Introduction to combinatorics

Piotr Nayar, 2019/2020

1 Extremal combinatorics

1.1 Fisher's inequality

Theorem 1 (Fisher's inequality)**.** Fix $1 \leq k \leq n$. Let $A_1, A_2, \ldots, A_m$ be distinct subsets of a n element set, such that $|A_i \cap A_j| = k$ for all $i \neq j$. Prove that $m \leq n$.

Proof. Let $v_1, \ldots, v_m$ be $\{0,1\}$ vectors such that jth coordinate of v_i is 1 if and only if $j \in A_i$. It suffices to prove that these vectors are linear independent. Suppose, by contradiction, that for some $\lambda_1, \ldots, \lambda_m$ we have $\sum_{i=1}^m \lambda_i v_i = 0$, with not all coefficients being zero. Note that $\langle v_i, v_j \rangle = k$ for $i \neq j$ and $\langle v_i, v_i \rangle = |A_i|$ for $i = 1, \ldots, m$. We have

$$0 = \left\langle \sum_{i=1}^m \lambda_i v_i, \sum_{i=1}^m \lambda_i v_i \right\rangle = \sum_{i=1}^m \lambda_i^2 |A_i| + k \sum_{i \neq j} \lambda_i \lambda_j$$
$$= \sum_{i=1}^m \lambda_i^2 (|A_i| - k) + k \left(\sum_{i=1}^m \lambda_i \right)^2.$$

There exist at least two indexes i, j such that $\lambda_i, \lambda_j \neq 0$. It follows that $|A_i| = |A_j| = k$. This contradicts the condition $|A_i \cap A_j| = k$ and $A_i \neq A_j$. □

1.2 Clubs in Oddtown

Suppose citizens of a certain town form clubs according to the following two rules:

(a) Each club has an odd number of members.

(b) Each pair of clubs share an even number of members.

What is the maximal number of clubs that can be formed in this town? The answer is given by the following theorem.

Theorem 2. Suppose $A_1, \ldots, A_m$ be distinct subsets of a given set of cardinality n. Suppose $|A_i|$ is odd for every i and $|A_i \cap A_j|$ is even for every $i \neq j$. Then $m \leq n$.

Remark. Equality can be achieved, for example if the sets A_i are all the singletons.

First proof. Let us assume that the citizens are numbered 1 through n. To each club we associate a vector $v_i \in \mathbb{Z}_2^n = \{0,1\}^n$ in such a way that the jth coordinate of v_i is equal to 1 if and only if the jth citizen is a member of the ith club. We shall work over the field $\mathbb{Z}_2$. Let us introduce the standard scalar product

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1 y_1 + \ldots + x_n y_n,$$

where the sum is taken in $\mathbb{Z}_2$. By our assumption we have $\langle v_i, v_j \rangle = 1$ for $i = j$ and $\langle v_i, v_j \rangle = 0$ for $i \neq j$. We claim that $v_1, \ldots, v_m$ are linearly independent. Indeed, suppose that $\lambda_1 v_1 + \ldots + \lambda_m v_m = 0$. Taking the scalar product of both sides with the vector v_i one gets $\lambda_i = 0$, which shows the claim. Since the vector space $(\mathbb{Z}_2^n, \mathbb{Z}_2)$ has dimension n, we must have $k \leq n$ (it is not possible to find more than n linearly independent vectors in a vector space of dimension n). □

Second proof. We again shall work in $\mathbb{Z}_2$. Let us consider vectors v_i as above and let M be an $m \times n$ matrix with rows v_i. We shall again show that the vectors v_i are linearly independent. By our assumption MM^T is the $m \times m$ identity matrix (note that the (i,j) entry of this matrix is $|A_i \cap A_j|$ in $\mathbb{Z}_2$). For any matrices A, B (over arbitrary field) such the number of columns of A equals the number of rows of B, we have

$$\operatorname{rank}(AB) \leq \min(\operatorname{rank}(A), \operatorname{rank}(B)).$$

Applying this for $A = M$ and $B = M^T$ we get $m = \operatorname{rank}(MM^T) \leq \operatorname{rank}(M) \leq n$, since M has n columns. □

1.3 Sperner's lemma

Theorem 3 (Sperner's lemma, [AI])**.** Let $\mathcal{F}$ be a family of subsets of a given n element set X, such that for any pair of subsets $A, B \in \mathcal{F}$ we have $A \not\subseteq B$. Then

$$|\mathcal{F}| \leq \binom{n}{[n/2]}$$

The family for which we have equality is the family of all subsets of cardinality $[n/2]$.

Proof. Without loss of generality we shall assume that $X = \{1, \ldots, n\}$. To prove the above fact we consider the family $\mathcal{F}$ and we count pairs (π, S), where π is a permutation of $\{1, \ldots, n\}$ and S is a set of the form $S = \{\pi(1), \ldots, \pi(k)\}$ for π, such that $S \in \mathcal{F}$. For each π we can have at most one $S \in \mathcal{F}$. Therefore, the number of pairs (π, S) is not greater than $n!$. Moreover, a fixed set $S \in \mathcal{F}$ of cardinality k will be counted exactly $k!(n-k)!$ times. So, if s_k is the number of sets in $\mathcal{F}$ of cardinality k then the number of pairs (π, S) is equal to $\sum_{k=0}^{n} s_k k!(n-k)!$. Thus, $\sum_{k=0}^{n} s_k k!(n-k)! \leq n!$. It means that $\frac{|\mathcal{F}|}{\binom{n}{[n/2]}} \leq \sum_{k=0}^{n} \frac{s_k}{\binom{n}{k}} \leq 1$. □

We have in fact proved the following fact.

Theorem 4 (LYM inequality)**.** Let X be an n element set and let $\mathcal{F}$ be an antichain over X, that is, a family of subsets of X such that no set in $\mathcal{F}$ is a subset of another set in $\mathcal{F}$. Let s_k be the number of sets in $\mathcal{F}$ of cardinality k. Then $\sum_{k=0}^{n} \frac{s_k}{\binom{n}{k}} \leq 1$.

Remark. LYM stands for Lubell–Yamamoto–Meshalkin.

Alternative proof. For every subset A of X exactly $|A|!(n-|A|)!$ maximal chains (chains having $n+1$ members of consecutive cardinalities) over X contain A. Since $\mathcal{F}$ is an antichain, none of the $n!$ maximal chains meet $\mathcal{F}$ more than once. Let $\mathcal{C}_A$ be the family of maximal chains that meet A. We have $|C_A| = |A|!(n-|A|)!$ and C_A for different A do not intersect. Thus $\sum_{A \in \mathcal{F}} |A|!(n-|A|)! = \sum_{A \in \mathcal{F}} |\mathcal{C}_A| \leq n!$. □

Theorem 5. Let $v_1, \ldots, v_n$ be real numbers such that $|v_i| \geq 1$ for $i = 1, \ldots, n$. Define

$$A = \{x = (x_1, \ldots, x_n) \in \{-1, 1\}^n, \quad |v_1 x_1 + \cdots + v_n x_n| < 1\}.$$

Then $|A| \leq \binom{n}{[n/2]}$. In other words, the probability that the random walk with steps $\pm v_i$ (each taken with probability $\frac{1}{2}$) ends up in the interval $[-1, 1]$ is upper bounded by $2^{-n}\binom{n}{[n/2]} = O(1/\sqrt{n})$.

Proof. This is a special case of the Littlewood-Offord problem, see [E]. Without loss of generality we can assume that $v_i \geq 1$ for $i = 1, \ldots, n$. A point x in $\{-1, 1\}^n$ can be seen as a subset B_x of $\{1, 2, \ldots, n\}$, i.e., $i \in B_x$ if and only if $x_i = 1$. It is easy to observe that if $|v_1 x_1 + \cdots + v_n x_n| < 1$ for some $x \in \{-1, 1\}^n$, then changing one or more signs x_i from -1 to 1 gives a point, for which $|v_1 x_1 + \cdots + v_n x_n| \geq 1$. It means that $\{B_x, x \in A\}$ satisfies the assumption of Sperner's lemma. Thus, $|A| \leq \binom{n}{[n/2]}$. □

1.4 Erdös-Ko-Rado theorem

Theorem 6 (Erdös-Ko-Rado theorem)**.** Let $2k \leq n$ and let $\mathcal{F}$ be a family of k element subsets of $[n]$ such that each subset in of size k and for every $A, B \in \mathcal{F}$ we have $A \cap B \neq \emptyset$. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof. The idea is to count pairs (π, S) where π is a circular permutation $(\pi(1), \pi(2), \ldots, \pi(n))$ (placing $\pi(1), \pi(2), \ldots, \pi(n)$ on the circle with no specified starting point) and S is an interval (on the circle) of length k in this permutation such that $S \in \mathcal{F}$. In other words S is an interval on the discrete circle, where the numbers are placed according to π and the elements in this interval must form a set from $\mathcal{F}$. We have $(n-1)!$ cyclic permutations. Each of them contains at most k pairwise intersecting intervals of length k and thus at most k elements of our family. In this step we have used the fact that $2k \leq n$. Each set in our family occurs in precisely $k!(n-k)!$ cyclic permutations. Thus, $|\mathcal{F}|k!(n-k)! \leq k(n-1)!$. Our assertion follows. □

1.5 Mirsky's and Dilworth's theorems

A *poset* is a partially ordered set. In a poset there are comparable and incomparable elements. A subset of a poset which consists of pairs of comparable elements is a *chain*. A subset which consists of pairwise incomparable elements is called an *antichain*.

We want to partition a given poset into as *few* chains (or antichains) as possible (clearly singletons give us a partition into both chains and antichains). Suppose that the maximal length of a chain in our poset is equal to r. Then it is not possible to have a partition of our poset into fewer than r antichains (since then from the pigeonhole principle we would have an antichain having at least two elements from our chain of maximal length, which is impossible). Is it always possible to partition our poset into exactly r antichains?

Now, suppose the cardinality of the maximal antichain in our poset equals r. Then it is not possible to create a partition into fewer than r chains, since then one of the chains would have at least two elements of our maximal antichain, which gives a contradiction. Is it always possible to partition our poset into exactly r chains?

Theorem 7 (Mirsky's theorem)**.** Suppose that in a given finite poset the maximal lenght of a chain is equal to r. Then the poset can be partitioned into r antichains.

Proof. For x is our poset its *rank* is the maximal possible cardinality l of a chain $x_1 < x_2 < \ldots x_l = x$. Let A_i consists of all the elements having rank i. Clearly A_i are non-empty only for $i \leq r$. We claim that each A_i is an antichain. Suppose by contradiction that $x, y \in A_i$ and, say, $x < y$. Then the maximal chain $x_1 < \ldots < x_i = x$ can be prolonged to $x_1 < \ldots < x_i = x < y$, which means that the rank of y is at least $i+1$, contradiction. □

Theorem 8 (Dilworth's theorem)**.** Suppose that in a give finite poset the maximal cardinality of an antichain is equal to r. Then the poset can be partitioned into r chains.

Proof. Induction on the cardinality of the poset. Let a be any maximal element in P and consider $P' = P \setminus \{a\}$. Suppose r is the size maximal size of an antichain in P'. From induction hypothesis we can partition P' into chains $C_1, \ldots, C_r$. We shall prove that one of the following two situations hold:

(a) P has an $r+1$ element antichain (and in this case we are done with the proof since we can easily partition P into $r+1$ chains just by taking the partition of P' into r chains from induction hypothesis, and then add a singleton chain $\{a\}$).

(b) P is a union of r chains (and in this case we are also done since in $P' \subset P$ there is an antichain of size r).

There exists an r element antichain in P' (by the definition of r). This antichain has exactly one element from each C_i (it cannot have two elements, since then it would not be an antichain). Let a_i be the maximal element in C_i which belongs to certain r element antichain in P' (by definition of r there is at least one r element antichain in P' and this antichain meets every C_i, so the elements a_i are well defined). Now, clearly $A = \{a_1, \ldots, a_r\}$ is an antichain in P'. Indeed, if $a_i < a_j$ then a_j is comparable to all the elements in C_i that are less then or equal a_i. Thus the r element antichain containing a_j has to meet C_i higher than at a_i, which contradicts the definition of a_i.

If $A \cup \{a\}$ is an antichain, then we are done ((a) holds). Otherwise $a > a_i$ for some i (it cannot be $a < a_i$ since a is maximal). Thus $C = \{a\} \cup \{x \in C_i : \ x \leq a_i\}$ is a chain in P. Observe that there are no r element antichains in $P'' = P \setminus C$, since $(P \setminus C) \cap C_i$ only contains element greater than a_i, which contradicts the definition of a_i as the maximal element in C_i participating in an r element anichain in P'. From the induction hypothesis P'' can be partitioned into $r-1$ chains and thus $P = P'' \cup C$ can be partitioned into r chains (note that P'' cannot be partitioned into fewer than $r-1$ chains since P cannot be partitioned into fewer than r chains, as P' cannot be partitioned in such a way, see the remark before the formulation of the theorem). □

1.6 Erdös-Szekeres theorem

Theorem 9 (Erdös-Szekeres theorem, [ES])**.**

(a) Any sequence of real numbers $x_1, x_2, \ldots$ contains a non-increasing or a non-decreasing subsequence.

(b) Let $n, m \geq 1$ be integers. Suppose we have a sequence of $(n-1)(m-1)+1$ real numbers. Then there exists a non-decreasing sequence of length n or a non-increasing sequence of length m.

Proof. (a) The assertion clearly hold when $x_1, x_2, \ldots$ is not bounded (take a monotone sequence converging to ∞ or to $-\infty$). If our sequence is bounded then from the Bolzano-Weierstrass we can find its converging subsequence $A = \{x_{i_1}, x_{i_2}, \ldots\}$. Let g be the limit of this subsequence. One of the sets $A \cap (-\infty, g], A \cap [g, \infty)$ is infinite. In the first case we can find a non-decreasing subsequence of A and in the second case we can find a non-increasing subsequence of A.

(b) This is the Erdös-Szekeres theorem, see [ES]. The presented proof can be found in [AZ]. Assume, by way of contradiction, that there are no non-decreasing sequence of length n. Define the function $f : \{1, 2, \ldots, (n-1)(m-1)+1\} \to \{1, 2, \ldots, n-1\}$ in the following way,

$$f(i) = \text{length of longest increasing subsequence that ends with } x_i.$$

The function f has domain o size $(n-1)(m-1)+1$ and the range of size $n-1$. Thus, there exist $i_1 < i_2 < \cdots < i_m$ and a number $k \in \{1, \ldots, n-1\}$ such that

$$f(i_1) = f(i_2) = \cdots = f(i_m) = k.$$

Note that $x_{i_j} > x_{i_{j+1}}$ since otherwise $f(i_{j+1}) = k+1$ (add the point $x_{i_{j+1}}$ to the longest sequence that ends with x_{i_j}). Thus, the sequence

$$x_{i_1} > x_{i_2} > \cdots > x_{i_m}$$

is a decreasing sequence of length m. □

1.7 Sauer-Shelach lemma

Definition 1. We say that a family $\mathcal{F}$ of subsets of a given set X *shatters* a set $S \subseteq X$ if for every $T \subseteq S$ there exists $F \in \mathcal{F}$ such that $S \cap F = T$. We also say that $\mathcal{F}$ has VC-dimension k if k is the largest cardinality of a subset of X that can be shattered by $\mathcal{F}$.

Theorem 10 (Sauer-Shelach lemma)**.** Suppose a family $\mathcal{F}$ of subsets of X with $|X| = n$ satisfies

$$|\mathcal{F}| > \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k-1}.$$

Then the VC-dimension of $\mathcal{F}$ is at least k, that is, there exists a set $S \subseteq [n]$ of cardinality k such that $\mathcal{F}$ shatters S.

We shall deduce the above theorem from a more general fact.

Theorem 11 (Pajor, [P])**.** Suppose $\mathcal{F}$ is a finite family of subsets of a given set X. Then $\mathcal{F}$ shatters at least $|\mathcal{F}|$ sets.

Proof of Sauer-Shelach lemma. From the assumption and form the above theorem $\mathcal{F}$ shatters more that $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k-1}$, which is the number of sets of cardinality at most $k-1$. Thus $\mathcal{F}$ has to shatter a set of cardinality at least k. □

Proof of Pajor's theorem. Induction on $|\mathcal{F}|$. If $|\mathcal{F}| = 1$ then the assertion holds since $\mathcal{F}$ shatters an empty set. Suppose $|\mathcal{F}| \geq 2$. Let $x \in X$ be an element that belongs to some but not all the members of $\mathcal{F}$. This gives a split $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$, where $\mathcal{F}_0$ consists of members of $\mathcal{F}$ not containing x, and $\mathcal{F}_1$ consists of members of $\mathcal{F}$ containing x. Note that $|\mathcal{F}_0| < |\mathcal{F}|$ and $|\mathcal{F}_1| < |\mathcal{F}|$. From induction hypothesis $\mathcal{F}_0$ shatters at least $|\mathcal{F}_0|$ sets and $\mathcal{F}_1$ shatters at least $|\mathcal{F}_1|$ sets. Clearly $|\mathcal{F}| = |\mathcal{F}_0| + |\mathcal{F}_1|$, but the problem is that some of the sets can be shattered by both $\mathcal{F}_0$ and $\mathcal{F}_1$.

We observe that none of the sets shattered by $\mathcal{F}_0$ and none of the sets shattered by $\mathcal{F}_1$ contains x. Indeed a set containing x cannot be shattered by $\mathcal{F}_0$ since none of the members of $\mathcal{F}_0$ contains x. But also a set S containing x cannot be shattered by $\mathcal{F}_1$, since $T = \emptyset \subset S$, but all the subsets of the form $S \cap F_1$, where $F_1 \in \mathcal{F}_1$ contain x.

We now claim that if S is shattered by both $\mathcal{F}_0$ and $\mathcal{F}_1$, then $x \notin S$ and both S and $S \cup \{x\}$ are shattered by $\mathcal{F}$. From the above observation we have the first part of the claim. Now, of course S is shattered by $\mathcal{F}$ as it is shattered by $\mathcal{F}_0$. We shall show that $S \cup \{x\}$ is shattered by $\mathcal{F}$. Subsets of $S \cup \{x\}$ have the form T or $T \cup \{x\}$, where $T \subseteq S$. There is a set $F_0 \in \mathcal{F}_0 \subseteq \mathcal{F}$ such that $T = S \cap F_0$ (since $\mathcal{F}_0$ shatters S). Also, there is a set $F_1 \in \mathcal{F}_1 \subseteq \mathcal{F}$ such that $T = S \cap F_1$ ($\mathcal{F}_1$ shatters S) and since $x \in F_1$, we get $T \cup \{x\} = (S \cup \{x\}) \cap F_1$.

Now, the sets S (do not containing x) shattered by $\mathcal{F}_0$ or by $\mathcal{F}_1$ are of three types. There are sets shattered only by $\mathcal{F}_0$ (call this collection $\mathcal{S}_0$), sets shattered only by $\mathcal{F}_1$ (call this collection $\mathcal{S}_1$) and sets shattered by both $\mathcal{F}_0$ and $\mathcal{F}_1$ (call this collection $\mathcal{S}_{01}$). These families are disjoint. We have $|\mathcal{S}_0 \cup \mathcal{S}_{01}| \geq |\mathcal{F}_0|$ and $|\mathcal{S}_1 \cup \mathcal{S}_{01}| \geq |\mathcal{F}_1|$. The number of sets S shattered by $\mathcal{F}_0$ or by $\mathcal{F}_1$ is thus $|\mathcal{S}_0| + |\mathcal{S}_1| + |\mathcal{S}_{01}| = |\mathcal{S}_0 \cup \mathcal{S}_{01}| + |\mathcal{S}_1 \cup \mathcal{S}_{01}| - |\mathcal{S}_{01}| \geq |\mathcal{F}_0| + |\mathcal{F}_1| - |\mathcal{S}_{01}|$. Above we proved that the number of sets of the form $S \cup \{x\}$ shattered by $\mathcal{F}$ is at least $|\mathcal{S}_{01}|$. Altogether, we gave at least $|\mathcal{F}_0| + |\mathcal{F}_1| - |\mathcal{S}_{01}| + |\mathcal{S}_{01}| = |\mathcal{F}_0| + |\mathcal{F}_1|$ shattered by $\mathcal{F}$. □

1.8 Ramsey theorem for graphs

Theorem 12. Let $r, b \geq 1$. There exists a number $R(r, b)$ depending only on r and b with the following property: for every complete graph G with $R(r, b)$ vertices whose edges are colored red or blue, there exists either a complete subgraph on r vertices which is entirely red, or a complete subgraph on b vertices which is entirely blue. We will assume that $R(r, b)$ is the smallest number having this property.

Moreover, we have

$$R(r, b) \leq R(r-1, b) + R(r, b-1), \quad r, b \geq 1$$

and $R(r, b) \leq \binom{r+b-2}{r-1}$.

Proof. This is the so-called Ramsey's theorem. We prove the inequality $R(r,b) \leq R(r-1,b)+R(r,b-1)$, where we assume that $R(r-1,b)$ and $R(r,b-1)$ exist and are finite. The proof then goes by induction on $r+b$ (in the case $r+b=2$, $r=b=1$ we trivially have $R(r,b)=1$). Take a complete graph V with $R(r-1,b)+R(r,b-1)$ elements and color its edges red of blue. We are to show that there exists a *blue* subgraph of b elements or a *red* subgraph of r element. Take any vertex $v \in V$. Since $\deg(v) = R(r-1,b)+R(r,b-1)-1$, there are at least $R(r-1,b)$ red edges incident to v or at least $R(r,b-1)$ blue edges incident to v. Without loss of generality we can assume the first possibility. Consider a subraph G of $R(r-1,b)$ vertices connected to v with red edges. We now use the definition of $R(r-1,b)$. If in this graph there exists a complete *blue* subgraph of b vertices, then triviali our assertion follows. We can therefore assume that there are $r-1$ vertices $v_1,\ldots,v_{r-1}$ that form a *red* subgraph. The graph induced by $v_1,\ldots,v_{r-1},v$ is *red* and has r vertices.

The second part follows trivially from the inequality we just proved and from the fact that $R(1,k) = R(k,1) = 1$. □

Remark. The above theorem is a cornerstone of the so-called Ramsey theory. The numbers $R(r,b)$ are called Ramsey numbers. The Ramsey numbers $R(k,k)$ are known only for $k \leq 4$. See [R] for more information and open problems on Ramsey numbers.

1.9 Ramsey theorem for sets

Theorem 13. Let $k \leq s$ be positive integers. There exists a number $R_r(k;s)$ such that whenever $n \geq R_r(k;s)$ then for any r-coloring (coloring with r colors) of k element subsets of a set X of cardinality n (there are $\binom{n}{k}$ such subsets and each of them gets one of r colors) there exists an s-subset (subset with s elements) that is k-monochromatic (that is, all of its k element subsets are colored with the same color). We assume that $R_r(k;s)$ is the smallest number having the above property. We shall split the proof into two parts.

Remark. Note that $R_2(2;s) = R(s,s)$ with notation from the previous section.

Remark. Clearly $R_r(k;s) \geq s \geq k$, since in a set with less than k elements there are no $s \geq k$ element subsets.

Step 1. We shall reduce the theorem to the case $r=2$. To do this we shall prove the inequality

$$R_{r+1}(k;s) \leq R_r(k;R_2(k;s)).$$

Let us take a set X having at least $R_r(k;R_2(k;s))$ elements and let us color its k-subsets using $r+1$ colors $0,1,2,\ldots,r$. Our goal is to show that there is an s-subset of X being k-monochromatic. We now consider a new coloring where we treat 0 and 1 as one color. Since $|X| \geq R_r(k;R_2(k;s))$ from the definition of $R_r(k;R_2(k;s))$ there exists an $R_2(k;s)$-subset Y of X that is k-monochromatic in the new coloring. The k-subsets of Y are either monochromatic is the old coloring (if their color in the new coloring is one of the colors $2,3,\ldots,r$) or they may have two different colors in the old coloring (if their color in the new coloring is $0=1$). In the first case we are done as $R_2(k;s) \geq s$ and so we can choose our desired set to be any s-element subset of Y. In the second case the set Y is an $R_2(k;s)$-set having k-subsets colored using two colors $0,1$. By the definition of $R_2(k;s)$ the set Y contains an s-subset that is k-monochromatic, and we are done.

Step 2. To deal with the case $r=2$, for $k \leq r,b$ we define Ramsey number $R(k;r,b)$ to be the smallest number such that if $n \geq R(k;r,b)$ then every coloring of k-subsets of a set X with $|X|=n$ using two colors (red and blue), there either exists a k-red r-subset of X, or a k-blue b-subset of X. Note that $R(k;s,s) = R_2(k;s)$. We shall show that the numbers $R(k;r,b)$ are finite.

Remark. We again clearly have $R(k;r,b) \geq \min(r,b) \geq k$.

The existence of $R(k;r,b)$ is proved by induction on k inside which there is an induction on $r+b$, based on the inequality

$$R(k;r,b) \leq R(k-1;R(k,r-1,b),R(k;r,b-1))+1, \qquad r,b \geq k+1, k \geq 2.$$

Note that the number on the right hand side is well defined as from the above remark we have $R(k,r-1,b), R(k;r,b-1) \geq k > k-1$. This inequality cannot be used either when $k=1$, in which case $R(1;r,s) = r+s-1$ is clearly finite, or if one of the numbers r,b equals k, in which case $R(k;r,b)$ is also finite as $R(k;k,l) = R(k;l,k) = l$ for $l \geq k$.

We now prove the above inequality. Let X be a set with $|X| = R(k-1;R(k,r-1,b),R(k;r,b-1))+1$. Suppose k-subsets of X are colored red or blue. Our goal is to either find a k-red r-subset of X or a k-blue b-subset of X. Let $X' = X \setminus \{x\}$. Clearly $|X'| = R(k-1;R(k,r-1,b),R(k;r,b-1))$. Note that our coloring χ induces a coloring χ' of $(k-1)$-subsets of X' by $\chi'(A) = \chi(A \cup \{x\})$. Then there either exists a $(k-1)$-red $R(k;r-1,b)$-subset of X' or a $(k-1)$-blue $R(k;r,b-1)$-subset of X'. Without loss of generality we can assume that the first possibility holds.

Let Y be $(k-1)$-red $R(k;r-1,b)$-subset of X'. We are now going to use the definition of $R(k;r-1,b)$. If this subset contains a k-blue (in coloring χ) b-subset then we are done. Otherwise Y contains a k-red (in coloring χ) $(r-1)$-subset Z_0. Define $Z = Z_0 \cup \{x\}$. We will show that this set is an k-red r-subset (in coloring χ), which will finish the proof.

Let A be a k-subset of Z.

Case 1. If $x \in A$ then $A' = A \setminus \{x\}$ is a $(k-1)$-subset of $Z_0 \subseteq Y$ and since Y was $(k-1)$-red (in χ'), the set A' is red in χ', which means that $\chi(A) = \chi'(A')$ is red.

Case 2. If $x \notin A$, then $A \subseteq Z_0$, $|A| = k$, and since Z_0 is k-red, the set A is red.

1.10 Extremal graph theory

Theorem 14 (Mantel's theorem)**.** If a graph G on n vertices contains more than $n^2/4$ edges, then G contains a triangle.

Proof. Suppose $G = (V,E)$ has no triangle. Then for $\{x,y\} \in E$ we have $d(x) + d(y) \leq n$, where $d(x)$ is the degree of x. Thus, we have

$$n|E| \geq \sum_{\{x,y\} \in E} (d(x)+d(y)) = \sum_{x \in V} d(x)^2 \geq \frac{1}{n}\left(\sum_{x \in V} d(x)\right)^2 = \frac{4|E|^2}{n}.$$

Thus $|E| \leq \frac{n^2}{4}$. □

Theorem 15 (Turan's theorem)**.** If a graph $G = (V,E)$ on n vertices has no $(k+1)$-clique then $|E| \leq \left(1-\frac{1}{k}\right)\frac{n^2}{2}$.

Proof. Induction on n. For $n=1$ the assertion is trivial. Without loss of generality we can assume that G has a k-clique A (otherwise just add edges). Consider $B = V \setminus A$. The number of edges within A is $|E_A| = \binom{k}{2}$. The number of edges within B satisfies $|E_B| \leq \frac{1}{2}(1-\frac{1}{k})(n-k)^2$ by induction hypothesis. Now, each vertex of B has at most $k-1$ neighbors in A since otherwise we would have a $(k+1)$-clique

in G. Thus the number of edges between A and B satisfies $|E_{A,B}| \leq (n-k)(k-1)$. Putting these things together and using the identity $(1-\frac{1}{k})\frac{n^2}{2} = \binom{k}{2}(\frac{n}{k})^2$ yields

$$|E| = |E_A| + |E_B| + |E_{A,B}| \leq \binom{k}{2} + \frac{1}{2}\left(1-\frac{1}{k}\right)(n-k)^2 + (n-k)(k-1)$$
$$= \binom{k}{2} + \binom{k}{2}\left(\frac{n-k}{k}\right)^2 + (n-k)(k-1) = \binom{k}{2}\left(1+\frac{n-k}{k}\right)^2 = \binom{k}{2}\left(\frac{n}{k}\right)^2 = \left(1-\frac{1}{k}\right)\frac{n^2}{2}.$$

□

2 Geometric combinatorics

2.1 Equiangular lines

In this section we will prove an upper bound on the number of pairwise equiangular lines in $\mathbb{R}^n$.

Theorem 16. Suppose $v_1, \ldots, v_n$ are unit vectors in $\mathbb{R}^d$ such that there exists $\theta \in (0, \pi/2]$ for which $|\langle v_i, v_j \rangle| = \cos\theta$ for all $i \neq j$. Then $n \leq \binom{d+1}{2}$.

Before we give a prove of this theorem, we shall show the following lemma of independent interest.

Lemma 1 (Sylvester identity)**.** Suppose X is an $m \times n$ matrix and Y is an $n \times m$ matrix. Then

$$\det(I_m + XY) = \det(I_n + YX).$$

Here I_n stands for the $n \times n$ identity matrix.

Proof. Let us first observe that we have the identity

$$\begin{pmatrix} I_n & -Y \\ X & I_m \end{pmatrix} \cdot \begin{pmatrix} I_n & Y \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ X & XY + I_m \end{pmatrix}.$$

Thus

$$\det\left(\begin{pmatrix} I_n & -Y \\ X & I_m \end{pmatrix} \cdot \begin{pmatrix} I_n & Y \\ 0 & I_m \end{pmatrix}\right) = \det\begin{pmatrix} I_n & 0 \\ X & XY + I_m \end{pmatrix} = \det(XY + I_m)$$

Since $\det(AB) = \det(BA)$, the left hand side is the same as

$$\det\left(\begin{pmatrix} I_n & Y \\ 0 & I_m \end{pmatrix} \cdot \begin{pmatrix} I_n & -Y \\ X & I_m \end{pmatrix}\right) = \det\begin{pmatrix} I_n + YX & 0 \\ X & I_m \end{pmatrix} = \det(I_n + YX).$$

□

We are now ready to give a proof of Theorem 16.

Proof of Theorem 16. Let us consider $d \times d$ matrices $v_i v_i^T$. These matrices belong to a space of symmetric $d \times d$ matrices which is a space of dimension $\binom{d}{2} + d = \binom{d+1}{2}$. It is therefore enough to show that these matrices are linearly independent.

Let us therefore assume that $\sum_{i=1}^n \lambda_i v_i v_i^T = 0$. Thus we get

$$0 = v_k^T \left(\sum_{i=1}^n \lambda_i v_i v_i^T\right) v_k = \sum_{i=1}^n \lambda_i v_k^T v_i v_i^T v_k = \sum_{i=1}^n \lambda_i \langle v_i, v_k \rangle^2 = \lambda_k + \sum_{i \neq k} \lambda_i \cos^2\theta.$$

Let I_n denote the $n \times n$ identity matrix and let J_n denote the $n \times n$ matrix with all entries equal to 1. The above equation means that the vector $\lambda = (\lambda_1, \ldots, \lambda_n)$ satisfies $((1 - \cos^2\theta)I_n + J_n \cos^2\theta)\lambda = 0$. To deduce that $\lambda = 0$ we only need to show that $I_n \sin^2\theta + J_n \cos^2\theta$ is non-singular. Let $\mathbf{1}$ denote the vector in $\mathbb{R}^n$ with all entries equal to 1. Then $J_n = \mathbf{1}\mathbf{1}^T$. We now use the Sylvester identity to get that

$$\begin{aligned}\det(I_n \sin^2\theta + J_n \cos^2\theta) &= \sin^{2n}(\theta) \det\left(I_n + \frac{\cos^2\theta}{\sin^2\theta}\mathbf{1}\mathbf{1}^T\right) = \sin^{2n}(\theta) \det\left(I_1 + \frac{\cos^2\theta}{\sin^2\theta}\mathbf{1}^T\mathbf{1}\right) \\ &= \sin^{2n}(\theta) + n \sin^{2n-2}(\theta)\cos^2(\theta) \neq 0.\end{aligned}$$

□

2.2 Two distance problem

Suppose $v_1, \ldots, v_m \in \mathbb{R}^n$ are such that $|v_i - v_j| = 1$ for $i \neq j$. It is not hard to show that then $m \leq n+1$ and the equality is achieved by a standard simplex.

It is much harder to upper bound the cardinality of a set having only two possible distances between its points. To be more precise, $A \subset \mathbb{R}^n$ is called a *two distance set* if there exist two numbers $a, b > 0$ such that for any distinct $u, v \in A$ we have $|u - v| \in \{a, b\}$.

