Part III – Combinatorics (Incomplete)

Based on lectures by Prof Béla Bollobás

Notes taken by Yaël Dillies

Michaelmas 2023

Contents

0 Introduction

For a finite set A, we write its cardinality $|A|$.

For a graph $G = (V, E)$ and $A, B \subseteq V$, we denote $\Gamma(A) = \{b | \exists a \in A, a \sim b\}$ the set of neighbors of A and $e(A, B)$ the number of edges between A and B.

1 Basic Results

1.1 Chains, Antichains and Scattered Sets of Vectors

Lecture 1

During WW2, Littlewood and Offord were interested in roots of polynomials with random coefficients. They came up with the following neat theorem.

Theorem (Littlewood-Offord, 1943)**.** If $z_1, \dots, z_n \in \mathbb{C}$ with $|z_i| \geq 1$, then, for any disk D of radius r,

$$\#\{\varepsilon \in \{-1,1\}^n | \sum_i \varepsilon_i z_i \in D\} \leq c \log n \frac{2^n}{\sqrt{n}}$$

for some constant c depending only on r.

Upon seeing this theorem, Erdős immediately knew he could drastically improve the bound if the z_i were real.

Theorem (Erdős, 1945)**.** If $x_1, \dots, x_n \in \mathbb{R}$, $|x_i| \geq 1$, then, for any interval I of length 2,

$$\#\{\varepsilon \in \{-1,1\}^n | \sum_i \varepsilon_i z_i \in I\} \leq \binom{n}{\frac{n}{2}}$$

This is best possible, as we see by taking $x_1 = \cdots = x_n = 1$.

Let G be a bipartite graph with parts U and W. A **complete matching** from U to W is an injective function $f : U \to W$ such that $\forall u \in U, u \sim f(u)$.
If G has a complete matching, then certainly $|A| \leq |\Gamma(A)|$. Surprisingly, this is enough.

Theorem 1.1 (Kőnig-Egerváry-Hall Theorem, Hall's Marriage Theorem)**.**

$$G \text{ has a complete matching} \iff \forall A \subseteq U, |A| \leq |\Gamma(A)|$$

Proof. Exercise □

Let $\mathcal{F} = (F_1, \dots, F_m)$ where the F_i are finite sets. We say $a_1, \dots, a_m$ is a **set of distinct representatives**, aka **SDR** if they are distinct and $\forall i, a_i \in F_i$. Certainly, if $\mathcal{F}$ has SDR, then $|I| \leq \left|\bigcup_{i \in I} F_i\right|$ for all $I \subseteq [m]$.

Theorem 1.2.

$$\mathcal{F} \text{ is a SDR} \iff \forall I \subseteq [m], |I| \leq \left|\bigcup_{i \in I} F_i\right|$$

Proof. Define a bipartite graph G with parts $[m]$ and $\bigcup_i F_i$ by $i \sim a \iff a \in F_i$. For all $I \subseteq [m]$, $|I| \leq \left|\bigcup_{i \in I} F_i\right| = |\Gamma(I)|$, so Theorem 1.1 applies. □

Theorem 1.3. If G is a bipartite graph with parts U, W such that $\deg(u) \geq \deg(w)$ for all $u \in U, w \in W$, then there is a complete matching from U to W.

Proof. Find d such that $\deg(u) \geq d \geq \deg(w)$ for all $u \in U, w \in W$. For all $A \subseteq U$, we have

$$d\,|A| \leq e(A, \Gamma(A)) \leq d\,|\Gamma(A)|$$

Hence $|A| \leq |\Gamma(A)|$. We're done by Theorem 1.1. □

For $A \subseteq U, B \subseteq W$, define $w(A) = \frac{|A|}{|U|}, w(B) = \frac{|B|}{|W|}$.

Say a bipartite graph G with parts U, W is (k, ℓ)-**biregular** if $\deg(u) = k, \deg(w) = \ell$ for all $u \in U, w \in W$.

Lemma 1.4. If G is biregular with parts U, W and $A \subseteq U$, then $w(A) \leq w(\Gamma(A))$.

Proof. First, $k\,|U| = e(G) = \ell\,|W|$. Second,

$$k\,|A| = e(A, \Gamma(A)) \leq \ell\,|\Gamma(A)|$$

Dividing the inequality by the equality gives the result. □

Lecture 2

Corollary 1.5. Let G be a (k, ℓ)-biregular graph with parts U, W. If $k \geq \ell$ (or equivalently $|U| \leq |W|$), then there is a complete matching from U to W.

Corollary 1.6. If $\left|s - \frac{n}{2}\right| \leq \left|r - \frac{n}{2}\right|$, then there exists an injection $f : X^{(r)} \hookrightarrow X^{(s)}$ such that either

- $r \leq s$ and $A \subseteq f(A)$ for all $A \in X^{(r)}$
- $s \leq r$ and $f(A) \subseteq A$ for all $A \in X^{(r)}$

Theorem 1.7 (Sperner, 1928)**.** Let $\mathcal{A} \subseteq \mathcal{P}(X)$ be an antichain. Then $|\mathcal{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$

Proof. A chain and an antichain can intersect in at most one element. If we manage to partition $\mathcal{P}(X)$ into $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ chains, we win.
But we can repeatedly use Corollary 1.6 to construct matchings $X^{(0)}$ to $X^{(1)}$, $X^{(1)}$ to $X^{(2)}$, ..., $X^{(\lceil \frac{n}{2} \rceil - 1)}$ to $X^{(\lceil \frac{n}{2} \rceil)}$ and $X^{(n)}$ to $X^{(n-1)}$, $X^{(n-1)}$ to $X^{(n-2)}$, ..., $X^{(\lfloor \frac{n}{2} \rfloor + 1)}$ to $X^{(\lfloor \frac{n}{2} \rfloor)}$, then "stack" the matchings together to make chains (if an element of the middle layer). Each chain goes through $X^{(\lfloor fracn2 \rfloor)}$, so we made $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. □

We can now understand the observation of Erdős (1945) about Littlewood-Offord (1943).

