Part III — Combinatorics
Theorems with proof

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–Erdös 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

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 $S \subseteq X$.

Proof. We may assume G is edge-minimal satisfying Hall's condition. We show that G is a complete matching from X to Y. For G to be a complete matching, we need the following two properties:

(i) Every vertex in X has degree 1

(ii) Every vertex in Y has degree 0 or 1.

We first examine the second condition. Suppose $y \in Y$ is such that there exists edges $x_1 y, x_2 y \in E$. Then the minimality of G implies there are sets, $X_1, X_2 \subseteq X$ such that $x_i \in X_i$ such that $|\Gamma(X_i)| = |X_i|$ and x_i is the only neighbour of y in X_i.

Now consider the set $X_1 \cap X_2$. We know $\Gamma(X_1 \cap X_2) \subseteq \Gamma(X_1) \cap \Gamma(X_2)$. Moreover, this is strict, as y is in the RHS but not the LHS. So we have

$$\Gamma(X_1 \cap X_2) \leq |\Gamma(X_i) \cap \Gamma(X_2)| - 1.$$

But also

$$
\begin{aligned}
|X_1 \cap X_2| &\leq |\Gamma(X_1 \cap X_2)| \\
&\leq |\Gamma(X_1) \cap \Gamma(X_2)| - 1 \\
&= |\Gamma(X_1)| + |\Gamma(X_2)| - |\Gamma(X_1) \cup \Gamma(X_2)| - 1 \\
&= |X_1| + |X_2| - |\Gamma(X_1 \cup X_2)| - 1 \\
&\leq |X_1| + |X_2| - |X_1 \cup X_2| - 1 \\
&= |X_1 \cap X_2| - 1,
\end{aligned}
$$

which contradicts Hall's condition.

One then sees that the first condition is also satisfied — if $x \in X$ is a vertex, then the degree of x certainly cannot be 0, or else $|\Gamma(\{x\})| < |\{x\}|$, and we see that $d(x)$ cannot be > 1 or else we can just remove an edge from x without violating Hall's condition. $\qquad\square$

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

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

Proof. Define a bipartite graph as follows — we let $X = \mathcal{A}$, and $Y = \bigcup_{i \in [m]} A_i$. Then draw an edge from x to A_i if $x \in A_i$. Then there is a complete matching of this graph iff $\mathcal{A}$ has a set of distinct representations, and the condition in the theorem is exactly Hall's condition. So we are done by Hall's theorem. $\qquad\square$

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.

Proof. Let d be such that $d(x) \geq d \geq d(y)$ for all $x \in X$ and $y \in Y$. For $S \subseteq X$ and $T \subseteq Y$, we let $e(S, T)$ be the number of edges between S and T. Let $S \subseteq X$, and $T = \Gamma(S)$. Then we have

$$e(S, T) = \sum_{x \in S} d(x) \geq d|S|,$$

but on the other hand, we have

$$e(S, T) \leq \sum_{y \in T} d(y) \leq d|T|.$$

So we find that $|T| \geq |S|$. So Hall's condition is satisfied. $\square$

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

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

Proof. Suppose G is (k, ℓ)-regular. Then

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

Thus we have

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

On the other hand, we can count that

$$|E| = |X|k = |Y|\ell,$$

and so

$$\frac{k}{\ell} = \frac{|Y|}{|X|}.$$

So we are done. $\square$

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 $f : X^{(r)} \to X^{(s)}$ 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 $g : X^{(s)} \to X^{(r)}$ such that $A \supseteq g(A)$ for all $A \in X^{(s)}$.

Proof. Note that $|\frac{n}{2} - r| \leq |\frac{n}{2} - s|$ iff $\binom{n}{r} \geq \binom{n}{s}$. $\square$

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 $X^{\lfloor n/2 \rfloor}$.

Proof. If $\mathcal{C}$ is a chain and $\mathcal{A}$ is an antichain, then $|\mathcal{A} \cap \mathcal{C}| \leq 1$. So it suffices to partition $\mathcal{P}(X)$ into

$$m = \max_k \binom{n}{k} = \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$$

many chains.

We can do so using the injections constructed at the end of the previous section. For $i \geq \lfloor \frac{n}{2} \rfloor$, we can construct injections $f_i : X_{i-1} \to X_i$ such that $A \subseteq f_i(A)$ for all A. By chaining these together, we get m chains ending in $X^{\lfloor \frac{n}{2} \rfloor}$.
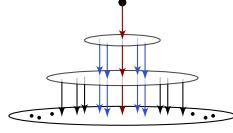
Similarly, we can partition $X^{(\leq \lfloor n/2 \rfloor)}$ into m chains with each chain ending in $X^{(\lfloor n/2 \rfloor)}$. Then glue them together. $\qquad\square$

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.

