ldots, w_k), f_{n-k}(w_{k+1}, \ldots, w_n)) = \det(w_1, \ldots, w_n).$$

We call the f_k maps the wedge product and write $f_k(w_1, \ldots, w_k) = w_1 \wedge \cdots \wedge w_k = \bigwedge w_i$. We call the codomain of f_k the kth *exterior power* of W and denote it by $\bigwedge^k W$.

Proof. Index the coordinates of $\bigwedge^k W$ by $J \in \binom{[n]}{k}$. Define $(w_1 \wedge \cdots \wedge w_k)_J := \det(A_J)$, where A_J is the $k \times k$ matrix obtained by starting with the matrix with rows $w_1, \ldots, w_k$ and then restricting to the columns given by J. For example, with $n = 3$, $k = 2$, $w_1 = (0,0,1)$, and $w_2 = (1,0,0)$, we have $w_1 \wedge w_2 = (0,-1,0)$, with the coordinates corresponding to $\{2,3\},\{1,3\},\{1,2\}$. We note that

this is a reasonable guess for the definition of f_k since we know for $k = n$ this is the right answer, and because each coordinates of $w_1 \wedge \cdots \wedge w_k$ is naturally identified by an element of $\binom{[n]}{k}$.
If $x \in \bigwedge^k W,\ y \in \bigwedge^{n-k} W$, we define

$$\beta_k(x, y) := (-1)^{k(k+1)/2} \sum_J (-1)^{\sum_{j \in J}} x_J y_{\overline{J}}.$$

For example, take the previous example together with $w_3 = (0, 1, 0)$. Then the pairing gives

$$(-1)^2 \cdot ((-1)^3 \cdot 0 \cdot 0 + (-1)^4 \cdot -1 \cdot 1 + (-1)^5 \cdot 0 \cdot 0) = -1.$$

Note that this equals the determinant of the matrix with rows w_1, w_2, w_3, and we claim without proof that this is true in general. $\square$

We will often write $x \wedge y = \beta_k(x, y)$. Thus with these definitions

$$(\bigwedge_{i=1}^{k} w_i) \wedge (\bigwedge_{i=k+1}^{n} w_i) = \bigwedge_{i=1}^{n} w_i.$$

To prove results about the f_k maps, we utilize their most important properties. Namely, they are k-linear and "alternating,"[1] which means $w_i = w_j$ implies $f(w_1, \ldots, w_n) = 0$. Let $f : W^k \to T$ be any k-linear alternating function.

Lemma 5.4. *If $w_1, \ldots, w_k \in W$ are linearly dependent, then $f(w_1, \ldots, w_k) = 0$.*

Proof. Assume $\sum \lambda_j w_j = 0$ with $\lambda_i \neq 0$. Then

$$f(w_1, \ldots, w_{i-1}, 0, w_{i+1}, \ldots, w_k) = f(w_1, \ldots, w_{i-1}, \sum \lambda_j w_j, w_{i+1}, \ldots, w_k)$$

$$= \sum \lambda_j f(w_1, \ldots, w_{i-1}, w_j, w_{i+1}, \ldots, w_k) = \lambda_i f(w_1, \cdots, w_k),$$

and k-lineariy implies the lefthand side of this equation is 0. Because $\lambda_i \neq 0$, we conclude the result. $\square$

Corollary 5.5. *$\bigwedge^k w_i = 0$ iff the w_i are linearly dependent.*

Proof. The above lemma shows that linearly dependency implies $\bigwedge^k w_i = 0$. If the w_i are linearly independent, extend the vectors to a basis $w_1, \ldots, w_n$. Then

$$(w_1 \wedge \cdots \wedge w_k) \wedge (w_{k+1} \wedge \cdots \wedge w_n) = \det(w_i) \neq 0,$$

and this implies that $\bigwedge^k w_i \neq 0$. $\square$

Lemma 5.6. *If $\operatorname{span}(u_1, \ldots, u_k) = \operatorname{span}(v_1, \ldots, v_k)$, then $f(u_1, \ldots, u_k) = \lambda f(v_1, \ldots, v_k)$ for some $\lambda \neq 0$.*

[1] This implies that swapping coordinates flips the sign of the function, hence the name alternating. However, the converse of this statement is false in characteristic 2

This isn't too hard to prove using k-linearity and we omit its proof. The main upshot of this lemma is the following.

Corollary 5.7. *Let $T \le W$ be a k-dimensional subspace and let $\wedge T \in \bigwedge^k W$ be defined by $\bigwedge t_i$ for some basis $\{t_i\}$ of T. Then the choice of $\wedge T$ is unique up to a non-zero scalar.*

Corollary 5.8. *We say that subspaces $U_1, \ldots, U_r \le W$ are linearly independent if the vectors $\wedge U_1, \ldots, \wedge U_r$ are linearly independent. This is well defined.*

Lemma 5.9. *If $U, V \le W$ with $\dim U + \dim V = n$, then $(\wedge U) \wedge (\wedge V) = 0$ iff $U \cap V \neq 0$.*

Proof. Let $\{u_1, \ldots, u_r\}, \{v_1, \ldots, v_s\}$ be a basis. Then the determinant of the matrix with rows u_i and v_j will be 0 iff the two subspaces intersect trivially. □

5.1 Asymmetric Bollobás inequality for subspaces

With all this in mind, we can prove an asymmetric Bollobás inequality for subspaces.

Theorem 5.10. *Let W be a vector space with $U_1, \ldots, U_m$ r-dimensional subspaces and $V_1, \ldots, V_m$ s-dimensional subspaces with $U_i \cap V_i = 0$ and $U_i \cap V_j \neq 0$ if $i < j$, then $m \le \binom{r+s}{r}$.*

Proof. We can assume W has finite dimension, say n. Note that $n \ge r + s$ since $U_i \cap V_i = 0$. Assume $n = r + s$. Let $u_i := \wedge U_i \in \bigwedge^r W$ and $v_i := V_i \in \bigwedge^s W$. By Lemma 5.9, we have $u_i \wedge v_j \neq 0$ if $i = j$ and $u_i \wedge v_j = 0$ if $i < j$.

