Combinatorics
Part C

Alex Scott

Michaelmas 2016

Last modified by Jason Long on March 30, 2020.

Contents

Chapter 1

Introduction and notation

1.1 Notes

These notes are intended to complement (but not replace) the Part C lecture course in Combinatorics. In particular, they do not give all the details that are explained in lectures.

The notes owe much to the book *Combinatorics* by Béla Bollobás, and to notes from two courses given elsewhere by Imre Leader. Thanks are due to Damiano Soardo and Albert Slawinksi, who contributed to earlier versions of the notes.

Please send any further corrections/suggestions to scott at maths.ox.ac.uk.

1.2 Notation and basic definitions

For a set X, we write $\mathcal{P}(X) = \{A : A \subseteq X\}$ for its power set (i.e. the set of all its subsets). A *family of sets* $\mathcal{F}$ *on a ground set* X is a subset $\mathcal{F} \subseteq \mathcal{P}(X)$. A family of sets is also called a *set system* or a *hypergraph*. For instance, with ground set $X = \{1, 2, 3, 4\}$, we could have the hypergraph $\mathcal{F} = \{1, 13, 124, 34\}$: note that we have dropped some brackets and commas for convenience (strictly speaking we should write $\mathcal{F} = \{\{1\}, \{1, 3\}, \{1, 2, 4\}, \{3, 4\}\}$, but this is more cumbersome).

Most of this course concerns properties of set systems with a finite ground set. So from now on *all sets will be assumed to be finite unless stated otherwise.*

For $n \geq 1$, we write $[n] := \{1, 2, \ldots, n\}$. We will usually write $\mathcal{P}(n)$ instead of $\mathcal{P}([n])$. Note that $|\mathcal{P}(n)| = 2^n$.

We will refer to sets of size k as *k-sets*. For $k \geq 0$ we write $X^{(k)} = \{A \in \mathcal{P}(X) : |A| = k\}$ for the set of all subsets of X of size k. We define $X^{(<k)}, X^{(\leq k)}, X^{(>k)}$ and $X^{(\geq k)}$ in the obvious way. A family $\mathcal{F} \subseteq \mathcal{P}(X)$ is *k-uniform* if $\mathcal{F} \subseteq X^{(k)}$.

We think of $X^{(0)}, X^{(1)}, \ldots$ as the *layers* of $\mathcal{P}(X)$, and refer to $X^{(i)}$ as the *ith layer*. So the ith layer of $\mathcal{P}(n)$ is $[n]^{(i)}$, which has cardinality $\binom{n}{i}$. The smallest layers of $\mathcal{P}(n)$ are the 0th layer and the nth layer: these are $\{\emptyset\}$ and $\{[n]\}$ respectively, and both have size 1. If n is even, the largest layer is $[n]^{(n/2)}$; if n is odd there are two largest layers, $[n]^{(\lfloor n/2 \rfloor)}$ and $[n]^{(\lceil n/2 \rceil)}$.

There are many ways of looking at the power set $\mathcal{P}(n)$. For instance:

- We can think of $\mathcal{P}(n)$ as a collection of sets with a partial order given by set containment: $A \subseteq B$. We will talk more about this later.
- We can turn $\mathcal{P}(n)$ into a graph: the *discrete cube* Q_n is the graph with vertex set $\mathcal{P}(n)$ and an edge between A and B if and only if $|A \triangle B| = 1$. Here $A \triangle B$ is the *symmetric difference*: $A \triangle B := (A \setminus B) \cup (B \setminus A)$.
- We can turn $\mathcal{P}(n)$ into an abelian group or a vector space $\mathbb{F}_2^n$ by identifying each $A \subseteq [n]$ with its *characteristic vector*

$$\chi_A = (\chi_A(1), \ldots, \chi_A(n)) \in \{0,1\}^n,$$

where

$$\chi_A(i) := \begin{cases} 1 & i \in A \\ 0 & i \notin A \end{cases}$$

We will move back and forward between these perspectives throughout the course.

Chapter 2

Chains, antichains and shadows

2.1 Sperner's Lemma, LYM Inequality and Dilworth's Theorem

A family $\mathcal{A} \subseteq \mathcal{P}(X)$ is a *chain* if, for all $A, B \in \mathcal{A}$, either $A \subseteq B$ or $B \subseteq A$. A family $\mathcal{A} \subseteq \mathcal{P}(X)$ is an *antichain* if, for all distinct $A, B \in \mathcal{A}$, we have $A \not\subseteq B$ and $B \not\subseteq A$.

For instance, $\{\emptyset, 1, 1234\}$ is a chain in $\mathcal{P}(4)$, and $\{12, 234, 14\}$ is an antichain. For any set X, the layers $X^{(0)}, X^{(1)}, \ldots$ are antichains.

How large can a chain in $\mathcal{P}(n)$ be? This has a simple answer.

Proposition 1. *Every chain in $\mathcal{P}(n)$ has at most $n+1$ elements. There are $n!$ different maximal chains with $n+1$ elements, and every chain C is contained in some chain of size $n+1$.*

Proof. Exercise. ■

How large can an antichain be? This is more interesting. We noted above that the layers of $\mathcal{P}(n)$ are antichains: the largest of these has size $\binom{n}{\lfloor n/2 \rfloor}$.

Theorem 2. (Sperner's Lemma) *An antichain in $\mathcal{P}(n)$ has size at most $\binom{n}{\lfloor n/2 \rfloor}$.*

We shall see two proofs of Sperner's Lemma.

For the first proof, we will need a result from Graph Theory. Let us recall that a graph $G = (V, E)$ is bipartite with vertex classes X, Y if $X \cup Y$ is a partition of V such that every edge of G contains one vertex from each of X

and Y. The *neighbourhood* $\Gamma(v)$ of a vertex $v \in V$ is $\Gamma(v) = \{u : vu \in E(G)\}$, and for $S \subseteq V$ we write $\Gamma(S) = \cup_{v \in X} \Gamma(v)$. A *complete matching from X to Y* is a collection of vertex-disjoint edges such that every vertex in X is incident to some edge in M. Here is the result that we will need.

Theorem 3. (Hall's Theorem) *Let $G = (V, E)$ be a bipartite graph with vertex classes X and Y. Then G has a complete matching from X to Y if and only if, for all $S \subseteq X$, we have*

$$|\Gamma(S)| \geq |S|. \tag{2.1}$$

We will refer to equation (2.1) as *Hall's Condition*. Note that G has a complete matching then (2.1) is clearly necessary. The point of Hall's Theorem is that it is also *sufficient*.

Sperner's Lemma will follow quickly from the following result.

Lemma 4. *There is a partition of $\mathcal{P}(n)$ into $\binom{n}{\lfloor n/2 \rfloor}$ chains.*

Proof. Consider the subgraph of the discrete cube Q_n between the vertices in two consecutive layers. We claim that:

1. for $r < n/2$, there is a complete matching from $[n]^{(r)}$ to $[n]^{(r+1)}$;
2. for $r > n/2$, there is a complete matching from $[n]^{(r)}$ to $[n]^{(r-1)}$.

If we glue these matchings together, we obtain a collection of $\binom{n}{\lfloor n/2 \rfloor}$ chains that partition $\mathcal{P}(n)$.

It is therefore enough to prove that these matchings exist. For $r < n/2$, we consider the bipartite subgraph G of Q_n induced by $[n]^{(r)} \cup [n]^{(r+1)}$. This has bipartition $([n]^{(r)}, [n]^{(r+1)})$ and an edge between $A \in [n]^{(r)}$ and $B \in [n]^{(r+1)}$ iff $A \subseteq B$. In order to prove that there is a complete matching, it is enough to verify Hall's Condition (2.1). We will do this by a double counting argument.

Consider a set $S \subseteq [n]^{(r)}$, and let $T = \Gamma(S)$. Each $A \in S$ has degree $n - r$ in G (as there are $n - r$ ways to add an element to A to get an $(r + 1)$-set). So the number of edges between S and T is

$$e(S, T) = (n - r)|S|.$$

On the other hand, each $B \in [n]^{(r+1)}$ has degree $r + 1$ (as there are $r + 1$ choices for an element to delete from B to get an r-set). So we have[1]

$$e(S, T) \leq (r + 1)|T|$$

[1]Note that we may not have equality here, as there may be edges incident with T that are not incident with S.

Putting these two bounds together, we get

$$|T| \geq \frac{n-r}{r+1}|S| \geq |S|,$$

as $r < n/2$ (and so $r \leq (n-1)/2$). So Hall's Condition is satisfied, and hence there is a complete matching from $[n]^{(r)}$ to $[n]^{(r+1)}$.

For $r > n/2$, we can argue similarly. Alternatively we can consider the effect of replacing every set by its complement. ■

Remarks:

1. Note that we cannot partition $\mathcal{P}(n)$ into fewer than $\binom{n}{\lfloor n/2 \rfloor}$ chains, because no two sets from the antichain $[n]^{(\lfloor n/2 \rfloor)}$ can belong to the same chain.

2. The chains that we get from Lemma 4 could be very 'asymmetric'. For instance, the chain that starts at $\emptyset$ could finish on a middle layer (rather than continuing all the way up to $[n]$).

3. As an exercise you should calculate: what is (roughly) the *average* length of the chains in the partition of $\mathcal{P}(n)$ given by Lemma 4?

We can now prove Sperner's Lemma.

First proof of Sperner's Lemma. This is now easy. A chain and an antichain meet in at most one element. We have partitioned $\mathcal{P}(n)$ into $\binom{n}{\lfloor n/2 \rfloor}$ chains, so no antichain can have more than $\binom{n}{\lfloor n/2 \rfloor}$ elements. ■

Sperner's Lemma tells us the maximal size of an antichain, but what can we say about uniqueness? And what happens if we start using sets of different sizes? The LYM Inequality (named after Lubell, Yamamoto and Meshalkin, who all gave independent proofs of the result) gives a much more refined picture.

Theorem 5. (LYM Inequality) *Let $\mathcal{F} \subseteq \mathcal{P}(n)$ be an antichain. Then*

$$\sum_{i=0}^{n} \frac{|\mathcal{F} \cap [n]^{(i)}|}{\binom{n}{i}} \leq 1. \tag{2.2}$$

Furthermore, we have equality in (2.2) if and only if $\mathcal{F} = [n]^{(i)}$ for some i.

We will give two proofs of the LYM Inequality. The first one will use a "local" version of the inequality.

Let $\mathcal{F} \subseteq X^{(k)}$ be a k-uniform family on X. The *(lower) shadow* $\partial\mathcal{F}$ *of* $\mathcal{F}$ is

$$\partial\mathcal{F} := \{B \in X^{(k-1)} : B \subseteq A \text{ for some } A \in \mathcal{F}\}.$$

Lemma 6. (Local LYM Inequality) *Let* $\mathcal{F} \subseteq [n]^{(r)}$. *Then*

$$\frac{|\partial\mathcal{A}|}{\binom{n}{r-1}} \geq \frac{|\mathcal{A}|}{\binom{n}{r}}.$$

We have equality if and only if $\mathcal{A} = \emptyset$ *or* $\mathcal{A} = [n]^{(r)}$.