Proof. A chain $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_m$ is maximal if it has $n+1$ elements. Moreover, there are $n!$ maximal chains, since we start with the empty set and then, given C_i, we produce C_{i+1} by picking one unused element and adding it to C_i.

For every maximal chain $\mathcal{C}$, we have $|\mathcal{C} \cap \mathcal{A}| \leq 1$. Moreover, every set of k elements appears in $k!(n-k)!$ maximal chains, by a similar counting argument as above. So

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

Then the result follows. $\qquad\square$

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 $\max_i |S_i|$.

Proof. We define the *span* of A to be

$$\text{span } A = \max_{A_j \neq \emptyset} j - \min_{A_i \neq \emptyset} i.$$

We do induction on span A.

If $\operatorname{span} A = 0$, then we are done. Otherwise, let $h_i = \max_{A_j \neq 0} j$, and set $B_{h-1} = \partial A_h$. Then since A is an anti-chain, we know $A_{h-1} \cap B_{h-1} = \emptyset$.

We set $A' = A \backslash A_h \cup B_{h-1}$. This is then another anti-chain, by the transitivity of $<$. We then have

$$w(A) = w(A') + w(A_h) - w(B_{h-1}) \leq w(A') \leq 1,$$

where the first inequality uses the downward-expanding hypothesis and the second is the induction hypothesis. $\qquad\square$

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

Proof. Let M be the number of maximal chains of length $(n+1)$, and for each $x \in S_k$, let $m(x)$ be the number of maximal chains through x. Then

$$m(x) = \prod_{i=1}^{k} r_i \prod_{i=k}^{n-1} s_i.$$

So if $x, y \in S_i$, then $m(x) = m(y)$.

Now since every maximal chain passes through a unique element in S_i, for each $x \in S_i$, we have

$$M = \sum_{x \in S_i} m(x) = |S_i| m(x).$$

This gives the formula

$$m(x) = \frac{M}{|S_i|}.$$

now let A be an anti-chain. Then A meets each chain in ≤ 1 elements. So we have

$$M = \sum_{\text{maximal chains}} 1 \geq \sum_{x \in A} m(x) = \sum_{i=0}^{n} |A \cap S_i| \cdot \frac{M}{|S_i|}.$$

So it follows that

$$\sum \frac{|A \cap S_i|}{|S_i|} \leq 1. \qquad\qquad\square$$

Theorem (Erdös, 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 $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof. We claim that we may assume $x_i \geq 1$ for all i. To see this, suppose we instead had $x_1 = -2$, say. Then whether or not $i \in A$ determines whether x_A should include 0 or -2 in the sum. If we replace x_i with 2, then whether or not $i \in A$ determines whether x_A should include 0 or 2. So replacing x_i with 2 just essentially shifts all terms by 2, which doesn't affect the difference.

But if we assume that $x_i \geq 1$ for all i, then we are done, since $\mathcal{A}$ must be an anti-chain, for if $A, B \in \mathcal{A}$ and $A \subsetneq B$, then $x_B - x_A = x_{B \backslash A} \geq 1$. $\qquad\square$

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

Proof. We prove by induction. In the case $n = 1$, we simply have to take $\{\emptyset, \{1\}\}$.

Now suppose $\mathcal{P}(n-1)$ has a symmetric chain decomposition $\mathcal{C}_1 \cup \cdots \cup \mathcal{C}_t$. Given a symmetric chain

$$\mathcal{C}_j = \{C_i, C_{i+1}, \ldots, C_{n-1-i}\},$$

we obtain two chains $\mathcal{C}_j^{(0)}, \mathcal{C}_j^{(1)}$ in $\mathcal{P}(n)$ by

$$\mathcal{C}_j^{(0)} = \{C_i, C_{i+1}, \ldots, C_{n-1-i}, C_{n-1-i} \cup \{n\}\}$$
$$\mathcal{C}_j^{(1)} = \{C_i \cup \{n\}, C_{i+1} \cup \{n\}, \ldots, C_{n-2-i} \cup \{n\}\}.$$

Note that if $|\mathcal{C}_j| = 1$, then $\mathcal{C}_j^{(1)} = \emptyset$, and we drop this. Under this convention, we note that every $A \in \mathcal{P}(n)$ appears in exactly one $\mathcal{C}_j^{(\varepsilon)}$, and so we are done. $\quad\square$

Theorem (Kleitman, 1970)**.** Let $x_1, x_2, \ldots, x_n$ 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 $\|\mathcal{A}\| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof. Call $\mathcal{F} \subseteq \mathcal{P}(n)$ *sparse* if $\|x_E - x_F\| \geq 1$ for all $E, F \in \mathcal{F}$, $E \neq F$. Note that if $\mathcal{F}$ is sparse, then $|\mathcal{F} \cap \mathcal{A}| \leq 1$. So if we can find a decomposition of $\mathcal{P}(n)$ into $\binom{n}{\lfloor n/2 \rfloor}$ sparse sets, then we are done.