Corollary 1.8. Let $x_1, \ldots, x_n \in \mathbb{R}$ be such that $|x_i| \geq 1$. Then at most $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ of the sums $\sum_i \varepsilon_i x_i$, $\varepsilon_i = \pm 1$ fall into the interior of an interval I of length 2.

Proof. WLOG $\forall i, x_i \geq 1$. Set $F_\varepsilon = \{i | \varepsilon_i = 1\}$. $\{F\varepsilon | \sum_i \varepsilon_i x_i \in I\}$ is an antichain (if $F_\varepsilon \subsetneq F_{\varepsilon'}$, then $\sum_i \varepsilon'_i x_i \geq \sum_i \varepsilon_i x_i + 2$, so both sums can't lie in I). □

Definition. A partial order P is **graded** if it has a partition P_i such that

- if $x < y$, $x \in P_i$, $y \in P_j$, then $i < j$ (in particular each P_i is an antichain)
- if $x < y$, $x \in P_i$, $y \in P_j$, $i + 2 \leq j$, then there exists z such that $x < z < y$.

For $a \in P$, we call the unique i for which $a \in P_i$ the **grade** or **rank** of a.
A graded order is **regular** if for every i there exists p_i such that every $x \in P_i$ is less than exactly p_k elements of P_{i+1}.
For $A \subseteq P$, define $A_i = A \cap P_i$ and $w(A) = \sum_i \frac{|A_i|}{|P_i|}$.

TODO: Insert picture

Theorem 1.9. Let A be an antichain in a connected regular graded order P. Then $w(A) \leq 1$.

Proof. The regularity condition means that for each i the bipartite graph G_i with parts P_{i-1}, P_i and $x \sim y \iff x < y$ is (p_{i-1}, q)-biregular. In particular, $w(A_i) \leq w(\Gamma_{G_i}(A_i))$. Now, write r the maximal rank of an element of A and define

$$B := A \setminus A_r \cup \Gamma_{G_r}(A_r)$$

The fact that A is an antichain means that B is an antichain as well and $\Gamma_{G_r}(A_r)$ is disjoint from A_{r-1}. Hence

$$\begin{aligned} w(A) &= w(A_r) + w(A_{r-1}) + \sum_{i<r-1} w(A_i) \\ &\leq w(\Gamma_{G_r}(A_r)) + w(A_{r-1}) + \sum_{i<r-1} w(A_i) \\ &= w(B_{r-1}) + \sum_{i<r-1} w(B_i) \\ &= w(B) \end{aligned}$$

We therefore have decreased the maximal rank without decreasing the weight. We can repeat the process until the antichain is contained in some P_i, in which case its weight is clearly at most 1. □

Lecture 3

Consider maximal chains in our regular graded order. Say there are M of them. Each $x \in P_h$ lies in the same number of chains $m(x)$, namely $\frac{m}{|P_h|}$.

Second proof. No two elements of A lie in the same maximal chain. Hence

$$M \geq \sum_{x \in A} m(x) = \sum_{x \in A} \frac{M}{\left|P_{\mathrm{rank}(x)}\right|} = Mw(A)$$

□

The following is a corollary of the above, but we provide a proof using Katona's circle method.

Theorem 1.10 (Lubell-Yamamoto-Meshalkin Inequality)**.** If $\mathcal{A} \subseteq 2^{[n]}$ is an antichain, then $\sum_{A \in \mathcal{A}} \binom{n}{|A|}^{-1} \leq 1$

Proof. We say that $A \in 2^{[n]}$ is **contained** in a permutation π if $A = \{\pi_1, \ldots, \pi_{|A|}\}$. Every permutation contains at most one element of $\mathcal{A}$ and every $A \in \mathcal{A}$ is contained in $|A|!(n - |A|)!$ permutations. □

We say a chain $C_i \subseteq C_{i+1} \subseteq \cdots \subseteq$ is **symmetric** if $|C_j| = j$ for all j.

Example. $\{1\} \subseteq \{1, 4\} \subseteq \{1, 3, 4\} \subseteq \{1, 3, 4, 6\} \subseteq \{1, 3, 4, 5, 6\}$ and $\{2, 4, 5\}$ are symmetric chains in $2^{[6]}$. $\{2, 5, 6\} \subseteq \{2, 4, 5, 6\}$ is a symmetric in $2^{[7]}$ but not in any other $2^{[n]}$.

Theorem 1.11 (Partition into Symmetric Chains)**.** Every finite powerset can be partitioned into symmetric chains.

Proof. Induction on n:

- $\{\{\}\}$ is a PSC for $n = 0$.
- Assume we have a PSC for n. For every chain $\mathcal{C} = \{C_i, \ldots, C_{n-i}\}$ in our PSC for n, add the following two chains to our PSC for $n+1$:

$$\mathcal{C}' = \{C_i, \ldots, C_{n-i}, C_{n-i} \cup \{n\}\}$$
$$\mathcal{C}'' = \{C_i \cup \{n\}, \ldots, C_{n-i-1} \cup \{n\}\}$$

  TODO: Insert figure

□

The number of symmetric chains of length $n+1-2i$ in a PSC is

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

Theorem 1.12. Let $x_1, \ldots, x_n$ be vectors of norm at least 1 a normed space. For $A \subseteq [n]$, set $x_A = \sum_{i \in A} x_i$. Let $\mathcal{A} \subseteq 2^{[n]}$ such that

$$\forall A, B \in \mathcal{A}, \|x_A - x_B\| < 1$$

Then $\mathcal{A} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Proof. Call $\mathcal{B} \subseteq 2^{[n]}$ **sparse** or **scattered** if $\forall A, B, \mathcal{B}, A \neq B, \|x_A - x_B\| \geq 1$. $\mathcal{A}$ intersects every sparse family in at most one set, so we would be done if there existed a partition of $2^{[n]}$ into $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ sparse chains. This is the next theorem. □

Lecture 4

Theorem 1.13 (Kleitman)**.** $2^{[n]}$ has a partition into $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ sparse chains.

