

Part III — Combinatorics

Theorems

Based on lectures by B. Bollobas

Notes taken by Dexter Chua

Michaelmas 2017

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

What can one say about a collection of subsets of a finite set satisfying certain conditions in terms of containment, intersection and union? In the past fifty years or so, a good many fundamental results have been proved about such questions: in the course we shall present a selection of these results and their applications, with emphasis on the use of algebraic and probabilistic arguments.

The topics to be covered are likely to include the following:

- The de Bruijn–Erdős theorem and its extensions.
- The Graham–Pollak theorem and its extensions.
- The theorems of Sperner, EKR, LYMB, Katona, Frankl and Füredi.
- Isoperimetric inequalities: Kruskal–Katona, Harper, Bernstein, BTBT, and their applications.
- Correlation inequalities, including those of Harris, van den Berg and Kesten, and the Four Functions Inequality.
- Alon’s Combinatorial Nullstellensatz and its applications.
- LLLL and its applications.

Pre-requisites

The main requirement is mathematical maturity, but familiarity with the basic graph theory course in Part II would be helpful.

Contents

1	Hall's theorem	3
2	Sperner systems	4
3	The Kruskal–Katona theorem	5
4	Isoperimetric inequalities	6
5	Sum sets	7
6	Projections	8
7	Alon's combinatorial Nullstellensatz	9

1 Hall's theorem

Theorem (Hall, 1935). A bipartite graph $G = (X, Y; E)$ has a complete matching from X to Y if and only if $|\Gamma(S)| \geq |S|$ for all $S \subseteq X$.

Theorem. \mathcal{A} has a set of distinct representatives iff for all $\mathcal{B} \subseteq \mathcal{A}$, we have

$$\left| \bigcup_{B \in \mathcal{B}} B \right| \geq |\mathcal{B}|.$$

Theorem. Let $G = (X, Y; E)$ be a bipartite graph such that $d(x) \geq d(y)$ for all $x \in X$ and $y \in Y$. Then there is a complete matching from X to Y .

Corollary. If $G = (X, Y; E)$ is a (k, ℓ) -regular bipartite graph with $1 \leq \ell \leq k$, then there is a complete matching from X to Y .

Theorem. Let $G = (X, Y; E)$ be biregular and $A \subseteq X$. Then

$$\frac{|\Gamma(A)|}{|Y|} \geq \frac{|A|}{|X|}.$$

Corollary. Let $G = (X, Y; E)$ be biregular and let $|X| \leq |Y|$. Then there is a complete matching of X into Y .

Corollary. Let $1 \leq r < s \leq |X| = n$. Suppose $|\frac{n}{2} - r| \geq |\frac{n}{2} - s|$. Then there exists an injection $f : X^{(r)} \rightarrow X^{(s)}$ such that $A \subseteq f(A)$ for all $A \in X^{(r)}$.

If $|\frac{n}{2} - r| \leq |\frac{n}{2} - s|$, then there exists an injection $g : X^{(s)} \rightarrow X^{(r)}$ such that $A \supseteq g(A)$ for all $A \in X^{(s)}$.

2 Sperner systems

Theorem (Sperner, 1928). For $|X| = n$, the maximal size of an antichain in $\mathcal{P}(X)$ is $\binom{n}{\lfloor n/2 \rfloor}$, witnessed by $X^{\lfloor n/2 \rfloor}$.

Theorem (LYM inequality). Let \mathcal{A} be an antichain in $\mathcal{P}(X)$ with $|X| = n$. Then

$$\sum_{r=0}^n \frac{|\mathcal{A} \cap X^{(r)}|}{\binom{n}{r}} \leq 1.$$

In particular, $|\mathcal{A}| \leq \max_r \binom{n}{r} = \binom{n}{\lfloor n/2 \rfloor}$, as we already know.

Theorem. If P is downward expanding and A is an anti-chain, then $w(A) \leq 1$. In particular, $|A| \leq \max_i |S_i|$.

Since each S_i is an anti-chain, the largest anti-chain has size $\max_i |S_i|$.

Proposition. An anti-chain in a regular poset has weight ≤ 1 .

Theorem (Erdős, 1945). Let x_i be all real, $|x_i| \geq 1$. For $A \subseteq [n]$, let

$$x_A = \sum_{i \in A} x_i.$$

Let $\mathcal{A} \subseteq \mathcal{P}(n)$. Then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Theorem. $\mathcal{P}(n)$ has a decomposition into symmetric chain.