We wish to show that this implies the u_i vectors are linearly independent, which we do through a series of easy claims.

Claim 5.11. *If Ω is a set and $f_1, \ldots, f_m : \Omega \to T$ are such that there exist $a_1, \ldots, a_m \in \Omega$ satisfying $f_i(a_j) \neq 0$ if $i = j$ and $f_i(a_j) = 0$ if $i < j$, then the f_i's are linearly independent in T^Ω.*

Proof. Assume $\sum \lambda_i f_i = 0$. Then

$$0 = \sum \lambda_i f_i(a_m) = \lambda_m f_m(a_m) \implies \lambda_m = 0.$$

We can then show that $\lambda_{m-1} = 0$ by plugging in a_{m-1} on both sides, and by repeating this we conclude that $\lambda_i = 0$ for all i. □

Claim 5.12. *Let W', T be vector spaces, Ω a set, and $f : W' \times \Omega \to T$ a map that is linear in the first variable. If there are $w_i \in W'$ and $a_j \in \Omega$ such that $f(w_i, a_j) \neq 0$ if $i = j$ and $f(w_i, a_j) = 0$ if $i < j$; then the w_i are linearly independent.*

Proof. Define $f_i : \Omega \to T$ via $f_i(\omega) = f(w_i, \omega)$. By the previous claim the f_i are linearly independent. If $\sum \lambda_i w_i = 0$, then

$$\sum \lambda_i f_i(\omega) = f(\sum \lambda_i w_i, \omega) = 0,$$

a contradiction. □

By taking $W' = \bigwedge^r W$, $\Omega = \bigwedge^s W$ and f the wedge product, we conclude by the above claim that the u_i are linearly independent. Thus

$$m \leq \dim \bigwedge^r \mathbb{R}^{r+s} = \binom{r+s}{r}.$$

This proves the result when $n = r + s$. For $n > r + s$ one can take a suitable projection so that $n = r + s$. We omit the details. $\square$

With this we immediately derive an asymmetric version of Theorem 5.1.

Corollary 5.13. *Let $A_1, \dots, A_m \in \binom{[n]}{r}$ and $B_1, \dots, B_m \in \binom{[n]}{s}$ be such that $|A_i \cap B_i| = 0$ and $|A_i \cap B_j| > 0$ if $i < j$. Then $m \leq \binom{r+s}{r}$.*

Proof. Let $X = \bigcup A_i \cup B_i$ and take a vector space W with basis $\{e_i : i \in X\}$. For $A = \{a_1, \dots, a_r\}$ let $U_A := \text{span}\{e_{a_i}\}$, and similarly define V_B. Then the subspaces U_{A_i}, V_{B_i} satisfy the conditions of Theorem 5.10 and we conclude the bound. $\square$

We finish by noting the above result is tight by consider $[r + s]$ and for $m = \binom{r+s}{r}$ letting $A_1, \dots, A_m \subset \binom{[r+s]}{r}$ be the distinct size r subsets of $[r + s]$ and $B_1, \dots, B_m$ be the corresponding complements.

6 Inclusion matrices for Extremal problems [16, 17]

In this section, we want to select subsets of $[n]$, with a fixed size k, such that the sizes of the intersections are restricted to belong to some given set L. In this case, we have the following theorem.

Theorem 6.1 (Frankl-Wilson)**.** [17] *Let $n > k \geq s$ be positive integers, and let p be a prime number. Let $L \subseteq \{0, 1, \dots, p-1\}$ be a set of s integers. Assume that $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $k \notin L \mod p$ and*

$$|F \cap F'| \in L \mod p$$

for any $F \neq F'$ in $\mathcal{F}$. Then $|\mathcal{F}| \leq \binom{n}{s}$.

The main part of the proof of Theorem 6.1 will be the following lemma.

Lemma 6.2. *Let p be a prime, $f \in \mathbb{Q}[x]$ degree s and $\mathcal{F} \subseteq \binom{n}{k}$ be such that for $F, F' \in \mathcal{F}$,*

$$f(|F \cap F'|) \begin{cases} \not\equiv 0 \mod p \text{ if } F = F'; \\ \equiv 0 \mod p \text{ if } F \neq F'. \end{cases}$$

Then $\mathcal{F}$ is s-independent.

Proof. Since f is of degree s we can write $f(x) = \sum_{i=0}^{s} \alpha_i \binom{x}{i}$ for $\alpha_i \in \mathbb{Q}$. Let $M_i = M(\mathcal{F}, \binom{[n]}{i})$. Then the (F, F')-entry of $M_i M_i^T$ counts the number of i-element subsets contained in both F and F', which equals $\binom{|F \cap F'|}{i}$. Write $A = \sum_{i=0}^{s} \alpha_i M_i M_i^T$, such that the (F, F')-entry of A is equal to

$f(|F \cap F'|)$. By the assumptions, this is a diagonal matrix with nonzero entries on the diagonal (modulo p), hence A has full rank, i.e. $\text{rank}(A) = |\mathcal{F}|$.