Proof. Induction on n:

- $\{\{\}\}$ is a sparse partition for $n = 0$.
- Assume we have a sparse partition for n. Let f be a support functional at x_n ($\forall x, f(x) \leq \|x\|$, with equality if $x = x_n$). For every sparse family $\mathcal{D} = \{D_1, \ldots, D_k\}$ in our sparse partition for n, find i maximising $f(x_{D_i})$ and add the following two sparse families to our sparse partition for $n+1$:

$$\mathcal{D}' = \mathcal{D} \cup \{D_i \cup \{n\}\}$$
$$\mathcal{D}'' = \{D_j \cup \{n\} | j \neq i\}$$

  $\mathcal{D}''$ is clearly sparse. $\mathcal{D}'$ is also sparse because for all $D \in \mathcal{D}$

$$\begin{aligned} \left\|x_{D_i \cup \{n\}} - x_D\right\| &= \|x_{D_i} + x_n - x_D\| \\ &\geq f(x_{D_i} + x_n - x_D) \\ &= f(x_{D_i}) - f(x_D) + \|x_n\| \\ &\geq 1 \end{aligned}$$

  The number of sparse partitions of length $n+1-2i$ is again $\binom{n}{i} - \binom{n}{i-1}$.

□

1.2 Around the Erdős-Ko-Rado theorem

Erdős-Ko-Rado says that if $\mathcal{A} \subseteq X^{(r)}$ is intersecting, then $|\mathcal{A}| \leq \binom{n-1}{r-1}$.

Lecture 5

Definition (Katona's circle method)**.** We consider a cyclic order on X, namely an equivalence $\pi : [n] \simeq X$, where $|X| = n$ and π, π' are identified if they differ by a shift. An **arc** is a set of consecutive elements, namely a set of the form $\{\pi_a, \dots, \pi_b\}$ (with wrap-around allowed).

TODO: Insert picture

For π a cyclic order and $\mathcal{A}$ a set family, we write $\mathcal{A}_\pi$ the π-arcs of $\mathcal{A}$.

There are $(n-1)!$ cyclic orders. Every cyclic order π supports exactly n arcs of size r, and every set A of size r is an arc of exactly $r!(n-r)!$ cyclic orders.

Lemma 1.14. Let $\mathcal{A} \subseteq X^{(\leq \frac{n}{2})}$ be an intersecting antichain of arcs in a cyclic order π. then

$$|\mathcal{A}| \leq \min_{A \in \mathcal{A}} |A|$$

Proof. WLOG $\pi_1, \dots, \pi_k$ is the shortest arc, $\mathcal{A}$ is nonempty and $k \geq 2$. For every $i \in [k]$, at most one arc separates x_i and x_{i+1}. Therefore $|\mathcal{A}| - 1 \leq k - 1$, namely $|\mathcal{A}| \leq k$. □

Theorem 1.15. Let $\mathcal{A} \subseteq X^{(\leq \frac{n}{2})}$ be an intersecting antichain. Then

$$\sum_{A \in \mathcal{A}} \binom{n-1}{|A|-1}^{-1} \leq 1$$

Proof. Consider the bipartite graph with parts $\mathcal{A}$ and the cyclic orders of X. Connect $A \in \mathcal{A}$ to a cyclic order π if A is a π-arc. Make the weight of the edge be $|A|^{-1}$. Then every $A \in \mathcal{A}$ has total weight $(|A|-1)!(n-|A|)!$ while each π has weight

$$\sum_{A in \mathcal{A}_\pi} |A|^{-1} \leq \frac{|\mathcal{A}_\pi|}{\min_{A \in \mathcal{A}} |A|} \leq 1$$

by Lemma 1.14. So

$$\sum_{A \in \mathcal{A}} (|A|-1)!(n-|A|)! \leq (n-1)!$$

□

Theorem 1.16. Let $r \leq \frac{n}{2}$ and $\mathcal{A} \subseteq X^{(\leq r)}$ be an intersecting antichain. Then $|\mathcal{A}| \leq \binom{n-1}{r-1}$.

Proof.

$$\frac{|\mathcal{A}|}{\binom{n-1}{r-1}} \leq \sum_{A \in \mathcal{A}} \binom{n-1}{|A|-1}^{-1} \leq 1$$

□

$\mathcal{A}$ being intersecting is the same as $|A \cap B| \geq 1$ for all $A, B \in \mathcal{A}$. We say $\mathcal{A}$ is **ℓ-intersecting** if $|A \cap B| \geq \ell$ for all $A, B \in \mathcal{A}$.

We know the size of an intersecting antichain in $X^{(r)}$ is maximised by taking all sets of size r containing a fixed element x. We would hope that the size of an ℓ-intersecting antichain in $X^{(r)}$ is maximised by taking all sets of size r containing a fixed set R of size ℓ (which would give $\binom{n-\ell}{r-\ell}$ as an upper bound). This is however not true for small n. The reason is that it might be better to make R a bit bigger than ℓ and in return ask for the sets in the antichain to intersect R into a bit more than ℓ elements (rather than containing it).

Precisely, pick your favorite number t and your favorite set R of size $\ell + 2t$. Now define

$$\mathcal{F}_t = \{A \in X^{(r)} \mid |A \cap R| \geq \ell + t\}$$

For every $A, B \in \mathcal{F}$,

$$|A \cap B| \geq |A \cap B \cap R| = |A \cap R| + |B \cap R| - |(A \cup B) \cap R| \geq 2\ell + 2t - (\ell + 2t) = \ell$$

So $\mathcal{F}_t$ is ℓ-intersecting. On the other hand,

$$|F_t| > \binom{n-\ell}{r-\ell}$$

for values of n on the same order of magnitude as r and ℓ.