Proof. Once more, we use double counting of edges in Q_n, here between $\mathcal{A}$ and $\partial\mathcal{A}$. Thus we are double counting elements of

$$E = \{(A, B) : A \in \mathcal{A}, B \in \partial\mathcal{A}, B \subseteq A\}.$$

Each element $A \in \mathcal{A}$ contains r sets of size $r-1$, so

$$|E| = r|\mathcal{A}|.$$

Each element $B \in \partial\mathcal{A}$ is contained in $n-r+1$ sets of size r (not all of which need be in $\mathcal{A}$). So

$$|E| \leq (n-r+1)|\partial\mathcal{A}|.$$

It follows that

$$(n-r+1)|\partial\mathcal{A}| \geq r|\mathcal{A}|, \tag{2.3}$$

and so

$$\frac{|\mathcal{A}|}{\binom{n}{r}} \leq |\partial\mathcal{A}| \cdot \frac{n-r+1}{r} \cdot \frac{1}{\binom{n}{r}} = \frac{|\partial\mathcal{A}|}{\binom{n}{r-1}},$$

as required.

If we have equality then we must have equality in (2.3), so for every $B \in \partial\mathcal{A}$ and every $i \notin B$ we have $B \cup i \in \mathcal{A}$. If $\mathcal{A} \neq \emptyset, [n]^{(r)}$ then choose r-sets $A_1 \in \mathcal{A}$ and $A_2 \notin \mathcal{A}$ with $|A_1 \triangle A_2|$ as small as possible. We can choose $a_1 \in A_1 \setminus A_2$ and $a_2 \in A_2 \setminus A_1$: then $A_1 - a_1$ is in $\partial\mathcal{A}$ and so $A_3 := (A_1 - a_1) \cup a_2$ is in $\mathcal{A}$. But this gives a contradiction, as $|A_3 \triangle A_2| < |A_1 \triangle A_2|$. ■

Remark: In the last paragraph, what we really used was the fact that E is the edge set of a connected graph. Note also that we are being a little informal with notation in expressions like $(A_1 - a_1) \cup a_2$. As with leaving out brackets in listing set elements, this is fine as long as it is not ambiguous.

We use the Local LYM Inequality to prove the LYM Inequality.

Proof of the LYM Inequality. Let $\mathcal{F} \subseteq \mathcal{P}(n)$ be an antichain and, for $i = 0, \ldots, n$, define

$$\mathcal{F}_i := \mathcal{F} \cap [n]^{(i)}.$$

The proof proceeds by 'pushing down one layer at a time'. Define $\mathcal{G} \subseteq [n]^{(i)}$ recursively by $\mathcal{G}_n = \mathcal{F}_n$ and, for $r < n$,

$$\mathcal{G}_r := \mathcal{F}_r \cup \partial \mathcal{G}_{r+1}.$$

Note that $\mathcal{F}_r$ and $\partial \mathcal{G}_{r+1}$ are disjoint, as every set in $\partial \mathcal{G}_{r+1}$ is contained in some element of $\mathcal{F}$, and $\mathcal{F}$ is an antichain.

We claim that, for $r = 0, \ldots, n$,

$$\frac{|\mathcal{G}_r|}{\binom{n}{r}} \geq \sum_{i=r}^{n} \frac{|\mathcal{F}_i|}{\binom{n}{i}}. \tag{2.4}$$

We prove this by (downwards) induction. For $r = n$ it is immediate. Now suppose it is true for $r+1$: we show it is true for r. We have

$$\begin{aligned}
\frac{|\mathcal{G}_r|}{\binom{n}{r}} &= \frac{|\mathcal{F}_r|}{\binom{n}{r}} + \frac{|\partial \mathcal{G}_{r+1}|}{\binom{n}{r}} && \text{as } \mathcal{F}, \partial \mathcal{G}_{r+1} \text{ disjoint} \\
&\geq \frac{|\mathcal{F}_r|}{\binom{n}{r}} + \frac{|\mathcal{G}_{r+1}|}{\binom{n}{r+1}} && \text{by Local LYM} \\
&\geq \frac{|\mathcal{F}_r|}{\binom{n}{r}} + \sum_{i=r}^{n} \frac{|\mathcal{F}_i|}{\binom{n}{i}} && \text{by induction}
\end{aligned}$$

as required. We conclude that (2.4) holds for every r.

Setting $r = 0$ in (2.4), we get

$$1 \geq \frac{|\mathcal{G}_0|}{\binom{n}{0}} \geq \sum_{i=0}^{n} \frac{|\mathcal{F}_i|}{\binom{n}{i}},$$

which gives (2.2) as required.

If we have equality at the end, we must have had equality at each application of Local LYM, and so we have $\mathcal{G}_r = \emptyset$ or $\mathcal{G}_r = [n]^{(r)}$ for each r. This implies that $\mathcal{F}_r = [n]^{(r)}$ for some r, and $\mathcal{F}_i = \emptyset$ for all other i. ■

We give a second proof of the LYM Inequality. It gives a very slick proof of the LYM inequality, but does not give the extremal set systems.

Second proof of the LYM Inequality. Let $\mathcal{F}$ be an antichain in $\mathcal{P}(n)$. Choose a maximal chain $C = (A_0, \ldots, A_n)$, where $\emptyset = A_0 \subseteq \ldots A_n = [n]$, uniformly at random from all $n!$ maximal chains. For $A \in \mathcal{F}$ with $|A| = k$ we have

$$\mathbb{P}[A \in C] = \frac{k!(n-k)!}{n!} = \frac{1}{\binom{n}{k}}.$$

The events $(A \in C)_{A \in \mathcal{F}}$ are pairwise disjoint, so by the union bound we have

$$1 \geq \sum_{A \in \mathcal{F}} \mathbb{P}[A \in C] = \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}},$$

which gives the LYM Inequality. ■

The LYM Inequality gives a second proof of Sperner's Lemma. In fact we get a bit more, as it allows us to characterize the extremal set systems.

Corollary 7. *Let $\mathcal{F} \subseteq \mathcal{P}(n)$ be an antichain. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$, with equality if and only if if $\mathcal{F} = [n]^{(\lfloor n/2 \rfloor)}$ or $\mathcal{F} = [n]^{\lceil n/2 \rceil}$.*

Proof. Let $\mathcal{F} \subseteq \mathcal{P}(n)$ be an antichain. By the LYM Inequality, we have

$$\begin{aligned} 1 &\geq \sum_{i=0}^{n} \frac{|\mathcal{F} \cap [n]^{(i)}|}{\binom{n}{i}} \\ &\geq \sum_{i=0}^{n} \frac{|\mathcal{F} \cap [n]^{(i)}|}{\binom{n}{\lfloor n/2 \rfloor}} \\ &= \frac{|\mathcal{F}|}{\binom{n}{\lfloor n/2 \rfloor}}, \end{aligned}$$

where the second inequality follows because $\binom{n}{\lfloor n/2 \rfloor}$ is the largest binomial coefficient. If we have equality in the first line (where we applied LYM) then we must have $\mathcal{F} = [n]^{(i)}$ for some i. But then to get equality in the second line we must have $i = \lfloor n/2 \rfloor$ or $i = \lceil n/2 \rceil$. ■

Lemma 4 and Sperner's Lemma together tell us that the minimum number of chains in a partition of $\mathcal{P}(n)$ is equal to the maximum size of an antichain. This is a special case of a more general theorem about partially ordered sets.

A *partially ordered set* or *poset* $(P, \leq)$ is a set P with a relation $\leq$ such that, for all $a, b, c \in P$, we have

- $a \leq a$ (reflexivity),
- if $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity),
- if $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry).

We write $a < b$ to mean $a \leq b$ and $a \neq b$.

Two elements $a, b \in P$ are *comparable* if either $a \leq b$ or $b \leq a$. Two elements are *incomparable* if they are not comparable.

A set $C \subseteq P$ is a *chain* if every pair of elements from C is comparable. A set $A \subseteq P$ is an *antichain* if every pair of distinct elements from A is incomparable.

Any set system $\mathcal{F}$ becomes a poset under the containment relation $\subseteq$. You should check that the chains and antichains in this poset are the same as in the earlier definition, and that a chain and an antichain can have at most one common element.

We say that a collection of chains *covers* a poset P if every element of P is contained in one of the chains. We can now state our main theorem about posets.

Theorem 8. (Dilworth's Theorem) *Let $(P, \leq)$ be a finite poset. The minimum number of chains needed to cover P is equal to the maximum size of an antichain.*

Proof. Since a chain and an antichain meet in at most one element, it is clear that the number of chains in any cover is at least as large as the maximum size of an antichain. So we need only prove that there is a cover with this many chains.

We argue by induction on $|P|$. The statement is immediate for $|P| = 0$, so we assume $|P| > 0$ and we have proved the statement for smaller posets.

Let m be the maximum size of an antichain and let C be a maximal chain (i.e. a chain C such that $C \cup \{a\}$ is not a chain, for any $a \in P \setminus C$). [Note that maximal chain does not necessarily mean chain of maximal size!]

If $P \setminus C$ contains no antichain of size m then we are done by induction: we can cover $P \setminus C$ with $m-1$ chains, and then add C to get a cover of P with m chains.

Otherwise, there is an antichain of size m in $P \setminus C$, say $A = \{a_1, \ldots, a_m\}$. Let

$$S^+ := \{x \in P : x \geq a_i \text{ for some } a_i \in A\}$$

and

$$S^- := \{x \in P : x \leq a_i \text{ for some } a_i \in A\}.$$

Then $S^+ \cap S^- = A$, as A is an antichain. Also, $S^+ \cup S^- = P$ as A is maximal (if there were $x \notin S^+ \cup S^-$ then $A \cup \{x\}$ would be a larger antichain).

We now check that S^+ and S^- are both *proper* subsets of P. Let the maximal chain C have elements $\{c_1, \ldots, c_k\}$, where $c_1 < \cdots < c_k$. Since C is maximal, c_k is a maximal element of P and c_1 is a minimal element of P. Then:

- $c_k \notin S^-$, because c_k is a maximal element of P and $c_k \notin A$
- $c_1 \notin S^+$, because c_k is a minimal element of P and $c_1 \notin A$.

Therefore, S^+ and S^- are proper subsets of P, and so by induction we can partition S^+ into m chains $C_1^+, \ldots, C_m^+$, and we can partition S^+ into m chains $C_1^-, \ldots, C_m^-$.

Since $A \subseteq S^+$ and A meets each chain C_i^+ in at most one elemen, we see that each C_i^+ must contain exactly one element of A. Relabelling if necessary, we may assume that $a_i \in C_i^+$, for $i = 1, \ldots, m$. Similarly, we may assume that $a_i \in C_i^-$, for $i = 1, \ldots, m$.

If a_i is not maximal in C_i^-, there exists $b \in C_i^-$ with $b > a_i$. But then, since $b \in S^-$, we can find $a_j \in A$ with $b \leq a_j$. This means $a_i < b \leq a_j$, so $a_i < a_j$, which gives us a contradiction as A is an antichain. So a_i is maximal in C_i^-. Similarly, a_i is minimal in C_i^+.

Finally, we glue C_i^+ and C_i^- together (the 'gluing point' being a_i) to obtain a partition of P into m chains. ■

There is a 'dual' of Dilworth's Theorem: the minimum number of antichains in a cover P is equal to the maximum size of a chain. The proof of this is an exercise on the first example sheet.

2.2 Symmetric chains and Littlewood-Offord

If $z_1, \ldots, z_n \in \mathbb{C}$ are such that $|z_i| \geq 1$, how many of the 2^n sums $\sum_{i \in I} z_i$, where $I \subseteq [n]$, can equal 0? This question was raised in 1938, by Littlewood and Offord. A few years later, Erdős found a neat solution in the real case.