One can check that

$$M(\mathcal{F}, \binom{[n]}{i}) \cdot M(\binom{[n]}{i}, \binom{[n]}{j}) = \binom{k-j}{i-j} M(\mathcal{F}, \binom{[n]}{j}),$$

hence the column space of M_j is contained in the column space of M_i when $i \leq j$. Therefore, the column space of A is contained in the column space of M_s, hence $|\mathcal{F}| \leq \text{rank}(A) \leq \text{rank}(M_s)$, showing that M_s has full rank as desired. □

Proof. Define $f(x) = \prod_{\ell \in L}(x - \ell)$. Then f satisfies the conditions of the above lemma, hence $|\mathcal{F}| \leq \binom{n}{s}$ by s-independence. □

An interesting question is whether or not we need p to be prime in Theorem 6.1. It turns out the result is false if we do not have this condition and we can see this by the following example. Let $\mathcal{G} = \{G \in \binom{m}{[11]} : \{1,2,3\} \subseteq G\}$, so that $|G \cap G'| \in \{3, 4, \ldots, 10\}$ when $G \neq G' \in \mathcal{G}$. Let $\mathcal{F} = \{\binom{G}{2} : G \in \mathcal{G}\}$, be a k-uniform family on $n = \binom{m}{2}$ vertices, where $k = \binom{11}{2} = 55 \equiv 1 \mod 6$.

One can check that

$$|F \cap F'| \in \left\{ \binom{i}{2} \ : \ 3 \leq i \leq 10 \right\} \equiv \{0, 3, 4\} \mod 6,$$

when $F \neq F'$. Now, $|\mathcal{F}| = |\mathcal{G}| = \binom{m-3}{8} = \Theta(m^8) = \Theta(n^4)$, so the Theorem 6.1 fails for $p = 6$ and $s = 3$.

6.1 Further applications

The method of Inclusion matrices can also be used to prove a t-intersecting version of Katona's shadow theorem. A family $\mathcal{F} \subset \binom{[n]}{k}$ is t-intersecting if for all $A, B \in \mathcal{F}$, $|A \cap B| \geq t$.

Theorem 6.3. *Let $1 \leq t \leq k \leq n$ and $\mathcal{F} \subset \binom{[n]}{k}$ a t-intersecting family, then for $u \in [k-t, k]$,*

$$\frac{|\sigma_u(\mathcal{F})|}{|\mathcal{F}|} \geq \frac{\binom{2k-t}{u}}{\binom{2k-t}{k}}$$

where $\sigma_u(\mathcal{F}) := \{S \in \binom{[n]}{u} : S \subset F \in \mathcal{F}\}$

Note that Equality may be obtained in Theorem 6.3 by taking $\mathcal{F} = \binom{[2k-t]}{k}$. In the next section, we will explore a vector space analog of the Frankl-Wilson theorem which is proved in a very similar manner.

7 Intersection Theorems for Vector Spaces [15]

The main point of this talk is to prove some vector space analogs or q-analog version of some previous results from this seminar which were proved in Section 2 and Section 6. This is based off of the work of Frankl and Graham [15]. Recall the q-analogs of n and $n!$:

$$[n]_q := (1 + q + \cdots + q^{n-1}) \text{ and}$$

$$[n]_q! = [n]_q \cdot [n-1]_q \cdots [1]_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Observe that plugging in $q = 1$ obtains the classical definition of the object. Let $\binom{\mathbb{F}_q^n}{k}$ denote the set of k-dimensional vector subspaces of $\mathbb{F}_q^n$.

Lemma 7.1.

$$\left|\binom{\mathbb{F}_q^n}{k}\right| = \binom{n}{k}_q := \frac{[n]_q!}{[n-k]_q![k]_q!}.$$

Proof. We will count the number of order k-tuples which are linearly independent in two different ways. First, by iteratively selecting vectors which are not in the span of the previously selected vectors we obtain

$$(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1}).$$

Equivalently, one selects a k-dimensional vector space $A \in \binom{\mathbb{F}_q^n}{k}$ and then selects an ordered k-tuple of linearly independent vectors from A to get

$$\left|\binom{\mathbb{F}_q^n}{k}\right|(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1}).$$

Dividing through and simplifying then yields the desired result. $\square$

Recall the Frankl-Wilson theorem from Section 6.

Theorem 7.2 (Frankl-Wilson [17]). *Let p be prime and let $L \subset [0, p-1]$ and $k \notin L(\mod p)$ with $|L| = s$. Suppose $\mathcal{F} \subset \binom{[n]}{k}$ is so that for all $F_1 \neq F_2 \in \mathcal{F}$, $|F_1 \cap F_2| \in L$. Then $|\mathcal{F}| \leq \binom{n}{s}$.*

The main result we will prove in this section is the q-analog of the Frankl-Wilson theorem.

Theorem 7.3 (Frankl-Graham [15]). *Let $b \in \mathbb{Z}^+$ let $L \subset [0, b-1]$ and $k \notin L(\mod b)$ with $|L| = s$. Suppose $\mathcal{F} \subset \binom{\mathbb{F}_q^n}{k}$ is so that for all $F_1 \neq F_2 \in \mathcal{F}$, $\dim(F_1 \cap F_2) \in L$. Then $|\mathcal{F}| \leq \binom{n}{s}_q$ except possibly for $q = 2$, $b = 6$, and $s \in \{3, 4\}$.*

In order to prove Theorem 7.3, we will need the following result from elementary number theory.

Theorem 7.4 (Bang). *Let $q, b \in \mathbb{Z}$ be so that $q \geq 2$, $b \geq 3$ and $(q, b) = (2, 6)$, then there exists a prime p so that for all $1 \leq l < b$, we have that $p|(q^b - 1)$, but $p \nmid (q^l - 1)$.*

We are now ready to prove Theorem 7.3.

