Algebraic methods in Combinatorics

Benny Sudakov

November 6, 2023

Contents

Chapter 1

Basic linear algebra methods

1.1 Introduction: Mantel's theorem

How many edges can a triangle-free graph on n vertices have? This is a classical question in extremal graph theory, and Mantel's theorem gives the answer.

Theorem 1.1 (Mantel, 1907)**.** *Every n vertex triangle free graph has at most $n^2/4$ edges.*

Mantel's theorem is tight: the bound is attained by the complete bipartite graph $K_{n/2,n/2}$, meaning a bipartite graph with bipartition A, B such that $|A| = |B| = n/2$ and all edges between A, B are present.

Crucially, this can be shown to be the *unique* extremal example. We will shortly see some examples of problems which have a much richer class of extremal examples. This tends to be an indication that methods from linear algebra may be relevant.

1.2 Rules and clubs (the Eventown/Oddtown problem)

In this section we'll give our first illustration of an application of basic linear algebra to combinatorics.

The setting is that there are two neighbouring towns: Eventown and Oddtown. In each town, there are n people who want to form clubs. In order to restrict the number of possible clubs, the town imposes certain rules. Here, clubs are just distinct subsets of $[n] = \{1, 2, \ldots, n\}$.

Eventown has the following rules.

- Every club has an even number of members
- Any 2 clubs share an even number of members

How many clubs can be formed under these rules?

Example 1.2. Provided n is even we can group the elements into pairs $\{1,2\};\{3,4\};\ldots;\{n-1,n\}$. Then, we can consider the collection of clubs obtained by taking arbitrary unions of these pairs. There are $2^{n/2}$ such clubs. One can show that this is maximal (Berlekamp 1969, Graver 1975).

In our setting, the rules of Eventown are "bad" because they are not very restrictive: the people can still form exponentially many clubs! Let's now consider the rules in Oddtown.

- Every club has an odd number of members
- Any 2 clubs share an even number of members

How many clubs may be formed in Oddtown?

Example 1.3. The following examples show that it is possible to have n clubs satisfying these rules.

- We could form the singleton clubs $\{1\},\ldots,\{n\}$.
- If n is even, we can form clubs of the form $[n]\backslash\{i\}$.
- Alternatively, if n is even we can form the clubs $\{1,3,\ldots,n\}$, $\{2,3,\ldots,n\}$ and $\{1,2,i\}$ for $i>2$.
- If $n=q^2+q+2$ for some odd prime power q, then we can use projective planes to construct an Oddtown. Indeed, if that is the case we know that there exists a projective plane with $n-1$ points (and lines)[1]. Let us represent the collection of lines as a family $\mathcal{A}=\{A_1,\ldots,A_{n-1}\}\subseteq 2^{[n-1]}$. The clubs forming the Oddtown in $[n]$ will be the sets $A_1\cup\{n\},\ldots,A_{n-1}\cup\{n\}$ and the set $[n-1]$. Let us check that the rules are satisfied. Every club indeed has an odd number of members since n is even and all the sets A_i have size $q+1$, which is even. Now take two clubs; if they are both of the form $A_i\cup\{n\}$, they have precisely 2 common members, since any two distinct sets A_i have exactly one common intersection point; if one of the clubs is $[n-1]$, then the intersection of the two clubs is of the size of a set A_i, that is, $q+1$, which is even.

We remark that there are actually $2^{n^2/8-o(n^2)}$ non-isomorphic configurations of size n (where an isomorphism is a relabelling of the ground set). This represents very different behaviour to Mantel's theorem!

In fact, Oddtown's rules are "better" than the rules of Eventown:

Claim 1.4 (Berlekamp, 1969)**.** *There are at most n clubs in any system of clubs in Oddtown.*

Proof. Let $F_1,\ldots,F_m\subseteq[n]$ denote the clubs. Let v_i be the characteristic vector over $\mathbb{F}_2$ of the i-th club F_i, so in particular $v_i=(x_1,x_2,\ldots,x_n)$ where $x_j=1$ if and only if $j\in F_i$. Suppose

$$\sum_{i=1}^{m}\alpha_i v_i=0.$$

Note that $v_i\cdot v_j=|F_i\cap F_j|$, so in particular the rules imply $v_i\cdot v_i=|F_i|\equiv 1 \bmod 2$ and for $i\neq j$ we have $v_i\cdot v_j=|F_i\cap F_j|\equiv 0 \bmod 2$. Using this, taking the dot product of the above equality with v_i for any i gives $\alpha_i=0$. So, the vectors are linearly independent in $\mathbb{F}_2^n$. As the dimension of this space is n there are at most n of them. □

[1] Take a look at the appendix for the definition and properties of projective planes, as well as an example.

1.3 Lines between points in the plane

Consider n points in the plane. How few lines can they define? Of course, by taking all the points to be collinear there can be only 1 line. What if we disallow all the points to be collinear?

Example 1.5. Take $n-1$ collinear points and one not on the same line.

This example shows there can be as few as n lines defined by n points. The following theorem shows that this is best possible.

Theorem 1.6 (Sylvester–Gallai, 1944)**.** *Any set of n non-collinear points in the plane defines at least n lines.*

Proof. Suppose for the sake of contradiction that $p_1, \dots, p_n$ define lines $\ell_1, \dots, \ell_m$, with $m < n$. Assign to each p_i a real variable x_i and consider the system of equations

$$\sum_{i: p_i \in \ell_j} x_i = 0.$$

That is, the sum of variables on each line should be zero. Since $m < n$ the system is underdetermined and has a nontrivial solution. For this solution we have:

$$0 = \sum_j \left(\sum_{p_i \in \ell_j} x_i \right)^2 = \sum_{i=1}^n a_i x_i^2 + 2 \sum_{i<j}^n a_{i,j} x_i x_j,$$

Here a_i is the number of lines on which p_i lies ($a_i \geq 2$ as the points are not collinear), and $a_{i,j}$ is the number of lines on which both p_i and p_j lie, so $a_{i,j} = 1$. Thus

$$0 = \underbrace{\sum_{i=1}^n (a_i - 1) x_i^2}_{>0} + \underbrace{\left(\sum_{i=1}^n x_i \right)^2}_{\geq 0} > 0,$$

which is a contradiction. □

We end this section with a different, non-algebraic proof of Theorem 1.6. For this, we need a lemma.

Lemma 1.7. *Given a set of n non-collinear points in the plane, there is a line containing exactly 2 of them.*

Proof of Lemma 1.7. Take the pair consisting of a line l, and a point $p \notin l$ from the set which minimizes the distance between p and l. Suppose there are 3 points p_1, p_2, p_3 on l, such that p_2 is on the segment $p_1 p_3$. At least 2 of the p_i are on the same side of the perpendicular from p to l, say p_2, p_3, but then it is easy to see that the distance from p_2 to line pp_3 is smaller than from p to l, which is impossible. Hence there are only 2 points on line l. □

Second Proof of Theorem 1.6. Let l be the line provided by Lemma 1.7 and remove one of the points defining it, thereby removing at least 1 line. We proceed by induction, the base case of 3 points being trivial. We distinguish 2 cases. In the first case we assume the first $n-1$ points are non-collinear so we can apply the inductive assumption to conclude there are at least $n-1$ lines defined by them, which together with the one removed initially make the desired n. In the second case the remaining $n-1$ points are collinear, so the setting corresponds to Example 1.5 and thus there are n lines. □

1.4 Subsystems with equal unions

Suppose $A_1, \ldots, A_m \subseteq [n]$ are non-empty with $m \geq n+1$.

Claim 1.8 (Lindström 1972, Tverberg 1971)**.** *There are nonempty $I, J \subseteq [m]$ with $I \cap J = \emptyset$, such that $\bigcup_{i\in I} A_i = \bigcup_{i \in J} A_i$.*

Proof. Let $v_1, \ldots, v_m$ be the characteristic vectors of $A_1, \ldots, A_m$. Since there are more than n of them, they are linearly dependent over $\mathbb{R}$. So, there is a nonzero $\alpha \in \mathbb{R}^m$ with

$$\sum_{i=1}^{m} \alpha_i v_i = 0.$$

Let $I = \{i : \alpha_i > 0\}$, $J = \{j : \alpha_j < 0\}$. The nonzero coordinates of $\sum_{i \in I} \alpha_i v_i$ correspond to the elements of $\bigcup_{i\in I} A_i$, which are the same as the nonzero coordinates of $\sum_{j\in J} \alpha_j v_j$ corresponding to $\bigcup_{j \in J} A_j$, completing the proof. □

Remark 1.9. We can also prove this with Hall's theorem.

Actually, if $m \geq n+2$, then we can make the further requirement that I and J give the same intersections.

Theorem 1.10. *There are nonempty $I, J \subseteq [m]$ with $I \cap J = \emptyset$, such that $\bigcup_{i\in I} A_i = \bigcup_{i\in J} A_i$ and $\bigcap_{i\in I} A_i = \bigcap_{j \in J} A_j$.*

Proof. Let $u_i \in \mathbb{R}^{n+1}$ be defined as $u_i = \begin{pmatrix} v_i \\ 1 \end{pmatrix}$. Again $u_1, \ldots, u_m$ are linearly dependent so there is a non-zero $\alpha \in \mathbb{R}^m$ such that

$$\sum \alpha_i u_i = 0.$$

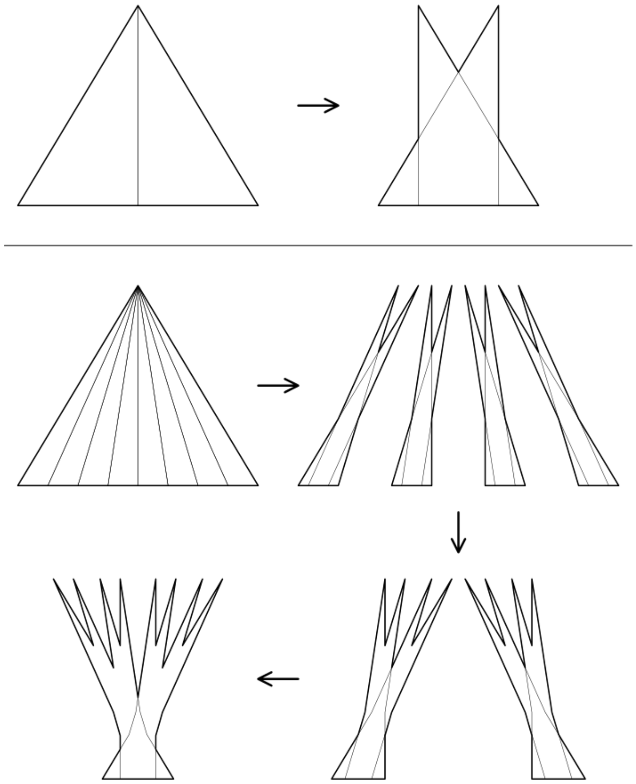
As before, let $I = \{i : \alpha_i > 0\}$, $J = \{j : \alpha_j < 0\}$. As in the above problem, looking at the first n coordinates we conclude $\bigcup_{i\in I} A_i = \bigcup_{i\in J} A_i$. But now we also know that $\sum_i \alpha_i = 0$ so $\sum_{i \in I} \alpha_i$ and $\sum_{j\in J} -a_j$ are equal to the same value t. Let $\beta_i = \alpha_i / t$ for $i \in I$ and $\gamma_j = -\alpha_j/t$ for $j \in J$, so in particular $\sum_{i\in I} \beta_i = 1 = \sum_{j\in J} \gamma_j$ and $\sum_{i \in I} \beta_i v_i = \sum_{j\in J} \gamma_j v_j$. Note that an element ℓ is in $\bigcap_{i\in I} A_i$ if and only if the ℓ-th coordinate of $\sum_{i\in I} \beta_i v_i$ equals 1, and is in $\bigcap_{j\in J} A_j$ if and only if the ℓ-th coordinate of $\sum_{j\in J} \gamma_j v_j$ is 1. Hence these coincide. □

1.5 The finite field Kakeya problem

The classical Kakeya problem is as follows: how small of a subset of $\mathbb{R}^n$ can we find, such that it contains a unit interval in every direction? Such a subset is called a *Kakeya set.* One may think that the smallest possible Kakeya set is a unit disk, but surprisingly there are arbitrarily small Kakeya sets.

Theorem 1.11 (Besicovitch, 1928)**.** *For all $\varepsilon > 0$, there exists $X \subseteq \mathbb{R}^2$ such that area$(X) < \varepsilon$ and X contains a unit interval in every direction.*

The basic idea of the proof is to take an equilateral triangle and cut it into 2^k slices and then iteratively overlap the slices, as shown in the diagram.



Note that the original triangle contains a unit interval for each angle between $-\pi/6$ and $\pi/6$. The cutting and overlapping preserves this property, while reducing the area. This gives 1/6 of all possible interval directions, so taking 3 rotated copies of this gives the desired construction.

In this section we will focus on a finite field variant of the Kakeya problem.

Definition 1.12. A is a Kakeya set if for all directions $v \in \mathbb{F}_p^n \backslash \{0\}$, there is a line $\{u + tv : t \in \mathbb{F}_p\}$ in A in that direction.

As in the real case, we ask how small a Kakeya set can be.

Theorem 1.13 (Dvir, 2008)**.** *For all $n \in \mathbb{N}$ there exists $c_n > 0$ such that if $A \subseteq \mathbb{F}_p^n$ is a Kakeya set, then $|A| \geq c_n p^n$.*

Remark 1.14. $c_n = 2^{-n}$ is best possible.

The basic idea of the proof is that if A is small then there exists a low degree polynomial $f(x_1, \ldots, x_n) \not\equiv 0$ such that $f(a) = 0$ for all $a \in A$. Then one can use properties of a Kakeya set to show that $f \equiv 0$, a contradiction.

For a multivariate polynomial $f(x_1, \ldots, x_n) = \sum_{\alpha \in S} C_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, we define its degree by $\deg(f) = \max\{\sum_{i=1}^n \alpha_i : \alpha \in S\}$. We will first need a few basic lemmas.

Lemma 1.15. *The number of monomials of degree at most $p-1$ is $\binom{p+n-1}{n} \approx \frac{p^n}{n!}$.*

Proof. Note that the number of monomials of degree at most $p-1$ is exactly the number of nonnegative integer solutions $\alpha_1, \dots, \alpha_n$ to the inequality $\alpha_1 + \ldots + \alpha_n \le p-1$, which in turn is the number of nonnegative integer solutions $\alpha_1, \dots, \alpha_{n+1}$ to the equation $\alpha_1 + \ldots + \alpha_{n+1} = p-1$. This is the classical 'balls and bins' problem, and it is well known that the number of solutions is $\binom{p+n-1}{n}$. □

Lemma 1.16. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a nontrivial polynomial with $\deg(f) \le d$. Then the number of roots of f is at most dp^{n-1}.*

Proof. We proceed by induction on n. For $n = 1$, we know that a univariate polynomial of degree at most d has at most d roots (by polynomial division). Now suppose $n > 1$. Then for $x \in \mathbb{F}_p^{n-1}$ and $y \in \mathbb{F}_p$, we may write

$$f(x, y) = g_0(x) + g_1(x)y + \ldots + g_k(x)y^k,$$

where g_i is a polynomial over $n-1$ variables with $\deg(g_i) \le d - i$. Thus by induction we have

$$|\{(x, y) : f(x, y) = 0 \wedge g_k(x) = 0\}| \le p|\{x : g_k(x) = 0\}| \le (d-k)p^{n-1}.$$

Moreover, for each choice of $x \in \mathbb{F}_p^{n-1}$ such that $g_k(x) \neq 0$, we have that $f(x, y)$ is a univariate polynomial in y of degree k that is not identically 0, so that it has at most k roots. It follows that

$$|\{(x, y) : f(x, y) = 0 \wedge g_k(x) \neq 0\}| = \sum_{x : g_k(x) \neq 0} |\{y : f(x, y) = 0\}| \le kp^{n-1},$$

and hence we conclude

$$\begin{aligned} |\{(x, y) : f(x, y) = 0\}| &= |\{(x, y) : f(x, y) = 0 \wedge g_k(x) = 0\}| + |\{(x, y) : f(x, y) = 0 \wedge g_k(x) \neq 0\}| \\ &\le (d-k)p^{n-1} + kp^{n-1} \\ &= dp^{n-1}. \end{aligned}$$

□

Now we may prove Theorem 1.13.

Proof of Theorem 1.13. Suppose $|A| < \binom{p+n-1}{n}$. Then there is a nontrivial polynomial f on n variables that vanishes on each $a \in A$ and has $\deg f \le p-1$. Indeed, any such f has the form

$$f(x_1, \dots, x_n) = \sum_{\alpha \in S} C_\alpha x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

where $S = \{\alpha \in \mathbb{N}_0^n : \sum_{i=1}^n \alpha_i \le p-1\}$ and $C_\alpha : \alpha \in S$ are coefficients, so we may find f by solving the system of linear equations $f(a) = 0 : a \in A$, in the variables $C_\alpha : \alpha \in S$. By Lemma 1.15, there are more variables than equations so a nontrivial solution must exist.

Let us write $f = p_0 + p_1 + \ldots + p_k$ where p_i is a homogenous polynomial of degree i (i.e. it is a linear combination of monomials, each having degree exactly i), and $p_k \not\equiv 0$. Since $\deg(f) \le p-1$, we have $k \le p-1$ and thus using Lemma 1.16, p_k has at most $kp^{n-1} \le (p-1)p^{n-1}$ roots.

Now choose a direction $v \in \mathbb{F}_p^n \backslash \{0\}$ and let $u \in \mathbb{F}_p^n$ be such that $u + tv \in A$ for all $t \in \mathbb{F}_p$. Then $f(u + tv)$ is a polynomial in t with degree k, and the leading term of $f(u + tv)$ is $p_k(v)t^k$. However by definition, $f(u + tv) = 0$ for all $t \in \mathbb{F}_p$ so this polynomial is identically 0, which implies that $p_k(v) = 0$. Since there are $p^n - 1$ possible directions, we conclude that p_k has at least $p^n - 1$ roots, a contradiction for $n \ge 2$. □

1.6 Restricted pairwise distances

Consider the following warm-up problem: suppose we have $P \subseteq \mathbb{R}^n$ such that all (Euclidean) distances between pairs of points in P are the same. What is the maximum possible size of P? It is not hard to see that the answer is $n+1$, and the extremal configuration is given by the vertices of a simplex.

For any metric on $\mathbb{R}^n$, we call a set P an *equidistant set* if all distances between distinct points in P are the same. If instead of the Euclidean metric ℓ_2, we ask the above question using the ℓ_∞ metric, then a maximum equidistant set has size 2^n (for the lower bound, consider $\{0,1\}^n$). Moreover, this actually holds for any norm-induced metric in $\mathbb{R}^n$.

What about if we use the ℓ_1 metric, meaning that the distance between $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is $\sum_{i=1}^n |x_i - y_i|$? Then the set $\{\pm e_i : 1 \le i \le n\}$ of $2n$ vectors is equidistant. This is conjectured to be best possible.

Conjecture 1.17 (Kusner, 1983)**.** *The maximum size of an equidistant set in $\mathbb{R}^n$ with the ℓ_1-distance, is $2n$.*

Remark 1.18. The best known upper bound is $O(n \log n)$ (Alon–Pudlák, 2003).

Now, going back to the Euclidean ℓ_2 metric, what if we allow the pairwise distances to take two different values (say δ_1 and δ_2)? It is possible to construct such a set with $\binom{n+1}{2}$ points, as follows.

Example 1.19. Take the vectors in $\{0,1\}^{n+1}$ with exactly 2 ones. Each pairwise distance could be 2 (if the 1s are disjoint) or $\sqrt{2}$ otherwise. Note that each of these points lie on the n-dimensional hyperplane $\sum x_i = 2$, so we can embed this point set isometrically in $\mathbb{R}^n$.

Now, we prove the following upper bound.

Claim 1.20 (Larman–Rogers–Seidel, 1977)**.** *Let P be a set of points in $\mathbb{R}^n$ such that $|x-y| \in \{\delta_1, \delta_2\}$ for all $x \ne y \in P$. Then $|P| \le \frac{(n+1)(n+4)}{2}$.*

Proof. Suppose $P = \{p_1, \ldots, p_m\}$, and consider the polynomials

$$f_j(x_1, \ldots, x_n) = \Big(|x - p_j|^2 - \delta_1^2\Big)\Big(|x - p_j|^2 - \delta_2^2\Big).$$

Note that $f_j(p_j) = \delta_1^2\delta_2^2 \ne 0$, and $f_j(p_k) = 0$ for $j \ne k$. It follows that $\{f_1, \ldots, f_m\}$ are independent as vectors. Indeed, if $\sum_{j=1}^n \alpha_j f_j \equiv 0$, then evaluating this polynomial at p_j gives $\alpha_j f_j(p_j) = 0$, which implies $\alpha_j = 0$.

Therefore it will be enough to show that $f_1, \ldots, f_m$ live in a $(n+1)(n+4)/2$-dimensional vector space. Note that $|x-b|^2 = \sum_{i=1}^n x_i^2 - 2\sum_{i=1}^n x_i b_i + \sum_{i=1}^n b_i^2$ so each f_j is spanned by the polynomials of the form

$$\left(\sum_{i=1}^n x_i^2\right)^2,\ x_k \sum_{i=1}^n x_i^2,\ x_i x_j,\ x_i^2,\ x_i,\ 1,$$

where $1 \le i, j \le n$. The dimension of this space of polynomials is therefore at most $1 + n + \binom{n}{2} + n + n + 1 = \frac{(n+1)(n+4)}{2}$. □

We make a few further remarks:

1. An idea for improving the bound is to find other polynomials in the spanned space that are linearly independent of each f_j. Using this, one can obtain the best known upper bound $\frac{(n+1)(n+2)}{2}$ (Blokhuis, 1984). The exact answer, however, isn't known.

2. The same proof works for sets of points with k distinct distances.

3. If δ_1 is far from δ_2, one can get an upper bound that is linear in n.

1.7 Fisher inequalities (set systems with restricted intersections)

Recall the Eventown/Oddtown problem from Section 1.2, where we were imposing restrictions on the sizes of intersections. The following theorem is in a similar spirit.

Theorem 1.21 (Fisher 1940, Bose 1949, Majumdar 1953)**.** *Let $\mathcal{F} = \{F_1, \ldots, F_m\} \subseteq 2^{[n]}$ be a family of non-empty sets, such that $|F_i \cap F_j| = \lambda$, for each $i \neq j$. Then $m \leq n$.*

The following examples show that, as in Section 1.2, there are many, very different, classes of extremal examples.

Example 1.22. The following Fisher families all have size n.

- With $\lambda = 0$, we can take singleton sets: $\mathcal{F} = \{\{1\}, \{2\}, \ldots, \{n\}\}$.
- With $\lambda = 1$ we can take rays through a single point: $\mathcal{F} = \{\{1,2\}, \{1,3\}, \ldots, \{1,n\}, \{2,\ldots,n\}\}$.
- If n is of the form p^2+p+1 for prime p, we can take $\lambda = 1$ and consider the set system arising from the projective plane over $\mathbb{F}_p$, as in Section 1.3.
- With $\lambda = n-2$ we can take complements of singletons: $\mathcal{F} = \{[n] \setminus \{i\} : i = 1\ldots, n\}$.
- To each $(k-1)$-dimensional subspace of $\mathbb{F}_p^k$, assign the set of all 1-dimensional subspaces it contains. In this case, $n = \frac{p^k-1}{p-1}$ and $\lambda = \frac{p^{k-2}-1}{p-1}$.

We could prove Theorem 1.21 with polynomials as in the last section, but for variety let's give a different proof. We'll need the following definition.

Definition 1.23. *The incidence matrix* of a set family $\mathcal{F} = \{F_1, \ldots, F_m\}$ is the matrix in which the i-th row is the characteristic vector of F_i.

Proof of Theorem 1.21. First consider the case when there is a set of size λ in the family (say $|F_1| = \lambda$). Then $\lambda \geq 1$ since the sets are non-empty, and by the intersection size property of a Fisher family, $F_1 \subset F_i$ for all i. So, each $F_i \backslash F_1$, for $i \geq 2$, need to be disjoint. In particular there are at most $n - \lambda$ such sets, showing $m \leq n - \lambda + 1 \leq n$.

It now suffices to consider the case where each $|F_i| > \lambda$. Let A be the incidence matrix of $\mathcal{F}$. Then

$$B = AA^\intercal = \begin{pmatrix} |F_1 \cap F_1| & |F_1 \cap F_2| & \dots & |F_1 \cap F_m| \\ |F_2 \cap F_1| & |F_2 \cap F_2| & \ddots & \vdots \\ \vdots & \ddots & \ddots & |F_{m-1} \cap F_m| \\ |F_m \cap F_1| & \dots & |F_m \cap F_{m-1}| & |F_m \cap F_m| \end{pmatrix} = \begin{pmatrix} |F_1| & \lambda & \dots & \lambda \\ \lambda & |F_2| & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \dots & \lambda & |F_m| \end{pmatrix}.$$

We will show this matrix has full rank. To do so it is enough to show $\det B \neq 0$. Indeed,

$$\det B = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & |F_1| & \lambda & \dots & \lambda \\ 0 & \lambda & |F_2| & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & \lambda \\ 0 & \lambda & \dots & \lambda & |F_m| \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ -\lambda & |F_1| - \lambda & 0 & \dots & 0 \\ -\lambda & 0 & |F_2| - \lambda & \ddots & \vdots \\ -\lambda & \vdots & \ddots & \ddots & 0 \\ -\lambda & 0 & \dots & 0 & |F_m| - \lambda \end{pmatrix} =$$

$$\det \begin{pmatrix} 1 + \sum_{i=1}^m \frac{\lambda}{|F_i| - \lambda} & 1 & 1 & \dots & 1 \\ 0 & |F_1| - \lambda & 0 & \dots & 0 \\ 0 & 0 & |F_2| - \lambda & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & |F_m| - \lambda \end{pmatrix} = \left(1 + \sum_{i=1}^m \frac{\lambda}{|F_i| - \lambda}\right) \prod_{i=1}^m (|F_i| - \lambda) > 0,$$

where the second equality follows by deducting λ times the first row from all other rows and the third equality follows by adding $\frac{\lambda}{|F_i| - \lambda}$ times the i-th column to the first column for each $i \geq 2$.