We call a partition $\mathcal{P}(n) = \mathcal{F}_1 \cup \cdots \cup F_t$ *symmetric* if the number of families with $n + 1 - 2i$ sets is $\ell(n, i)$, i.e. the "profile" is that of a symmetric chain decomposition.

Claim. $\mathcal{P}(n)$ has a symmetric decomposition into sparse families.

We again induct on n. When $n = 1$, we can take $\{\emptyset, \{1\}\}$. Now suppose Δ_{n-1} is a symmetric decomposition of $\mathcal{P}(n-1)$ as $\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_t$.

Given $\mathcal{F}_j$, we construct $\mathcal{F}_j^{(0)}$ and $\mathcal{F}_j^{(1)}$ "as before". We pick some $D \in \mathcal{F}_j$, to be decided later, and we take

$$\mathcal{F}_j^{(0)} = \mathcal{F}_j \cup \{D \cup \{n\}\}$$
$$\mathcal{F}_j^{(1)} = \{E \cup \{n\} : E \in \mathcal{F}_j \setminus \{D\}\}.$$

The resulting set is certainly still symmetric. The question is whether it is sparse, and this is where the choice of D comes in. The collection $\mathcal{F}_j^{(1)}$ is certainly still sparse, and we must pick a D such that $\mathcal{F}_j^{(0)}$ is sparse.

To do so, we use Hahn–Banach to obtain a linear functional f such that $\|f\| = 1$ and $f(x_n) = \|x_n\| \geq 1$. We can then pick D to maximize $f(x_D)$. Then we check that if $E \in \mathcal{F}_j$, then

$$f(x_{D \cup \{n\}} - x_2) = f(x_D) - f(x_E) + f(x_n).$$

By assumption, $f(x_n) \geq 1$ and $f(x_D) \geq f(x_E)$. So this is ≥ 1. Since $\|f\| = 1$, it follows that $\|x_{D \cup \{n\}} - x_E\| \geq 1$. $\quad\square$

3 The Kruskal–Katona theorem

Lemma. We have

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

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

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

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

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 $\max V > \max U$.

Proof. $\Rightarrow$ is clear. Suppose $\mathcal{A}$ is (U, V) compressed for all such U, V. If $\mathcal{A}$ is not an initial segment, then there exists $B \in \mathcal{A}$ and $C \notin \mathcal{A}$ such that $C < B$. Then $\mathcal{A}$ is not $(C \setminus B, B \setminus C)$-compressed. A contradiction. $\hfill\square$

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

$$|\mathcal{B}| = |\mathcal{A}|, |\partial \mathcal{B}| \leq |\partial \mathcal{A}|. \tag{$*$}$$

Proof. Let $\mathcal{B}$ be such that

$$\sum_{B \in \mathcal{B}} \sum_{i \in B} 2^i$$

is minimal among those $\mathcal{B}$'s that satisfy $(*)$. We claim that this $\mathcal{B}$ will do. Indeed, if there exists (U, V) such that $|U| = |V|$, $\max V > \max U$ and $C_{UV}(\mathcal{B}) \neq \mathcal{B}$, then pick such a pair with $|U|$ minimal. Then apply a (U, V)-compression, which is valid since given any $u \in U$ we can pick any $v \in V$ that is not $\max V$ to satisfy the requirements of the previous lemma. This decreases the sum, which is a contradiction. $\hfill\square$

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.

Proof. Let

$$\mathcal{A}_0 = \{A \in \mathcal{A} : 1 \notin A\}$$
$$\mathcal{A}_1 = \{A \in \mathcal{A} : 1 \in A\}.$$

For convenience, we write

$$\mathcal{A}_1 - 1 = \{A \setminus \{1\} : A \in \mathcal{A}_1\}.$$

We may assume $\mathcal{A}$ is (i, j)-compressed for all $i < j$. We induct on r and then on $|\mathcal{A}|$. We have

$$|\mathcal{A}_0| = |\mathcal{A}| - |\mathcal{A}_1|.$$

We note that $\mathcal{A}_1$ is non-empty, as $\mathcal{A}$ is left-compressed. So $|\mathcal{A}_0| < |\mathcal{A}|$.

If $r = 1$ and $|\mathcal{A}| = 1$ then there is nothing to do.