Theorem 17. Let $m(n)$ be the biggest possible cardinality of a two-distance set in $\mathbb{R}^n$. Then $\frac{1}{2}n(n+1) \leq m(n) \leq \frac{1}{2}(n^2 + 5n + 4)$.

Proof. The lower bound is easy and is left as an exercise. We shall prove the upper bound. Let $A = \{v_1, \ldots, v_m\}$ be a two-distance set with distances $a, b > 0$. Define

$$f_i(x) = (|x - v_i|^2 - a^2)(|x - v_i|^2 - b^2).$$

The functions $f_1, \ldots, f_m$ are multivariate polynomials in x. We first claim that these polynomials are linearly independent over $\mathbb{R}$. To see this suppose that

$$\alpha_1 f_1(x) + \alpha_2 f_2(x) + \ldots + \alpha_m f_m(x) = 0, \qquad \forall x \in \mathbb{R}^n.$$

Taking $x = v_j$ one gets $f_i(v_j) = 0$ for $i \neq j$ and $f_j(v_j) = a^2b^2 \neq 0$. Thus the above equation reduces to $\alpha_j a^2 b^2 = 0$, which gives $\alpha_j = 0$.

Since we proved that f_i are linearly independent, it is enough to show that they belong to a linear space of dimension at most $\frac{1}{2}(n^2 + 5n + 4)$. Note that

$$f_i(x) = |x - v_i|^4 - (a^2 + b^2)|x - v_i|^2 + a^2b^2.$$

We have

$$|x - v_i|^4 = (|x|^2 - 2\langle x, v_i\rangle + |v_i|^2)^2 = |x|^4 + 4\langle x, v_i\rangle^2 + |v_i|^4 - 4|x|^2\langle x, v_i\rangle + 2|x|^2|v_i|^2 - 4\langle x, v_i\rangle |v_i|^2.$$

This belongs to a space spanned by

$$1,\ |x|^4,\ |x|^2 x_i,\ x_i x_j,\ x_i \qquad i, j = 1, \ldots, n.$$

The function $-(a^2 + b^2)|x - v_i|^2 + a^2b^2$ belongs to the space spanned by

$$x_i x_j,\ x_i,\ 1 \qquad i, j = 1, \ldots, n.$$

Thus every f_i is in the span of functions

$$1,\ |x|^4,\ |x|^2 x_i,\ x_i x_j,\ x_i, \qquad i, j = 1, \ldots, n.$$

This is a collection of $1 + 1 + n + \left(\binom{n}{2} + n\right) + n = 2 + 3n + \frac{1}{2}n(n-1) = \frac{1}{2}(n^2 + 5n + 4)$ functions. □

2.3 Borsuk's conjecture

The celebrated Borsuk's conjecture was that every set X in $\mathbb{R}^d$ of finite diameter can be partitioned into $d+1$ subsets of smaller diameter. One can check that this is indeed true for an Euclidean ball and for the standard simplex. A partition with this property will be called a *diameter reducing partition*. Kahn and Kalai disproved Borsuks's conjecture. In this section we shall present their construction.

Theorem 18 (Kahn-Kalai)**.** For every prime number p there exists a set X in $\mathbb{R}^{d^2}$, where $d = 4p$, with no diameter reducing partition into fewer than 1.1^d parts.

Remark. We have $1.1^d > d^2 + 1$ for $d \geq 96$. Thus, we need $p \geq \frac{96}{4} = 24$ to get a counterexample to Borsuk's conjecture from the above theorem. Therefore one should choose $p = 29$, in which case $d = 116$. Thus the counterexample is constructed in $\mathbb{R}^{13456}$.

We shall prove yet another lemma concerning extremal combinatorics of set systems. This lemma will be crucial in the proof of Theorem 18.

Lemma 2. Let p be a prime number and let $\mathcal{F}$ be a family of $(2p-1)$-element subsets of an n-element set. Suppose that $|A \cap B| \neq p-1$ for $A \neq B$, $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}$.

Corollary 1. Let p be a prime number and let $\mathcal{F}$ be a family of $(2p-1)$-element subsets of an $n = 4p$ element set. Suppose that $|A \cap B| \neq p-1$ for $A \neq B$, $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \leq \frac{1}{1.1^n}\binom{n}{2p-1}$.

Remark. The number of $(2p-1)$-element subsets of an n-element set is $\binom{n}{2p-1}$. For each two distinct $(2p-1)$-element subsets of an n-element set one has $|A \cap B| \in \{0, 1, 2, \ldots, 2p-2\}$. Note that $p-1$ is the middle point of this set of numbers. The corollary says that for $n = 4p$ forbidding this middle size intersection forces the family to have much fewer than $\binom{n}{2p-1}$ elements.

Proof of Corollary 1. If $n \geq 4k$, $k \geq 1$ then

$$\binom{n}{k-1} = \frac{n!}{(n-k+1)!(k-1)!} = \frac{k}{n-k+1} \cdot \frac{n!}{(n-k)!k!} = \frac{k}{n-k+1}\binom{n}{k} \leq \frac{k}{4k-k+1}\binom{n}{k} \leq \frac{1}{3}\binom{n}{k}.$$

Thus for $k = 0, 1, \ldots, p-1$ we have $\binom{n}{k} \leq \frac{1}{3^{p-k}}\binom{n}{p}$. Applying Lemma 2 leads therefore to

$$|\mathcal{F}| \leq \left(\frac{1}{3^p} + \frac{1}{3^{p-1}} + \ldots + \frac{1}{3}\right)\binom{n}{p} < \frac{1}{3} \cdot \frac{1}{1-\frac{1}{3}}\binom{n}{p} = \frac{1}{2}\binom{n}{p}.$$

We get

$$\begin{aligned}\frac{\binom{n}{2p-1}}{|\mathcal{F}|} &\geq 2\frac{\binom{n}{2p-1}}{\binom{n}{p}} = 2 \cdot \frac{p!}{(2p-1)!} \cdot \frac{(n-p)!}{(n-2p+1)!} = 2 \cdot \frac{p!}{(2p-1)!} \cdot \frac{(3p)!}{(2p+1)!} \\ &= 2 \cdot \frac{3p(3p-1)\ldots(2p+2)}{(2p-1)(2p-2)\ldots(p+1)} = 2 \cdot \frac{3p}{2p-1} \cdot \frac{3p-1}{2p-2} \cdot \ldots \cdot \frac{2p+2}{p+1}.\end{aligned}$$

Since $\frac{3p-k}{2p-1-k} \geq \frac{3}{2}$ for $k = 0, 1, \ldots, p-2$, we get

$$\frac{\binom{n}{2p-1}}{|\mathcal{F}|} \geq 2 \cdot \left(\frac{3}{2}\right)^{p-1} = \frac{4}{3} \cdot \left(\frac{3}{2}\right)^{p} = \frac{4}{3} \cdot \left(\frac{3}{2}\right)^{n/4} > \left(\frac{3}{2}\right)^{n/4} = \left(\sqrt[4]{\frac{3}{2}}\right)^{n} > 1.1^n.$$

□

Proof of Lemma 2. We can assume that the underlying set in $\{1,\ldots,n\}$. We shall work over the field $\mathbb{Z}_p$. For $A \in \mathcal{F}$ let $\mathbf{1}_A \in \{0,1\}^n$ be its incidence vector, that is the vector whose ith coordinate is 1 if and only if $i \in A$. Consider $f_A : \{0,1\}^n \to \mathbb{Z}_p$ given by

$$f_A(x) = \prod_{k=0}^{p-2} \left(\left(\sum_{i \in A} x_i \right) - k \right),$$

where the values are taken modulo p. Let $V = \{f : \{0,1\}^n \to \mathbb{Z}_p\}$ be the space of all functions on $\{0,1\}^n$ having values in $\mathbb{Z}_p$. We treat V as a vector space over $\mathbb{Z}_p$ (for arbitrary X the space $\{f : X \to \mathbb{Z}_p\}$ can be treated as a vector space over $\mathbb{Z}_p$). Let $V_{\mathcal{F}} = \operatorname{span}\{f_A, A \in \mathcal{F}\}$. It is enough to prove the following two claims.

Claim 1. The vectors f_A for $A \in \mathcal{F}$ are linearly independent. Thus $\dim(V_{\mathcal{F}}) = |\mathcal{F}|$.

Claim 2. We have $\dim(V_{\mathcal{F}}) \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}$.

Proof of Claim 1. Note that

$$f_A(\mathbf{1}_A) = \prod_{k=0}^{p-2}(|A| - k) = \prod_{k=0}^{p-2}(2p-1-k) = \prod_{k=0}^{p-2}(2p-1-k) = (-1)^{p-1}\prod_{k=0}^{p-2}(k+1) = (-1)^{p-1}(p-1)! \neq 0,$$

where the last but one equality follows from the fact that we work in $\mathbb{Z}_p$. If now $A \neq B$ then $f_A(\mathbf{1}_B) = \prod_{k=0}^{p-2}(|A \cap B| - k) = 0$ as $|A \cap B| \mod p \in \{0,1,2,\ldots,p-2\}$ since $|A \cap B| \neq p-1$ by our assumption. If we now evaluate the equality $\sum_{B \in \mathcal{F}} \lambda_B f_B = 0$ on $\mathbf{1}_A$ we shall get $\lambda_A(p-1)! = 0$ and thus $\lambda_A = 0$. This proves the desired independence of the elements f_A. □

Proof of Claim 2. The function f_A is clearly a linear combination of monomials $x_1^{j_1} \ldots x_n^{j_n}$ with $j_1 + \ldots j_n \leq p-1$ (as it is a product of $p-1$ linear function). But since for $j_i \neq 0$ and $x_i \in \{0,1\}$ we have $x_i^{j_i} = x_i$ we actually see that f_A is a linear combination of monomials $x_1^{j_1} \ldots x_n^{j_n}$ with $j_1, \ldots, j_n \in \{0,1\}$ and $j_1 + \ldots + j_n \leq p-1$. There are exactly $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}$ such monomials. Let V' be the space spanned by these monomials. We have $V_{\mathcal{F}} \subseteq V'$ and thus $\dim(V_{\mathcal{F}}) \leq \dim(V') \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}$. □

The proof of Lemma 2 is completed. □

We are now ready to prove Theorem 18.

Proof of Theorem 18. Let p be a prime number, $d = 4p$ and let $\mathcal{A}$ be the family of all $(2p-1)$-element subsets of $\{1,\ldots,d\}$. For $A \in \mathcal{A}$ w define $u_A \in \mathbb{R}^d$ via $u_A = 2\mathbf{1}_A - \mathbf{1}$, where $\mathbf{1}_A$ is the usual incidence vector of A and $\mathbf{1} = \mathbf{1}_{\{1,\ldots,d\}}$ is the vector with all entries equal 1. We will show that $X = \{u_A \otimes u_A : A \in \mathcal{A}\}$ is the desired set in $\mathbb{R}^{d^2}$. Recall that for $u \in \mathbb{R}^{d_1}$ and $v \in \mathbb{R}^{d_2}$, $u \otimes v$ is the $d_1 \times d_2$ matrix with entries $(u_i v_j)_{i \leq d_1, j \leq d_2}$. Of course every $d_1 \times d_2$ matrix can be treated, in a natural way, as an element of $\mathbb{R}^{d_1 d_2}$.

Fact. For any $x_1, y_1 \in \mathbb{R}^{d_1}$ and $x_2, y_2 \in \mathbb{R}^{d_2}$ we have $x_1 \otimes x_2 \in \mathbb{R}^{d_1 d_2}$, $y_1 \otimes y_2 \in \mathbb{R}^{d_1 d_2}$ and $\langle x_1 \otimes x_2, y_1 \otimes y_2 \rangle = \langle x_1, y_1 \rangle \langle x_2, y_2 \rangle$, where the scalar product $\langle \cdot, \cdot \rangle$ is the standard scalar product in $\mathbb{R}^{d_1 d_2}$.

Proof of the Fact. For $x \in \mathbb{R}^d$ let $x^{(i)}$ be the ith coordinate of x. We have

$$\langle x_1 \otimes x_2, y_1 \otimes y_2 \rangle = \sum_{i \leq d_1, j \leq d_2} x_1^{(i)} x_2^{(j)} y_1^{(i)} y_2^{(j)} = \left(\sum_{i \leq d_1} x_1^{(i)} y_1^{(i)} \right) \left(\sum_{j \leq d_1} x_2^{(j)} y_2^{(j)} \right) = \langle x_1, y_1 \rangle \langle x_2, y_2 \rangle .$$

□

We continue the proof of Theorem 18. Note that

$$\begin{aligned}\langle u_A, u_B\rangle &= \langle 2\mathbf{1}_A - \mathbf{1}, 2\mathbf{1}_B - \mathbf{1}\rangle = 4|A\cap B| - 2|A| - 2|B| + d\\ &= 4|A\cap B| - 4(2p-1) + 4p = 4|A\cap B| - 4p + 4 = 4(|A\cap B| - p + 1).\end{aligned}$$

In particular, $\langle u_A, u_A\rangle = 4(2p-1-p+2) = 4p = d$. Moreover, $\langle u_A, u_B\rangle = 0$ if and only of $|A\cap B| = p-1$. Let $q_A = u_A \otimes u_A$. Then by the Fact

$$|q_A - q_B|^2 = \langle q_A, q_A\rangle + \langle q_B, q_B\rangle - 2\langle q_A, q_B\rangle = \langle u_A, u_A\rangle^2 + \langle u_B, u_B\rangle^2 - 2\langle u_A, u_B\rangle^2 = 2d^2 - 2\langle u_A, u_B\rangle^2.$$

Since $\langle u_A, u_B\rangle^2 \geq 0$ with equality if and only if $|A\cap B| = p-1$. Thus, the diameter of X is $2d^2$ and any subset X' of X has diameter $2d^2$ as long as it contains two points q_A, q_B such that $|A\cap B| = p-1$.

Suppose now we partition X into fewer than 1.1^d parts. Then one of the parts X' of X is of size greater than $\frac{1}{1.1^d}|\mathcal{A}| = \frac{1}{1.1^d}\binom{d}{2p-1}$. Then by Corollary 1 X' is too big to satisfy $|A\cap B| \neq p-1$ for all its distinct members A, B. So X' has two elements A, B satisfying $|A\cap B| = p-1$. Thus the diameter of X' equals the diameter of X. As a consequence our partition is not diameter reducing.

□

3 The polynomial method

3.1 Combinatorial Nullstellensatz

Theorem 19 (N. Alon)**.** Let $\mathbb{F}$ be an arbitrary field and let $P(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Suppose that the degree of P is $\sum_{i=1}^n k_i$, where each k_i is a non-negative integer and suppose that the coefficient of $x_1^{k_1}\cdot\ldots\cdot x_n^{k_n}$ is non-zero. Then for any subsets $A_1, \ldots, A_n$ of $\mathbb{F}$ satisfying $|A_i| \geq k_i + 1$ for all $i = 1, \ldots, n$, there exist $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.

Proof. We present the proof of Michałek, see [M]. We proceed by induction on $\deg(P)$. If $\deg(P) = 0$ then our assertion is trivial (P is a non-zero constant). Suppose that $\deg(P) > 1$ and P satisfies the assumptions of the theorem but the assertion is false, that is $P(x) = 0$ for every $x \in A_1 \times \cdots \times A_n$. Without loss of generality we assume that $k_1 > 0$. Fix $a \in A_1$. There exist polynomials $Q \in \mathbb{F}[x_1, \ldots, x_n]$ and $R \in \mathbb{F}[x_2, \ldots, x_n]$ such that

$$P = (x_1 - a)Q + R. \tag{1}$$

Note that $\deg(Q) = \deg(P) - 1$ and that Q has a non-vanishing monomial of the form $x_1^{k_1-1}x_2^{k_2}\cdot\ldots\cdot x_n^{k_n}$. Take any $x \in \{a\} \times A_2 \times \cdots \times A_n$. Since $P(x) = 0$ we obtain $R(x) = 0$. However, R does not contain x_1, thus $R(x) = 0$ for all $x \in (A_1\backslash\{a\}) \times A_2 \times \cdots \times A_n$. Take such an x and substitute it to (1). Since $x_1 - a$ is non-zero and $P(x) = R(x) = 0$ we obtain $Q(x) = 0$. So, $\deg(Q) = \deg(P) - 1$, Q contains a monomial $x_1^{k_1-1}x_2^{k_2}\cdot\ldots\cdot x_n^{k_n}$ and Q vanishes on the set $(A_1\backslash\{a\}) \times A_2 \times \cdots \times A_n$, where $|A_1\backslash\{a\}| \geq k_1, |A_2| \geq k_2 + 1, \ldots, |A_n| \geq k_n + 1$. This contradicts the inductive assumption. □

Theorem 20 (N. Alon, Z. Füredi, [AF, A])**.** Suppose that the hyperplanes $H_1, \ldots, H_m \subset \mathbb{R}^n$ cover the set $\{0,1\}^n\backslash\{0\}$ and that $0 \notin \bigcup_{i=1}^m H_i$. Prove that $m \geq n$.

Proof. Suppose that the hyperplane H_i is given by the equation $\langle a_i, x\rangle = b_i$. We have $b_i \neq 0$ since H_i does not cover the origin. Assume that our assertion is false and $m < n$. Define the following polynomial,

$$P(x) = (-1)^{n+m+1}\left(\prod_{j=1}^m b_j\right)\prod_{i=1}^n (x_i - 1) + \prod_{i=1}^m \left(\langle a_i, x\rangle - b_i\right).$$

The degree of this polynomial is n and the coefficient of $\prod_{i=1}^n x_i$ is $(-1)^{n+m+1}\prod_{j=1}^m b_j \neq 0$. Therefore, from part a) there exists $x_0 \in \{0,1\}^n$ such that $P(x_0) \neq 0$. This point is not the origin since clearly $P(0) = 0$. Therefore, in x_0 the polynomial $\prod_{j=1}^n (x_i - 1)$ vanishes and thus

$$P(x_0) = \prod_{i=1}^m (\langle a_i, x_0\rangle - b_i) \neq 0.$$

It means that $\langle a_i, x_0\rangle \neq b_i$ for all $i = 1, \ldots, m$ and therefore $x_0 \notin \bigcup_{i=1}^m H_i$. This is a contradiction. □

3.2 Chevalley-Warning theorem

Theorem 21. Let p be a prime number. Suppose $P_1, \ldots, P_m \in \mathbb{Z}_p[x_1, \ldots, x_n]$ and assume that $n > \sum_{i=1}^m \deg(P_i)$. Assume also that $P_1, \ldots, P_m$ have a common zero $(c_1, \ldots, c_n)$. Then these polynomials have another common zero.

Proof. Proof by N. Alon, [A]. Assume that the assertion is not true. Define

$$Q(x_1, \ldots, x_n) = \prod_{i=1}^m \left(1 - P_i(x_1, \ldots, x_n)^{p-1}\right) - \delta \prod_{j=1}^n \prod_{c \in \mathbb{Z}_p, c \neq c_j} (x_j - c),$$

where δ is chosen so that $Q(c_1, \ldots, c_n) = 0$, that is, $\delta = \left(\prod_{c \in \mathbb{Z}_p, c \neq c_j} (c_j - c)\right)^{-1} \neq 0$ (recall that P_i vanish in $(c_1, \ldots, c_n)$). We claim that $Q \equiv 0$. We already know that $Q(c_1, \ldots, c_n) = 0$. If $(x_1, \ldots, x_n) \neq (c_1, \ldots, c_n)$ then from the fact that P_i do not have a common zero other than $(c_1, \ldots, c_n)$ we get that there exists i such that $P_i(x_1, \ldots, x_n) \neq 0$ and thus $P_i(x_1, \ldots, x_n)^{p-1} = 1$ (Fermat's little theorem – recall that we work in $\mathbb{Z}_p$). Thus the first product in the definition of Q vanishes. The other product also vanishes since there exists x_j such that $x_j \neq c_j$ and so for this j we have $\prod_{c \in \mathbb{Z}_p, c \neq c_j} (x_j - c) = 0$ (since $c = x_j$ is allowed in this product as $x_j \neq c_j$). We have proved the claim that $Q \equiv 0$.

Now, observe that the degree of $\prod_{i=1}^m (1 - P_i(x_1, \ldots, x_n)^{p-1})$ is $(p-1)\sum_{i=1}^m \deg(P_i) < (p-1)n$. Moreover the degree of $\delta \prod_{j=1}^n \prod_{c \in \mathbb{Z}_p, c \neq c_j} (x_j - c)$ is precisely $(p-1)n$ (recall that $\delta \neq 0$) and the highest degree monomial is $\delta \cdot x_1^{p-1} \ldots x_n^{p-1}$. Since $|\mathbb{Z}_p| = p$, from Theorem 19 we get that Q cannot be identically zero, contradiction. □

We now use the Chevalley-Warning theorem to prove the following combinatorial fact.

Theorem 22. Suppose p is a prime number and $G = (V, E)$ is a $(2p-1)$-regular graph. Then there exists a p-regular subgraph $G' = (V', E')$ of G (a graph obtained by deleting certain vertices from V together with adjacent edges, and certain edges from E).

Proof. To every edge $\{i, j\} \in E$ we associate a variable $x_{ij} \in \mathbb{Z}_p$. Once the numbers x_{ij} are chosen, we can define a subgraph $G' = (V, E')$ by taking $\{i, j\} \in E'$ if and only if $x_{ij} \neq 0$. Let $\deg(i, G')$ be the degree of the vertex i in G'. Note that in $\mathbb{Z}_p$ we have

$$\deg(i, G') = \sum_{j:\ \{i,j\} \in E} x_{ij}^{p-1},$$

since if $x_{ij} = 0$ then $\{i, j\} \notin E'$ and the contribution to the above sum is zero, and if $x_{ij} \neq 0$ then $\{i, j\} \in E'$ and by Fermat's little theorem we have $x_{ij}^{p-1} = 1$ in $\mathbb{Z}_p$, so the contribution to the above sum is one.

Note that $P_i = \deg(i, G')$ is a polynomial in the variables x_{ij}. The system of equations $\det(i, G') = 0$ has a trivial solution (P_i have a trivial common zero), that is, $x_{ij} = 0$ for all $\{i, j\} \in E$. We claim that

it is enough to find a non-trivial solution to this system of equations (non-trivial common zero of P_i). Indeed, suppose in $\mathbb{Z}_p$ we have $\deg(i, G') = 0$ for all $i \in V$ and that at least one of the variables x_{ij} is non-zero. This means that for all i we have $p | \deg(i, G')$, so in $\mathbb{Z}$ we have $\deg(i, G') = 0$ or $\deg(i, G') = p$ (note that $\deg(i, G') \leq 2p - 1$). If for some i we have $\deg(i, G') = 0$ then the vertex i is isolated in G'. In this case we delete it from G'. We are left with a connected graph whose vertices have degree p. This graph is non-empty, since at least one of the variables x_{ij} was non-zero, which corresponds to a non-isolated vertex in G'.

To find a non-trivial common root of P_i it suffices to use the Chevalley-Warning theorem with $(c_1, \ldots c_n) = (0, \ldots, 0)$. The number of variables x_{ij} (call it n) is precisely $\frac{1}{2}(2p-1)|G|$ since every vertex in G has degree $2p - 1$. We have

$$n = \frac{1}{2}(2p-1)|G| > (p-1)|G| = \sum_i \deg(P_i),$$

so the assumptions of the Chevalley-Warning theorem are satisfied. □

3.3 Graham Pollak theorem

We now want to answer the following question: what is the smallest m such that the clique on n vertices K_n can be decomposed into m edge-disjoint complete bipartite graphs? A graph is complete bipartite if its set of vertices is $A \cup B$ with $A \cap B = \emptyset$ and the edges is the set $A \times B$ (all possible edges going from A to B).

Clearly $m \leq n - 1$, since we can always decompose $K_n = \{1, \ldots, n\}$ into complete bipartite graphs $(A_1, B_1), \ldots (A_{n-1}, B_{n-1})$ where $A_i = \{i\}$ and $B_i = \{i+1, \ldots, n\}$. Graham and Pollak showed 1971 that this is the best possible. We present a beautiful proof of Tverberg from 1982.

Theorem 23. (Graham-Pollak) Suppose the clique K_n is decomposed into m edge-disjoint bipartite graphs. Then $m \geq n - 1$.

Proof. To every vertex i of K_n let us associate a real variable x_i. Let us consider the polynomial $S(x) = \sum_{1 \leq i < j \leq n} x_i x_j$. Suppose we have decomposed K_n into complete bipartite graphs $(A_1, B_1), \ldots (A_m, B_m)$. Let $a_i(x) = \sum_{j \in A_i} x_j$ and $b_i(x) = \sum_{j \in B_j} x_j$. Every product $x_i x_j$ corresponds to an edge of K_n. Clearly

$$S(x) = \sum_{i=1}^{m} \sum_{j \in A_i, k \in B_i} x_j x_k = \sum_{i=1}^{m} \left(\sum_{j \in A_i} x_j \right) \left(\sum_{j \in B_j} x_j \right) = \sum_{i=1}^{m} a_i(x) b_i(x).$$

Thus

$$\sum_{i=1}^{n} x_i^2 = \left(\sum_{i=1}^{n} x_i \right)^2 - 2S(x) = \left(\sum_{i=1}^{n} x_i \right)^2 - 2 \sum_{i=1}^{m} a_i(x) b_i(x). \tag{2}$$

Consider the system of $m + 1$ linear equations $a_1(x) = 0, \ldots, a_m(x) = 0$, $x_1 + \ldots + x_n = 0$. Assume that $m \leq n - 2$. Then the number of equations is at most $n - 1$ and thus (basic linear algebra) this system has a solution $x \neq 0$, $x \in \mathbb{R}^n$. Plugging this x into (2) gives a contradiction, since the left hand side is positive whereas the right hand side vanishes. □

4 Elements of graph theory

4.1 Eulerian graphs

We say that a graph G is *Eulerian* if it contains an *Eulerian cycle*, that is, a cycle $v_1 \to v_2 \to \ldots \to v_n \to v_1$ that visits every **edge** exactly once. We prove the following well-known theorem.

Theorem 24. A connected graph G is Eulerian if and only of the degree of every vertex is even.

We first prove the following simple lemma.

Lemma 3. Suppose that the degree of every vertex in graph G is at least 2. Then G contains a cycle (with non-repeated edges and vertices).

Proof. We can assume that G has no loops and no multiple edges, since otherwise the result is trivial. Now, start with any vertex v_0 of G and in the first step go to one of the neighbors v_1 of v_0. Then from v_1 we go to a vertex $v_2 \neq v_0$, which is possible since the degree of v_1 is at least 2. For $i \geq 2$ in the ith step we go from v_{i-1} to $v_i \neq v_{v-2}$. Since G has finitely many vertices, at some point we will choose a vertex that has been chosen before. In this way we construct a path $v_0 \to v_1 \to \ldots \to v_k \to v_{k+1} \to \ldots \to v_n \to v_k$, where v_i are different. Then $v_k \to v_{k+1} \to \ldots \to v_n \to v_k$ is the desired cycle. □

Proof of Theorem 24. If G has an Eulerian cycle then clearly every vertex has an even degree (whenever we enter a vertex we have to leave it).

The proof of the harder implication goes via the induction on the number of edges, with a trivial base case. Suppose G is a connected graph. Since every vertex has even degree, it follows that every vertex has degree at least 2 and thus from Lemma 3 the graph G contains a cycle C. If $G = C$ then we are done. Otherwise remove edges (keep vertices) of C from G. The resulting graph H may have several connected components $H_1, \ldots, H_n$. Each component H_i has at least one vertex in common with C (otherwise G would not be connected). Moreover, the degree of every vertex in each connected component is still even (we have only changed the degrees of vertices on C and these degree decreased by 2). From induction hypothesis each H_i has an Eulerian cycle. The Eulerian cycle in G is constructed as follows. Take any vertex of v in C. Follow the edges of C until we reach the first non-isolated connected component H_{i_1} and vertex v_1. We then follow the Eulerian cycle in H_{i_1} which returns to v_1. We then continue tracing C until we reach the second connected component H_{i_2} at a vertex v_2. We then follow the Eulerian cycle in H_{i_2}. If we continue this procedure we shall finally reach v and close the cycle. □

4.2 Hamiltonian graphs

We say that G is *Hamiltonian* if G contains a cycle that visits every vertex exactly once. Note that in such a cycle the edges are also not repeated.

It turns out that not much is known about Hamiltonian graphs. In particular, no simple description (similar to the one presented for Eulerian graphs) is known. Here we give a simple sufficient condition for a graph to have a Hamiltonian cycle.

Theorem 25 (Ore, 1960)**.** Suppose a simple graph (no loops, no multiple edges) with $n \geq 3$ vertices satisfies $\deg(u) + \deg(v) \geq n$ for every pair of non-adjacent vertices u, v in G. Then G has a Hamiltonian cycle.

Proof. Suppose, by contradiction, that G has no Hamiltonian cycle. Then by adding edges to G (which will not violate the assumptions of the lemma), we can assume that G is *almost Hamiltonian*, that is, that adding any further vertex will create a Hamiltonian graph.

It follows that there is a path $v_1 \to v_2, \ldots \to v_n$ visiting all the vertices of G. This path is constructed from the Hamiltonian cycle $v_1 \to \ldots v_n \to v_1$ that would occur if we add an arbitrary edge (here the edge $v_n \to v_1$) to G. The above path is obtained by removing the edge $v_n \to v_1$ from the cycle and thus existed in G before adding $v_n \to v_1$.

Since G is not Hamiltonian, the vertices v_1, v_n are non-adjacent and thus $\deg(v_1, v_n) \geq n$. We now claim that there is a pair of vertices v_{i-1}, v_i such that in G there is an edge connecting v_1 and v_i and an edge connecting v_n and v_{i-1}. Indeed suppose this is not true and that there are, precisely k vertices

$v_{i_1}, \ldots, v_{i_k}$ from the set $\{v_3, \ldots, v_{n-1}\}$ adjacent to v_1. Then $v_{i_1-1}, \ldots, v_{i_k-1} \subseteq \{v_2, \ldots, v_{n-2}\}$ cannot be neighbors of v_n. Thus there are only $n-3-k$ possible neighbors of v_n in $\{v_2, \ldots, v_{n-2}\}$. Together with v_{n-1} the vertex v_n can have at most $n-2+k$ neighbors. The vertex v_1 has $k+1$ neighbors (note that v_2 is a neighbor of v_1 and v_n is not). Altogether we have $n \leq \deg(v_1)+\deg(v_n) \leq (n-2+k)+(k+1) = n-1$. This is a contradiction.

One we proved our claim it is now straightforward to construct the desired Hamiltonian cycle. This is the cycle $v_1 \to v_2 \to \ldots v_{i-1} \to v_n \to v_{n-1} \to \ldots \to v_i \to v_1$. □

Corollary 2 (Dirac, 1952)**.** Suppose a simple graph (no loops, no multiple edges) with $n \geq 3$ vertices satisfies $\deg(v) \geq n/2$ for every vertex v in G. Then G has a Hamiltonian cycle.

4.3 Trees

4.4 Planar graphs

Planar graphs are graphs that can be drawn on the plane with no edge intersections. Of course a planar graph can have many different drawings, see Figure 1. On the other hand there are graphs that are non-planar. Two most basic examples of such graphs in the clique K_5 and the complete bipartite graph $K_{3,3}$, see Figure 1.

Figure 1: On the left: K_4 and its two different drawings. On the right: $K_{3,3}$ and K_5 that are not planar.

In fact, in some sense every non-planar graph has to contain a copy of either K_5 or $K_{3,3}$. To make it more precise, we say that two graphs are *homeomorphic* if they can be obtained from a certain graph by adding vertices of degree 2 on the edges of this graph, see Figure 2

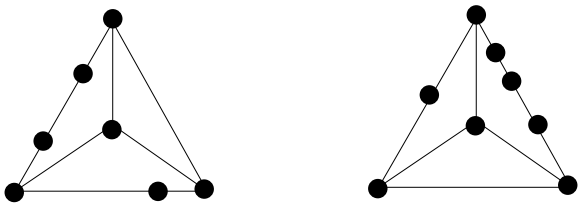


Figure 2: Two homeomorphic graphs obtained from K_4.

Note that a subgraph of a planar graph must also be planar. The following famous theorem gives a characterization of planarity. We shall not prove this theorem in these notes.

Theorem 26 (Kuratowski, 1930)**.** A graph G is planar if and only if it does not have a subgraph homeomorphic to K_5 or $K_{3,3}$.

For every drawing of a planar graph we get a set of vertices, edges and faces, see Figure 3.
Note that every drawing of a finite graph has an inifinite "outer" face. In fact by using the inverse of the stereographic projection we can think of a drawing of a planar graph on a surface of a sphere. The infinite face corresponds to the face that contains the "north pole" of the sphere. If we rotate the sphere and project the graph again onto the plane, we shall see that every face can be chosen as the outer face.

We shall now prove the famous Euler's formula.

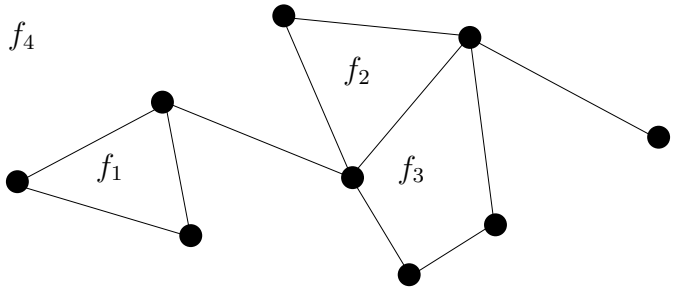


Figure 3: A drawing of a planar graph with 4 faces. The face f_4 is infinite.

Theorem 27. Suppose that in a drawing of a planar connected graph G there are v vertices, e edges and f faces. Then $v - e + f = 2$.