Theorem 1.17. Let $1 \leq \ell < r$ be fixed. If n is large enough and $\mathcal{A} \subseteq X^{(r)}$ is an ℓ-intersecting family, then $|\mathcal{A}| \leq \binom{n-\ell}{r-\ell}$.

Proof. We may assume $\mathcal{A}$ is maximal. In particular, find $A_1, A_2 \in \mathcal{A}$ such that

$$|A_1 \cap A_2| = \ell$$

If $\left|\bigcap_{A \in \mathcal{A}} A\right| \geq \ell$, we're done. So find some $A_3 \in \mathcal{A}$ such that

$$|A_1 \cap A_2 \cap A_3| < \ell$$

Set $U = A_1 \cup A_2 \cup A_3$. $|U| \leq 3r$ and every element of $\mathcal{A}$ intersects U in at least $\ell + 1$ elements. Hence

$$|\mathcal{A}| \leq \binom{3r}{\ell+1}\binom{n}{r-(\ell+1)} \leq \binom{n-\ell}{r-\ell}$$

for large enough n. □

Lecture 6

What if $2r \geq n$ and $\mathcal{F} \subseteq X^{(r)}$ is such that $A \cup B \neq X$ for all $A, B \in \mathcal{F}$? This is just Erdős-Ko-Rado again by taking complements: $\{A^c \mid A \in \mathcal{F}\} \subseteq X^{(n-r)}$ is an intersecting antichain with $2(n-r) \leq n$, so

$$|\mathcal{F}| = |\{A^c \mid A \in \mathcal{F}\}| \leq \binom{n-1}{(n-r)-1} = \binom{n-1}{r}$$

What happens now if $kr \geq n$ and no k sets in $\mathcal{F}$ have union X? For $k = 2$, this is Erdős-Ko-Rado. We can take $\mathcal{F} = (\{1\}^c)^{(r)}$ to achieve

$$|\mathcal{F}| \leq \binom{n-1}{r}$$

Theorem 1.18 (Frankl)**.** Let k, r, n be such that $n \leq kr$ and $\mathcal{F} \subseteq X^{(r)}$ be such that no union of k sets in $\mathcal{F}$ is X. then

$$|\mathcal{F}| \leq \binom{n-1}{r}$$

This bound is sharp.

Proof. Every $F \in \mathcal{F}$ is an arc in exactly $r!(n-r)!$ cyclic orders. If we knew that each cyclic order supports at most $n-r$ elements of $\mathcal{F}$, we would get

$$|\mathcal{F}|\, n!(n-r)! = \#\{(f, \pi) \mid f \in \mathcal{F}_\pi\} \leq (n-1)!(n-r)$$

namely $|\mathcal{F}| \leq \binom{n-1}{r}$. So let's prove that.
Assume π is a cyclic order. WLOG, assume $[\![n-r+1, n]\!] \in \mathcal{F}$. Define

$$K = \{\text{endpoint of } F \mid F \in \mathcal{F}_\pi\} \cup [\![n+1, kr]\!]$$

For each $0 < j \leq r$, we know that $\{j, j+k, \ldots, j+(r-1)k\} \not\subseteq K$ as otherwise the corresponding arcs would cover X. Hence

$$|\mathcal{F}_\pi| = |K| + n - kr \leq (k-1)r + n - kr = n - r$$

□

Corollary 1.19. Let k, r, n be such that $r \leq \frac{k-1}{k} n$ and $\mathcal{A} \subseteq X^{(r)}$ be a k-intersecting family. Then $|\mathcal{A}| \leq \binom{n-1}{r-1}$.

Proof. Set $\mathcal{F} = \{A^c \mid A \in \mathcal{A}\}$. Then Theorem 1.18 applies and gives

$$|\mathcal{A}| = |\mathcal{F}| \leq \binom{n-1}{n-r} = \binom{n-1}{r-1}$$

□

1.3 The Vertex Isoperimetric Problem in the Cube and the Kruskal-Katona Theorem

We are interested in the isoperimetric problem in the discrete cube.

Define Q_n to be the graph with vertices $2^{[n]}$ and

$$x \sim y \iff |x \triangle y| = 1$$

$|x \triangle y|$ is more generally the distance between x and y in Q_n. Given $A \subseteq Q_n$, write

$$N(A) = A \cup \Gamma(A) = \{x \in Q_n \mid d(x, A) \leq 1\}$$

the **neighborhood** of A.

Question. How large is $|N(A)|$ when $|A| = \alpha$?

Our life will be made incredibly easier here by the fact that the extremal A are *nested*. That is to say we will find $I_0 \subseteq I_1 \subseteq \dots$ such that $|I_\alpha| = \alpha$ and $|N(A)| \geq |N(I_\alpha)|$ for all A of size α.

This is to compare to the usual isoperimetric inequality in $\mathbb{R}^d$, where the extremal sets (ie balls) are also nested. In both cases, this means we can make any set look more and more like an extremal set by *thickening* or *compressing* it.

TODO: Insert potatoes

Lecture 7

A nested sequence of sets is equivalent to the sequence of initial segments of some order. What order do we want here?

For $x, y \in X^{(r)}$, say x is less than y in the **lexicographic order**, written $x \overset{\text{lex}}{<} y$, if $\min(x \triangle y) \in x$. The slogan is "Keep small elements small". For $n = 5, r = 3$, the lex order is

$$123 < 124 < 125 < 134 < 135 < 145 < 234 < 235 < 245 < 345$$

We extend the lex orders on the $X^{(r)}$ to the **simplicial order** on Q_n by

$$x < y \iff |x| < |y| \text{ or } |x| = |y| \text{ and } x \overset{\text{lex}}{<} y$$

The simplicial order on Q_5 starts

$$\varnothing, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, \dots$$

Definition. For $A \subseteq Q_n$, define

$$A_+^{(i)} = \{x \mid i \notin x, x \cup \{i\} \in A\}$$
$$A_-^{(i)} = \{x \mid i \notin x, x \in A\}$$

The i**-compression** of A is the set B such that $B_\pm^{(i)}$ are the initial segments in the simplicial order with $\left|B_\pm^{(i)}\right| = \left|A_\pm^{(i)}\right|$.