Now observe that $\partial \mathcal{A} \subseteq \mathcal{A}_1 - 1$, since if $A \in \mathcal{A}$, $1 \notin A$, and $B \subseteq A$ is such that $|A \setminus B| = 1$, then $B \cup \{1\} \in \mathcal{A}_1$ since $\mathcal{A}$ is left-compressed. So it follows that

$$|\partial \mathcal{A}_0| \leq |\mathcal{A}_1|.$$

Suppose $|\mathcal{A}_1| < \binom{x-1}{r-1}$. Then

$$|\mathcal{A}_0| > \binom{x}{r} - \binom{x-1}{r-1} = \binom{x-1}{r}.$$

Therefore by induction, we have

$$|\partial \mathcal{A}_0| > \binom{x-1}{r-1}.$$

This is a contradiction, since $|\partial \mathcal{A}_0| \leq |\mathcal{A}_1|$. Hence $|\mathcal{A}_1| \geq \binom{x-1}{r-1}$. Hence we are done, since

$$|\partial \mathcal{A}| \geq |\partial \mathcal{A}_1| = |\mathcal{A}_1| + |\partial(\mathcal{A}_1 - 1)| \geq \binom{x-1}{r-1} + \binom{x-1}{r-2} = \binom{x}{r-1}. \quad \square$$

4 Isoperimetric inequalities

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

Proof. We have

$$|N(A)| = |N(A_+) \cup A_-| + |N(A_-) \cup A_+|$$

Take $B = C_i(A)$. Then

$$
\begin{aligned}
|N(B)| &= |N(B_+) \cup B_-| + |N(B_-) \cup B_+| \\
&= \max\{|N(B_+)|, |B_-|\} + \max\{|N(B_-)|, |B_+|\} \\
&\leq \max\{|N(A_+)|, |A_-|\} + \max\{|N(A_-)|, |A_+|\} \\
&\leq |N(A_+) \cup A_i| + |N(A_-) \cup A_+| \\
&= |N(A)| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \square
\end{aligned}
$$

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.

Proof. For the first part, simply note that complementation is an order-reversing bijection $Q_n \to Q_n$, and $|Q_n|$ is even. So the 2^{n-1}th element is the only such element z.

Now if B is not an initial segment, then we can find some $x < y$ such that $x \notin B$ and $y \in B$. Since B is compressed, it must be the case that for each i, there is exactly one of x and y that contains i. Hence $x = y^c$. Note that this is true for all $x < y$ such that $x \notin B$ and $y \in B$. So if we write out the simplicial order, then B must look like

$$\bullet \;\; \bullet \;\; \bullet \;\; \bullet \;\; \bullet \;\; \bullet \;\; \bullet \;\; \bullet \;\; \circ \;\; \bullet \;\; \circ \;\; \circ \;\; \circ \;\; \circ \;\; \circ \;\; \circ \quad \cdots$$

since any $x \notin B$ such that $x < y$ must be given by $x = y^c$, and so there must be a unique such x, and similarly the other way round. So it must be the case that y is the successor of x, and so $x = z$. $\qquad \square$

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 $|\partial_e C| \leq |\partial_e A|$.

Proof. We induct on n using codimension-1 compressions. Recall that we previously defined the sets $A_\pm^{(i)}$.

The i-compression of A is the set $B \subseteq Q_n$ such that $|B_\pm^{(i)}| = |A_\pm^{(i)}|$, and $B_\pm^{(i)}$ are initial segments in the binary order. We set $D_i(A) = B$.

Observe that performing D_i reduces the edge boundary. Indeed, given any A, we have

$$|\partial_e A| = |\partial_e A_+^{(i)}| + |\partial_e A_-^{(i)}| + |A_+^{(i)} \Delta A_i^{(i)}|.$$

Applying D_i clearly does not increase any of those factors. So we are happy. Now note that if $A \neq D_i A$, then

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

So after applying compressions finitely many times, we are left with a compressed set.

We now hope that a compressed subset must be an initial segment, but this is not quite true.

Claim. If A is compressed but not an initial, then

$$A = \tilde{B} = \mathbb{P}(X \setminus \{n\}) \setminus \{123 \cdots (n-1)\} \cup \{n\}.$$

By direct computation, we have

$$|\partial_e \tilde{B}| = 2^{n-1} - 2(n-2),$$

and so the initial segment is better. So we are done.

The proof of the claim is the same as last time. Indeed, by definition, we can find some $x < y$ such that $x \notin A$ and $y \in A$. As before, for any i, it cannot be the case that both x and y contain i or neither contain i, since A is compressed. So $x = y^c$, and we are done as before. $\square$

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

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

Proof. We may assume $1 \leq |A| \leq |B|$. Apply induction on $|A|$. If $|A| = 1$, then there is nothing to do. So assume $A \geq 2$.

Since everything is invariant under translation, we may assume $0, a \in A$ with $a \neq 0$. Then $\{a, 2a, \ldots, pa\} = \mathbb{Z}_p$. So there exists $k \geq 0$ such that $ka \in B$ and $(k+1)a \notin B$.