Proof sketch. Induction on e. If $e = 0$ then $v = 1$ and $f = 1$ (we only have the outer face), so the formula holds true. Suppose now that we are give a graph G with e edges. If G has no cycle, then it is a tree and thus $e = v - 1$ and $f = 1$, so the formula is valid. Let us therefore assume that G has a cycle. Removing an edge from this cycle creates a graph G' with $v' = v$ vertices, $e' = e - 1$ edges and $f' = f - 1$ faces (this operation joins two faces together). Note also that since the edge was removed from a cycle, the resulting graph G' is still connected (if the removed edge E was a part of a path joining two vertices, then we still create a path by using the rest of the cycle whenever the original path uses E). The assertion follows from the induction hypothesis, since $v - e + f = v' - (e' + 1) + (f' + 1) = v' - e' + f' = 2$. □

By projecting a convex polytope onto the sphere S^2 and then onto the plane using stereographic projection we get the following corollary.

Corollary 3. Suppose that a convex polytope in $\mathbb{R}^3$ has v vertices, e edges and f faces. Then we have $v - e + f = 2$.

Corollary 4. Suppose G is a simple connected planar graph with $v \geq 3$ vertices and e edges. Then

(i) $e \leq 3v - 6$

(ii) if additionally G has no triangles, then $e \leq 2v - 4$.

Proof. (i) If G has no cycles then it is a tree and thus $e = v - 1$ and so $v - 1 \leq 3v - 6$ is equivalent to $v \geq 3$. If G has at least one finite face, then the boundary of every face (including the outer face) consists of at least 3 edges (note that for a tree with $v = 2, 3$ vertices this is not true for the outer face). Since every edge belongs to the boundary of at most 2 faces, we deduce that $3f \leq 2e$ (every face uses 3 edges and the total number of "uses" is at most $2e$). From the Euler's formula we get $3e = 3(v + f - 2) = 3v + 3f - 6 \leq 3v + 2e - 6$. Rearranging gives $e \leq 3v - 6$.

(ii) The assertion for trees is equivalent to $v - 1 \leq 2v - 4$ which holds true for $v \geq 3$. If G has at least one cycle, then the boundary of every face (including the outer face) consists of at least 4 edges and thus $4f \leq 2e$. Thus $4e = 4(v + f - 2) = 4v + 4f - 8 \leq 4v + 2e - 8$. Rearranging yields $e \leq 2v - 4$. □

Corollary 5. The graphs K_5 and $K_{3,3}$ are non-planar.

Proof. If K_5 was planar, from Corollary 4(i) we would get $10 = e \leq 3v - 6 = 9$, contradiction. If $K_{3,3}$ was planar, from Corollary 4(ii) we would get $9 = e \leq 2v - 4 = 8$, contradiction (note that $K_{3,3}$ contains no triangle). □

Corollary 6. Every simple planar graph G contains a vertex of degree at most 5.

Proof. We can assume that G is connected (otherwise, pass to a connected component). We can clearly assume that the number of vertices is at least 3 (otherwise the assertion is trivial). Suppose that every vertex has degree at least 6. Then $2e = \sum_{v \in G} \deg(v) \geq 6v$. Thus $e \geq 3v$. On the other hand from Corollary 4(i) we get $e \leq 3v - 6$, contradiction. □

We conclude this chapter by proving the so-called 5-color theorem. The same result holds true with 5 replaced with 4, but has a very complicated proof.

Theorem 28. Let G be a simple planar graph. Then the vertices of G can be colored using 5 colors in such a way that no two adjacent vertices receive the same color.

Proof sketch. Induction on the number of vertices. If the number of vertices is at most 5, the assertion is trivial. To do the induction step note that from Corollary 6 there exists a vertex v of degree at most 5. Remove this vertex together with adjacent edges and color $G' = G \setminus \{v\}$ using induction hypothesis. If v had less that 5 neighbors then one of the colors is still available for v and we are done. Thus we can assume that there are 5 neighbors $v_1, \ldots, v_5$ of v (drawn is a clockwise order around v) in G and that they all received different colors (say, v_i received color i).

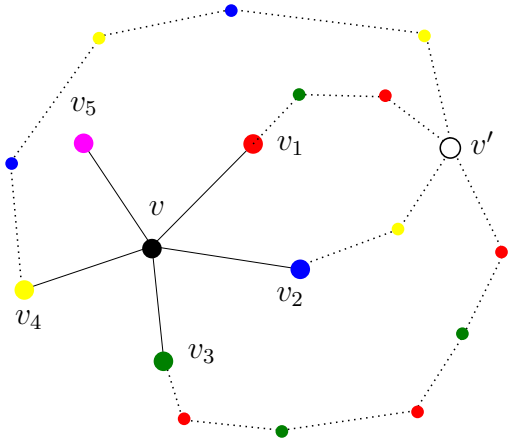


Figure 4: The red-green path have to intersect the blue-yellow path.

Now, let G_{ij} be the subgraph of G' induced by the vertices with colors i and j. Let C be the connected component of G_{13} containing v_1. Note that we can exchange colors in C and still get a valid coloring of G'. If C does not contain v_3 then after applying this operation the color 1 is available for v and we are done. Otherwise there is a path P_{13} from v_1 to v_3 with alternating colors 1 and 3. We repeat the same reasoning for the pair of colors 2 and 4 and we succeed whenever there is no path P_{24} from v_2 to v_4 with alternating colors 2 and 4. Otherwise we get a contradiction, since the paths P_{13} and P_{24} have to intersect in a vertex v' (the graph is planar, no edge intersections are allowed), which then has to have a color from the set $\{1, 3\} \cap \{2, 4\} = \emptyset$ (see Figure 4). □

4.5 Networks

We introduce the following definitions an notation.

- A pair (V, E), where V is a finite set and $E \subseteq V \times V$, is called a **directed graph**. An element $(x, y) \in E$ will be called a **directed edge** from x to y.
- We shall say that y is reachable from x if there is a path from x to y following directed edges.

- A triple (V, E, c) is called a **network** if (V, E) is a directed graph and $c : E \to [0, \infty)$ is some non-negative function on edges. The quantity $c(x, y)$ (we shall write like this instead of $c((x, y))$ for simplicity) will be called the **capacity** of the edge (x, y).
- Let (V, E, c) be a network. Take two distinct points $s, t \in V$. For a function $f : E \to [0, \infty)$ and $x \in V$ we define $f_+(x) = \sum_{y:(x,y)\in E} f(x, y)$ and $f_-(x) = \sum_{y:(y,x)\in E} f(y, x)$. A function $f : E \to [0, \infty)$ is called a **flow** from s to t if

  (i) $f(e) \leq c(e)$ for every $e \in E$,

  (ii) for every $x \notin \{s, t\}$ we have $f_+(x) = f_-(x)$ (Kirchhoff's law),

  (iii) we have $f_+(s) - f_-(s) > 0$ and $f_+(t) - f_-(t) < 0$. The vertex s is called the **source** and t is called the **sink**. Note that there might be some ingoing edges to s and some outgoing edges from t. The quantity $f_+(s) - f_-(s)$ will be called the **value** of f and will be denoted by $|f|$.
- For a flow f and subsets $A, B \subseteq V$ we define $f(A, B) = \sum_{(a,b)\in(A\times B)\cap E} f(a, b)$.
- A flow f is called **maximum** if $|f| = \max_{f'} |f'|$ where the maximum is taking over all flows. Note that the maximum is attained due to an easy compactness argument.
- For a network (V, E, c) and a pair of vertices $s, t \in V$ a **cut** is a subset $\Pi \subseteq E$ such that removing edges E' from E gives a directed graph in which t is not reachable from t. The **capacity** of the cut Π is $C(\Pi) = \sum_{e\in\Pi} c(e)$. The cut is called **minimum** if it has the minimal value of $C(\Pi)$ among all cuts.

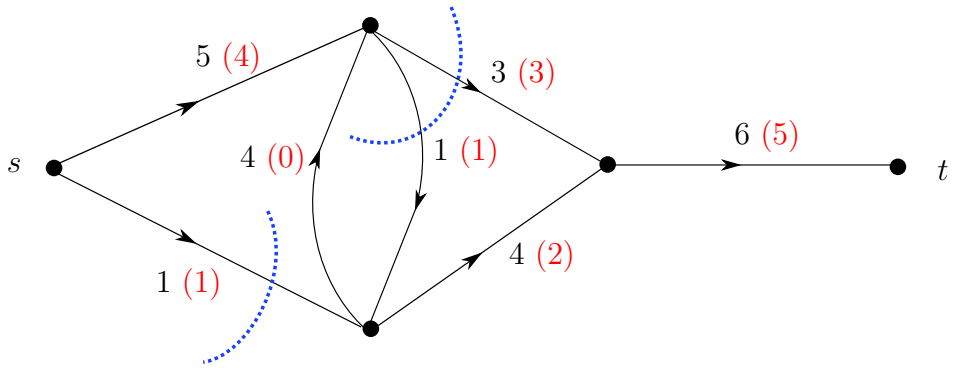


Figure 5: A network with source s, and sink t. Black numbers indicate edge capacities, red numbers indicate values of a maximum flow. In blue – minimum cut.

We are ready to prove the first easy lemma.

Lemma 4. Let (V, E, c) be a network and let f be a flow from s to t. Suppose $A \subseteq V$ is such that $s \in A$ and $t \notin A$. Then $f(A, V \setminus A) - f(V \setminus A, A) = |f|$.

Proof. Since $f_+(x) = f_-(x)$ for $x \neq s, t$, we have

$$|f| = f_+(s) - f_-(s) = \sum_{x\in A}(f_+(x) - f_-(x)) = \sum_{x\in A} f_+(x) - \sum_{x\in A} f_-(x) = f(A, V) - f(V, A)$$
$$= (f(A, A) + f(A, V \setminus A)) - (f(A, A) + f(V \setminus A, A)) = f(A, V \setminus A) - f(V \setminus A, A).$$

□

We can now show that the value of any flow is upper bounded by the capacity of any cut.

Lemma 5. Let (V, E, c) be a network with source s and sink t. Then for any flow f and for any cut Π we have $|f| \leq C(\Pi)$.

Proof. Suppose that we are given a flow f and a cut Π separating s from t. Let A be the set of all the points reachable from s after deleting from the network all the edges belonging to Π. Then since $t \notin A$, from Lemma 4 we get

$$\begin{aligned} |f| &= f(A, V \setminus A) - f(V \setminus A, A) \leq f(A, V \setminus A) \\ &= \sum_{(a,b) \in A \times (V \setminus A)} f(a,b) \leq \sum_{(a,b) \in A \times (V \setminus A)} c(a,b) \leq \sum_{(a,b) \in \Pi} c(a,b) = C(\Pi), \end{aligned}$$

where the last but one inequality follows from the fact that every edge (a, b) from A to $V \setminus A$ must belong to the cut (otherwise b would be reachable and thus would be a member of A). □

The above lemma shows that $\max_f |f| \leq \min_\Pi C(\Pi)$. The celebrated Max-flow min-cut theorem of Ford and Fulkerson shows that this is in fact equality.

Theorem 29 (Ford-Fulkerson, 1962)**.** Let (V, E, c) be a network with source s and sink t. Then $\max_f |f| = \min_\Pi C(\Pi)$.

Proof. We can assume that t is reachable from s. Let f be the maximum flow (it exists due to an easy compactness argument). From Lemma 5 it suffices to show that there exist Π such that $|f| = C(\Pi)$. A sequence $x_0, x_1, \ldots, x_n$ with $x_0 = s$ of vertices is called an *augmentable* path if for any pair x_i, x_{i+1}, $i = 0, \ldots, n-1$ we either have $(x_i, x_{i+1}) \in E$ with $f(x_i, x_{i+1}) < c(x_i, x_{i+1})$ (**forward** edge) or $(x_{i+1}, x_i) \in E$ with $c(x_i, x_{i+1}) > 0$ (**backward** edge).

Claim. Let A be the set of vertices a for which there exists an augmentable path $x_0, x_1, \ldots, x_n$ such that $x_n = a$. Then $t \notin A$.

Proof. Suppose $t \in A$. Then there exists an augmentable path $x_0, x_1, \ldots, x_n$ with $x_0 = s$ and $x_n = t$. Call this path P. Let

$$\varepsilon = \min \left\{ \min\{c(e) - f(e), e \text{ - forward edge in } P\},\ \min\{f(e), e \text{ - backward edge in } P\} \right\}.$$

Clearly $\varepsilon > 0$ from the definition of the augmentable path. If we now modify the flow f be taking $f(e) + \varepsilon$ instead of $f(e)$ for every forward edge in P and $f(e) - \varepsilon$ for every backward edge is P, we shall get a valid flow, whose value is $|f| + \varepsilon$ (recall that $(x_0, x_1) = (s, x_1)$ is a forward edge). Contradiction with maximality of f. □

Let us now define Π to be the set of all the edges from the set A (defined in the above claim) to its complement $V \setminus A$. If $e = (a, b) \in A \times (V \setminus A)$ then $f(e) = c(e)$ since otherwise b would be in A. If $e = (b, a) \in (V \setminus A) \times A$ then $f(e) = 0$ since otherwise b would also be in A. By Lemma 4 we get

$$|f| = f(A, V \setminus A) - f(V \setminus A, A) = f(A, V \setminus A) = \sum_{(a,b) \in A \times (V \setminus A)} c(a,b) = C(\Pi).$$

The proof is completed. □

Remark. If all the capacities are integers, then from the above proof one gets that there exists a maximum flow with $f(e) \in \mathbb{Z}$ for any $e \in E$. Indeed the above argument works if we consider only integer-valued flows (note that in this case we have $\varepsilon \in \mathbb{Z}$).

Remark. The above argument, with obvious adjustments, works also for networks with multiple edges.

The rest of this subsection is devoted to applications of the Max-flow min-cut theorem.

Theorem 30 (Hall's theorem)**.** Let $G = (V, E)$ be a bipartite graph with parts A and B with $|A| \leq |B|$. Then G has a set of $|A|$ vertex disjoint edges (a matching of cardinality $|A|$) if and only if for any subset $A' \subseteq A$ the number $N(A') = \{b \in B : \exists a' \in A', \{a', b\} \in E\}$ of the neighbors of A' satisfies $|N(A')| \geq |A'|$.

Proof. The condition given in the theorem is clearly necessary for the existence of the matching of cardinality $|A|$.

We prove the sufficiency. Let $n = |A|$. Add vertices s and t to G and all the edges from s to A and all the edges from B to t. Create a network as follows:

(a) take directed edges from s to A and from B to t with capacities 1,

(b) for edges between A and B that already existed in G take directions from A to B and capacities $n + 1$.

In this network there is a cut with capacity n (the cut separating s from A). We claim that the capacity of any cut is at least n. Indeed it is enough to consider only cuts that do not contain edges between A and B (if there is such an edge in the cut the claim is obvious as the capacity of such an edge is n). Suppose that the edges participating in this cut and going from v to A have endpoints in A forming the set A'. Let $B' \subseteq B$ be the set of endpoints in B of the edges from $A \setminus A'$ to B. From our assumption we have $|B'| \geq |A \setminus A'| = n - |A'|$. We can see that the points from B' have to be separated from t, which means that among the edges in the cut there are at least $|B'| \geq n - |A'|$ edges from B to t. Altogether we have at least $|A'| + (n - |A'|) = n$ edges in the cut.

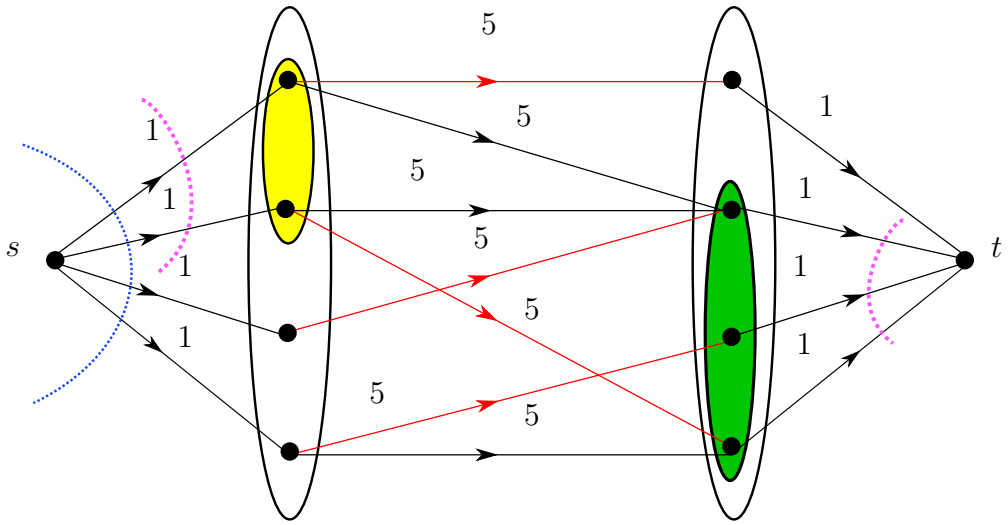


Figure 6: The blue cut is the minimum cut. The alternative purple cut generates the yellow set A' and the green set B') . In red - a set of $|A|$ vertex disjoint edges.

We have proved that the minimum cut has capacity n. Thus from the Max-flow min-cut theorem the maximum flow must have value n. From the second remark after the proof of Max-flow min-cut theorem there exists a maximum integer valued flow. So $f(s, a) = 1$ for all $a \in A$ and $f(b, t) \in \{0, 1\}$ for all $b \in B$. As a consequence of Kirchhoff's law, the flow has to send these "units" through vertex disjoint edges between A and B. This set of edges is clearly a perfect matching. □

Theorem 31 (Menger's theorem)**.** Let G be an undirected graph and let s, t be two different vertices in G. Then the minimum number of edges that one has to remove to separate s from t is equal to the maximal number of edges disjoint paths connecting s and t.

Proof. We create a network on $G = (V, E)$ by taking both directed edges (x, y) and (y, x) whenever $\{x, y\} \in E$. We give capacities 1 to those edges.

Claim 1. The capacity C of the minimum cut is equal to the minimum number m of edges that one has to remove to separate s and t.

Proof. For a minimum set of edges E' that separate s and t (in the undirected graph) let A be the connected component of s in $G' = (V, E \setminus E')$ (in the undirected graph). Then for every $e \in E'$ we must have $e \in A \times (V \setminus A)$ (otherwise such an edge is redundant and thus the cut is not minimum). If we now take the cut in our network consisting of edges E' taken with direction outgoing from A, we get a cut in the network (every directed path in the network from s to t must cross one of these directed edges). Thus $C \leq m$.

On the other hand, if we are given a minimum cut in the network, then removing all the corresponding undirected edges from G separates s from t (if not, there is a path in G connecting s and t and thus directed edges in the network following this path give a connection of s and t in the network). Thus $m \leq C$. □

Claim 2. The value F of the maximum flow equals the number P of edge disjoint paths from s to t.

Proof. We clearly have $F \geq P$ since we can always create a flow f with value $|f| = F$ by taking the edges of the P edge disjoint paths from s to t and creating the flow by putting $f(e) = 1$ for every such edge, where e is taken with direction of the path from s to t.

It suffices to show that $F \leq P$. Observe that there exists a maximum flow with $f(e) \in \{0, 1\}$ (see the first remark after the proof of Max-flow min-cut theorem). We construct a directed graph G' on the vertices of G by taking e to be an edge if and only if the corresponding value of the flow is 1. The difference between the number of outgoing edges from s and the number of ingoing edges to s is clearly equal to F. By the Kirchhoff's law, for any vertex x different from s and t the number of edges ingoing to x equals the number of edges outgoing from x. If there are directed cycles in G', we remove them (the above Kirchhoff's law will still be satisfied and the difference between the number of outgoing edges from s and the number of ingoing edges to s is still equal to F). Now we construct a paths from s to t step by step starting from s. Whenever we reach a new vertex different from t, we can always leave it, as the number of ingoing edges equals the number of outgoing edges. Since our graph has no loops, we will eventually reach t. Then we remove the edges of the path. We can continue like this creating at least F paths as there are at least F edges outgoing from s. □

The assertions follows by combining Claim 1 and Claim 2, together with Max-flow min-cut theorem. □

Recall that for an undirected graph $G = (V, E)$ a set of edges $E' \subseteq E$ is called a **matching** if no two elements of E' share a common endpoint. A matching is called **maximum** if no other matching has bigger cardinality.

A set of vertices $V' \subseteq V$ is called a **vertex cover** if every element of E has at least one endpoint in V'. A vertex cover is called **minimum** if no other vertex cover has smaller cardinality.

Theorem 32 (König, Egerváry, 1931)**.** In a bipartite graph G the cardinality of any maximum matching is equal to the cardinality of any minimum vertex cover.

Proof. The proof is similar to the proof of Hall's theorem. Let A, B be the two parts of G. Add a source s and a sink t, connect s to all the vertices in A with directed edges with capacities 1, to all the edges from A to B give capacities $\min\{|A|, |B|\}+1$, and finally connect all the vertices of B to w with directed edges of capacities 1. There exists a maximum flow f such that for all $e \in E$ we have $f(e) \in \mathbb{Z}$ (see the first remark after the proof of Max-flow min-cut theorem). It follows that $f(e) \in \{0, 1\}$ for all E

(this follows from Kirchhoff's law by observing that $f(s,a) \leq 1$ and $f(b,t) \leq 1$ for all $a \in A$ and $b \in B$; from the latter we get that for any $e \in A \times B$ we must also have $f(e) \leq 1$). The edges $e \in A \times B$ such that $f(e) = 1$ clearly correspond to a maximum matching. Thus the number of egdes in the maximum matching is $|f|$.

We now argue that the cardinality of a minimum vertex cover equals the cardinality of the minimum cut in our network. The assertion of the theorem will then follow by Max-flow min-cut theorem. We observe that cuts that do not use edges from $A \times B$ are in one-to-one correspondence with vertex covers. Indeed for every vertex cover D the corresponding cut is obtained by taking edges (s,a) if $a \in D$ and (b,t) if $b \in D$. The obtained set of edges is a cut since otherwise there would be a path of the form $s \to a \to b \to t$, which means that (a,b) has not been covered, contradiction. Similarly, for every cut the corresponding vertex cover is obtained by taking the endpoints of edges in the cut that belong to $A \cup B$. The set obtained in this way is a vertex cover since otherwise if (a,b) is not covered then none of the edges (s,a), (b,t) has been removed, which means that $s \to a \to b \to t$ is a path from s to t, contradiction. Note that in this correspondence the cardinalities of the cuts and vertex covers are the same (every vertex corresponds to precisely one edge). Now it suffices to observe the minimum cut does not use edges from $A \times B$ (there is a cut of capacity $\min\{|A|, |B|\}$) and thus the assertion follows from the Max-flow min-cut theorem.

□

5 The probabilistic method

5.1 Elements of probability theory

We introduce some definitions.

1. A pair (Ω, p) is called a *discrete probability space* if Ω is a finite set and $p : \Omega \to [0,1]$ is a function satisfying $\sum_{\omega \in \Omega} p(\omega) = 1$. The subsets $A \subseteq \Omega$ will be called *events*. The probability of an event A is defined as $\mathbb{P}(A) = \sum_{\omega \in A} p(\omega)$.

2. If $A_1, \ldots, A_n$ are any events, then $\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) \leq \sum_{i=1}^n \mathbb{P}(A_i)$. This follows immediately from the definition of $\mathbb{P}$. This inequality is called the *union bound*.

3. A function $X : \Omega \to M$, where M is any set, is called a random variable. For a random variable X and $B \subseteq M$ we also write $\mathbb{P}(X \in B) := \mathbb{P}(X^{-1}(B))$. This is interpreted as the probability that the random variable X has value in the set B.

4. Random variables $X_1, \ldots, X_n$ are independent if for all $k_1, \ldots, k_n$ in the range of $X_1, \ldots, X_n$ respectively, we have

$$\mathbb{P}(X_1 = k_1, \ldots, X_n = k_n) := \mathbb{P}\left(\bigcap_{i=1}^n X_i^{-1}(k_i)\right) = \prod_{i=1}^n \mathbb{P}\left(X_i^{-1}(k_i)\right) = \prod_{i=1}^n \mathbb{P}(X_i = k_i).$$

We observe that if $X_1, \ldots, X_n$ are independent then for any sets $A_1, \ldots, A_n$ we have

$$\mathbb{P}(X_1 \in A_1, \ldots X_n \in A_n) = \mathbb{P}(X_1 \in A_1) \cdot \ldots \mathbb{P}(X_n \in A_n).$$

Indeed, we have

$$\mathbb{P}(X_1 \in A_1, \ldots X_n \in A_n) = \sum_{a_i \in A_i, i=1,\ldots,n} \mathbb{P}(X_1 = a_1, \ldots, X_n = a_n) = \sum_{a_i \in A_i, i=1,\ldots,n} \prod_{i=1}^n \mathbb{P}(X_i = a_i)$$
$$= \prod_{i=1}^n \sum_{a_i \in A_i} \mathbb{P}(X_i = a_i) = \prod_{i=1}^n \mathbb{P}(X_i \in A_i).$$

In also follows that a subset of a set of independent random variables form a set of independent random variables (take A_i corresponding to random variables not in this set to be equal to Ω).

5. We say that events $A_1, \ldots, A_n \subseteq \Omega$ are independent if their indicator $\mathbf{1}_{A_1}, \ldots, \mathbf{1}_{A_n}$ are independent random variables. In other words, if by A^0 we denote $\Omega \setminus A$ and by A^1 we mean just A, when independence of $A_1, \ldots, A_n$ is equivalent to the following condition: for any $\varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}$ we have
$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i^{\varepsilon_i}\right) = \prod_{i=1}^{n} \mathbb{P}\left(A_i^{\varepsilon_i}\right).$$
One can show (easy exercise) that this condition is equivalent to the following one: for any sequence $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ one has
$$\mathbb{P}\left(A_{i_1} \cap A_{i_2} \cap \ldots A_{i_k}\right) = \mathbb{P}\left(A_{i_1}\right)\mathbb{P}\left(A_{i_2}\right)\ldots\mathbb{P}\left(A_{i_k}\right).$$

6. Suppose we are give independent random variables $X_1, \ldots, X_n$. We split the index set $\{1, \ldots, n\}$ into sets $S_1, \ldots, S_l$. Then we can consider random variables $(X_i)_{i\in S_1}$, ..., $(X_i)_{i\in S_l}$. It turns out that for any functions $f_1, \ldots, f_l$ (no matter what the range of these functions is!) the random variables $f_1((X_i)_{i\in S_1})$, ..., $f_l((X_i)_{i\in S_l})$ are independent. This means that independent random variables can be put in "packages" S_j and each package can be further "processed" by f_j and the resulting random variables will be independent. We will be using this principle frequently. Let us prove it. We want to show that
$$\mathbb{P}\left(f_1((X_i)_{i\in S_1}) = k_1, \ldots, f_l((X_i)_{i\in S_l}) = k_l\right) = \mathbb{P}\left(f_1((X_i)_{i\in S_1}) = k_1\right)\cdot\ldots\cdot\mathbb{P}\left(f_l((X_i)_{i\in S_l}) = k_l\right)$$
In other words, we want to show that
$$\mathbb{P}\left((X_i)_{i\in S_1} \in f_1^{-1}(k_1), \ldots, (X_i)_{i\in S_l} \in f_l^{-1}(k_l)\right) = \mathbb{P}\left((X_i)_{i\in S_1} \in f_1^{-1}(k_1)\right)\cdot\ldots\cdot\mathbb{P}\left((X_i)_{i\in S_1} \in f_l^{-1}(k_l)\right).$$
Take $A_i = f_i^{-1}(k_i)$. Then our goal is to show that
$$\mathbb{P}\left((X_i)_{i\in S_1} \in A_1, \ldots, (X_i)_{i\in S_l} \in A_l\right) = \mathbb{P}\left((X_i)_{i\in S_1} \in A_1\right)\cdot\ldots\cdot\mathbb{P}\left((X_i)_{i\in S_1} \in A_l\right).$$
Now, in view of the previous point it is enough to show that $(X_i)_{i\in S_1}$, ..., $(X_i)_{i\in S_l}$ are independent. But this is clear as
$$\begin{aligned}\mathbb{P}\left((X_i)_{i\in S_1} = (k_i)_{i\in S_1}, \ldots, (X_i)_{i\in S_l} = (k_i)_{i\in S_l}\right) &= \mathbb{P}\left(X_1 = k_1, \ldots, X_n = k_n\right) = \prod_{i=1}^{n}\mathbb{P}\left(X_i = k_i\right)\\ &= \mathbb{P}\left((X_i)_{i\in S_1} = (k_i)_{i\in S_1}\right)\cdot\ldots\cdot\mathbb{P}\left((X_i)_{i\in S_l} = (k_i)_{i\in S_l}\right).\end{aligned}$$

7. The *expectation* of a random variable $X : \Omega \to \mathbb{R}$ is defined as $\mathbb{E}[X] = \sum_{\omega\in\Omega} X(\omega)p(\omega)$. This is just the mean value of X. It is extremely important to notice the following obvious fact: if $X, Y : \Omega \to \mathbb{R}$ are random variables and $a, b \in \mathbb{R}$ then
$$\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y].$$
Indeed $\mathbb{E}[aX + bY] = \sum_\omega (aX(\omega) + bY(\omega))p(\omega) = a\sum_\omega X(\omega)p(\omega) + b\sum_\omega Y(\omega)p(\omega) = a\mathbb{E}[X] + b\mathbb{E}[Y]$.

8. Suppose $X, Y : \Omega \to \mathbb{R}$ are independent random variables. Then $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$. Indeed,
$$\begin{aligned}\mathbb{E}[XY] &= \sum_{x\in X(\Omega), y\in Y(\Omega)} xy\mathbb{P}\left(X = x, Y = y\right) = \sum_{x\in X(\Omega), y\in Y(\Omega)} xy\mathbb{P}\left(X = x\right)\mathbb{P}\left(Y = y\right)\\ &= \left(\sum_{x\in X(\Omega)} x\mathbb{P}\left(X = x\right)\right)\left(\sum_{y\in Y(\Omega)} y\mathbb{P}\left(Y = y\right)\right) = \mathbb{E}[X]\mathbb{E}[Y].\end{aligned}$$

9. Suppose $X \geq 0$ is a random variable and $f : [0, \infty) \to [0, \infty)$ be non-decreasing. Then for any $t > 0$ we have

$$\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}[f(X)]}{f(t)}.$$

Indeed, we have $\mathbb{E}[f(X)] \geq \mathbb{E}f(X)\mathbf{1}_{\{X \geq t\}} \geq f(t)\mathbb{E}\mathbf{1}_{\{X \geq t\}} = f(t)\mathbb{P}(X \geq t)$. In particular, by taking $f(t) = t$ and $f(t) = t^2$ we obtain the following Markov inequalities

$$\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}X}{t}, \qquad \mathbb{P}(X \geq t) \leq \frac{\mathbb{E}X^2}{t^2}.$$

10. For a random variable $X : \Omega \to \mathbb{R}$ we define the variance $\mathrm{Var}(X) = \mathbb{E}X^2 - (\mathbb{E}X)^2$. Note that

$$\mathbb{E}|X - \mathbb{E}X|^2 = \mathbb{E}[X^2 - 2X\mathbb{E}X + (\mathbb{E}X)^2] = \mathbb{E}[X^2] - 2\mathbb{E}[X]\mathbb{E}[X] + (\mathbb{E}[X])^2 = \mathbb{E}[X^2] - (\mathbb{E}[X])^2 = \mathrm{Var}(X),$$

so the an alternative equivalent definition of the variance is $\mathrm{Var}(X) = \mathbb{E}|X - \mathbb{E}X|^2$. Note that $\mathrm{Var}(X)$ controls how much X deviates from its mean. We also observe that by the second Markov inequality

$$\mathbb{P}(|X - \mathbb{E}X| \geq t) \leq \frac{\mathrm{Var}(X)}{t^2}, \qquad t > 0.$$

11. If $X : \Omega \to \mathbb{R}$ then

$$\mathbb{P}(X = 0) \leq \frac{\mathrm{Var}(X)}{\mathbb{E}[X^2]}.$$

To see this observe that by the Cauchy-Schwarz inequality for any two real-valued random variables X, Y we have $(\mathbb{E}[XY])^2 \leq \mathbb{E}[X^2]\mathbb{E}[Y^2]$ (for the proof just express both sides in terms of sums and use the usual weighted Cauchy-Schwarz inequality for real numbers). Taking $Y = \mathbf{1}_{\{X \neq 0\}}$ we get $(\mathbb{E}[X])^2 = (\mathbb{E}[X\mathbf{1}_{\{X \neq 0\}}])^2 \leq \mathbb{E}[\mathbf{1}_{\{X \neq 0\}}]\mathbb{E}[X^2] = \mathbb{P}(X \neq 0)\,\mathbb{E}[X^2]$. Thus

$$\mathbb{P}(X = 0) = 1 - \mathbb{P}(X \neq 0) \leq 1 - \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]} = \frac{\mathrm{Var}(X)}{\mathbb{E}[X^2]}.$$

12. For random variables $X, Y : \Omega \to \mathbb{R}$ we define their covariance by

$$\mathrm{Cov}(X, Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y].$$

Clearly $\mathrm{Cov}(X, X) = \mathrm{Var}(X)$. Note that if X, Y are independent then $\mathrm{Cov}(X, Y) = 0$. If $X_1, \ldots, X_n : \Omega \to \mathbb{R}$ then

$$\begin{aligned}\mathrm{Var}(X_1 + \ldots + X_n) &= \mathbb{E}[(X_1 + \ldots + X_n)^2] - (\mathbb{E}[X_1 + \ldots + X_n])^2 \\ &= \sum_{i,j}(\mathbb{E}[X_i X_j] - \mathbb{E}[X_i]\mathbb{E}[X_j]) = \sum_{i,j}\mathrm{Cov}(X_i, X_j).\end{aligned}$$

If $X_1, \ldots, X_n$ are independent, then only the diagonal terms are non-zero and we get

$$\mathrm{Var}(X_1 + \ldots + X_n) = \mathrm{Var}(X_1) + \ldots + \mathrm{Var}(X_n).$$

13. (example of **Chernoff's bound**) Suppose $\varepsilon_1, \ldots, \varepsilon_n$ are independent random variables such that $\mathbb{P}(\varepsilon_i = 1) = \mathbb{P}(\varepsilon_i = -1) = 1/2$ for all $i = 1, \ldots, n$. Assume $a_1, \ldots, a_n$ are real numbers satisfying $\sum_{i=1}^n a_i^2 = 1$. Then

$$\mathbb{P}\left(\sum_{i=1}^n a_i \varepsilon_i \geq t\right) \leq e^{-t^2/2}, \qquad t \geq 0.$$

By using symmetry we also get

$$\mathbb{P}\left(\left|\sum_{i=1}^{n} a_i\varepsilon_i\right| \geq t\right) \leq 2e^{-t^2/2}, \qquad t \geq 0.$$

To prove it we use Markov inequality, namely for any $\lambda > 0$ we have

$$\mathbb{P}\left(\sum_{i=1}^{n} a_i\varepsilon_i \geq t\right) = \mathbb{P}\left(e^{\lambda\sum_{i=1}^{n} a_i\varepsilon_i} \geq e^{\lambda t}\right) \leq \frac{\mathbb{E}[e^{\lambda\sum_{i=1}^{n} a_i\varepsilon_i}]}{e^{\lambda t}} = \frac{\prod_{i=1}^{n}\mathbb{E}[e^{\lambda a_i\varepsilon_i}]}{e^{\lambda t}} = \frac{\prod_{i=1}^{n}\cosh(\lambda a_i)}{e^{\lambda t}}.$$

We now use the inequality $\cosh(x) \leq e^{x^2/2}$ (this is true since $\cosh x = \sum_{n=0}^{\infty}\frac{x^{2n}}{(2n)!} \leq \sum_{n=0}^{\infty}\frac{x^{2n}}{2^n n!} = e^{x^2/2}$) to get that $\prod_{i=1}^{n}\cosh(\lambda a_i) \leq \prod_{i=1}^{n} e^{\frac{1}{2}\lambda^2 a_i^2} = e^{\lambda^2/2}$. We arrive at

$$\mathbb{P}\left(\sum_{i=1}^{n} a_i\varepsilon_i \geq t\right) \leq e^{\lambda^2/2-\lambda t}.$$

Taking $\lambda = t$ gives the desired result.