Theorem 9. (Erdős) *Suppose that $x_1, \ldots, x_n \in \mathbb{R}$ satisfy $|x_i| \geq 1$ for all i. For every $\alpha \in \mathbb{R}$, there are at most $\binom{n}{\lfloor n/2 \rfloor}$ subsets $I \subseteq [n]$ such that $\sum_{i \in I} x_i \in [\alpha, \alpha + 1)$.*

Note that the bound in this theorem is sharp: take $x_i = 1$ for all i, and set $\alpha = \lfloor n/2 \rfloor$.

Proof of Theorem 9. Consider first the effect of replacing x_i with $-x_i$. Let $S_1, \ldots, S_N$ denote the $N = 2^{n-1}$ sums corresponding to subsets $I \subseteq [n]$ that do not contain i. Then the full collection of sums of subsets is

$$S_1, \ldots, S_N, S_1 + x_i, S_2 + x_i, \ldots, S_N + x_i.$$

If we replace x_i with $-x_i$, this becomes

$$S_1, \ldots, S_N, S_1 - x_i, S_2 - x_i, \ldots, S_N - x_i,$$

which is just a translation (and reordering) of the first collection. So replacing x_i by $-x_i$ does not affect the truth of the theorem.

We may assume that $x_i \geq 1$ for all i. But now, if we take any $\binom{n}{\lfloor n/2 \rfloor} + 1$ subsets of $[n]$, then by Sperner's Lemma there must be some pair I, J with $I \subsetneq J$. Then $\sum_{i \in J} x_i \geq \sum_{i \in I} x_i + 1$, so we cannot have both sums in $[\alpha, \alpha + 1)$. ■

We will also see a solution to the Littlewood-Offord problem in the complex case, but first let us think a bit more about chains.

A chain $C_1 \subseteq C_2 \subseteq \cdots \subseteq C_m$ in $\mathcal{P}(n)$ is *symmetric* if $|C_{i+1}| = |C_i| + 1$, for all $i = 1, \ldots, m-1$, and $|C_1| + |C_m| = n$. We saw in Proposition 4 that $\mathcal{P}(n)$ can be partitioned into $\binom{n}{\lfloor n/2 \rfloor}$ chains, but the chains we obtained could be asymmetric.

Proposition 10. *For $n \geq 1$, there is a partition of $\mathcal{P}(n)$ into symmetric chains.*

Proof. We argue by induction on n. The case $n = 1$ is easy! So suppose that $n > 1$ and that $\mathcal{C}_1, \ldots, \mathcal{C}_m$ is a partition of $\mathcal{P}(n-1)$ into symmetric chains. For each chain $\mathcal{C}_i$, say $\mathcal{C}_i = \{A_1, \ldots A_k\}$ with $A_1 \subseteq \ldots \subseteq A_k$, we define two chains in $\mathcal{P}(n)$:

$$\mathcal{C}_i' := \{A_1, A_2, \ldots, A_k, A_k \cup n\}$$

and

$$\mathcal{C}_i'' := \{A_1 \cup n, \ldots, A_{k-1} \cup n\}.$$

If $k = 1$ then $\mathcal{C}_i''$ is empty: we discard these empty chains. The resulting chains give a partition of $\mathcal{P}(n)$ into symmetric chains. ■

A symmetric chain decomposition of $\mathcal{P}(n)$ has $\binom{n}{\lfloor n/2 \rfloor}$ chains, each of which contains an element from the middle layer (or contains an element from each middle layer, if n is odd). For each $i \leq n/2$, there are

$$\binom{n}{i} - \binom{n}{i-1}$$

chains of size $n - 2i + 1$, and these run from the ith layer to the $(n-i)$th layer.

We now return to the Littlewood-Offord problem, and in fact answer it in any number of dimensions (note that the case $k = 2$ deals with the special case of complex numbers).

Theorem 11. *Let $k, n \geq 1$ and suppose that $x_1, \ldots, x_n \in \mathbb{R}^k$ satisfy $||x_i||_2 \geq 1$ for all i. Let $K \subseteq \mathbb{R}^k$ have diameter $\mathrm{diam}(K) < 1$. Then there are at most $\binom{n}{\lfloor n/2 \rfloor}$ subsets $I \subseteq [n]$ such that $\sum_{i \in I} x_i \in K$.*

Proof. Let us define, for $A \subseteq [n]$, $x_A = \sum_{i \in A} x_i$. We shall call a family $\mathcal{A} \subseteq \mathcal{P}(n)$ *sparse* if

$$||x_A - x_B|| \geq 1$$

for all distinct $A, B \in \mathcal{A}$.

We shall say that a partition $D_1 \cup \cdots \cup D_m$ of $\mathcal{P}(n)$ is *symmetric* if it has the same number of sets of each size as a symmetric chain decomposition of $\mathcal{P}(n)$.

It is enough to show that $\mathcal{P}(n)$ has a symmetric partition into sparse families, as a sparse partition has $\binom{n}{\lfloor n/2 \rfloor}$ sets, and if I is a sparse set then there is at most one $A \in I$ with $x_A \in K$.

We prove the existence of a symmetric partition into sparse families by induction on n. The case $n = 1$ is easy. So suppose that $n > 1$ and that $\mathcal{F}_1, \ldots, \mathcal{F}_m$ is a symmetric partition of $\mathcal{P}(n-1)$ into sparse families (with respect to the vectors $x_1, \ldots, x_{n-1}$).

Suppose $\mathcal{F}_i = \{A_1, \ldots, A_t\}$, where

$$\langle x_{A_1}, x_n \rangle \leq \cdots \leq \langle x_{A_t}, x_n \rangle,$$

and $\langle \cdot, \cdot \rangle$ is the usual inner product on $\mathbb{R}^k$. Define two new families in $\mathcal{P}(n)$:

$$\mathcal{F}_i' := \{A_1, A_2, \ldots, A_t, A_t \cup n\}$$

and

$$\mathcal{F}_i'' := \{A_1 \cup n, A_2 \cup n, \ldots, A_{t-1} \cup n\},$$

discarding empty families (as in Proposition 10). We claim that this gives a symmetric partition of $\mathcal{P}(n)$ into sparse families.

It is clear that the construction gives the same number of sets of each size as in a symmetric chain decomposition of $\mathcal{P}(n)$; and that $\mathcal{F}_i''$ is sparse, since the corresponding sums are translations by x_n of the sums corresponding to $\mathcal{F}_i$. To see that $\mathcal{F}_i'$ is also sparse, we note that $\mathcal{F}_i$ is a sparse subset. Also, for any $j \in [r]$, we have (writing $\hat{x}_n = x_n / ||x_n||_2$ for the unit vector in direction x_n)

$$\begin{aligned} ||x_{A_t \cup \{n\}} - x_{A_j}||_2 &\geq \langle x_{A_t \cup \{n\}} - x_{A_j}, \hat{x}_n \rangle \\ &= \langle x_{A_t \cup \{n\}}, \hat{x}_n \rangle - \langle x_{A_j}, \hat{x}_n \rangle \\ &= \langle x_{A_t} + x_n, \hat{x}_n \rangle - \langle x_{A_j}, \hat{x}_n \rangle \\ &\geq 1 + \langle x_{A_t}, \hat{x}_n \rangle - \langle x_{A_j}, \hat{x}_n \rangle \\ &\geq 1, \end{aligned}$$

since $\langle x_{A_r}, x_n \rangle \geq \langle x_{A_j}, x_n \rangle$. ■

2.3 Shadows and Kruskal-Katona

For $\mathcal{A} \subseteq [n]^{(r)}$, the Local LYM Inequality tells us that

$$\frac{|\partial \mathcal{A}|}{\binom{n}{r-1}} \geq \frac{|\mathcal{A}|}{\binom{n}{r}},$$

with equality iff $\mathcal{A} = \emptyset$ or $\mathcal{A} = [n]^r$. What happens in between?

It will be helpful to define two orders on $[n]^{(r)}$: the lexicographic and colexicographic orders.

In *lexicographic order* or *lex*, we have

$$A < B \text{ if } A \neq B \text{ and } \min(A \triangle B) \in A.$$

Equivalently, for distinct $A, B \in [n]^{(r)}$, with elements $a_1 < \cdots < a_r$ and $b_1 < \cdots < B_r$, we have $A < B$ if $a_i < b_i$, where $i = \min\{j : a_j \neq b_j\}$. This is the familiar dictionary order.

In *colexicographic order* or *colex*,

$$A < B \text{ if } A \neq B \text{ and } \max(A \triangle B) \in B.$$

Equivalently, we have $A < B$ if

$$\sum_{i \in A} 2^i < \sum_{i \in B} 2^i.$$

This can be thought of as 'binary' order.

We write $A <_{\text{lex}} B$ and $A <_{\text{colex}} B$ to distinguish betwen the two orders.

Lex and colex are very different. For instance, if we order pairs of natural numbers by colex we get

$$12, 13, 23, 14, 24, 34, 15, 25, 35, \ldots$$

while in lex we have

$$12, 13, 14, \ldots, 23, 24, 25, \ldots, 34, 35, 36, \ldots \ , \ldots .$$

The aim of this section is to prove the following theorem.

Theorem 12. (Kruskal-Katona Theorem) *Let $\mathcal{F} \subseteq [n]^{(r)}$ and let $\mathcal{A}$ be the family consisting of the first $|\mathcal{F}|$ elements of $[n]^{(r)}$ in colex order. Then $|\partial \mathcal{F}| \geq |\partial \mathcal{A}|$.*

In other words:

shadows are minimized by taking initial segments of colex.

Our strategy to prove the Kruskal-Katona Theorem is as follows: we replace $\mathcal{F}$ with a family $\mathcal{F}' \subseteq [n]^{(r)}$ such that

- $|\mathcal{F}'| = |\mathcal{F}|$
- $|\partial\mathcal{F}'| \leq |\partial\mathcal{F}|$
- $\mathcal{F}'$ is 'closer' to an initial segment of $[n]^{(r)}$.

We repeat, making the family 'nicer' at each step, and (hopefully) end up with an initial segment of colex.

In order to carry out this strategy, we will employ compression operators.[2] For distinct $i, j \in [n]$, the *compression operator* C_{ij} is the function from $\mathcal{P}(n)$ to $\mathcal{P}(n)$ defined by

$$C_{ij}(A) = \begin{cases} (A \setminus j) \cup i & \text{if } i \notin A, j \in A \\ A & \text{otherwise.} \end{cases}$$

For a set system $\mathcal{F}$, we define

$$C_{ij}(\mathcal{F}) := \{C_{ij}(A) : A \in \mathcal{F}\} \cup \{A \in \mathcal{F} : C_{ij}(A) \in \mathcal{F}\}.$$

If $i < j$, we sometimes refer to C_{ij} as a *left compression*.

Note that, for any $A \subseteq [n]$ and any $\mathcal{F} \subseteq \mathcal{P}(n)$, we have:

- $|C_{ij}(A)| = |A|$
- $|C_{ij}(\mathcal{F})| = |\mathcal{F}|$
- $C_{ij}(C_{ij}(\mathcal{F})) = C_{ij}(\mathcal{F})$
- if $j \in A$ and $A \in C_{ij}(\mathcal{F})$ then $A \in \mathcal{F}$ and $C_{ij}(A) \in \mathcal{F}$.

You should check all of these as an exercise!

If compressions are to be useful, we need to know that they interact well with shadows. This is indeed the case.

[2] Actually, these compression operators won't quite be enough to get what we want. But we will shortly define a slightly more general compression operator, and those *will* be enough.