By translating B, we may assume $0 \in B$ and $a \notin B$.

Now $0 \in A \cap B$, while $a \in A \setminus B$. Therefore we have

$$1 \leq |A \cap B| < |A|.$$

Hence

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

Also, clearly

$$(A \cap B) + (A \cup B) \subseteq A + B.$$

So we are done.   □

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

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

Then

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

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

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

in $\mathbb{Z}_n$.

Proof. First consider the case $n = p$ is a prime. Write

$$0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} < p.$$

If $a_i = a_{i+p-1}$, then there are p terms that are the same, and so we are done by adding them up. Otherwise, set $A_i = \{a_i, a_{i+p-1}\}$ for $i = 1, \ldots, p-1$, and $A_p = \{a_{2p-1}\}$, then $|A_i| = 2$ for $i = 1, \ldots, p-1$ and $|A_p| = 1$. Hence we know

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

Thus, every element in $\mathbb{Z}_p$ is a sum of some p of our terms, and in particular 0 is.

In general, suppose n is not a prime. Write $n = pm$, where p is a prime and $m > 1$. By induction, for every $2m - 1$ terms, we can find m terms whose sum is a multiple of m.

Select *disjoint* $S_1, S_2, \ldots, S_{2p-1} \in [2n-1]^{(m)}$ such that

$$\sum_{j \in S_i} a_j = mb_i.$$

This can be done because after selecting, say, $S_1, \ldots, S_{2p-2}$, we have

$$(2n - 1) - (2p - 2)m = 2m - 1$$

elements left, and so we can pick the next one.

We are essentially done, because we can pick $j_1, \ldots, j_p$ such that $\sum_{k=1}^{p} b_{i_k}$ is a multiple of p. Then

$$\sum_{k=1}^{p} \sum_{j \in S_{i_k}} a_j$$

is a sum of $mp = n$ terms whose sum is a multiple of mp. $\square$

6 Projections

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

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

Proof. Suppose first that each section of K is a square, i.e.

$$K(x) = (0, f(x)) \times (0, f(x)) \, \mathrm{d}x$$

for all x and some f. Then

$$|K| = \int f(x)^2 \, \mathrm{d}x.$$

Moreover,

$$|K_{12}| = \left(\sup_x f(x) \right)^2 \equiv M^2, \quad |K_{13}| = |K_{23}| = \int f(x) \, \mathrm{d}x.$$

So we have to show that

$$\left(\int f(x)^2 \, \mathrm{d}x \right)^2 \leq M^2 \left(\int f(x) \, \mathrm{d}x \right)^2,$$

but this is trivial, because $f(x) \leq M$ for all x.

Let's now consider what happens when we compress K. For the general case, define a new body $L \subseteq \mathbb{R}^3$ by setting its sections to be

$$L(x) = (0, \sqrt{|K(x)|}) \times (0, \sqrt{|K(x)|}).$$

Then $|L| = |K|$, and observe that

$$|L_{12}| \leq \sup |K(x)| \leq \left| \bigcup K(x) \right| = |K_{12}|.$$

To understand the other two projections, we introduce

$$g(x) = |K(x)_1|, \quad h(x) = |K(x)_2|.$$

Now observe that
$$|L(x)| = |K(x)| \leq g(x)h(x),$$

Since $L(x)$ is a square, it follows that $L(x)$ has side length $\leq g(x)^{1/2}h(x)^{1/2}$. So

$$|L_{13}| = |L_{23}| \leq \int g(x)^{1/2}h(x)^{1/2} \, \mathrm{d}x.$$

So we want to show that

$$\left(\int g^{1/2}h^{1/2} \, \mathrm{d}x \right)^2 \leq \left(\int g \, \mathrm{d}x \right) \left(\int h \, \mathrm{d}x \right).$$

Observe that this is just the Cauchy–Schwarz inequality applied to $g^{1/2}$ and $h^{1/2}$. So we are done. $\qquad \square$

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

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

Proof. Let $\mathcal{A}$ be a k-uniform cover of $[k]$. Note that $\mathcal{A}$ is a *multiset*. Write

$$\mathcal{A}_- = \{A \in \mathcal{A} : n \notin A\}$$
$$\mathcal{A}_+ = \{A \setminus \{n\} \in \mathcal{A} : n \in A\}$$

We have $|\mathcal{A}_+| = k$, and $\mathcal{A}_+ \cup \mathcal{A}_-$ forms a k-uniform cover of $[n-1]$.