Proof. Let $\mathcal{F} = \{F_1, \ldots, F_m\} \subset \binom{\mathbb{F}_q^n}{k}$ be as in the theorem statement and $L = \{l_1, \ldots, l_s\}$. Observe that $\binom{x}{i}_q$ is a polynomial of degree i in q^x for all $0 \le i \le s$ and hence we may find $\alpha_i \in \mathbb{Q}$ so that

$$\prod_{i\in[s]} (q^{x-l_i} - 1) = p(x) = \sum_{i=0}^{s} \alpha_i \binom{x}{i}_q.$$

Next, let

$$N_i := \mathcal{M}(\binom{\mathbb{F}_q^n}{i}, \mathcal{F})^T \mathcal{M}(\binom{\mathbb{F}_q^n}{i}, \mathcal{F}) = \left(\binom{\dim(F_r \cap F_t)}{i}_q\right)_{1\le r,t\le m}$$

where $\mathcal{M}(\binom{\mathbb{F}_q^n}{i}, \mathcal{F})$ is the q-analog inclusion matrix (cf. Section 6).
Define $N := \sum_{i=0}^{s} \alpha_i N_i$ and observe that

$$(N)_{r,t} = \prod_{i\in[s]} (q^{\dim(F_r\cap F_t)-l_i} - 1).$$

As long as $(q, b) \neq (2, 6)$, we may use Theorem 7.4 to get that there exists a prime p so that $p|(q^b - 1)$, but $p \nmid (q^l - 1)$ for all $1 \le l < b$. Hence

$$p|(N)_{r,t} \iff r \neq t$$

and thus $\det(N) \neq 0 (\mathrm{mod}\ p)$. As in the Section 6, we note that

$$\mathrm{rowspace}(N) \subset \mathrm{rowspace}(N_i)$$

and thus we get the desired result as

$$m = \mathrm{rank}(N) \le \mathrm{rank}(N_s) = \binom{n}{s}_q.$$

Some case work can be done when $(q, b) = (2, 6)$ and $s \notin \{3, 4\}$. □

7.1 Constructive Ramsey lower bound

Theorem 7.3 also yields a constructive lower bound the the Ramsey number $r(t, t)$ which grows faster than any polynomial. Let $k = b^2 - 1$ and let $V = \binom{\mathbb{F}_q^n}{k}$ where $(F_1, F_2) \in E(G)$ if and only if we have that $\dim(F_1 \cap F_2) = -1(\mod b)$ and note that a clique in G corresponds to such a family from Theorem 7.3 with $L = \{b - 1, 2b - 1, \ldots, b^2 - b - 1\}$ and hence Theorem 7.3 yields

$$\omega(G) \le \binom{n}{b-1}_q.$$

Moreover an independent set in G corresponds to such a family from Theorem 7.3 with $L = [0, b-2]$ and hence Theorem 7.3 yields

$$\alpha(G) \le \binom{n}{b-1}_q.$$

8 Slice rank and capset problem [10, 12, 25]

A lot of effort has been made to determine the largest size of an arithmetic-free subset of $[n]$. The following result is an important step towards this problem, which was cited as one of the two reasons for Klaus Roth's Fields Medal.

Theorem 8.1 (Roth [29]). *There exists a constant c such that for every positive integer n, if $A \subset [n]$ and $|A| > cn/\log\log n$, then A must contain a 3-term arithmetic progression.*

A finite field variant of this problem is the *capset problem.* A subset $A \subset \mathbb{F}_3^n$ is called a *capset* if it contains no 3-term arithmetic progression. The capset problem ask for the largest size of a capset on $\mathbb{F}_3^n$. We denote this number as $r_3(n)$.

For the lower bound, an easy construction is $\{0,1\}^n$, which gives $r_3(n) \geq 2^n$. The best lower bound so far is $r_3(n) = \Omega(2.217^n)$, given by Edel [14] in 2004.

With respect to upper bound, Brown and Buhler [7] first showed in 1982 that $r_3(n) = o(3^n)$, which is improved to $O(3^n/n)$ by Meshulam [24]. Later, Bateman and Katz [8] proved that $r_3(n) = O(3^n/n^{1+\epsilon})$. The best known upper bound is the following theorem, which dramatically improved the previous bounds with a surprisingly short proof:

Theorem 8.2 (Ellenberg and Gijswijt [12]). *$r_3(n) = O(2.76^n)$.*

Before presenting the proof of this upper bound, let's first do a warm-up problem.

8.1 The two distances problem

A point set P is a *two-distance set* if there exists two real numbers r, s such that the distance between any two points in P is either r or s. The two distances problem ask for the maximum two-distance set in $\mathbb{R}^d$.

For the lower bound, an easy construction is the set of points with 2 coordinates being 1 and d-2 coordinates being 0. One can check that the distance between two points in this set is either $\sqrt{2}$ or 2. This gives a lower bound $\binom{d}{2}$.

For the upper bound, we have the following:

Theorem 8.3. *Every two-distance set in $\mathbb{R}^d$ has size as most $\binom{d}{2} + 3d + 2$.*

Proof. Let $\mathbf{P} = \{P_1, P_2, \ldots, P_m\}$ be a two-distance set in $\mathbb{R}^d$, where the two distances are r and s. Let $f : \mathbf{P} \times \mathbf{P} \to \mathbb{R}$ be a function defined as follow:

$$f(x,y) = (\sum_{i=1}^{d} (x_i - y_i)^2 - r^2)(\sum_{i=1}^{d} (x_i - y_i)^2 - s^2).$$

We can view f as a matrix by considering a matrix A such that $A_{x,y} = f(x,y)$. By definition we know that A is diagonal with positive diagonal entries, hence we have $\text{rank}(A) = |\mathbf{P}|$.

If we consider y as a constant, then it's not hard to check that $f(x, y)$ is a linear combinations of the following $\binom{d}{2} + 3d + 2$ polynomials:

$$(\sum_{j=1}^{d} x_j^2)^2,\ x_k(\sum_{j=1}^{d} x_j^2),\ x_k x_l,\ x_k,\ 1.$$

Denote these polynomials by $g_1(x), g_2(x), \ldots, g_{\binom{d}{2}+3d+2}(x)$. Then there exist h_i with

$$f(x, y) = \sum_{i=1}^{\binom{d}{2}+3d+2} g_i(x) h_i(y).$$

Each term in the right hand side of the equation corresponds to a matrix of at most rank 1. So

$$|\mathbf{P}| = \text{rank}(A) \leq \binom{d}{2} + 3d + 2.$$

□

The idea of this proof can be extended to the capset problem. Notice that in the two distances problem, the relations we have are between two elements. These relations can be captured by a two-variate function, which can be considered as a matrix. However, in the capset problem, the relations are between three elements. To captured these relations, naturally we would need a three-variate function, which can only be considered as a tensor and hence we need the corresponding notion of rank for tensors.