Lemma 13. *For $1 \leq i < j \leq n$ and $\mathcal{F} \subseteq [n]^{(r)}$, we have $|\partial C_{ij}(\mathcal{F})| \leq |\partial \mathcal{F}|$.*

Proof. Let $\mathcal{G} = C_{ij}(\mathcal{F})$: so we must show that $|\partial \mathcal{G}| \leq |\partial \mathcal{F}|$. It will be enough to show the following.

Claim. *Let $G' \in \partial \mathcal{G} \setminus \partial \mathcal{F}$. Then*

1. *$i \in G'$, $j \notin G'$*
2. *$(G' \setminus i) \cup j \in \partial \mathcal{F} \setminus \partial \mathcal{G}$.*

If the claim holds, then it implies that C_{ji} gives an injection

$$C_{ji} : \partial \mathcal{G} \setminus \partial \mathcal{F} \to \partial \mathcal{F} \setminus \partial \mathcal{G}.$$

Indeed, (1) shows that C_{ji} is injective on $\partial G \setminus \partial \mathcal{F}$, and (2) shows that the image is contained in $\partial \mathcal{F} \setminus \partial \mathcal{G}$.

Thus we need only prove the claim. So consider $G' \in \partial \mathcal{G} \setminus \partial \mathcal{F}$. There are $G \in \mathcal{G}$ and $x \in [n]$ such that $G = G' \cup x$. Since $G' \in \partial \mathcal{G} \setminus \partial \mathcal{F}$, we must have $G \in \mathcal{G} \setminus \mathcal{F}$ and so $i \in G$ and $j \notin G$; we must also have $F := (G \setminus i) \cup j \in \mathcal{F} \setminus \mathcal{G}$.

If $x = i$ then $G' \subseteq F$, so we must have $x \neq i$. So $i \in G'$ and $j \notin G'$, which proves (1).

Let $F' = C_{ji}(G') = (G' \setminus i) \cup j$. Then $F' \subseteq F$, so $F' \in \partial \mathcal{F}$. All that remains is to show that

$$F' \notin \partial \mathcal{G}.$$

Suppose otherwise. Then there is z such that

$$F' \cup z = (G' \setminus i) \cup j \cup z \in \mathcal{G}.$$

Two cases:

- $z \neq i$: since $C_{ij}(\mathcal{G}) = \mathcal{G}$, we have

  $$C_{ij}(F' \cup z) = G' \cup z \in \mathcal{G}.$$

  But then $F' \cup z$ and $C_{ij}(F' \cup z)$ are both in $\mathcal{G}$, and so both are in $\mathcal{F}$. This gives a contradiction, as then $G' \subseteq C_{ij}(F' \cup z)$, so $G' \in \partial \mathcal{F}$.

- $z = i$: then $F' \cup z = G' \cup j \in \mathcal{G}$. Since $i, j \in G' \cup j$ we also have $G' \cup j \in \mathcal{F}$, which again gives a contradiction as then $G' \in \partial \mathcal{F}$.

■

We say that a family $\mathcal{F} \subseteq \mathcal{P}(n)$ is *left-compressed* if $C_{ij}(\mathcal{F}) = \mathcal{F}$ for all $1 \leq i < j \leq n$.

Corollary 14. *Let $\mathcal{F} \subseteq [n]^{(r)}$. Then there is a left-compressed family $\mathcal{A} \subseteq [n]^{(r)}$ such that $|\mathcal{A}| = |\mathcal{F}|$ and $|\partial\mathcal{A}| \leq |\partial\mathcal{F}|$.*

Proof. For $\mathcal{A} \subseteq \mathcal{P}(n)$, we define the function

$$f(\mathcal{A}) := \sum_{A \in \mathcal{A}} \sum_{a \in A} 2^a.$$

Then for any $i < j$, applying C_{ij} either leaves $\mathcal{A}$ unchanged or strictly decreases the value of f.

Let $\mathcal{A} \subseteq \mathcal{P}(n)$ satisfy $|\mathcal{A}| = |\mathcal{F}|$, $|\partial\mathcal{A}| \leq |\partial\mathcal{F}|$ and, subject to this, have $f(\mathcal{A})$ minimal. Then, by the lemma above, $\mathcal{A}$ must be left-compressed. ■

Any initial segment of $[n]^{(r)}$ in colex is left-compressed, so we might hope that Corollary 14 is enough to prove Kruskal-Katona. Unfortunately, not every left-compressed set system is an initial segment of colex: for instance $\{12, 13, 14\}$ is left-compessed but $23 <_{\text{colex}} 14$.

We will need a more general compression operator to prove Kruskal-Katona Theorem.

Let $U, V \subseteq [n]$ satisfy $|U| = |V|$ and $U \cap V = \emptyset$. The *UV-compression operator* C_{UV} is the function from $\mathcal{P}(n)$ to $\mathcal{P}(n)$ defined by

$$C_{UV}(A) = \begin{cases} (A \setminus V) \cup U & \text{if } U \cap A = \emptyset, V \subseteq A \\ A & \text{otherwise.} \end{cases}$$

For a set system $\mathcal{F}$, we define

$$C_{UV}(\mathcal{F}) := \{C_{UV}(A) : A \in \mathcal{F}\} \cup \{A \in \mathcal{F} : C_{UV}(A) \in \mathcal{F}\}.$$

A family $\mathcal{A}$ is *(U, V)-compressed* if $C_{UV}(\mathcal{A}) = \mathcal{A}$.

It is clear that $|C_{UV}(A)| = |A|$ and $|C_{UV}(\mathcal{A})| = |\mathcal{A}|$. We will use the following technical lemma, which extends Lemma 13.

Lemma 15. *Let $U, V \subseteq [n]$ be disjoint sets with $|U| = |V|$. Suppose that $\mathcal{F} \subseteq [n]^{(r)}$ satisfies*

$$\forall u \in U \ \exists v \in V \text{ such that } \mathcal{F} \text{ is } (U \setminus u, V \setminus v)\text{-compressed.} \tag{2.5}$$

Then $|\partial C_{UV}(\mathcal{F})| \leq |\partial\mathcal{F}|$.

Proof. We generalize the proof of Lemma 13. Let $\mathcal{G} = C_{UV}(\mathcal{F})$ and consider $G' \in \partial\mathcal{G} \setminus \partial\mathcal{F}$. We will show:

Claim. *Let $G' \in \partial\mathcal{G} \setminus \partial\mathcal{F}$. Then*

1. $U \subseteq G'$, $V \cap G' = \emptyset$
2. $(G' \setminus U) \cup V \in \partial\mathcal{F} \setminus \partial\mathcal{G}$.

As before, this implies that C_{VU} gives an injection from $\partial\mathcal{G} \setminus \partial\mathcal{F}$ to $\partial\mathcal{F} \setminus \partial\mathcal{G}$, and the lemma follows.

Thus we need only prove the claim. So suppose we are given G' as in the claim. There are $G \in \mathcal{G}$ and $x \in [n]$ such that $G = G' \cup x$. Since $G' \in \partial\mathcal{G} \setminus \partial\mathcal{F}$, we must have $G \in \mathcal{G} \setminus \mathcal{F}$ and so $U \subseteq G$ and $V \cap G = \emptyset$; we must also have $F := (G \setminus U) \cup V \in \mathcal{F} \setminus \mathcal{G}$.

If $x \in U$ then by (2.5) there is $y \in V$ such that $\mathcal{F}$ is $(U \setminus x, V \setminus y)$-compressed, so

$$C_{U\setminus x, V\setminus y}(F) = (G \setminus x) \cup y \in \mathcal{F}.$$

But then $G' = G \setminus x \subseteq F$, which gives a contradiction. So we must have $x \notin U$. So $U \subseteq G'$ and $V \cap G' = \emptyset$, which proves (1).

Let $F' = C_{VU}(G') = (G' \setminus U) \cup V$. Then $F' \subseteq F$, so $F' \in \partial\mathcal{F}$. All that remains is to show that

$$F' \notin \partial\mathcal{G}.$$

Suppose otherwise. Then there is z such that

$$F' \cup z = (G' \setminus U) \cup V \cup z \in \mathcal{G}.$$

Two cases:

- $z \notin U$: since $C_{UV}(\mathcal{G}) = \mathcal{G}$, we have

  $$C_{UV}(F' \cup z) = G' \cup z \in \mathcal{G}.$$

  But then $F' \cup z$ and $C_{UV}(F' \cup z)$ are both in $\mathcal{G}$, and so both are in $\mathcal{F}$. This gives a contradiction, as then $G' \subseteq C_{UV}(F' \cup z)$, so $G' \in \partial\mathcal{F}$.

- $z \in U$: then $F' \cup z \in \mathcal{G}$ and $F' \cup z$ meets both U and V, so we must have $F' \cup z \in \mathcal{F}$. But there is $y \in V$ such that $\mathcal{F}$ is $(U \setminus u, V \setminus v)$-compressed, and so $C_{U\setminus u, V\setminus v}(F' \cup z) = G' \cup y \in \mathcal{F}$, which again gives a contradiction as then $G' \in \partial\mathcal{F}$.

■

We can now prove the Kruskal-Katona Theorem:

Proof of Kruskal-Katona. Let $\mathcal{A} \subseteq [n]^{(r)}$ satisfy

- $|\mathcal{A}| = |\mathcal{F}|$
- $|\partial\mathcal{A}| \leq |\partial\mathcal{F}|$
- subject to this, $\sum_{A\in\mathcal{A}} \sum_{i\in A} 2^i$ is minimal.

Let

$$\Lambda = \{(U, V) : |U| = |V| > 0, U \cap V = \emptyset, \max U < \max V\}.$$

If $\mathcal{A}$ is (U, V)-compressed for all $(U, V) \in \Lambda$ then $\mathcal{A}$ is an initial segment of colex: if $A \in \mathcal{A}$ and $B <_{\text{colex}} A$ then $\max(B \setminus A) < \max(A \setminus B)$ and so $\mathcal{A}$ is $(B \setminus A, A \setminus B)$-compressed, which implies $C_{B\setminus A, A\setminus B}(A) = B \in \mathcal{A}$.

Otherwise, pick $(U, V) \in \Lambda$ such that $\mathcal{A}$ is not (U, V)-compressed and $|U|$ is minimal. Then $\mathcal{A}$ is $(U \setminus u, V \setminus \min V)$-compressed for all $u \in U$, and so by Lemma 15 we have $|\partial C_{UV}(\mathcal{A})| \leq |\partial\mathcal{A}|$. But $C_{UV}(\mathcal{A})$ has strictly smaller weight than $\mathcal{A}$, which contradicts the minimality of the weight of $\mathcal{A}$. ■

Chapter 3

Intersections and traces

3.1 Erdős-Ko-Rado and the Two Families Theorem

A family $\mathcal{A} \subseteq \mathcal{P}(n)$ is *intersecting* if $|A \cap B| \neq \emptyset$, for all $A, B \in \mathcal{A}$.

What is the maximum size of an intersecting family in $\mathcal{P}(n)$? The set $\{A \subseteq [n] : 1 \in A\}$ is intersecting and has size 2^{n-1}. It is easy to show that this is best possible.