We have shown that B has full rank so $m = \operatorname{rank} AA^\intercal \leq \operatorname{rank} A \leq n$ (note that $\operatorname{rank} XY \leq \operatorname{rank} X$). □

1.8 Hypergraph Turán theory

How many edges can a graph on n vertices have and not contain an $(r+1)$-clique K_{r+1}? The answer is $(1 - 1/r + o(1))n^2/2$, attained by a complete multipartite graph with r parts. This famous theorem was proved by Turán, and is a generalisation of Theorem 1.1 from the introductory chapter.

A natural generalisation of a graph is a *hypergraph*, where the edges may consist of more than two vertices. A *k-uniform* hypergraph is a hypergraph where each edge has exactly k vertices. Generalising Turan's theorem to hypergraphs is very challenging, and an important direction of research in modern combinatorics. One particular success in this area involves 4-uniform hypergraphs, where one forbids a certain 4-uniform hypergraph H_r related to K_r. Specifically, H_r has vertices $[2r]$ with hyperedges $\{2i-1, 2i, 2j-1, 2j\}$ for all $i < j$.

It is known that if we forbid H_{r+1} we have at most $((r-1)/r + o(1))\binom{n}{4}$ edges, and that this is tight if and only if r is a power of 2. It turns out that justifying this fact boils down to proving the following theorem, for which we need the following definition.

Definition 1.24. Given a proper edge-colouring of K_n in $n-1$ colours, it is *consistent* if for any 4 vertices inducing a copy of K_4, either all edges have distinct colours or all 3 perfect matchings are monochromatic.

Remark 1.25. Note that in any proper edge-colouring of K_n in $n-1$ colours, every colour class induces a perfect matching.

Theorem 1.26 (Keevash-Sudakov). *A consistent colouring of K_n exists if and only if n is a power of 2.*

Proof. Suppose such a colouring c exists, with colours $c_1, \ldots, c_{n-1}$. Then we can define addition on colours by $c_1+c_2 = c_3$ if and only if there are vertices u, w, v with $c(uw) = c_1$, $c(uv) = c_2$ and $c(wv) = c_3$. To see that this is well-defined, suppose we have two triangles (u, w, v), (u', w', v') demonstrating two potentially different values of $c_1 + c_2$. But then consider the clique on $(u, u', w, w,')$. Since $c(uw) = c(u'w')$, by consistency $c(ww') = c(uu')$. Similarly $c(vv') = c(uu')$. But then consistency on the 4-clique (w, v, w', v') shows that $c(wv) = c(w'v')$ so $c_1 + c_2$ is well-defined. See Figure 1.1 for an illustration. Also, let us introduce an auxiliary element c_0 and define $c_i + c_i = c_0$ and $c_i + c_0 = c_i$. Note that by definition + is commutative.

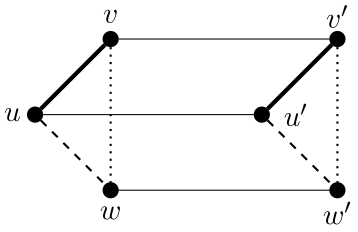


Figure 1.1: Here, c_1 is dashed, c_2 is thick, c_3 is dotted and $c(vv') = c(ww') = c(uu')$ is thin.

Now we will prove that addition is associative; in particular we claim that $(c_i+c_j)+c_k = c_i+(c_j+c_k)$ for all $i, j, k \geq 0$. If any of i, j or k are 0 the claim holds trivially. If $i = j$, $(c_i+c_i)+c_k = (c_0)+c_k = c_k$. Let u, w, v be such that $c(uw) = c_i$, $c(uv) = c_k$ and $c(wv) = c_i + c_k$; from the perspective of w we have $c_i + (c_i + c_k) = c_k$ as desired. By commutativity the claim also follows when $j = k$. If $i = k$ the claim follows directly from commutativity. Now the remaining case is $i \neq j, j \neq k, i \neq k,$. Let u, w, v be such that $c(uw) = c_i$ and $c(uv) = c_j$. If $c_i + c_j = c_k$ then considering the edges of u, v, w gives $c_j + c_k = c_i$ and both sides of the equality are c_0. Otherwise if $c_i + c_j \neq c_k$, let r be such that $c(vr) = c_k$. Now $(c_i + c_j) + c_k = c(wv) + c(vr) = c(wr) = c(uw) + c(ur) = c_i + (c_j + c_k)$, completing the proof of the claim.

We have shown that $\{c_0, \ldots, c_{n-1}\}$ is a vector space over $\mathbb{F}_2$. But that means $|\{c_0, c_1, \ldots, c_{n-1}\}|$ is a power of 2.

In the other direction, we can use $\mathbb{F}_2^t$ to give an explicit consistent colouring. Indeed, identify the vertices with elements of $\mathbb{F}_2^t$ and for two vectors u, v, colour the edge between them in colour $u + v \in \mathbb{F}_2^t \setminus \{0\}$. It is easy to verify this produces a consistent colouring. □

1.9 The joints problem

Definition 1.27. A point in $\mathbb{R}^3$ is said to be a *joint* if it is an intersection of 3 non-coplanar lines.

Question 1.28. *How many joints can n lines define?*

Remark 1.29. The reason we require non-planarity is because there can be $\Omega(n^2)$ 3-fold intersections of n lines in a plane (consider a planar grid with diagonals), which is not much smaller than the total number of intersections.

A natural example to consider might be a grid.

Example 1.30. Consider the cubic grid $[t]^3$, and the set of all lines parallel to the coordinate axes passing through points of the grid. The number of joints is t^3, as any point of the grid is a joint, and there are $3t^2$ lines.

The following theorem shows that this is best possible up to a constant factor.

Theorem 1.31 (Guth–Katz, 2008)**.** *Given n lines $\ell_1, \dots, \ell_n$ in $\mathbb{R}^3$, there are at most $(3n)^{3/2}$ joints defined by these lines.*

The main ingredient in the proof is the following lemma.

Lemma 1.32. *If $\ell_1, \dots, \ell_n$ are lines in $\mathbb{R}^3$ having J joints then there is a line ℓ_i with at most $3J^{1/3}$ joints.*

Before proving Lemma 1.32 we explain how to deduce Theorem 1.31. Given ℓ_i as guaranteed by Lemma 1.32, we can delete it and destroy at most $3J^{1/3}$ joints. Iterating, after n deletions there are 0 lines and 0 joints, so $J \le n(3J^{1/3})$ and $J \le 3^{3/2}n^{3/2}$, proving Theorem 1.31.

Proof of Lemma 1.32. Suppose for the purpose of contradiction that the desired conclusion is false, so every line ℓ_i has more than $3J^{1/3}$ joints. We will use similar reasoning as for the finite field Kakeya problem.

By Lemma 1.15, the number of monomials $x^a y^b z^c$ such that $a+b+c \le d$ equals $\binom{d+3}{3}$. If $d = 3J^{1/3}$ then $\binom{d+2}{3} > J$ so the number of such monomials is greater than number of joints. This implies that there is a non-zero polynomial $P(x, y, z)$ of degree at most $3J^{1/3}$ which is zero on all joints. Indeed, consider the system of equations of the form

$$\sum_{(a,b,c):a+b+c\le d} \alpha_{a,b,c} x^a y^b z^c = 0$$

in the unknowns $\alpha_{a,b,c}$, where (x, y, z) ranges over all joints. This system of equations has a non-trivial solution: the number of variables (being the number of monomials we just enumerated) is greater than number of equations (being the number of joints). Consider a suitable polynomial P with minimum possible degree, and without loss of generality assume it is non-trivial in x (meaning that $\alpha_{a,b,c} \ne 0$ for some $a > 0$).

For any point $u \in \mathbb{R}^3$ which is a joint, there exist 3 non-coplanar lines $\ell_{k_1}, \ell_{k_2}, \ell_{k_3}$ passing through u with directions w_1, w_2, w_3. For any $i \in \{1, 2, 3\}$, $P(u + tw_i)$ is a one-variable polynomial in t with degree at most $3J^{1/3}$. This polynomial takes the value zero on all joints on ℓ_{k_i}. By assumption, the number of joints is greater than $3J^{1/3}$, so in fact this polynomial is identically zero: $P(u+tw_i)=0$ for all $t \in \mathbb{R}$.

We now consider directional derivatives. Let $D(u,w) = \frac{dP(u+tw)}{dt}\Big|_{t=0}$ be the derivative of P in direction w at the point u. Then $P(u+tw_i)$ being identically zero implies that $D(u,w_i)=0$. Since the lines were non-coplanar, w_1, w_2, w_3 form a basis in $\mathbb{R}^3$, meaning that there exist $c_1, c_2, c_3 \in \mathbb{R}$ such that $c_1w_1+c_2w_2+c_3w_3=e_1$. Thus we conclude

$$\frac{dP}{dx}(u) = D(u,e_1) = c_1D(u,w_1)+c_2D(u,w_2)+c_3D(u,w_3) = 0.$$

We have proved that $\frac{dP}{dx}$ is a polynomial of smaller degree than P which still takes the value zero on all joints. (Because we assumed P was assumed non-trivial in x, $\frac{dP}{dx}$ is nonzero). This is a contradiction. □

1.10 More on set systems with restricted intersections

Definition 1.33. Let $\mathcal{F} \subseteq 2^{[n]}$ be a finite system of sets, and consider some set of integers $L = \{\ell_1, \ldots, \ell_s\}$. We say $\mathcal{F}$ is *L-intersecting* iff $|F \cap F'| \in L$ for all $F \neq F' \in \mathcal{F}$. We say $\mathcal{F}$ is *L-mod p-intersecting* if $|F| \notin L \pmod p$ but $|F \cap F'| \in L \pmod p$ for all $F \neq F' \in \mathcal{F}$.

The main question of interest regarding L-intersecting and L-mod p-intersecting families is the following.

Question 1.34. *Given s and n, how large can $|\mathcal{F}|$ be?*

We next give two important examples of large L-intersecting and L-mod p-intersecting families.

Example 1.35. We can take $L = \{0, \ldots, s-1\}$, and let $\mathcal{F}$ be the family of all sets with s or fewer elements, giving an L-intersecting family with $|\mathcal{F}| = \sum_{i=0}^{s} \binom{n}{i}$.

Example 1.36. We can take $L = \{0, \ldots, s-1\}$, and let $\mathcal{F}$ be the family of all sets with exactly s elements, giving an L-mod p-intersecting family with $|\mathcal{F}| = \binom{n}{s}$, provided that $s < p$.

Now we prove some upper bounds. The proofs which we present are mostly due to Alon, Babai and Suzuki.

Theorem 1.37 (Frankl–Wilson, 1981)**.** *Let $\mathcal{F} \subseteq 2^{[n]}$ be an L-mod p-intersecting family for some prime p with $|L| = s$. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Proof. Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ and $L = \{\ell_1, \ldots, \ell_s\}$. Let v_i be the characteristic vector of F_i and define $f_i : \mathbb{F}_p^n \to \mathbb{F}_p$ by $f_i(x) = \prod_{j=1}^{s}(x \cdot v_i - \ell_j)$. Since $v_i \cdot v_j = |F_i \cap F_j|$, we obtain that $f_i(v_i) \neq 0$ and $f_i(v_j) = 0$ for all $j \neq i$. Thus $f_1, \ldots, f_m$ are linearly independent over $\mathbb{F}_p$. Indeed, if $\sum_{i=1}^{m} \alpha_i f_i = 0$ then evaluating both sides at v_i gives $\alpha_i f_i(v_i) = 0$, which implies $\alpha_i = 0$.

Thinking of f_i as a polynomial in the variables $x_1, \ldots, x_n$, let g_i be the polynomial obtained from f_i by replacing each instance of x_q^a by x_q, for $1 \leq q \leq n$ and $a \geq 1$. Observe that since $0^a = 0$ and

$1^a = 1$ for all $a \geq 1$ and each $v_k \in \{0,1\}^n$, we have $f_i(v_k) = g_i(v_k)$ for all i, k. Thus by the same reasoning as above, we may conclude that $g_1, \ldots, g_m$ are linearly independent over $\mathbb{F}_p$.

Moreover, we observe that $g_1, \ldots, g_m$ are multilinear polynomials in n variables such that each monomial has at most s variables. The number of such monomials is $\sum_{i=0}^{s} \binom{n}{i}$ and hence $g_1, \ldots, g_m$ live in a space of dimension $\sum_{i=0}^{s} \binom{n}{i}$. □

Theorem 1.38 (Frankl-Wilson, 1981). *Let $\mathcal{F} \subseteq 2^{[n]}$ be an L-intersecting family with $|L| = s$. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Proof. The proof is almost the same as that of Theorem 1.37, but we have to deal with the issue that there may exist $F \in \mathcal{F}$ with $|F| \in L$.

Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ with $|F_1| \leq \ldots \leq |F_m|$ and let $L = \{\ell_1, \ldots, \ell_s\}$. Let v_i be the characteristic vector of F_i and define $f_i : \mathbb{R}^n \to \mathbb{R}$ by $f_i(x) = \prod_{j : \ell_j < |F_i|} (x \cdot v_i - \ell_j)$. Then we observe that $f_i(v_i) \neq 0$ and $f_i(v_k) = 0$ if $k < i$. This is actually sufficient to show that $f_1, \ldots, f_m$ are linearly independent (over $\mathbb{R}$). Indeed, suppose that $\sum_{i=1}^{m} \alpha_i f_i = 0$. If not all α_i are 0, then choose a minimal i_0 such that $\alpha_{i_0} \neq 0$ and $\alpha_i = 0$ for all $i < i_0$. Evaluating the previous expression at v_{i_0}, we obtain

$$0 = \alpha_{i_0} f_{i_0}(v_{i_0}) + \sum_{i > i_0} \alpha_i f_i(v_{i_0}) = \alpha_{i_0} f_{i_0}(v_{i_0}),$$

which implies $\alpha_{i_0} = 0$, a contradiction.

Again as in the proof of Theorem 1.37, we may obtain polynomials g_i from f_i by replacing each instance of x_q^a by x_q. We have $g_i(v_k) = f_i(v_k)$, so we again have that $g_1, \ldots, g_m$ are linearly independent multilinear polynomials of degree at most s and the space of such polynomials has dimension $\sum_{i=0}^{s} \binom{n}{i}$. This completes the proof. □

Theorem 1.39 (Ray-Chaudhuri-Wilson, 1975). *Let $\mathcal{F} \subseteq 2^{[n]}$ be an L-intersecting family with $|L| = s$ such that $|F| = k$ for all $F \in \mathcal{F}$. Provided every element of L is smaller than k we get $|\mathcal{F}| \leq \binom{n}{s}$.*

Proof. Note that the intersection of two different sets of size k has size in $\{0, 1, \ldots, k-1\}$, so the assumption that every element of L is smaller than k is in a certain sense vacuous, but we require it only because the function $\binom{n}{s}$ is not increasing in s. This assumption gives us that $s \leq k$ and that $k \notin L$. Thus we can avoid the issue that we had in the proof of Theorem 1.38 and proceed in the same way as the proof of Theorem 1.37.

Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ and $L = \{\ell_1, \ldots, \ell_s\}$. Let v_i be the characteristic vector of F_i and define $f_i : \mathbb{R}^n \to \mathbb{R}$ by $f_i(x) = \prod_{j=1}^{s} (x \cdot v_i - \ell_j)$. Then we have $f_i(v_i) \neq 0$ and $f_i(v_k) = 0$ for all $k \neq i$. As before, we can obtain polynomials g_i such that $g_i(v_k) = f_i(v_k)$ for all i, k, by taking the f_i and replacing each instance of x_q^a by x_q.

The new idea will be to use the fact that all sets are of size k in order to add an additional $\sum_{i=0}^{s-1} \binom{n}{i}$ independent multilinear polynomials that are also independent of $g_1, \ldots, g_m$. To this end, for $I \subseteq [n]$ with $|I| < s \leq k$, define $h_I(x) = (x_1 + \cdots + x_n - k) \prod_{i \in I} x_i$. Then $h_I(v_i) = 0$ for all i.

We claim that the polynomials in $\{g_1, \dots, g_m\} \cup \{h_I : |I| < s\}$ are linearly independent. Indeed, suppose that

$$\sum_{i=1}^{m} \alpha_i g_i + \sum_{|I|<s} \beta_I h_I = 0.$$

Then evaluating at v_i gives $\alpha_i g_i(v_i) = 0$, which implies $\alpha_i = 0$. Hence we obtain $\sum_{|I|<s} \beta_I h_I = 0$. Let x_J be the characteristic vector of J and note that $h_I(x_J) = 0$ whenever $I \not\subseteq J$. In particular, $h_I(x_J) = 0$ when $|I| \geq |J|$ and $I \neq J$. Thus, if we suppose for sake of contradiction that not all β_I are zero, and choose J with $|J|$ minimal such that $\beta_J \neq 0$, then evaluating the sum at x_J gives

$$0 = \sum_{|I|<s} \beta_I h_I(x_J) = \beta_J h_J(x_J) + \sum_{|I| \geq |J|, I \neq J} \beta_I h_I(x_J) = \beta_J h_J(x_J).$$

Since $s - 1 < k$, we have that $h_J(x_J) = |J| - k < 0$ and hence $\beta_J = 0$, a contradiction.

Since the space of multilinear polynomials of degree at most s has dimension $\sum_{i=0}^{s} \binom{n}{i}$ and we have shown that $\{g_1, \dots, g_m\} \cup \{h_I : |I| < s\}$ is a collection of $m + \sum_{i=0}^{s-1} \binom{n}{i}$ independent polynomials living in this space, we conclude that $m \leq \sum_{i=0}^{s} \binom{n}{i} - \sum_{i=0}^{s-1} \binom{n}{i} = \binom{n}{s}$. □

The following mod-p analogue of Theorem 1.39 also holds.

Theorem 1.40 (Alon-Babai-Suzuki, 1991)**.** *For any prime p, let $\mathcal{F} \subseteq 2^{[n]}$ be an L-mod p-intersecting family with $|L| = s$ such that $|F| = k \pmod p$ for all $F \in \mathcal{F}$, $k \notin L \pmod p$, $s \leq p-1$ and $s+k \leq n$. Then $|\mathcal{F}| \leq \binom{n}{s}$.*

We remark that the proof of Theorem 1.40 is the same as that of Theorem 1.39, but to show that $h_I : |I| < s$ are linearly independent requires the Möbius inversion formula, which will not be covered in this course.

1.11 Explicit constructions of Ramsey graphs

Definition 1.41. We define the *Ramsey number* $R(s,t)$ to be the minimum N such that every red-blue edge-colouring of K_N has either a red K_s or a blue K_t.

It is an important and surprisingly difficult problem to determine the approximate asymptotic behaviour of the *diagonal* Ramsey numbers $R(n,n)$. The following bounds are classical, but in the last 50 years have seen only incremental improvements.

Claim 1.42. $2^{t/2} \leq R(t,t) \leq 2^{2t}$ *for* $t \geq 2$.

Proof. For the upper bound, we show by induction on $s+t$ that $R(s,t) \leq 2^{s+t}$. The base case is trivial. Now consider a red-blue edge-colouring of $K_{2^{s+t}}$ for some s,t. Fix any vertex v and consider the red neighbours R and blue neighbours B of v. One of R, B will have size at least 2^{s+t-1}, say R. By induction, we know that R has either a blue K_t, in which case we are done, or a red K_{s-1}, in which case adding v to it gives a red K_s, so we are done.

For the lower bound we will use the probabilistic method. Let $N = 2^{t/2}$ and consider a random edge-colouring of K_N were each edge is coloured red or blue independently with probability $1/2$. Then the probability that a given set of t vertices forms a red K_t or a blue K_t is exactly $2(1/2)^{\binom{t}{2}}$, and there are $\binom{N}{t}$ such sets. We conclude that the probability that some set of t vertices forms a red or a blue K_t is at most

$$\binom{N}{t} 2 \left(\frac{1}{2}\right)^{\binom{t}{2}} \leq \frac{N^t}{t!} 2^{-t^2/2+t/2+1} = \frac{2^{t/2+1}}{t!} \to 0.$$

Since this probability is less than 1 for $t \geq 3$, we know there exists a colouring of K_N with no red K_t and no blue K_t. □

The above lower bound is non-constructive. It is a major open problem to construct explicit examples of large graphs with no K_t or $\overline{K_t}$. One may consider the following natural example, which falls far short of the probabilistic lower bound above. (Reformulating, note that the above lower bound says that there is a graph G on N vertices with $\alpha(G), \omega(G) \leq c \log N$,where $\alpha(G)$ and $\omega(G)$ are the largest independent set and largest clique of G respectively).

Example 1.43. The graph G consisting of the disjoint union of $t-1$ copies of K_{t-1} has $N = (t-1)^2$ vertices, and has $\alpha(G), \omega(G) \leq c\sqrt{N}$.

The following example does a bit better but still falls well short of the probabilistic bound.

Example 1.44 (Nagy 1973)**.** Let G be the graph whose vertices are the $N = \binom{t}{3}$ subsets of $[t]$ of size 3, and with an edge between X and Y if $|X \cap Y|$ is even. A maximal clique is a family $\{A_1, \ldots, A_\omega\}$ with $|A_i|$ odd and $|A_i \cap A_j|$ even, for $i \neq j$. So $\omega(G) \leq t \approx N^{1/3}$. An independent set has $|A_i \cap A_j| = 1$ for all $i \neq j$, so by Fisher's inequality $\alpha(G) \leq t \approx N^{1/3}$ as well.

The following example gives a major improvement over the above construction, but is based on the same underlying idea.

Example 1.45 (Frankl-Wilson, 1981)**.** Consider a prime p and define the graph G as follows. The vertices of G are the $N = \binom{p^3}{p^2-1}$ subsets of $\left[p^3\right]$ of size $p^2 - 1$, and we put an edge between subsets X and Y if and only if $|X \cap Y| \equiv -1 \pmod{p}$.

Let $L = \{0, \ldots, p-2\}$. For any independent set I, observe that $|X| = p^2 - 1 \equiv -1 \pmod{p}$ (that is, $|X| \notin L \pmod{p}$) for all $X \in I$, and $|X \cap Y| \in L \pmod{p}$ for all $X \neq Y \in I$. By Theorem 1.40, it follows that $\alpha(G) \leq \binom{p^3}{p-1}$. For any clique C and any $X \neq Y \in C$, we have $|X| = p^2 - 1$ so $|X \cap Y| < |X| = p^2 - 1$. Moreover, $|X \cap Y| \equiv -1 \pmod{p}$ and hence $|X \cap Y| \in \{p-1, 2p-1, \ldots, (p-1)p-1\}$. Thus by Theorem 1.39, $\omega(G) \leq \binom{p^3}{p-1}$.

Now, observe that $N = \binom{p^3}{p^2-1} \approx \left(\frac{p^3}{p^2}\right)^{p^2} = 2^{p^2 \log p}$. This means $\log N \approx p^2 \log p$ and hence $p \approx \sqrt{\log N / \log \log N}$, and we have

$$\alpha(G), \omega(G) \leq \binom{p^3}{p-1} \approx \left(\frac{p^3}{p}\right)^p = 2^{2p \log p} \approx 2^{\sqrt{\log N \log \log N}}.$$

The parameter p^3 was chosen to obtain this optimal result.

We remark that in both of the above examples we used both the modular and non-modular version of the Frankl–Wilson Theorem.

The above example was the best known explicit construction of a Ramsey graph until some recent work by the theoretical computer science community. The current state of the art is due to Cohen who constructed an N vertex graph G with $\alpha(G), \omega(G) \leq (\log N)^{(\log\log\log N)^c}$ for some constant c.

We finish this section with a few other approaches towards constructions of Ramsey graphs. The next example is quite simple and gives a comparable bound to the Frankl–Wilson construction. The construction itself involves randomness, but unlike in the naive approach at the start of this section, we can efficiently verify that our randomly constructed Ramsey graph indeed has no large cliques or independent sets.

To present this construction we need a simple fact about lexicographic products of graphs.

Definition 1.46. The *lexicographic product* $G_1 \times G_2$ of G_1 and G_2 has vertex set $V_1 \times V_2$ and $(u, v) \sim (u', v')$ if $u \sim u'$ in G_1 or $u = u'$ and $v \sim v'$ in G_2. Note $\times$ is associative so G^k is well-defined.

Proposition 1.47.

$$\omega(G_1 \times G_2) = \omega(G_1)\omega(G_2)$$

$$\alpha(G_1 \times G_2) = \alpha(G_1)\alpha(G_2)$$

Proof. Left as an exercise. □

Now we present the promised Ramsey construction.