8.2 Slice Rank

Definition 8.4. Let A be a finite set, $\mathbb{F}$ be a field, $f : A \times A \times A \to \mathbb{F}$ be a function. Then we say f has slice rank 1 if there exist functions $g : A \to \mathbb{F}$ and $h : A \times A \to \mathbb{F}$ such that

$$f(x, y, z) = g(x)h(y, z) \ or \ g(y)h(x, z) \ or \ g(z)h(x, y).$$

Generally speaking, the *slice rank* of f is the smallest integer k such that f can be written as the sum of k function of slice rank 1. We denote the slice rank of f as $sr(f)$.

The heart of the proof of Theorem 8.2 is the following lemma on the property of slice rank.

Lemma 8.5. *Let A be a finite set, $f : A \times A \times A \to \mathbb{F}$ be a function that satisfy $f(x, y, z) \neq 0$ if and only if $x = y = z$. Then $sr(f) = |A|$.*

Proof. For $a \in A$, let $\delta_a : A \to \mathbb{F}$ be defined as

$$\delta_a = \begin{cases} 1, & x = a, \\ 0, & x \neq a. \end{cases}$$

Then we have $f(x,y,z) = \sum_{i=1}^{a} f(a,a,a)\delta_a(x,y,z)$. This implies that $sr(f) \leq |A|$. On the other hand, by definition there exists functions $f_j : A \to \mathbb{F}$ and $g_j : A \times A \to \mathbb{F}$, $1 \leq j \leq sr(f)$, such that

$$f(x,y,z) = \sum_{j=1}^{s} f_j(x)g_j(y,z) + \sum_{j=s+1}^{t} f_j(y)g_j(x,z) + \sum_{j=t+1}^{sr(f)} f_j(z)g_j(x,y). \tag{3}$$

Let P be the set of functions $h : A \to \mathbb{F}$ that satisfy $\sum_{a\in A} h(a)f_j(a) = 0$ for all $1 \leq j \leq s$. For a polynomial $h \in P$, denote the support of h as $S_h = \{a \in A : h(a) \neq 0\}$. Fix $h \in P$ with maximal support. If $|S_h| < |A| - s$, then there exists nonzero function $h' \in P$ such that h' vanishes on S_h. Then $h + h' \in P$ has larger support than h, contradicting the choice of h. So we conclude that $|S_h| \geq |A| - s$. Recalling equation (3), we have

$$\sum_{a\in A} h(a)f(a,y,z) = \sum_{j=s+1}^{t} f_j(y) \sum_{a\in A} h(a)g_j(a,z) + \sum_{j=t+1}^{sr(f)} f_j(z) \sum_{a\in A} h(a)g_j(a,y).$$

Similar to the Two Distances Problem proof, the left hand side of this equation can be considered as a diagonal matrix with $|S_h|$ nonzero diagonal entries, hence has rank $|S_h|$. Right hand side can be considered as a sum of $sr(f)-s$ matrix of rank at most 1. This implies that $sr(f)-s \geq |S_h| \geq |A|-s$. So we have $sr(f) \geq |A|$, which completes the proof. □

Now the proof of Theorem 8.2 is mostly an application of Lemma 8.5

Proof of Theorem 8.2. Let $f : A \times A \times A \to \mathbb{F}$ be defined as

$$f(x,y,z) = \prod_{j=1}^{n} (1 - (x_i + y_i + z_i)^2).$$

Since A is a capset, $f(x,y,z) \neq 0$ if and only if $x = y = z$. So by Lemma 8.5, we have $sr(f) = |A|$. For $x = (x_1, x_2, \ldots, x_n)$, $p = (p_1, p_2, \ldots, p_n)$, write $x^p = x_1^{p_1} x_2^{p_2} \ldots x_n^{p_n}$, $|p| = \sum_{i=1}^{n} p_i$. Then by the pigeonhole principle, we have

$$f(x,y,z) = \sum_{\substack{p\in\mathbb{F}_3^n \\ |p|\leq 2n/3}} x^p g_{x,p}(y,z) + \sum_{\substack{p\in\mathbb{F}_3^n \\ |p|\leq 2n/3}} y^p g_{y,p}(x,z) + \sum_{\substack{p\in\mathbb{F}_3^n \\ |p|\leq 2n/3}} z^p g_{z,p}(x,y).$$

for some functions $g_{x,p}, g_{y,p}, g_{z,p}$. Let $r = |\{p \in \mathbb{F}_3^n : |p| \leq 2n/3\}|$. Then by definition of slice rank, we have $|A| \leq 3r$. What remain to be done is to derive an upper bound for r. For $p \in \mathbb{F}_3^n$, let m_j be the number of coordinates with j in p. With this notation, we get

$$r = \sum_{\substack{m_0+m_1+m_2=n \\ m_1+2m_2\leq 2n/3}} \frac{n!}{m_0!m_1!m_2!}.$$

By the multinomial theorem, we have

$$(1 + x + x^2)^n = \sum_{m_0+m_1+m_2=n} \frac{n!}{m_0!m_1!m_2!} x^{m_1+2m_2}.$$

Assuming that $0 < x < 1$, the above leads to

$$x^{-2n/3}(1+x+x^2)^n = \sum_{m_0+m_1+m_2=n} \frac{n!}{m_0!m_1!m_2!} x^{m_1+2m_2-2n/3} \geq \sum_{\substack{m_0+m_1+m_2=n \\ m_1+2m_2 \leq 2n/3}} \frac{n!}{m_0!m_1!m_2!} = r.$$

By basic calculus we know that $x^{-2/3}(1+x+x^2)$ obtain minimum at $(\sqrt{33}-1)/8$. This minimum is less than 2.76. So we have $|A| = O(2.76^n)$. □

9 Interlacing and Sensitivity conjecture [22]

Our topic today is boolean functions, which we define as follows:

Definition 9.1. A *boolean function* is a map $f : \{\pm 1\}^n \to \{\pm 1\}$.