Examples. The idea behind defining probability spaces is that they should model certain random "experiments". It is important to understand that the same random experiment can be modeled is many different ways.

Example. Suppose we want to model a traditional dice with six sides. For this purpose we can use any finite set $\Omega = \{a_1, a_2, a_3, a_4, a_5, a_6\}$, and define $p(a_i) = 1/6$ for $i = 1, 2, 3, 4, 5, 6$. Let $X : \Omega \to \{1, 2, 3, 4, 5, 6\}$ be given by $X(a_i) = i$. The random variable X is interpreted as the result of rolling a dice. Note that $\mathbb{P}(X = i) = \mathbb{P}(X^{-1}(i)) = \mathbb{P}(\{a_i\}) = p(a_i) = 1/6$, as desired. The probability that the result of rolling a dice is an even number is

$$\mathbb{P}(X \text{ is even}) = \mathbb{P}(X \in \{2, 4, 6\}) = \mathbb{P}\left(X^{-1}(\{2, 4, 6\})\right) = \mathbb{P}(\{a_2, a_4, a_6\}) = p(a_2) + p(a_4) + p(a_6) = 1/2.$$

The expectation of X is $\mathbb{E}X = \sum_{i=1}^{6} ip(a_i) = \frac{1}{6}\sum_{i=1}^{6} i = \frac{7}{2}$.

Example. Now suppose we want to roll two dice, one with six sides and one with four sides, and we want to do this *independently*. Here independence means that the probability that the result in the first dice was $k \in \{1, 2, 3, 4, 5, 6\}$ and at the same time the result on the second dice was $l \in \{1, 2, 3, 4\}$ is the product of the probability that on the first dice we get k and the probability that on the second dice we get l.

To model this experiment it is convenient to use the product space $\Omega = \{a_1, a_2, a_3, a_4, a_5, a_6\} \times \{b_1, b_2, b_3, b_4\}$ with $p(a_i, b_j) = \frac{1}{6} \cdot \frac{1}{4} = \frac{1}{24}$. The random variable $X : \Omega \to \mathbb{R}$ given by $X(a_i, b_j) = i$ is interpreted as the result of rolling the first dice whereas the random variable $Y : \Omega \to \mathbb{R}$ given by $Y(a_i, b_j) = j$ is interpreted as the result of rolling the second dice. Now the random variable $(X, Y) : \Omega \to \mathbb{R} \times \mathbb{R}$ is interpreted as a result of rolling two dice. Instead of writing $\mathbb{P}((X, Y) = (k, l))$ we shall write $\mathbb{P}(X = k, Y = l)$. Observe that indeed X, Y are independent, since

$$\mathbb{P}(X = k, Y = l) = \mathbb{P}\left((X, Y)^{-1}(k, l)\right) = \mathbb{P}(a_k, b_l) = \frac{1}{24} = \frac{1}{6} \cdot \frac{1}{4}$$
$$4 \cdot \frac{1}{24} \cdot 6 \cdot \frac{1}{24} = \mathbb{P}\left(X^{-1}(k)\right) \cdot \mathbb{P}\left(Y^{-1}(l)\right) = \mathbb{P}(X = k) \cdot \mathbb{P}(Y = l).$$

We can now compute the expectation of the sum of the results on the six-side dice and four-side dice: $\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y] = \frac{1}{6}\sum_{i=1}^{6} i + \frac{1}{4}\sum_{i=1}^{4} i = \frac{7}{2} + \frac{5}{2} = 6$.

Our next example is the so-called Erdös-Rényi model $G(n,p)$ of a random graph on n vertices.

Example. Suppose we want to model the following random graph. Given a set V of n vertices, for every pair of vertices $\{u,v\}$ we want to add this pair to the set of edges with probability p and not add it with probability $1-p$. What is important is that we want to do this *independently*. What does this mean? For all $\binom{n}{2}$ "potential" edges e we write $f(e)=1$ if e was chosen to be an edge and $f(e)=0$ otherwise. Independence means that for any $\{0,1\}$-valued function g on the set of edges we want to have

$$\mathbb{P}\left(\forall e\ f(e)=g(e)\right)=\prod_e \mathbb{P}\left(f(e)=g(e)\right).$$

For this purpose we introduce a probability space (Ω,p) with $\Omega=\{0,1\}^N$ where $N=\binom{n}{2}$. The ith coordinate of Ω corresponds to the ith potential edge. If the ith coordinate is 1 then the interpretation is that the ith edge is present is our random graph. If the ith coordinate is 0 then the corresponding edge is not present. For every $\omega=(\omega_i)_{i=1,\dots,}$ we take $p(\omega)=p^{|\{i\colon\ \omega_i=1\}|}(1-p)^{|\{i\colon\ \omega_i=0\}|}$. Note that $\omega_i:\Omega\to\{0,1\}$ (that is, $\omega_i(\omega_1,\dots,\omega_N)=\omega_i$) is a random variable indicating whether the ith edge is present in the graph or not. Note that

$$\begin{aligned}\mathbb{P}\left(\omega_i=1\right)&=\mathbb{P}\left(\omega_i^{-1}(1)\right)=\sum_{\omega\colon\ \omega_i=1}p(\omega)=\sum_{\omega\colon\ \omega_i=1}p^{|\{j\colon\ \omega_j=1\}|}(1-p)^{|\{j\colon\ \omega_j=0\}|}\\&=p\sum_{\omega_j\in\{0,1\},\ j\neq i}p^{|\{j\neq i\colon\ \omega_j=1\}|}(1-p)^{|\{j\neq i\colon\ \omega_j=0\}|}=p\sum_{k=0}^{N-1}\binom{N-1}{k}p^k(1-p)^{N-1-k}\\&=p(p+(1-p))^{N-1}=p.\end{aligned}$$

Clearly we also get $\mathbb{P}\left(\omega_i=0\right)=1-p$.

These random variables are independent, that is, for any sequence of signs $(s_i)_{i=1}^N$ we have

$$\mathbb{P}\left(\forall_i\ \omega_i=s_i\right)=p^{|\{i\colon\ \omega_i=1\}|}(1-p)^{|\{i\colon\ \omega_i=0\}|}=\prod_i\mathbb{P}\left(\omega_i=s_i\right).$$

5.2 Probabilistic counting

Theorem 33. Let $k\geq 3$. The Ramsey number $R(k,k)$ satisfies the inequality $R(k,k)>[2^{k/2}]$. In other words, there exists a coloring of edges of the $[2^{k/2}]$-clique without monochromatic k-clique.

Proof. Let $n=[2^{k/2}]$ and let us color the edges of the clique K_n randomly (red with probability $1/2$ and blue with probability $1/2$). Let us fix an k-element subset S of vertices of K_n. The probability that the clique on S is entirely red is $2^{-\binom{k}{2}}$, since for each of $\binom{k}{2}$ edges its color has to be red. Similarly the probability that S is entirely blue is $2^{-\binom{k}{2}}$. Thus, the probability of the event A_S that the clique on S is monochromatic is $\mathbb{P}\left(A_S\right)=2\cdot 2^{-\binom{k}{2}}$. The event A that there exists a monochromatic k-clique is $\bigcup_{S\colon\ |S|=k}A_S$ and thus its probability satisfies

$$\mathbb{P}\left(A\right)=\mathbb{P}\left(\bigcup_{S\subseteq K_n\colon\ |S|=k}A_S\right)\leq\sum_{S\subseteq K_n\colon\ |S|=k}\mathbb{P}\left(A_S\right)=\binom{n}{k}2\cdot 2^{-\binom{k}{2}}.$$

Since $\binom{n}{k}=\frac{n(n-1)\dots(n-k+1)}{k!}\leq\frac{n^k}{k!}$, we get

$$\mathbb{P}\left(A\right)\leq\frac{n^k}{k!}\cdot 2\cdot 2^{-\binom{k}{2}}\leq\frac{2^{\frac{k^2}{2}}}{k!}\cdot 2^{1-\frac{k(k-1)}{2}}=\frac{2^{1+\frac{k}{2}}}{k!}<1.$$

If follows that the complement of A has positive probability and thus there exists a point in the probability space not belonging to A, which corresponds to a graph with no monochromatic k-clique. □

Theorem 34. A tournament is a competition where every two participants play with each other precisely once and the is always a winner. Fix a positive integer k. There exists a tournament with the following property: for every subset of k players there exists a player who won with all these k players.

Proof. Consider a tournament with n players. We think of it as of a clique K_n with directed edges (an edge goes from u to v if u won with v). We choose directions of edges independently and uniformly at random (each direction with probability 1/2). For a k-element subset of vertices of K_n (players) let $A_{S,v}$ be the event that the player $v \notin S$ did not win with all the players from S. We have $\mathbb{P}(A_{S,v}) = 1 - 2^{-k}$. Thus the even A_S that none of the players $v \notin S$ won with all the players from S satisfies $\mathbb{P}(A_S) = \mathbb{P}\left(\bigcap_{v \notin S} A_{S,v}\right) = \prod_{v \notin S} \mathbb{P}(A_{S,v}) = (1-2^{-k})^{n-k}$. Note that the second equality follows from the fact that the events $A_{S,v}$ for different v depend on pairwise disjoint subsets of edges and thus they are independent. Let A be the even that there exists S of cardinality k such that none of the players $v \notin S$ won with all the players from S. Thus $A = \bigcup_{S:\ |S|=k} A_S$. We get

$$\mathbb{P}(A) = \mathbb{P}\left(\bigcup_{S:\ |S|=k} A_S\right) \leq \sum_{S:\ |S|=k} \mathbb{P}(A_S) = \binom{n}{k}(1-2^{-k})^{n-k} < n^k(1-2^{-k})^{n-k}.$$

If k is fixed and $n \to \infty$ then the $n^k(1-2^{-k})^{n-k} \to 0$ and thus for big n we get $\mathbb{P}(A) < 1$. Thus the complement of A has positive probability and so there exists a choice of directions of edges with the desired property. □

5.3 First moment method

In this section we are going to show examples where the following obvious rule is applied: if $X : \Omega \to \mathbb{R}$ is a random variable such that $\mathbb{E}X \geq a$ then there exist $\omega \in \Omega$ such that $X(\omega) \geq a$.

Theorem 35. There exists a tournament on n vertices in which where are at least $n!2^{-(n-1)}$ directed Hamiltonian paths (paths that follow directed edges and visit all the vertices).

Proof. Consider a random tournament T on v vertices (directions of edges are chosen independently with probabilities 1/2). Fix a permutation $\sigma = (\sigma_1, \ldots, \sigma_n)$ of vertices of T. Let X_σ be a random variable having value 1 if the sequence $\sigma_1 \to \sigma_2 \to \ldots \to \sigma_n$ is a Hamiltonian path and 0 otherwise. Thus $\mathbb{E}[X_\sigma]$ is equal to the probability that $\sigma_1 \to \sigma_2 \to \ldots \to \sigma_n$ is a Hamiltonian path and thus $\mathbb{E}[X_\sigma] = 2^{-(n-1)}$ (we have to choose correct directions of $n-1$ edges $\{\sigma_i, \sigma_{i+1}\}$, $i = 1, \ldots, n-1$). Let $X = \sum_\sigma X_\sigma$, where the sum runs over all permutations of the set of vertices. Note that the random variable X is precisely the number of Hamiltonian paths in our random tournament. From linearity of expectation we have $\mathbb{E}[X] = \sum_\sigma \mathbb{E}[X_\sigma] = n!2^{-(n-1)}$. Thus, there exists at least one point ω of the probability space such that $X(\omega) \geq n!2^{-(n-1)}$, which gives the desired tournament. □

Theorem 36. Suppose $v_1, \ldots, v_n$ are random vectors on $\mathbb{R}^n$ with $|v_i| = 1$ for $i = 1, \ldots, n$. Then there exist $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ such that $|\varepsilon_1 v_1 + \ldots + \varepsilon_n v_n| \leq \sqrt{n}$.

Proof. Consider independent random signs $\varepsilon_1, \ldots, \varepsilon_n$ (each with probability 1/2). In other words, every sequence of signs gets probability 2^{-n}. Take $X = |\varepsilon_1 v_1 + \ldots + \varepsilon_n v_n|^2$. We have

$$\mathbb{E}[X] = \mathbb{E}\left[\sum_{i,j=1}^{n} \varepsilon_i \varepsilon_j \langle v_i, v_j \rangle\right] = \sum_{i,j=1}^{n} \langle v_i, v_j \rangle \mathbb{E}[\varepsilon_i \varepsilon_j] = \sum_{i}^{n} \langle v_i, v_i \rangle = \sum_{i=1}^{n} |v_i|^2 = n.$$

Thus there exists a sequence of signs such that $X \leq n$. □

Theorem 37. Let n be a positive integer. Every set $\{b_1, \ldots, b_n\}$ of non-zero integers contains a sum-free subsets A with $|A| > \frac{n}{3}$, that is, a set such that for all $a_1, a_2, a_3 \in A$ we have $a_1 + a_2 \neq a_3$.

Proof. Let $p = 3k+2$ be a prime number satisfying $p > 2\max_i |b_i|$. Take $C = \{k+1, k+2, \ldots, 2k+1\}$. Note that C is a sum-free subset of the cyclic group $\mathbb{Z}_p$. We choose an integer x uniformly at random from the set $\{1, 2, \ldots, p-1\}$. Define $d_i = xb_i \mod p$. Since x runs over all element of $\{1, \ldots, p-1\}$, the random variable d_i runs over all elements of $\{1, \ldots, p-1\}$ and thus $\mathbb{P}(d_i \in C) = |C|/(p-1) = (k+1)/(3k+1) > \frac{1}{3}$. Let X_i be a random variable having value 1 if $d_i \in C$ and 0 otherwise. Then $X = \sum_{i=1}^n X_i$ is equal to $|\{i : d_i \in C\}|$. We have $\mathbb{E}[X] = \sum_{i=1}^n \mathbb{E}[X_i] > n/3$. It follows that there exists x such that $|\{i : d_i \in C\}| > n/3$. Fix this x. By the assumption assumption that $p > 2\max_i |b_i|$ we know that the numbers d_i are different. Let A be the set of number b_i such that the corresponding d_i are in C. Thus $|A| > n/3$. We claim that A is sum free. Suppose $b_{i_1}, b_{i_2}, b_{i_3} \in A$ satisfy $b_{i_1} + b_{i_2} = b_{i_3}$. Then $b_{i_1}x + b_{i_2}x = b_{i_3}x$ and thus $d_{i_1} + d_{i_2} = d_{i_3}$, which shows that C is not sum-free, contradiction. □

In our next example we are going to use the so-called Markov inequality. Suppose X is a nonnegative random variable. Then for $t > 0$ we have $\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}[X]}{t}$. Indeed, note that $\mathbb{E}[X] \geq \mathbb{E}[X\mathbf{1}_{X \geq t}] \geq t\mathbb{E}[\mathbf{1}_{X \geq t}] = t\mathbb{P}(X \geq t)$.

The *girth* $g(G)$ of a graph G is the length of the shortest cycle in G. The chromatic number of G is denoted by $\chi(G)$. The cardinality of the largest independent set of vertice in G is denoted by $\alpha(G)$.

Theorem 38. For any k and l there exists a graph G with $g(G) > l$ and $\chi(G) > k$.

Proof. Let us consider the Erdös-Rényi random graph $G(n,p)$, that is, the probability that a fixed edge is present is equal p and these events are independent. Take $\theta < 1/l$ and take $p = n^{\theta-1}$.The probability that a (cyclic) sequence of r distinct vertices form a cycle in G is p^r. The number of (cyclic) sequences of vertices of length r is upper bounded by $n(n-1)\ldots(n-r+1) \leq n^r$. Let Σ be a (cyclic) sequence of vertices of G. Let X_Σ be 1 if Σ forms a cycle in G and 0 otherwise. Let X be the number of cycles of length at most r. Then

$$\mathbb{E}[X] = \sum_{|\Sigma| \leq r} \mathbb{E}[X_\Sigma] = \sum_{r=3}^{l} \sum_{|\Sigma|=r} \mathbb{E}[X_\Sigma] \leq \sum_{r=3}^{l} n^r p^r = \sum_{r=3}^{l} n^r n^{(\theta-1)r} = \sum_{r=3}^{l} n^r p^r = \sum_{r=3}^{l} n^{\theta r} \leq (l-2)n^{\theta l} = o(n).$$

Thus from Markov inequality we get $\mathbb{P}(X \geq n/2) \leq \frac{2}{n}\mathbb{E}[X] = o(1)$.

Since every set of vertices with fixed color in a proper coloring of G is an independent set, we get $\chi(G)\alpha(G) \geq n$. If S is a set of vertices then the probability of an event A_S that there are no edges between vertices from S is $(1-p)^{\binom{|S|}{2}}$. We have

$$\mathbb{P}(\alpha(G) \geq a) = \mathbb{P}\left(\bigcup_{|S|=a} A_S\right) \leq \sum_{|S|=a} \mathbb{P}(A_S) = \binom{n}{a}(1-p)^{\binom{a}{2}} \leq n^a(1-p)^{\binom{a}{2}} = (n(1-p)^{\frac{a-1}{2}})^a.$$

Let us now take $a = \lceil \frac{3}{p}\ln n \rceil > 1$. From the well known inequality $1 + x \leq e^x$ we get $n(1-p)^{\frac{a-1}{2}} \leq e^{-\frac{p}{2}(a-1)} \leq ne^{-\frac{3}{2}\ln n}e^{\frac{p}{2}} = n^{-\frac{1}{2}}e^{\frac{p}{2}} = n^{-\frac{1}{2}}e^{\frac{1}{2}n^{\theta-1}} = o(1)$. Thus also $(n(1-p)^{\frac{a-1}{2}})^a = o(1)$ as $a > 1$.

We conclude that for big n with probability close to 1 our graph has at most $n/2$ cycles of length at most l and the size of largest independent set smaller than $a = \lceil \frac{3}{p}\ln n \rceil$. Let us pick one realization of such a graph. It has at most cycles of lengths not exceeding l, so by removing at most $n/2$ vertices we can get read of these cycles. The new graph G' satisfies $g(G') > l$ and still has at least $n/2$ vertices and $\alpha(G') < a$. We have $\chi(G')\alpha(G') \geq \frac{n}{2}$, which leads to

$$\chi(G') \geq \frac{n}{2\alpha(G')} > \frac{n}{2a} = \frac{n}{2\lceil \frac{3}{p}\ln n \rceil} = \frac{n}{2\lceil \frac{3}{n^{\theta-1}}\ln n \rceil} > \frac{n}{2 + 2\frac{3}{n^{\theta-1}}\ln n} = \cdot\frac{n^\theta}{2n^{\theta-1} + 6\ln n} \xrightarrow[n\to\infty]{} \infty.$$

Thus, if n is big enough we can also satisfy the desired inequality $\chi(G') > k$. □

5.4 Second moment method

Here we present examples of combinatorial problems that can be solved using estimates involving second moment $\mathbb{E}[X^2]$ of certain random variables, e.g., involving the variance.

Let $f(n)$ be the maximal number k such that there exist numbers $x_1, \ldots, x_k \in \{1, \ldots, n\}$ such that all the sums of the form $x_{i_1} + \ldots + x_{i_l}$ where $i_1 < \ldots < i_l$ and $1 \le l \le k$ are distinct. Note that the set $2^0, 2, 2^2, \ldots, 2^{\lfloor \log_2 n \rfloor}$ has the above property. Indeed, to see this it is enough to show that if $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 0, 1\}$ satisfy $\sum_{i=0}^{k} \varepsilon_i 2^i$ (here $k = \lfloor \log_2 n \rfloor$) then $\varepsilon_i = 0$ for all $i = 0, \ldots, k$. If k_0 is the index of the last non-zero element in this sum then $\left| \sum_{i=0}^{k} \varepsilon_i 2^i \right| \ge 2^k - \sum_{i=0}^{k-1} 2^i = 1 > 0$, so the claim follows.

We just showed that $f(n) \ge 1 + \lfloor \log_2 n \rfloor$. It is interesting to ask about upped bound on $f(n)$. Let $k = f(n)$ and consider the numbers $x_1, \ldots, x_k \in \{1, \ldots, n\}$ with distinct sums. Each sum cannot exceed nk (since there are at most k number in the sum and each of the does not exceed n). Since all the 2^k possible sums are different and they occupy the set $\{0, 1, \ldots, nk\}$, we get $2^k \le nk + 1 \le 2nk$. Also, Thus $k \le \log_2(nk + 1)$. Iterating this and using the obvious bound clearly $k \le n$ we obtain for $n \ge 2$

$$\begin{aligned} k &\le \log_2(2nk) = 1 + \log_2(nk) \le 1 + \log_2(n \log_2(2nk)) \le 1 + \log_2(nk) \le 1 + \log_2(n \log_2(2n^2)) \\ &= 1 + \log_2 n + \log_2(1 + 2\log_2 n) \le 1 + \log_2 n + \log_2(3 \log_2 n) = \log_2 n + \log_2 \log_2 n + 1 + \log_2 3. \end{aligned}$$

This shows that $f(n) \le \log_2 n + \log_2 \log_2 n + 3$. By using the second moment method we can get a slightly better bound

Theorem 39. Let $n \ge 2$ and let $f(n)$ be the maximal number k such that there exist numbers $x_1, \ldots, x_k \in \{1, \ldots, n\}$ such that all the sums of the form $x_{i_1} + \ldots + x_{i_l}$ where $i_1 < \ldots < i_l$ and $1 \le l \le k$ are distinct. Then $f(n) \le \log_2 n + \frac{1}{2} \log_2 \log_2 n + 3$.

Proof. Let $x_1, \ldots, x_k \in \{1, \ldots, n\}$ be such that the sums of x_i are distinct. Let $\varepsilon_1, \ldots, \varepsilon_n$ be independent random variables such that $\mathbb{P}(\varepsilon_i = 0) = \mathbb{P}(\varepsilon_i = 1) = 1/2$ for $i = 1, \ldots, n$. Define $X = \varepsilon_1 x_1 + \ldots + \varepsilon_k x_k$. We have $\mathbb{E}[X] = \frac{1}{2}(x_1 + \ldots + x_k)$ and by independence

$$\operatorname{Var}(X) = \sum_{i=1}^{k} \operatorname{Var}(\varepsilon_i x_i) = \sum_{i=1}^{k} x_i^2 \operatorname{Var}(\varepsilon_i) = \frac{1}{4} \sum_{i=1}^{k} x_i^2 \le \frac{1}{4} n^2 k.$$

By Markov inequality we get $\mathbb{P}(|X - \mathbb{E}X| \ge t) \le \frac{\operatorname{Var}(X)}{t^2} \le \frac{n^2 k}{4t^2}$. Taking $t = n\sqrt{k}$ we get the inequality $\mathbb{P}\left(|X - \mathbb{E}X| \ge n\sqrt{k}\right) \le \frac{1}{4}$ and thus $\mathbb{P}\left(|X - \mathbb{E}X| < n\sqrt{k}\right) > \frac{3}{4}$.

On the other hand, since the sums of x_i are distinct, each values of $X - \mathbb{E}X$ is achieved with probability 2^{-k}. Moreover, two each two of these values differ by at least 1, so in the interval $[-n\sqrt{k}, n\sqrt{k}]$ there are at most $2n\sqrt{k} + 1$ such values. Thus, $\mathbb{P}\left(|X - \mathbb{E}X| < n\sqrt{k}\right) \le 2^{-k}(2n\sqrt{k} + 1)$. We arrive at $\frac{3}{4} \le 2^{-k}(2n\sqrt{k} + 1)$. Thus, $2^k \le \frac{4}{3}(2n\sqrt{k} + 1) \le 4n\sqrt{k}$. Taking the logarithm and then iterating and using the inequality $k \le n \le n^2$ we get

$$\begin{aligned} k &\le 2 + \log_2(n\sqrt{k}) = 2 + \log_2 n + \frac{1}{2} \log_2 k \le 2 + \log_2 n + \frac{1}{2} \log_2 \log_2(4n\sqrt{k}) \\ &\le 2 + \log_2 n + \frac{1}{2} \log_2 \log_2(4n^2) \le 2 + \log_2 n + \frac{1}{2} \log_2 \log_2(n^4) = 3 + \log_2 n + \frac{1}{2} \log_2 \log_2 n. \end{aligned}$$

□

Our next example deals with the Edrs-Rényi random graph. We say that an event A is *monotone* if adding edges to our graph can only help this even to hold. For example, events like being connected, having Hamiltonian cycles, containing a copy of K_l clique are all monotone.

We say that $p_0(n) \in [0,1]$ is a *threshold* for a monotone event A if for any function $p(n)$ with $p(n)/p_0(n) \to 0$ we have $\mathbb{P}(G(n,p(n)) \in A) \to 0$ and for any function $p(n)$ with $p(n)/p_0(n) \to \infty$ we have $\mathbb{P}(G(n,p) \in A) \to 1$.

Before we prove this theorem, we shall present the proof of the so-called Margulis-Russo lemma. Suppose $\Omega = \{0,1\}^N$ is equipped with weights

$$\mu_{p_1,\dots,p_N}(\omega_1,\dots,\omega_N) = \prod_{i:\ \omega_i=1} p_i \prod_{i:\ \omega_i=0} (1-p_i).$$

An event $A \subseteq \Omega$ is called monotone if for every $\omega = (\omega_1,\dots,\omega_N) \in \Omega$ and $\omega' = (\omega'_1,\dots,\omega'_N) \in \Omega$ such that $\omega_i \le \omega'_i$ for every $i = 1,\dots,N$ we have that $\omega \in A$ implies $\omega' \in A$. The probability of A is defined as $\mathbb{P}_{p_1,\dots,p_N}(A) = \sum_{\omega\in A} \mu_{p_1,\dots,p_n}(\omega)$. The ith influence of A is defined as

$$I^{(i)}_{p_1,\dots,p_N}(A) = \mathbb{P}_{p_1,\dots,p_N}(\{s \in \{0,1\}^N : (s_1,\dots,s_{i-1},0,s_{i+1},\dots,s_N) \notin A, (s_1,\dots,s_{i-1},1,s_{i+1},\dots,s_N) \in A\}).$$

This is just the probability that changing the ith bit will influence the event A.

Lemma 6 (Margulis-Russo lemma)**.** For every monotone event we have $\frac{\partial}{\partial p_i}\mathbb{P}_{p_1,\dots,p_n}(A) = I^{(i)}_{p_1,\dots,p_N}(A) \ge 0$.

Proof. We can assume that $i = 1$. Let $B_0 = \{s \in \{0,1\}^{N-1} :\ (0,s) \in A\}$. Note that $\{0\} \times B \subseteq A$ and by monotonicity of A we also get $\{1\} \times B \subseteq A$. Let $B = \{s \in \{0,1\}^{N-1} :\ (0,s) \notin A, (1,s) \in A\}$. We get $A = (\{0,1\} \times B_0) \cup (\{1\} \times B)$. We get

$$\mathbb{P}_{p_1,\dots,p_n}(A) = \mathbb{P}_{p_2,\dots,p_n}(B_0) + p_1\mathbb{P}_{p_2,\dots,p_n}(B).$$

Thus

$$\frac{\partial}{\partial p_1}\mathbb{P}_{p_1,\dots,p_n}(A) = \mathbb{P}_{p_2,\dots,p_n}(B) = \mathbb{P}_{p_1,p_2,\dots,p_n}(\{0,1\} \times B) = I_{p_1,\dots,p_N}(A).$$

□

Corollary 7. Suppose $G(n,p_1,\dots,p_N)$ be the generalized Erdös-Rényi graph in which the probability of the occurrence of the ith edge is p_i and and these events are independent. Then probabilities of monotone event (property) A are non-decreasing functions of p_i. In particular, if $0 \le p \le q \le 1$ then

$$\mathbb{P}(G(n,p) \text{ has property } A) \le \mathbb{P}(G(n,q) \text{ has property } A).$$

Theorem 40. Let us consider the graph $G(n,p)$ and let A be the event that $G(n,p)$ has a cycle. Then $p_0(n) = \frac{1}{n}$ is a threshold for this event.

Proof. Suppose first that $np(n) \to 0$. Then we have to show that the probability that $G(n,p(n))$ has a cycle tends to 0. For any cyclic permutation of vertices S let X_S be a random variable being equal to 1 if S forms a cycle and 0 otherwise. Let $p = p(n)$ (one should remember that p depends on n). We have

$$\mathbb{P}(G(n,p) \text{ has a cycle}) \le \mathbb{E}[\#\text{ cycles is } G(n,p)] = \mathbb{E}\left[\sum_{k=3}^{n}\sum_{S:\ |S|=k} X_S\right] = \sum_{k=3}^{n}\sum_{S:\ |S|=k}\mathbb{E}[X_S]$$
$$= \sum_{k=3}^{n}\sum_{S:\ |S|=k}\mathbb{P}(S \text{ forms a cycle}) = \sum_{k=3}^{n}\sum_{S:\ |S|=k} p^k = \sum_{k=3}^{n}\binom{n}{k}\frac{(k-1)!}{2}p^k.$$

Now, since $\binom{n}{k} \leq \frac{n^k}{k!}$, we arrive at

$$\mathbb{P}\left(G(n,p) \text{ has a cycle}\right) \leq \sum_{k=3}^{n} (np)^k \leq (np)^3 \frac{1}{1-np} \xrightarrow[n\to\infty]{} 0.$$

Now suppose that $np(n) \to \infty$. Then we have to show that the probability that $G(n,p(n))$ has a cycle is tends to 1. Let X be the number of edges in $G(n,p)$. It is enough to show that $\mathbb{P}(X \geq n) \to 1$ as $n \to \infty$ since having n edges implies that G contains a cycle (if G has no cycle then it is a forest and therefore its number of edges is $n-k$ where k is the number of connected components, which follows from the fact that trees on l vertices have $l-1$ edges). Let X_e be 1 if the edge e is present in G and 0 otherwise. Thus $X = \sum_e X_e$. We have $\mathbb{E}[X] = \sum_e \mathbb{E}[X_e] = \binom{n}{2} p$. Now, since X_e are independent, we get

$$\operatorname{Var}\left(\sum_e X_e\right) = \sum_e \operatorname{Var}(X_e) = \binom{n}{2} p(1-p) \leq n^2 p.$$

It suffices to prove our claim for $p = \frac{4}{n}$ (the original p will be bigger for sufficiently large n since $np(n) \to \infty$). For $p = \frac{4}{n}$ we have $\mathbb{E}[X] = \binom{n}{2} p = 2(n-1)$. Note that $X < n$ implies $|X - \mathbb{E}[X]| \geq \mathbb{E}[X] - X > \mathbb{E}[X] - n = n - 2$. By Markov inequality

$$\mathbb{P}(X < n) \leq \mathbb{P}(|X - \mathbb{E}X| \geq n-2) \leq \frac{\operatorname{Var}(X)}{(n-2)^2} \leq \frac{n^2 p}{(n-2)^2} = \frac{4n}{(n-2)^2} \xrightarrow[n\to\infty]{} 0.$$

Thus $\mathbb{P}(X \geq n) \to 1$ as $n \to \infty$. □

5.5 Lovász Local Lemma

In probabilistic counting our strategy was the following: in order to construct some combinatorial object we introduce a random model and show that the family of "bad" events $A_1, \ldots, A_n$ (obstacles for our desired object) does not occupy the whole probability space, that is, $\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) < 1$, which leads to $\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) > 0$. The usual strategy for proving this is to use the union bound $\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) \leq \sum_{i=1}^n \mathbb{P}(A_i)$. The union bound is very often too weak and the sum $\sum_{i=1}^n \mathbb{P}(A_i)$ exceeds 1.