Now note that if $K = \mathbb{R}^n$ and $n \notin A$, then

$$|K_A| \geq |K(x)_A| \tag{1}$$

for all x. Also, if $n \in A$, then

$$|K_A| = \int |K(x)_{A \setminus \{n\}}| \, \mathrm{d}x. \tag{2}$$

In the previous proof, we used Cauchy–Schwarz. What we need here is Hölder's inequality

$$\int fg \, \mathrm{d}x \leq \left(\int f^p \, \mathrm{d}x \right)^{1/p} \left(\int g^q \, \mathrm{d}x \right)^{1/q},$$

where $\frac{1}{p} + \frac{1}{q} = 1$. Iterating this, we get

$$\int f_1 \cdots f_k \, \mathrm{d}x \leq \prod_{i=1}^{k} \left(\int f_i^k \, \mathrm{d}x \right)^{1/k}.$$

Now to perform the proof, we induct on n. We are done if $n = 1$. Otherwise, given $K \subseteq \mathbb{R}^n$ and $n \geq 2$, by induction,

$$
\begin{aligned}
|K| &= \int |K(x)| \, \mathrm{d}x \\
&\leq \int \prod_{A \in \mathcal{A}_-} |K(x)_A|^{1/k} \prod_{A \in \mathcal{A}_+} |K(x)_A|^{1/k} \, \mathrm{d}x && \text{(by induction)} \\
&\leq \prod_{A \in \mathcal{A}_-} |K_A|^{1/k} \int \prod_{A \in \mathcal{A}_+} |K(x)_A|^{1/k} \, \mathrm{d}x && \text{(by (1))} \\
&\leq \prod_{A \leq |\mathcal{A}_-} |K_A|^{1/k} \prod_{A \in \mathcal{A}_+} \left(\int |K(x)_A| \right)^{1/k} && \text{(by Hölder)} \\
&= \prod_{A \in \mathcal{A}} |K_A|^{1/k} \prod_{A \in \mathcal{A}_+} |K_{A \cup \{n\}}|^{1/k}. && \text{(by (2))}
\end{aligned}
$$

$\square$

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 $[n]$.

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be covers. We say $\mathcal{A} < \mathcal{B}$ if $\mathcal{A}$ is a "subset" of $\mathcal{B}$, i.e. for each $A \subseteq [n]$, the multiplicity of A in $\mathcal{A}$ is less than the multiplicity in $\mathcal{B}$.

Then note that the set of irreducible uniform k-covers form an anti-chain, and observe that there cannot be an infinite anti-chain.

□

Proof of box theorem. For $\mathcal{A}$ an irreducible cover, we have

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

Also,

$$|K_A| \leq \prod_{i \in A} |K_{\{i\}}|.$$

Let $\{x_A : A \subseteq [n]\}$ be a minimal array with $x_A \leq |K_A|$ such that for each irreducible k-cover $\mathcal{A}$, we have

$$|K|^k \leq \prod_{A \in \mathcal{A}} x_A \tag{1}$$

and moreover

$$x_A \leq \prod_{i \in A} x_{\{i\}} \tag{2}$$

for all $A \subseteq [n]$. We know this exists since there are only finitely many inequalities to be satisfied, and we can just decrease the x_A's one by one. Now again by finiteness, for each x_A, there must be at least one inequality involving x_A on the right-hand side that is in fact an equality.

Claim. For each $i \in [n]$, there exists a uniform k_i-cover $\mathcal{C}_i$ containing $\{i\}$ with equality

$$|K|^{k_i} = \prod_{A \in \mathcal{C}_i} x_A.$$

Indeed if x_i occurs on the right of (1), then we are done. Otherwise, it occurs on the right of (2), and then there is some A such that (2) holds with equality. Now there is some cover $\mathcal{A}$ containing A such that (1) holds with equality. Then replace A in $\mathcal{A}$ with $\{\{j\} : j \in A\}$, and we are done.

Now let

$$\mathcal{C} = \bigcup_{i=1}^n \mathcal{C}_i, \quad \mathcal{C}' = \mathcal{C} \setminus \{\{1\}, \{2\}, \dots, \{n\}\}, \quad k = \sum_{i=1}^n k_i.$$

Then

$$|K|^k = \prod_{A \in \mathcal{C}} x_A = \left(\prod_{A \in \mathcal{C}^1} x_A \right) \geq |K|^{k-1} \prod_{i=1}^n x_i.$$

So we have

$$|K| \geq \prod_{i=1}^n x_i.$$

But we of course also have the reverse inequality. So it must be the case that they are equal.