We will interpret -1 as True and 1 as false. The rather unusual interpretation of true and false will make our definitions much simpler. In particular, one can note that $\{\pm 1\}^n$ is an abelian group isomorphic to $\mathbb{Z}_2^n$. Then boolean functions are class functions on this group. One might naturally ask for the irreducible characters, i.e. the basis for class functions on $\{\pm 1\}^n$.

Definition 9.2. The Fourier characters $\chi_S(\vec{x}) : \{\pm 1\}^n \to \{\pm 1\}$ are

$$\chi_S(\vec{x}) = \prod_{i \in S} x_i$$

where $\chi_\emptyset(\vec{x}) = 1$.

Basic representation theory gives us the following:

Theorem 9.3. *Under the following inner product* $\langle f, g \rangle = \frac{1}{2^n} \sum_{\vec{x} \in \{\pm 1\}^n} f(\vec{x}) g(\vec{x})$, *the* $\{\chi_S\}_{S \subseteq [n]}$ *is an orthonormal basis for the set of boolean functions.*

Corollary 9.4. *Every boolean function f can be written as*

$$f(\vec{x}) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S(\vec{x})$$

The coefficients $\hat{f}(S)$ *are called the Fourier coefficients.*

Finally, for $S \subseteq [n]$ let $\vec{x}^S$ denote the vector with the coordinates in S flipped.

9.1 Complexity Measures

Now that we have some definitions, what else can we do with a boolean function? From a more computer science perspective, we want to say that one boolean function is harder to compute than another. To that end, we have several complexity measures.

1. A *decision tree* is a binary tree with each node labeled by a coordinate x_i, and each out-edge labeled by either 1 or -1. The leaves of the tree are labeled by 1 or -1. A decision tree T computes a boolean function f if for each input $\vec{x}$, the leaf associated to $\vec{x}$ by the tree gives the value $f(\vec{x})$. The smallest decision tree (in terms of number of nodes) computing a boolean function f is $D(f)$.

2. A partial assignment of inputs $c \in \{1, -1, *\}^n$ is called a *certificate* if $f(c')$ is constant for every $c' \in \{1, -1\}^n$ which is consistent with c. The minimum size of a certificate is $C(f)$

3. The *degree* of a boolean function f is $\deg(f) := \max\{|S|\,|\hat{f}(S) \neq 0\}$.

4. The *local sensitivity* of a boolean function $s(f, \vec{x}) := \left|\{i|f(\vec{x}) \neq f(\vec{x}^i)\right|$. The **sensitivity** of a boolean function is then $s(f) := \max_{\vec{x} \in \{\pm 1\}^n} s(f, \vec{x})$.

5. The *local block sensitivity* of a boolean function f is $bs(f, \vec{x})$ is the maximum number of disjoint sets $B_1, \ldots, B_t \subseteq [n]$ such that $f(\vec{x}) \neq f(\vec{x}^{B_i})$ for all B_i. The *block sensitivity* of f is $bs(f) := \max_{\vec{x} \in \{\pm 1\}^n} bs(f, \vec{x})$.

Given all these complexity measures, another natural question to ask is whether these measures are in fact different. In fact they are all equivalent in the following way. We say that two complexity measures A, B are polynomially equivalent if there are polynomials $p_1(n), p_2(n)$ such that

$$B(f) \leq p_1(A(f)), \qquad A(f) \leq p_2(B(f))$$

Then, $D(f)$, $C(f)$, $\deg(f)$, and $bs(f)$ are all polynomially equivalent ([26]). But what about $s(f)$? it is clear from the definitions that $s(f) \leq bs(f)$. Naturally, Nisan and Szegedy conjectured the following:

Conjecture 9.5. *Sensitivity Conjecture* [26] *There exists an absolute constant C such that*

$$bs(f) \leq s(f)^C$$

After much work on the conjecture (see [21] for a good survey) the problem remained wide open until the short and simple work of Hao Huang [22], whose proof is explained in the sections below. The one lemma we shall need from the above reductions is that

Lemma 9.6. [31]

$$bs(f) \leq \deg(f)^2$$

9.2 Gotsman and Linial's Reduction

In light of Lemma 9.6, it would make sense to reduce the sensitivity conjecture to relating $s(f)$ and $\deg(f)$. But first, we shall go in a wildly different direction: hypercube graphs.

Definition 9.7. The hypercube graph Q_n has vertex set $\{\pm 1\}^n$, and $\vec{x} \sim \vec{y}$ iff $\vec{x}$ and $\vec{y}$ differ in exactly 1 coordinate. Alternately, Q_n is the cayley graph of $\mathbb{Z}_2^n$ with the generating set of vectors with a single nonzero coordinate.

Why do we care about hypercube graphs when we have been talking about boolean function? The connection is simple; we can identify an induced subgraph $H \leq Q_n$ by $\{\vec{x} \in \{\pm 1\}^n | f(\vec{x}) = -1\}$. This is clearly a bijection between boolean functions and induced subgraphs of the hypercube. Furthermore, Gotsman and Linial showed that the sensitivity conjecture has an equivalent formulation in terms of subgraphs of the hypercube.