There is another case when we can easily conclude that $\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) > 0$, namely when $A_1, \ldots, A_n$ are independent and $\mathbb{P}(A_i) < 1$, $i = 1, \ldots, n$, in which case $\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) = \prod_{i=1}^n \mathbb{P}(A_i^c) = \prod_{i=1}^n (1 - \mathbb{P}(A_i)) > 0$. Unfortunately in practice the events A_i are not independent. The Lovász Local Lemma deals with the case when $A_1, \ldots, A_n$ are not "too dependent". In fact, as we will see, it interpolates between the union bound and the independency bound.

Let $A_1, \ldots, A_n$ be events. For $S \subseteq [n] \setminus \{i\}$ we say that A_i is mutually independent of the events $\{A_j, j \in S\}$ if for every $S' \subseteq S$ we have

$$\mathbb{P}\left(A_i \cap \bigcap_{j \in S'} A_j\right) = \mathbb{P}(A_i) \cdot \mathbb{P}\left(\bigcap_{j \in S'} A_j\right). \tag{3}$$

Recall that conditional probability is defined as $\mathbb{P}(A|B) = \mathbb{P}(A \cap B)/\mathbb{P}(B)$. Thus (3) can be rewritten as $\mathbb{P}\left(A_i \,\middle|\, \bigcap_{j \in S'} A_j\right) = \mathbb{P}(A_i)$. Let us mention that in the condition 3 we can replace some of the A_j's with their complements. Indeed, to replace A_j with A_j^c it is enough to write (3) for $S' \setminus \{j\}$ and for S' and substract these equations. In particular, if (3) is satisfied for every $S' \subseteq S$ then we also have

$$\mathbb{P}\left(A_i \,\middle|\, \bigcap_{j \in S'} A_j^c\right) = \mathbb{P}(A_i). \tag{4}$$

We introduce the notion of **dependency digraph** for the events $A_1, \dots, A_n$ to be **any** directed graph with no loops (digraph) $G = (V, E)$ on the set of vertices $V = \{1, \dots, n\}$ such that for all i the event A_i is mutually independent of the events $\{A_j : (i,j) \notin E\}$. In other words, a dependency digraph for $A_1, \dots, A_n$ is a family of subsets $S_1, \dots, S_n$ (where $S_i = \{j : (i,j) \in E\}$) of events such that A_i is mutually independent of the family S_i. In practice we know that our events A_i are independent of some families S_i and we construct our dependency graph just by drawing only edges from i to $\{j : A_j \notin S_i\}$. Note that we do not require this graph to encode all the independence structure of our problem (if we, say, add edges to dependency digraph then it is also a dependency digraph).

Remark. We note that not all independences can be "encoded" in the dependency digraph. Suppose that $\Omega = \{1,2,3,4\}$ and $p(i) = 1/4$ for all $i = 1,2,3,4$. Consider events $A = \{1,2\}$, $B = \{2,3\}$ and $C = \{1,3\}$. Then $\mathbb{P}(A \cap B) = \mathbb{P}(B \cap C) = \mathbb{P}(C \cap A) = 1/4$ and $\mathbb{P}(A) = \mathbb{P}(B) = \mathbb{P}(C) = 1/2$ and thus A, B, C are pairwise independent. However, the events A, B, C are not independent, since $\mathbb{P}(A \cap B \cap C) = 0 \neq \frac{1}{8} = \mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C)$. The graph on 3 vertices with no edges is the only graph that encodes pairwise independencies of random variables. But since it is not true that A is mutually independent of $\{B, C\}$ (otherwise we would get $\mathbb{P}(A \cap B \cap C) = \mathbb{P}(A)\mathbb{P}(B \cap C) = pA\mathbb{P}(B)\mathbb{P}(C)$), the empty graph is not a dependency digraph of our events.

Theorem 41 (Lovász Local Lemma)**.** Let $A_1, \dots, A_n$ be events and let (V, E) be their dependency digraph. Suppose that there exist real numbers $x_1, \dots, x_n$ such that $0 \leq x_i < 1$ for $i = 1, \dots, n$ and $\mathbb{P}(A_i) \leq x_i \prod_{(i,j)\in E}(1 - x_j)$ for all $i = 1, \dots, n$. Then $\mathbb{P}(\bigcap_{i=1}^n A_i^c) \geq \prod_{i=1}^n (1 - x_i) > 0$.

Remark. Let us consider two extremal cases of Theorem 41. If (V, E) is the complete graph then the assumption gives $\mathbb{P}(A_i) \leq x_i \prod_{j\neq i}(1 - x_i)$. To prove the theorem in this case it suffices use the union bound

$$\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) \geq 1 - \sum_{i=1}^n \mathbb{P}(A_i) \geq 1 - \sum_{i=1}^n x_i \prod_{j\neq i}(1 - x_i).$$

We now only need to verify the inequality $1 - \sum_{i=1}^n x_i \prod_{j\neq i}(1 - x_i) \geq \prod_{i=1}^n (1 - x_i)$. After dividing by $\prod_{i=1}^n (1 - x_i)$ this reduces to $\prod_{i=1}^n \frac{1}{1-x_i} > 1 + \sum_{i=1}^n \frac{x_i}{1-x_i}$, which follows since

$$\prod_{i=1}^n \frac{1}{1 - x_i} = \prod_{i=1}^n \left(1 + \frac{x_i}{1 - x_i}\right) \geq 1 + \sum_{i=1}^n \frac{x_i}{1 - x_i}.$$

The other extremal case is $E = \emptyset$. In this case it is not hard to deduce that the events $A_1, \dots, A_n$ are independent and $\mathbb{P}(A_i) \leq x_i$. Thus $\mathbb{P}(\bigcap A_i^c) = \prod_{i=1}^n \mathbb{P}(A_i^c) \geq \prod_{i=1}^n (1 - x_i) > 0$.

In fact one can formulate a more genera version of the lemma, where no notion of mutual independence is needed.

Theorem 42. Let $A_1, \dots, A_n$ be events and let (V, E) be any directed graph on $V = \{1, \dots, n\}$ with no loops. Suppose there exist numbers $x_1, \dots, x_n$ such that $0 \leq x_i < 1$ for $i = 1, \dots, n$ and that for any $i = 1, \dots, n$ and any $S \subseteq \{j : (i,j) \notin E\} \setminus \{i\}$ we have

$$\mathbb{P}\left(A_i \,\middle|\, \bigcap_{j\in S} A_j^c\right) \leq x_i \prod_{j:(i,j)\in E} (1 - x_j). \tag{5}$$

Then $\mathbb{P}(\bigcap_{i=1}^n A_i^c) \geq \prod_{i=1}^n (1 - x_i) > 0$.

We first show how Theorem 42 implies Theorem 41.

Proof of Theorem 41. We shall use Theorem 42 with (V, E) being the dependency graph of our events. Take $i \in \{1, \ldots, n\}$ and let $S \subseteq \{j : (i,j) \notin E\} \setminus \{i\}$ By the definition of dependency graph and by (4) we get

$$\mathbb{P}\left(A_i \;\middle|\; \bigcap_{j \in S} A_j^c\right) = \mathbb{P}(A_i) \leq x_i \prod_{j:(i,j)\in E} (1 - x_j).$$

Thus the assumption of Theorem 42 is satisfied. □

Before we prove Theorem 42 we recall some simple facts concerning conditional probabilities.

1. For any events $B_1, \ldots, B_n, C$ we have

$$\mathbb{P}(B_1 \cap \ldots \cap B_n | C) = \mathbb{P}(B_1|C) \cdot \mathbb{P}(B_2|B_1 \cap C) \cdot \ldots \cdot \mathbb{P}(B_n|B_1 \cap B_2 \cap \ldots \cap B_{n-1} \cap C). \tag{6}$$

   This can be proved easily by using definition of conditional probability and observing that the right hand side is a telescoping product.

2. For any events A, B, C we have

$$\mathbb{P}(A|B \cap C) = \frac{\mathbb{P}(A \cap B|C)}{\mathbb{P}(B|C)} \tag{7}$$

   This is in fact (6) for $n = 2$.

Proof of Theorem 42. We shall prove the following claim:

Claim. For any $S \subseteq \{1, \ldots, n\}$ with $|S| < n$ and for any $i \notin S$ we have

$$\mathbb{P}\left(A_i \;\middle|\; \bigcap_{j \in S} A_j^c\right) \leq x_i.$$

Here for $S = \emptyset$ we adapt the notation $\bigcap_{j\in\emptyset} A_j^c = \Omega$. We now show how this claim implies our theorem. By (6) applied with $B_i = A_i^c$ and $C = \Omega$ we get

$$\begin{aligned}
\mathbb{P}(A_1^c \cap \ldots \cap A_n^c) &= \mathbb{P}(A_1^c) \cdot \mathbb{P}(A_2^c|A_1^c) \cdot \mathbb{P}(A_3^c|A_1^c \cap A_2^c) \cdot \ldots \cdot \mathbb{P}\left(A_n^c|A_1^c \cap \ldots \cap A_{n-1}^c\right) \\
&= (1 - \mathbb{P}(A_1)) \cdot (1 - \mathbb{P}(A_2|A_1^c)) \cdot (1 - \mathbb{P}(A_3|A_1^c \cap A_2^c)) \cdot \ldots \cdot \left(1 - \mathbb{P}\left(A_n|A_1^c \cap \ldots \cap A_{n-1}^c\right)\right) \\
&\geq (1 - x_1)(1 - x_2)(1 - x_3)\ldots(1 - x_n) > 0,
\end{aligned}$$

where the claim was applied for the following pairs (i, S):

$$(1, \emptyset), \quad (2, \{1\}), \quad (3, \{1, 2\}), \qquad \ldots, \qquad (n, \{1, 2, \ldots, n-1\}).$$

Proof of the Claim. Induction on $s = |S|$. If $s = 0$ then $S = \emptyset$ and the claim $\mathbb{P}(A_i) \leq x_i$ follows easily from the assumption. Now, suppose the assertion holds true for $s' < s$. We shall show it for s. Take $S \subseteq \{1, \ldots, n\}$ with $|S| = s$ and $i \notin S$. Define $S_1 = \{j \in S : (i,j) \in E\}$ and $S_2 = S \setminus S_1$. If $S_1 = \emptyset$ then $S \subseteq \{1, \ldots, n\} \setminus (\{j : (i,j) \in E\} \cup \{i\}) = \{j : (i,j) \notin E\} \setminus \{i\}$, thus we get

$$\mathbb{P}\left(A_i \;\middle|\; \bigcap_{j \in S} A_j^c\right) \leq x_i \prod_{j:(i,j)\in E} (1 - x_j) \leq x_i,$$

by the assumptions of our theorem. Thus, suppose that S_1 is nonempty. Define

$$A = A_i, \qquad B = \bigcap_{j \in S_1} A_j^c, \qquad C = \bigcap_{l \in S_2} A_l^c.$$

By (7) we get

$$\mathbb{P}\left(A_i \;\middle|\; \bigcap_{j\in S} A_j^c\right) = \mathbb{P}\left(A_i \;\middle|\; B\cap C\right) = \frac{\mathbb{P}\left(A_i\cap B \mid C\right)}{\mathbb{P}\left(B \mid C\right)}.$$

Let us upper bound the numerator. Since $S_2 \subseteq \{j : (i,j)\notin E\}\setminus\{i\}$, by the assumptions of the theorem we have

$$\mathbb{P}\left(A_i\cap B \mid C\right) \le \mathbb{P}\left(A_i|C\right) = \mathbb{P}\left(A_i \;\middle|\; \bigcap_{l\in S_2} A_l^c\right) \le x_i \prod_{j:(i,j)\in E}(1-x_j). \tag{8}$$

To lower bound the denominator we shall use induction hypothesis. Suppose $S_1 = \{j_1,\ldots,j_r\}$ with $r\ge 1$. From (6) we get

$$\begin{aligned}\mathbb{P}\left(B|C\right) &= \mathbb{P}\left(A_{j_1}^c\cap\ldots\cap A_{j_r}^c \mid C\right) = \mathbb{P}\left(A_{j_1}^c|C\right)\cdot\mathbb{P}\left(A_{j_2}^c|A_{j_1}^c\cap C\right)\cdot\ldots\cdot\mathbb{P}\left(A_{j_r}^c|A_{j_1}^c\cap\ldots\cap A_{j_{r-1}}^c\right)\\ &= \left(1-\mathbb{P}\left(A_{j_1}|C\right)\right)\left(1-\mathbb{P}\left(A_{j_2}|A_{j_1}^c\cap C\right)\right)\cdot\ldots\cdot\left(1-\mathbb{P}\left(A_{j_r}|A_{j_1}^c\cap\ldots\cap A_{j_{r-1}}^c\right)\right)\\ &\ge (1-x_{j_1})(1-x_{j_2})\ldots(1-x_{j_r}) \ge \prod_{j:(i,j)\in E}(1-x_j).\end{aligned}$$

The assertion follows by combining this inequality with (8),

$$\mathbb{P}\left(A_i \;\middle|\; \bigcap_{j\in S} A_j^c\right) = \frac{\mathbb{P}\left(A_i\cap B \mid C\right)}{\mathbb{P}\left(B \mid C\right)} \le \frac{x_i\prod_{j:(i,j)\in E}(1-x_j)}{\prod_{j:(i,j)\in E}(1-x_j)} = x_i.$$

□

The proof of the theorem is completed. □

Usually the following symmetric version of the lemma is the most convenient. It easily follows from Theorem 41.

Theorem 43. Let $A_1,\ldots,A_n$ be events. Suppose that for any i the event A_i is mutually independent of a set of all the other events A_j but at most d. Also, suppose that $\mathbb{P}\left(A_i\right)\le p$, where $0\le p<1$ satisfies $ep(d+1)\le 1$. Then $\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) > 0$.

Proof. Let us construct a dependency digraph for our events by taking, for each i, all the edges from i to $\{j : j\notin S_i\}$. Thus, the out-degree of every vertex is at most d. Take $x_i = \frac{1}{d+1}$. We can assume that $d\ge 0$ (to make sure that $x_i\ne 1$) since otherwise the events A_i are independent and the claim follows easily. Then in order to apply Theorem 41 it suffices to check that $p\le \frac{1}{d+1}\left(1-\frac{1}{d+1}\right)^d$. This is true since $\left(1-\frac{1}{d+1}\right)^d > \frac{1}{e}$, which follows by taking logarithm and applying the well known inequality $\ln(1+x)\ge\frac{x}{x+1}$. □

We now present selected applications of the Lovász Local Lemma.

Theorem 44. Suppose $k\ge 10$. Then the vertices of every k-regular simple graph can be colored in such a way that no vertex has a monochromatic neighborhood.

Proof. We can assume that the graph is connected. Let us color the vertices with two colors at random (each color with probability 1/2). Let A_v the the event that the vertex v has a monochromatic neighborhood. Let V_k^v for $k\ge 1$ be the set of vertices having distance k from v. The indicator of A_v is a function of the colors of vertices from the set V_1^v. On the other hand the indicators of A_w for $w\in\bigcup_{k\ge 3} V_k^v$ is a function of colors of vertices from $V_3^v, V_4^v,\ldots$. Thus, $\mathbf{1}_{A_v}$ is independent of the random variable $(\mathbf{1}_{A_w})_{w\in\bigcup_{k\ge 3} V_k^v}$. Thus, for every vertex v the event A_v is mutually independent of all the events A_w but at most $k+k(k-1)=k^2$. Clearly $\mathbb{P}\left(A_v\right)=2^{-k+1}$. If $e2^{-k+1}(k^2+1)\le 1$, then Theorem 43 can be applied. This holds true when $k\ge 10$. □

Theorem 45. Let $w(k)$ be the van der Waerden number, that is, the smallest number with the following property: whenever $n \geq w(k)$ then in every coloring of $\{1, \ldots, n\}$ with 2 colors there exists a monochromatic arithmetic progression of length k. Then $w(k) \geq \frac{2^k}{2ek^2}$.

Proof. Let us color the numbers from $\{1, \ldots, n\}$ with two colors at random (each color with probability $1/2$). Let c be an arithmetic progression (AP) in $\{1, \ldots, n\}$. Let A_c be the event that c is monochromatic. Clearly $\mathbb{P}(A_c) = 2^{-k+1}$. Now, if $c, c_1, c_2, \ldots, c_l$ are AP's such that $c \cap \bigcup_{i=1}^{l} c_i = \emptyset$, then A_c is independent of the family $(A_{c_i})_{i=1}^{l}$ (since A_c depends on the colors of numbers disjoint from the set of numbers forming the AP c_i). Let c be an AP. Then c has a common element with at most $k^2(n-1)$ other AP's. Indeed, to get an AP c' that intersects c it is enough to choose an element of c that will be contained in c' (there are k ways to do this), choose a position of this element in c' (in k ways) and choose the difference between two consecutive elements in c' (in at most $n-1$ ways). We get that A_c is independent of all but at most $k^2(n-1) \leq k^2 n - 1$ events $A_{c'}$. Thus applying Theorem 43 with $d = k^2 n - 1$ and $p = 2^{-k+1}$ shows that if $e2^{-k+1}k^2 n \leq 1$ then there is a coloring with no monochromatic k-AP. Thus $w(k) > \frac{2^k}{2ek^2}$. □

6 Fourier analysis on the hypercube

6.1 Walsh-Fourier system

In this section we shall work with the probability space $\Omega = \{-1, 1\}^n$ with the uniform measure $p(\omega) = 2^{-n}$ for all $\omega \in \Omega$. Note that in $f : \Omega \to \mathbb{R}$ is a random variable, then $\mathbb{E}f = 2^{-n} \sum_{x \in \Omega} f(x)$. For $f, g : \Omega \to \mathbb{R}$ we shall define $\langle f, g \rangle = \mathbb{E}[fg] = 2^{-n} \sum_{x \in \Omega} f(x)g(x)$. Since every function on Ω can we interpreted as a vector in $\mathbb{R}^{2^n}$, we see that $\langle f, g \rangle$ is just a normalized scalar product of these vectors corresponding to f and g.

For $S \subseteq [n]$ (here $[n] = \{1, \ldots, n\}$) consider a function $w_S : \{-1, 1\}^n \to \mathbb{R}$ defined by $w_S(x) = \prod_{i \in S} x_i$. Here we use a convention $w_\emptyset(x) \equiv 1$. Note that

$$\mathbb{E}w_S = \begin{cases} 0 & S \neq \emptyset \\ 1 & S = \emptyset \end{cases}.$$

Clearly,

$$w_S(x)w_T(x) = \prod_{i \in S} x_i \prod_{j \in T} x_j = \prod_{i \in S \Delta T} x_i \prod_{i \in S \cap T} x_i^2 = \prod_{i \in S \Delta T} x_i = w_{S \Delta T}(x).$$

Since $w_S w_T = w_{S \Delta T}$, we get

$$\mathbb{E}[w_S w_T] = \begin{cases} 0 & S \neq T \\ 1 & S = T \end{cases}, \qquad \text{in other words} \qquad \langle w_S, w_T \rangle = \begin{cases} 0 & S \neq T \\ 1 & S = T \end{cases}$$

The function w_S are therefore linearly independent. Indeed, if $\sum_{S \subseteq [n]} a_S w_S \equiv 0$ the by taking a scalar product with w_T we get

$$0 = \left\langle \sum_{S \subseteq [n]} a_S w_S, w_T \right\rangle = \sum_{S \subseteq [n]} a_S \langle w_S, w_T \rangle = a_T.$$

Since the dimension of $\{f : \Omega \to \mathbb{R}\}$ is clearly equal to 2^n, we get that $(w_S)_{S \subseteq [n]}$ is an orthonormal basis, that is every function $f : \Omega \to \mathbb{R}$ admits an unique expansion $f = \sum_{S \subseteq [n]} a_S w_S$. By taking a scalar product of both sides with w_T we get that $a_T = \langle f, w_T \rangle$. We define the *Fourier coefficient* $\widehat{f}(S) = \langle f, w_T \rangle$. The set of numbers $(\widehat{f}(S))_{S \subseteq [n]}$ is called the *spectrum* of f. We get

$$f = \sum_{S \subseteq [n]} \langle f, w_S \rangle w_S = \sum_{S \subseteq [n]} \widehat{f}(S) w_S.$$

This can be also seen by an elementary argument. Indeed, the indicator of $\{x\}$ satisfies

$$\mathbf{1}_x(y) = \prod_{i=1}^{n} \frac{1 + x_i y_i}{2} = 2^{-n} \sum_{S \subseteq [n]} w_S(x) w_S(y).$$

Hence,

$$f(x) = \sum_{y \in \Omega} f(y) \mathbf{1}_y(x) = \sum_{S \subseteq [n]} \left(2^{-n} \sum_{y \in \Omega} f(y) w_S(y) \right) w_S(x) = \sum_{S \subseteq [n]} \langle f, w_S \rangle \, w_S(x).$$

Note that we have $\mathbb{E} f = a_\emptyset$ and by orthogonality

$$\mathbb{E}[f^2] = \mathbb{E}\left[\left(\sum_{S \subseteq [n]} a_S w_S \right)^2 \right] = \sum_{S,T \subseteq [n]} a_S a_T \mathbb{E}[w_S w_T] = \sum_{S \subseteq [n]} a_S^2.$$

This is the so-called *Parseval's identity*. We also note that

$$\mathrm{Var}(f) = \mathbb{E}[f^2] - (\mathbb{E}[f])^2 = \sum_{S \neq \emptyset} a_S^2.$$

We also observe that if $f = \sum_{S \subseteq [n]} a_S w_S$ and $g = \sum_{S \subseteq [n]} b_S w_S$, then

$$\langle f, g \rangle = \left\langle \sum_S a_S w_S, \sum_S b_S w_S \right\rangle = \sum_{S,T} a_S b_T \langle w_S, w_T \rangle = \sum_S a_S b_S.$$

6.2 Poincaré inequality

For $f : \Omega \to \mathbb{R}$ we define its ith *gradient* by

$$(\nabla_i f)(x) = \frac{f(x) - f(x^i)}{2}, \qquad \text{where} \quad x^i = (x_1, \ldots, -x_i, \ldots, x_n).$$

The *gradient* of f is defined as $(\nabla_i f, \ldots, \nabla_n f) : \Omega \to \mathbb{R}^n$. We also take $|\nabla f| = (\sum_{i=1}^n |\nabla_i f|^2)^{1/2}$.

Theorem 46. For every $f : \Omega \to \mathbb{R}$ we have $\mathrm{Var}(f) \leq \mathbb{E}[|\nabla f|^2]$.

Proof. To this end consider the Walsh-Fourier expansion of f, namely $f = \sum_{S \subseteq [n]} a_S w_S$. Recall that then $\mathrm{Var}(f) = \sum_{|S| \geq 1} a_S^2$. Observe that

$$\nabla_i w_S = \begin{cases} w_S & i \in S \\ 0 & i \notin S \end{cases}.$$

Let us compute the Walsh-Fourier expansion of $\nabla_i f$,

$$(\nabla_i f)(x) = \sum_{S \subseteq [n]} a_S (\nabla_i w_S)(x) = \sum_{S : i \in S} a_S w_S(x).$$

Thus, Parseval's identity gives $\mathbb{E}[|\nabla_i f|^2] = \sum_{S : i \in S} a_S^2$. Therefore,

$$\mathbb{E}[|\nabla f|^2] = \sum_{i=1}^n \mathbb{E}[|\nabla_i f|^2] = \sum_{i=1}^n \sum_{S : i \in S} a_S^2 = \sum_S |S| a_S^2 = \sum_{S : \, |S| \geq 1} |S| a_S^2 \geq \sum_{|S| \geq 1} a_S^2 = \mathrm{Var}(f).$$

□

Note that in Ω we can introduce a graph structure by taking $x \sim y$ if and only if $|x-y|=2$ (that is, x, y differ on precisely one coordinate). If we now take $A \subseteq \Omega$ and

$$f(x) = \begin{cases} 1 & x \in A \\ -1 & x \notin A \end{cases},$$

then $\mathbb{E}[f] = 2^{-n}(|A| - |A^c|)$ and thus

$$\begin{aligned} \mathrm{Var}(f) &= \mathbb{E}[f^2] - (\mathbb{E}[f])^2 = 1 - (2^{-n}(|A| - |A^c|))^2 = (1 - 2^{-n}|A| + 2^{-n}|A^c|)(1 + 2^{-n}|A| - 2^{-n}|A^c|) \\ &= 2^{-n}(2^n - |A| + |A^c|) \cdot 2^{-n}(2^n - |A^c| + |A|) = 4^{-n} \cdot 2|A| \cdot 2|A^c| = 4^{-n+1}|A| \cdot |A^c| \end{aligned}$$

Moreover, we see that

$$\mathbb{E}[|\nabla_i f|^2] = 2^{-n} \cdot 2\#\{\text{egdes between } A \text{ and } A^c \text{ in the } i\text{th direction}\},$$

since the endpoints x, y of every such edge satisfy $|\nabla_i f|(x) = |\nabla_i f|(y) = 1$ and if x, y both belong to A or to A^c then $|\nabla_i f|(x) = |\nabla_i f|(y) = 0$. Define $\partial A = \{(a, a') \in A \times A^c : \ a \sim a'\}$. Then

$$\mathbb{E}[|\nabla f|^2] = \sum_{i=1}^{n} \mathbb{E}[|\nabla_i f|^2] = 2^{-n+1}|\partial A|.$$

Thus the Poincaré inequality gives $2^{-n+1}|\partial A| \geq 4^{-n+1}|A| \cdot |A^c|$, that is,

$$|\partial A| \geq 2^{-n+1}|A| \cdot |A^c|.$$

In particular, if $|A| = 2^{n-1}$ then we get $|\partial A| \geq 2^{n-1}$, which is optimal (take $A = \{1\} \times \{-1, 1\}^{n-1}$).

6.3 The Blum-Luby-Rubinfeld Test

For $x, y \in \Omega$ we define $x \cdot y = (x_1 y_1, \ldots, x_n y_n)$. It is easy to see that for $f : \{-1, 1\}^n \to \{-1, 1\}$ the following two conditions are equivalent:

(1) $f(x \cdot y) = f(x)f(y)$, $x, y \in \{-1, 1\}^n$,

(2) for some $S \subseteq [n]$ we have $f = w_S$.

Suppose now that we want to consider approximately multiplicative functions. We can define this notion either through point (1) or using (2). The definition (2') reads as follows:

(2') $f : \{-1, 1\}^n \to \{-1, 1\}$ is ε close to being multiplicative if there is w_S such that $\mathbb{P}_x(f(x) \neq w_S(x)) \leq \varepsilon$, where x is uniform on $\{-1, 1\}^n$.

Here we write $\mathbb{P}_x$ to remember that the randomness is with respect to x. The definition (1) can be rewritten using the so called Blum-Luby-Rubinfeld test. In BLR test we consider two independent random inputs $x, y \in \Omega$ and accept f if $f(x \cdot y) = f(x)f(y)$. Thus, this test uses only three queries.

(1') We say that f is ε BLR-close to being multiplicative if $\mathbb{P}_{x,y}(f(x \cdot y) = f(x)f(y)) \geq 1 - \varepsilon$, where x, y are independent and uniform in $\{-1, 1\}^n$. In other words, BLR test excepts f with probability at least $1 - \varepsilon$.

We show that both definitions are equivalent. First, if f is ε close to certain w_S then BLR test accepts f with probability at least $1 - 3\varepsilon$, since

$$\begin{aligned} \mathbb{P}(f(x \cdot y) \neq f(x)f(y)) &\leq \mathbb{P}(f(x) \neq w_S(x) \text{ or } f(x) \neq w_S(y) \text{ or } f(x \cdot y) \neq w_S(x \cdot y)) \\ &\leq \mathbb{P}(f(x) \neq w_S(x)) + \mathbb{P}(f(y) \neq w_S(y)) + \mathbb{P}(f(x \cdot y) \neq w_S(x \cdot y)) \\ &= 3\mathbb{P}(f(x) \neq w_S(x)) \leq 3\varepsilon. \end{aligned}$$

What is non-trivial is that we have the reverse implication.

Theorem 47. If BLR test accepts f with probability at least $1-\varepsilon$ then f is ε close to certain w_S.

Proof. Take $f:\{-1,1\}^n \to \{-1,1\}$. Let $h(x) = \mathbb{E}_y f(y)f(x\cdot y)$. If $f = \sum_S a_S w_S$ then

$$h(x) = \mathbb{E}_y \left(\sum_S a_S w_S(y)\right)\left(\sum_S a_S w_S(x\cdot y)\right) = \mathbb{E}_y \left(\sum_S a_S w_S(y)\right)\left(\sum_S a_S w_S(x)w_S(y)\right)$$
$$= \sum_{S,T} a_S a_T w_S(x)\mathbb{E}_y w_S(y)w_T(y) = \sum_S a_S^2 w_S(x).$$

using orthogonality of the Walsh system. We have

$$\frac{1}{2} + \frac{1}{2}f(x)f(y)f(x\cdot y) = \begin{cases} 1 & f(x)f(y) = f(x\cdot y) \\ 0 & f(x)f(y) \neq f(x\cdot y) \end{cases}.$$

Thus,

$$1-\varepsilon = \mathbb{P}_{x,y}(f(x\cdot y) = f(x)f(y)) = \mathbb{E}\left(\frac{1}{2} + \frac{1}{2}f(x)f(y)f(x\cdot y)\right)$$
$$= \frac{1}{2} + \frac{1}{2}\mathbb{E}_x f(x)\mathbb{E}_y f(y)f(x\cdot y) = \frac{1}{2} + \frac{1}{2}\mathbb{E}_x f(x)h(x).$$

We get

$$1-2\varepsilon = \mathbb{E}_x f(x)h(x) = \sum_S a_S^3 \leq (\max_S a_S)\sum_S a_S^2 = \max_S a_S.$$

Therefore, there exists w_S such that $1-2\varepsilon \leq \mathbb{E} f w_S = 1 - 2\mathbb{P}_x(f(x) \neq w_S(x))$. Thus, f is ε close to w_S. □

6.4 Arrow's theorem

Suppose we have three candidates a, b, c and we want to elect one using some voting procedure. Assume we have n voters and each voter has his own ranking of candidates. In other words for each pair (a,b), (b,c), (c,a) a voter gives a number in $\{-1,1\}$, with 1 meaning that he prefers the first candidate. Thus, each voter V_i delivers a triple $(x_i, y_i, z_i) \in \{-1,1\}^3$. Note that only six triples are allowed. Indeed, the triples $(1,1,1)$ and $(-1,-1,-1)$ are not allowed because a voter can not prefer a than b, b than c and c than a (nor the opposite cycle). So, for each voter we have the following allowed rankings

$$(-1,-1,1),(-1,1,-1),(-1,1,1),(1,-1,-1),(1,-1,1),(1,1,-1).$$

Now suppose we use some function $f:\{-1,1\}^n \to \{-1,1\}$ to decide whether the society prefers a than b, etc. by considering $f(x) = f(x_1,\ldots,x_n)$, $f(y) = f(y_1,\ldots,y_n)$ and $f(z) = f(z_1,\ldots,z_n)$. For example $f(x_1,\ldots,x_n) = 1$ means that the society prefers a than b. In other words, w consider all three pairwise elections.

We say that there is a Condorcet winner if there is a candidate who wins all the pairwise elections he participated in. So, there is a Condorcet winner if

$$(f(x), f(y), f(z)) \in \{(-1,-1,1),(-1,1,-1),(-1,1,1),(1,-1,-1),(1,-1,1),(1,1,-1)\}.$$

Here is an example of a voting with Condorcet winner.

However, the following voting shows that there may not be a Condorcet winner. This is called the Condorcet paradox.

We show that essentially the only voting scheme free from the Condorcet paradox is dictatorship.

	V_1	V_2	V_3	f
$a(+)$ vs. $b(-)$	$+$	$+$	$+$	$+$
$b(+)$ vs. $c(-)$	$-$	$+$	$-$	$-$
$c(+)$ vs. $a(-)$	$+$	$-$	$-$	$-$

Table 1: Voting with $n = 3$ voters using $f(x) = \mathrm{sgn}(x_1 + x_2 + x_3)$. Here we get the ranking $(1, -1, -1)$ which means $c > a > b$ and thus c is the winner.

	V_1	V_2	V_3	f
$a(+)$ vs. $b(-)$	$+$	$+$	$-$	$+$
$b(+)$ vs. $c(-)$	$+$	$-$	$+$	$+$
$c(+)$ vs. $a(-)$	$-$	$+$	$+$	$+$

Table 2: Voting with $n = 3$ voters using $f(x) = \mathrm{sgn}(x_1 + x_2 + x_3)$. Here we get the ranking $(1, 1, 1)$ which means $a > b$, $b > c$ and $c > a$ and thus we cannot choose a winner.

Theorem 48 (Arrow's Theorem)**.** Let $f : \{-1, 1\}^n \to \{-1, 1\}$ be the voting rule used in three candidate Condorcet elections. If there is always a Condorcet winner, then $f(x) = \pm x_k$ for some $k \in [n]$.