Theorem (Kleitman, 1970). Let x_1, x_2, \dots, x_n be vectors in a normed space with norm $\|x_i\| \geq 1$ for all i . For $A \in \mathcal{P}(n)$, we set

$$x_A = \sum_{i \in A} x_i.$$

Let $\mathcal{A} \subseteq \mathcal{P}(n)$ be such that $\|x_A - x_B\| < 1$. Then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

3 The Kruskal–Katona theorem

Lemma. We have

$$\partial C_{ij}(\mathcal{A}) \subseteq C_{ij}(\partial \mathcal{A}).$$

In particular, $|\partial C_{ij}(\mathcal{A})| \leq |\partial \mathcal{A}|$. \square

Lemma. Let $\mathcal{A} \subseteq X^{(r)}$ and $U, V \in X^{(s)}$, $U \cap V = \emptyset$. Suppose for all $u \in U$, there exists v such that \mathcal{A} is $(U \setminus \{u\}, V \setminus \{v\})$ -compressed. Then

$$\partial C_{UV}(\mathcal{A}) \subseteq C_{UV}(\partial \mathcal{A}). \quad \square$$

Lemma. $\mathcal{A} \subseteq X^{(r)}$ is an initial segment of $X^{(r)}$ in colex if and only if it is (U, V) -compressed for all U, V disjoint with $|U| = |V|$ and $\max V > \max U$.

Lemma. Given $\mathcal{A} \in X^{(r)}$, there exists $\mathcal{B} \subseteq X^{(r)}$ such that \mathcal{B} is (U, V) -compressed for all $|U| = |V|$, $U \cap V = \emptyset$, $\max V > \max U$, and moreover

$$|\mathcal{B}| = |\mathcal{A}|, |\partial \mathcal{B}| \leq |\partial \mathcal{A}|. \quad (*)$$

Theorem (Kruskal 1963, Katona 1968). Let $\mathcal{A} \subseteq X^{(r)}$, and let $\mathcal{C} \subseteq X^{(r)}$ be the initial segment with $|\mathcal{C}| = |\mathcal{A}|$. Then

$$|\partial \mathcal{A}| \geq |\partial \mathcal{C}|.$$

Theorem (Lovász, 1979). If $\mathcal{A} \subseteq X^{(r)}$ with $|\mathcal{A}| = \binom{x}{r}$ for $x \geq 1$, $x \in \mathbb{R}$, then

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

This is best possible if x is an integer.

4 Isoperimetric inequalities

Lemma. For $A \subseteq Q_n$, we have $|N(C_i(A))| \leq |N(A)|$.

Lemma. For any $A \subseteq Q_n$, there is a compressed set $B \subseteq Q_n$ such that

$$|B| = |A|, \quad |N(B)| \leq |N(A)|.$$

Lemma. For each n , there exists a unique element $z \in Q_n$ such that z^c is the successor of z .

Moreover, if $B \subseteq Q_n$ is compressed but not an initial segment, then $|B| = 2^{n-1}$ and B is obtained from taking the initial segment of size 2^{n-1} and replacing x with x^c .

Theorem (Harper, 1967). Let $A \subseteq Q^n$, and let C be the initial segment in the simplicial order with $|C| = |A|$. Then $|N(A)| \geq |N(C)|$. In particular,

$$|A| = \sum_{i=0}^r \binom{n}{i} \text{ implies } |N(A)| \geq \sum_{i=0}^{r+1} \binom{n}{i}.$$

Theorem. Let $A \subseteq Q_n$ be a subset, and let $C \subseteq Q_n$ be the initial segment of length $|A|$ in the binary order. Then $|\partial_e C| \leq |\partial_e A|$.

5 Sum sets

Theorem (Cauchy–Davenport theorem). Let A and B be non-empty subsets of \mathbb{Z}_p with p a prime, and $|A| + |B| \leq p + 1$. Then

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

Corollary. Let A_1, \dots, A_k be non-empty subsets of \mathbb{Z}_p such that

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

Then

$$|A_1 + \dots + A_k| \geq \sum_{i=1}^k |A_i| - k + 1.$$

Theorem (Erdős–Ginzburg–Ziv). Let $a_1, \dots, a_{2n-1} \in \mathbb{Z}_n$. Then there exists $I \in [2n-1]^{(n)}$ such that

$$\sum_{i \in I} a_i = 0$$

in \mathbb{Z}_n .

6 Projections

Proposition. Let K be a body in \mathbb{R}^3 . Then

$$|K|^2 \leq |K_{12}||K_{13}||K_{23}|.$$

Theorem (Uniform cover inequality). If A_1, \dots, A_r is a uniform k -cover of $[n]$, then

$$|K|^k = \prod_{i=1}^r |K_{A_i}|.$$

Theorem (Box Theorem (Bollobás, Thomason)). Given a body $K \subseteq \mathbb{R}^n$, i.e. a non-empty bounded open set, there exists a box L such that $|L| = |K|$ and $|L_A| \leq |K_A|$ for all $A \subseteq [n]$.

Lemma. There are only finitely many irreducible covers of $[n]$.