Theorem 9.8 (Gotsman-Linial [18]). *The following are equivalent:*

1. *For any induced subgraph H of Q_n with $|H| \neq 2^{n-1}$* $\max\{\Delta(H), \Delta(Q_n - H)\} \geq \sqrt{n}$
2. *For any boolean function h,* $\deg(h) < s(f)^2$

Proof. We first transform statement (1). Let h be the boolean function defined by $h(\vec{x}) = -1 \iff \vec{x} \in H$. Then, $\deg_H(\vec{x}) = n - s(h, \vec{x})$, as the sensitivity counts the number of directions in which the function changes. The same holds for the induced subgraph $Q_n - H$. Furthermore, the statement that $|H| \neq 2^{n-1}$ is equivalence to $\hat{h}(\emptyset) \neq 0$. Thus, (1) is equivalent to

1' For any boolean function h with $\hat{h}(\emptyset) \neq 0$, there is an input $\vec{x}$ such that $s(f, \vec{x}) \leq n - \sqrt{n}$

We also transform statement (2). By substituting n for $s(f)^2$, we have that (2) is equivalent to

2' For any boolean function h, $s(h) < \sqrt{n}$ implies $\deg(h) < n$.

Now we will show that $1' \iff 2'$. First, given a boolean function f, the boolean function g by

$$g(\vec{x}) = f(\vec{x})\chi_{[n]}(\vec{x}).$$

We note that

$$g = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S\chi_{[n]} = \sum_{S \subseteq [n]} \hat{f}([n] - S)\chi_S$$

so $\hat{g}(S) = \hat{f}([n] - S)$. Second, $s(g, \vec{x}) = n - s(f, \vec{x})$, as the parity function $\chi_{[n]}$ changes value when any one bit changes. Thus, every direction which contributes to the local sensitivity of f no longer contributes to the local sensitivity of g and vice-versa.
We shall first show $1' \implies 2'$. Assume for contradiction that $s(f) \leq \sqrt{n}$ and yet $\deg(f) = n$. Thus, $\hat{f}([n]) \neq 0$ by definition of degree and hence $\hat{g}(\emptyset) \neq 0$. By (1'), $\exists \vec{x} : s(g, \vec{x}) \leq n - \sqrt{n}$, so it follows that $\exists \vec{x} : s(f, \vec{x}) \geq \sqrt{n}$. This contradicts the premise of (2').

Now, we will show that $2' \implies 1'$. Again assume for contradiction that $\hat{g}(\emptyset) \neq 0$ and yet $\forall \vec{x} : s(g, \vec{x}) > n - \sqrt{n}$. Hence, $s(f, \vec{x}) < \sqrt{n}$ for every $\vec{x}$ and thus $s(f) < \sqrt{n}$. By 2', $\deg(f) < n$, and so $0 = \hat{f}([n]) = \hat{g}(\emptyset)$, which contradicts the premise of 1'.

□

Remark. In Gotsman and Linial's original paper, the function $\sqrt{n}$ was an arbitrary monotonic function $h(n)$. We never use any properties of $\sqrt{n}$ in the above proof, but specified the function to improve readability.

Furthermore, the following was known regarding in induced subgraphs of the hypercube.

Theorem 9.9. [9] *If n is a perfect square, there is a subgraph $H \leq Q_n$ with precisely $2^{n-1}+1$ vertices such that*

$$\Delta(H) \leq \sqrt{n}.$$

By comparison to the Gotsman and Linial theorem, the actual proof of the sensitivity conjecture is quite simple. The key idea is the following:

Definition 9.10. Let the matrix B_n be defined by

$$B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad B_{n+1} = \begin{bmatrix} B_n & I_{2^n} \\ I_{2^n} & -B_n \end{bmatrix}.$$

By comparison the adjacency matrix of Q_n can be defined as

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad A_{n+1} = \begin{bmatrix} A_n & I_{2^n} \\ I_{2^n} & A_n \end{bmatrix}.$$

Furthermore, we have the following general result analogous to the relationship $\Delta(H) \geq \lambda_1(A(H))$.

Lemma 9.11. *Let G be a graph on n vertices and B an $n \times n$ matrix such that*

- $B_{ij} \in \{1, 0, -1\} \forall i, j$
- $B_{ij} \neq 0 \iff i \sim j$
- *B is symmetric.*

Then,

$$\Delta(H) \geq \lambda_1(B).$$

Proof. As B is symmetric, let v be an eigenvector corresponding to λ_1 and assume, without loss of generality, that v_1 is the largest coordinate by absolute value. Then,

$$\left|(\lambda_1 v)_1\right| = \left|(Av)_1\right| \leq \sum_{i \sim 1} |A_{1i}||v_i| \leq \sum_{i \sim 1} |v_1| \leq \Delta(H)|v_1|.$$

□

To lower bound the maximum degree, all we must do is compute the eigenvalues of B_n.

Lemma 9.12. *The spectrum of B_n is $\{\sqrt{n}, -\sqrt{n}\}$, each with multiplicity 2^{n-1}.*

Proof. We first show by that $B_n^2 = I$. Clearly, $B_1^2 = I$. Then, by induction

$$B_{n+1}^2 = \begin{bmatrix} B_n & I \\ I & -B_n \end{bmatrix}^2 = \begin{bmatrix} B_n^2 + I & 0 \\ 0 & B_n^2 + I \end{bmatrix} = \begin{bmatrix} (n+1)I & 0 \\ 0 & (n+1)I \end{bmatrix} = (n+1)I$$

and thus it follows that the eigenvalues of B_n are $\sqrt{n}, -\sqrt{n}$. As $\mathrm{Trace}(B_n) = 0$ by construction, each eigenvalue occurs with equal multiplicity. □

We now have all the pieces we need:

Theorem 9.13. [22] *Let H be an arbitrary subgraph of Q_n with exactly $2^{n-1}+1$ vertices. Then,*

$$\Delta(H) \geq \sqrt{n}.$$

Proof. Let H be a subgraph of Q_n with exactly $2^[n-1]+1$ vertices, and let B' be the corresponding principal minor of B_n. By the Cauchy Interlacing Theorem and (9.12),

$$\lambda_1(B') \geq \lambda_{2^{n-1}+1-1}(B_n) = \lambda_{2^{n-1}}(B_n) = \sqrt{n}$$

By (9.11), it follows that $\Delta(H) \geq \lambda_1(B') \geq \sqrt{n}$. □

Corollary 9.14.

$$bs(f) \leq s(f)^4.$$

Proof. By (9.13) and (9.8), $\deg(f) \leq s(f)^2$. The corollary follows by (9.6). □

Corollary 9.15. *Let $\Lambda = \min\{\Delta(H) : H \leq Q_n; |H| = 2^{n-1}+1\}$. Then, $\Lambda = \sqrt{n}$.*

References

[1] N. Alon, Decomposition of the complete r-graph into complete r-partite r-graphs, Graphs and Combin., 2, 95–100, 1986.

[2] N. Alon, Neighborly Families of Boxes and Bipartite Coverings, In: Graham R.L., Nešetřil J. (eds) The Mathematics of Paul Erdös II. Algorithms and Combinatorics, 14, 1997.

[3] N.Alon, L.Babai, H. Suzuki, Multilinear polynomials and Frankl-Ray-Chaudhuri types intersection theorems, J. Combin. Theory Ser. A, 1991.

[4] L. Babai, P. Frankl, Linear algebra methods in Combinatorics, Dept. of Computer Science, The University of Chicago, 1992.

[5] E.R. Berlekemp, On subsets with intersections of Even Cardiniality, Canad. Math. Bull., 12, 471-474, 1969.

[6] B. Bollobás, On generalized graph, Acta Math. Acad. Sci. Hungar. 16, 447-452, 1965.

[7] T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey theorem, J. Combin. Theory Ser. A, 32, 20-34, 1982.

[8] M. Bateman and N. Katz, New bounds on cap sets, Journal of the American Mathematical Society 25, 585–613, 2012.

[9] F.R.K Chung, Zoltan Fúredi, R.L Graham, and P. Seymour, On induced subgraphs of the cube, J. Combin. Theory Ser. A, 49(1), 180-187, 1988.

[10] E. Crook, V. Lev, P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. Annals of Mathematics. 185, 2017.

[11] M. Deza, P. Frankl, N.M. Singhi, On functions of strength t Combinatorica, 3, 331-339, 1981.

[12] J. Ellenberg, D. Gijswijt, On large subsets of $\mathbb{F}_n^q$ with no three-term arithmetic progression, Annals of Mathematics, Vol. 185, 2017.

[13] P. Erdős, Three point collinearity, Amer. Math. Monthly, 50 (1943), p. 65; Solution in 51, 169-171, 1944.

[14] Y. Edel, Extensions of generalized product caps, Designs, Codes and Cryptography, 31, 5–14, 2004.

[15] P.Frankl, R. Graham, Intersection Theorems for Vector Spaces, European Journal of Combinatorics, 1985.

[16] P. Frankl, N. Tokushige, Extremal problems for finite sets, AMS Student mathematical library, Vol 86, 2018.

[17] P. Frankl, R. Wilson, Intersection theorems with geometric consequences, Combinatorica, 1981.

[18] C. Gotsman, N. Linial, The equivalence of two problems on the cube, J. Combin. Theory Ser. A, 61(1), 142-146, 1992.

[19] R. Graham, H. Pollak, On embedding graphs in squashed cubes, In:Graph Theory and Appl., Springer Lecture Notes in Math. 303, pp. 99-110, 1972.

[20] J. Graver, Boolean designs and self-dual matroids, Linear Algebra and Appl., 10, 111-128, 1975.

[21] Pooya Hatami, Raghav Kulkarni, and Denis Pankratov, Variations on the Sensitivity Conjecture, Number 4 in Graduate Surveys. Theory of Computing Library, 2011.

[22] H. Huang, Induced subgraphs of hypercubes and a proof of the Sensitivity Conjecture, to appear in Annals of Mathematics, 2019.

[23] L. Lovasz, Flats in matroids and geometric graphs, in Combinatorial Surveys (P. J. Cameron, ed.), Academic Press, New York, 45-86, 1977.

[24] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, J. Combin. Theory Ser. A, 71, 168–172, 1995.

[25] E. Naslund, W. Sawin, Upper bounds for Sunflower-Free Sets, Forum Mathematics Sigma, Vol. 5 (15), 2017.

[26] Noam Nisan and Mario Szegedy, On the degree of boolean functions as real polynomials, computational complexity, 4(4), 301–313, 1994.

[27] G. Peck, A new proof of a theorem of Graham and Pollak, Discrete Math., 49:327–328, 1984.

[28] D.K. Ray-Chaudhuri and R.M. Wilson, On t-designs, Osaka J. Math., 12, 737-744. 1975.

[29] K. Roth, On certain sets of integers, J. London Math Soc., 28, 104-109, 1953.

[30] H. Snevily, A sharp bound for the number of sets that pairwise intersect at k positive values, Combinatorica, 2003.

[31] Avishay Tal, Properties and applications of boolean function composition, In Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS '13, 441–454, New York, NY, USA, ACM, 2013.

[32] H. Tverberg, On the decomposition of K_n into complete bipartite graphs, J. Graph Theory, 6, 493–494, 1982.

[33] S. Vishwanathan, A polynomial space proof of the Graham-Pollak theorem, J. Combin. Theory Ser. A, 115, 674–676, 2008.

[34] S. Vishwanathan, A counting proof of the Graham-Pollak theorem. Discrete Math., 313(6):765–766, 2013.