Example 1.48. Let N be a parameter, which will be the size of our final graph. Let $n = 2^{\frac{1}{2}\sqrt{\log N}}$, and take a random graph G on n vertices such that every edge appears independently with probability $\frac{1}{2}$. With probability very close to 1 this G has both $\alpha(G), \omega(G) \leq \sqrt{\log N}$. Importantly, we can verify that indeed $\alpha(G), \omega(G) \leq \sqrt{\log N}$ in time $\binom{n}{\sqrt{\log N}} \leq n^{\sqrt{\log N}} = 2^{\frac{1}{2}\log N} = \sqrt{N}$, so this gives an explicit way of generating such a G. Now let's take a product G^k of G with itself $k = 2\sqrt{\log N}$ times. The number of vertices of G^k is $n^k = \left(2^{\frac{1}{2}\sqrt{\log N}}\right)^{2\sqrt{\log N}} = N$, while $\alpha(G^k), \omega(G^k) \leq (\sqrt{\log N})^{2\sqrt{\log N}} = 2^{\sqrt{\log N}\log\log N}$.

Finally, it is worth mentioning the *Paley graph* (otherwise known as the quadratic residue graph), defined as follows.

Example 1.49. Let p be a prime with $p \equiv 1 \pmod 4$. Consider a graph with vertices $\{0, 1, \ldots, p-1\}$ and put an edge between x and y if there exists z such that $x - y = z^2 \pmod p$. This graph is regular with degree $\frac{p-1}{2}$ and in several different senses it is "pseudo-random", which means it resembles the random graph where each edge occurs with probability 1/2. It is conjectured that this graph has very small α, ω, but a proof of this is, unfortunately, still out of reach of current ideas in number theory.

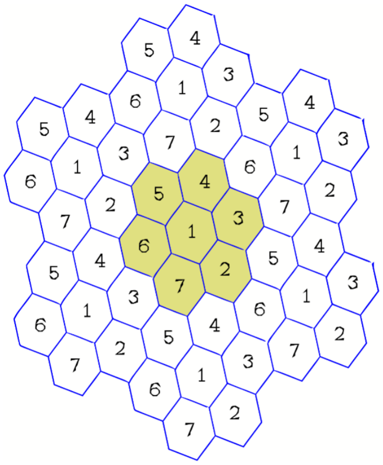
1.12 Chromatic number of $\mathbb{R}^n$

Consider the following infinite graph. The vertex set is $\mathbb{R}^n$, and we put an edge between x and y if and only if $d(x, y) = 1$ (where $d(x, y)$ is the Euclidean distance between x and y). It is an important open problem to determine $\chi(\mathbb{R}^n)$. We remark that only the case $n \geq 2$ is interesting, because $\chi(\mathbb{R}^1) = 2$, as can be seen with the colouring c given by $c(x) =$ parity of $\lfloor x \rfloor$.

Claim 1.50. $4 \leq \chi(\mathbb{R}^2) \leq 7$.

Proof. For the lower bound, suppose for the purpose of contradiction that 3 colours are enough. Note that any equilateral triangle with side length 1 has a different colour on each vertex so if we glue two equilateral triangles into a rhombus, the far vertices have the same colour. As we can place the above picture anywhere in the plane, any two points with $d(x, y) = \sqrt{3}$ have the same colour. Thus, if we consider a circle with radius $\sqrt{3}$, all vertices on the circle need to have the same colour as the center. However, if we consider two points on such a circle at a distance of 1, we get a contradiction.

For the upper bound, we exhibit a 7-colouring. Consider a regular hexagon with side length 1/2. Since the diameter is 1, we can colour all points in its interior and the bottom half of its boundary with the same colour. Now consider a big hexagon made from 7 smaller hexagons of side length 1/2, and colour each a different colour. Tiling the plane periodically with these big hexagons gives a desired 7 colouring, as depicted.



□

We remark that instead of considering the infinite graph on the vertex set $\mathbb{R}^n$, it suffices to work with induced subgraphs on arbitrarily large finite sets of $\mathbb{R}^n$. It is possible to use a compactness argument to show that in general, to bound the chromatic number of an infinite graph, it suffices to bound the chromatic number of all its finite subgraphs. We remark that this argument uses the axiom of choice, through Tychonoff's theorem!

The hexagon example above is only valid in $\mathbb{R}^2$, but in general we can use a similar idea to tile $\mathbb{R}^n$ with a hypercube split into smaller hypercubes, giving rise to the following claim.

Claim 1.51. $\chi(\mathbb{R}^n) \leq (\sqrt{n} + 2)^n$.

Proof. Consider the $\frac{1}{\sqrt{n}} \times \cdots \times \frac{1}{\sqrt{n}}$ hypercube with diameter 1, i.e. $\left[0, \frac{1}{\sqrt{n}}\right)^n$. We can use one colour for the whole cube. Now tile a cube with side-length $(\lceil \sqrt{n} \rceil + 1) \cdot \frac{1}{\sqrt{n}}$ with such "small" cubes of side-length $\frac{1}{\sqrt{n}}$, and assign each of the small cubes a different color. Call this a "big cube". The number of small cubes is $(\lceil \sqrt{n} \rceil + 1)^n \leq (\sqrt{n} + 2)^n$. Now tile the space periodically with such big cubes. If two points are in different big cubes and receive the same color, then their distance is bigger than 1. So this gives a colouring of $\mathbb{R}^n$ with at most $(\sqrt{n} + 2)^n$ colours. □

In higher dimensions, there is actually a significantly better bound, which is only exponential in n.

Theorem 1.52 (Larman–Rogers, 1972)**.** *$\chi(\mathbb{R}^n) \leq 9^n$.*

Proof. The basic idea is to use balls instead of cubes. Let $C \subseteq \mathbb{R}^n$ be an inclusion-maximal subset of points in $\mathbb{R}^n$ such that for all $x, y \in C$, $d(x, y) \geq 1/2$. Then $\bigcup_{x \in C} B(x, 1/2) = \mathbb{R}^n$ by maximality, and also the balls $B(y, 1/4)$, for $y \in C$, are disjoint. The idea will be to assign a colour to elements of C and then colour $B(x, 1/2)$ with the colour of x.

To be precise, consider the graph H with vertex set C and an edge between x and y when $d(x, y) < 2$. Consider a proper colouring of H. We use this to obtain a proper colouring of $\mathbb{R}^n$ as follows. For each $x \in C$, colour $B(x, 1/2)$ with the colour of x. If this would result in assigning multiple colours to a single point of $\mathbb{R}^n$, we just choose one of the colours arbitrarily. It is easy to check that the resulting colouring of $\mathbb{R}^n$ is proper.

So, in order to prove the desired bound on $\chi(\mathbb{R}^n)$, it suffices to show that H can be properly coloured with 9^n colours. Let K be the maximum over $x \in C$ of the number of y in C with $d(x, y) < 2$, so that $K - 1$ is the maximum degree of H. Note that any graph with maximum degree $K - 1$ can be coloured with K colours greedily, so it suffices to bound K. Observe that if $d(x, y) < 2$ then $B(y, 1/4) \subseteq B(x, 9/4)$. Recall that the balls $B(y, 1/4)$, for $y \in C$, are disjoint, so K is bounded by the number of disjoint balls of radius 1/4 that we can fit within a ball of radius 9/4. It follows that $K \leq \frac{\mathrm{vol}(B(x,9/4))}{\mathrm{vol}(B(y,1/4))} \leq 9^n$. □

Our next goal is to give an exponential lower bound on $\chi(\mathbb{R}^n)$. For this, we will first prove the following theorem.

Theorem 1.53. *If $n = 4p$ with p prime, then there is a collection of $\frac{1}{2}\binom{n}{n/2}$ different ± 1 vectors of length n such that any subcollection of more than $\binom{n}{n/4-1}$ vectors contains a pair of orthogonal vectors.*

Proof. Consider all the ± 1 vectors of length n with exactly $2p$ "1"s and $2p$ "-1"s, such that the first coordinate is 1. The number of such vectors is $\frac{1}{2}\binom{n}{n/2}$.

Now, note that there is a correspondence between subsets of $[n]$ and ± 1 vectors in $\mathbb{R}^n$. Indeed, for any subset A of $[n]$ we define the corresponding ± 1 vector v_A by $(v_A)_i = 1$ if $i \in A$ and $(v_A)_i = -1$ if $i \notin A$. Then the set of vectors described above corresponds to the family $\mathcal{F} = \{A \subseteq [n] : 1 \in A, |A| = 2p\}$. Moreover, for any $A, B \in \mathcal{F}$

$$\begin{aligned} v_A \cdot v_B &= -(|A| - |A \cap B|) - (|B| - |A \cap B|) + |A \cap B| + n - |A \cup B| \\ &= 4|A \cap B| - 2(|A| + |B|) + n \\ &= 4|A \cap B| - n. \end{aligned}$$

This implies that $v_A \cdot v_B = 0$ if and only if $|A \cap B| = n/4 = p$.

Next, consider a subfamily $I \subseteq \mathcal{F}$ such that $v_A \cdot v_B \neq 0$ for all $A, B \in I$. Then for all $A \neq B \in I$, we have $|A| = |B| = 2p$ and $|A \cap B| \not\equiv 0 \pmod{p}$ (since $|A \cap B| \neq p$ and we cannot have $A \cap B = \emptyset$ because $1 \in A \cap B$). Hence $|A \cap B| \in \{1, \dots, p-1\} \pmod{p}$ and thus by Theorem 1.40 we have $|I| \leq \binom{n}{p-1}$. □

Now we can prove the promised exponential lower bound on $\chi(\mathbb{R}^n)$.

Theorem 1.54 (Frankl–Wilson, 1981)**.** $\chi(\mathbb{R}^n) \geq 1.2^n$.

Proof. For simplicity, we present a slightly weaker, yet still exponential lower bound. Let p be a prime, let $n = 4p$, and consider the $N = \frac{1}{2}\binom{4p}{2p}$ vectors given by Theorem 1.53. By scaling these vectors appropriately (by $1/\sqrt{2n}$), we have a collection of N vectors such that, for all u and v in the collection, we have $d(u, v) = 1$ if and only if $u \cdot v = 0$. Now, define the graph $G \subseteq \mathbb{R}^n$ to have these vectors as vertices, and to have an edge between a pair of vectors u, v if and only if they are at distance 1 (equivalently, having $u \cdot v = 0$). By construction, a maximum independent set in G has size $\alpha(G) \leq \binom{4p}{p-1}$.

Now, since a proper colouring of G partitions the vertices into independent sets, we have that

$$\chi(G) \geq \frac{N}{\alpha(G)} \geq \frac{\frac{1}{2}\binom{4p}{2p}}{\binom{4p}{p-1}} \approx \frac{2^n}{2^{H(1/4)n}} > 1.11^n,$$

where $H(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function. We have obtained an exponential lower bound when $n = 4p$ for some prime number p. In order to get the desired bound for all n, we use the fact for any $\varepsilon > 0$ and large enough N, there exists a prime number in $[N, (1+\varepsilon)N]$, combined with the simple observation that $\chi(\mathbb{R}^n)$ is non-decreasing in n. Hence, we obtain that $\chi(\mathbb{R}^n) > 1.1^n$ for all large enough n. □

Remark 1.55. The original bound of Frankl and Wilson can be obtained by more carefully tuning the parameters and a very similar construction due to Raigorodski yields the best known lower bound $\chi(\mathbb{R}^n) > (1.239\ldots + o(1))^n$.

1.13 Borsuk's conjecture

The following conjecture was made by Borsuk in 1932.

Conjecture 1.56 (Borsuk, 1932)**.** *Every set $S \subseteq \mathbb{R}^d$ of diameter 1 can be partitioned into $d+1$ sets, each having diameter strictly less than 1.*

To discuss Borsuk's conjecture, we also make the following definition.

Definition 1.57. Define $f(d)$ to be the minimum N such that we can partition any set $S \subseteq \mathbb{R}^d$ of diameter 1 into N parts, each having diameter less than 1.

Observe that the "$d+1$" cannot be improved, because if S contains the $d+1$ vertices of a regular simplex in $\mathbb{R}^d$, we must put each point of S in a different part.

Borsuk's conjecture is known to be true in the cases $d = 2, 3$, the case where S has a smooth boundary, and the case where S is centrally symmetric and convex. In general, only the substantially weaker bound $f(d) \leq (\sqrt{3/2})^d$ is known.

In 1993 it was proved by Kahn and Kalai that Borsuk's conjecture is actually in general false, in the following strong sense.

Theorem 1.58 (Kahn–Kalai, 1993)**.** *$f(d) \geq 1.2^{\sqrt{d}}$.*

Their idea was to start with a collection of vectors where it is hard to avoid an orthogonal pair and then transform that collection so that all angles are at most $\pi/2$ but orthogonality is preserved.

Definition 1.59. If $x = (x_1, \ldots, x_n)^\intercal$ and $y = (y_1, \ldots, y_m)^\intercal$, then the tensor product of x and y is defined to be

$$x \otimes y := xy^\intercal = \begin{pmatrix} x_1y_1 & \cdots & x_1y_m \\ \vdots & \ddots & \vdots \\ x_ny_1 & \cdots & x_ny_m \end{pmatrix} \in \mathbb{R}^{nm}.$$

Now observe that for any $n \times m$ matrices A, B, we have that $\operatorname{tr}(A^\intercal B) = \sum_{i=1}^n \sum_{j=1}^m A_{i,j}B_{i,j} = \langle A, B\rangle$, where $\langle A, B\rangle$ is the standard inner product between A and B if we regard them as vectors in $\mathbb{R}^{nm}$. Thus, a key property of the above definition is that

$$\langle x_1 \otimes y_1, x_2 \otimes y_2\rangle = \operatorname{tr}((x_1y_1^\intercal)^\intercal x_2y_2^\intercal) = \operatorname{tr}(y_1(x_1^\intercal x_2)y_2^\intercal) = (x_1^\intercal x_2)\operatorname{tr}(y_1y_2^\intercal) = \langle x_1, x_2\rangle\langle y_1, y_2\rangle$$

for all $x_1, x_2 \in \mathbb{R}^n$, $y_1, y_2 \in \mathbb{R}^m$.

Proof of Theorem 1.58. Let p be prime, $n = 4p$, $d = n^2$ and let $v_1, \ldots, v_N$ be the $N = \frac{1}{2}\binom{n}{n/2}$ ± 1 vectors given by Theorem 1.53, so that any subcollection of more than $\binom{n}{n/4-1}$ vectors has an orthogonal pair.

Now, for each i, define $w_i \in \mathbb{R}^{n^2}$ by $w_i = v_i \otimes v_i$. Then for all i, j we observe that $\langle w_i, w_j\rangle = \langle v_i, v_j\rangle^2 \geq 0$ and $|w_i|^2 = \langle v_i, v_i\rangle^2 = n^2$, so that we have

$$|w_i - w_j| = \sqrt{|w_i|^2 + |w_j|^2 - 2\langle w_i, w_j\rangle} \leq \sqrt{2}n,$$

with equality occurring if and only if w_i is orthogonal to w_j, which happens if and only if $v_i \perp v_j$. Thus $\{w_1, \ldots, w_N\}$ has diameter $\sqrt{2}n$. If we were to partition it into parts each having diameter less than $\sqrt{2}n$, then each part would have no orthogonal pairs and hence have size at most $\binom{n}{n/4-1}$. Thus by the same calculation as in the proof of Theorem 1.54, we would need at least

$$\frac{N}{\binom{n}{n/4-1}} \approx 1.2^n = 1.2^{\sqrt{d}}$$

parts. Thus, the collection $\{\frac{1}{\sqrt{2}n}w_1, \ldots, \frac{1}{\sqrt{2}n}w_N\}$ has diameter 1 and demonstrates that $f(d) \geq 1.2^{\sqrt{d}}$. □

1.14 Geometry

In this section we'll introduce some of the most fundamental theorems in discrete geometry, many of which have proofs related to linear algebra. First we need some basic definitions.

Definition 1.60. A set $C \subseteq \mathbb{R}^d$ is called *convex* if for all $x, y \in C$, the line segment $[x, y] = \{tx + (1-t)y : 0 \leq t \leq 1\}$ is contained in C. Given any point set $X \subseteq \mathbb{R}^d$, we define the *convex hull* $\operatorname{conv}(X)$ of X to be the smallest convex set C such that $X \subseteq C$.

Given $x_1, \ldots, x_n \in \mathbb{R}^d$, a *convex combination* is a linear combination $x = \sum_{i=1}^n \alpha_i x_i$, where each $\alpha_i \geq 0$ and $\sum_{i=1}^n \alpha_i = 1$.

Claim 1.61. *For any $X \subseteq \mathbb{R}^d$, conv(X) is the set of all convex combinations of finite subsets of X.*

Proof. Let y be a convex combination of some finite subset of X. That is, $y = \sum_{i=1}^n \alpha_i x_i$ for some $x_1, \ldots, x_n \in X$ such that $\alpha_i \geq 0$ and $\sum_{i=1}^n \alpha_i = 1$. We first show that all such y lie in $C := \operatorname{conv}(X)$. We do this by induction on n.

For $n = 1$, we trivially have $y = x_1 \in X \subseteq C$. Now let $n \geq 2$ and suppose the claim holds for $n-1$. Note that $x_n \in X \subseteq C$ so that if $\alpha_n = 1$ then we trivially have $y = x_n \in C$. Otherwise observe that $\sum_{i=1}^{n-1} \frac{\alpha_i}{1-\alpha_n} = 1$ and hence $\sum_{i=1}^{n-1} \frac{\alpha_i}{1-\alpha_n} x_i \in C$ by induction. By the definition of a convex set, we conclude

$$y = (1-\alpha_n) \sum_{i=1}^{n-1} \frac{\alpha_i}{1-\alpha_n} x_i + \alpha_n x_n \in C.$$

In the other direction, we claim that the set of all y as above (that is, the set of all convex combinations of finite subsets of X) is a convex set. Indeed, consider $y = \sum_{i=1}^n \alpha_i x_i$ and $z = \sum_{i=1}^n \beta_i x_i$, satisfying $\alpha_i, \beta_i \geq 0$ and $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i = 1$. For any $t \in [0, 1]$, we have $t\alpha_i + (1-t)\beta_i \geq 0$ and $\sum_{i=1}^n t\alpha_i + (1-t)\beta_i = 1$ so that

$$ty + (1-t)z = \sum_{i=1}^n (t\alpha_i + (1-t)\beta_i) x_i$$

is a convex combination of points in X. □

Theorem 1.62 (Carathéodory, 1907 and 1911)**.** *If $z \in \operatorname{conv}(X)$, then z is a convex combination of at most $d+1$ points.*

Proof. Since $z \in \operatorname{conv}(X)$, by Claim 1.61 we may choose $x_1, \ldots, x_n \in X$ and $\alpha_i \geq 0$, $\sum_{i=1}^n \alpha_i = 1$ such that $z = \sum_{i=1}^n \alpha_i x_i$. Make these choices in such a way that n is minimum possible. Now suppose for sake of contradiction that $n \geq d+2$. Then the system of equations

$$\sum_{i=1}^n \beta_i x_i = 0, \quad \sum_{i=1}^n \beta_i = 0$$

consists of $d+1$ equations with $n \geq d+2$ variables so has a nontrivial solution, say $\beta \in \mathbb{R}^n$. Let i_0 be the value of i such that α_i/β_i is minimized over all $i : \beta_i > 0$, and let $t = \alpha_{i_0}/\beta_{i_0}$. Then $\alpha_i - t\beta_i \geq 0$ for all $i \in [n]$ and $\sum_{i=1}^n \alpha_i - t\beta_i = 1$, so we conclude that

$$z = \sum_{i \in [n]} (\alpha_i - t\beta_i)x_i = \sum_{i \in [n]\setminus\{i_0\}} (\alpha_i - t\beta_i)x_i$$

is a convex combination, contradicting the assumption that n was minimal. □

We now consider the following question.

Question 1.63. *Is it true that if a finite point set $X \subseteq \mathbb{R}^d$ is large enough (as a function of d and r), then X can be partitioned into r parts $X = X_1 \cup \ldots \cup X_r$ such that $\bigcap_{i=1}^r \operatorname{conv}(X_i) \neq \emptyset$?*

Example 1.64. For $d = 2, r = 2$, it is easy to see that for a 3-point set X there is no such partition. However, with 4 points A, B, C, D it is always possible to find a suitable partition. To see this, note that there are two cases to consider. If there are two pairs, say $\{A, B\}$ and $\{C, D\}$, such that AB and CD intersect, then we take $\{A, B\}$ and $\{C, D\}$. Otherwise there is a point, say D, which is within the triangle ABC, so we may take $\{A, B, C\}$ and $\{D\}$.

The answer to this question is given by Radon's theorem, as follows.

Theorem 1.65 (Radon, 1921)**.** *For any $X \subseteq \mathbb{R}^d$ with $|X| \geq d+2$, there is a partition $X = X_1 \cup X_2$ such that $\operatorname{conv}(X_1) \cap \operatorname{conv}(X_2) \neq \emptyset$.*

We remark that Radon's theorem is tight, as one may see by considering a regular simplex.

Proof. Write $X = \{x_1, \ldots, x_n\}$, so that $n \geq d+2$, and for each i, define $y_i = \begin{pmatrix} x_i \\ 1 \end{pmatrix} \in \mathbb{R}^{d+1}$. Since $n > d+1$, the vectors $y_1, \ldots, y_n$ are linearly dependent and thus there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ not all zero such that $\sum_{i=1}^n \alpha_i y_i = 0$. Thus $\sum_{i=1}^n \alpha_i x_i = 0$ and $\sum_{i=1}^n \alpha_i = 0$. Now, define $I = \{i : \alpha_i > 0\}$ and $J = \{j : \alpha_j \leq 0\}$. Let $X_1 = \{x_i : i \in I\}$ and $X_2 = \{x_j : j \in J\}$ so that X_1 and X_2 partition X. To see that $\operatorname{conv}(X_1) \cap \operatorname{conv}(X_2) \neq \emptyset$, let $\alpha = \sum_{i \in I} \alpha_i = \sum_{j \in J} -\alpha_j$ and note that $\alpha > 0$. Hence $y = \sum_{i \in I} \frac{\alpha_i}{\alpha} x_i = \sum_{j \in J} \frac{-\alpha_j}{\alpha} x_j$ are both convex combinations, so that $y \in \operatorname{conv}(X_1) \cap \operatorname{conv}(X_2)$. □

A generalization of Radon's theorem was obtained by Tverberg.

Theorem 1.66 (Tverberg, 1966)**.** *For $X \subseteq \mathbb{R}^d$ with $|X| \geq (r-1)(d+1)+1$, there is a partition $X = X_1 \cup \cdots \cup X_r$ such that $\bigcap_{i=1}^r \operatorname{conv}(X_i) \neq \emptyset$.*

We remark that Tverberg's theorem is tight. Consider a simplex with vertices $v_1, \ldots, v_{d+1}$ in $\mathbb{R}^d$. For each vertex v_i, consider the intersection of all outer half-spaces of faces of the simplex passing through v_i and let B_i be a set of some $r-1$ points in this region. Let $X = \bigcup_{i=1}^{d+1} B_i$ and note that X has $(r-1)(d+1)$ elements. Suppose for sake of contradiction that there is a partition $X = X_1 \cup \ldots \cup X_r$ such that $\bigcap_{i=1}^r \operatorname{conv}(X_i) \neq \emptyset$. For any $i \in [d+1]$, since $|B_i| = r-1$, there must be some j such that $X_j \cap B_i = \emptyset$. Thus if we let H_i be the outer half-space defined by the face of the simplex not containing v_i, then since $B_k \subseteq H_i$ for all $k \neq i$, we have that $\operatorname{conv}(X_j) \subseteq H_i$. Thus we conclude $\bigcap_{j=1}^r \operatorname{conv}(X_i) \subseteq \bigcap_{i=1}^{d+1} H_i = \emptyset$, a contradiction.

Another fundamental theorem in discrete geometry is Helly's theorem (proven by Radon, 1921), as follows.

Theorem 1.67 (Helly, 1913)**.** *Let $C_1, \dots, C_n \subseteq \mathbb{R}^d$ be convex sets, such that any $d+1$ of them intersect. Then $\bigcap_{i=1}^n C_i \neq \emptyset$.*

Again, we remark that this theorem is tight, as one can see by considering the outer half-planes of a regular simplex in $\mathbb{R}^d$. We also remark that it is important that the number of subsets is finite: otherwise, the statement of Helly's theorem is false, as one can see by considering a sequence of nested half-planes.

Proof. We proceed by induction on n. For $n = d+1$ the statement trivially holds. Now let $n \geq d+2$ and suppose that for any i, we have $\bigcap_{j\in[n]\setminus\{i\}} C_j \neq \emptyset$, so that we may choose $v_i \in \bigcap_{j\in[n]\setminus\{i\}} C_j$. Then, by Radon's Theorem there is a partition $I \cup J = [n]$ such that if we let $X_1 = \{v_i : i \in I\}$ and $X_2 = \{v_j : j \in J\}$, there exists $y \in \operatorname{conv}(X_1) \cap \operatorname{conv}(X_2)$. Now, for all $i \in I$, by definition $X_2 \subseteq C_i$, so $y \in \operatorname{conv}(X_2) \subseteq C_i$. Similarly, for all $j \in J$, $X_1 \subseteq C_j$, we have $y \in \operatorname{conv}(X_1) \subseteq C_j$. We conclude that $y \in \bigcap_{i=1}^n C_i$. □

We now consider some applications of the theorems so far. Recall that one definition of a median y of a set of numbers $x_1, \dots, x_n$ is that y satisfies $|\{x_i : x_i \geq y\}|, |\{x_i : x_i \leq y\}| \geq n/2$. This motivates the following definition.

Definition 1.68. Let $X \subseteq \mathbb{R}^d$ be finite. A point $y \in \mathbb{R}^d$ is a *centerpoint* if for any hyperplane h through y, we have

$$\left|h^+ \cap X\right|, \left|h^- \cap X\right| \geq \frac{|X|}{d+1}$$

We note that here h^+, h^- are closed half-spaces.