Proposition 16. *Let $\mathcal{A} \subseteq \mathcal{P}(n)$ be intersecting. Then $|\mathcal{A}| \leq 2^{n-1}$.*

Proof. $\mathcal{A}$ contains at most one set from each pair $(A, [n] \setminus A)$. ■

A much more interesting question is: what is the largest intersecting family of r-sets in $\mathcal{P}(n)$? There are three regimes to consider:

- $r > n/2$: This case is trivial, as we can take the entire layer $[n]^{(r)}$.
- $r = n/2$: (Obviously, this only happens when n is even.) This case is easy: we can take at most one from each pair $(A, [n] \setminus A)$, and any system obtained in this way is intersecting. Thus the maximum is

$$\frac{1}{2}\binom{n}{n/2} = \binom{n-1}{n/2-1} = \binom{n-1}{r-1}.$$

- $r < n/2$: This is more interesting! One example is to take all r-sets containing a fixed element, say 1. This gives a system of size $\binom{n-1}{r-1}$.

Very good. But we could also take all sets that contain at least two elements from $\{1,2,3\}$. This also gives an intersecting system, and a litle calculation shows that it has size $3\binom{n-3}{r-2} + \binom{n-3}{r-3}$. A little more calculation shows that the first system is bigger, but of course we want to handle all possible systems.

This last case is where the Erdős-Ko-Rado Theorem comes in.

Theorem 17. *(Erdős-Ko-Rado Theorem) For $r \leq n/2$, if $\mathcal{A} \subseteq [n]^{(r)}$ is intersecting then $|\mathcal{A}| \leq \binom{n-1}{r-1}$.*

Remark: In fact, for $r < n/2$, we get equality only for the systems that consist of all r-sets containing a fixed point. (We won't prove this here.) For $r = n/2$ it is easy to construct many nonisomorphic systems.

We shall give two proofs: the first uses Katona's ingenious circle method; the second uses the Kruskal-Katona Theorem.

First proof of the Erdős-Ko-Rado Theorem. Consider any bijection $f : [n] \to \mathbb{Z}_n$. We say that A maps to an interval under f if $f(A) := \{f(a) : a \in A\} = \{i, i+1, \ldots, i+k-1\}$, for some $0 \leq i \leq n-1$ (where addition is modulo n). We will double count the number N of pairs (f, A) such that $f : [n] \to \mathbb{Z}_n$ is a bijection and $f(A)$ is an interval.

For any fixed f, we claim that at most k sets in $\mathcal{A}$ map to intervals under f. Indeed, suppose $A \in \mathcal{A}$ and $f(A) = \{i, i+1, \ldots, i+k-1\}$. Since $\mathcal{A}$ is intersecting, any other interval that we get under f must be of form

$$\{j, j-1, \ldots, j-(k-1)\}$$

or

$$\{j+1, j+2, \ldots, j+k\}),$$

for some $j \in \{i, i+1, \ldots, i+k-2\}$. But for each j we can get at most one of these two intervals (as they are disjoint). So we get at most $k-1$ such intervals, and hence at most k in total. Summing over all $n!$ bijections from $[n]$ to $\mathbb{Z}_n$, we see that

$$N \leq kn!.$$

On the other hand, each $A \in \mathcal{A}$ is an interval under $n(n-k)!k!$ bijections, so

$$N = |\mathcal{A}|n(n-k)!k!.$$

Combining these bounds on N gives

$$|\mathcal{A}| \leq \frac{kn!}{n(n-k)!k!} = \binom{n-1}{k-1}.$$

■

Now for a proof involving shadows. Recall that $\partial\mathcal{A}$ is the shadow of the set system $\mathcal{A}$. We write $\partial^{(2)}\mathcal{A} = \partial(\partial A)$, $\partial^{(3)}\mathcal{A} = \partial(\partial^{(2)}A)$, and so on. Note that $\partial^{(k)}\mathcal{A}$ is the collection of sets B that can be obtained from some $A \in \mathcal{A}$ by deleting k elements.

Second proof of the Erdős-Ko-Rado Theorem. Let $\mathcal{A} \subseteq [n]^{(r)}$ be an intersecting family, and set

$$\mathcal{B} = \{A^c : A \in \mathcal{A}\} \subseteq [n]^{(n-r)}.$$

Since $\mathcal{A}$ is intersecting, no set $A \in \mathcal{A}$ is contained in any set $B \in \mathcal{B}$. So

$$\partial^{(n-2r)}\mathcal{B} \subseteq [n]^{(r)}$$

is disjoint from $\mathcal{A}$.

Now if $|\mathcal{A}| \geq \binom{n-1}{r-1}$ then

$$|\mathcal{B}| = |\mathcal{A}| \geq \binom{n-1}{r-1} = \binom{n-1}{n-r}.$$

We now apply Kruskal-Katona repeatedly:

$$|\partial\mathcal{B}| \geq |\partial[n-1]^{(n-r)}| = \binom{n-1}{n-r-1}$$

and so

$$|\partial^{(2)}\mathcal{B}| \geq |\partial[n-1]^{(n-r-1)}| = \binom{n-1}{n-r-2},$$

and so on, showing at each step that $|\partial^{(i)}\mathcal{B}| \geq \binom{n-1}{n-r-i}$, until we get

$$|\partial^{(n-2r)}\mathcal{B}| \geq |\partial[n-1]^{(r+1)}| = \binom{n-1}{n-r-(n-2r)} = \binom{n-1}{r}.$$

So if $|\mathcal{A}| > \binom{n-1}{r-1}$, we get

$$\binom{n}{r} \geq |\mathcal{A} \cup \partial^{(n-2r)}\mathcal{B}| > \binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r},$$

which gives a contradiction. ■

Theorem 18 (Liggett's Theorem)**.** *Suppose that $Y_1, \ldots, Y_n$ are independent random variables with $\mathbb{P}(Y_i = 1) = 1 - \mathbb{P}(Y_i = 0) = p \geq 1/2$ for each i. Let $\alpha_1, \ldots, \alpha_n$ be non-negative numbers summing to 1. Then*

$$\mathbb{P}\left(\sum_i \alpha_i Y_i \geq 1/2\right) \geq p.$$

Proof. Suppose first that no proper subset of the α_i sum to $1/2$. Let

$$\mathcal{A} = \{A \subseteq [n] : \sum_{i \in A} \alpha_i > 1/2\}$$

and let $\mathcal{A}_k = \mathcal{A} \cap [n]^{(k)}$. Let $N_k = |\mathcal{A}_k|$.

Then $N_k + N_{n-k} = \binom{n}{k}$ since for every set B of size k exactly one of $\{B, B^c\}$ belongs to $\mathcal{A}$. Also, for each k the family $\mathcal{A}_k$ is intersecting, so by the Erdős-Ko-Rado theorem we have that $N_k \leq \binom{n-1}{k-1}$ when $2k \leq n$.

We also have that

$$\mathbb{P}\left(\sum_i \alpha_i Y_i \geq 1/2\right) = \sum_{k=0}^{n} p^k (1-p)^{n-k} N_k$$

and (by binomial expansion of $(1 - p + p)^{n-1}$) we have

$$p = \sum_{k=0}^{n} p^k (1-p)^{n-k} \binom{n-1}{k-1}.$$

So

$$\mathbb{P}\left(\sum_i \alpha_i Y_i \geq 1/2\right) - p = \sum_{k=0}^{n} \left(p^k (1-p)^{n-k} \left(N_k - \binom{n-1}{k-1}\right)\right)$$

$$= \sum_{2k \leq n} \left(p^k (1-p)^{n-k} \left(N_k - \binom{n-1}{k-1}\right)\right) + \sum_{2k > n} \left(p^k (1-p)^{n-k} \left(N_k - \binom{n-1}{k-1}\right)\right).$$

Changing variables in the second sum gives

$$\sum_{2k<n} \left(p^{n-k}(1-p)^k \left(N_{n-k} - \binom{n-1}{k}\right)\right) = \sum_{2k<n} \left(p^{n-k}(1-p)^k \left(\binom{n-1}{k-1} - N_k\right)\right)$$

so we get that

$$\mathbb{P}\left(\sum_i \alpha_i Y_i \geq 1/2\right) - p$$

$$\geq \sum_{2k<n} \left(\left(p^k(1-p)^{n-k} - p^{n-k}(1-p)^k\right) \left(N_k - \binom{n-1}{k-1}\right)\right)$$

which is non-negative (term-wise) for $p \geq 1/2$.

The case where a proper sumset of the α_i sum to $1/2$ follows either by a limiting argument or a more careful version of the above argument (non-examinable). ■

We next prove the Two Families Theorem, which is due to Bollobás.

Theorem 19. (Two Families Theorem) *Let $A_1, \ldots, A_k$ and $B_1, \ldots, B_k$ be finite sets such that, for all i,*

$$A_i \cap B_i = \emptyset$$

and, for all $i \neq j$,

$$A_i \cap B_j \neq \emptyset.$$

Then

$$\sum_{i=1}^{k} \binom{|A_i| + |B_i|}{|A_i|}^{-1} \leq 1.$$

If we specify the size of the sets, we get the following useful corollary.

Corollary 20. *Let $A_1, \ldots, A_k$ be a-sets and $B_1, \ldots, B_k$ be b-sets such that, for all i,*

$$A_i \cap B_i = \emptyset$$

and, for all $i \neq j$,

$$A_i \cap B_j \neq \emptyset.$$

Then

$$k \leq \binom{a+b}{a}.$$

Corollary 20 is an immediate consequence of the Two Families Theorem.

Proof of the Two Families Theorem. We may assume that all sets are subsets of $[n]$. For a permutation π of $[n]$, we write $A <_\pi B$ if

$$\max \pi(A) < \min \pi(B),$$

where we write $\pi(S) := \{\pi(x) : x \in S\}$.

Let $\pi \in S_n$ be chosen uniformly at random from the set of permutations of $[n]$. Then, for each i, as $A_i \cap B_i = \emptyset$, we have

$$\mathbb{P}(A_i <_\pi B_i) = \binom{|A_i| + |B_i|}{|A_i|}^{-1},$$

On the other hand, if $A_i <_\pi B_i$ then $A_j \not<_\pi B_j$ for $j \neq i$ (as $A_i \cap B_j$ and $A_j \cap B_i$ are both nonempty). So the events $(A_i <_\pi B_i)_{i \in [k]}$ are disjoint, and so

$$1 \geq \sum_{i=1}^{k} \mathbb{P}(A_i <_\pi B_i) = \sum_{i=1}^{k} \binom{|A_i| + |B_i|}{|A_i|}^{-1},$$

which gives the required inequality. ■

Let us see an application of the Two Families Theorem.

An *r-uniform hypergraph* $H = (V, E)$ consists of a set V (of *vertices*) and a set $E \subseteq V^{(r)}$ (of *edges*). The *complete r-uniform hypergraph on k vertices* is $K_k^{(r)} := ([k], [k]^{(r)})$. Isomorphism is defined just as you expect. If H' is isomorphic to H we will often say that H' is a *copy* of H.

Let H be an r-uniform hypergraph. We say that an r-uniform hypergraph G is H-saturated if G does not contain a copy of H, but if we add any edge to G then the resulting hypergraph contains a copy of $\mathcal{H}$.

For instance, in the case of graphs, if $H = K_3$ then Turán's Theorem tells us that the mamximal number of edges in an H-saturated graph on n vertices is $\lfloor n^2/4 \rfloor$; it is an exercise to show that the minimum number of edges is $n - 1$.

In general, it is very hard to determine the maximum number of edges in a $K_k^{(r)}$-saturated hypegraph. Suprisingly, Bollobás determined the *minimum* number precisely.