Proof. Let us do a random election. Each voter chooses one of the 6 possible rankings uniformly at random. We compute the probability of Condorcet winner. For this we need a function $\sigma : \{-1, 1\}^3 \to \{0, 1\}$ which is equal to 1 if and only if the argument (x, y, z) does not belong to the set $\{(-1, -1, -1), (1, 1, 1)\}$. It is easy to see that

$$\sigma(x, y, z) = \frac{3}{4} - \frac{1}{4}(xy + yz + zx).$$

Thus,

$$\begin{aligned}\mathbb{P}(\exists \text{ Condorcet winner}) &= \mathbb{E}\sigma(f(x), f(y), f(z)) \\ &= \frac{3}{4} - \frac{1}{4}\mathbb{E}[f(x)f(y) + f(y)f(z) + f(z)f(x)] = \frac{3}{4} - \frac{3}{4}\mathbb{E}[f(x)f(y)].\end{aligned}$$

Recall that (x_i, y_i, z_i), $i = 1, \ldots, n$ are independent. Moreover, the distribution of each (x_i, y_i, z_i) is uniform over all 6 admissible rankings. Therefore, it is easy to see that $\mathbb{E}x_i = \mathbb{E}y_i = 0$ and $\mathbb{E}x_iy_i = -\frac{1}{3}$. Let $f = \sum_S a_S w_S$. We get

$$\begin{aligned}\mathbb{E}[f(x)f(y)] &= \sum_{S,T} a_S a_T \mathbb{E}[w_S(x)w_T(y)] = \sum_S a_S^2 \mathbb{E}[w_S(x)w_S(y)] \\ &= \sum_S a_S^2 (\mathbb{E}[x_1y_1])^{|S|} = \sum_S a_S^2 \left(-1/3\right)^{|S|}.\end{aligned}$$

We arrive at

$$\mathbb{P}(\exists \text{ Condorcet winner}) = \frac{3}{4} - \frac{3}{4}\sum_S a_S^2 \left(-1/3\right)^{|S|}.$$

Let $W_k[f] = \sum_{|S|=k} a_S^2$. We have

$$\begin{aligned}\frac{3}{4} - \frac{3}{4}\sum_S a_S^2 (-1/3)^{|S|} &= \frac{3}{4} - \frac{3}{4}\sum_{k=0}^{n} W_k[f] (-1/3)^k \le \frac{3}{4} - \frac{3}{4}\sum_k W_{2k+1}[f] (-1/3)^{2k+1} \\ &= \frac{3}{4} + \frac{3}{4}\sum_k W_{2k+1}[f] (1/3)^{2k+1} \le \frac{3}{4} + \frac{3}{4}\left(\frac{1}{3}W_1[f] + \frac{1}{27}\sum_{k>0} W_{2k+1}[f]\right) \\ &\le \frac{3}{4} + \frac{3}{4}\left(\frac{1}{3}W_1[f] + \frac{1}{27}(1 - W_1[f])\right) = \frac{7}{9} + \frac{2}{9}W_1[f] = \frac{7}{9} + \frac{2}{9}\sum_{k=1}^{n} a_{\{k\}}^2.\end{aligned}$$

Thus,

$$1 = \mathbb{P}(\exists \text{ Condorcet winner}) \le \frac{7}{9} + \frac{2}{9}\sum_{k=1}^{n} a_{\{k\}}^2 \le \frac{7}{9} + \frac{2}{9}\sum_S a_S^2 = 1.$$

Thus $\sum_{k=1}^n a_{\{k\}}^2 = \sum_S a_S^2 = 1$ which implies $f(x) = \sum_{k=1}^n a_{\{k\}} x_k$. Taking $x_i = \operatorname{sgn}(a_{\{i\}})$ for $a_i \neq 0$ (and $x_i = 1$ when $a_{\{i\}} = 0$) we get $\sum_k |a_{\{k\}}| = 1$. Together with $\sum_{k=1}^n a_{\{k\}}^2 = 1$ this gives the existence of l such that $|a_{\{l\}}| = 1$ and $a_{\{k\}} = 0$ for all $k \neq l$. Thus $f(x) = \pm x_k$.

□

7 Spectral graph theory

7.1 Min-max principle & Cauchy interlacing

Recall that if A is a symmetric real $n \times n$ matrix, then the matrix A is diagonalizable using orthogonal matrix, namely there exist an orhogonal matrix U (that is, matrix satisfying $U^T U = I$) and a diagonal matrix $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ such that $A = UDU^T$. In other words, the columns $u_1, \ldots, u_n$ of U form an orthonormal basis for $\mathbb{R}^n$ and $Au_i = \lambda_i u_i$. To see the latter we observe that the equality $A = UDU^T$ is equivalent to $U^T A = DU^T$ and by taking transposition of both sides we get $AU = UD$, which precisely means that $Au_i = \lambda_i u_i$.

If $u_1, \ldots, u_n$ is an orthonormal basis of eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_n$, then for every x written in this basis, that is $x = \sum_{i=1}^n a_i u_i$, we have

$$\begin{aligned}\langle Ax, x\rangle &= \left\langle A\left(\sum_{i=1}^n a_i u_i\right), \sum_{i=1}^n a_i u_i \right\rangle = \left\langle \sum_{i=1}^n a_i A u_i, \sum_{i=1}^n a_i u_i \right\rangle = \left\langle \sum_{i=1}^n \lambda_i a_i u_i, \sum_{i=1}^n a_i u_i \right\rangle \\ &= \sum_{i,j=1}^n \lambda_i a_i a_j \langle u_i, u_j\rangle = \sum_{i=1}^n \lambda_i a_i^2.\end{aligned}$$

Repeating the same computation for $A = I$ gives $|x|^2 = \langle x, x\rangle = \sum_{i=1}^n a_i^2$.

Theorem 49 (Courant–Fischer–Weyl min-max principle)**.** Let A be a symmetric matrix with eigenvalues $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$. Then for every $k = 1, 2, \ldots, n$ we have

$$\lambda_k = \max_{U:\ \dim(U)=k} \min_{x\in U,\ x\neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle} = \min_{U:\ \dim(U)=n-k+1} \max_{x\in U,\ x\neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

In particular

$$\lambda_1 = \max_{x\neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}, \qquad \lambda_n = \min_{x\neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

Proof. Let $u_1, \dots, u_n$ be the orthonormal basis for $\mathbb{R}^n$ such that u_i is an eigenvector with an eigenvalue λ_i, $i = 1, \dots, n$. Take a subspace U of $\mathbb{R}^n$ such that $\dim(U) = k$ and take $V = \operatorname{span}\{u_k, \dots, u_n\}$. Note that $U \cap V$ contains a non-zero vector x. Thus, $x = \sum_{i=k}^{n} a_i u_i$. Therefore,

$$\frac{\langle Ax, x\rangle}{\langle x, x\rangle} = \frac{\sum_{i=k}^{n} \lambda_i a_i^2}{\sum_{i=k}^{n} a_i^2} \le \lambda_k.$$

It follows that

$$\lambda_k \ge \min_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

and therefore

$$\lambda_k \ge \max_{U:\ \dim(U)=k} \min_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

To see the opposite inequality it suffices to take $U = \operatorname{span}\{u_1, \dots, u_k\}$. Observe that every $x \in U$ has the form $x = \sum_{i=1}^{k} \lambda_i u_i$. We get

$$\frac{\langle Ax, x\rangle}{\langle x, x\rangle} = \frac{\sum_{i=1}^{k} \lambda_i a_i^2}{\sum_{i=1}^{k} a_i^2} \ge \lambda_k$$

Thus,

$$\min_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle} \ge \lambda_k.$$

We get

$$\lambda_k \le \max_{U:\ \dim(U)=k} \min_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}.$$

The equality

$$\lambda_k = \max_{U:\ \dim(U)=n-k+1} \min_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}$$

can be proved in a similar way. □

Theorem 50. Suppose A is an $n \times n$ symmetric matrix with eigenvalues $\lambda_1 \ge \ldots \ge \lambda_n$. Let B be its principal $m \times m$ submatrix and assume that B has eigenvalues $\mu_1 \ge \ldots \ge \mu_m$. Then

$$\lambda_k \ge \mu_k \ge \lambda_{k+n-m}, \qquad k = 1, \dots, m.$$

Proof. By the Courant–Fischer–Weyl min-max principle we have

$$\lambda_k = \max_{U \subseteq \mathbb{R}^n,\ \dim(U)=k} \min_{x \in U, x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}, \qquad \mu_k = \max_{U \subseteq \mathbb{R}^m,\ \dim(U)=k} \min_{x \in U, x \neq 0} \frac{\langle Bx, x\rangle}{\langle x, x\rangle}$$

Without loss of generality we can assume that $B = (A_{ij})_{1 \le i,j \le m}$. In this case $\langle Bx, x\rangle = \langle Ay, y\rangle$, where $y = (x, 0) \in \mathbb{R}^n$ (here $x \in \mathbb{R}^m$ and $0 \in \mathbb{R}^{n-m}$). Thus we have

$$\mu_k = \max_{\substack{U \subseteq \mathbb{R}^n,\ \dim(U)=k \\ U \subseteq \{x_{m+1} = \ldots = x_n\}}} \min_{x \in U, x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle} \quad \le \quad \lambda_k.$$

To prove the second inequality we observe that again by the Courant–Fischer–Weyl min-max principle we have

$$\mu_k = \min_{U:\ \dim(U)=m-k+1} \max_{x \in U,\ x \neq 0} \frac{\langle Bx, x\rangle}{\langle x, x\rangle}, \qquad \lambda_{k+n-m} = \min_{U:\ \dim(U)=m-k+1} \max_{x \in U,\ x \neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle}$$

Thus, again by the same observation as above,

$$\mu_k = \min_{\substack{U\subseteq\mathbb{R}^n,\ \dim(U)=m-k+1 \\ U\subseteq\{x_{m+1}=\ldots=x_n\}}} \max_{x\in U, x\neq 0} \frac{\langle Ax, x\rangle}{\langle x, x\rangle} \quad \geq \quad \lambda_{k+n-m}.$$

□

7.2 Basic facts in spectral graph theory

For a graph $G = (V, E)$ with n vertices we define its adjacency matrix $A = (a_{uv})_{u,v\in V}$ by taking

$$a_{uv} = \begin{cases} 1 & u \sim v \\ 0 & \text{otherwise} \end{cases}.$$

The matrix A is symmetric and thus has real eigenvalues $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n$.

Lemma 7. Suppose A is an adjacency matrix of a d regular graph G. Then

(a) for any $x \in \mathbb{R}^n$ we have $\langle x, (dI - A)x\rangle = \sum_{\{u,v\}\in E}(x_u - x_v)^2 \geq 0$,

(b) the larges eigenvalue λ_1 of A is equal d and the corresponding eigenvector is $\mathbf{1} = (1, \ldots, 1)$.

Proof. (a) For any vector $x \in \mathbb{R}^n$ we have

$$\langle x, (dI - A)x\rangle = d\sum_{v\in V} x_v^2 - 2\sum_{\{u,v\}\in E} x_u x_v = \sum_{\{u,v\}\in E}(x_u - x_v)^2 \geq 0.$$

Here the notation $\{u, v\} \in E$ means that the edge (u, v) is the same as (v, u) and is counted once.

(b) If $\mathbf{1} = (1, \ldots, 1)$ then $A\mathbf{1} = d\mathbf{1}$ (this is due to the fact that G is d-regular). Thus d is an eigenvalue of A and thus $\lambda_1 \geq d$. In the proof of point (a) we showed that $\langle Ax, x\rangle \leq d|x|^2$. From Theorem 49 we get $\lambda_1 = \max_{x\neq 0} \langle Ax, x\rangle / |x|^2 \leq d$. □

We also introduce the notation

$$e(S, T) = \{(u, v) \mid u \in S, v \in T\}.$$

Note that if $S \cap T = \emptyset$, then $e(S, T) \leq |S| \cdot |T|$. Our next fact provides a reverse bound in terms of second largest eigenvalue of the adjacency matrix.

Fact 1. Let $G = (V, E)$ be a d-regular graph on n vertices. Let λ_2 be the second largest eigenvalue of its adjacency matrix A. Then for every partition $V = S \cup T$ we have

$$e(S, T) \geq \frac{d - \lambda_2}{n} \cdot |S| \cdot |T|.$$

Proof. For any $x \perp \mathbf{1}$ we have $x^T Ax \leq \lambda_2|x|^2$. Indeed, if u_i is the eigenvector corresponding to the eigenvalue λ_i then x can be written as $x = \sum_{i=1}^n a_i u_i$, but since $\langle x, u_1\rangle = \langle x, \mathbf{1}\rangle = 0$ we get $a_1 = 0$ and thus $\sum_{i=2}^n a_i u_i$. It follows that $\langle Ax, x\rangle = \sum_{i=2}^n \lambda_i a_i^2 \leq \lambda_2 \sum_{i=2}^n a_i^2 = \lambda_2|x|^2$.

Take $x = \mathbf{1}_S - \frac{|S|}{n}\mathbf{1}$, where $\mathbf{1}_S$ is the incidence vector of the set S (the position corresponding to the vertex $v \in V$ is 1 if and only if $v \in S$). Clearly $x \perp \mathbf{1}$. We therefore have

$$(d - \lambda_2)|x|^2 \leq \langle x, (dI - A)x\rangle = \sum_{\{u,v\}\in E}(x_u - x_v)^2 = e(S, V \setminus S).$$

To finish the proof it suffices to observe that

$$|x|^2 = \langle x, x\rangle = \left\langle \mathbf{1}_S - \frac{|S|}{n}\mathbf{1}, \mathbf{1}_S - \frac{|S|}{n}\mathbf{1}\right\rangle = |S| - 2\frac{|S|^2}{n} + \frac{|S|^2}{n} = \frac{1}{n}|S|(n-|S|).$$

□

Definition 2. Let $G = (V, E)$ be a d-regular graph. We say that G is an (n, d, ϕ)-edge expander when $|V| = n$, G is d-regular and for any $S \subset V$ with $|S| \leq n/2$ we have $|e(S, S^c)| \geq \phi \cdot d|S|$.

Fact 2. Let λ_2 be the second eigenvalue of the adjacency matrix A of a d regular graph G on n vertices. Then G is a $\left(n, d, \frac{d-\lambda_2}{2d}\right)$-expander.

Proof. From the previous lemma, for $|S| \leq n/2$ we have

$$|e(S, S^c)| \geq \frac{d-\lambda_2}{n}|S|(n-|S|) \geq \frac{d-\lambda_2}{2}|S|.$$

□

Remark. The quantity $\Delta(G) = \frac{d-\lambda_2}{d}$ is called the **spectral gap** of G (more precisely, of the Laplace operator $L = I - \frac{1}{d}A$). The quantity $\phi(G) = \min_{0<|S|\leq n/2} \frac{|e(S,S^c)|}{d|S|}$ is called the **conductance** of the graph G. We showed the inequality $\frac{1}{2}\Delta(G) \leq \phi(G)$. The reverse inequality is also true. This is known as Cheeger inequality, namely $\phi(G) \leq \sqrt{2\Delta(G)}$.

Consider a random d-regular graph on n vertices (we consider all d regular graphs and take each of them with equal probability). What is the expected number of edges going between two disjoint sets S and T? Well, there are $|S| \cdot |T|$ potential edges and each of them will appear with probability d/n. Thus, the answer is $\frac{d}{n}|S| \cdot |T|$. Our next lemma shows that if the quantity $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$ is small, then G behaves like a random graph.

Theorem 51 (Expander mixing lemma)**.** Let $G = (V, E)$ be a d-regular graph on n vertices. Suppose its adjacency matrix has eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_n$. Define $\lambda = \max\{\ |\lambda_2|, |\lambda_n|\}$. Then for $S, T \subseteq V$ we have

$$\left|e(S,T) - \frac{d}{n} \cdot |S| \cdot |T|\right| \ \leq \ \lambda\sqrt{|S| \cdot |T|},$$

where in $e(S, T)$ we count edges contained in the intersection $S \cap T$ twice.

Proof. Let u_i be the eigenvector of A corresponding to λ_i. Recall that we can take $u_1 = \mathbf{1}$. Let J be the all 1's matrix. The vectors u_i are eigenvectors of J. Indeed u_1 is an eigenvector with eigenvalue n. Since u_i for orthogonal basis, we get that $\langle \mathbf{1}, u_i\rangle = \langle u_1, u_i\rangle = 0$ for all $i \geq 2$ and thus for $i \geq 2$ we have $Ju_i = (\langle u_1, , u_i\rangle, \ldots, \langle u_1, u_i\rangle)^T = 0$. Thus, if we take $M = A - \frac{d}{n}J$, then the eigenvalues of M are equal to $0, \lambda_2, \ldots, \lambda_n$ (and the corresponding eigenvector are $u_1, \ldots, u_n$). Let $\mathbf{1}_S$ and $\mathbf{1}_T$ be characteristic vectors of S and T. We observe that $\langle \mathbf{1}_S, A\mathbf{1}_T\rangle = \sum_{(u,v)\in S\times T} A_{uv} = |e(S, T)|$. Thus,

$$\left|e(S,T) - \frac{d}{n}\right| = \left|\left\langle \mathbf{1}_S, \left(A - \frac{d}{n}J\right)\mathbf{1}_T\right\rangle\right| = |\ \langle \mathbf{1}_S, M\mathbf{1}_T\rangle\ | \leq |\mathbf{1}_S| \cdot |M\mathbf{1}_T| = \sqrt{|S|} \cdot |M\mathbf{1}_T|.$$

To finish the proof we observe that the eigenvalues $\lambda_2^2, \ldots, \lambda_n^2$ of M^2 are positive and upper bounded by λ^2 and thus $|M\mathbf{1}_T|^2 = \langle M\mathbf{1}_T, M\mathbf{1}_T\rangle = \langle \mathbf{1}_T, M^2\mathbf{1}_T\rangle \leq \lambda^2 \langle \mathbf{1}_T, \mathbf{1}_T\rangle = \lambda^2|T|$. Thus $|M\mathbf{1}_T| \leq \lambda\sqrt{|T|}$, which finishes the proof. □

7.3 Cheeger inequality.

Let λ_2 be the second largest eigenvalue of of the adjacency matrix of a d-regular graph G. Define $\Delta = \frac{d-\lambda_2}{d}$. Recall that

$$\Delta = \min_{x\neq 0,\, x\perp \mathbf{1}} \frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{d\sum_v x_v^2}.$$

For $x \perp \mathbf{1}$ we have

$$\sum_{u,v\in V}(x_u - x_v)^2 = 2n\sum_v x_v^2 - 2\sum_{u,v} x_u x_v = 2n\sum_v x_v^2 - 2\left(\sum_v x_v\right)^2 = 2n\sum_v x_v^2.$$

Thus,

$$\begin{aligned}\Delta &= \min_{x\neq 0,\, x\perp \mathbf{1}} \frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{\frac{d}{2n}\sum_{u,v\in V}(x_u - x_v)^2} = \min_{x-\text{non-constant}} \frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{\frac{d}{2n}\sum_{u,v\in V}(x_u - x_v)^2} \\ &= \min_{x-\text{non-constant}} \frac{\frac{1}{nd/2}\sum_{\{u,v\}\in E}(x_u - x_v)^2}{\frac{1}{n^2}\sum_{u,v\in V}(x_u - x_v)^2} = \min_{x-\text{non-constant}} \frac{\mathbb{E}_{\{u,v\}\in E}(x_u - x_v)^2}{\mathbb{E}_{u,v\in V}(x_u - x_v)^2},\end{aligned}$$

where $\mathbb{E}_{\{u,v\}\in E}$ is the expectation with respect to the uniform distribution on E and $\mathbb{E}_{u,v}$ refers to independent uniform choice of u and v. The above minimization problem is a relaxation of uniform sparsest cut problem,

$$\mathrm{USC}(G) = \frac{n}{d}\min_{S\subseteq V}\frac{|e(S, V\setminus S)|}{|S|\cdot|V\setminus S|} = \min_{\substack{x-\text{non-constant}\\ x\in\{-1,1\}^n}} \frac{\mathbb{E}_{\{u,v\}\in E}(x_u - x_v)^2}{\mathbb{E}_{u,v\in V}(x_u - x_v)^2}.$$

Clearly we have $\mathrm{USC}(G) \geq \Delta$.

Definition 3. Let $S \subseteq V$. We define the conductance of S and the conductance of graph G,

$$\phi(S) = \frac{|e(S, V\setminus S)|}{d|S|}, \qquad \phi(G) = \min_{0<|S|\leq |V|/2}\phi(S).$$

Let us observe that $\mathrm{USC}(G) \leq 2\phi(G)$. Indeed,

$$\begin{aligned}\mathrm{USC}(G) &= \frac{n}{d}\min_{S\subseteq V}\frac{|e(S, V\setminus S)|}{|S|\cdot|V\setminus S|} \leq \frac{n}{d}\min_{0<|S|\leq |V|/2}\frac{|e(S, V\setminus S)|}{|S|\cdot|V\setminus S|} \\ &\leq 2\min_{0<|S|\leq |V|/2}\frac{|e(S, V\setminus S)|}{d|S|} = 2\phi(G).\end{aligned}$$

Theorem 52. We have $\Delta \leq \mathrm{USC}(G) \leq 2\phi(G) \leq \sqrt{8\Delta}$.

Proof. The only non-trivial inequality is $\phi(G) \leq \sqrt{2\Delta}$. Given a solution x of the minimization problem for Δ we are to find a good Boolean approximation (set S). We do this in several steps.

Step 1. Given a solution x with $x \perp \mathbf{1}$ it is enough to construct a vector $y \in \mathbb{R}^n$ such that $y_v \geq 0$, $|\{v : y_v > 0\}| \leq n/2$, $\max_v y_v = 1$ and

$$\frac{\sum_{\{u,v\}\in E}|y_u - y_v|}{d\sum_v |y_v|} \leq 2\sqrt{\frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{d\sum_v x_v^2}} = 2\sqrt{\lambda_2}.$$

Indeed, having such a vector y we construct the set $S \subseteq V$ (in fact we will find $S \subseteq \{v : y_v > 0\}$ and thus we will get $|S| \le |V|/2$) as follows. Take a random threshold $t \sim \mathrm{Unif}[0, \max_v y_v]$ and define $S = \{v : y_v \ge t\}$. We have

$$\frac{\mathbb{E}|e(S, V \setminus S)|}{d\mathbb{E}|S|} = \frac{\sum_{\{u,v\}\in E} \mathbb{P}(|\{u,v\} \cap S| = 1)}{d \sum_v \mathbb{P}(v \in S)} = \frac{\sum_{\{u,v\}\in E} |y_u - y_v|}{d \sum_v |y_v|}.$$

Now it suffices to observe that

$$\min_{0<|S|\le|V|/2} \frac{|e(S, V \setminus S)|}{d|S|} \le \frac{\mathbb{E}|e(S, V \setminus S)|}{d\mathbb{E}|S|}.$$

This is due to the general and easy inequality $\min\left(\frac{X}{Y}\right) \le \frac{\mathbb{E}X}{\mathbb{E}Y}$ valid for any positive real random variable X, Y. Indeed, the inequality $\frac{X}{Y} > \frac{\mathbb{E}X}{\mathbb{E}Y}$ leads to $X\mathbb{E}Y > Y\mathbb{E}X$ which is, after taking expectation of both sides, a contradiction.

Step 2a. Take $z_v = x - \mathrm{Med}(x)$. Observe that

$$\frac{\sum_{\{u,v\}\in E}(z_u - z_v)^2}{d \sum_v z_v^2} \le \frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{d \sum_v x_v^2}.$$

This follows from the fact that

$$|z|^2 = |x - \mathrm{Med}(x)\mathbf{1}|^2 = |x|^2 - \mathrm{Med}(X)\,\langle x, \mathbf{1}\rangle + n\,\mathrm{Med}(X)^2 = |x|^2 + n\,\mathrm{Med}(X)^2 \ge |x|^2.$$

Step 2b. Define

$$z_v^+ = \begin{cases} 0 & z_v < 0 \\ z_v & z_v \ge 0 \end{cases}, \qquad z_v^- = \begin{cases} 0 & z_v < 0 \\ -z_v & z_v < 0 \end{cases}.$$

Thus, $z = z^+ - z^-$ and $z^+ \perp z^-$. Note that $|z_u - z_v|^2 \ge |z_u^+ - z_v^+|^2 + |z_u^- - z_v^-|^2$ Therefore,

$$\lambda_2 \ge \frac{\sum_{\{u,v\}\in E}(z_u - z_v)^2}{d \sum_v z_v^2} \ge \frac{\sum_{\{u,v\}\in E}(z_u^+ - z_v^+)^2 + \sum_{\{u,v\}\in E}(z_u^- - z_v^-)^2}{d \sum_v (z_v^+)^2 + d \sum_v (z_v^-)^2}.$$

We get that

$$\lambda_2 \ge \frac{\sum_{\{u,v\}\in E}(z_u^+ - z_v^+)^2}{d \sum_v (z_v^+)^2} \qquad \text{or} \qquad \lambda_2 \ge \frac{\sum_{\{u,v\}\in E}(\sum_{\{u,v\}\in E}(z_u^- - z_v^-)^2}{d \sum_v (z_v^-)^2}.$$

Note that since z has median 0, we have $|\{v : z_v^+ > 0\}| \le n/2$ and $|\{v : z_v^- > 0\}| \le n/2$. Moreover $z_v^\pm \ge 0$.

Step 2c. We have constructed a vector w such that $w_v \ge 0$, $|v : w_v > 0| \le n/2$ and

$$\lambda_2 \ge \frac{\sum_{\{u,v\}\in E}(w_u - w_v)^2}{d \sum_v w_v^2}$$

Take $y_v = w_v^2$. Clearly $y_v \ge 0$, $|v : y_v > 0| \le n/2$. We have

$$\begin{aligned} \sum_{\{u,v\}\in E} |w_u^2 - w_v^2| &= \sum_{\{u,v\}\in E} |w_u - w_v||w_u + w_v| \\ &\le \left(\sum_{\{u,v\}\in E} |w_u - w_v|^2\right)^{1/2} \left(\sum_{\{u,v\}\in E} |w_u + w_v|^2\right)^{1/2}. \end{aligned}$$

Moreover,

$$\sum_{\{u,v\}\in E} |w_u + w_v|^2 \le 2 \sum_{\{u,v\}\in E} (w_u^2 + w_v^2) = 2d \sum_v w_v^2.$$

We arrive at

$$\frac{\sum_{\{u,v\}\in E} |y_u - y_v|}{d\sum_v |y_v|} = \frac{\sum_{\{u,v\}\in E} |w_u^2 - w_v^2|}{d\sum_v w_v^2} \le \sqrt{\frac{\sum_{\{u,v\}\in E} |w_u - w_v|^2}{d\sum_v w_v^2}} \le \lambda_2.$$

□

7.4 Harper's theorem

Recall that on the discrete cube we have a natural graph structure with the set of edges given by $E = \{(x, y) : \ d_H(x, y) = 1\}$, where $d_H(x, y) = |\{i : x_i \neq y_i\}|$. Also, for a set $S \subseteq \{0, 1\}^d$ we define its boundary $\partial S = \{(x, y) \in E : x \in S, y \notin S\}$. On $\{0, 1\}^d$ we can define the lexicographical order induced by $1 > 0$. Let $L_d[n]$ be the set of first n vertices according to this order.

Theorem 53 (Harper's theorem)**.** We have $|\partial S| \ge |\partial L_d[|S|]|$, i.e., the set of size n minimizing the edge boundary is $L_d[n]$.

Proof. We proceed by induction on d. For $d = 1$ the assertion is trivial. Suppose $d \ge 2$ and the theorem holds for $d - 1$.

We now define the compression of a subset of $\{-1, 1\}^d$. For every coordinate $i \in [d]$ we can decompose T into two subsets $T_{i=0}, T_{i=1} \subseteq \{0, 1\}^{d-1}$ according to the value of ith coordinate. Formally

$$T_{i=\varepsilon} = \{x \in \{0, 1\}^{d-1} : (x_1, \ldots, x_{i-1}, \varepsilon, x_{i+1}, \ldots, x_n) \in T\}, \qquad \varepsilon \in \{0, 1\}.$$

Let $C_i(T)$ be the set obtained by replacing $T_{i=0}$ with $L_{d-1}[|T_{i=0}|]$ and $T_{i=1}$ with $L_{d-1}[|T_{i=1}|]$. Of course $|C_i(T)| = |T|$.

Claim. We have $|\partial C_i(T)| \le |\partial T|$.

Proof. Note that

$$\begin{aligned} |\partial C_i(T)| &= |\partial L_{d-1}[|T_{i=0}|]| + |\partial L_{d-1}[|T_{i=1}|]| + |L_{d-1}[|T_{i=0}|] \ \Delta \ L_{d-1}[|T_{i=1}|]| \\ &= |\partial L_{d-1}[|T_{i=0}|]| + |\partial L_{d-1}[|T_{i=1}|]| + ||T_{i=0}| - |T_{i=1}|| \\ &\le |\partial T_{i=0}| + |\partial T_{i=1}| + |T_{i=0} \ \Delta \ T_{i=1}| = |\partial T|. \end{aligned}$$

Here the inequalities

$$|\partial L_{d-1}[|T_{i=0}|] \le |\partial T_{i=0}|, \qquad |\partial L_{d-1}[|T_{i=1}|] \le |\partial T_{i=1}|$$

follow from the induction assumption and the inequality $||T_{i=0}| - |T_{i=1}|| \le |T_{i=0} \ \Delta \ T_{i=1}|$ is a general bound $|A \Delta B| \ge ||A| - |B||$ valid for any finite sets A, B. □

Let us apply $C_1, \ldots, C_n$ in a cyclic fashion,

$$S \to C_1(S) \to C_2C_1(S) \to \ldots \to C_dC_{d-1} \ldots C_1(S) \to C_1C_dC_{d-1} \ldots C_1(S) \to \ldots$$

We shall show that this sequence eventually stabilizes, that is, we reach a subsets invariant under all the operations C_i. Such subsets will be called *compressed*. Since along the sequence of compression the cardinality of the boundary is non-increasing and the cardinalities of the sets stay constant, it will be therefore enough to prove the statement only for compressed sets.

Let us first introduce an order on the set of subsets of $\{0, 1\}^d$. Each such subset can be identified with a vector in $\{0, 1\}^{2^d}$ (since there are 2^d subsets of $\{0, 1\}^d$). Here the order of coordinates corresponds to the lexicographical order on $\{0, 1\}^d$.

Example. For $d = 3$ we have the following order on $\{0,1\}^d$,

$$(000) < (001) < (010) < (011) < (100) < (101) < (110) < (111).$$

Thus, e.g., the vector $(01101001) \in \{0,1\}^{2^3}$ corresponds to the following subset of $\{0,1\}^3$.

$$\{(001), (010), (100), (111)\}.$$

The order $\prec$ on $\{0,1\}^{2^d}$ (and thus the order on subsets of $\{0,1\}^d$) is defined to be the reverse lexicographical order. It is the usual order (where $1 > 0$) but the order of reading the coordinates is reversed.

By the construction we have the following obvious fact.

Fact. If $x, y \in \{0,1\}^d$, $y \in T \subseteq \{0,1\}^d$ and $x < y$ then $((T \setminus \{y\}) \cup \{x\}) \prec T$. In particular, if $C_i(T) \neq T$ for some i then $C_i(T) \prec T$. It follows that the sequence of compressions eventually stabilizes.

It is now enough to describe all possible compressed sets and prove that the satisfy the inequality. Let us define a new order $\ll$ on $\{0,1\}^d$ (compressibility order). If all compressed sets containing $y \in \{0,1\}^d$ also contain $x \in \{0,1\}^d$ then we write $x \ll y$.

Fact. We have $x < y$ implies $x \ll y$ unless $x = 01...1$ and $y = 10...0$.

Proof. We first consider the case when $x_i = y_i = \varepsilon$ for some $i = 1, \ldots, d$, $\varepsilon \in \{0,1\}$. Let T be compressed. Suppose $y \in T$ and $x < y$. We are to show that $x \in T$. We have $C_i(T) = T$. Clearly x is in T since $T_{i=\varepsilon} = L_{d-1}[|T_{i=\varepsilon}|]$.

We now consider the case when $x_i \neq y_i$ for all $i = 1, \ldots, d$. Since $x < y$ we get $x_1 = 0$ and $y_1 = 1$. Assume that x, y are not equal to $x = 01...1$ and $y = 10...0$. Thus, there is $i > 1$ such that $x_i = 0$ and $y_i = 1$. Therefore, x, y have the form $x = (0a0b)$ and $y = (1\bar{a}1\bar{b})$, where $\bar{a} = 1 - a$. Take $z = (0a1b)$. We have $x < z$ and $x_1 = z_1$. Thus, from the previous case, $x \ll z$. Moreover, $z < y$ and $z_i = y_i$. Thus, $z \ll y$. We get $x \ll z \ll y$ and therefore $x \ll y$. □

Let $L = \{x : x < 01...1\}$ and $H = \{x : x > 10...0\}$. On L and H the orders $<$ and $\ll$ are the same. The only non-comparable points are $x = 01...1$ and $y = 10...0$. To see that they are indeed non-comparable, we take $T = \{(0a) : a \in \{0,1\}^{d-1}\} \cup (10...0) \setminus (01...1)$. Then T is compressed and contains y but it does not contain x. On the other hand $T = \{0a : a \in \{0,1\}^{d-1}\}$ is compressed and it contains x but does not contain y. Thus x and y are not comparable in $\ll$.

Take our compressed set T. If $T \cap H \neq \emptyset$ then there is a unique maximal point z in T. Since $z \in T$ we get that $x < z$ implies $x \in T$ for any x. Thus, in this case T is a prefix in $<$.