Theorem 1.69. *Every finite set has a centerpoint.*

We remark that the constant $\frac{1}{d+1}$ in the definition of a centerpoint was chosen such that Theorem 1.69 holds. By considering the vertices of a simplex, we see that we cannot replace $\frac{1}{d+1}$ by any $\alpha > \frac{1}{d+1}$.

To prove Theorem 1.69 we will need the following lemma.

Lemma 1.70. *A point y is a centerpoint for a finite set $X \subseteq \mathbb{R}^d$ if and only if y belongs to every open half-space containing strictly more than $\frac{d}{d+1}|X|$ points of X.*

Proof. Let y be a centerpoint and let H be a half-space containing more than $\frac{d}{d+1}|X|$ points of X. If y is not in H then considering the hyperplane h passing through y which is parallel to the defining hyperplane of H, we would have less than $\frac{|X|}{d+1}$ points on the side opposite to H, a contradiction.

On the other hand, suppose y is not a centerpoint, meaning that there is a hyperplane h through y for which $|h^+ \cap X| < \frac{|X|}{d+1}$. Hence, $|(h^- \setminus h) \cap X| > \frac{d}{d+1}|X|$. Now, $h^- \setminus h$ is an open half-space with more than $\frac{d}{d+1}|X|$ points of X, and y does not belong to $h^- \setminus h$, as required. □

Now we prove Theorem 1.69.

Proof of Theorem 1.69. Let $\mathcal{H}$ be the collection of all the open half-spaces containing more than $\frac{d}{d+1}|X|$ points of X and define $\mathcal{C} = \{\operatorname{conv}(H \cap X) : H \in \mathcal{H}\}$, so that we have $|\overline{C} \cap X| < \frac{1}{d+1}|X|$ for all $C \in \mathcal{C}$ (where $\overline{C}$ denotes the complement of C). Note that if there exists $y \in \bigcap_{C \in \mathcal{C}} C$, then $y \in \bigcap_{H \in \mathcal{H}} H$ so by Lemma 1.70, y is a centerpoint. Thus it will be enough to show that $\bigcap_{C \in \mathcal{C}} C \neq \emptyset$. Moreover, observe that any element of $\mathcal{C}$ is a convex hull of a subset of X, which is finite, so in particular $\mathcal{C}$ is finite. For any $d+1$ sets $C_1, \dots, C_{d+1} \in \mathcal{C}$.

$$|C_1 \cap \cdots \cap C_{d+1} \cap X| \geq |X| - \sum_{i=1}^{d+1} \left|\overline{C_i} \cap X\right| > |X| - (d+1)\frac{1}{d+1}|X| = 0.$$

In particular, $\bigcap_{i=1}^{d+1} C_i \neq \emptyset$. So by Helly's theorem the claim follows. □

Another generalization of the median is given by the so-called ham sandwich theorem, which we state without proof.

Theorem 1.71. *For any finite sets $X_1, \dots, X_d \subseteq \mathbb{R}^d$, there is a hyperplane h such that $|h^- \cap X_i|$, $|h^+ \cap X_i| \geq |X_i|/2$.*

Let us now return to Tverberg's theorem. Before giving a proof, we note that it can be used to prove the following result. We leave the proof as an exercise.

Theorem 1.72. *For all $\varepsilon > 0$ and $d \in \mathbb{N}$, there is $N \in \mathbb{N}$ such that the following holds. For any finite $X \subseteq \mathbb{R}^d$, there exists $Y \subseteq \mathbb{R}^d$ with $|Y| \leq N$ such that for all convex sets C with $|X \cap C| \geq \varepsilon|X|$, we have $|C \cap Y| \neq \emptyset$.*

Now we proceed to the proof of Tverberg's theorem. We will need the following lemma, proved by Barany.

Lemma 1.73 ("Colourful" version of Carathéodory's Theorem)**.** *Let $M_1, \dots, M_{d+1} \subseteq \mathbb{R}^d$ be such that $a \in \operatorname{conv}(M_i)$ for all i. Then there exist $b_i \in M_i$ such that $a \in \operatorname{conv}(b_1, \dots, b_{d+1})$.*

Proof. Note that we can assume $M_1, \dots, M_{d+1}$ are finite. Suppose, for the sake of contradiction, that the theorem is false. For any $b_i \in M_i : i \in [d+1]$, we call $\operatorname{conv}(b_1, \dots, b_{d+1})$ a *rainbow* simplex. Note that as there are finitely many rainbow simplices, there exists a rainbow simplex S with minimal distance to a.

Let $x \in S$ be a closest point of S to a (which exists by compactness) and let h be the hyperplane orthogonal to the line between a and x, through x. Since S is convex and x is the closest point on S to a, note that S and a lie on opposite sides of h. Next, observe that $S' = S \cap h$ is a k-simplex for some $k \leq d$ and so, without loss of generality, there exist $b_1, \dots, b_k$ with $b_i \in M_i$ such that $S' = \operatorname{conv}(b_1, \dots, b_k)$. Now observe that for any $i > k$, since $a \in \operatorname{conv}(M_i)$, there is a point $y_i \in M_i$ on the same side of h as a. But then $\operatorname{conv}(b_1, \dots, b_k, y_{k+1}, \dots, y_{d+1})$ is a rainbow simplex closer to a, a contradiction. □

Proof of Tverberg's Theorem. Write $X = \{x_0, x_1, \ldots, x_N\}$, and note that it suffices to prove the result for the case $N = (r-1)(d+1)$. Define

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ \ldots,\ v_{r-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},\ v_r = \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \in \mathbb{R}^{r-1},$$

so that $v_1 + \ldots + v_r = 0$. For each $i \in \{0, \ldots, N\}$, define $y_i = \begin{pmatrix} x_i \\ 1 \end{pmatrix} \in \mathbb{R}^{d+1}$, and consider the $r(N+1)$ vectors of the form $v_j y_i^\intercal \in \mathbb{R}^{(r-1)(d+1)}$. Since $v_1 + \ldots + v_r = 0$, we have

$$0 \in \operatorname{conv}(v_1 y_i^\intercal, v_2 y_i^\intercal, \ldots, v_r y_i^\intercal),$$

for all i. Thus, by Lemma 1.73, there are $N+1$ vectors $v_{f(0)} y_0^\intercal, \ldots, v_{f(N)} y_N^\intercal$ such that $0 \in \operatorname{conv}\big(v_{f(0)} y_0^\intercal, \ldots, v_{f(N)} y_N^\intercal\big)$ for some function $f : \{0, \ldots, N\} \to \{1, \ldots, r\}$. This means there exist $\alpha_i \geq 0$ with $\sum_{i=0}^N \alpha_i = 1$ such that

$$0 = \sum_{i=0}^{N} \alpha_i v_{f(i)} y_i^\intercal. \tag{1.1}$$

Now, for each $j \in [r]$, define $I_j = \{i : f(i) = j\}$ and $X_j = \{x_i : i \in I_j\}$. We claim that $\sum_{i \in I_j} \alpha_i y_i^\intercal = \sum_{i \in I_{j'}} \alpha_i y_i^\intercal$ for all $j \neq j' \in [r]$. Indeed, if we define $u \in \mathbb{R}^{r-1}$ by $u_j = 1, u_{j'} = -1$ and $u_k = 0$ for all $k \neq j, j'$ then since $u^\intercal v_j = 1$, $u^\intercal v_{j'} = -1$ and $u^\intercal v_k = 0$ for all $k \neq j, j'$, we can left-multiply (1.1) by $u^\intercal$ to obtain $\sum_{i \in I_j} \alpha_i y_i^\intercal = \sum_{i \in I_{j'}} \alpha_i y_i^\intercal$.

This implies that $\sum_{i \in I_j} \alpha_i x_i = \sum_{i \in I_{j'}} \alpha_i x_i$ and $\sum_{i \in I_j} \alpha_i = \sum_{i \in I_{j'}} \alpha_i \neq 0$ for all $j \neq j' \in [r]$, and hence we conclude that

$$\frac{\sum_{i \in I_j} \alpha_i x_i}{\sum_{i \in I_j} \alpha_i} \in \operatorname{conv}(X_j)$$

for all $j \in [r]$. □

Chapter 2

Spectral graph theory

2.1 Basic definitions and results

Central to this chapter is the notion of an adjacency matrix and its eigenvalues.

Definition 2.1. Given a graph G with n vertices $v_1, \ldots, v_n$, we define the *adjacency matrix* A_G to be the $n \times n$ matrix such that

$$(A_G)_{i,j} = \begin{cases} 1 & \text{if } v_i v_j \in E \\ 0 & \text{else.} \end{cases}$$

Definition 2.2. We let $I = I_n$ denote the $n \times n$ identity matrix and $J = J_n$ denote the $n \times n$ matrix of all ones. We omit the dimension n when it is implicitly clear.

Remark 2.3. For any graph G with n vertices, A_G is symmetric and hence there exist eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$ and orthonormal eigenvectors $v_1, \ldots, v_n$ so that $A_G v_i = \lambda_i v_i$ (Note that $\lambda_1, \ldots, \lambda_n$ are the roots of $\det(A_G - \lambda I) = 0$). We will refer to these as the eigenvalues and eigenvectors of G.

Next, let's compute the eigenvalues of a couple of important graphs.

Example 2.4. Let $G = K_n$ be the complete graph and observe that it has adjacency matrix $A_G = J - I$. Since J has eigenvalue n with eigenvector $v_1 = (1, \ldots, 1)^\intercal$ and the remaining eigenvalues all 0 with eigenvectors $v_2, \ldots, v_n$ given by

$$(v_i)_j = \begin{cases} 1 & \text{if } j = i - 1 \\ -1 & \text{if } j = i \\ 0 & \text{else,} \end{cases}$$

it follows that A_G has eigenvalue $n - 1$ with eigenvector v_1 and the remaining eigenvalues all -1 with eigenvectors $v_2, \ldots, v_n$.

Remark 2.5. If G is a d-regular graph then d is always a maximum eigenvalue of A_G with eigenvector $v_1 = (1, \ldots, 1)^\intercal$. Moreover, if G is connected then d is the unique maximum eigenvalue of A_G. This can be proved by considering the coordinate of an eigenvector of λ_1 with the largest absolute value.

Example 2.6. Let $G = K_{m,n}$ be a complete bipartite graph. Let $\mathbf{0}_{a\times b}$ and $\mathbf{1}_{a\times b}$ denote the zero matrix and the all-ones matrix with dimensions $a \times b$. Then the adjacency matrix of G can be written as

$$A_G = \left(\begin{array}{c|c} \mathbf{0}_{m\times m} & \mathbf{1}_{m\times n} \\ \hline \mathbf{1}_{n\times m} & \mathbf{0}_{n\times n} \end{array}\right).$$

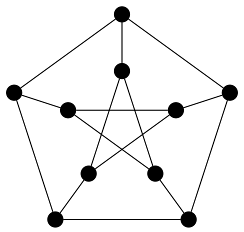
Since there are only two distinct column vectors, we have $\operatorname{rank}(A_G) = 2$, and so the eigenvalues of A_G are $\lambda_1, \lambda_2, 0, \ldots, 0$. Now note that $0 = \operatorname{tr}(A_G) = \lambda_1 + \lambda_2$ so $\lambda_2 = -\lambda_1$. Moreover, observe that

$$2\lambda_1^2 = \lambda_1^2 + \lambda_2^2 = \operatorname{tr}(A_G^2) = \sum_{i,j} (A_G)_{i,j}^2 = 2mn,$$

so we conclude that $\lambda_1 = \sqrt{mn}$ and $\lambda_2 = -\sqrt{mn}$.

Remark 2.7. Consider a connected graph G with eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$. Then G is bipartite if and only if $\lambda_n = -\lambda_1$. Actually, G is bipartite if and only if $\{-\lambda_1, \ldots, -\lambda_n\} = \{\lambda_1, \ldots, \lambda_n\}$; that is to say, the spectrum of A_G is symmetric around zero.

As a first application of spectral graph theory, we'll prove a theorem about the Petersen graph, which is depicted below:



Note that the Petersen graph is 3-regular, and it is plausible that the 9-regular complete graph K_{10} could be partitioned into 3 edge-disjoint copies of the Petersen graph. Is this indeed possible?

Theorem 2.8 (Schwenk)**.** *K_{10} cannot be partitioned into 3 copies of the Petersen graph.*

To prove this theorem, we will need to compute the eigenvalues of the Petersen graph.

Claim 2.9. *The eigenvalues of the Petersen graph are* $3, 1, 1, 1, 1, 1, -2, -2, -2, -2$.

Before proving Claim 2.9 we show how Schwenk's theorem may be deduced.

Proof of Schwenk's theorem. Suppose we can decompose K_{10} into 3 copies of the Petersen graph. Then $J - I = A_{K_{10}} = A + B + C$, where A, B, C are adjacency matrices of isomorphic copies of the Petersen graph. Let U and W be the 5-dimensional eigenspaces for eigenvalue 1 in A and B respectively. Since both are orthogonal to $(1, \ldots, 1)^\intercal$ (the eigenvector of 3), U and W must share a nontrivial subspace. Thus we can choose a nonzero vector $x \in U \cap W$ to obtain

$$-x = (J - I)x = Ax + Bx + Cx = 2x + Cx$$

so that $Cx = -3x$, which is a contradiction because -3 is not an eigenvalue of C. $\square$

We will give a clean proof of Claim 2.9 using a few basic lemmas about eigenvalues of graphs and their transformations. First, we relate the spectrum of the complement of a graph to the spectrum of the original graph.

Lemma 2.10. *Let G be d-regular with eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$. Then the complement graph $H = \overline{G}$ has eigenvalues $n-1-\lambda_1, -(\lambda_2+1), \ldots, -(\lambda_n+1)$.*

Proof. Let $v_1, \ldots, v_n$ be the eigenvectors corresponding to the eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$. We have $A_H = J - A_G - I$ and hence

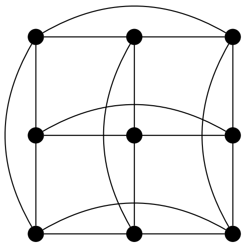
$$A_H v_i = J v_i - A_G v_i - v_i = J v_i - (\lambda_i + 1) v_i = \begin{cases} (n-1-\lambda_1) v_1 & \text{if } i = 1 \\ -(\lambda_i + 1) v_i & \text{if } i \geq 2 \end{cases}.$$

Thus $n-1-\lambda_1, -(\lambda_2+1), \ldots, -(\lambda_n+1)$ are the eigenvalues of H, as claimed. □

Next we'll consider the spectrum of the *line graph* of a graph. We'll need some definitions.

Definition 2.11. Given a graph $G = (V, E)$, we define the *line graph* $L(G)$ to have vertex set E and put $e \sim e'$ iff $e \cap e' \neq \emptyset$, i.e. whenever e and e' are incident to a common vertex of G.

Example 2.12. Let $G = K_{3,3}$. Then $L(G)$ is



Definition 2.13. Let G be a graph with vertices $v_1, \ldots, v_n$ and edges $e_1, \ldots, e_m$. We define the $n \times m$ incidence matrix B_G by $(B_G)_{i,j} = \begin{cases} 1 & \text{if } v_i \in e_j \\ 0 & \text{if } v_i \notin e_j \end{cases}$.

The following two lemmas give a relation between eigenvalues of a graph and its line graph.

Lemma 2.14. *For any d-regular graph G with n vertices and m edges, we have*

$$A_G = B_G B_G^{\intercal} - d I_n,$$
$$A_{L(G)} = B_G^{\intercal} B_G - 2 I_m.$$

Remark 2.15. The second part of the above lemma does not require the graph to be regular.

Lemma 2.16. *For any $n \times m$ matrix A and $m \times n$ matrix B, the nonzero eigenvalues of AB are equal (with the same geometric multiplicities) to the nonzero eigenvalues of BA.*

Proof. Suppose $\lambda \neq 0$ is an eigenvalue of AB with multiplicity k, and eigenbasis $v_1, \ldots, v_k$. Then we have

$$BABv_i = B\lambda v_i = \lambda Bv_i$$

for all $i \in [k]$. We claim that $Bv_1, \ldots, Bv_k$ are independent and thus an eigenbasis of BA for the eigenvalue λ. Indeed, if $\sum_{i=1}^{k} c_i Bv_i = 0$ then left-multiplying by A we obtain

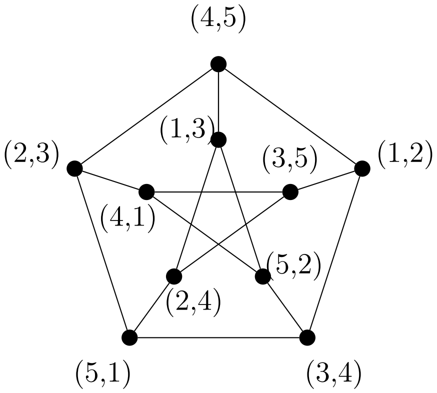
$$0 = \sum_{i=1}^{k} c_i ABv_i = \sum_{i=1}^{k} c_i \lambda v_i = \lambda \sum_{i=1}^{k} c_i v_i,$$

which implies that $c_1 = \ldots = c_k = 0$, since $v_1, \ldots, v_k$ are independent. □

Remark 2.17. Although we will not need this fact, in the lemma above one can also prove that the algebraic multiplicities of all nonzero eigenvalues are the same in BA and AB.

Now we can finally prove Claim 2.9.

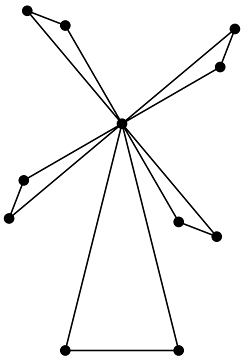
Proof of Claim 2.9. We observe that the Petersen graph is precisely equal to the complement $\overline{L(K_5)}$ of the line graph of K_5 (the vertices below are labelled with the edges of K_5).



Now, recalling Example 2.4, we know that K_5 has eigenvalues $4, -1, -1, -1, -1$. We'll deduce the eigenvalues of $\overline{L(K_5)}$ with the above few lemmas. First, by Lemma 2.14, $B_{K_5}B_{K_5}^{\intercal}$ has eigenvalues $8, 3, 3, 3, 3$. Next, by Lemma 2.16, the 10×10 matrix $B_{K_5}^{\intercal}B_{K_5}$ has 10 eigenvalues $8, 3, 3, 3, 3, 0, 0, 0, 0, 0$. Again using Lemma 2.14, $L(K_5)$ has eigenvalues $6, 1, 1, 1, 1, -2, -2, -2, -2, -2$. Finally, using Lemma 2.10 we conclude that $\overline{L(K_5)}$ has eigenvalues $3, -2, -2, -2, -2, 1, 1, 1, 1, 1$. □

2.2 Friendship graphs

We say a graph is a *friendship graph* if every two vertices have exactly one common neighbour. We say a graph is a *windmill graph* if one vertex is adjacent to all other vertices, and the other vertices induce a perfect matching.



It is easy to see that every windmill graph is a friendship graph. In this section we will prove that the converse is also true!

Theorem 2.18 (Erdős–Rényi-Sós, 1966)**.** *Let G be a friendship graph. Then G is a windmill graph.*

As a stepping stone towards proving Theorem 2.18, we prove the following weaker result.

Claim 2.19. *Let G be a friendship graph. Then G is either a regular graph or a windmill graph.*

Proof. First note that the neighbourhood of any vertex v in V induces a perfect matching in G. Indeed, given a vertex $u \in N(v)$ there exists a unique common neighbour of u and v, so the degree of u within $N(v)$ is precisely 1.

Now, given non-neighbouring vertices u and v, let $N(u) = \{u_1, \dots, u_k\}$. By the above observation, we can suppose without loss of generality that $u_1u_2, \dots, u_{k-1}u_k$ are edges of G. Also without loss of generality, suppose u_2 is the common neighbour of u and v. Denote by w_i the common neighbour of v and u_i for each i, and note that $w_1 = u_2$. Now, given $i \neq j$, note that $w_i \neq w_j$ for $i, j \neq 1$, because u_i and u_j have a unique common neighbour, namely u. Also, $w_i \neq u$, because $w_i \sim v$ but $u \nsim v$. This shows that $d(v) \geq d(u)$, and repeating this argument with u and v swapped, we obtain $d(u) = d(v)$ whenever u and v are not adjacent.

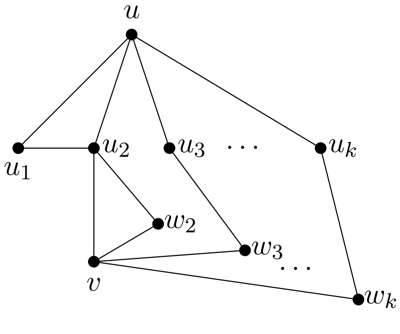


Figure 2.1: Proof of Claim 2.19

Now, suppose that $d(u) \neq d(v)$ for some $u \sim v$. (Otherwise, G is a regular graph and we are done). If a vertex of G has degree $n - 1$, then by the observation at the beginning of the proof

G is a windmill graph and we are done. So, let us assume for the purpose of contradiction that every vertex has a non-neighbour. In this case there are w, t such that ut, vw are non-edges, so $d(u) = d(t) \neq d(v) = d(w)$. This means that uw, vt, wt are edges in G, meaning that v and w are are common neighbours of u and t, contradicting the fact that G is a friendship graph. □

Now we prove Theorem 2.18.

Proof of Theorem 2.18. By Claim 2.19 we may assume G is a regular graph, with degree k, say. Every vertex v has k neighbours, and each of those neighbours has $k-2$ neighbours outside $v \cup N(v)$. By the unique-neighbour property of a friendship graph, all these $k(k-2)$ vertices are distinct, and actually the $1+k+k(k-2)$ vertices we have described so far comprise all the vertices of G. Indeed, any vertex u of G has a common neighbour with v, and thus u must either be in $N(v)$ or be a neighbour of a vertex in $N(v)$. We have proved that the number of vertices in G is $n = 1+k+k(k-2) = k^2-k+1$.

Let A be the adjacency matrix of G. We have

$$(A^2)_{ij} = \sum_{l=1}^{n} A_{il}A_{lj} = \text{ number of common neighbours of } i \text{ and } j = \begin{cases} 1 \text{ if } i \neq j, \\ k \text{ if } i = j, \end{cases}$$

so

$$A^2 = \begin{pmatrix} k & 1 & 1 & \dots & 1 \\ 1 & k & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & k \end{pmatrix}$$

Although it will not be necessary for this proof, we remark that, in general, $(A^t)_{ij}$ is the number of walks of length t between i and j.

One can compute that the eigenvalues of A^2 are k^2 with multiplicity 1 and $k-1$ with multiplicity $n-1$ (the eigenvectors are as in Example 2.4). Now, it is a basic fact from linear algebra that if λ is an eigenvalue of A then λ^2 is an eigenvalue of A^2 (with multiplicity equal to that of λ plus that of $-\lambda$). In our particular case, this implies that one of the eigenvalues of A is either k or $-k$, and the other eigenvalues are all $\pm\sqrt{k-1}$. As G is k-regular, k is an eigenvalue of A, so $-k$ is not an eigenvalue. Let r be the multiplicity of eigenvalue $\sqrt{k-1}$ and $s = n-1-r$ the multiplicity of $-\sqrt{k-1}$. (Another way to see this is to notice that $A^2-(k-1)I = J$ where J is the all ones matrix. Then taking an orthonormal eigenbasis of A it is also an orthonormal eigenbasis of $A^2-(k-1)I$ which implies that if $\lambda_1, \dots, \lambda_n$ are eigenvalues of A then $\lambda_1^2-(k-1), \dots, \lambda_n^2-(k-1)$ are eigenvalue of J and we know J has eigenvalues n with multiplicity 1 and 0 with multiplicity $n-1$. This implies the same restrictions on the eigenvalues as above.)

Note that $0 = \operatorname{tr}(A) = k + r\sqrt{k-1} - s\sqrt{k-1}$, which implies that $k^2 = (s-r)^2(k-1)$. So, $k-1 \mid k^2$. But $k^2-1 = (k-1)(k+1)$, implying that $k-1 \mid 1$, which is only possible if $k \leq 2$. This in turn implies that $n = 3$ or $n = 1$, so G is a triangle or an isolated vertex, therefore a windmill graph. □

2.3 Eigenvalues of Cayley graphs

In this section we will see how to calculate eigenvalues of Cayley graphs, a large class of graphs arising from group theory. We start by presenting some basic facts about groups and their characters and then proceed to show how one can use these facts to find the spectrum of Cayley graphs.

A *group* is a set Γ with operation $\cdot : \Gamma \times \Gamma \to \Gamma$ with $(a, b) \to a \cdot b$, such that:

- Associativity: $(a \cdot (b \cdot c)) = ((a \cdot b) \cdot c)$ for all $a, b, c \in \Gamma$
- Identity: there is $e \in \Gamma$ such that $e \cdot a = a \cdot e = a$ for all $a \in \Gamma$
- Inverse: for all $a \in \Gamma$ there is $a^{-1} \in \Gamma$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

A group is said to be *Abelian* if for all $a, b \in \Gamma$, we have $a \cdot b = b \cdot a$.

Example 2.20. The following are groups:

- $\mathbb{Z}/n\mathbb{Z}$ with addition.
- $(\mathbb{Z}/2\mathbb{Z})^n$
- $\mathbb{F}^\times$ ($\mathbb{F}$ a field) with multiplication.