Theorem 21. *Let G be an r-uniform hypergraph with vertex set $[n]$, and suppose that adding any edge to G creates a copy of $K_r^{(r+s)}$. Then G has at least*

$$\binom{n}{r} - \binom{n-s}{r}$$

edges.

Proof. Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be the *non-edges* of G. For each i, there is an $(r+s)$-element set $K_i \supset A_i$ such that adding A_i to $\mathcal{G}$ creates a copy of $K^{(r)}_{r+s}$ with vertex set K_i. Let $B_i = [n] \setminus K_i$. Then

- $|A_i| = r$ and $|B_i| = n - r - s$ for each i;
- $A_i \cap B_i = \emptyset$ for each i;
- for distinct i, j, we have $A_i \cap B_j \neq \emptyset$ (or else we would have $A_i \subseteq [n] \setminus B_j = K_j$, and so G would be missing two edges A_i, A_j from the complete r-graph with vertex set K_j).

So we can apply the Two Families Theorem to get

$$m \leq \binom{r + (n-r-s)}{r} = \binom{n-s}{r}.$$

■

The above bound is sharp: we can take the r-uniform hypergraph with vertex class $[n]$ and edges $\{F \in [n]^{(r)} : F \cap [s] \neq \emptyset\}$.

3.2 VC-dimension

Let $\mathcal{F} \subseteq \mathcal{P}(X)$ and $S \subseteq X$. The *trace of $\mathcal{F}$ on S* is the set system

$$\mathcal{F}|S := \{A \subseteq S : \text{there exists } F \in \mathcal{F} \text{ such that } F \cap S = A\}.$$

We set

$$\mathrm{tr}_{\mathcal{F}}(S) = |\mathcal{F}|S| \,,$$

i.e. the number of sets in the trace of $\mathcal{F}$ on S. We say that S *is shattered by* $\mathcal{F}$ if $\mathcal{F}|S = \mathcal{P}(S)$ (in other words, $\mathrm{tr}_{\mathcal{F}}(S) = 2^{|S|}$).

The *VC-dimension of $\mathcal{F}$* is $\max\{|S| : S \subseteq X \text{ is shattered by } \mathcal{F}\}$. [VC stands for Vapnik-Chervonenkis.]

Example 1. The family $[n]^{\leq d}$ has VC-dimension d.

What is the VC-dimension of the (infinite) family $\mathcal{H}$ consisting of all half-planes (in $\mathbb{R}^2$)? For instance, $\{(1,1),(2,1),(3,1)\}$ cannot be shattered

by $\mathcal{H}$ (there is not way to obtain the subset $\{(1,1),(3,1)\}$ by intersecting $\{(1,1),(2,1),(3,1)\}$ with half-planes!). However, $\{(0,1),(1,0),(1,2)\}$ is easily seen to be shattered by $\mathcal{H}$. So the VC-dimension of $\mathcal{H}$ is at least 3. (Tricky question: What is the VC-dimension of this system?)

The Sauer-Shelah Theorem tells us that if a family $\mathcal{A} \subseteq \mathcal{P}(n)$ contains more than $|[n]^{(\leq d)}|$ sets, then its VC-dimension is greater than d:

Theorem 22. *If $\mathcal{A} \subseteq \mathcal{P}(n)$ has VC-dimension at most d, then*

$$|\mathcal{A}| \leq |[n]^{(\leq d)}| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}.$$

We shall see a couple of proofs.

Proof 1 of the Sauer-Shelah Theorem. We argue by induction on $n + d$. Let

$$f(n,d) = |[n]^{(\leq d)}| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}.$$

If $n = 0$ or $d = 0$, the result is trivial. If $n + d > 0$, with $n, d > 0$, let

$$\mathcal{B} = \{A \setminus n : A \in \mathcal{A}\} \subseteq \mathcal{P}(n-1),$$

$$\mathcal{C} = \{A \in \mathcal{A} : n \notin A, A \cup \{n\} \in \mathcal{A}\} \subseteq \mathcal{P}(n-1).$$

Then $\mathcal{B}$ has VC-dimension at most d, while $\mathcal{C}$ has VC-dimension at most $d-1$ (as if S is shattered by $\mathcal{C}$, then $S \cup \{n\}$ is shattered by $\mathcal{A}$; so $|S| \leq d-1$). Hence, by induction, $|\mathcal{B}| \leq f(n-1,d)$ and $|\mathcal{C}| \leq f(n-1,d-1)$ and

$$|\mathcal{A}| = |\mathcal{B}| + |\mathcal{C}| \leq f(n-1,d) + f(n-1,d-1) = f(n,d).$$

■

Proof 2 of the Sauer-Shelah Theorem. Define the *i-compression operator* by

$$\pi_i(A) = A \setminus \{i\}$$

and

$$\pi_i(\mathcal{A}) = \{\pi_i(A) : A \in \mathcal{A}\} \cup \{A \in \mathcal{A} : \pi_i(A) \in \mathcal{A}\}.$$

Then π_i does not increase the VC-dimension of a set system (exercise) and $|\mathcal{A}| = |\pi_i(\mathcal{A})|$. Thus we can repeatedly apply the i-compression operator

until our family is i-compressed for all $i \in [n]$ (this terminates, as every compression either leaves the family unchanged or decreases the quantity $\sum_{A \in \mathcal{A}} |A|$).

So consider $\mathcal{B}$, the i-compressed family obtained from $\mathcal{A}$. If $\mathcal{B}$ contains any set B of size at least $d+1$ then $\mathcal{B}$ contains all subsets of B, and so has VC-dimension at least $d+1$. Otherwise,

$$|\mathcal{A}| = |\mathcal{B}| \leq |[n]^{(\leq d)}| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}.$$

■

3.3 A brief interlude on upsets and downsets

A family $\mathcal{A}$ is an *upset* if $A \in \mathcal{A}$ and $A \subseteq B$ implies that $B \in \mathcal{A}$. $\mathcal{A}$ is a *downset* if $A \in \mathcal{A}$ and $A \supset B$ implies that $B \in \mathcal{A}$.

Theorem 23. (Kleitman's Theorem) *Let $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(n)$ be downsets. Then*

$$|\mathcal{A} \cap \mathcal{B}| \geq \frac{|\mathcal{A}||\mathcal{B}|}{2^n}.$$

Proof. We argue by induction on n. The case $n = 1$ is straightforward. For $n > 1$, define

$$\mathcal{A}^+ = \{A \subseteq [n-1] : A \cup \{n\} \in \mathcal{A}\}$$

and

$$\mathcal{A}^- = \{A \subseteq [n-1] : A \in \mathcal{A}\}.$$

Define $\mathcal{B}^+$ and $\mathcal{B}^-$ similarly.

Since $\mathcal{A}$ is a downset, $\mathcal{A}^+, \mathcal{A}^-$ are downsets and $\mathcal{A}^+ \subseteq \mathcal{A}^-$; similarly for $\mathcal{B}^+$ and $\mathcal{B}^-$. Then, by induction,

$$\begin{aligned}
|\mathcal{A} \cap \mathcal{B}| &= |\mathcal{A}^+ \cap \mathcal{B}^+| + |\mathcal{A}^- \cap \mathcal{B}^-| \\
&\geq \frac{|\mathcal{A}^+||\mathcal{B}^+|}{2^{n-1}} + \frac{|\mathcal{A}^-||\mathcal{B}^-|}{2^{n-1}} \\
&= \frac{1}{2^n}(|\mathcal{A}^+| + |\mathcal{A}^-|)(|\mathcal{B}^+| + |\mathcal{B}^-|) + \frac{1}{2^n}(|\mathcal{A}^+| - |\mathcal{A}^-|)(|\mathcal{B}^+| - |\mathcal{B}^-|) \\
&\geq \frac{|\mathcal{A}||\mathcal{B}|}{2^n},
\end{aligned}$$

since $(|\mathcal{A}^+| - |\mathcal{A}^-|) \leq 0$ and $(|\mathcal{B}^+| - |\mathcal{B}^-|) \leq 0$. ■

Some authors call the above Theorem "Harris' Lemma" or "Harris-Kleitman Lemma".

3.4 More on intersecting families

A family $\mathcal{A} \subseteq \mathcal{P}(n)$ is *t-intersecting* if $|A \cap B| \geq t$, for all $A, B \in \mathcal{A}$.

When n is large enough, the Erdős-Ko-Rado Theorem generalises as follows.

Theorem 24. *Let $1 < t \leq k$ be positive integers. There exists an integer $n_0 = n_0(k,t)$ such that the following holds. For all $n > n_0$, if $\mathcal{A} \subseteq [n]^{(k)}$ is t-intersecting, then*

$$|\mathcal{A}| \leq \binom{n-t}{k-t},$$

with equality if and only if $\mathcal{A}$ is of the form $\{A \in [n]^{(k)} : T \subseteq A\}$, where T is a t-element subset of $[n]$.

Proof. We may assume that $\mathcal{A}$ is maximal and so there are $A, B \in \mathcal{A}$ with $|A \cap B| = t$ (exercise).

Let us fix $A, B \in \mathcal{A}$ with $|A \cap B| = t$. If $A \cap B \subseteq C$, for all $C \in \mathcal{A}$, then $|\mathcal{A}| \leq \binom{n-t}{k-t}$ as required.

So suppose that there exists $C \in \mathcal{A}$ with $A \cap B \not\subseteq C$. Every $D \in \mathcal{A}$ must have at least $t+1$ elements in $A \cup B \cup C$. Thus

$$|\mathcal{A}| \leq \binom{|A \cup B \cup C|}{t+1}\binom{n}{k-t-1} \leq (3k)^{t+1} n^{k-t-1} < \binom{n-t}{k-t},$$

provided n is large enough. ■

What if we allow only intersection of a fixed size?

Theorem 25 (Fisher's Inequality)**.** *Let $k \geq 1$. Suppose that $\mathcal{A} \subseteq \mathcal{P}(n)$ satisfies $|A \cap B| = k$ for all distinct $A, B \in \mathcal{A}$. Then $|\mathcal{A}| \leq n$.*

Proof. If there exists $A \in \mathcal{A}$ with $|A| = k$, then $A \subseteq B$ for all $B \in \mathcal{A}$, and the family $\{B \setminus A : B \in \mathcal{A}\}$ consists of pairwise disjoint sets, and so $|\mathcal{A}| \leq n$.

Otherwise, we may assume that $|A| > k$ for all $A \in \mathcal{A}$. Let $\chi_A \in \mathbb{R}^n$ denote the characteristic vector of A, so

$$\chi_A(i) = \begin{cases} 1 & i \in A \\ 0 & i \notin A. \end{cases}$$

We claim that the vectors in $\{\chi_A : A \in \mathcal{A}\}$ are linearly independent. Then $|\mathcal{A}| = |\{\chi_A : A \in \mathcal{A}\}| \leq \dim(\mathbb{R}^n) = n$.

So suppose that $\sum_{A\in\mathcal{A}} \lambda_A \chi_A = 0$. For any $B \in \mathcal{A}$, since $\langle \chi_A, \chi_B \rangle = |A \cap B| = k$ for $A \neq B$ and $\langle \chi_B, \chi_B \rangle = |B|$, we have

$$0 = \langle \sum_{A\in\mathcal{A}} \lambda_A \chi_A, \chi_B \rangle = \lambda_B |B| + \sum_{A\neq B} \lambda_A k = \lambda_B(|B| - k) + \Lambda k,$$

where $\Lambda = \sum_{A\in\mathcal{A}} \lambda_A$. Thus (noting that $|B| > k$)

$$\lambda_B = -\frac{k\Lambda}{|B| - k}.$$

If $\Lambda = 0$, then $\lambda_B = 0$ for all $B \in \mathcal{A}$. If $\Lambda \neq 0$, then Λ and λ_B have opposite sign. But this holds for any $B \in \mathcal{A}$, which is impossible since $\Lambda = \sum_{B\in\mathcal{A}} \lambda_B$. We conclude that the vectors χ_A are linearly independent, as required. ■

We continue with *modular* intersection theorems, where the allowed sizes of intersections are specified modulo p. Here is our first example.