Let us now assume that $T \cap H = \emptyset$. If $T \cap \{(01...1), (10...0)\} = \emptyset$ then in the same way we get the same conclusion. If $T \cap \{(01...1), (10...0)\} \neq \emptyset$ then we proceed similarly if the cases

$$T \cap \{(01...1), (10...0)\} = \{(01...1), (10...0)\}, \qquad T \cap \{(01...1), (10...0)\} = \{(01...1)\}.$$

The only non-trivial case is $T = L \cup \{(10...0)\}$. In this case we compute the size of edge boundary explicitly,

$$|\partial T| = 2^{d-1} - 2 + 2(d-1) \geq 2^{d-1} = |\partial L_{d-1}[|T|]|.$$

□

8 Enumerative combinatorics

8.1 Generating functions

The function

$$\phi[(a_n)_{n\geq 0}](x) = \sum_{n=0}^{\infty} a_n x^n \tag{9}$$

is called the *generating function* of the sequence of complex numbers $(a_n)_{n\geq 0}$. Sometimes we shall treat this expression as a formal sum, sometimes as a Taylor series of an actual function. Whenever we treat the function ϕ as a Taylor series, we have the expression for its nth coefficient,

$$a_n = \frac{1}{n!}\phi^{(n)}(0).$$

To use this expression we have to make sure that the series converges in some neighborhood of 0, which happens if and only if $\limsup_{n\to\infty} \sqrt[n]{|a_n|} < \infty$ (AM.1.2). We will however not always bother to discusses this convergence issues in great details here, as it is both not hard and not the most exciting part of our study.

Here are some basic facts and general rules for computing generating functions (GF):

1. We have the obvious expression for the GF of the truncated sequence

$$\phi[(a_{n+k})_{n\geq 0}](x) = \frac{\phi[(a_n)_{n\geq 0}] - \sum_{i=0}^{k-1} a_i x^i}{x^k}.$$

2. By differentiating (9) k times we find out that $\phi^{(k)}[(a_n)_{n\geq 0}](x) = \sum_{n\geq 0} n(n-1)\dots(n-k+1)a_n x^{n-k}$, which leads to
$$\phi[(n(n-1)\dots(n-k+1)a_n)_{n\geq 0}](x) = \phi^{(k)}[(a_n)_{n\geq 0}](x)\cdot x^k.$$

3. If α, β are some complex numbers then

$$\phi[(\alpha a_n + \beta b_n)_{n\geq 0}](x) = \alpha\phi[(a_n)_{n\geq 0}](x) + \beta\phi[(b_n)_{n\geq 0}](x), \qquad \phi[(a_n\beta^n)_{n\geq 0}](x) = \phi[(a_n)_{n\geq 0}](\beta x).$$

4. The function $\phi(x) = (1-x)^{-k}$ generates the sequence $a_n = \binom{k+n-1}{k-1}$.

   Proof. We have $a_n = \frac{1}{n!}\phi^{(n)}(0)$ and thus it suffices to compute $\phi^{(n)}(0)$, which is very easy as $\phi^{(n)}(x) = k(k+1)\dots(k+n-1)(1-x)^{-(k+n)}$. We obtain $a_n = \frac{1}{n!}k(k+1)\dots(k+n-1) = \frac{(k+n-1)!}{n!(k-1)!} = \binom{k+n-1}{k-1}$. □

   Remark. Note that $\phi(x) = (\sum_{n=0}^{\infty} x^n)^k$ and thus $a_n = \binom{k+n-1}{k-1}$ is the number of solutions in $\{0,1,2,\dots\}$ to the equation $y_1 + \dots y_k = n$ (to compute the coefficient in front of x^n we have to pick some term x^{n_i} from the ith bracket is such a way that the sum of the exponents equals n). An alternative way of deriving this equality is to observe that the above representations of n as a sum of k non-negative numbers can be obtained by considering $n+k-1$ cells placed one after the other and putting $k-1$ bars into these cells, one bar in one cell. Clearly there are $\binom{n+k-1}{k-1}$ ways to do this. The lengths of "intervals" of empty cells correspond to the numbers $n_1, \dots, n_k$. This is called the *stars and bars* method.

5. For sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ let us define $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. The sequence $(c_n)_{n\geq 0}$ is called the convolution of $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$, or their Cauchy product. We note that the generating function of the Cauchy product is equal to the product of generating function, since

$$\phi[(a_n)_{n\geq 0}](x)\cdot\phi[(b_n)_{n\geq 0}](x) = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right)x^n,$$

provided that these series converge absolutely (say, use Merten's theorem).

Binet formula. We will find the explicit formula for the Fibonacci sequence, $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$. Let $\phi(x) = \sum_{n=0}^{\infty} F_n x^n$ be the generating function of $(F_n)_{n\geq 0}$. Multiplying the recurrence relation by x^{n+2} and summing over n we get

$$\sum_{n=0}^{\infty} F_{n+2}x^{n+2} = \sum_{n=0}^{\infty} F_{n+1}x^{n+2} + \sum_{n=0}^{\infty} F_n x^{n+2}.$$

This means that

$$\phi(x) - F_0 - F_1 x = x(\phi(x) - F_0) + x^2\phi(x).$$

Using the initial conditions $F_0 = 0$ and $F_1 = 1$ we get $\phi(x) - x = (x+x^2)\phi(x)$, which yields $\phi(x) = \frac{x}{1-x-x^2}$. To find F_n it is enough to find the Taylor expansion of ϕ. Let $x_- < x_+$ be the roots of the equation $x^2+x-1 = 0$. We shall apply the usual technique of writing the rational function as a sum of elementary function. For some constants a, b we have

$$\phi(x) = \frac{x}{1-x-x^2} = \frac{-x}{(x-x_+)(x-x_-)} = \frac{a}{x-x_+} + \frac{b}{x-x_-}.$$

Multiplying the last equality by $x - x_+$ and then taking $x = x_+$ we get $a = \frac{-x_+}{x_+-x_-}$. Multiplying it by $x - x_-$ and then taking $x = x_-$ we get $b = \frac{-x_-}{x_--x_+}$. We arrive at

$$\begin{aligned}\phi(x) &= \frac{a}{x-x_+} + \frac{b}{x-x_-} = \frac{x_+}{x_+-x_-}\cdot\frac{1}{x_+-x} - \frac{x_-}{x_+-x_-}\cdot\frac{1}{x_--x} = \frac{1}{x_+-x_-}\left(\frac{1}{1-\frac{x}{x_+}} - \frac{1}{1-\frac{x}{x_-}}\right)\\ &= \sum_{n=0}^{\infty}\frac{1}{x_+-x_-}\left(\frac{1}{x_+^n} - \frac{1}{x_-^n}\right)x^n.\end{aligned}$$

We arrive at $F_n = \frac{1}{x_+-x_-}\left(\frac{1}{x_+^n} - \frac{1}{x_-^n}\right)$. If we now use the fact that $x_\pm = \frac{-1\pm\sqrt{5}}{2}$, we get $x_+ - x_- = \sqrt{5}$. Moreover from Vieta's formulas we get $x_+x_- = -1$, which give $x_+^{-1} = -x_-$ and $x_-^{-1} = -x_+$. Thus,

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

General linear recurrence with constant coefficients. Suppose now that we have a recurrence $\beta_k a_{n+k} + \beta_{k-1}a_{n+k-1} + \ldots + \beta_1 a_{n+1} + \beta_0 a_n = 0$ for $k \geq 0$. Let us assume that $\beta_0, \beta_k \neq 0$. In order to define this sequence uniquely we need to know the values of $a_0, \ldots, a_{k-1}$. Take $P_l(x) = \sum_{i=0}^{l} a_i x^i$ (these are known polynomials). Multiplying the recurrence relations by x^{n+k} and summing over n we get

$$\beta_k\sum_{n=0}^{\infty} a_{n+k}x^{n+k} + \beta_{k-1}\sum_{n=0}^{\infty} a_{n+k-1}x^{n+k} + \ldots + \beta_1\sum_{n=0}^{\infty} a_{n+1}x^{n+k} + \beta_0\sum_{n=0}^{\infty} a_n x^{n+k} = 0.$$

This can be written as

$$\beta_k(\phi(x) - P_{k-1}(x)) + \beta_{k-1}x(\phi(x) - P_{k-2}(x)) + \ldots + \beta_1 x^{k-1}(\phi(x) - P_0(x)) + \beta_0 x^k \phi(x) = 0.$$

From this we get

$$\phi(x) = \frac{\beta_k P_{k-1}(x) + \beta_{k-1}xP_{k-2}(x) + \ldots + \beta_1 x^{k-1}P_0(x)}{\beta_k + \beta_{k-1}x + \ldots + \beta_1 x^{k-1} + \beta_0 x^k} = \frac{P(x)}{Q(x)}.$$

This is a rational function and the degree of the numerator is smaller than the degree of the denominator. From the standard theorem (AM.I.2) it is possible to write $\phi(x)$ in the form

$$\phi(x) = \sum_{i=1}^{l} \sum_{j=1}^{k_i} \frac{c_{ij}}{(x - \lambda_i)^j},$$

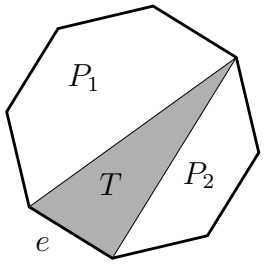
where $\lambda_1, \ldots, \lambda_l$ are the roots of $Q(x)$ with multiplicities $k_1, \ldots, k_l$. Note that λ_i might be complex. Thus from Point 4 we get

$$\phi(x) = \sum_{i=1}^{l} \sum_{j=1}^{k_i} \frac{c_{ij}}{(-1)^j \lambda_i^j} \cdot \frac{1}{\left(1 - \frac{x}{\lambda_i}\right)^j} = \sum_{i=1}^{l} \sum_{j=1}^{k_i} \frac{c_{ij}}{(-1)^j \lambda_i^j} \sum_{n=0}^{\infty} \binom{j+n-1}{j-1} \left(\frac{x}{\lambda_i}\right)^n.$$

Thus

$$a_n = \sum_{i=1}^{l} \sum_{j=1}^{k_i} c_{ij}(-1)^j \lambda_i^{-(j+n)} \binom{j+n-1}{j-1}.$$

Catalan numbers. The Catalan numbers are the number $C_n = \frac{1}{n+1}\binom{2n}{n}$. These numbers appear in various combinatorial structures. As an example let us consider triangulations of a convex n-gon. We a triangulation means cutting of the polygon into triangles by connecting vertices with non-crossing line segments. We claim that the number of triangulations of a convex $(n+2)$-gon is precisely C_n.



Consider an $(n+3)$-gon P. Let us fix some edge e. Choosing the position of the triangle T to which e belongs divides the polygon into two smaller polygons P_1 and P_2, say, $(k+2)$-gon and $(n-k+2)$-gon. These polygons can be further triangulated. We therefore get the following recurrence relation for the number a_n of triangulations of the $(n+2)$-gon

$$a_{n+1} = a_n + a_1 a_{n-1} + a_2 a_{n-2} + \ldots + a_{n-1}a_1 + a_n.$$

Let us put $a_0 = 1$. We then get the equation

$$a_{n+1} = \sum_{i=0}^{n} a_i a_{n-i}, \qquad a_0 = 1.$$

Let us observe that the right hand side is the Cauchy product of (a_n) with itself. Let ϕ e the generating function of $(a_n)_{n\geq 0}$. By Points 1 and 5 we get $\phi(x)^2 = \frac{\phi(x)-c_0}{x} = \frac{\phi(x)-1}{x}$. This gives the equation $x\phi(x)^2 - \phi(x) + 1 = 0$. We are looking for an analytic function that satisfies this equation, at least in some small neighborhood of 0. We get

$$x\phi(x)^2 - \phi(x) + 1 = 0 \quad \Longrightarrow \quad \phi(x)^2 - \frac{1}{x}\phi(x) + \frac{1}{x} = 0 \quad \Longrightarrow \quad \left(\phi(x) - \frac{1}{2x}\right)^2 = \frac{1}{4x^2} - \frac{1}{x}.$$

Thus we get two solutions

$$\phi_{\pm}(x) = \frac{1}{2x} \pm \sqrt{\frac{1}{4x^2} - \frac{1}{x}}.$$

We have to choose one of these functions (note that choosing $\phi_+(x)$ for some values of x and $\phi_-(x)$ for other values makes no sense since we need our function to be analytic, in particular continuous). If we choose $\phi(x) = \phi_+(x)$ for $x > 0$ then $\lim_{x\to 0^+} \phi(x) = \infty$ and so our function in not analytic. If we choose $\phi(x) = \phi_-(x)$ for $x < 0$ then $\lim_{x\to 0^+} \phi(x) = -\infty$ and again our function in not analytic. We therefore have to choose

$$\phi(x) = \frac{1}{2x} - \operatorname{sgn}(x)\sqrt{\frac{1}{4x^2} - \frac{1}{x}} = \frac{1}{2x} - \frac{1}{2x}\sqrt{1-4x} = \frac{1-\sqrt{1-4x}}{2x}, \qquad x \neq 0$$

If we manage to prove that this function is analytic in some neighborhood of 0 by extending it to 0 taking $\phi(0) = 1$ (which corresponds to the initial condition $a_0 = 1$), then $\phi(x)$ is the generating function of $(a_n)_{n\geq 0}$ since by the equation for $\phi(x)$ this function generates a sequence that satisfies the recurrence relation and the initial condition.

Let us take $f(x) = \sqrt{1-4x}$. It is easy to observe that $f^{(n)}(x) = b_n(1-4x)^{\frac{1}{2}-n}$ for some numbers b_n. We have $f^{(n+1)}(x) = b_n(-4)(\frac{1}{2}-n)(1-4x)^{\frac{1}{2}-n-1}$, which leads to $b_{n+1} = 2(2n-1)b_n$, $b_0 = 1$. Thus $f^{(n)}(0) = b_n = -2^n(2n-3)!!$ for $n \geq 2$ and $b_1 = -2$. We get

$$1 - \sqrt{1-4x} = 1 - \left(1 - 2x + \sum_{n=2}^{\infty} \frac{-2^n(2n-3)!!}{n!}x^n\right) = 2x + \sum_{n=2}^{\infty} \frac{2^n(2n-3)!!}{n!}x^n.$$

Thus,

$$\phi(x) = \frac{1-\sqrt{1-4x}}{2x} = 1 + \sum_{n=2}^{\infty} \frac{2^{n-1}(2n-3)!!}{n!}x^{n-1} = 1 + \sum_{n=1}^{\infty} \frac{2^n(2n-1)!!}{(n+1)!}x^n = 1 + \sum_{n=1}^{\infty} \frac{(2n)!}{(n+1)!n!}x^n$$

We arrive at

$$\phi(x) = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n}x^n, \qquad a_n = \frac{1}{n+1}\binom{2n}{n}, \quad n \geq 0.$$

Thus $a_n = C_n$.

Motzkin numbers. Let us consider the following recurrence relation

$$M_0 = M_1 = 1, \qquad M_{n+1} = \frac{2n+3}{n+3}M_n + \frac{3n}{n+3}M_{n-1}.$$

Would it be possible to give a formula for M_n? Interestingly, the numbers M_n turn out to be integers! We shall provide a combinatorial description later. Now we show a technique allowing us to prove this using generating functions.

Let ϕ be the generating function of $(M_n)_{n\geq 0}$ (below we write $\phi \sim M_n$ for "ϕ generates $(M_n)_{n\geq 0}$"). We have

$$\phi \sim M_n, \qquad x\phi'(x) \sim nM_n, \qquad \phi'(x) \sim (n+1)M_{n+1}, \qquad \frac{\phi(x)-1}{x} \sim M_{n+1}, \qquad \frac{\phi'(x)-1}{x} \sim (n+2)M_{n+2},$$

The recurrence

$$(n+4)M_{n+2} = (2n+5)M_{n+1} + 3(n+1)M_n$$

gives us therefore

$$\frac{\phi'(x)-1}{x} + 2\frac{\phi(x)-1-x}{x^2} = 2\phi'(x) + 3\cdot\frac{\phi(x)-1}{x} + 3x\phi'(x) + 3\phi(x),$$

equivalently

$$x(\phi'(x)-1) + 2(\phi(x)-1-x) = 2x^2\phi'(x) + 3x(\phi(x)-1) + 3x^3\phi'(x) + 3x^2\phi(x).$$

This is

$$\phi'(x)(x-2x^2-3x^3) = \phi(x)(-2+3x+3x^2) + 2.$$

We get

$$\phi'(x) = \frac{-2+3x+3x^2}{x(1+x)(1-3x)}\phi(x) + \frac{2}{x(1+x)(1-3x)}.$$

Let us consider this type of differential equation in more general form

$$\phi'(x) = R(x)\phi(x) + S(x). \tag{10}$$

In order to find the solution we can first solve the equation $\phi_0'(x) = R(x)\phi_0(x)$. This equation is equivalent to $(\ln|\phi_0|)' = R(x)$, which leads to $\ln|\phi_0| = \int R(x)\mathrm{d}x$ and thus $\phi_0(x) = \exp(\int R(x)\mathrm{d}x)$ is a positive solution to this equation. We now try to find the solution to (10) in the form $\phi(x) = \phi_0(x)C(x)$. We get the equation

$$\phi_0'(x)C(x) + \phi_0(x)C'(x) = R(x)\phi_0(x)C(x) + S(x).$$

We therefore get $C'(x) = \frac{S(x)}{\phi_0(x)}$. We can therefore take $C(x) = \int \frac{S(x)}{\phi_0(x)}\mathrm{d}x$.

In our case this procedure gives (using standard integration techniques)

$$\begin{aligned}(\ln|\phi_0(x)|)' &= \int \frac{-2+3x+3x^2}{x(1+x)(1-3x)}\mathrm{d}x = \int\left(\frac{-2}{x} + \frac{1}{\cdot}\frac{1}{1+x} - \frac{3}{2}\cdot\frac{1}{1-3x}\right)\mathrm{d}x \\ &= -2\ln|x| + \frac{1}{2}\ln|1+x| + \frac{1}{2}\ln|1-3x|.\end{aligned}$$

Taking the exponent and neglecting the absolute value we get that

$$\phi_0(x) = \frac{\sqrt{(1+x)(1-3x)}}{x^2}$$

satisfies

$$\phi_0'(x) = \frac{-2+3x+3x^2}{x(1+x)(1-3x)}\phi_0(x).$$

We remark here that in general the above integration gives a unique function only up to some absolute constant C, but this constant would only multiply ϕ_0, which we will anyway do in the next step.

Next we take $\phi(x) = \phi_0(x)C(x)$ and we get (after evaluating the integral using standard techniques)

$$C(x) = \int \frac{2x}{((1+x)(1-3x))}\mathrm{d}x = \frac{1-x}{2\sqrt{(1+x)(1-3x)}} + C.$$

We arrive at

$$\phi(x) = \frac{\sqrt{(1+x)(1-3x)}}{x^2}\left(\frac{1-x}{2\sqrt{(1+x)(1-3x)}} + C\right).$$

We want to have $\phi(0) = M_0 = 1$. In order to get this (and actually avoid blow ups near zero), we have to take $C = -\frac{1}{2}$. We arrive at

$$\phi(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x^2} = \frac{1-x-\sqrt{(1-x)^2-4x^2}}{2x^2}.$$

We see right away that ϕ solves the equation $a\phi^2 + \phi + c$ with $a = x^2$, $b = x-1$ and $c = 1$. Thus

$$x^2\phi(x)^2 + (x-1)\phi(x) + 1 = 0.$$

Comparing the coefficients in front of x^n we get

$$M_n = M_{n+1} + \sum_{k=0}^{n-2} M_k M_{n-k-2}, \quad n \geq 2, \qquad M_0 = M_1 = 0$$

Thus, we got another recurrence relation from which we easily see that M_n are integers.

8.2 Characteristic polynomials

In this chapter we describe an efficient method to deal with linear recurrences with constant coefficients. In out first theorem we show how to construct sequences satisfying a givie equation.

Theorem 54. Suppose $c_0, c_1, \ldots, c_k$ are complex numbers and $c_0, c_k \neq 0$. Let $\lambda_1, \ldots, \lambda_p$ be the complex roots of the polynomial $S(z) = \sum_{j=0}^{k} c_j z^j$ with multiplicities $l_1, \ldots, l_p$, that is

$$c_k z^k + c_{k-1} z^{k-1} + \ldots + c_1 z + c_0 = c_k (z-\lambda_1)^{l_1} (z-\lambda_2)^{l_2} \ldots (z-\lambda_p)^{l_p}.$$

Then for any polynomials $Q_1, \ldots, Q_p$, such that $\deg(Q_i) \leq l_i - 1$ for $i = 1, \ldots, p$, the sequence

$$a_n = Q_1(n)\lambda_1^n + \ldots + Q_p(n)\lambda_p^n$$

satisfies the equation $\sum_{i=0}^{k} c_i a_{n+i} = 0$, for $n \geq 0$.

Proof. The crucial observation is that our equation is linear and thus if two sequences satisfy this equation then their linear combination will also satisfy it. Thus it is enough to prove that the equation is satisfied by the sequences

$$\lambda_i^n, \quad , n\lambda_i^n, \quad n^2\lambda_i^n, \quad \ldots, \quad n^{l_i-1}\lambda_i^n, \qquad i = 1, \ldots, p,$$

since any sequence of the form $Q_i(n)\lambda_i^n$ where $\deg(Q_i) \leq l_i - 1$ is a linear combination of these sequences. It will actually be more convenient to consider another basis, namely

$$\lambda_i^n, \quad , n\lambda_i^{n-1}, \quad n(n-1)\lambda_i^{n-2}, \quad \ldots, \quad n(n-1)\ldots(n-l_i+1)\lambda_i^{n-l_i+1}, \qquad i = 1, \ldots, p,$$

Again any sequence of the form $Q_i(n)\lambda_i^n$ where $\deg(Q_i) \leq l_i - 1$ is a linear combination of these sequences. In other words we have to check that our equation is satisfied for the following sequences

$$a_n = \frac{n!}{(n-j)!} \cdot \lambda^{n-j}, \qquad j = 0, 1, \ldots, l-1,$$

where λ is a root of S with multiplicity l. Thus, we have to check that

$$\sum_{i=0}^{k} c_i \frac{(n+i)!}{(n+i-j)!}\lambda^{n+i-j} = 0, \qquad n \geq 0.$$

Define $T(z) = z^n S(z) = \sum_{i=0}^{k} c_i z^{n+i}$. The above equality is equivalent to $T^{(j)}(\lambda) = 0$ for $j = 0, 1, \ldots, l-1$. This immediately follows from the fact that λ is a root of T with multiplicity l. □

The space of solutions to a linear equation is a linear space over $\mathbb{C}$. In order to prescribe our sequence we need to provide the values of $(a_0, \ldots, a_{k-1})$ (initial conditions). The map $(a_0, \ldots, a_{k-1}) \mapsto (a_n)_{n\geq 0}$ is linear. Since the sequences of initial conditions $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ form a basis of initial conditions, the space of solutions has dimension k. In the above theorem we have presented a family of $l_1 + \ldots + l_p = \deg(S) = k$ solutions

$$\lambda_i^n, \quad , n\lambda_i^n, \quad n^2\lambda_i^n, \quad \ldots, \quad n^{l_i-1}\lambda_i^n, \qquad i = 1, \ldots, p,$$

To show that these sequence form a basis of solutions it is enough to show that these sequences are linearly independent. This will be done during the classes.

8.3 Random walk and reflection principle

Consider a particle that moves on $\mathbb{Z}$ with the following rule: at a current point x the particle moves to $x+1$ with probability p and to $x-1$ with probability $1-p$. If $p = \frac{1}{2}$ then the random walk is called *symmetric*.

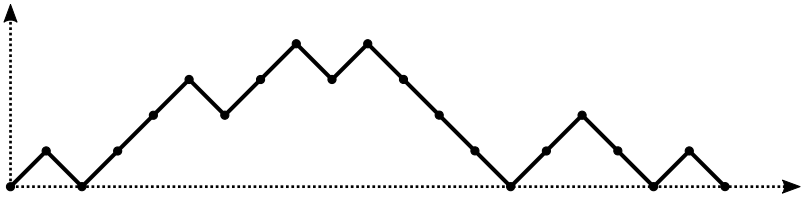
Suppose out random walk stars from 0. In order to get to the point k after n steps we need to make precisely $\frac{1}{2}(n+k)$ steps to the right (note that if n and k have the same parity then it is not possible to get from 0 to k in n steps). This means that the probability of reaching k from 0 after n steps is

$$\mathbb{P}_n(0 \to k;\ p) = \binom{n}{\frac{1}{2}(n+k)} p^{\frac{1}{2}(n+k)}(1-p)^{\frac{1}{2}(n-k)}.$$

If $p = \frac{1}{2}$ then we simply have

$$\mathbb{P}_n(0 \to k) = \frac{1}{2^n}\binom{n}{\frac{1}{2}(n+k)}.$$

The trajectory of a random walk can be visualize in a form of time-space diagram. One can see that the



event that a random walk starting from 0 reaches 0 after $2n$ steps and never goes below zero is precisely

$$\mathbb{P}_{2n}^{\geq 0}(0 \to 0;\ p) = C_n p^n (1-p)^n = \frac{1}{n+1}\binom{2n}{n} p^n (1-p)^n,$$

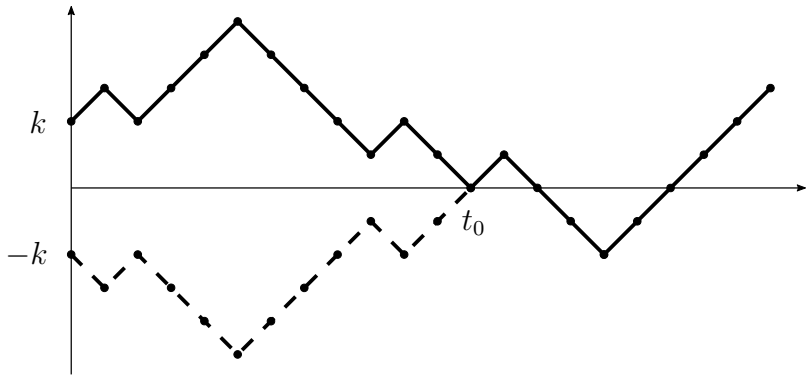
where C_n is the n-th Catalan number (Dyck path interpretation of Catalan numbers). Let $S_0, S_1, \ldots, S_{2n}$ be the trajectory of the random walk. The above equality can be rewritten as

$$\mathbb{P}_0(S_1 \geq 0, \ldots, S_{2n-1} \geq 0 \mid S_{2n} = 0) = \frac{\mathbb{P}_{2n}^{\geq 0}(0 \to 0;\ p)}{\mathbb{P}_{2n}(0 \to 0;\ p)} = \frac{\frac{1}{n+1}\binom{2n}{n} p^n (1-p)^n}{\binom{2n}{n} p^n (1-p)^n} = \frac{1}{n+1}.$$

where the subscript 0 in $\mathbb{P}_0$ indicates that the random walk starts from 0.

We now introduce a trick called the *reflection principle*.

Theorem 55. Let $\mathbb{P}_n^0(k \to l)$ be the probability that a symmetric random walk goes from k to l in n steps and hits 0 at some time $0 \leq t \leq n$. Then for $k, l \geq 1$ we have $\mathbb{P}_n^0(k \to l) = \mathbb{P}_n(-k, l)$.



Proof. It is enough to show that the number of paths from k to l hitting 0 is equal to the number of paths from $-k$ to l. Consider the time-space graphs of our paths. For any path from k to l that hits 0 we consider the first time t_0 when this happens and we reflect the path from time 0 to time t_0 with respect to the X axis. We get a path from $-k$ to l. It is clear that this actually gives a one-to-one correspondence since every path from $-k$ to l has to intersect X axis (due to the fact that $k > 0$) and by taking the first time t_0 of intersection and reflecting the path from time 0 to time t_0 with respect to the X axis we get the inverse bijection. □

Our next theorem answers the following question: in an election where candidate A receives P votes and candidate B receives Q votes with $P > Q$, what is the probability that A will be strictly ahead of B throughout the count of the votes. We assume that we count the votes in a random way. The answer is $\frac{P-Q}{P+Q}$.

Theorem 56 (Bertrand's ballot theorem)**.** Let $m > 0$. The probability that the random walk starting form 0 stays positive, conditioned on the event that it finally reaches m in n steps is $\frac{m}{n}$.

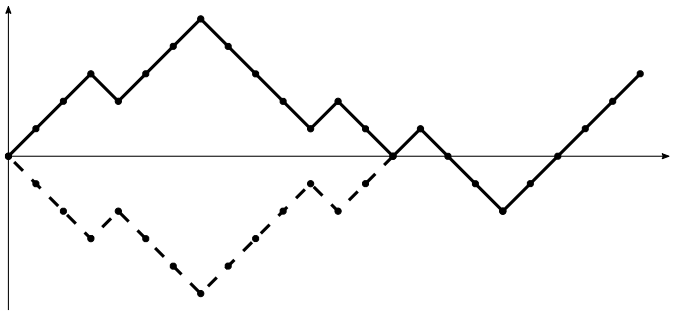
Proof. For any fixed p all the paths from 0 to m of length n have the same probability and therefore in our computations we shall omit the probabilistic factor and just focus on the number of paths. We introduce the following notation for paths of length n:

1. $N_n^{\nearrow,0}(m)$ – # of paths from 0 to m starting with step $+1$ and hitting 0 before reaching m.
2. $N_n^{\nearrow,+}(m)$ – # of paths from 0 to m starting with step $+1$ and staying positive.
3. $N_n^{\searrow}(m)$ – # of paths from 0 to m starting with step -1.
4. $N_n(m)$ – # of all paths from 0 to m.

We have $N_n(m) = \binom{n}{\frac{1}{2}(n-m)}$ and $N_n^{\searrow}(m) = \binom{n-1}{\frac{1}{2}(n-m)-1}$. Thus $\frac{N_n^{\searrow}(m)}{N_n(m)} = \frac{n-m}{2n}$. A reflection similar to the one presented in the last theorem gives $N_n^{\nearrow,0}(m) = N_n^{\searrow}(m)$.
Our probability is therefore equal to

$$\frac{N_n^{\nearrow,+}(m)}{N_n(m)} = \frac{N_n(m) - N_n^{\nearrow,0}(m) - N_n^{\searrow}(m)}{N_n(m)} = \frac{N_n(m) - 2N_n^{\searrow}(m)}{N_n(m)} = 1 - \frac{n-m}{n} = \frac{m}{n}.$$

□



8.4 Young tableaux

For a sequence of positive integers $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_m$ we consider the *Young diagram (Ferrers diagram)* of row lengths λ_i as shown in the Figure 7 below. If in the cells of this diagram we put numbers $1, \ldots, n$, where n is the total number of cells in the diagram, in such a way that in every row and every column the sequence of numbers is increasing, the we get a *Young tableaux*.

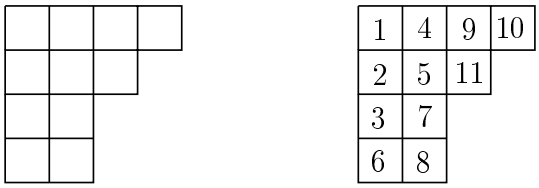


Figure 7: Ferrers diagram and Young tableaux built on it.

The hook length formula. We shall give a proof of the famous hook length formula for the number of standard Young tableaux of a given shape. Suppose λ is a shape (Ferrers diagram). The *hook* at cell (i, j) in λ is the set of cells in λ of the form (i', j) where $i' \geq i$ or (i, j') where $j' \geq j$ (see Figure 8).

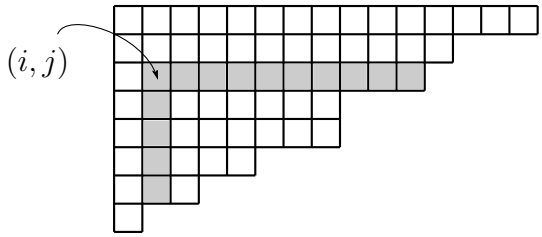


Figure 8: A hook of length at $(i, j) = (2, 3)$ and length 14.

The *hook length* $h_\lambda(i, j)$ is simply the number of cells in the hook at (i, j) in λ.

Theorem 57. The number of standard Young tableaux of shape λ and n cells is equal to $\frac{n!}{\prod_{(i,j)\in\lambda} h_\lambda(i,j)}$.

Proof (C. Greene, A. Nijenhuis, H.S. Wilf, 1979). The shape λ can be described by the lengths $\lambda_1, \ldots, \lambda_m$ of its rows. Let us define

$$F(\lambda_1, \ldots, \lambda_m) = \begin{cases} \frac{n!}{\prod_{(i,j)} h_\lambda(i,j)} & \lambda_1 \geq \ldots \geq \lambda_m \\ 0 & \text{otherwise} \end{cases}$$

Moreover, let $f(\lambda_1, \ldots, \lambda_m)$ be the number of standard Young tableaux of shape λ. Our goal is to show that $f(\lambda_1, \ldots, \lambda_m) = F(\lambda_1, \ldots, \lambda_m)$.

Our first observation is that in every standard Young tableaux the number n must appear at the *corner* namely cell being last in its row and column. Thus removing it gives the following recurrence relation

$$f(\lambda_1, \ldots, \lambda_m) = \sum_k f(\lambda_1, \ldots, \lambda_{k-1}, \lambda_k - 1, \lambda_{k+1}, \ldots, \lambda_m),$$

where we use the convention that $f(\lambda_1, \ldots, \lambda_m) = 0$ if there exists i such that $\lambda_i < \lambda_{i+1}$ (which is consistent with the definition of F). It is therefore enough to show that F satisfies the same recurrence relations (the initial values coincide as $F(1, 0, \ldots, 0) = f(1, 0, \ldots, 0) = 1$). We note that in these relations some of the rows may be empty and thus it may happen that $\lambda_i = 0$ for some numbers i.