Let Γ be a finite and Abelian group. $S \subseteq \Gamma$ is a *generating set* if for all $a \in \Gamma$ there are $s_1, \ldots, s_t \in S$ such that $s_1 \cdots s_t = a$. We will always assume our generating set is *symmetric*, i.e. for all $s \in S$ we also have $s^{-1} \in S$.

Let $G = G(\Gamma, S)$ be the graph with $V(G) = \Gamma$ and $E(G) = \{(a, sa) : s \in S, a \in \Gamma\}$. It is easy to see that G is connected and $|S|$-regular.

Example 2.21. The following graphs are Cayley graphs:

- If $\Gamma = (\mathbb{Z}/n\mathbb{Z}, +)$ and $S = \pm 1$, then $G(\Gamma, S)$ is a cycle of length n.
- If $\Gamma = (\mathbb{Z}/2\mathbb{Z})^n$ and S is the set of standard basis vectors, then $G(\Gamma, S)$ is a hypercube: a graph whose vertices are zero-one sequences of length n and whose edges are between sequences which differ in exactly one coordinate.

Let Γ be a group. A *character* of Γ is a homomorphism χ from Γ to the unit circle in $\mathbb{C}$. This means that for any $a, b \in \Gamma$ we have $\chi(a \cdot b) = \chi(a)\chi(b)$. In particular, this implies $\chi(e) = \chi(e \cdot e) = (\chi(e))^2$, which means $\chi(e) = 1$.

Example 2.22. Here are the characters of some of the groups we've seen so far:

- Suppose $\Gamma = (\mathbb{Z}/n\mathbb{Z}, +)$. We have $1 = \chi(0) = \chi(1 + \ldots + 1) = (\chi(1))^n$, meaning that $\chi(1)$ is an n-th root of unity. Note that this value of $\chi(1)$ determines the whole character via $\chi(i) = (\chi(1))^i$. Let ω be any n-th root of unity ($\omega^n = 1, \omega^m \neq 1$ for $1 \leq m < n$). Then the characters of Γ are given by: $\chi_i : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C} : a \mapsto \omega^{ia}$, for $i = 1, \ldots, n$.

- Suppose $\Gamma = (\mathbb{Z}/2\mathbb{Z})^n$. Then the characters are given by $\chi_\sigma : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{C} : (a_1, \ldots, a_n) \mapsto (-1)^{a_1\sigma_1 + \ldots a_n\sigma_n}$, for any $\sigma = (\sigma_1, \ldots, \sigma_n) \in \{0, 1\}^n$.

We record a few basic facts about characters.

Lemma 2.23. *Let Γ be a group, $\Gamma = \{a_1, \ldots, a_n\}$. The following standard facts are easy to check.*

1. *Let χ_1, χ_2 be distinct characters of Γ. For $i \in \{1, 2\}$, let v_i be the vector with jth entry $\chi_i(a_j)$, so $v_i \in \mathbb{C}^n$. Then $\langle v_1, v_2\rangle = 0$ (with respect to standard inner product over $\mathbb{C}$). As $\chi(e) = 1$, no v_i is the zero vector, so this implies the number of distinct characters is at most n.*

2. *If Γ is Abelian, then the number of characters is at least n. This combined with the previous fact implies there are exactly n characters.*

Now we relate the spectra of a Cayley graph to the characters of the corresponding group. Consider a finite Abelian group Γ, and write $\Gamma = \{a_1, \ldots, a_n\}$. Let S be a generating set which is closed under inverses, and let $G = G(\Gamma, S)$ be the Cayley graph of Γ generated by S. Let $\chi_1, \ldots \chi_n$ be the characters of Γ, and as in Lemma 2.23, let v_i be the vector with jth entry $\chi_i(a_j)$. Let $A = A(G)$ be the adjacency matrix of G.

Lemma 2.24. *The vectors $v_1, \ldots, v_n$ as defined above comprise an eigenbasis of $A(G)$. The eigenvector v_i has corresponding eigenvalue equal to $\lambda_i = \left(\sum_{s\in S} \chi_i(s)\right)$.*

Before proving Lemma 2.24, we remark that the quantity $\sum_{s\in S} \chi(s) \in \mathbb{R}$ is always real, because S is closed under inverses.

Proof. Observe that

$$(Av_i)_j = \sum_{\ell=1}^{n} A_{j\ell}(v_i)_\ell = \sum_{\ell=1}^{n} A_{j\ell}\chi_i(a_\ell) = \sum_{\ell : a_\ell \sim a_j} \chi_i(a_\ell) = \sum_{s\in S} \chi_i(sa_j).$$

The last inequality follows by observing that a_ℓ is a a neighbour of a_j if and only if there is an $s \in S$ such that $a_\ell = a_j \cdot s$. Next, observe that

$$\sum_{s\in S} \chi_i(sa_j) = \sum_{s\in S} \chi_i(s)\chi_i(a_j) = \left(\sum_{s\in S} \chi_i(s)\right)\chi_i(a_j) = \lambda_i(v_i)_j$$

It follows that $Av_i = \lambda_i v_i$, so as v_i is not a zero-vector ($\chi_i(e) = 1$), it is an eigenvector with eigenvalue λ_i. By Lemma 2.23, the v_i are independent, and because there are n of them, they are spanning. This means that $\{v_1, \ldots, v_n\}$ is an eigenbasis. □

We can use Lemma 2.24 to deduce the eigenvalues of a cycle graph, as follows.

Example 2.25. Let $\Gamma = (\mathbb{Z}/n\mathbb{Z}, +)$ and $S = 1, -1$, so $G(\Gamma, S)$ is a cycle of length n. We determined the characters of $\Gamma = (\mathbb{Z}/n\mathbb{Z}, +)$ in Example 2.22: they are given by $\chi_i : \Gamma \to \mathbb{C} : a \mapsto \omega^{ia}$, for an nth root ω of unity. Lemma 2.24 implies that the eigenvalues of $G(\Gamma, S)$ are then given by $\lambda_i = \chi_i(1) + \chi_i(-1) = \omega^i + \omega^{-i} \in \mathbb{R}$.

2.4 Spectral inequality and corollaries

Let us first make a couple of easy linear algebraic observations, regarding expansion of vectors in terms of an orthonormal eigenbasis, which will come in handy in the next few chapters. Let $\{v_1, \ldots, v_n\}$ be an orthonormal eigenbasis for a matrix A, corresponding to eigenvalues $\lambda_1, \ldots, \lambda_n$. We have $Av_i = \lambda_i v_i$, $\langle v_i, v_i \rangle = 1$ and $\langle v_i, v_j \rangle = 0$ for $i \neq j$. If $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ then

$$\begin{aligned}\langle Ax, x\rangle &= \langle \alpha_1 A v_1 + \ldots + \alpha_n A v_n, \alpha_1 v_1 + \ldots + \alpha_n v_n\rangle \\ &= \langle \alpha_1 \lambda_1 v_1 + \ldots + \alpha_n \lambda_n v_n, \alpha_1 v_1 + \ldots + \alpha_n v_n\rangle \\ &= \sum_{i,j} \lambda_i \alpha_i \alpha_j \langle v_i, v_j\rangle = \sum_i \lambda_i \alpha_i^2, \qquad (2.1)\end{aligned}$$

and similarly

$$\langle x, x\rangle = \sum_i \alpha_i^2. \qquad (2.2)$$

Lemma 2.26. *Suppose G is a d-regular graph with $d = \lambda_1 \geq \ldots \geq \lambda_n$. Then for $x_1, \ldots, x_n$,*

$$\sum_{i \sim j} (x_i - x_j)^2 \leq (d - \lambda_n) \sum_{i=1}^n x_i^2$$

($i \sim j$ denotes that i is adjacent to j and we count the contribution of edge ij only once) and if $\sum x_i = 0$ then

$$(d - \lambda_2) \sum_{i=1}^n x_i^2 \leq \sum_{i \sim j} (x_i - x_j)^2.$$

Proof. Note that

$$\sum_{i \sim j} (x_i - x_j)^2 = d \sum_{i=1}^n x_i^2 - 2 \sum_{i \sim j} x_i x_j = d \sum_{i=1}^n x_i^2 - \sum_{i \neq j} a_{ij} x_i x_j.$$

Let $x = \sum_{i=1}^n \alpha_i v_i$, where the v_i give an orthonormal eigenbasis of $A(G)$ such that $v_1 = \frac{1}{\sqrt{n}}(1, \ldots, 1)^\intercal$. Then by (2.2) and (2.1) we have $\sum_{i,j} a_{ij} x_i x_j = \langle Ax, x\rangle = \sum_i \lambda_i \alpha_i^2 \geq \lambda_n \sum_i \alpha_i^2 = \lambda_n \langle x, x\rangle$, implying the first part of the lemma.

For the second part note that the condition $\sum_{i=1}^n x_i = 0$ is equivalent to $\langle x, v_1\rangle = 0$, which in turn is equivalent to $\alpha_1 = 0$. Now by (2.2) and (2.1):

$$\sum_{i,j} a_{ij} x_i x_j = \langle Ax, x\rangle = \sum_{i=1}^n \lambda_i \alpha_i^2 = \sum_{i=2}^n \lambda_i \alpha_i^2 \leq \lambda_2 \sum_{i=1}^n \alpha_i^2 = \lambda_2 \langle x, x\rangle.$$

Substituting into the first expression in this proof yields the second part of the lemma. □

Now we shall present some consequences of the above lemma. First, Hoffman's bound gives an upper bound on the size of the largest independent set of a graph.

Corollary 2.27 (Hoffman's bound)**.** *For a d-regular graph G with largest independent set of size $\alpha(G)$, we have*

$$\alpha(G) \leq \frac{-\lambda_n}{d-\lambda_n} n$$

Proof. Suppose $A \subseteq G$ is an independent set, with $|A| = a$. Define

$$x_i = \begin{cases} n-a & i \in A \\ -a & i \notin A. \end{cases}$$

Note that there are no edges within A so all the edges incident to vertices of A go between A and its complement $\overline{A}$. In particular, since G is d-regular, $e(A, \overline{A}) = da$. Note also that the x_i were defined such that $\sum_{i\sim j}(x_i - x_j)^2 = n^2 e(A, \overline{A})$.

Using these observations together with Lemma 2.26, we obtain

$$n^2 da = n^2 e\big(A, \overline{A}\big) = \sum_{i\sim j}(x_i - x_j)^2 \leq (d-\lambda_n)\sum_{i=1}^{n} x_i^2.$$

Finally, notice that $\sum_{i=1}^n x_i^2 = a(n-a)^2 + (n-a)a^2 = na(n-a)$. Substituting and rearranging yields the desired result. □

We remark that Hoffman's bound is sometimes tight. For instance, consider the complete graph K_n. Alternatively, consider the line graph $L(G)$ of any connected d-regular graph G containing a perfect matching. Another particularly important example is the graph of subsets of $[n]$ with edges $A \sim B$ when $A \cap B = \emptyset$. One can apply Hoffman's bound to this graph to yield the famous Erdős–Ko–Rado theorem. This states that any family $\mathcal{A}$ of subsets of $[n]$ of size r which is *intersecting*, that is, such that for all $A, B \in \mathcal{A}$ we have $A \cap B \neq \emptyset$, must have size at most $\binom{n-1}{r-1}$. Furthermore, the only extremal examples (i.e. the ones which achieve this bound) are collections of sets of size r which all contain a specified element in $[n]$.

Next, we show how to apply Lemma 2.26 to the *max cut* of a graph.

Definition 2.28. The *max cut* of a graph G is defined to be the maximum number of edges $e(A, B)$ between any pair A, B of disjoint subsets that partition $V(G)$.

We note that the max cut of any graph G is always at least $e(G)/2$. Indeed, choose each vertex to be in part A or part B independently with probability 1/2 and observe that each edge will contribute to the cut with probability 1/2 (not independently, but this isn't important). Thus the expected number of edges in the cut will be $e(G)/2$ and hence the max cut is at least this big. The following corollary of Lemma 2.26 gives an upper bound.

Corollary 2.29 (Max cut)**.** *For any d-regular graph G with smallest eigenvalue λ_n, the max cut is at most*

$$\frac{e(G)}{2} - \frac{\lambda_n n}{4} = \frac{n}{4}(d - \lambda_n).$$

Proof. Let A, B be a partition of $V(G)$ giving the max cut and let $a = |A|$. Similarly to the previous proof, define

$$x_i = \begin{cases} n-a & i \in A \\ -a & i \in B. \end{cases}$$

and observe that $\sum_{i\sim j}(x_i - x_j)^2 = n^2 e(A,B)$. Moreover, since $a(n-a) \leq n^2/4$, we have

$$\sum_{i=1}^{n} x_i^2 = a(n-a)^2 + (n-a)a^2 = a(n-a)n \leq \frac{n^3}{4}.$$

Thus, using Lemma 2.26, we conclude that

$$n^2 e(A,B) = \sum_{i\sim j}(x_i - x_j)^2 \leq (d-\lambda_n)\sum_{i=1}^{n} x_i^2 \leq (d-\lambda_n)\frac{n^3}{4}.$$

Dividing by n^2 gives the desired result. □

Our final application of Lemma 2.26 concerns the important notion of an *expander graph.*

Definition 2.30. We say that a graph G is a δ*-expander* if for every partition $A \cup B$ of its vertex set $V(G)$ with $|A| \leq |B|$, we have $e(A,B) \geq \delta|A|$.

The following corollary allows us to conclude that any d-regular graph with second largest eigenvalue λ_2 is a $\frac{d-\lambda_2}{2}$-expander.

Corollary 2.31. *Let G be a d-regular graph with second largest eigenvalue λ_2 and let $A \cup B$ be a partition of $V(G)$. Then*

$$e(A,B) \geq \frac{d-\lambda_2}{n}|A||B|.$$

Proof. As in previous proofs, define

$$x_i = \begin{cases} n-a & i \in A \\ -a & i \in B, \end{cases}$$

and observe that $\sum_{i\sim j}(x_i - x_j)^2 = n^2 e(A,B)$ and $\sum_{i=1}^{n} x_i^2 = a(n-a)n$. We observe that $\sum_{i=1}^{n} x_i = a(n-a) + (n-a)(-a) = 0$, so we may use Lemma 2.26 to conclude that

$$n^2 e(A,B) = \sum_{i\sim j}(x_i - x_j)^2 \geq (d-\lambda_2)\sum_{i=1}^{n} x_i^2 = (d-\lambda_2)a(n-a)n.$$

Dividing by n^2 and noting that $a = |A|$ and $n-a = |B|$ completes the proof. □

Remark 2.32. The quantity $d - \lambda_2$ from the corollary above is also called the spectral gap of the adjacency matrix. Alon and Boppana showed that in a d-regular graph G we always have $\lambda_2 \geq 2\sqrt{(d-1)} - \frac{2\sqrt{d-1}-1}{\lceil m/2 \rceil}$ where m is the diameter of G, which in particular gives that the spectral gap is always at most $d - 2\sqrt{d-1} + o(1)$ when we let m tend to infinity with d being fixed.

2.5 Nearly orthogonal vectors

Definition 2.33. A set X of unit vectors in $\mathbb{R}^d$ is said to be *nearly orthogonal* if for any 3 distinct vectors $u, v, w \in X$, there is some pair of vectors which are orthogonal.

We know that the largest set of orthogonal vectors in $\mathbb{R}^d$ has size d, but what about the largest set of nearly orthogonal vectors? It is not too hard to see that one can get $2d$ vectors by considering $\{\pm e_i : 1 \leq i \leq d\}$ where e_i is the standard unit vector in the ith direction. The following theorem of Rosenfeld shows that this is best possible.

Theorem 2.34 (Rosenfeld, 1991)**.** *Any set X of nearly orthogonal vectors in $\mathbb{R}^d$ has size at most $2d$.*

In order to prove this theorem, we will need some simple but useful lemmas.

Lemma 2.35 (Parseval's inequality)**.** *For any set of orthogonal unit vectors X in $\mathbb{R}^d$ and any $v \in \mathbb{R}^d$, we have*

$$\sum_{x \in X} (x \cdot v)^2 \leq |v|^2.$$

Proof. Let $X = \{x_1, \ldots, x_k\}$, which is an orthonormal set of vectors - it can then be extended to an orthonormal basis $\{x_1, \ldots, x_d\}$ of $\mathbb{R}^d$. Write v as a linear combination $v = \sum_i \alpha_i x_i$ and note that by definition, for each i we have $x_i \cdot v = \alpha_i^2$ and moreover, $|v|^2 = \sum_i \alpha_i^2$. Therefore,

$$\sum_{x \in X} (x \cdot v)^2 \leq \sum_i (x_i \cdot v)^2 = |v|^2.$$

□

Lemma 2.36. *For any symmetric matrix A, we have*

$$\operatorname{rank} A \geq \frac{(\operatorname{tr} A)^2}{\operatorname{tr} A^2}.$$

Proof. Let $r = \operatorname{rank} A$ and let $\lambda_1, \ldots, \lambda_r$ be the nonzero eigenvalues of A. Then we note that $\operatorname{tr} A = \sum_{i=1}^r \lambda_i$ and $\operatorname{tr} A^2 = \sum_{i=1}^r \lambda_i^2$, so using the Cauchy–Schwarz inequality, we conclude

$$\frac{\operatorname{tr} A^2}{r} = \frac{\sum_{i=1}^r \lambda_i^2}{r} \geq \left(\frac{\sum_{i=1}^r \lambda_i}{r} \right)^2 = \frac{(\operatorname{tr} A)^2}{r^2}.$$

□

Now we prove Theorem 2.34.

Proof of Theorem 2.34. Let $X = \{v_1, \ldots, v_n\}$ be a set of nearly orthogonal vectors in $\mathbb{R}^d$ and let A be the Gram matrix of these vectors, i.e. the $n \times n$ matrix such that $A_{i,j} = v_i \cdot v_j$. Note that we have $A = B^\intercal B$ where B is the matrix with $v_1, \ldots, v_n$ as column vectors, so that $\operatorname{rank} A \leq \operatorname{rank} B = d$. Thus it will suffice to show that $\operatorname{rank} A \geq n/2$.

To this end we would like to use Lemma 2.36, so we compute $\operatorname{tr} A = \sum_{i=1}^n v_i \cdot v_i = n$ and $\operatorname{tr} A^2 = \sum_{i=1}^n \sum_{j=1}^n (v_j \cdot v_i)^2$. Moreover, for any distinct i, j, k, if $v_j, v_k \not\perp v_i$ then $v_j \perp v_k$. Thus for any i, we have that $\{v_j : v_j \not\perp v_i, j \neq i\}$ is a set of orthogonal unit vectors, and hence by Parseval's inequality

$$\sum_{j : v_j \not\perp v_i, j \neq i} (v_j \cdot v_i)^2 \leq |v_i|^2 = 1.$$

Thus, for any i we have

$$\sum_{j=1}^n (v_j \cdot v_i)^2 = (v_i \cdot v_i)^2 + \sum_{j : v_j \perp v_i, j \neq i} (v_j \cdot v_i)^2 + \sum_{j : v_j \not\perp v_i, j \neq i} (v_j \cdot v_i)^2 \leq 1 + 0 + 1 = 2,$$

and hence

$$\operatorname{tr} A^2 = \sum_{i=1}^n \sum_{j=1}^n (v_j \cdot v_i)^2 \leq 2n.$$

Thus using Lemma 2.36, we conclude $\operatorname{rank} A \geq \frac{(\operatorname{tr} A)^2}{\operatorname{tr} A^2} \geq \frac{n^2}{2n} = n/2$. □

2.6 Variational definition of eigenvalues

The following formulas are widely useful in linear algebra.

Lemma 2.37. *Let A be a symmetric real matrix. Then*

$$\begin{aligned} \lambda_k(A) &= \max_{\substack{U \subseteq \mathbb{R}^n \\ \dim U = k}} \ \min_{\substack{x \in U, \\ |x| \neq 0}} \frac{\langle Ax, x \rangle}{\langle x, x \rangle} \\ &= \min_{\substack{W \subseteq \mathbb{R}^n \\ \dim W = k-1}} \ \max_{\substack{x \in W^\perp, \\ |x| \neq 0}} \frac{\langle Ax, x \rangle}{\langle x, x \rangle}. \end{aligned}$$

Proof. We prove the first part, the second part can be proved in a very similar way and is left as an exercise. Let $\{v_1, \ldots, v_n\}$ be an orthonormal eigenbasis for A, corresponding to eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. Let $U = \operatorname{span}\{v_1, \ldots, v_k\}$, so $\dim U = k$. Then for any $x \in U, |x| \neq 0$ we have $x = \sum_{i=1}^k \alpha_i v_i$ which by (2.2) and (2.1) implies:

$$\frac{\langle Ax, x \rangle}{\langle x, x \rangle} = \frac{\sum_{i=1}^k \lambda_i \alpha_i^2}{\sum_{i=1}^k \alpha_i^2} \geq \frac{\sum_{i=1}^k \lambda_k \alpha_i^2}{\sum_{i=1}^k \alpha_i^2} = \lambda_k.$$

In particular

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

So we obtain $RHS \geq \lambda_k$.

Now let $U \subseteq \mathbb{R}^n$ be such that $\dim U = k$. Let $W = \operatorname{span}\{v_k, \ldots, v_n\}$. Then since $\dim U \cap W = \dim U + \dim W - \dim U + W \geq k + n - k + 1 - n \geq 1$ there exists $0 \neq x \in U \cap W$. For this x we have $x = \sum_{i=k}^n \alpha_i v_i$ which by (2.2) and (2.1) implies:

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

In particular,

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

As U was arbitrary, we obtain $RHS \leq \lambda_k$. □

The following theorem is an often very useful easy corollary of the above lemma. Given an $n \times n$ matrix A, a submatrix of A is said to be *principal* if it can be obtained by deleting the same set of rows and columns from A.

Theorem 2.38. *(Cauchy's Interlace Theorem) Let A be a symmetric $n \times n$ matrix, and B be an $m \times m$ principal submatrix of A, for some $m < n$. If the eigenvalues of A are $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, and the eigenvalues of B are $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$, then for all $1 \leq i \leq m$,*

$$\lambda_i \geq \mu_i \geq \lambda_{i+n-m}.$$

Proof. We may w.l.o.g. assume that B is indexed by $[m]$ and A by $[n]$ (so that B is the $m \times m$ submatrix of A in the upper left corner of A). Let $e_1, \ldots, e_n$ denote the standard basis vectors. For a vector $x \in \mathbb{R}^m$ let $x' \in \mathbb{R}^n$ be obtained by appending $n - m$ zeros to x. For $U \subseteq \mathbb{R}^m$ let $U' := \{x' \mid x \in U\}$ so $\dim U = \dim U'$.

$$\begin{aligned}
\mu_i(B) &= \max_{\substack{U\subseteq\mathbb{R}^m\\ \dim U = i}} \min_{\substack{x\in U,\\ |x|\neq 0}} \frac{\langle Bx, x\rangle}{\langle x, x\rangle} \\
&= \max_{\substack{U'\subseteq\mathbb{R}^n\\ \dim U' = i\\ U'\perp \mathrm{span}\{e_{m+1},\ldots,e_n\}}} \min_{\substack{x'\in U',\\ |x'|\neq 0}} \frac{\langle Ax', x'\rangle}{\langle x', x'\rangle} \\
&\leq \max_{\substack{U'\subseteq\mathbb{R}^n\\ \dim U' = i}} \min_{\substack{x'\in U',\\ |x'|\neq 0}} \frac{\langle Ax', x'\rangle}{\langle x', x'\rangle} = \lambda_i(A)
\end{aligned}$$

Where the inequality follows since we are taking a maximum over a larger set.

The lower bound follows similarly and is left as an exercise. □

If $m = n-1$ in the above theorem it gives $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \ldots \geq \lambda_n$, hence the name interlacing theorem. Note the following trivial corollary of the above.

Corollary 2.39. *Let G be a graph on n vertices and H an induced subgraph on $m \leq n$ vertices. If the eigenvalues of G are $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, and the eigenvalues of H are $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$, then for all $1 \leq i \leq m$,*

$$\lambda_i \geq \mu_i \geq \lambda_{i+n-m}.$$

2.7 Sensitivity conjecture

The Sensitivity conjecture posed by Nisan and Szegedy in 1991 is one of the very few classical conjectures in theoretical computer science which was proved but only after resisting some of the greatest names in the field for quite some time. It has many implications in theoretical computer science and in this section we present Huang's amazingly short recent proof. We prove an equivalent extremal set theoretic statement given by Gotsman and Linial.

Let Q^n be the n-dimensional hypercube graph, whose vertex set consists of vectors in $\{0,1\}^n$, and two vectors are adjacent iff they differ in exactly one coordinate.

Theorem 2.40 (Huang, 2019)**.** *For any integer $n \geq 1$, let H be an arbitrary $(2^{n-1}+1)$-vertex induced subgraph of Q^n, then the maximum degree of H is at least $\sqrt{n}$.*

Proof. Before starting the proof, let us first give an important recursive formulation of the adjacency matrix of the hypercube graph. Let A_n denote the adjacency matrix of Q^n - this is a $2^n \times 2^n$ matrix. Then,

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_n = \begin{pmatrix} A_{n-1} & I \\ I & A_{n-1} \end{pmatrix},$$

which follows by noting that the vertices of Q^n with a fixed last coordinate induce a subgraph isomorphic to Q^{n-1}, and the two identity blocks correspond to the perfect matching connecting these two subcubes Q^{n-1}, corresponding to changing the value of the last coordinate of elements in Q_n. Now, let us say that given a matrix A with $\{0,1\}$-entries, a matrix B is a *signing* of A if it can be obtained from A by changing some entries with a 1 to a -1.