Lemma 1.20.

$$|N(C_i(A))| \leq |N(A)|$$

Proof. Write $B = C_i(A)$.

$$\begin{aligned}
|N(B)| &= \left|N(B)^{(i)}_+\right| + \left|N(B)^{(i)}_-\right| \\
&= \left|N\left(B^{(i)}_+\right) \cup B^{(i)}_-\right| + \left|N\left(B^{(i)}_-\right) \cup B^{(i)}_+\right| \\
&= \max\left(\left|N\left(B^{(i)}_+\right)\right|, \left|B^{(i)}_-\right|\right) + \max\left(\left|N\left(B^{(i)}_-\right)\right|, \left|B^{(i)}_+\right|\right) \text{ by nestedness} \\
&= \max\left(\left|N\left(C_i\left(A^{(i)}_+\right)\right)\right|, \left|A^{(i)}_-\right|\right) + \max\left(\left|N\left(C_i\left(A^{(i)}_-\right)\right)\right|, \left|A^{(i)}_+\right|\right) \\
&\leq \max\left(\left|N\left(A^{(i)}_+\right)\right|, \left|A^{(i)}_-\right|\right) + \max\left(\left|N\left(A^{(i)}_-\right)\right|, \left|A^{(i)}_+\right|\right) \\
&= \left|N(A)^{(i)}_+\right| + \left|N(A)^{(i)}_-\right| \\
&= |N(A)|
\end{aligned}$$

□

Lemma 1.21. For every $A \subseteq Q_n$, there exists a **compressed set** B (namely $C_i(B) = B$ for all i) such that $|B| = |A|$ and $|N(B)| \leq |N(A)|$.

Proof. Repeatedly i-compress A for various i. This must terminate since i-compressing reduces A in the lex order on $Q_n^{(|A|)}$. (Warning, we're taking the lex order of the simplicial order here!) □

Lecture 8

We would be extremely lucky if the only compressed sets were initial segments of the simplicial order. We are merely incredibly lucky and there is exactly one exceptional set which is compressed but not an initial segment.

Define the **half-space** $H_n = I_{2^{n-1}}$, and the **exceptional set** $E_n = H_n \setminus \{\max H_n\} \cup \{\min H_n^c\}$ which is H_n with its last element $\max H_n$ replaced by $\min H_n^c$, the next element in the simplex order (which also happens to be the complement of $\max H_n$).

- If $n = 2k+1$, then $H_n = X^{(\leq k)}$ and
$$E_n = H_n \setminus \{\{k+2, \dots, 2k+1\}\} \cup \{\{1, \dots, k+1\}\}$$
- If $n = 2k$, then $H_n = X^{(\leq k-1)} \cup \{x \cup \{1\} \mid x \in (\{1\}^c)^{(k-1)}\}$ and
$$E_n = H_n \setminus \{\{1, k+2, \dots, 2k\}\} \cup \{\{2, \dots, k+1\}\}$$

In both cases, E_n is compressed but not an initial segment. We also notice that the element we remove is the complement of the element we add.

Lemma 1.22. If $A \subseteq Q_n$ is compressed but not an initial segment, then $A = E_n$.

Proof. For every $x \notin A, y \in A$ such that $x < y$, we see that $i \in x \iff i \notin x$ for all i as otherwise A wouldn't be i-compressed. Hence x and y are complements. In particular, such x and y are unique. Since A is not an initial segment, such x and y exist. So

$$A = \text{initial segment} \setminus \{\text{last}\} \cup \{\text{next}\}$$

where $\text{last}^c = \text{next}$. But there is only one element which follows its complement in the lex order. So $A = E_n$ as claimed. □

Remark.

$$|N(E_n)| = |N(H_n)| + \left\lfloor \frac{n-1}{2} \right\rfloor$$

Theorem 1.23 (Vertex Isoperimetric Inequality)**.** If $A \subseteq Q_n$, then $|N(A)| \geq \left|N(I_{|A|})\right|$.

Proof. Apply Lemmas 1.20, 1.21, 1.22. □

Definition. For $\mathcal{A} \subseteq \mathcal{P}(X)$, define the **lower shadow** of $\mathcal{A}$

$$\underline{\partial}\mathcal{A} = \{A \setminus \{a\} \mid a \in A \in \mathcal{A}\}$$

and the **upper shadow** of $\mathcal{A}$

$$\overline{\partial}\mathcal{A} = \{A \cup \{a\} \mid a \notin A \in \mathcal{A}\}$$

TODO: Insert graded potato

Question. How large is $|\mathcal{A}|$ when $\mathcal{A} \subseteq X^{(r)}$ and $|\mathcal{A}| = a$?

From Lemma 1.4, we know the bound $|\underline{\partial}\mathcal{A}| \geq \frac{r}{n-r+1}|\mathcal{A}|$, but we can do much better now that we have the vertex isoperimetric inequality. Indeed,

$$N\left(X^{(\geq r+1)} \cup \mathcal{A}\right) = X^{(\geq r)} \cup \underline{\partial}\mathcal{A}$$

and $X^{(\geq r)}$ is disjoint from $\underline{\partial}\mathcal{A}$.