Theorem 26. (Oddtown Theorem) *Let $\mathcal{A} \subseteq \mathcal{P}(n)$ be a family such that*

- *$|A|$ is odd for all $A \in \mathcal{A}$*
- *$|A \cap B|$ is even for all distinct $A, B \in \mathcal{A}$.*

Then $|\mathcal{A}| \leq n$.

First proof of the Oddtown Theorem. We work over the field with two elements $\mathbb{F}_2$. We identify each element of with its characteristic vector in $\mathbb{F}_2^n$.

Then, for all $A, B \in \mathcal{A}$, we have

$$\langle \chi_A, \chi_B \rangle = |A \cap B| = \begin{cases} 0 & \text{if } A \neq B \\ 1 & A = B. \end{cases}$$

We claim that $\{\chi_A : A \in \mathcal{A}\}$ is linearly independent in $\mathbb{F}_2^n$. If $\sum_{A\in\mathcal{A}} \lambda_A \chi_A = 0$, then, for all $B \in \mathcal{A}$, we have

$$0 = \langle \sum_{A\in\mathcal{A}} \lambda_A \chi_A, \chi_B \rangle = \lambda_B.$$

Hence the vectors $\{\chi_A : A \in \mathcal{A}\}$ are linearly independent and so $|\mathcal{A}| \leq n$. ■

Proof 2 of the Oddtwon Theorem. We work over the field with two elements $\mathbb{F}_2$. Let $\mathcal{A} = \{A_1, \ldots, A_m\}$.

Let $M = (m_{ij})$ be the $m \times n$ incidence matrix where

$$m_{ij} = \begin{cases} 1 & j \in A_i \\ 0 & j \notin A_i. \end{cases}$$

Then $N = MM^T$ is the $m \times m$ identity matrix. But then $\text{rank}(N) = m = |\mathcal{A}| \leq \text{rank}(M) \leq n$. ■

For the next theorem, we need to introduce the *multilinearization trick*. Given a polynomial f in one or more variables, we define $\tilde{f}$ to be the polynomial obtained by replacing every occurrence x^i, $i > 1$, of each variable x by just x^1. For instance if $f(x, y, z) = 4x^3 + xy + z^{10}$ then $\tilde{f}(x, y, z) = 4x + xy + z$. Here is the crucial observation: if we evaluate f and $\tilde{f}$ at a point where all variables take values 0 or 1 then they both take the same value.

Here is good example of this trick in action.

Theorem 27 (Modular Frankl-Wilson Theorem)**.** *Let p be prime and $S \subseteq \{0, 1, \ldots, p-1\}$. Suppose that $\mathcal{A} \in \mathcal{P}(n)$ satisfies:*

- *$|A| \notin S \bmod p$, for all $A \in \mathcal{A}$;*
- *$|A \cap B| \in S$ (modulo p), for all distinct $A, B \in \mathcal{A}$.*

Then

$$|\mathcal{A}| \leq \sum_{i=0}^{|S|} \binom{n}{i}.$$

Proof. We work over the field with prime number of elements $\mathbb{F}_p$, and introduce variables $x = (x_1, \ldots, x_n)$. For each $A \in \mathcal{A}$, we define the polynomial

$$f_A(x) = \prod_{s \in S} \left(\sum_{i \in A} x_i - s \right).$$

Then, for $B \in \mathcal{A}$, if $B \neq A$ we have

$$f_A(\chi_B) = \prod_{s \in S} (|A \cap B| - s) = 0,$$

while if $A = B$ we have

$$f_A(\chi_B) = \prod_{s \in S}(|A| - s) \neq 0.$$

We now replace each polynomial f_A by the corresponding multilinear polynomial $\tilde{f}_A$. For any $\chi \in \{0,1\}^n$, we have

$$\tilde{f}_A(\chi) = f_A(\chi).$$

It follows that, for $B \in \mathcal{A}$, if $B \neq A$ we have

$$\tilde{f}_A(\chi_B) = \prod_{s \in S}(|A \cap B| - s) = 0,$$

while if $B = A$ we have

$$\tilde{f}_A(\chi_A) = \prod_{s \in S}(|A| - s) = \alpha_A \neq 0.$$

The polynomials $\{\tilde{f}_A(x) : A \in \mathcal{A}\}$ are linearly independent. For if $\sum \lambda_A \tilde{f}_A = 0$ then, for any $B \in \mathcal{A}$,

$$0 = \left(\sum_{A \in \mathcal{A}} \lambda_A \tilde{f}_A\right)(\chi_B) = \alpha_B \lambda_B,$$

thus $\lambda_B = 0$. The $\tilde{f}_A$ are therefore linearly independent, and lie in the space of multilinear polynomials of degree at most $|S|$. This has dimension

$$\sum_{i=0}^{|S|} \binom{n}{i}$$

(it is spanned by the monomials $\{\prod_{i \in A} x_i : |A| \leq |S|\}$). Thus $|\mathcal{A}| \leq \sum_{i=0}^{|S|} \binom{n}{i}$. ■

What if we drop the modular constraint?

For a set $S \subseteq \mathbb{N}$, we say that a family $\mathcal{A}$ is *S-intersecting* if $|A \cap B| \in S$ for all distinct $A, B \in \mathcal{A}$.

Theorem 28 (Frankl-Wilson Theorem)**.** *Let $\mathcal{A} \subseteq \mathcal{P}(n)$ be S-intersecting. Then*

$$|\mathcal{A}| \leq \sum_{i=0}^{|S|} \binom{n}{i}.$$

We won't prove the full version of F-W here: instead we prove it under the additional assumption that $|A| \notin S$ for all $A \in \mathcal{A}$.

Proof. This is an easy deduction from the Modular Frankl-Wilson Theorem: just apply the modular version of the theorem with $p > n$. ■

The next result is a uniform version of the Modular Frankl-Wilson Theorem.

Theorem 29 (Ray-Chaudhuri-Wilson Theorem)**.** *Let $\mathcal{A} \subseteq [n]^{(k)}$ be an S-intersecting system, where $S \subseteq \{0, \ldots, k-1\}$. Then*

$$|\mathcal{A}| \leq \binom{n}{|S|}.$$

Proof. Let $x = (x_1, \ldots, x_n)$. For each $A \in \mathcal{A}$, we define

$$f_A(x) = \prod_{s \in S} \left(\sum_{i \in A} x_i - s \right).$$

So for $A, B \in \mathcal{A}$ we have

$$f_A(\chi_B) = \prod_{s \in S} (|A \cap B| - s) = \begin{cases} 0 & A \neq B \\ \neq 0 & A = B. \end{cases}$$

Now for $B \subseteq [n]$, let

$$p_B(x) = \prod_{i \in B} x_i.$$

(In particular $p_\emptyset = 1$.) We have

$$p_A(\chi_B) = \begin{cases} 1 & A \subseteq B \\ 0 & A \not\subseteq B. \end{cases}$$

Finally, define

$$q(x) = \sum_{i=0}^{n} x_i - k,$$

so $q(\chi_B) = 0$ for $B \in \mathcal{A}$, and $q(\chi_B) \neq 0$ if $|B| < k$.

Define the collection

$$\mathcal{G}: \qquad \{f_A : A \in \mathcal{A}\} \cup \{q \cdot p_B : |B| \leq |S| - 1\},$$

and let $\tilde{\mathcal{G}}$ be the multilinearized collection

$$\tilde{\mathcal{G}}: \qquad \{\tilde{f}_A : A \in \mathcal{A}\} \cup \{\widetilde{qp_B} : |B| \leq |S| - 1\}.$$

We claim that the collection $\tilde{\mathcal{G}}$ is linearly independent. If this is true then note that all the polynomials in $\tilde{\mathcal{G}}$ are multilinear and have degree at most s. Thus they lie in a space of dimension $\sum_{i=0}^{|S|} \binom{n}{i}$. However, the set $\{\widetilde{qp}_B : |B| \leq |S| - 1\}$ has size $\sum_{i=0}^{|S|-1} \binom{n}{i}$. So the set $\mathcal{A}$ has size at most $\binom{n}{|S|}$.

All that remains is to prove our claim. Suppose that

$$\sum_{A \in \mathcal{A}} \lambda_A \tilde{f}_A + \sum_{|B| \leq |S|-1} \mu_B \widetilde{qp_B} = 0.$$

For $C \in \mathcal{A}$, we have

$$\widetilde{qp_B}(\chi_C) = qp_B(\chi_C) = 0,$$

so for all $C \in \mathcal{A}$ we have

$$0 = \left(\sum_{A \in \mathcal{A}} \lambda_A \tilde{f}_A + \sum_{|B| \leq |S|-1} \mu_B \widetilde{qp_B} \right)(\chi_C) = \lambda_C.$$

It follows that we must have

$$\sum_{|B| \leq |S|-1} \mu_B \widetilde{qp_B} = 0.$$

Now if not all μ_C are 0 then let C be of minimal size with $\mu_C \neq 0$. Then

$$\mu_B \widetilde{qp_B}(\chi_C) = \begin{cases} 0 & B \subseteq C, B \neq C \text{ (as } \mu_B = 0) \\ 0 & B \not\subseteq C \text{ (as } p_B(\chi_C) = 0) \\ \neq 0 & B = C. \end{cases}$$

So

$$0 = \sum_{|B| \leq |S|-1} \mu_B \widetilde{qp_B}(\chi_C) = \mu_C \widetilde{qp_C}(\chi_C) \neq 0,$$

which gives a contradiction. Thus the claim holds. ■

3.5 Borsuk's Conjecture

In 1933, Borsuk conjectured that if $K \subseteq \mathbb{R}^d$ has diameter 1 then it can be partitioned into $d+1$ sets of diameter less than 1. (It's easy to see that there are sets for which $d+1$ is necessary: consider the regular simplex.)

Borsuk's conjecture remained open until 1993, when Kahn and Kalai showed that it is false.

Theorem 30. *Let $k(d)$ be the smallest integer k such that every subset of $\mathbb{R}^d$ of diameter 1 can be partitioned into $k(d)$ sets of smaller diameter. Then there exists $c > 1$ such that*

$$k(d) \geq c^{\sqrt{d}}$$

for infinitely many d.

In fact, Kahn and Kalai proved that (with a little more work) the bound holds for all d. Surprisingly, their result uses the Modular Frankl-Wilson Theorem.

We will need a preliminary lemma.