Lemma 2.41. *For all n, there is a signing matrix B_n of A_n such that $B_n^2 = nI_n$. Moreover, the spectrum of B_n consists of 2^{n-1} eigenvalues $\sqrt{n}$ and 2^{n-1} eigenvalues $-\sqrt{n}$.*

Proof. Define B_n in the following recursive manner.

$$B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B_n = \begin{pmatrix} B_{n-1} & I \\ I & -B_{n-1} \end{pmatrix}.$$

By induction, B_n is a signing of A_n. Further, note that inductively we have

$$B_n^2 = \begin{pmatrix} B_{n-1}^2 + I & 0 \\ 0 & B_{n-1}^2 + I \end{pmatrix} = \begin{pmatrix} (n-1)I + I & 0 \\ 0 & (n-1)I + I \end{pmatrix} = nI.$$

Finally, this implies that the eigenvalues of B_n are either $\sqrt{n}$ or $-\sqrt{n}$. Since $Tr[B_n] = 0$, we know that B_n has exactly half of the eigenvalues being $\sqrt{n}$ and the rest being $-\sqrt{n}$. □

Now we prove a lemma concerning a spectral property which is preserved when taking a signing of the adjacency matrix.

Lemma 2.42. *Let G be a graph and B a signing matrix of its adjacency matrix. Then the largest eigenvalue of B is at most $\Delta(G)$.*

Proof. Let A be the adjacency matrix of G, λ_1 be the largest eigenvalue of B and $\vec{v}$ a a corresponding eigenvector. Suppose wlog that v_1 is the coordinate of $\vec{v}$ with the largest absolute value. Then,

$$|\lambda_1 v_1| = |(B\vec{v})_1| = \left|\sum_{j=1}^{m} B_{\,1,j} v_j\right| = \left|\sum_{j\sim 1} B_{1,j} v_j\right| \leq \sum_{j\sim 1} |B_{1,j}||v_1| = \sum_{j\sim 1} A_{1,j}|v_1| \leq \Delta(G)|v_1|.$$

So, $\lambda_1 \leq \Delta(G)$. □

We can finish the proof now that we have the previous two lemmas. Indeed, let H be a $(2^{n-1}+1)$-vertex induced subgraph of Q^n. Consider the principal submatrix B_n' of B_n naturally induced by H. Note that since B_n is a signing of A_n, then also B_n' is a signing of the adjacency matrix of H. Therefore, letting μ_1 denote the largest eigenvalue of B_n', we have by Lemma 2.42 that $\mu_1 \leq \Delta(H)$. In turn, let $\lambda_{2^{n-1}}$ be the (2^{n-1}) largest eigenvalue of B_n, which by Lemma 2.41 is $\sqrt{n}$. By Cauchy's Interlace Theorem (Theorem 2.38), we then have

$$\Delta(H) \geq \mu_1 \geq \lambda_{2^{n-1}} = \sqrt{n}.$$

□

Chapter 3

More advanced methods

3.1 The Chevalley–Warning Theorem

The following extremely useful theorem can be viewed as a generalisation of a fact that an underdetermined system of linear equations can have either zero or infinitely many solutions.

Theorem 3.1 (Chevalley–Warning, 1935)**.** *Let $\mathbb{F}$ be a finite field of characteristic p. Suppose $P_1, \dots, P_m \in \mathbb{F}[x_1, \dots, x_n]$ are n-variable polynomials over $\mathbb{F}$, such that $\sum_{i=1}^m \deg P_i < n$. Then the number of simultaneous solutions of $P_i = 0$ for $i = 1, \dots, m$, is divisible by p.*

Remark 3.2. Note that any finite field has size p^k for some prime p. This p is called the characteristic of $\mathbb{F}$ and is usually defined as the smallest integer a such that $\underbrace{1+1+\ldots+1}_{a} = 0$ in $\mathbb{F}$.

The proof relies on the following two simple facts about finite fields. The first one is sometimes even used as a definition of a finite field, so we omit the proof.

Lemma 3.3. *Let $\mathbb{F}$ be a finite field of size $q = p^\ell$. If $x \neq 0$ then $x^{q-1} = 1$.*

Lemma 3.4. *Let $\mathbb{F}$ be a finite field of size $q = p^\ell$ and assume $0 < k < q-1$. Then $\sum_{x \in \mathbb{F}_q} x^k = 0$.*

Proof. Assume $0 < k < q-1$, so the equation $x^k = 1$ has at most $k < q-1$ solutions and therefore there is $z \neq 0$ such that $z^k \neq 1$. Let $a = \sum_{x \in \mathbb{F}} x^k$. Note that $z^k a = \sum_{x \in \mathbb{F}} (zx)^k = a$, where the last equality follows from the fact that $\{zx \mid x \in \mathbb{F}\} = \mathbb{F}$ due to z being nonzero, hence invertible. As $z^k \neq 1$ this implies $a = 0$ as claimed. □

We are now ready to proceed with the proof of the Chevalley–Warning theorem.

Proof of Theorem 3.1. Let q be the size of $\mathbb{F}$. The number of simultaneous solutions of $P_i = 0$ is equal to

$$N = \sum_{x_1, \dots, x_n \in \mathbb{F}} \prod_{j=1}^m \Big(1 - P_j^{q-1}(x_1, \dots, x_n)\Big).$$

To see this note that by Lemma 3.3, $P_j^{q-1}(x_1, \ldots, x_n) = 1$ if $P_j(x_1, \ldots, x_n) \neq 0$, and otherwise $P_j^{q-1}(x_1, \ldots, x_n) = 0$, so the summand corresponding to $x = (x_1, \ldots, x_n)$ is equal to 1 if x is a simultaneous solution and equal to 0 otherwise. Expanding the equation we obtain:

$$N = \sum_{x_1,\ldots,x_n} \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} \prod_{i=1}^{n} x_i^{k_i}$$

for some constants $a_{k_1,\ldots,k_n} \in \mathbb{F}$. All monomials in the sum satisfy $\sum_{i=1}^{n} k_i \leq \sum_{i=1}^{m} (q-1) \deg P_i < (q-1)n$. So for every monomial there is an i such that $k_i < q-1$. Changing the order of summations and product we obtain:

$$\begin{aligned} N &= \sum_{x_1,\ldots,x_n} \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} \prod_{i=1}^{n} x_i^{k_i} \\ &= \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} \prod_{i=1}^{n} \sum_{x_i} x_i^{k_i}. \end{aligned}$$

Now, consider any monomial, and consider an i such that $k_i < q-1$. If $k_i \neq 0$, by Lemma 3.4, the corresponding sum $\sum_{x_i} x_i^{k_i}$ is zero, which means that the entire product $\prod_{i=1}^{n} \sum_{x_i} x_i^{k_i}$ is zero. Otherwise, if $k_i = 0$ then the sum is equal to $\sum_{x_i} 1 = |F| = 0 \,(\text{mod } p)$, so the entire product is zero again. We have proved that $N = 0$. □

Now we shall present some applications of the Chevalley–Warning theorem.

Conjecture 3.5 (Berge–Sauer). *Every 4-regular simple graph has a 3-regular subgraph.*

In 1982, Tashkinov gave a proof of the above conjecture that was nontrivial and combinatorial in nature. However, Alon, Friedland and Kalai showed that if you add just one edge to a 4-regular graph, then there is a simple argument using the Chevalley–Warning theorem that lets one find a 3-regular subgraph.

Theorem 3.6 (Alon–Friedland–Kalai, 1984). *Every 4-regular graph plus an edge has a 3-regular subgraph.*

Before giving the proof, we remark that this theorem actually holds for any multigraph G on n vertices such that $e(G) > 2n$ and $\Delta(G) \leq 5$. On the other hand, Conjecture 3.5 fails for multigraphs.

Proof. Let H be a 4-regular graph. Then $e(H) = \frac{1}{2}\sum_{v \in V(H)} d(v) = 2n$ so if G is obtained by adding one edge to H, then G satisfies $e(G) = 2n+1$ and $\Delta(G) \leq 5$. For each $e \in E(G)$ we define a variable x_e which takes values in Z_3. Now, for each vertex $v \in V(G)$, we define the polynomial $p_v = \sum_{v \in e} x_e^2$. Since $\sum_{v \in V(G)} \deg p_v = 2n$ and the number of variables is $2n+1$, we may apply the Chevalley–Warning to conclude that the number of simultaneous solutions $(x_e)_{e \in E(G)}$ to all the p_v is divisible by 3. There is a trivial solution given by $x_e = 0$ for all $e \in E(G)$, so there must exist another solution in which not all variables are 0.

Note that for any $x \in \mathbb{Z}_3$, $x^2 = 1$ in $\mathbb{Z}_3$ if and only if $x \neq 0$. Thus if $\sum_{v \in e} x_e^2 = 0$ in $\mathbb{Z}_3$ and $|\{v \in e : x_e \neq 0\}| > 0$, then since $d(v) \leq 5$, we must have $|\{v \in e : x_e \neq 0\}| = 3$. It follows that the subgraph having edge set $\{e \in E(G) : x_e \neq 0\}$ is 3-regular and nonempty. □

Another application of the Chevalley–Warning theorem relates to blocking sets of affine hyperplanes. An *affine hyperplane* is the set of solutions $x = (x_1, \dots, x_n) \in \mathbb{F}_p^n$ to $a_1x_1 + \dots a_nx_n = c$, for some $a = (a_1, \dots, a_n) \in \mathbb{F}_p^n \setminus \vec{0}, c \in \mathbb{F}_p$, which we denote by $A_{a,c}$. A *blocking set* of a hypergraph is a set of vertices which intersects every edge. For a prime p let $\mathcal{H}_{n,p}$ be the hypergraph on $\mathbb{F}_p^n$ consisting of all affine hyperplanes. So $\mathcal{H}_{n,p}$ has p^n vertices and every edge has size p^{n-1}. We are interested in the minium size of a blocking set of $\mathcal{H}_{n,p}$. The following lemma gives an example of size $n(p-1)+1$.

Lemma 3.7. *Let $B \subseteq \mathbb{F}_p^n$ consist of all n-vectors with at most one non-zero coordinate. Then B is a blocking set for $\mathcal{H}_{n,p}$.*

Proof. Let $A_{a,c}$ be an affine hyperplane. Let i be such that $a_i \neq 0$. If we take $x_i = c(a_i)^{-1}, x_j = 0 \ \forall j \neq i$ then $x \in B$ and $x \in A_{a,c}$. □

The following result of Jamison; Brouwer and Schrijver from the 70's shows that the above example in fact has the smallest possible size. The proof we present is due to Alon.

Theorem 3.8. *Let p be a prime. If B is a blocking set in $\mathcal{H}_{n,p}$ then $|B| \geq n(p-1)+1$.*

Proof. By translating B we may assume $\vec{0} \in B$. Let $B' = B \setminus \{\vec{0}\}$. Then B' intersects all affine hyperplanes not containing $\vec{0}$. In particular, for any $u \in \mathbb{F}_p^n \setminus \{\vec{0}\}$ the equation $u \cdot b = 1$ has a solution $b \in B'$. So for

$$f(u) := \prod_{b \in B'} (1 - u \cdot b)$$

we have $f(u) = 0$ for all $u \in \mathbb{F}_p^n$ and $f(\vec{0}) = 1$. For $i \in [p-1]$ let

$$F_i(x^{(i)}) := 1 - f(x^{(i)})$$

where $x^{(1)}, x^{(2)}, \dots, x^{(p-1)} \in \mathbb{F}_p^n$ are $p-1$ vectors consisting of n new variables each. Let $F(x^{(1)}, x^{(2)}, \dots, x^{(p-1)}) = \sum F_i(x^{(i)})$. As $f(u)$ is always 0 except for $u = \vec{0}$ when it is 1. We conclude that all $F(x^{(1)}, x^{(2)}, \dots, x^{(p-1)}) = 0$ if and only if $x^{(i)} = 0$ for all i (since there are at most $p-1$ summands each of which is 0 or 1). In particular, polynomial F has precisely 1 solution, which is not divisible by p. Since it has $n(p-1)$ variables we must have by Chevalley-Warning theorem that $n(p-1) \leq \deg F \leq \max \deg F_i \leq |B'| \leq |B| - 1$. □

Another application of the Chevalley–Warning theorem is the following theorem of Erdős, Ginzburg and Ziv.

Theorem 3.9 (Erdős–Ginzburg–Ziv, 1961)**.** *Consider $A = \{a_1, \dots, a_{2n-1}\}$ with each $a_i \in \mathbb{Z}_n$. Then there is a subset of indices I of size $|I| = n$, such that $\sum_{i \in I} a_i = 0$.*

Proof. Let us first prove the theorem for $n = p$ a prime. Afterward, we will show how to extend this to non-prime n. Let

$$P_1(x_1, \dots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1},$$

$$P_2(x_1,\dots,x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1}.$$

Since $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$, we may apply the Chevalley–Warning theorem to conclude that the number of simultaneous solutions to the equations $P_1 = 0, P_2 = 0$ is divisible by n. In particular, since $(0,\dots,0)$ is a solution, there must exist a non-zero solution $(y_1,\dots,y_{2p-1})$ of both equations. Now define $I = \{i \mid y_i \neq 0\}$ and observe that the first equation together with Lemma 3.3 implies $p \mid |I|$, so since y is non-zero and $|I| \leq 2p-1$, we conclude $|I| = p$. The second equation together with Lemma 3.3 implies $0 = \sum_{i=1}^{2p-1} a_i x_i^{p-1} = \sum_{i\in I} a_i$, completing the proof for the case $n = p$ a prime.

To complete the proof we show that if the theorem holds for k and ℓ then it also holds for $k\ell$, so that using the result for prime n as a base case, we may conclude that the theorem holds for any n by induction.

Let $A = \{a_1 \dots, a_{2k\ell-1}\}$. Applying the result for k we can find I_1 such that $|I_1| = k$ and $\sum_{i\in I_1} a_i = 0 \bmod k$. Remove I_1 from A, which leaves $2k\ell - 1 - k = (2k-1)\ell - 1$ elements, so repeat the argument to find $I_1, \dots, I_{2\ell-1}$ such that $|I_i| = k$ and $\sum_{i\in I_j} a_i = 0 \bmod k$ for all $j = 1,\dots,2\ell-1$. Now define $b_i = \frac{1}{k}\sum_{i\in I_j} a_i \in \mathbb{Z}$, which is an integer by construction. Now apply the result with ℓ and $b_1 \dots, b_{2\ell-1}$ to obtain a set J of size $|J| = \ell$ such that $\sum_{j\in J} b_j = 0 \bmod \ell$. Expanding this in terms of a_i, we conclude that $I = \cup_{j\in J} I_j$ satisfies $|I| = k\ell$ and $\sum_{i\in I} a_i = 0 \bmod k\ell$, as desired. □

Note that Chevalley–Warning only gives the number of solutions modulo p even when the field has size p^k for $k > 1$. We now demonstrate how, sometimes, one can still show the result implied by Chevalley–Warning when dealing with prime powers.

We start with a definition.

Definition 3.10. Given a finite, Abelian group G, the *Davenport constant* $S(G)$ of G is defined to be the least integer s such that for any $g_1 \dots, g_s \in G$ there is a nonempty subset of indices $I \subseteq [s]$ such that $\sum_{i=I} g_i = 0$.

Recall the structure theorem for finite Abelian groups:

Theorem 3.11. *If G is a finite Abelian group then $G = \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$ for some integers $n_1, \dots, n_k$.*

Consider the following example.

Proposition 3.12. *If Let G be a finite Abelian group with $|G|$ being a power of a prime p (by the structure theorem G is of the form $\mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}}$). Then $S(G) \geq 1 + \sum_{i=1}^{k}(p^{\alpha_i} - 1)$.*

Proof. Let $g_i = (0,\dots,0,1,0\dots,0)$ be the group element which is 1 in the $\mathbb{Z}_{p^{\alpha_i}}$-coordinate and zero elsewhere. Taking each g_i exactly $p^{\alpha_i} - 1$ times gives $\sum_{i=1}^{k}(p^{\alpha_i} - 1)$ elements such that no subset sums to zero. This shows $S(G) \geq 1 + \sum_{i=1}^{k}(p^{\alpha_i} - 1)$. □

Olsen proved that the above bound is tight. Let us first prove this in the special case when $\alpha_i = 1$ for all i.

Theorem 3.13. *Let $G = \mathbb{Z}_p^k := \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$. For any $v_1 \ldots, v_t \in G$ with $t \geq k(p-1)+1$ there is $I \neq \emptyset$ such that $\sum_{i \in I} v_i = 0$.*

Proof. Consider the equation $\sum_{i=1}^t v_i x_i^{p-1} = 0$ in the variables $x_1, \ldots, x_t \in \mathbb{Z}_p$. This single equation in $\mathbb{Z}_p^k$ corresponds to k polynomial equations in $\mathbb{Z}_p$, one for each coordinate. The total degree of these equations is $k(p-1) < t$ and so we may apply the Chevalley–Warning theorem. So, the number of solutions is divisible by p and since the 0 vector is a solution, there is a non-zero solution $y_1, \ldots, y_t$. Then $I = \{i \mid y_i \neq 0\}$ satisfies the claim of the theorem. □

To prove Olson's theorem in full generality, a slightly different approach is needed. We need the concept of group rings, but will use them only at a very basic level.

Definition 3.14. A *group ring $R(G)$* of an Abelian group G over a field $\mathbb{F}$ is a commutative ring consisting of all formal linear combinations $\{a_1 g_1 + \ldots + a_k g_k \mid a_i \in \mathbb{F}, g_i \in G\}$, where addition is done elementwise and multiplication is distributive. We will often omit terms with a coefficient of zero, we will often write "g" instead of "$1g$", and if the group identity is e, we will often just write "1" for $1e = e$.

Example 3.15. Let us illustrate the operations in a group ring with an example, so let $F = \mathbb{Z}_3$ and let $g_1, g_2 \in G$. Now it holds that

$$(2g_1 + g_2)(2g_1 - 2g_2) = g_1^2 - g_1 g_2 + 2g_2 g_1 - 2g_2^2 = g_1^2 + g_1 g_2 + g_2^2.$$

We now state and prove Olson's theorem in full generality.

Theorem 3.16 (Olson, 1969)**.** *Let $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}}$. For $v_1 \ldots, v_t \in G$ with $t \geq 1 + \sum_{i=1}^k (p^{\alpha_i} - 1)$, there is $I \neq \emptyset$ such that $\sum_{i \in I} v_i = 0$.*

Leading up to our proof of Theorem 3.16, we will write the group operation as multiplication instead of addition, so that we can work in the group ring of G (over $\mathbb{Z}_p$). Let $g_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ be the group element which is 1 in the $\mathbb{Z}_{p^{\alpha_i}}$-coordinate and zero elsewhere. So, a general element of the group is represented as $g = g_1^{c_1} \cdots g_k^{c_k}$. We will deduce Theorem 3.16 from the following claim.

Claim 3.17. *Under the conditions of Theorem 3.16, in the group ring of G over $\mathbb{Z}_p$, we have*

$$\prod_{i=1}^t (1 - v_i) = 0$$

Before continuing to the proof of this claim, let us show how it implies Theorem 3.16.

Proof of Theorem 3.16. Notice that $\prod_{i=1}^t (1 - v_i) = 1 + \sum_{\emptyset \neq I \subseteq [t]} (-1)^{|I|} \prod_{i \in I} v_i$. Now, each of the terms $\prod_{i \in I} v_i$ is a group element, so the only way the linear combination $1 + \sum_{\emptyset \neq I \subseteq [t]} (-1)^{|I|} \prod_{i \in I} v_i$ could be equal to zero (as claimed in Claim 3.17) is if one of the terms $\prod_{i \in I} v_i$ is the group identity. But (recalling that group addition is written as addition, not multiplication, in the statement of Theorem 3.16), this term corresponds precisely to the I we seek. □

Now, towards the proof of Claim 3.17, we establish some simple facts.

Claim 3.18. *For $u_1, \ldots, u_\ell$ in a group G we have*

$$1 - u_1 \cdots u_\ell = (1 - u_1) + u_1(1 - u_2) + \cdots + u_1 \cdots u_{\ell-1}(1 - u_\ell).$$

Proof. We have

$$\begin{aligned}
&(1 - u_1) + u_1(1 - u_2) + \cdots + u_1 \cdots u_{\ell-1}(1 - u_\ell) \\
&\quad = 1 - u_1 + u_1 - u_1u_2 + u_1u_2 - \ldots - u_1 \cdots u_{\ell-1} + u_1 \cdots u_{\ell-1} - u_1 \cdots u_\ell \\
&\quad = 1 - u_1 \cdots u_\ell
\end{aligned}$$

□

Continuing with our buildup to the proof of Claim 3.17, the following claims will be used to show that a certain subcollection of terms vanishes in a similar fashion as in the proof of the Chevalley–Warning theorem.

Claim 3.19. *Given a group G of the form in Theorem 3.16, and any $g \in G$, we have $(1-g)^p = 1-g^p$.*

Proof. We expand the left hand side using the binomial theorem, obtaining

$$(1 - g)^p = 1 + \sum_{i=1}^{p-1} (-1)^i \binom{p}{i} g^i + (-1)^p g^p = 1 - g^p.$$

We have used the fact that, if $1 \leq i \leq p - 1$, then $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is divisible by p (hence is zero in $\mathbb{Z}_p$) since the numerator is divisible by p and denominator is not. We have also used the fact that $(-1)^p = -1$; this is clear if p is odd, and if $p = 2$ then $-1 = 1$ in $\mathbb{Z}_p$. □

Claim 3.20. *Recalling the definition of the g_i from after the statement of Theorem 3.16, we have $(1 - g_i)^{p^{\alpha_i}} = 0$ for each i.*

Proof. Repeatedly using Claim 3.19 we obtain

$$(1 - g_i)^{p^{\alpha_i}} = (1 - g_i^p)^{p^{\alpha_i - 1}} = \ldots = 1 - g_i^{p^{\alpha_i}} = 0.$$

□

We are finally ready to prove Claim 3.17.

Proof of Claim 3.17. Let $c_{i,j}$ be the ith coefficient in v_i; that is, $v_i = \prod_{j=1}^k g_j^{c_{i,j}}$. Applying Claim 3.18, we have

$$\prod_{i=1}^t (1 - v_i) = \prod_{i=1}^t \left(1 - \prod_{j=1}^k g_j^{c_{i,j}} \right) = \prod_{i=1}^t \left(\sum_{j=1}^k (1 - g_j) f_{i,j} \right),$$

for some group elements $f_{i,j}$. Now, exchanging the order of product and summation we obtain

$$\prod_{i=1}^t \left(\sum_{j=1}^k (1 - g_j) f_{i,j} \right) = \sum_{\substack{\beta_1, \ldots, \beta_k \\ \sum_{i=1}^k \beta_i = t}} \prod_{i=1}^k \Big((1 - g_i)^{\beta_i} \Big) f'_{\beta_1, \ldots, \beta_k},$$

for some group ring elements $f'_{\beta_1,\ldots,\beta_k}$. Now notice that for each $\beta_1, \ldots, \beta_k$ with $\sum_{i=1}^k \beta_i = t > \sum_{i=1}^k p^{\alpha_i} - 1$, there is an i such that $\beta_i \geq p^{\alpha_i}$. Claim 3.20 then implies $(1 - g_i)^{\beta_i} = 0$, which in turn implies each term of the sum is 0 and the whole sum is zero as claimed. □

3.2 The Combinatorial Nullstellensatz

Theorem 3.21 (Hilbert's Nullstellensatz)**.** *Let $\mathbb{F}$ be an algebraically closed field and $f, g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials such that f vanishes over all common zeros of $g_1, \ldots, g_m$. Then there exists a $k \in \mathbb{N}$ and polynomials $h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f^k = \sum_i h_i g_i$.*

The following is a combinatorial version of the above result, which works for any field.

Theorem 3.22 (Combinatorial Nullstellensatz, Alon 1999)**.** *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial over some field $\mathbb{F}$ and consider $S_1, \ldots, S_n \subseteq \mathbb{F}$ such that f vanishes on $S_1 \times \ldots \times S_n$. For each i, define the polynomial $g_i(x_1, \ldots, x_n) = \prod_{s \in S_i}(x_i - s)$. Then there exist polynomials $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f = \sum_i h_i g_i$.*

The following corollary will turn out to be what we actually use for applications. Moreover, instead of proving the above theorem we just give a direct proof of this corollary.

Corollary 3.23. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial over some field $\mathbb{F}$ such that $\deg f = \sum_{i=1}^n t_i$ and the coefficient of $\prod_{i=1}^n x_i^{t_i}$ is nonzero. If $S_1, \ldots, S_n \subseteq \mathbb{F}$ are such that $|S_i| \geq t_i + 1$, then there exists $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

In order to prove the above corollary, we will need the following lemma.

Lemma 3.24. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial over some field $\mathbb{F}$, such that the degree of f as a single variable polynomial in x_i is at most t_i. If $S_1, \ldots, S_n \subseteq \mathbb{F}$ satisfy $|S_i| \geq t_i + 1$ and $f = 0$ on $S_1 \times \cdots \times S_n$, then $f = 0$ everywhere.*

Proof. We proceed by induction on n. For $n = 1$, it is well known that a nonzero polynomial of degree t_1 has at most t_1 roots, so f must be the zero polynomial.