TODO: Insert graded potato

Lecture 9

Recall we defined $x \overset{\text{lex}}{<} y$ to mean $\min(x \triangle y) \in x$. Define the **colexicographic order** by

$$x \overset{\text{colex}}{<} y \iff \max(x \triangle y) \in y$$

The slogan this time is "Keep big elements small". The colex order for $n = 5, r = 3$ is

$$123, 124, 134, 234, 125, 135, 235, 145, 245, 345$$

colexicographic order is dual to the lexicographic order in the sense that

$$x \overset{\text{colex}}{<} y \iff y^c \overset{\text{lex}}{<} x^c$$

Since we have proved the vertex isoperimetric inequality for the lex order, we will reuse it rather than the colex order (hence we bound $\overline{\partial}$ instead of $\underline{\partial}$). Define

$$I_\alpha^{(r)} = \text{initial segment of size } \alpha \text{ in } X^{(r)} \text{ in colex}$$
$$J_\alpha^{(r)} = \text{initial segment of size } \alpha \text{ in } X^{(r)} \text{ in lex}$$

We observe that initial segments of the simplicial order are of the form $X^{(\leq r-1)} \cup J_a^{(r)}$.

Theorem 1.24 (Kruskal 1963, Katona 1968)**.** If $\mathcal{A} \subseteq X^{(r)}$, then $|\underline{\partial}\mathcal{A}| \geq \left|\underline{\partial} I_{|\mathcal{A}|}^{(r)}\right|$.

Proof. By taking complements, we will instead prove the analogous statement for the upper shadow.

$$\begin{aligned}
\left|X^{(\leq r)}\right| + \left|\overline{\partial}\mathcal{A}\right| &= \left|X^{(\leq r)} \cup \overline{\partial}\mathcal{A}\right| \\
&= \left|N\left(X^{(\leq r-1)} \cup \mathcal{A}\right)\right| \\
&\geq \left|N\left(X^{(\leq r-1)} \cup J^{(r)}_{|\mathcal{A}|}\right)\right| \text{ by the vertex isoperimetric inequality} \\
&= \left|X^{(\leq r)} \cup \overline{\partial} J^{(r)}_{|\mathcal{A}|}\right| \\
&= \left|X^{(\leq r)}\right| + \left|\overline{\partial} J^{(r)}_{|\mathcal{A}|}\right|
\end{aligned}$$

So $\left|\overline{\partial}\mathcal{A}\right| \geq \left|\overline{\partial} J^{(r)}_{|\mathcal{A}|}\right|$. □

1.4 Sums of sets

Let G be an additive abelian group, $A, B \subseteq G$. Define

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

This is called **pointwise addition** of sets or the **Minkowski sum**.

Theorem 1.25 (Brunn-Minkowski)**.** Let $A, B \subseteq \mathbb{R}^n$ be compact sets. Then

$$|A + B|^{\frac{1}{n}} \geq |A|^{\frac{1}{n}} + |B|^{\frac{1}{n}}$$

Sketch proof. Assuming our sets are nice, eg they are finite disjoint unions of rectangles, then the question becomes combinatorial. □

If A, B are finite nonempty sets of integers, say $A = \{a_1, \ldots, a_k\}, a_1 < \cdots < a_k$ and $B = \{b_1, \ldots, b_\ell\}, b_1 < \cdots < b_\ell$, then $|A + B| \geq |A| + |B| - 1$ as

$$a_1 + b_1 < \cdots < a_1 + b_\ell < \cdots < a_k + b_\ell$$

are $k + \ell - 1$ distinct elements of $A + B$.

If A, B are finite nonempty sets in a finite abelian group G such that $|A| + |B| > |G|$, then $A + B = G$. Indeed, for every $x \in G$, we have $|x - A| + |B| > |G|$, so there must be some $b \in (x - A) \cap B$. Writing $b = x - a$ for some $a \in A$, we see that $x = a + b \in A + B$.

Lecture 10

Theorem 1.26 (Cauchy 1813, Davenport 1935)**.** If p is prime and A, B are finite nonempty sets in $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \leq p + 1$, then

$$|A + B| \geq |A| + |B| - 1$$

Proof. Apply induction on $|A|$.

- If $|A| = 1$, say $A = \{a\}$, then

$$|A + B| = |a + B| = |B| = |A| + |B| - 1$$

- If $|A| \geq 2$, we may assume $0 \in A \cap B$ and find some $a \neq 0$ such that $a \in A$. Since $a, 2a, \ldots, pa$ are all distinct elements of $\mathbb{Z}/p\mathbb{Z}$, and $|B| \leq p + 1 - |A| < p$, we can find some k such that $ka \in B$ but $(k+1)a \notin B$. Shifting B by ka, we may assume $0 \in A \cap B, a \in A\ B$, so that $1 \leq |A \cap B| < |A|$. By induction hypothesis and observing that $A \cup B + A \cap B \subseteq A + B$,

$$|A + B| \geq |A \cup B + A \cap B| \geq |A \cup B| + |A \cap B| - 1 = |A| + |B| - 1$$

□

Corollary 1.27. Let $A_1, \ldots, A_k$ be nonempty sets in $\mathbb{Z}/p\mathbb{Z}$ for p prime. Then

$$|A_1 + \cdots + A_k| \geq \min(|A_1| + \cdots + |A_k| - (k - 1), p)$$

Proof. Trivial induction on k from Theorem 1.26. □

Theorem 1.28 (Macbeath 1953, Kneser 1955)**.** Let A, B be nonempty subsets of a finite abelian group G such that $|A|+|B| \leq |G|$. Then G has a proper subgroup H such that

$$|A+B| \geq |A| + |B| - |H|$$

Proof. Induction on $|B|$.

- If $|B| = 1$, say $B = \{b\}$, then one can take $H = \{0\}$ so that

$$|A+B| = |A+b| = |A| = |A| + |B| - |H|$$

- If $|B| \geq 1$, we may assume $0 \in A \cap B$. We will have two cases. The first one is essentially trivial while the second one is the heart of the proof.

  Case 1: $A + B - B = A$
  Set $H = \langle B \rangle$.

$$|A+B| \geq |A| \geq |A| + |B| - |H|$$

  and $H \neq G$ since $A + H = A \neq G$.

  Case 2: $A + B - B \neq A$
  Find $a \in A$ and $b, c \in B$ such that $a + b - c \notin A$. Set $d = a - c$.