Corollary. If K is a union of translates of the unit cube, then for any (not necessarily uniform) k -cover \mathcal{A} , we have

$$|K|^k \leq \prod_{A \in \mathcal{A}} |K_A|.$$

7 Alon's combinatorial Nullstellensatz

Theorem (Alon's combinatorial Nullstellensatz). Let \mathbb{F} be a field, and let S_1, \dots, S_n be non-empty finite subsets of \mathbb{F} with $|S_i| = d_i + 1$. Let $f \in \mathbb{F}[X_1, \dots, X_n]$ have degree $d = \sum_{i=1}^n d_i$, and let the coefficient of $X_1^{d_1} \dots X_n^{d_n}$ be non-zero. Then f is not identically zero on $S = S_1 \times \dots \times S_n$.

Proposition (Division algorithm). Let $f, g \in R[X]$ with g monic. Then we can write

$$f = hg + r,$$

where $\deg h \leq \deg f - \deg g$ and $\deg r < \deg g$.

Lemma. Let $f \in R[X]$, and for $i = 1, \dots, n$, let $g_i(X_i) \in R[X_i] \subseteq R[X]$ be monic of degree $\deg g_i = \deg_{X_i} g_i = d_i$. Then there exist polynomials $h_1, \dots, h_n, r \in R[X]$ such that

$$f = \sum f_i g_i + r,$$

where

$$\begin{aligned} \deg h_i &\leq \deg f - \deg d_i & \deg_{X_i} r &\leq d_i - 1 \\ \deg_{X_i} h_i &\leq \deg_{X_i} f - d_i & \deg_{X_i} r &\leq \deg_{X_i} f \\ \deg_{X_j} h_i &\leq \deg_{X_j} f & \deg r &\leq \deg f \end{aligned}$$

for all i, j .

Lemma. Let S_1, \dots, S_n be non-empty finite subsets of a field \mathbb{F} , and let $h \in \mathbb{F}[X]$ be such that $\deg_{X_i} h < |S_i|$ for $i = 1, \dots, n$. Suppose h is identically 0 on $S = S_1 \times \dots \times S_n \subseteq \mathbb{F}^n$. Then h is the zero polynomial.

Lemma. For $i = 1, \dots, n$, let S_i be a non-empty finite subset of \mathbb{F} , and let

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s) \in \mathbb{F}[X_i] \subseteq \mathbb{F}[X].$$

Then if $f \in \mathbb{F}[X]$ is identically zero on $S = S_1 \times \dots \times S_n$, then there exists $h_i \in \mathbb{F}[X]$, $\deg h_i \leq \deg f - |S_i|$ and

$$f = \sum_{i=1}^n h_i g_i.$$

Theorem (Alon's combinatorial Nullstellensatz). Let S_1, \dots, S_n be non-empty finite subsets of \mathbb{F} with $|S_i| = d_i + 1$. Let $f \in \mathbb{F}[X]$ have degree $d = \sum_{i=1}^n d_i$, and let the coefficient of $X_1^{d_1} \dots X_n^{d_n}$ be non-zero. Then f is not identically zero on $S = S_1 \times \dots \times S_n$.

Theorem (Chevalley, 1935). Let $f_1, \dots, f_m \in \mathbb{F}_q[X_1, \dots, X_n]$ be such that

$$\sum_{i=1}^m \deg f_i < n.$$

Then the f_i cannot have exactly one common zero.

Theorem (Warning). Let $f(X) = f(X_1, \dots, X_n) \in \mathbb{F}_q[X]$ have degree $< n$. Then $N(f)$, the number of zeroes of f is a multiple of p .

Theorem (Cauchy–Davenport theorem). Let p be a prime and $A, B \subseteq \mathbb{Z}_p$ be non-empty subsets with $|A| + |B| \leq p + 1$. Then $|A + B| \geq |A| + |B| - 1$.

Theorem (Erdős–Ginzburg–Ziv). Let p be a prime and $a_1, \dots, a_{2p+1} \in \mathbb{Z}_p$. Then there exists $I \in [2p - 1]^{(p)}$ such that

$$\sum_{i \in I} a_i = 0 \in \mathbb{Z}_p.$$

Theorem. Let $A, B \subseteq \mathbb{Z}_p$ be such that $2 \leq |A| < |B|$ and $|A| + |B| \leq p + 2$. Then $A + B \geq |A| + |B| - 2$.

Corollary (Erdős–Heilbronn conjecture). If $A, B \subseteq \mathbb{Z}_p$, non-empty and $|A| + |B| \leq p + 3$, and p is a prime, then $|A + B| \geq |A| + |B| - 3$.

Theorem. If $2n + 1$ is a prime, then this can be done.

Theorem. If $b_1, \dots, b_p \in \mathbb{Z}_p$ are such that $\sum b_i = 0$, then there exists numerations a_1, \dots, a_p and b_1, \dots, b_p of the elements of \mathbb{Z}_p such that for each i , we have

$$a_i + b_i = c_i.$$