Now let $n \geq 2$ and suppose the result holds for $n - 1$. Then we may write

$$f(x_1, \ldots, x_{n-1}, x_n) = \sum_{i=0}^{t_n} g_i(x_1, \ldots, x_{n-1}) x_n^i$$

where each g_i is a polynomial on $n - 1$ variables. For any particular choice of $x_1, \ldots, x_{n-1} \in S_1 \times \ldots \times S_{n-1}$, $f(x_1, \ldots, x_{n-1}, x_n)$ is a single-variable polynomial in x_n of degree at most t_n which vanishes on S_n. Applying the case $n = 1$ we conclude that it is identically 0 and hence $g_i(x_1, \ldots, x_{n-1}) = 0$ for all $0 \leq i \leq t_n$. This means that $g_i = 0$ on $S_1 \times \ldots \times S_{n-1}$ and so, by induction, $g_i = 0$ everywhere. Thus $f = 0$ everywhere. □

Proof of Corollary 3.23. Suppose for sake of contradiction that $f = 0$ on $S_1 \times \cdots \times S_n$, and without loss of generality assume $|S_i| = t_i + 1$. Note that $\prod_{s \in S_i}(x_i - s)$ is identically 0 over $S_1 \times \ldots \times S_n$ and has degree $t_i + 1$. Now, until there are no more such instances, replace in f every instance of $x_i^{t_i+1}$ with the degree-t_i polynomial $x_i^{t_i+1} - \prod_{s \in S_i}(x_i - s)$. Let g be the resulting polynomial. Note that $g = f = 0$ on $S_1 \times \ldots S_n$ and as a single variable polynomial in x_i, g has degree at most t_i. Hence we may apply Lemma 3.24 to g to conclude that $g = 0$ everywhere.

Moreover, we observe that the term $\prod_{i=1}^n x_i^{t_i}$ will never arise from a replacement. Indeed, suppose it did, and the replacement was from an instance of $x_i^{t_i+1}$ in a term $\prod_j x_j^{r_j}$ with $r_i \geq t_i + 1$. For $\prod_{i=1}^n x_i^{t_i}$ to arise, we must have had $r_j = t_j$ for all $j \neq i$, but this would contradict the maximum degree assumption of f. Thus, since the coefficient of $\prod_{i=1}^n x_i^{t_i}$ is nonzero in f, it must also be nonzero in g. This contradicts the fact that $g = 0$ everywhere. □

We will now discuss some applications. First, the Cauchy–Davenport theorem.

Definition 3.25. For a group G with operation $+$ and any $A, B \subseteq G$, we define $A + B = \{a + b : a \in A, b \in B\}$.

For any $A, B \subseteq \mathbb{R}$, one can easily show that $|A + B| \geq |A| + |B| - 1$, using the fact that $\mathbb{R}$ has a total ordering that is preserved under addition. Using the combinatorial Nullstellensatz, one can show the following similar result for Z_p, originally due to Cauchy and Davenport.

Theorem 3.26 (Cauchy–Davenport, 1813)**.** *For any non-empty $A, B \subseteq \mathbb{Z}_p$ with p prime, we have $|A + B| \geq \min(|A| + |B| - 1, p)$.*

We remark that the Cauchy-Davenport theorem is tight: suppose $A = \{0, \ldots, a-1\}$ and $B = \{0, \ldots, b-1\}$. Then $|A + B| = \{0, \ldots, a+b-2\}$.

Proof of Theorem 3.26. If $|A| + |B| \geq p + 1$ then for any $x \in \mathbb{Z}_p$, $(x - A) \cap B \neq \emptyset$ by the pigeonhole principle, so that there exist $a \in A, b \in B$ such that $x - a = b$ and hence $x \in A + B$. Thus $A + B = \mathbb{Z}_p$ and so $|A + B| = p$.

Otherwise we have $|A| + |B| \leq p$. Suppose for the sake of contradiction that $|A + B| \leq |A| + |B| - 2$. Then we may choose $C \supset A + B$ such that $|C| = |A| + |B| - 2$. Now define the polynomial $f(x, y) = \prod_{c \in C}(x + y - c)$ over $\mathbb{Z}_p$ and observe that $f = 0$ on $A \times B$ and $\deg f = |C| = (|A| - 1) + (|B| - 1)$. Moreover, observe that the coefficient of the term $x^{|A|-1} y^{|B|-1}$ in f is exactly $\binom{|A|+|B|-2}{|A|-1} \pmod p$, which is not zero (the numerator of this expression is a product of positive integers of size at most $|A| + |B| - 2 < p$ and hence none of them are divisible by p). Thus we may apply Corollary 3.23 to reach a contradiction. □

Next, we consider the following (closely related) conjecture, made by Erdős and Heilbronn in 1964. Let $A \hat{+} B = \{a + b : a \in A, b \in B, a \neq b\}$.

Conjecture 3.27 (Erdős–Heilbronn, 1964)**.** *For p prime and any $A \subseteq \mathbb{Z}_p$, we have $|A \hat{+} A| \geq \min(2|A| - 3, p)$.*

Note that if $A = \{0, \ldots, a-1\}$ then $A \hat{+} A = \{1, \ldots, 2a-3\}$, so the conjecture is tight if true.

Interestingly, the original method used to prove the Cauchy–Davenport theorem did not seem to be able to settle this related question. However, it turns out that the above proof using the combinatorial Nullstellensatz can be easily generalized to verify this conjecture. To this end, we prove the following lemma.

Lemma 3.28. *For p prime if non-empty $A, B \subseteq \mathbb{Z}_p$ with $|A| \neq |B|$, then $|A\hat{+}B| \geq \min(|A|+|B|-2, p)$.*

Proof of Conjecture 3.27. Fix $a \in A$ and define $B = A \backslash \{a\}$ so that $|A| \neq |B|$. Thus we may apply Lemma 3.28 to conclude that

$$|A\hat{+}A| \geq |A\hat{+}B| \geq \min(2|A|-3, p). \qquad \square$$

Proof of Lemma 3.28. If $|A|+|B| \geq p+2$ then for any $x \in \mathbb{Z}_p$, we have

$$|(x-A) \cap B| = |x-A| + |B| - |(x-A) \cup B| \geq |A|+|B|-p \geq 2$$

so there exist $a_1 \neq a_2 \in A$ and $b_1 \neq b_2 \in B$ such that $x - a_1 = b_1$ and $x - a_2 = b_2$. Note that if $a_1 = b_1$ and $a_2 = b_2$ then $2a_1 = x = 2a_2$, contradicting the fact that $a_1 \neq a_2$. Thus without loss of generality say $a_1 \neq b_1$. It follows that $x = a_1 + b_1 \in A\hat{+}B$. Thus $A\hat{+}B = \mathbb{Z}_p$ and so $|A\hat{+}B| = p$.

Otherwise we have $|A|+|B| \leq p+1$. Suppose for sake of contradiction that $\left|A\hat{+}B\right| \leq |A|+|B|-3$. Then we may choose $C \supset A+B$ such that $|C| = |A|+|B|-3$. Now define the polynomial $f(x,y) = (x-y)\prod_{c \in C}(x+y-c)$ over $\mathbb{Z}_p$ and observe that $f = 0$ on $A \times B$ and $\deg f = |C|+1 = (|A|-1)+(|B|-1)$. Moreover, observe that the coefficient of the term $x^{|A|-1}y^{|B|-1}$ in f is exactly $\binom{|A|+|B|-3}{|A|-2} - \binom{|A|+|B|-3}{|A|-1} \pmod p$. Now note that

$$\binom{|A|+|B|-3}{|A|-2} - \binom{|A|+|B|-3}{|A|-1} = \frac{(|A|-|B|)(|A|+|B|-3)!}{(|A|-1)!(|B|-1)!} \neq 0 \pmod p,$$

since the numerator of the above expression is a product of positive integers of size at most $|A|+|B|-3 < p$, in addition to the integer $|A|-|B|$, which satisfies $|A|-|B| \neq 0$ and $-p+1 \leq |A|-|B| \leq p-1$. Thus we may apply Corollary 3.23 to reach a contradiction. $\square$

Now let us switch gears and consider the following question.

Question 3.29. *What is the minimal number of affine hyperplanes in $\mathbb{R}^d$ necessary to cover all the vertices of the d-dimensional hypercube $\{0,1\}^d$?*

It is easy to see that the answer to the above question is two (say, the hyperplane of vectors whose first coordinate is zero, and the hyperplane of vectors whose first coordinate is one). However, if we modify the question so that the hyperplanes must all fail to cover a specific vertex, say the zero vector $\vec{0}$, then we arrive at a more interesting problem.

Question 3.30. *What is the minimal number of affine hyperplanes in $\mathbb{R}^d$ that don't pass through $\vec{0}$, which are necessary to cover $\{0,1\}^d \backslash \vec{0}$?*

It is easy to see that for $d = 2$ we need 2 hyperplanes and for $d = 3$ we need 3. Indeed, we shall use the combinatorial Nullstellensatz to show that in d dimensions, it is necessary to have d hyperplanes. (This is best possible, because for each coordinate we can consider the hyperplane of vectors which are equal to one in that coordinate; this collection of d vectors has the required property).

Theorem 3.31. *Let $H_1, \ldots, H_n$ be affine hyperplanes in $\mathbb{R}^d$ such that $\bigcup_{i=1}^n H_i \supset \{0,1\}^d \backslash \vec{0}$ and $\vec{0} \notin \bigcup_{i=1}^n H_i$. Then $n \geq d$.*

Proof. Observe that for each j, since $\vec{0} \notin H_j$, we may write $H_j = \{x \in \mathbb{R}^d : a_j \cdot x = 1\}$ where $a_j \in \mathbb{R}^d \backslash \vec{0}$. Now define the polynomial $f : \mathbb{R}^d \to \mathbb{R}$ by

$$f(x) = \prod_{j=1}^{n} (a_j \cdot x - 1) + (-1)^{n+d-1} \prod_{i=1}^{d} (x_i - 1).$$

and observe that $f(\vec{0}) = (-1)^n + (-1)^{n+d-1}(-1)^d = 0$. Moreover, for all $v \in \{0,1\}^d \backslash \vec{0}$, since there exists j such that $a_i \cdot v - 1 = 0$ and there exists i such that $v_i = 1$, we have that $f(v) = 0$. If we assume that $n < d$, then $\deg f = d$ and f has coefficient $(-1)^{n+d-1}$ for the maximal degree term $\prod_{i=1}^d x_i$, so we may apply Corollary 3.23 to obtain a contradiction. □

Let us now consider a different application for the combinatorial Nullstellensatz towards the *permanent lemma.*

Definition 3.32. Let S_n be the set of all permutations of $[n]$. For an $n \times n$ matrix A over a field $\mathbb{F}$, we define the *permanent* of A to be $\operatorname{per} A = \sum_{\sigma \in S_n} \prod_{i=1}^n A_{i,\sigma(i)}$.

We remark that the permanent is simply what one obtains by ignoring all the fiddly ±1 signs in the definition of the determinant. As an example, the permanent of the $n \times n$ all-1s matrix is $n!$.

Lemma 3.33 (Permanent lemma)**.** *Let A be an $n \times n$ matrix over a field $\mathbb{F}$ with* $\operatorname{per} A \neq 0$. *Then for all $b \in \mathbb{F}^n$ and any choice of $S_1, \ldots, S_n \subseteq \mathbb{F}$, each of size 2, there is a vector $x \in S_1 \times \cdots \times S_n$ such that $(Ax)_i \neq b_i$ for all i.*

Proof. Define $f(x_1, \ldots, x_n) = \prod_{i=1}^n \Big(\sum_{j=1}^n A_{ij} x_j - b_i \Big)$ and observe that $\deg f = n$ and that the coefficient of $\prod_{i=1}^n x_i$ is precisely $\operatorname{per} A$. By Corollary 3.23, we may conclude that there exists $x \in S_1 \times \ldots \times S_n$ such that $f(x_1, \ldots, x_n) \neq 0$, which implies that $(Ax)_i = \sum_{j=1}^n A_{ij} x_j - b_i \neq 0$ for all i. □

Using the permanent lemma, we can give an alternative proof of the Erdős–Ginzburg–Ziv theorem as follows.

Claim 3.34. *If $a_1, \ldots, a_{2p-1} \in \mathbb{Z}_p$ for p prime then there is $I \subseteq [2p-1]$ with $|I| = p$ such that $\sum_{i \in I} a_i = 0$.*

Proof. Without loss of generality assume that $0 \leq a_1 \leq \cdots \leq a_{2p-1} \leq p-1$. Now consider a_i and a_{i+p-1} for $i = 1, \ldots, p-1$. If for some i, $a_i = a_{i+p-1}$ then $a_i = a_{i+1} = \cdots = a_{i+p-1}$ so we have $\sum_{j=i}^{i+p-1} a_j = pa_i = 0 \pmod p$ and hence we are done.

Otherwise $a_i \neq a_{i+p-1}$ for all i, so that for $1 \leq i \leq p-1$, if we define $S_i = \{a_i, a_{i+p-1}\}$ then we have $|S_i| = 2$. Now let A be the $(p-1) \times (p-1)$ all ones matrix (which has permanent $(p-1)! \neq 0$ in $\mathbb{Z}_p$) and note that for all $x \in S_1 \times \ldots \times S_{p-1}$, we have

$$(Ax)_i = \sum_{j=1}^{p-1} x_j.$$

Thus if we define $b \in \mathbb{Z}_p^{p-1}$ by $b_i = i - a_{2p-1}$ then we may apply Lemma 3.33 to conclude that there exists $x \in S_1 \times \ldots \times S_k$ such that $\sum_{j=1}^{p-1} x_j \neq i - a_{2p-1}$ for all $1 \leq i \leq p-1$. Therefore $\sum_{j=1}^{p-1} x_j = -a_{2p-1}$ and hence $\{x_1, \ldots, x_{p-1}, a_{2p-1}\}$ constitute a set of size p that sums to zero, as desired. □

While the permanent lemma may be useful, its downside is that computing the permanent is not easy, except for very special matrices (such as the all-ones matrix above). Computing the determinant, however, is much easier. It would therefore be useful to have an analogous lemma for the determinant, as in the following question.

Question 3.35. *Suppose A is an $n \times n$ matrix over a field $\mathbb{F}$ with $|\mathbb{F}| > 3$ such that $\det A \neq 0$. Does there exist an $x \in \mathbb{F}^n$ such that $x_i \neq 0$ and $(Ax)_i \neq 0$ for all i.*

We remark that if $\mathbb{F}$ is of order p^k for $k \geq 2$, one may answer the above question in the affirmative, using the permanent lemma. Furthermore, very recently it was shown that the statement holds if the order of $\mathbb{F}$ is any large enough prime. Nevertheless, it stays open for small primes; in particular, when $\mathbb{F} = \mathbb{F}_5$.

Finally, let us consider one more application of the combinatorial Nullstellensatz, this time towards colourability of a graph.

Definition 3.36. Given a graph G, a *proper colouring* of G with k colours is a map $f : V(G) \to \{1, \ldots, k\}$ such that $f(u) \neq f(v)$ for all edges $uv \in E(G)$. More generally, given a list L_v for each vertex $v \in V(G)$, a *proper list colouring* of G given lists L_v is a map $f : V(G) \to \bigcup_v L_v$ such that $f(u) \neq f(v)$ for all $uv \in E(G)$ and $f(v) \in L_v$ for all $v \in V(G)$.

Finding out if a graph is k-colourable is difficult in general. Indeed it is NP-hard for $k \geq 3$. The next definition associates a polynomial to an oriented version of a graph G which will allow us to conclude that under a certain condition, G is k-colourable (we will actually prove a more general list colouring theorem).

Definition 3.37. Given a graph G with vertex set $\{v_1, \ldots, v_n\}$, if each edge $v_i v_j \in E(G)$ is given an ordering, say $v_i \to v_j$, then the resulting directed graph D is called an *orientation* of G. Given a directed graph D, we define the polynomial

$$f_D(x_1, \ldots, x_n) = \prod_{v_i \to v_j} (x_i - x_j). \tag{3.1}$$

An immediate observation is that if $f_D(x) \neq 0$ for some $x \in L_1 \times \cdots \times L_n$, then G can be properly coloured from the lists $L_1, \ldots, L_n$ by giving vertex v_i colour x_i.

Definition 3.38. Given a directed graph D, a subgraph $H \subseteq D$ is called *Eulerian* if for every vertex v, we have $d_H^+(v) = d_H^-(v)$, where $d_H^+(v)$ and $d_H^-(v)$ are the out- and in-degrees of v in H. We say that H is *even* if the number of edges in H is even, and otherwise we say it is *odd*. We define $\mathrm{EE}(D)$ to be the number of even Eulerian subgraphs of D, and similarly define $\mathrm{EO}(D)$ to be the number of odd Eulerian subgraphs of D.

The main theorem is as follows.

Theorem 3.39 (Alon–Tarsi, 1992). *Let G be a graph with vertex set $\{v_1, \dots, v_n\}$ and let D be an orientation of G such that d_i is the out-degree of vertex v_i. If $\mathrm{EE}(D) \neq \mathrm{EO}(D)$ and $L_1, \dots, L_n$ are lists such that $|L_i| \geq d_i + 1$, then G has a proper list colouring with lists $L_1, \dots, L_n$.*

Proof. Observe that $\deg f_D = \sum_{i=1}^n d_i$ and moreover that the coefficient of the term $\prod_{i=1}^n x_i^{d_i}$ is precisely $\mathrm{EE}(D) - \mathrm{EO}(D)$. To see the latter claim note that when expanding (3.1) each obtained term corresponds to a choice between v_i and v_j for every edge $v_i \to v_j$, where the former case contributes an x_i factor and latter $-x_j$. We can encode each such choice by a subgraph H of D in which we only keep edges for which we picked the latter case. We claim that H is Eulerian if and only if the term corresponding to H is $\pm \prod_{i=1}^n x_i^{d_i}$. Since we obtain this term iff each vertex v_i was chosen for exactly d_i of its out-edges or in-edges. An edge incident to v_i was added to H if either it was its in-edge and we have chosen v_i or if it was its out-edge and we have not chosen v_i for that edge. Since v_i has d_i out-edges this means that we obtain our term if and only if $d_H^+(v_i) = d_H^-(v_i)$ for all v_i. Additionally the term comes with the sign $(-1)^{|E(H)|}$ since each edge we have included in H contributes a term with the minus sign, establishing the claim.

Thus we may apply Corollary 3.23 to f_D. Together with the remark after Definition 3.37, this completes the proof. □

Given a graph G, what is the smallest number ℓ such that the vertices of G can be properly list coloured from any choice of lists of size ℓ? Obviously, if a graph is properly ℓ-list-colourable, then it is also properly ℓ-colourable, as in particular all lists can be chosen to contain the same ℓ-colours. One might think that the converse is also true, since it 'seems' that if all the lists are the same, this can only make our colouring job harder. It turns out that this intuition is misleading - given any integer ℓ, it is not hard to show that there exists a large enough n such that the complete bipartite graph $K_{n,n}$ is not ℓ-list-colourable (and obviously it is 2-colourable). Nevertheless, by imposing certain structural conditions on bipartite graphs, we can make the list-colouring number smaller. A nice application of the theorem above is the following.

Theorem 3.40 (Alon-Tarsi, 1992). *Any bipartite planar graph G can be properly list coloured from any choice of lists of size* 3.

Proof. By above theorem it is enough to show that there is an orientation D of G such that $d_D^+(v) \leq 2$ for every vertex v. This is since $\mathrm{EE}(D) > 0$ as empty subgraph is Eulerian and $\mathrm{EO}(D) = 0$ since G is bipartite so every cycle in D is even and one can always decompose an Eulerian graph into cycles.

To show that such an orientation exists consider a bipartite subgraph B whose left side consists of 2 copies of every vertex in G and the right side is consists of edges of G. Every edge of G (so vertex on the right) we join in B to the copies of its vertices in B. For any subset of the right side E', it corresponds to a subset of $E(G)$ so to a subgraph of G with $N_B(E')$ consisting of two copies of its vertex set V'. In particular, since it is also planar and bipartite we have $|E'| \leq 2|V'| - 4 = |N_B(E')| - 4$. So Hall's theorem applies and implies that B has a matching M covering E'. We now obtain D by orienting each edge $e \in E(G)$ from the vertex whose copy it was joined to in M. Since every vertex has 2 copies on the left of B at most 2 edges will be oriented from it in D as desired. □

3.3 The cap-set problem

The following question was asked by Erdős and Turán in the 1930s. Recall that a k-term arithmetic progression is a sequence of numbers of the form $x, x+d, \ldots, x+(k-1)d$.

Question 3.41. *Consider $A \subseteq [n]$. How large does $|A|$ need to be to imply that A contains a k-term arithmetic progression?*

In 1952, Roth proved that if $|A| = \delta n$ (for any fixed $\delta > 0$ and sufficiently large n), then A has a 3-term arithmetic progression. In 1967 Szemerédi famously showed that the same holds for k-term arithmetic progressions. This result, and the ideas in its proof, have resulted in a number of important breakthroughs, notably including the Green-Tao theorem that the primes contain arbitrarily long arithmetic progressions.

It is still an open problem to determine the order of magnitude of the best possible condition on $|A|$ in the Erdős–Turán problem. In the case $k = 3$, the best known result is that (for some constant c), any subset of $[n]$ of size at least $\frac{n}{\log n}(\log\log n)^c$ has a 3-term arithmetic progression. For comparison, we remark that in $[n]$ there are about $n/\log n$ primes.

In order to better understand the Erdős–Turán problem, it is natural to consider an analogous problem for finite fields. In particular, we are interested in the following question.

Question 3.42. *Let $A \subseteq \mathbb{Z}_3^k$ such that A has no 3-term arithmetic progressions. How large can $|A|$ be?*

Note that any 3-term arithmetic progression consists of 3 elements x, y, z such that $x + z = 2y$, but in $\mathbb{Z}_3^k$, this is equivalent to the condition $x + y + z = 0$. That is to say, arithmetic progressions are the same as lines in $\mathbb{Z}_3^k$. If a subset of $\mathbb{Z}_3^n$ contains no line it is called a *cap-set.*

It is easy to show that for any cap-set $A \subseteq \mathbb{Z}_3^k$, we have $|A| \leq \frac{3^n}{n}$ (this was first shown by Meshulam). Note that if $N = 3^n$ then this is about $\frac{N}{\log N}$, which "beats" the best known bound for arithmetic progressions in $\mathbb{Z}$. Also, one can construct (exercise!) a set of size 2^n without a 3-term arithmetic progression. The next notable improvement was by Bateman and Katz, who showed that any cap-set $A \subseteq \mathbb{Z}_3^k$ satisfies $|A| \geq \frac{3^n}{n^{1+\varepsilon}}$.

Very recently, Croot, Lev and Pach made an important breakthrough for an analogous problem in $\mathbb{Z}_4^n$ using a new type of polynomial method. Only a week later, using their ideas Ellenberg and Gijswijt observed how to get an exponentially better upper bound for the cap-set problem in $\mathbb{Z}_3^n$:

Theorem 3.43 (Ellenberg-Gijswijt, 2017)**.** *Every subset $A \subseteq \mathbb{Z}_3^k$ such that $|A| \geq (2.756)^k$ has a 3-term arithmetic progression.*

Instead of directly presenting the proof of Theorem 3.43, we'll discuss and prove a different theorem (more closely related to this course's theme of extremal graph and hypergraph theory) using the same approach. At the end of this section we'll explain how to adapt the proof for Theorem 3.43.

The following definition was coined by Erdős and Rado.

Definition 3.44. A *k-sunflower* is a collection of subsets $F_1, \ldots, F_k \subseteq [n]$ for which there is an $S \subseteq [n]$ such that $F_i \cap F_j = S$ for all pairs $i \neq j$.

Erdős and Rado asked the following question, as k-sunflowers are often very useful in inductive proofs.

Question 3.45. *Let $\mathcal{F} \subseteq 2^{[n]}$ with no k-sunflower, how large can $|\mathcal{F}|$ be?*

It was observed by Alon, Shpilka and Umans that the 3-term cap-set problem reduces in a certain sense to the 3-sunflower problem. They posed the following conjecture.

Conjecture 3.46. *For each fixed k there is $C_k < 2$ such that the following holds. For any $\mathcal{F} \subseteq 2^{[n]}$ with no k-sunflower, we have $|\mathcal{F}| \leq C_k^n$.*

This conjecture was proved by Naslund and Sawin using the same methods as introduced for the cap-set problem by Croot, Lev and Pach and by Ellenberg and Gijswijt. Used directly, these methods give better bounds than the aforementioned reduction.

Theorem 3.47. *Let $\mathcal{F} \subseteq 2^{[n]}$, and let $\mathcal{F}$ have no 3-sunflower, then $|\mathcal{F}| \leq (1.89)^n$.*

We remark that the best known lower bound is $(1.55)^n$. Now, in order to prove Theorem 3.47 we introduce the notion of *slice rank*.

Definition 3.48. Given a set A, a function $h : A^k \to \mathbb{F}$ is said to be a *rank 1 function* if there is an index i and functions $f : A \to \mathbb{F}$ and $g :^{k-1} \to \mathbb{F}$ such that $h(x_1, \ldots, x_k) = f(x_i) \cdot g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$.

Definition 3.49. Let T be a function $T : \underbrace{A \times A \times \cdots A}_{k} \to \mathbb{F}$. The *slice rank* of T, denoted $\mathrm{sl}(T)$ is the minimal number of rank 1 functions whose sum is T.

We will now show how to use this concept to prove Theorem 3.47. We start with the following lemma.

Lemma 3.50. *Consider $T : A^3 \to \mathbb{F}$ such that $T(x, y, z) \neq 0$ if and only if $x = y = z$. We have* $\mathrm{sl}(T) \geq |A|$.

Although it will not be necessary for us, it is easy to see that $\mathrm{sl}(T) \leq |A|$, so the above lemma actually implies equality.