  Claim.

$$1 \leq |A \cap (B+d)| < |B|$$

  Proof. $b + d \in B + d$ but $b + d = a + b - c \notin A$, so $|A \cap (B+d)| < |B+d| < |B|$. On the other hand, $a = c + d \in A \cap (B+d)$. □

  Hence by the induction hypothesis, find some strict subgroup H such that

$$|A \cup (B+d) + A \cap (B+d)| \geq |A \cup (B+d)| + |A \cap (B+d)| - |H|$$

  Since $A \cup (B+d) + A \cap (B+d) \subseteq A + B + d$, we get

$$\begin{aligned} |A+B| &= |A+B+d| \\ &\geq |A \cup (B+d) + A \cap (B+d)| \\ &\geq |A \cup (B+d)| + |A \cap (B+d)| - |H| \\ &= |A| + |B+d| - |H| \\ &= |A| + |B| - |H| \end{aligned}$$

□

Lecture 11

Theorem 1.29 (Erdős-Ginzburg-Ziv, 1961)**.** Let $a_1, \ldots, a_{2n-1} \in \mathbb{Z}/n\mathbb{Z}$. Then there exists a subsequence of length n summing to 0.

Proof.
Case 1: $n = p$ **is prime**
Write $0 \leq a_1, \cdots \leq a_{2p-1} < p$. If $a_i = \ldots, a_{i+p-1}$, then their sum is 0. Otherwise, set $A_i = \{a_i, a_{i+p-1}\}$ for $i = 1, \ldots, p-1$ and $A_p = \{a_{2p-1}\}$. Then Corollary 1.27 gives us

$$|A_1 + \cdots + A_p| \geq \min(2p - 1 - (p-1), p) = p$$

Hence every $b \in \mathbb{Z}/p\mathbb{Z}$, in particular 0, is the sum of a subsequence of length p.

Case 2: n is composite
Instead of looking at sequences in $\mathbb{Z}/n\mathbb{Z}$ which sum to 0, look at sets in $\mathbb{Z}$ whose sum is divisible by n. Induction on the number of prime factors.
We know the result for n a prime, so write $n = ab$ where $a, b < n$ and assume the result for a and b. By induction hypothesis for b, repeatedly pick sets $S_1, \dots S_{2a-1}$ of size b whose sum is divisible by b. This is possible since after having picked $k \leq 2a-2$ such sets, there are $2n-1-kb \geq 2n-1-(2a-2)b = 2b-1$ elements left. Now, apply the induction hypothesis for a on

$$\frac{S_1}{b}, \cdots + \frac{S_{2a+1}}{b}$$

to find $i_1, \dots, i_a$ such that

$$\frac{S_{i_1}}{b} + \cdots + \frac{S_{i_a}}{b}$$

is divisible by a. But then $S_{i_1} + \cdots + S_{i_a}$ is divisible by n. □

Remark. This is sharp since no subsequence of length n sums to 0 in

$$\underbrace{0, \dots, 0}_{n-1}, \underbrace{1, \dots, 1}_{n-1}$$

2 Polynomials in Combinatorics

2.1 Alon's Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, sometimes algebraically closed, often finite. Write

$$\mathbb{F}[X] = \mathbb{F}[X_1, \dots, X_n]$$

Theorem (Hilbert's Nullstellensatz)**.** Let $\mathbb{F}$ be an algebraically closed field and I be an ideal of $\mathbb{F}[X]$. Write

$$V(I) = \{x \in \mathbb{F}^n \mid \forall f \in I, f(x) = 0\}$$

If $f \in \mathbb{F}[X]$ vanishes on $V(I)$ then $f^k \in I$ for some k.

For finitely generated ideals, we have two versions.

Theorem (Weak version of Hilbert's Nullstellensatz for finitely generated ideals)**.** Let $f_1, \dots, f_m \in \mathbb{F}[X]$ be polynomials with no common zeroes. Then

$$\langle f_1, \dots, f_n \rangle = \mathbb{F}[X]$$

Theorem (Strong version of Hilbert's Nullstellensatz for finitely generated ideals)**.** Let $f, f_1, \dots, f_m \in \mathbb{F}[X]$. If f vanishes on $V(\langle f_1, \dots, f_m \rangle)$, then $f^k \in I$ for some k, ie $f^k = g_1 f_1 + \cdots + g_m f_m$ for some $g_1, \dots, g_m \in \mathbb{F}[X]$.

For some time it was thought that the strong version was harder than the weak version. But in fact they're equivalent.

Proof that weak version $\implies$ strong version. Add a variable X_0 and a polynomial $f_0 = fX_0 - 1$. By construction, $f_0, \dots, f_m$ have no common zeroes. So

$$\langle f_0, \dots, f_m \rangle = \mathbb{F}[X_0, \dots, X_n]$$

In particular, we can find $g_0, \dots, g_m \in \mathbb{F}[X_0, \dots, X_n]$ such that

$$1 = g_0(fX_0 - 1) + g_1 f_1 + \cdots + g_m f_m$$

Substituting $X_0 = \frac{1}{f}$, we get

$$1 = g_1 f_1 + \cdots + g_m f_m = \sum_{i=1}^{m} g_i \left(\frac{1}{f}, X_1, \dots, X_m \right) f_i = \frac{\sum_{i=1}^{m} h_i f_i}{f^k}$$

for some integer k and polynomials h_i, namely

$$f^k = \sum_{i=1}^{m} h_i f_i$$

□

Lecture 12

Theorem 2.1 (Alon's Combinatorial Nullstellensatz, 1995)**.** Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[X_1, \dots, x_n]$ have degree $d = \sum_{i=1}^{n} d_i$. Let $S_1, \dots, S_n \subseteq \mathbb{F}$ be such that $|S_i| > d_i$. If $X_1^{d_1} + \cdots + X_n^{d_n}$ is a monomial in the expansion of f, then f is non-zero somewhere on $S_1 \times \cdots \times S_n$.

Proof (Michałek). Note that

$$X^k = (X-t)(X^{k-1} + tX^{k-2} + \cdots + t^{k-1}) + t^k$$

Induction on d.