Lemma 31. *Let p be a prime and suppose $\mathcal{A} \subseteq [4p]^{(2p)}$. Suppose there is no pair of distinct $A, B \in \mathcal{A}$ with $|A \cap B| = p$. Then $|\mathcal{A}| \leq 4\binom{4p}{p-1}$.*

Proof. For $x \in [4p]$, let $\mathcal{A}_x := \{A \in \mathcal{A} : x \in A\}$. We can choose x such that $|\mathcal{A}_x| \geq \frac{1}{2}|\mathcal{A}|$. Then, for distinct $A, B \in \mathcal{A}_x$, we have $|A \cap B| \neq 0, p, 2p$. So, for distinct $A, B \in \mathcal{A}_x$, we have

$$|A \cap B| \not\equiv 0 \bmod p.$$

On the other hand, for all $A \in \mathcal{A}_x$,

$$|A| \equiv 0 \bmod p.$$

We can therefore apply the Modular Frankl-Wilson Theorem (with $S = \{1, \ldots, p-1\}$) to get

$$|\mathcal{A}_x| \leq \sum_{i=0}^{p-1} \binom{4p}{i} \leq 2\binom{4p}{p-1},$$

since $2\binom{4p}{i} \geq \binom{4p}{i-1}$, for all $i \leq p-1$. The result follows. ■

Proof of the Kahn-Kalai Theorem. Let $d = \binom{4p}{2}$, where p is a prime. We shall construct a set $K \subseteq \mathbb{R}^d$. In fact, let

$$W = [4p]^{(2)} = E(K_{4p}),$$

so we identify $[4p]^{(2)}$ with the edges of the complete graph with vertex set $[4p]$. We will work in $\mathbb{R}^W$. Note that

- Coordinates in $\mathbb{R}^W$ are indexed by edges of K_{4p}; and
- 0-1 vectors correspond to subgraphs of K_{4p}.

For each $A \in [4p]^{(2p)}$, let

$$E_A = \{\{i,j\} \in W : |A \cap \{i,j\}| = 1\};$$

in other words E_A is the edge set of the complete bipartite graph with vertex classes A and A^c. We set

$$\mathcal{F} = \{E_A : A \in [4p]^{(2p)}\}.$$

Since $|A| = |A^c| = 2p$ and $E_A = E_{A^c}$, we have

$$|\mathcal{F}| = \frac{1}{2}\binom{4p}{2p}.$$

We identify each element E_A of $\mathcal{F}$ with the vector $v_A \in \mathbb{R}^W$ given by

$$(v_A)_e = \begin{cases} 1 & e \in E_A \\ 0 & e \notin E_A. \end{cases}$$

Let K be the set of points in $\mathbb{R}^W$ corresponding to $\mathcal{F}$.

Now for $A, B \in [4p]^{(2p)}$,

$$\begin{aligned} ||v_A - v_B||_2 &= \left(\sum_e (v_A(e) - v_B(e))^2\right)^{1/2} \\ &= (|E_A| + |E_B| - 2|E_A \cap E_B|)^{1/2}. \end{aligned}$$

So $||v_A - v_B||_2$ increases as $|E_A \cap E_B|$ decreases. It is easy to check that $|E_A \cap E_B|$ is minimal if and only if $|A \cap B| = p$.

Now suppose $L \subseteq K$ satisfies $\mathrm{diam}(L) < \mathrm{diam}(K)$. In the set $\mathcal{A} \subseteq \mathcal{F}$ corresponding to L there can be no pair A, B with $|A \cap B| = p$. So by the lemma, $|\mathcal{A}| \leq \binom{4p}{p-1}$, and so

$$|\mathcal{F}|/|\mathcal{A}| \geq \frac{1}{2}\binom{4p}{2p}\Big/\binom{4p}{p-1}.$$

For large p, an application of Stirling's formula shows that this is at least 1.7^p, which is at least $1.2^{\sqrt{d}}$. Thus if we want to partition K into sets of smaller diameter we need at least $1.2^{\sqrt{d}}$ sets. ■

Remark. A couple of people asked if I could provide a few more details for that last application of Stirling. By Example sheet 1, question 5(b), we have that $\binom{4p}{2p} = 2^{(1+o(1))4p}$ and $\binom{4p}{p-1} = 2^{(1+o(1))H(1/4)4p}$ where $H(1/4) = -(1/4)\log_2(1/4) - (3/4)\log_2(3/4) \approx 0.81$. So

$$\frac{1}{2}\binom{4p}{2p}\Big/\binom{4p}{p-1} = 2^{(1+o(1))(1-H(1/4))4p} > 2^{0.8p}.$$

Then we observe that $d = \binom{4p}{2} = 8(1+o(1))p^2$ so $p = \frac{1+o(1)}{2\sqrt{2}}\sqrt{d}$, so $2^{0.8p} > 1.2^{\sqrt{d}}$.

Chapter 4

Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field. It is an elementary fact that if $f \in \mathbb{F}[x]$ has degree t, and $S \subseteq \mathbb{F}$ has $|S| > t$ then there is $s \in S$ with $f(s) \neq 0$.

Theorem 32 (Combinatorial Nullstellensatz)**.** *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree t. Suppose that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero, where $t_1 + \cdots + t_n = t$. If $S_1, \ldots, S_n$ are subsets of $\mathbb{F}$ with $|S_i| \geq t_i + 1$ for each i then there is $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

Proof. We argue by induction on $t = \deg(f)$. If $t = 1$ then the result is trivial. So suppose $t > 1$, and $f(x) = 0$ for all $x \in S_1 \times \cdots \times S_n$. Without loss of generality, $t_1 > 0$. Choose $s_1 \in S_1$ and write f as

$$f(x) = (x_1 - s_1)q(x) + r(x),$$

where $\deg(q) = t - 1$, and q has a monomial $x_1^{t_1 - 1} x_2^{t_2} \ldots x_n^{t_n}$ with nonzero coefficient, and $r(x) \in \mathbb{F}[x_2, \ldots, x_n]$.

For any $(s_2, \ldots, s_n) \in S_2 \times \ldots S_n$ we have

$$f(s_1, \ldots, s_n) = r(s_2, \ldots, s_n)$$

and so r vanishes on $S_2 \times \cdots \times S_n$. Thus for any $s' = (s_1', \ldots, s_n') \in S_1 \times \cdots \times S_n$, we have

$$f(s') = (s_1' - s_1)q(s') + r(s') = (s_1' - s_1)q(s').$$

In particular, as $s_1' - s_1 \neq 0$ for $s_1' \in S_1 \setminus s_1$, we see that q vanishes on $(S_1 \setminus s_1) \times S_2 \times \cdots \times S_n$. But this contradicts the inductive hypothesis. ■

Let us see some applications.

How many hyperplanes we need to cover all vertices of a cube in $\mathbb{R}^n$? This is trivial: two hyperplanes will do. But what if we want to cover *all but one* vertex, and leave the last vertex uncovered? It is easy to show that n planes suffice. It turns out that this is the minimum!

Theorem 33. *Let $H_1, \ldots, H_m$ be a family of m hyperplanes in $\mathbb{R}^n$ whose union contains exactly $2^n - 1$ vertices from $\{0,1\}^n$. Then $m \geq n$.*

Proof. We may assume the uncovered vertex is $\mathbf{0}$. Work over the reals. Each hyperplane H_i is defined by an equation of form

$$\langle \mathbf{x}, \mathbf{a}_i \rangle = b_i$$

Note that $b_i \neq 0$ as $\mathbf{0} \notin H_i$. So rescaling $\mathbf{a_i}$ and b_i, we may assume H_i is given by

$$\langle \mathbf{x}, \mathbf{a_i} \rangle = 1$$

Define

$$P(\mathbf{x}) = (-1)^{m+n} \prod_{j=1}^{n} (x_j - 1) - \prod_{i=1}^{m} (\langle \mathbf{x}, \mathbf{a_i} \rangle - 1)$$

If $m < n$ then the coefficient of $x_1 \ldots x_n$ is nonzero, so by the Combinatorial Nullstellensatz there is $\mathbf{s} \in \{0,1\} \times \cdots \times \{0,1\}$ such that $P(\mathbf{s}) \neq 0$. But if $\mathbf{s} \neq \mathbf{0}$ then both parts of $P(\mathbf{x})$ are 0; while if $\mathbf{s} = \mathbf{0}$ then we again have $P(\mathbf{s}) = 0$. This gives a contradiction. ■

This is essentially the last point that we reached in lectures. In the next section are two more well-known applications of the Nullstellensatz, which are nice to see but do not form part of the examinable material this year.

Non-examinable applications

Given sets A, B in an abelian group, we write

$$A + B = \{a + b : a \in A, b \in B\}.$$

If $A, B \subseteq \mathbb{Z}$ then $|A+B| \geq |A| + |B| - 1$ (exercise). The same thing happens in $\mathbb{Z}_p$.

Theorem 34 (Cauchy-Davenport)**.** *If p is a prime and $A, B \subseteq \mathbb{Z}_p$ then*

$$|A+B| \geq \min\{p, |A|+|B|-1\}$$

Proof. Work over $\mathbb{Z}_p$. Suppose first that $|A|+|B| > p$. Then for every $c \in \mathbb{Z}_p$, the sets $A, c-B$ must have a common element, and so there is a solution to $x+y=c$ with $x \in A, y \in B$.

Now suppose $|A|+|B| \leq p$ and $|A+B| \leq |A|+|B|-2$. Pick $C \supset A+B$ with $|C| = |A|+|B|-2$, and set

$$f(x,y) = \prod_{c \in C}(x+y-c)$$

This has degree $|A|+|B|-2$, and the coefficient of $x^{|A|-1|}y^{|B|-1}$ is

$$\binom{|A|+|B|-2}{|A|-1},$$

which is nonzero in $\mathbb{Z}_p$.

But now, applying the Combinatorial Nullstellensatz with $S_x = A$ and $S_y = B$, we see that there must be $(a,b) \in A \times B$ with $f(a,b) \neq 0$, which implies that $a+b \notin C$, a contradiction. ■

Let's prove a variant of Cauchy-Davenport. For sets A, B define

$$A \widehat{+} B = \{a+b : a \in A, b \in B, a \neq b\}$$

Note that if $A = B = \{0, \ldots, a-1\}$ then $A \widehat{+} B = \{1, \ldots, 2a-3\}$, so $|A \widehat{+} B| = |A|+|B|-3$.

Theorem 35. *Let p be prime and $A, B \subseteq \mathbb{F}_p$ be nonempty. Then*

$$|A \widehat{+} B| \geq \min\{p, |A|+|B|-3\}$$

Proof. We will prove the stronger result that $|A \widehat{+} B| \geq \min\{p, |A|+|B|-3\}$, and if $|A| \neq |B|$ then $|A \widehat{+} B| \geq \min\{p, |A|+|B|-2\}$.

We work over $\mathbb{F}_p$. Note first that if $|A|+|B| \geq p+2$ then for any $c \in \mathbb{Z}_p$ the set $A \cap (c-B)$ has size at least 2. So there are two pairs $(a,b) \in A \times B$ with $a+b=c$, and one of these must have $a \neq b$.

Now if $|A|=1$ or $|B|=1$ the result is immediate. Also, if $|A|=|B|$ then we may delete any element from A and use the stronger result. So we may assume that $|A|+|B| \leq p+1$ and $|A| \neq |B|$.

Choose C such that $|C| = |A| + |B| - 3$ and $A \widehat{+} B \subseteq C$. Define

$$P(x, y) = (x - y) \prod_{c \in C} (x + y - c).$$

Then P has degree $|A| + |B| - 2$ and vanishes on $A \times B$. On the other hand, the coefficient of $x^{|A|-1} y^{|B|-1}$ is

$$\binom{|A| + |B| - 3}{|A| - 2} - \binom{|A| + |B| - 3}{|A| - 1} = \frac{(|A| + |B| - 3)!}{(|A| - 1)!(|B| - 1)!} \big((|A| - 1) - (|B| - 1) \big)$$

which is nonzero in $\mathbb{F}_p$ (exercise), giving a contradiction. ■