Finally, for each A, consider $\mathcal{A} = \{A\} \cup \{\{i\} : i \notin A\}$. Then dividing (1) by $\prod_{i \in A} x_i$ gives us

$$\prod_{i \notin A} x_i \leq x_A.$$

By (2), we have the inverse equality. So we have

$$x_A = \prod_{i \in A} x_i$$

for all i. So we are done by taking L to be the box with side length x_i.   □

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

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

Proof. Observe that if $B \subseteq A$, then $|K_B| \leq |K_A|$. So we can reduce $\mathcal{A}$ to a uniform k-cover.   □

7   Alon's combinatorial Nullstellensatz

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

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 $i = 1, \ldots, n$, 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 exists polynomials $h_1, \ldots, h_n, r \in R[X]$ such that

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

where

$$\deg h_i \leq \deg f - \deg d_i \qquad \deg_{X_i} r \leq d_i - 1$$
$$\deg_{X_i} h_i \leq \deg_{X_i} f - d_i \qquad \deg_{X_i} r \leq \deg_{X_i} f$$
$$\deg_{X_j} h_i \leq \deg_{X_j} f \qquad \deg r \leq \deg f$$

for all i, j.

Proof. Consider f as a polynomial with coefficients in $R[X_2, \ldots, X_n]$, then divide by g_1 using the division algorithm. So we write

$$f = h_1 g_1 + r_1.$$

Then we have

$$\deg_{X_1} h_1 \leq \deg_{X_1} f - d_1 \qquad \deg_{X_1} r_1 \leq d_1 - 1$$
$$\deg h_1 \leq \deg f \qquad \deg_{X_j} r_1 \leq \deg_{X_j} f$$
$$\deg_{X_j} h_1 \leq \deg_{X_j} f \qquad \deg r \leq \deg f.$$

Then repeat this with f replaced by r_1, g_1 by g_2, and X_1 by X_2. □

Lemma. Let $S_1, \ldots, S_n$ 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 $i = 1, \ldots, n$. Suppose h is identically 0 on $S = S_1 \times \cdots \times S_n \subseteq \mathbb{F}^n$. Then h is the zero polynomial.

Proof. Let $d_i = |S_i| - 1$. We induct on n. If $n = 1$, then we are done. For $n \geq 2$, consider h as a one-variable polynomial in $F[X_1, \ldots, X_{n-1}]$ in X_n. Then we can write

$$h = \sum_{i=0}^{d_n} g_i(X_1, \ldots, X_{n-1}) X_m^i.$$

Fix $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots S_{n-1}$, and set $c_i = g_i(x_1, \ldots, x_{n-1}) \in \mathbb{F}$. Then $\sum_{i=0}^{d_n} c_i X_n^i$ vanishes on S_n. So $c_i = g_i(x_1, \ldots, x_{n-1}) = 0$ for all $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$. So by induction, $g_i = 0$. So $h = 0$. □

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

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

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

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

Proof. By the division algorithm, we can write

$$f = \sum_{i=1}^{n} h_i g_i + r,$$

where r satisfies $\deg_{X_i} r < \deg g_i$. But then r vanishes on $S_1 \times \cdots \times S_n$, as both f and g_i do. So $r = 0$. $\qquad\square$

Theorem (Alon's combinatorial Nullstellensatz)**.** Let $S_1, \ldots, S_n$ 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 $X_1^{d_1} \cdots X_n^{d_n}$ be non-zero. Then f is not identically zero on $S = S_1 \times \cdots \times S_n$.

Proof. Suppose for contradiction that f is identically zero on S. Define $g_i(X_i)$ and h_i as before such that

$$f = \sum h_i g_i.$$

Since the coefficient of $X_1^{d_1} \cdots X_n^{d_n}$ is non-zero in f, it is non-zero in some $h_j g_j$. But that's impossible, since

$$\deg h_j \leq \left(\sum_{i=1}^{n} d_i \right) - \deg g_j = \sum_{i \neq j} d_i - 1,$$

and so h_j cannot contain a $X_1^{d_1} \cdots \hat{X}_j^{d_j} \cdots X_n^{d_n}$ term. $\qquad\square$

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

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

Then the f_i cannot have exactly one common zero.

Proof. Suppose not. We may assume that the common zero is $0 = (0, \ldots, 0)$. Define

$$f = \prod_{i=1}^{m} (1 - f_i(X)^{q-1}) - \gamma \prod_{i=1}^{n} \prod_{s \in \mathbb{F}_q^{\times}} (X_i - s),$$

where γ is chosen so that $F(0) = 0$, namely the inverse of $\left(\prod_{s \in \mathbb{F}_q^{\times}} (-s) \right)^m$.

Now observe that for any non-zero x, the value of $f_i(x)^{q-1} = 1$, so $f(x) = 0$.