- Obvious for $d = 0$.
- If $d \geq 1$, say $d_1 \geq 1$, pick $s_1 \in S_1$. Then $f = (X_1 - s_1)q(X) + r(X)$ where $\deg q = d - 1$ and $r \in \mathbb{F}[X_2, \ldots, X_n]$. Assume that f vanishes on $S_1 \times \cdots \times S_n$. Then s vanishes on $\{s_1\} \times S_2 \times \cdots \times S_n$. But r does not depend on X_1, so in fact r vanishes on $S_1 \times \cdots \times S_n$. Therefore q is zero on $S_1 \setminus \{s_1\} \times \cdots \times S_n$, which contradicts the induction hypothesis.

□

Theorem 2.2 (Chevalley-Warning)**.** Let $\mathbb{F}$ be a finite field and

$$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$$

be such that $\sum_{i=1}^m \deg f_i < n$. If the f_i have a common zero, then they have another one.

Proof. Write q the order of $\mathbb{F}$. Recall that for $z \in Z$

$$z^{q-1} = \begin{cases} 0 \text{ if } z = 0 \\ 1 \text{ if } z \neq 0 \end{cases}$$

Assume (by shifting) that the common zero of the f_i is 0. Define

$$f = \prod_{i=1}^m (1 - f_i^{q-1}) + \gamma \prod_{i=1}^n \prod_{s \neq 0} (X_i - s)$$

where we choose $\gamma \neq 0$ such that $f(0) = 0$.

$$\deg f \leq \max((n-1)(q-1), n(q-1)) = n(q-1)$$

and the monomial $X_1^{q-1} \ldots X_n^{q-1}$ has coefficient $\gamma \neq 0$ in f. So the Combinatorial Nullstellensatz gives us a such that $f(a) \neq 0$. Then $a \neq 0$ and $f_1(a) = \cdots = f_m(a) = 0$. □

Theorem 2.3. Let $\mathbb{F}$ be a finite field of characteristic p. Let $f \in \mathbb{F}[X_1, \ldots, X_n]$. If $\deg f < n$, then the number of zeroes of f is a multiple of p.

Proof. Denote q the order of $\mathbb{F}$.Write $N(f)$ the number of zeroes of f. We have

$$N(f) = \sum_x (1 - f(x)^{q-1}) = -\sum_x f(x)^{q-1}$$

Expand $f(x)^{q-1}$ into monomials of degree at most $(n-1)(q-1)$. □

Lecture 13

Theorem 2.4. Let $f_1, \ldots, f_m \in \mathbb{F}_p[X_1, \ldots, X_n]$ such that $\sum_i = \deg f_i < n$. Then p divides the number of common zeroes. In particular, if there is a common zero, then there is another one.

Proof. Let $z_1, \ldots, z_k \in \mathbb{F}_p^n$ be the common zeroes. Assume $p \nmid k$. Define

$$f = \underbrace{\prod_{i=1}^{m}(1 - f_i^{p-1})}_{g} - \underbrace{\sum_{j=1}^{k}\prod_{i=1}^{n}(1 - (X_i - z_{i,j})^{p-1})}_{h}$$

f is identically 0 since, for each j,

$$f(z_j) = h(z_j) - g(z_j) = 1 - 1 = 0$$

And if $z \neq z_1, \ldots, z_k$, then

$$f(z) = h(z) - g(z) = 0 - 0 = 0$$

□

2.2 Applications of Alon's Combinatorial Nullstellensatz

Theorem 2.5 (Cauchy-Davenport for primes)**.** Let p be a prime and A, B sets in $\mathbb{F}_p$ such that $1 \leq |A| \leq |B|$ and $|A| + |B| \leq p + 1$. Then

$$|A + B| \geq |A| + |B| - 1$$

Proof. Assume not. Then find C of size $|A| + |B| - 2$ such that $A + B \subseteq C$. Define $f \in \mathbb{F}_p[X, Y]$ by

$$f(X, Y) = \prod_{c \in C} (X + Y - c)$$

Then f vanishes on $A \times B$. But the coefficient of $X^{|A|-1}Y^{|B|-1}$ in f is

$$\binom{|A| + |B| - 2}{|A| - 1} \neq 0 \mod p$$

contradicting Alon's Combinatorial Nullstellensatz. □

Theorem 2.6 (Erdős-Ginzburg-Ziv for primes)**.** Let $a_1, \ldots, a_{2p-1} \in \mathbb{F}_p$. Then there exists $I \in [2p-1]^{(p)}$ such that $\sum_{i \in I} a_i = 0$.

Proof. Define $f_1 = \sum_{i=1}^{2p-1} X_i^{p-1}$, $f_2 = \sum_{i=1}^{2p-1} a_i X_i^{p-1}$. Then $\deg f_1 + \deg f_2 < 2p - 1$, so if f_1 and f_2 have a common zero, then they have another one. But $f_1(0) = f_2(0) = 0$, so find $z \neq 0$ another common zero. Define $I = \{i \mid z_i \neq 0\}$. Then

$$|I| = \sum_{i \in I} z_i^{p-1} = 0$$
$$\sum_i a_i = \sum_{i \in I} a_i z_i^{p-1} = 0$$

so $p \mid |I|$. Since $I \neq \varnothing$ ($z \neq 0$) and $|I| < 2p$, it must be that $|I| = p$. □

Define

$$A \oplus B = \{a + b \mid a \in A, b \in B, a \neq b\}$$

For A an interval in $\mathbb{Z}$, $|A \oplus A| = 2|A| - 3$. The Erdős-Heilbronn conjecture says this is best possible.

Theorem 2.7 (Alon-Nathanson-Ruzsa proof)**.** Let A, B be sets in $\mathbb{F}_p$ such that $1 \leq |A| < |B|$. Then

$$|A \oplus B| \geq |A| + |B| - 2$$

Proof. Homework. □

Lecture 14