We now introduce the following random process. With probability $\frac{1}{n}$ we choose a cell $(a, b) = (a_1, b_1)$. If the chosen cell was a corner we stop the process. If not with uniform probability $\frac{1}{h_{a_1 b_1} - 1}$ we choose a cell (a_2, b_2) in the hook H_{a_1, b_1} at (a_1, b_1) (it is forbidden to take the cell (a_1, b_1)). If (a_2, b_2) is a corner, we stop the process, if not we choose uniformly with probability $\frac{1}{h_{a_2 b_2} - 1}$ a cell in the hook H_{a_2, b_2} at (a_2, b_2). We continue like this until we reach a corner.

Let $p(\alpha, \beta)$ be the probability that the process terminates at (α, β). The sequence

$$(a, b) = (a_1, b_1) \to (a_2, b_2) \to (a_3, b_3) \to \ldots \to (a_l, b_l) = (\alpha, \beta) \tag{11}$$

will be called a trajectory of our process. The sets

$$A = \{a_1, \ldots, a_l\}, \qquad B = \{b_1, \ldots, b_l\} \tag{12}$$

will be called the horizontal and vertical projections of our trajectory. Let $p(A, B|a, b)$ be the probability that a random trajectory has projection A and B given that the first cell is (a, b). Note that this is non-zero only if $a = \min A$ and $b = \min B$. We observe that many different trajectories may have the same projections, for example for $n = 2$, $\lambda_1 = \lambda_2 = 2$ the trajectory $(1, 1) \to (1, 2) \to (2, 2)$ has the the same projections as $(1, 1) \to (2, 1) \to (2, 2)$ (here $A = B = \{1, 2\}$).

Lemma 8. For any corner (α, β) and any (a, b) and A, B with $a = \min A$, $b = \min B$, $\alpha = \max A$, $\beta = \max B$ we have

$$p(A, B \mid a, b) = \prod_{i \in A, i \neq \alpha} \frac{1}{h_{i\beta} - 1} \cdot \prod_{j \in B, j \neq \beta} \frac{1}{h_{\alpha j} - 1}.$$

Proof. Let us denote the product on the right hand side by Π. We shall proceed by induction on the length of the path l. We adapt the convention that the empty product equals 1. Consider again the random trajectory (11) and the projections (12). Let us proceed by the induction on $|A| + |B|$. Suppose $A = \{a = a_1 < a_2 < \ldots\}$ and $B = \{b = b_1 < b_2 < \ldots\}$. We have (depending on whether the process goes down or right from (a, b)

$$p(A, B \mid a, b) = \frac{1}{h_{ab} - 1}\big(p(A \setminus \{a_1 = a\}, B \mid a_2, b_1) + p(A, B \setminus \{b_1 = b\} \mid a_1, b_2)\big).$$

By the induction hypothesis we have

$$p(A \setminus \{a_1 = a\}, B \mid a_2, b_1) = (h_{a\beta} - 1)\Pi, \qquad p(A, B \setminus \{b_1 = b\} \mid a_1, b_2)\big) = (h_{\alpha b} - 1)\Pi.$$

The assertion follows from the fact that $h_{ab} - 1 = (h_{a\beta} - 1) + (h_{\alpha b} - 1)$. Indeed, we have (with the notation introduced in Figure 9) Indeed, we have

$$\begin{aligned}(h_{a\beta} - 1) + (h_{\alpha b} - 1) &= (\alpha - a + v - \beta + 1 - 1) + (u - \alpha + \beta - b + 1 - 1) \\ &= v - a + u - b = h_{a,b} - 1.\end{aligned}$$

□

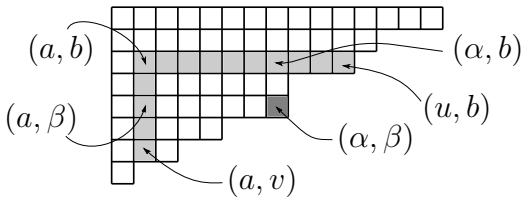


Figure 9: Definition of u and v.

From Lemma 8 we get

$$p(\alpha,\beta) = \frac{1}{n}\sum_{a,b} \sum_{\substack{A\subseteq\{1,\dots,\alpha\},\ B\subseteq\{1,\dots,\beta\}\\ \min A=a,\min B=b\\ \max A=\alpha,\max B=\beta}} p(A,B \mid a,b)$$

$$= \frac{1}{n}\sum_{a,b} \sum_{\substack{A\subseteq\{1,\dots,\alpha\},\ B\subseteq\{1,\dots,\beta\}\\ \min A=a,\min B=b\\ \max A=\alpha,\max B=\beta}} \prod_{i\in A, i\neq\alpha} \frac{1}{h_{i\beta}-1}\cdot \prod_{j\in B, j\neq\beta} \frac{1}{h_{\alpha j}-1}$$

$$= \frac{1}{n} \sum_{\substack{A\subseteq\{1,\dots,\alpha\},\ B\subseteq\{1,\dots,\beta\}\\ \max A=\alpha,\max B=\beta}} \prod_{i\in A, i\neq\alpha} \frac{1}{h_{i\beta}-1}\cdot \prod_{j\in B, j\neq\beta} \frac{1}{h_{\alpha j}-1}.$$

Lemma 9. We have

$$p(\alpha,\beta) = \frac{F_\alpha}{F} := \frac{F(\lambda_1,\dots,\lambda_{\alpha-1},\lambda_\alpha-1,\lambda_{\alpha+1}\dots,\lambda_m)}{F(\lambda_1,\dots,\lambda_m)}.$$

Proof. We first observe that if $\lambda_{\alpha+1} > \lambda_\alpha - 1$ then the right hand side is zero which corresponds to the case when (α,β) is not corner. Thus is this case our claim is true.

Now assume that (α,β) is a corner. Using the definition of F we see that removing the cell (α,β) results in shortening of the hooks $H_{i\beta}$ and $H_{\alpha j}$ by 1. Also n drops down to $n-1$. We therefore get

$$\frac{F_\alpha}{F} = \frac{1}{n}\prod_{1\le i<\alpha}\frac{h_{i\beta}}{h_{i\beta}-1}\prod_{1\le j<\beta}\frac{h_{\alpha j}}{h_{\alpha j}-1} = \frac{1}{n}\prod_{1\le i<\alpha}\left(1+\frac{1}{h_{i\beta}-1}\right)\prod_{1\le j<\beta}\left(1+\frac{1}{h_{\alpha j}-1}\right)$$

$$= \frac{1}{n}\sum_{A\subseteq\{1,\dots,\alpha-1\},\ B\subseteq\{1,\dots,\beta-1\}} \prod_{i\in A}\frac{1}{h_{i\beta}-1}\cdot\prod_{j\in B}\frac{1}{h_{\alpha j}-1}$$

$$= \frac{1}{n}\sum_{\substack{A\subseteq\{1,\dots,\alpha\},\ B\subseteq\{1,\dots,\beta\}\\ \max A=\alpha,\max B=\beta}} \prod_{i\in A, i\neq\alpha}\frac{1}{h_{i\beta}-1}\cdot\prod_{j\in B, j\neq\beta}\frac{1}{h_{\alpha j}-1} = p(\alpha,\beta).$$

□

To finish the proof we observe that for any α the is at most one β such that (α,β) is a corner and thus

$$\sum_\alpha \frac{F_\alpha}{F} = \sum_{(\alpha,\beta)\ -\text{corner}} \frac{F_\alpha}{F} = \sum_{(\alpha,\beta)\ -\text{corner}} p(\alpha,\beta) = 1.$$

In other words

$$F(\lambda_1,\ldots,\lambda_m)=\sum_k F(\lambda_1,\ldots,\lambda_{k-1},\lambda_k-1,\lambda_{k+1},\ldots,\lambda_m),$$

which was the desired equality. □

9 Combinatorics of convex sets

9.1 Helly, Radon and Carathéodory theorems

Theorem 58 (Radon's theorem)**.** Let A be a subset of $\mathbb{R}^d$ with $n\geq d+2$. Then there exists a partition $A=X\cup Y$ such that $\mathrm{conv}(X)\cap\mathrm{conv}(Y)\neq\emptyset$.

Proof. Without loss of generality we can assume that $n=d+2$. Suppose $A=\{x_1,\ldots,x_{d+2}\}$. Note that $\{x_1-x_{d+2},\ldots x_{d+1}-x_{d+2}\}$ is the collection of $d+1$ vectors. Thus, these vectors are linear dependent, i.e. there exists a sequence of real numbers $a_1,\ldots,a_{d+1}$ such that $\sum_{j=1}^{d+1}a_j(x_j-x_{d+2})=0$ and $a_{j_0}\neq 0$ for some j_0. Take $b_1=a_1,\ldots,b_{d+1}=a_{d+1}$ and $b_{d+2}=-(a_1+\cdots+a_{d+1})$. It follows that $\sum_{j=1}^{d+2}b_j=0$ and $\sum_{j=1}^{d+2}b_jx_j=0$. The sets $I_+=\{i:\ b_i>0\}$, $I_-=\{i:\ b_i<0\}$ are both nonempty and $\sum_{i\in I_+}b_i=\sum_{i\in I_-}(-b_i)$. Thus,

$$\frac{\sum_{i\in I_+}b_ix_i}{\sum_{i\in I_+}b_i}=\frac{\sum_{i\in I_-}(-b_i)x_i}{\sum_{i\in I_-}(-b_i)}.$$

The left hand side of the above equality belongs to $\mathrm{conv}\{x_i:i\in I_+\}$ while the right hand side is in $\mathrm{conv}\{x_i:i\in I_-\}$. □

Theorem 59 (Helly's theorem)**.** Let $K_1,K_2,\ldots,K_n$ be a finite family of convex subsets of $\mathbb{R}^d$ with the following property: for every $I\subseteq[n]$ with $|I|=d+1$ we have $\bigcap_{i\in I}K_i\neq\emptyset$. Then $\bigcap_{i=1}^n K_i\neq\emptyset$.

Proof. The case $n\leq d+1$ is trivial. We first give a solution in the case $n=d+2$. Take the sets $L_i=\bigcap_{j\neq i}K_j$. Each of them is nonempty. Take $x_i\in L_i$, $1\leq i\leq d+2$. If these points are not distinct, say $x_i=x_k$, $i\neq k$, we see that $x_i\in L_i\cap L_k=\bigcap_{i=1}^{d+2}K_i$. We can therefore assume that our points are distinct. From Radon's theorem there exist a partition of $\{1,\ldots,d+2\}$ into two sets I,J such that $\mathrm{conv}\{x_i:\ i\in I\}$ and $\mathrm{conv}\{x_j:\ j\in J\}$ have a nonempty intersection. Let y be a point belonging to this intersection. We show that $y\in K_1$. In the same way we can prove that $y\in K_j$ for every $1\leq j\leq d+2$. Without loss of generality we can assume that $1\in I$. We have $\{x_j:\ j\in J\}\subset K_1$, since the only point which does not belong to K_1 is x_1. It follows that $y\in\mathrm{conv}\{x_j:\ j\in J\}\subset\mathrm{conv}(K_1)=K_1$.

Now we use induction on n. Take $n>d+2$ and suppose that our assertion is true for $n-1$. Take the sets $K_1,K_2,\ldots,K_{n-2},K_{n-1}\cap K_n$. From the case $n=d+2$ we see that any $d+1$ elements in this collection have nonempty intersection. Thus, from the induction hypothesis the whole collection has a nonempty intersection. □

Theorem 60 (Carathéodory theorem)**.** Let $d\geq 1$ and let $X\subset\mathbb{R}^d$. Suppose $x\in\mathrm{conv}(X)$. Prove that there exists a set $X_0\subset X$ with $|X_0|\leq d+1$ such that $x\in\mathrm{conv}(X_0)$.

Proof. It is easy to see that

$$\mathrm{conv}(X)=\left\{\sum_{i=1}^n\lambda_ix_i:\ x_i\in X,\ \lambda_i\geq 0,\ \sum_{i=1}^n\lambda_i=1,\ n\geq 1\right\}.$$

Thus, we can write $x=\sum_{i=1}^n\lambda_ix_i$. If $n\leq d+1$ then there is nothing to prove. Assume that $n>d+1$. As in the proof of Radon's theorem there exists a sequence $b_1,\ldots,b_n$ such that $\sum_{i=1}^n b_i=0$ and $\sum_{i=1}^n b_ix_i=0$

with $b_{j_0} \neq 0$ for some j_0. Thus, $x = \sum_{i=1}^{n}(\lambda_i - cb_i)x_i$ and $\sum_{i=1}^{n}(\lambda_i - cb_i) = 1$ for every $c \in \mathbb{R}$. Take c such that $\lambda_i - cb_i \geq 0$, $1 \leq i \leq n$ and at least one such value is 0 (the existence of such c can be achieved by increasing c from 0 and taking the smallest value of c for which one of the number $\lambda_i - cb_i$ equals 0). We have expressed x as a convex combination of $n-1$ elements of X. We can further decrease the length of this sum as long as the condition $n > d+1$ is satisfied. □

Remarks. Radon's theorem generalizes to the following Tverberg's theorem.

Theorem 61. Take $d \geq 1$ and $r \geq 2$. Given at least $(r-1)(d+1)+1$ points in $\mathbb{R}^d$, we can always partition these points into r parts such that the convex hulls of these parts intersect.

9.2 Brunn-Minkowski inequality & isoperimetric problem.

Isoperimetric inequality. The isoperimetric inequality states that among sets of prescribed volume in $\mathbb{R}^n$ the sets minimizing the surface area measure are Euclidean balls. For our purposes the surface area measure is defined as

$$\mathrm{vol}^+(\partial A) = \liminf_{t \to 0^+} \frac{\mathrm{vol}(A_t) - \mathrm{vol}(A)}{t},$$

where $A_t = \{x \in \mathbb{R}^n : \mathrm{dist}(A, x) \leq t\}$ is the so-called t-enlargement of A. If t is small then $A_t \setminus A$ is shell of width t above the boundary of A, see Figure 10.

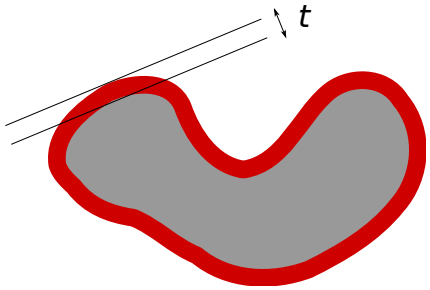


Figure 10: Set A with its t-enlargement. The red part is $A_t \setminus A$. If $t \to t^+$ the red part "approximates" the boundary ∂A.

In order to prove isoperimetric inequality it is enough to show that $\mathrm{vol}(A) = \mathrm{vol}(B)$ (where B is a ball) implies $\mathrm{vol}(A_t) \geq \mathrm{vol}(B_t)$ for $t > 0$. Indeed the then get

$$\mathrm{vol}^+(\partial A) = \liminf_{t \to 0^+} \frac{\mathrm{vol}(A_t) - \mathrm{vol}(A)}{t} \geq \liminf_{t \to 0^+} \frac{\mathrm{vol}(B_t) - \mathrm{vol}(B)}{t} = \mathrm{vol}^+(\partial B).$$

Let us introduce the notion of the Minkowski sum:

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

We now observe that $A_t = A + B(t)$, where $B = B(t)$ is a closed ball of radius t centered at 0. Let r be such that $|A| = |B(r)|$. Since $B(r)_t = B(r+t)$, we get

$$\begin{aligned}\mathrm{vol}(B(r)_t)^{\frac{1}{n}} &= \mathrm{vol}(B(r+t))^{\frac{1}{n}} = (r+t)\,\mathrm{vol}(B(1))^{\frac{1}{n}} = r\,\mathrm{vol}(B(1))^{\frac{1}{n}} + t\,\mathrm{vol}(B(1))^{\frac{1}{n}} \\ &= \mathrm{vol}(B(r))^{\frac{1}{n}} + \mathrm{vol}(B(t))^{\frac{1}{n}} = \mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B(t))^{\frac{1}{n}}\end{aligned}$$

If we could prove that

$$\mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B(t))^{\frac{1}{n}} \leq \mathrm{vol}(A + B(t))^{\frac{1}{n}} = \mathrm{vol}(A_t)^{\frac{1}{n}},$$

we would get the desired inequality $\mathrm{vol}(B(r)_t) \leq \mathrm{vol}(A_t)$. This will be done in the next paragraph.

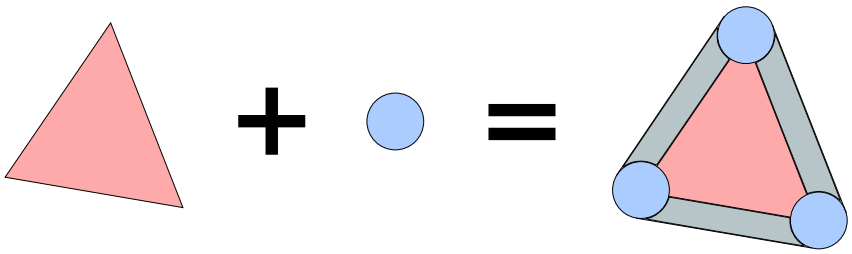


Figure 11: Minkowski sum of a triangle and a ball.

Brunn-Minkowski inequality. Our goal is to show the following theorem.

Theorem 62. Suppose A, B are measurable non-empty subsets of $\mathbb{R}^n$ such that $A+B$ is also measurable. Then

$$\mathrm{vol}(A+B)^{\frac{1}{n}} \geq \mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B)^{\frac{1}{n}}.$$

We first prove the Brunn-Minkowski inequality in the case of simple sets being finite non-empty unions of disjoint boxes

$$[c_1, d_1] \times \ldots \times [c_n, d_n], \qquad c_i < d_i,\ i = 1, \ldots, n.$$

We proceed by induction on the sum l of the number of boxes in A and the number of boxes in B. The base case is $l = 2$, that is A and B consist of only one box. We note that we can always shift our sets since this does not affect our inequality. We can therefore assume that

$$A = [0, a_1] \times \ldots [0, a_n], \qquad B = [0, b_1] \times \ldots \times [0, b_n].$$

In this case we clearly have $A + B = [0, a_1 + b_1] \times \ldots \times [0, a_n + b_n]$. Our inequality amounts then to

$$\sqrt[n]{(a_1 + b_1) \ldots (a_n + b_n)} \geq \sqrt[n]{a_1 \ldots a_n} + \sqrt[n]{b_1 \ldots b_n}.$$

By the AM-GM inequality we get

$$1 = \frac{1}{n}\sum_{i=1}^{n} \frac{a_i}{a_i + b_i} + \frac{1}{n}\sum_{i=1}^{n} \frac{b_i}{a_i + b_i} \geq \sqrt[n]{\frac{a_1}{a_1 + b_1} \cdot \ldots \cdot \frac{a_n}{a_n + b_n}} + \sqrt[n]{\frac{b_1}{a_1 + b_1} \cdot \ldots \cdot \frac{b_n}{a_n + b_n}}.$$

Multiplying by $\sqrt[n]{(a_1 + b_1) \ldots (a_n + b_n)}$ yields the desired inequality.

We now proceed to the induction step. Suppose that the sum of the number of boxes in A and the number of boxes in B is $l \geq 3$ and suppose that the assertion is true for all cases in which this number is less than l. Without loss of generality assume that in A there are at least two boxes I_1 and I_2. Since the boxes are disjoint, there is some $i \in \{1, \ldots, n\}$ and some h such that I_1 lies in the open halfspace $\{x_i > h\}$ and I_2 lies in the open halfspace $\{x_i < h\}$ or vice versa. By shifting A be can assume that $h = 0$. Cutting the space with this halfspace is called *Hadwiger-Ohman cut* and is in fact the crux of the whole proof.

Denote by A_- and A_+ the intersections of A with the closed halfspaces $\{x_i \leq 0\}$ and $\{x_i \geq 0\}$, respectively. Then each of A_- and A_+ is non-empty and is a union of fewer than l pairwise disjoint boxes. (Perhaps the hyperplane $x_i = 0$ cuts other boxes of A, but we do not pay attention about that. We are only interested in separating I_1 and I_2). Since A is the pairwise disjoint union of A_+, A_- and a set of volume zero, we have $\mathrm{vol}(A) = \mathrm{vol}(A_+) + \mathrm{vol}(A_-)$. Let $\alpha := \mathrm{vol}(A_+)/\mathrm{vol}(A) \in (0, 1)$. Now, it is possible to shift B in such a way the set $B_+ = B \cap \{x_i \geq 0\}$ "catches" the α proportion of B. We also define $B_- = B \cap \{x_i \leq 0\}$. Thus we get

$$\frac{\mathrm{vol}(A_+)}{\mathrm{vol}(A)} = \frac{\mathrm{vol}(B_+)}{\mathrm{vol}(B)} = \alpha, \qquad \frac{\mathrm{vol}(B^-)}{\mathrm{vol}(B)} = \frac{\mathrm{vol}(A^-)}{\mathrm{vol}(A)} = 1 - \alpha.$$

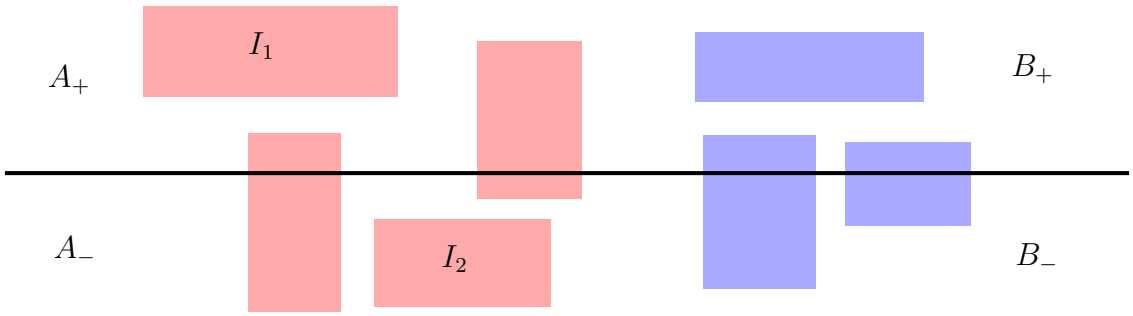


Figure 12: The set A is divided into two parts A_+ and A_- using the Hadwiger-Ohman cut. The boxes I_1 and I_2 has been separated.

The set $A_+ + B_+$ is contained in $\{x_i \geq 0\}$ whereas $A_- + B_-$ is contained in $\{x_i \leq 0\}$. Therefore,

$$\mathrm{vol}((A_+ + B_+) \cup (A_- + B_-)) = \mathrm{vol}(A_+ + B_+) + \mathrm{vol}(A_- + B_-). \tag{13}$$

Moreover, these two sets are clearly subsets of $A + B$ as $A_+, A_- \subseteq A$ and $B_+, B_- \subseteq B$. This gives

$$\mathrm{vol}(A + B) \geq \mathrm{vol}((A_+ + B_+) \cup (A_- + B_-)) = \mathrm{vol}(A_+ + B_+) + \mathrm{vol}(A_- + B_-). \tag{14}$$

The sum of the number of boxes in A_+ and the number of boxes in B_+ is at most $l - 1$ boxes (since one of the boxes I_1, I_2 is not in A_+). The same applies to A_- and B_-. Thus, by induction hypothesis applied twice (to A_+, B_+ and A_-, B_-), we get

$$\begin{aligned}\mathrm{vol}(A + B) &\geq \mathrm{vol}((A_+ + B_+) + \mathrm{vol}(A_- + B_-) \geq (\mathrm{vol}(A_+)^{\frac{1}{n}} + \mathrm{vol}(B_+)^{\frac{1}{n}})^n + (\mathrm{vol}(A_-)^{\frac{1}{n}} + \mathrm{vol}(B_-)^{\frac{1}{n}})^n \\ &= \alpha(\mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B)^{\frac{1}{n}})^n + (1-\alpha)(\mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B)^{\frac{1}{n}})^n = (\mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B)^{\frac{1}{n}})^n.\end{aligned}$$

The assertion follows.

In the next paragraph w show how Brunn-Minkowski inequality for boxes implies the general case.

From boxes to measurable sets. Suppose that we already ensured about the validity of the Brunn-Minkowski inequality for some family of simple sets, for example for compact (or open) set or for even smaller family of finite unions of closed boxes of the form

$$[a_1, b_1] \times \ldots \times [a_n, b_n], \qquad a_i < b_i, \ i = 1, \ldots, n. \tag{15}$$

Then we would like to deduce the Brunn-Minkowski inequality for general measurable sets. This is possible due to the following proposition.

Lemma 10. Assume that the Brunn-Minkowski inequality holds true for non-empty sets being finite unions of boxes of the form (15). Then it holds true for all pairs of measurable sets whose sum is also measurable.

Proof. Let A and B be non-empty measurable sets whose sum is also measurable. Assume we know how to prove the Brunn-Minkowski inequality for compact sets. Let (A_k) and (B_k) be sequences of compact sets approximating A and B from below, namely $A_k \subseteq A$, $B_k \subseteq B$ and

$$\lim_{k\to\infty} \mathrm{vol}(A_k) = \mathrm{vol}(A), \qquad \lim_{k\to\infty} \mathrm{vol}(B_k) = \mathrm{vol}(B).$$

Such approximations exist due to the inner regularity of Lebesgue measure. Indeed, for any measurable set A in $\mathbb{R}^n$, we have

$$\mathrm{vol}(A) = \sup\{\mathrm{vol}(K) : \ K \subseteq A, \quad K - \text{compact}\}.$$

Since for any n we have $A_n + B_n \subseteq A + B$, we get

$$\mathrm{vol}(A+B)^{\frac{1}{n}} \geq \mathrm{vol}(A_k + B_k)^{\frac{1}{n}} \geq \mathrm{vol}(A_k)^{\frac{1}{n}} + \mathrm{vol}(B_k)^{\frac{1}{n}}.$$

Taking the limit as $k \to \infty$ gives the result.

Now suppose we know how to prove our inequality for non-empty open sets. We shall deduce the inequality for non-empty compact sets. To this end take non-empty compact sets A and B and consider the sets $A_r = A + r\tilde{B}_2^n$ and $B_r = B + \tilde{B}_2^n$, where $\tilde{B}_2^n$ is the open Euclidean unit ball centred at the origin. In particular the sets A_r, B_r are clearly open. We clearly have

$$A_r = \{x \in \mathbb{R}^n : \ \mathrm{dist}(A, x) < r\},$$

where the distance is taken in the standard Euclidean metric. Thus, we get

$$\begin{aligned}\mathrm{vol}(A + B + 2r\tilde{B}_2^n)^{\frac{1}{n}} &= \mathrm{vol}((A + r\tilde{B}_2^n) + (B + r\tilde{B}_2^n))^{\frac{1}{n}} \\ &\geq \mathrm{vol}(A + r\tilde{B}_2^n)^{\frac{1}{n}} + \mathrm{vol}(B + r\tilde{B}_2^n)^{\frac{1}{n}} \\ &\geq \mathrm{vol}(A)^{\frac{1}{n}} + \mathrm{vol}(B)^{\frac{1}{n}}.\end{aligned}$$

The set $C = A + B$ is compact as a Minkowski sum of two compact sets. Take $r_k = \frac{1}{2k}$, $k \geq 1$. Then $A + B + 2r_k\tilde{B}_2^n = C + \frac{1}{k}\tilde{B}_2^n$. Let us denote this set by C_k. The Lebesgue measure is continuous, namely for arbitrary sequence of measurable sets $C_1 \supseteq C_2 \supseteq \ldots$ with $\mathrm{vol}(C_1) < \infty$ we have $\mathrm{vol}(\bigcap_{k=1}^{\infty} C_k) = \lim_{k\to\infty} \mathrm{vol}(C_k)$. Applying this principle to our sets C_k and using the fact that due to the compactness of C, we have

$$\bigcap_{k=1}^{\infty} C_k = \bigcap_{k=1}^{\infty} \left(C + \frac{1}{k}B_2^n\right) = \{x \in \mathbb{R}^n : \ \mathrm{dist}(C, x) = 0\} = C,$$

gives $\lim_{k\to\infty} \mathrm{vol}(A + B + 2rB_2^n) = \lim_{k\to\infty} \mathrm{vol}(C_k) = \mathrm{vol}(C) = \mathrm{vol}(A + B)$. The assertion of the Brunn-Minkowski inequality follows.

Finally, assume that the Brunn-Minkowski inequality holds true for finite unions of boxes. We shall deduce it for arbitrary non-empty open sets U and V. There exist sequences (C_k) and (D_k) of sets being finite unions of boxes such that $C_k \subseteq U$, $D_k \subseteq V$ and

$$\lim_{k\to\infty} \mathrm{vol}(C_k) = \mathrm{vol}(U), \qquad \lim_{k\to\infty} \mathrm{vol}(D_k) = \mathrm{vol}(V).$$

This is a well known property of Lebesgue measure, which follows for example from the fact that every open set U is a union of countably many open balls and thus also countably many boxes B_k, $k \geq 1$. Due to the continuity of the Lebesgue measure (for measurable sets $S_1 \subseteq S_2 \subseteq \ldots$ we have $\mathrm{vol}(\bigcup_{k=1}^{\infty} S_k) = \lim_{k\to\infty} \mathrm{vol}(S_k)$), we get

$$\mathrm{vol}(U) = \mathrm{vol}\left(\bigcup_{k=1}^{\infty} B_k\right) = \mathrm{vol}\left(\bigcup_{k=1}^{\infty}\bigcup_{j=1}^{k} B_j\right) = \lim_{k\to\infty} \mathrm{vol}\left(\bigcup_{j=1}^{k} B_j\right).$$

Thus setting $C_k = \bigcup_{j=1}^{k} B_j$ gives the desired approximation. Now it suffice to observe that

$$\mathrm{vol}(U+V)^{\frac{1}{n}} \geq \mathrm{vol}(C_k + D_k)^{\frac{1}{n}} \geq \mathrm{vol}(C_k)^{\frac{1}{n}} + \mathrm{vol}(D_k)^{\frac{1}{n}} \xrightarrow[k\to\infty]{} \mathrm{vol}(U)^{\frac{1}{n}} + \mathrm{vol}(V)^{\frac{1}{n}}.$$

□

Remark. The example of a fat Cantor set shows that it is not possible to directly approximate measurable sets by finite unions of boxes.

References

[AF] N. Alon, Z. Füredi, Covering the cube by affine hyperplanes, European Journal of Combinatorics 14 (1993), 79-83.

[ES] P. Erdös, G. Szekeres, *A combinatorial problem in geometry*, Compositio Math, 2:463–470, 1935.

[K1] http://www.ma.huji.ac.il/∼kalai/erdos100.pdf

[R] S. Radziszewski, *Small Ramsey numbers*, The Electronic Journal of Combinatorics.

[AI] I. Anderson, *Combinatorics of Finite Sets*, Oxford University Press, New York, 1st edition, 1987, 2-4.

[A] N. Alon, *Combinatorial Nullstellensatz*, Combin. Prob. Comput. 8 (1999), 7-29.

[E] P. Erdös, *On a lemma of Littlewood and Offord*, Bulletin of the American Mathematical Society 51 (1945), 898–902

[LS73] P.W.H. Lehmmens and J. J. Seidel, Equiangular lines, J. of Algebra 24 (1973), 494–512.

[M] Michałek, *A short proof of Combinatorial Nullstellensatz*, American Mathematical Monthly 117 (2010), 821–823.

[Z] A. Zygmund, *A Remark on Conjugate Series*, Proc. London Math. Soc. S2-34 no. 1, 392.

[A] D.D. Adamović, *Quelques remarques relatives aux généralisations des inégalités de Hlawka et de Hornich*, Mat. Vesnik, vol. 1, 16, 1964, 241-242.

[BVW] J. Bourgain, V. Vu, P.M. Wood, http://arxiv.org/abs/0905.0461.

[D] D.Z. Djoković, *Generalizations of Hlawka's inequality*, Glas. Mat.–Fiz. Astronom., Ser. II, Drustvo Mat. Fiz. Hratske 18 (1963), 169–175.

[K] J. Komlos, *On the determinant of* $(0,1)$ *matrices*, Studia Sci. Math. Hungar. 2 (1967), 7-2 1.

[KKS] J. Kahn, J. Komlós, E. Szemerédi, *On the probability that a random* ± 1*-matrix is singular*, J. Amer. Math. Soc. 8 (1995), no. 1, 223–240.

[M] Mateusz Michałek, A short proof of Combinatorial Nullstellensatz The American Mathematical Monthly 117, no. 9 (2010), 821-823.

[TV] T. Tao, V. Vu, *On the singularity probability of random Bernoulli matrices*, J. Amer. Math. Soc. 20 (2007), 603–628.

[AZ] M. Aigner, G. Ziegler, *Proofs from the book*, Springer, 2003 (third edition).

[ES] P. Erdös, G. Szekeres, *A combinatorial problem in geometry*, Compositio Math, 2:463–470, 1935.

[GNT] O. Guédon, P. Nayar, T. Tkocz, *Concentration inequalities and geometry of convex bodies*, submitted to IMPAN Lecture Notes, 2012.

[W] Wildon's Weblog, http://wildonblog.wordpress.com/2011/01/

[P] Pajor, Alain (1985), Sous-espaces l_1^n des espaces de Banach, Travaux en Cours [Works in Progress], 16, Paris: Hermann