Thus, we can set $S_i = \mathbb{F}_q$, and they satisfy the hypothesis of the theorem. In particular, the coefficient of $X_1^{q-1} \cdots X_n^{q-1}$ is $\gamma \neq 0$. However, f vanishes on $\mathbb{F}_q^n$. This is a contradiction. $\qquad\square$

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

Proof. We have

$$1 - f(x)^{q-1} = \begin{cases} 1 & f(x) = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Thus, we know

$$N(f) = \sum_{x \in \mathbb{F}_q^n} (1 - f(x)^{q-1}) = -\sum_{x \in \mathbb{F}_q^n} f(x)^{q-1} \in \mathbb{F}_q.$$

Further, we know that if $k \geq 0$, then

$$\sum_{x \in \mathbb{F}_q^n} x^k = \begin{cases} -1 & k = q - 1 \\ 0 & \text{otherwise} \end{cases}.$$

So let's write $f(x)^{q-1}$ as a linear combination of monomials. Each monomial has degree $< n(q-1)$. So there is at least one k such that the power of X_k in that monomial is $< q - 1$. Then the sum over X_k vanishes for this monomial. So each monomial contributes 0 to the sum. $\square$

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

Proof. Suppose for contradiction that $A + B \subseteq C \subseteq \mathbb{Z}_p$, and $|C| = |A| + |B| - 2$. Let's come up with a polynomial that encodes the fact that C contains the sum $A + B$. We let

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

Then f vanishes on $A \times B$, and $\deg f = |C|$.

To apply the theorem, we check that the coefficient of $X^{|A|-1} Y^{|B|-1}$ is $\binom{|C|}{|A|-1}$, which is non-zero in $\mathbb{Z}_p$, since $C < p$. This contradicts Alon's combinatorial Nullstellensatz. $\square$

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

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

Proof. Define

$$f_1(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1}.$$

$$f_2(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} a_i X_i^{p-1}.$$

Then by Chevalley's theorem, we know there cannot be exactly one common zero. But 0 is one common zero. So there must be another. Take this solution, and let $I = \{i : x_i \neq 0\}$. Then $f_1(X) = 0$ is the same as saying $|I| = p$, and $f_2(X) = 0$ is the same as saying $\sum_{i \in I} a_i = 0$. $\square$

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

Proof. Suppose not. Define

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

where $A \dot{+} B \subseteq C \subseteq \mathbb{Z}_p$ and $|C| = |A| + |B| - 3$.

Then $\deg g = |A| + |B| - 2$, and the coefficient of $X^{|A|-1} Y^{|B|-1}$ is

$$\binom{|A| + |B| - 3}{|A| - 2} - \binom{|A| + |B| - 3}{|A| - 1} \ne 0.$$

Hence by Alon's combinatorial Nullstellensatz, $f(x, y)$ is not identically zero on $A \times B$. A contradiction. $\square$

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

Proof. We may assume $2 \le |A| \le |B|$. Pick $a \in A$, and set $A' = A \setminus \{a\}$. Then

$$|A \dot{+} B| \ge |A' \dot{+} B| \ge |A'| + |B| - 2 = |A| + |B| - 3. \qquad \square$$

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

Proof. We may wlog assume the host is at 0. We want to partition $\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^{\times}$ into n pairs $\{x_i, x_i + d_i\}$. Consider the polynomial ring $\mathbb{Z}_p[X_1, \dots, X_n] = \mathbb{Z}_p[X]$. We define

$$f(x) = \prod_i X_i(X_i + d_i) \prod_{i<j} (X_i - X_j)(X_i + d_i - X_j)(X_i - X_j - d_j)(X_i + d_i - X_j - d_j).$$

We want to show this is not identically zero on $\mathbb{Z}_p^n$

First of all, we have

$$\deg f = 4\binom{n}{2} + 2n = 2n^2.$$

So we are good. The coefficient of $X_1^{2n} \cdots X_n^{2n}$ is the same as that in

$$\prod X_i^2 \prod_{i<j} (X_i - X_j)^4 = \prod X_i^2 \prod_{i \ne j} (X_i - X_j)^2 = \prod X_i^{2n} \prod_{i \ne j} \left(1 - \frac{X_i}{X_j}\right)^2.$$

This, we are looking for the constant term in

$$\prod_{i \ne j} \left(1 - \frac{X_i}{X_j}\right)^2.$$

By a question on the example sheet, this is

$$\binom{2n}{2, 2, \dots, 2} \ne 0 \text{ in } \mathbb{Z}_p. \qquad \square$$

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

$$a_i + b_i = c_i.$$

Proof. It suffices to show that for all (b_i), there are distinct $a_1, \cdots, a_{p-1}$ such that $a_i + b_i \neq a_j + b_j$ for all $i \neq j$. Consider the polynomial

$$\prod_{i<j}(X_i - X_j)(X_i + b_i - X_j - b_j).$$

The degree is

$$2\binom{p-1}{2} = (p-1)(p-2).$$

We then inspect the coefficient of $X_1^{p-2} \cdots X_{p-1}^{p-2}$, and checking that this is non-zero is the same as above. $\qquad\square$