The following claim gives a toy example to help us understand the problem, and will be used in the proof of Lemma 3.50.

Claim 3.51. *Consider $T : A^2 \to \mathbb{F}$ such that $T(x, y) \neq 0$ if and only if $x = y$. We have* $\mathrm{sl}(T) \geq |A|$.

Proof. Note that a rank 1 function of 2 variables is of the form $f(x)g(y)$. So, suppose $T(x,y) = \sum_{i=1}^{k} f_i(x)g_i(y)$. Consider the $|A| \times |A|$ matrix C indexed by elements of A, where $C_{x,y} = T(x,y)$. Also, define the matrices B^i by $B^i_{x,y} = f_i(x)g_i(y)$, so $C = \sum_{i=1}^{k} B^i$. Now, note that each B^i has rank 1, because it can be expressed as a tensor product of two vectors, as follows:

$$B^i = \begin{pmatrix} f_i(a_1) \\ f_i(a_2) \\ \vdots \\ f_i(a_{|A|}) \end{pmatrix} \cdot (g_i(a_1), \ldots, g_i(a_{|A|})).$$

The rank of a sum of matrices is bounded by the sum of the ranks, so C has rank at most k. On the other hand, our assumption on T implies that C is a diagonal matrix with non-zero diagonal entries, so it has rank $|A|$. We conclude that $k \geq |A|$ as desired. □

The following claim is a simple exercise in linear algebra, which we will use later.

Claim 3.52. *Given a subspace V of $\mathbb{F}^n$ with $\dim V = k$, there exists $u \in V$ which has at least k non-zero coordinates.*

Proof. Consider a basis of V, and write it as a $k \times n$ matrix. There are k independent columns, and the $k \times k$ matrix defined by these columns has full rank k. Because row rank is equal to column rank, the rows in this $k \times k$ submatrix span an all-1 vector. Taking the same linear combination of the original vectors gives a vector in V which has 1 in these k coordinates. □

We also need one other lemma before proving Lemma 3.50:

Lemma 3.53. *Consider $T : A^3 \to \mathbb{F}$ such that $T(x,y,z) \neq 0$ if and only if $x = y = z$, consider $h : A \to \mathbb{F}$, and define $G : A^2 \to \mathbb{F}$ by $G(y,z) = \sum_{x \in A} h(x)T(x,y,z)$. Then, we have*

$$G(x,y) = \begin{cases} 0 & y \neq z \\ h(a)T(a,a,a) & y = z = a. \end{cases}$$

Proof. If $y \neq z$ then $T(x,y,z) = 0$ for all x, so $G(y,z) = \sum_x h(x)T(x,y,z) = 0$. If $y = z = a$ then $T(x,a,a) = 0$ unless $x = a$, so $G(a,a) = \sum_x h(x)T(x,a,a) = h(a)T(a,a,a)$. □

We are now ready to prove Lemma 3.50.

Proof of Lemma 3.50. Let us write T as a sum of rank 1 functions, as follows.

$$T(x,y,z) = \sum_{i=1}^{k} f_i(x)g_i(y,z) + \sum_{i=1}^{l} p_i(y)q_i(x,z) + \sum_{i=1}^{m} r_i(z)s_i(x,y)$$

Our goal is to prove that $k + l + m \geq |A|$.

Without loss of generality, suppose that $k < |A|$. Each $f_1, \ldots, f_k$ can be thought of as a vector in $\mathbb{F}^{|A|}$. Apply Claim 3.52 to the orthogonal complement of the span of $f_1, \ldots, f_k$ to obtain a vector in $\mathbb{F}^{|A|}$, corresponding to a function h, with the following properties. For each i, we have $\langle h, f_i\rangle = \sum_x h(x)f_i(x) = hf = 0$, and there is an $A' \subseteq A$ with size $|A'| \geq |A| - k$ such that $h(x) \neq 0$ on A'. Let $G(y, z) = \sum_{x\in A} h(x)T(x, y, z)$, and observe that for $y, z \in A'$, we have $G(y, z) \neq 0$ if and only if $y = z$. We may therefore apply Claim 3.51 to the restriction of G to $(A')^2$, proving that $\operatorname{sl} G \geq |A'| \geq |A| - k$. On the other hand, recalling that each $\sum_x f_i(x)h(x) = 0$, and writing $q_i'(z) = \sum_x h(x)q_i(x, z)$ and $\sum_x h(z)s_i(x, y) = s_i'(z)$, we get

$$\begin{aligned}
G(y,z) &= \sum_x h(x)T(x,y,z)\\
&= \sum_{i=1}^{k}\left(\sum_x f_i(x)h(x)\right)g_i(y,z) + \sum_{i=1}^{l} p_i(y)\sum_x h(x)q_i(x,z) + \sum_{i=1}^{m} r_i(z)\sum_x h(z)s_i(x,y)\\
&= \sum_{i=1}^{l} p_i(y)q_i'(z) + \sum_{i=1}^{m} r_i(z)s_i'(y).
\end{aligned}$$

This implies $\operatorname{sl} G \leq l+m$. Combined with the above inequality this gives $|A|-k \leq |A'| \leq \operatorname{sl} G \leq l+m$, as desired. □

We remark that this proof can be straightforwardly extended for more variables. Now, finally, we prove Theorem 3.47.

Theorem 3.54. *Let $\mathcal{F} \subseteq 2^{[n]}$, if $\mathcal{F}$ has no 3-sunflower then $|\mathcal{F}| \leq 3(n+1)\sum_{k=0}^{n/3}\binom{n}{k} \approx \binom{n}{n/3} \approx 2^{H(1/3)n}$.*

Recall that $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the entropy function.

Proof of Theorem 3.47. We will prove that if $\mathcal{F}$ has no 3-sunflower then $|\mathcal{F}| \leq 3(n+1)\sum_{k=0}^{n/3}\binom{n}{k}$. This is about $\binom{n}{n/3} \approx 2^{H(1/3)n} \approx (1.89)^n$, where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the entropy function. (We omit this deduction).

To this end, let $\mathcal{F}_\ell$ denote the elements of $\mathcal{F}$ of size ℓ. For each ℓ, we will show that $|\mathcal{F}_\ell| \leq 3\sum_{k=0}^{n/3}\binom{n}{k}$. There are only $n+1$ possible sizes of a subset of $[n]$, so this implies the desired inequality.

Subsets of $[n]$ can be thought of as vectors in $\{0,1\}^n$. Under this identification, for a family to contain no 3-sunflower means that for all distinct $x, y, z \in \mathcal{F}_\ell$ there is a coordinate i such that $\{x_i, y_i, z_i\} = \{0, 1, 1\}$ (as a multiset). This is because for x, y, z to be a sunflower means that there is no element appearing in exactly two of the three sets.

Set $A = \mathcal{F}_\ell$ for any ℓ and consider the function $T : A \times A \times A \to \mathbb{R}$ defined by $T(x, y, z) = \prod_{i=1}^{n}(2 - (x_i + y_i + z_i))$. We want to show that T satisfies the condition in Lemma 3.50. First note that $T(x, x, x) \neq 0$ as each term in the product defining T is either 2 or -1. Also note that when x, y, z are all distinct we have $T(x, y, z) = 0$, because $\mathcal{F}_\ell$ has no 3-sunflower. It remains to consider the case when two of x and y are equal and the third is different. Without loss of generality suppose $x \neq y = z$. Because each of x, y, z are of the same size, there is an element in z and y which is not in x. This gives a coordinate i such that $\{x_i, y_i, z_i\} = \{0, 1, 1\}$, and therefore for the same reason $T(x, y, z) = 0$. Hence, the conditions for Lemma 3.50 are met, and we have $\operatorname{sl} T \geq |\mathcal{F}_\ell|$.

On the other hand, expanding the product in the definition of T gives an expression of the form

$$T(x,y,z) = \sum c_{\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n,\gamma_1,\ldots,\gamma_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot y_1^{\beta_1} \cdots y_n^{\beta_n} \cdot z_1^{\gamma_1} \cdots z_n^{\gamma_n},$$

where for each term we have $\sum \alpha_i + \sum \beta_i + \sum \gamma_i \le n$, so at least one of $\sum \alpha_i, \sum \beta_i, \sum \gamma_i$ must be no greater than $n/3$. We'll now use this information to give an upper bound on the slice rank of T.

Consider any $\alpha_1, \ldots, \alpha_n$ such that $\sum \alpha_i \le n/3$, and consider the sum of all terms involving the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. This is a rank 1 function of the form $f(x)g(y,z)$. There are only $\sum_{k=1}^{n/3} \binom{n}{k}$ possible choices of α, and accounting for β and γ it follows that T can be represented as a sum of at most $3\sum_{k=1}^{n/3} \binom{n}{k}$ rank 1 functions. This implies that $|\mathcal{F}_\ell| \le \operatorname{sl} T \le 3\sum_{k=1}^{n/3} \binom{n}{k}$, as desired. □

We remark that for the cap-set problem that motivated this section, given $A \subset \mathbb{Z}_3^n$ with no x, y, z such that $x + y + z = 0$, we can use the function $T(x,y,z) = \prod_{i=1}^{n} (1 - (x_i + y_i + z_i)^2)$ and the same method.

Chapter 4

Appendix: Linear algebra recap

4.1 Fields

In mathematics, a field is a set on which addition, subtraction, multiplication, and division are defined, and behave similarly to the corresponding operations on rational and real numbers. Here is a definition:

Definition 4.1. $\mathbf{F} = (F, +, \cdot)$ is a field on the set F with operations $+$ and $\cdot$ if for every $x, y, z \in F$ the following holds:

- $x + y = y + x$ (commutativity of addition)
- $(x + y) + z = x + (y + z)$ (associativity of addition)
- There is an element $0 \in F$, called zero, such that $x + 0 = x$. (existence of an additive identity)
- For each $w \in F$, there is an element $-w \in F$ such that $w + (-w) = 0$. (existence of additive inverses)
- $xy = yx$ (commutativity of multiplication)
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $(x + y) \cdot z = x \cdot z + y \cdot z$ and $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivity)
- There is an element $1 \in F$, such that $1 \neq 0$ and $x \cdot 1 = x$. (existence of a multiplicative identity)
- If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. (existence of multiplicative inverses)

Example 4.2. What follows are examples of fields:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ - these are the sets $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ with standard multiplication and addition.

- $\mathbb{F}_p$ - the equivalence classes of $\mathbf{Z}$ modulo p where p is prime with addition and multiplication modulo p.
  For eg. every element in $\mathbb{F}_p^*$ is invertible: Let $a \in \mathbb{F}_p^*$. Then a, p are coprime and so there exist integers x, y such that $ax + py = 1$ which implies $ax \equiv 1(mod\ p)$.
  Useful fact: $x^{p-1} = 1$ for every $\mathbb{F}_p^*$ (Fermat's little theorem).

- General finite fields (some useful definitions and facts)
  - The characteristic of a field F is $\text{char}(F) = \min\{n \mid \underbrace{1 + \ldots + 1}_{n \text{ times}} = 0\}$
    If F is finite, then $\text{char}(F)$ is finite and prime.
  - It follows that every finite field of characteristic p contains $\mathbb{F}(p)$.
  - Every finite field has order p^n for a prime p and integer n.
  - If $|F| = q = p^n$ then $x^{q-1} = 1$ for all $x \in F^*$.
  - There is an element in F^* whose order is $q - 1$, i.e. $\exists a \in F^*$ s.t. $a^{q-1} = 1$ and $a^n \neq 1$ for $1 \leq n < q$.
  - All finite fields of order p^n are isomorphic.
  - If $char(F) = p$ then $(x + y)^p = x^p + y^p$.

4.2 Vector spaces

A vector space over a field F is a set V with addition and multiplication by elements from F, that satisfy certain rules: Let $X, Y, Z \in V$ and $r, s \in F$

- Commutativity: $X + Y = Y + X$.
- Associativity of vector addition:$(X + Y) + Z = X + (Y + Z)$.
- Additive identity: For all X, $0 + X = X + 0 = X$.
- Existence of additive inverse: For any X, there exists a $-X$ such that $X + (-X) = 0$.
- Associativity of scalar multiplication: $r(sX) = (rs)X$.
- Distributivity of scalar sums: $(r + s)X = rX + sX$.
- Distributivity of vector sums: $r(X + Y) = rX + rY$.
- Scalar multiplication identity: $1X = X$.

Example 4.3. • $\mathbb{C}$ is a vector space over $\mathbb{R}$ and also over $\mathbb{Q}$.

- $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_p$.
- F^n is a vector space over F, with multiplication coordinate-wise
- $F^{n \times m}$ - matrices of size $n \times m$ are a vector space over F.
- $F[X]$ - polynomials in X with coefficients in F are also a vector space over F.

4.2.1 Dimension of Vector Space

Let V be a vector space over F, and $u_1, u_2, \ldots \in V$ and $\alpha_1, \alpha_2 \ldots \in F$.

Definition 4.4. (Independence) Vectors $u_1, \ldots, u_n$ are linearly independent if

$$\alpha_1 u_1 + \ldots + \alpha_n u_n = 0 \implies \alpha_1 = \ldots = \alpha_n = 0$$

.

Definition 4.5. (Span)

$$\operatorname{Span}(\{u_1, \ldots, u_n\}) = \{\alpha_1 u_1 + \ldots + \alpha_n u_n \mid \alpha_i \in F\}$$

We say that a set $S \subset V$ spans V if $\operatorname{Span}(S) = V$.

Definition 4.6. (Dimension) The dimension $\dim_F(V) = \dim(V)$ of V over F is defined as the maximal number n such that there exist n linearly independent vectors in V. If the maximum does not exist, then we say that V is infinite dimensional.

Proposition 4.7. *Let* $\dim(V) < \infty$. *The dimension of* V *is equal to the size of a minimal spanning set, i.e.* $\dim(V) = \min\{n \mid \exists S \subset V,\ |S| = n,\ \mathit{Span}(S) = V\}$

Example 4.8.

- $dim_F(F^n) = n$
- $dim_{F_p}(F_{p^n}) = n$
- $dim_F(F[X]) = \infty$

Remark 4.9. If V has dimension n over F and F is finite, then $|V| = |F|^n$. Indeed, note that $V = \{\alpha_1 u_1 + \ldots + \alpha_n u_n \mid \alpha_i \in F\}$ where $u_1, \ldots, u_n$ are independent.

Some other properties of vector spaces:

- A subset of vectors $U \subset V$ is called a subspace of V if together with the same operations U itself forms a vector space.
- The intersection of two subspaces U_1, U_2 is again a subspace. If $\dim U_1 = \dim(U_1 \cap U_2)$ then U_1 is a subspace of U_2.
- For a vector space V and any $U \subseteq V$, $\operatorname{Span}(U)$ is a subspace of V.
- Let U_1, U_2 be subspaces of V. We define the sum of those subspaces as $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$. $U_1 + U_2$ is then also a subspace.
- For subspaces $U_1, U_2 \subset V$ it holds that: $\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim(U_1) + \dim(U_2)$.

Example 4.10. (Projective planes)
A projective plane is a pair (P, L) - (points, lines) such that:

- Each line (element of L) is a set of points (subset of P).
- Each two lines intersect in exactly one point.

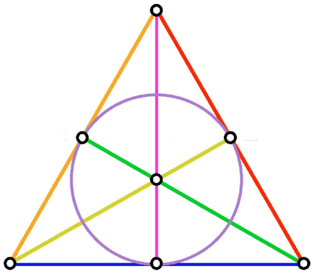


Figure 4.1: Projective plane with 7 points and 7 lines

- Every two points are contained in exactly one line.
- (Non-degeneracy) There exist 4 points such that each line contains at most 2 of them.

Exercise 4.11. Prove that in a finite projective plane all lines have the same number of points, all points are incident with the same number of lines, and #points=#lines.
Show that in fact there exists an n such that #points=#lines=n^2+n+1, each line has $n+1$ points and each point is in $n+1$ lines.

Example 4.12. Let $V = (\mathbb{F}_p)^3$ over $\mathbb{F}_p$, $L = \{\text{subspaces of V of dimension 2}\}$, $P = \{\text{subspaces of V of dimension 1}\}$. If we identify each element of L with the set of elements of P which are subsets of L we get that (P, L) is a projective plane.

Proof.

- Any two distinct subspaces of dimension 1 intersect only in the zero element. Hence any 2-dimensional subspace is a union of 1 dimensional subspaces. I.e. first condition holds.
- For two distinct subspaces $L_1, L_2 \in L$ it holds that $L_1 \cap L_2 \in P$: Let u_1, u_2 be two linearly independent vectors in L_1 and w_1, w_2 in L_2. We prove that there is a non-zero vector in $L_1 \cap L_2$. Since u_1, u_2, w_1, w_2 live in $(\mathbb{F}_p)^3$ which is of dimension 3, they are linearly dependant, meaning that there exists a non-trivial linear combination

  $$\alpha_1 u_1 + \alpha_2 u_2 + \beta_1 w_1 + \beta_2 w_2 = 0$$

  or equivalently

  $$L_1 \ni \alpha_1 u_1 + \alpha_2 u_2 = -\beta_1 w_1 - \beta_2 w_2 \in L_2$$

  so we found our non-zero vector v. In particular $\dim L_1 \cap L_2 \geq 1$ and as $L_1 \neq L_2$ we have $\dim L_1 \cap L_2 = 1$.
- Every two distinct subspaces $P_1, P_2 \in P$ are contained in exactly one subspace in L: Let $P_1 = \text{span}(u_1)$ and $P_2 = \text{span}(u_2)$. u_1, u_2 are linearly independent so $\text{span}(u_1, u_2) = L$ is of dimension 2.
- There exist 4 points such that each line contains at most 2 of them: the vectors $(1,0,0), (1,1,0), (0,1,1), (0,0,1)$ individually span a subspace of V of dimension 1. Every subspace which contains three of them is of dimension at least 3.

□

Exercise 4.13. Prove that the above example indeed gives a projective plane with the number of points $|P| = \frac{p^3-1}{p-1} = p^2 + p + 1$.

Remark 4.14. One can get a projective plane by using any finite field in place of $\mathbb{F}_p$ above. These are the only known examples of finite projective planes!

4.3 Systems of linear equations

Homogeneous systems are equations of the form $Ax = 0$ (where A is a $m \times n$ matrix over a field F and x is $n \times 1$). Note that each row multiplied with x produces one equation.

Definition 4.15. The rank $rk(A)$ of a matrix A is the dimension of the space spanned by the columns (or rows) of A.

The following lemma tells us that the number of solutions of a homogeneous system is equal to the difference of the number of variables and number of non-redundant equations in the system.

Lemma 4.16. *The set of solutions S of the equation $Ax = 0$ is a subspace of F^n of dimension $n - rk(A)$.*

In particular, if #variables > #equations then there exists a non-zero solution of $Ax = 0$. Also if F is finite then the number of solutions is $|F|^{n-rk(A)}$.

The following is useful to know:

Lemma 4.17. *$rk(AB) \leq rk(A), rk(B)$ and $rk(A+B) \leq rk(A) + rk(B)$ for compatible matrices A and B.*

Definition 4.18. (Inner product)
Let $V = F^n$ be a vector space over F. Define the inner product $\langle u, w\rangle = \sum u_i w_i$ where $u, w \in F^n$ and $u = (u_1, \ldots, u_n)$ and $w = (w_1, \ldots, w_n)$. If $\langle u, w\rangle = 0$ then we say that u and w are orthogonal.

Definition 4.19. (Orthogonal Complement)
Let $U \subset V$. We define the orthogonal complement of U to be the set of all vectors in V orthogonal to all vectors in U and write $U^\perp = \{v \in V \mid \forall u \in U \langle u, w\rangle = 0\}$.

Note that the intersection of U and $U^\perp$ can be non-empty. (Find such an example for $V = \mathbb{R}^2$)

Claim 4.20. *Let $U \subset V$ be a subspace.* $\dim(U) + \dim(U^\perp) = n$

Proof. $U^\perp$ is the set of solutions of

$$\begin{pmatrix} -a_1- \\ \cdot \\ \cdot \\ \cdot \\ -a_k- \end{pmatrix} x = 0$$

where $\{a_1, \ldots, a_k\}$ is a basis of U. Hence $\dim(U^\perp) = n - k = n - \dim(U)$. This finishes the proof. □

4.3.1 Non-homogeneous systems

These are systems of the form $Ax = b$.

Claim 4.21. *$Ax{=}b$ has a solution iff $rk(A) = rk(A|b)$ ($A|b$ is the matrix we get when we add b to A as one extra column)*

In particular, if $rk(A) = \#rows$, then $Ax = b$ has a solution.

Suppose $Ax = b$ has a solution u. Let S be the space of solutions of $Ax = 0$. Then the solutions of $Ax = b$ are given by $S + u = \{w + u \mid w \in S\}$. In particular, if F is finite, #solutions$= |F|^{n-rk(A)}$.

4.4 Eigenvalues and Eigenvectors

Let F be a field and $A \in F^{n\times n}$ a matrix over this field.

Definition 4.22. If for a non-zero vector $x \in F^n$ and a scalar $\lambda \in F$ it holds that $Ax = \lambda x$ then we call x an *eigenvector* of A and λ the *eigenvalue* associated to x.

Geometrically, an eigenvector, corresponding to a real nonzero eigenvalue, points in a direction in which it is stretched by the transformation and the eigenvalue is the factor by which it is stretched.

Eigenvectors and eigenvalues are central notions in linear algebra. In this overview we give some of the basic results concerning these notions, which we will use later.

First we note that the eigenvectors associated to the same eigenvalue form a subspace of F^n.

Lemma 4.23. *Let $A \in F^{n\times n}$ and λ one of its eigenvalues. Then*

$$S_A(\lambda) = \{x \mid Ax = \lambda x\}$$

is a subspace of R^n. We call $S_A(\lambda)$ the eigenspace associated to λ and $\dim(S_A(\lambda))$ the geometric multiplicity of λ.

Proof. Let $x, y \in S_A(\lambda)$. Then

$$A(\alpha x + \beta y) = \alpha Ax + \beta Ay = \alpha\lambda x + \beta\lambda y = (\alpha x + \beta y)\lambda$$

so $\alpha x + \beta y \in S_A(\lambda)$ and therefore $S_A(\lambda)$ is a subspace of F^n. □

Notice that $Ax = \lambda x$ is equivalent to $(A - \lambda I)x = 0$. If we view this as an equation system, then it has a non-trivial solution for x, if the matrix $(A - \lambda I)$ has rank at most $n - 1$ (Lemma 4.16). Therefore $\det(A - \lambda I) = 0$. We conclude the following.

Theorem 4.24. *Let $f(\lambda) = \det(A - \lambda I)$. Each of the n roots of f is an eigenvalue of A. The (algebraic) multiplicity of each eigenvalue of A is defined as the multiplicity of it as a root of f.*

We call f from the previous theorem the characteristic polynomial of A and we usually denote its roots (eigenvalues of A) with:

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$$

Definition 4.25. The minimal polynomial m_A of a matrix A is the polynomial with coefficients in F with smallest degree such that the leading term is equal to 1 and $m_A(A) = 0$.

Lemma 4.26. *λ is an eigenvalue of A iff $(x - \lambda)$ divides $m_A(x)$.*

Definition 4.27. If a set of eigenvectors of A forms a basis of F^n, then this basis is called an *eigenbasis.*

The following two results we mention without a proof.

Theorem 4.28 (Perron-Frobenius)**.** *Let A be a positive square (real) matrix and let λ_1 be its largest eigenvalue. Then λ_1 is associated to a positive eigenvector and $|\lambda_1| > |\lambda_i|$ for all other eigenvalues λ_i of A.*

Proposition 4.29. *Let A be a real or complex matrix. Then $\operatorname{tr} A = \lambda_1 + \ldots + \lambda_n$, where $\operatorname{tr} A$ is the trace of the matrix A - the sum of the elements on the main diagonal.*

Definition 4.30. A matrix A is said to be diagonalizable if there exists an invertible matrix P such that $P^{-1}AP = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ where the last matrix is the diagonal matrix with the eigenvalues of A on the main diagonal.

4.4.1 Symmetric Matrices

Matrices which will be of special interest to us are symmetric matrices, as we will use them to encode graphs as a adjacency matrices.

Definition 4.31. A $n \times n$ matrix A is *symmetric* if $A_{i,j} = A_{j,i}$ for all $i, j \in [n]$.

It can be shown that every symmetric matrix is also diagonalizable. Now we state 2 important results about symmetric matrices.

Proposition 4.32. *Let $A \in \mathbb{R}^{n \times n}$ be a symmetric matrix. The following holds:*

- *All eigenvalues of A are real.*
- *Eigenvectors of A corresponding to distinct eigenvalues are orthogonal.*

The next result relates the multiplicity of each eigenvalue to the dimension of its associated eigenspace.

Proposition 4.33. *Let A be a real symmetric matrix and λ one of its eigenvalues. Then the multiplicity of λ is equal to the dimension of its eigenspace $\dim(S_A(\lambda))$.*

The above statements imply the following very useful fact.

Corollary 4.34. *Every real symmetric matrix has an orthonormal eigenbasis.*

Proof. Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix. For the eigenspace of each eigenvalue λ find an orthonormal basis. The union of those gives n vectors (Proposition 4.33) which are pairwise orthogonal (Proposition 4.32). □

Proposition 4.35. *Let λ be an eigenvalue of a symmetric real matrix A. Then λ^2 is an eigenvalue of A^2 and its multiplicity is the sum of the multiplicities of λ and $-\lambda$ with respect to A.*

Proof. Let $x \in S_A(\lambda) \cup S_A(-\lambda)$. Then it holds that

$$A^2x = A(Ax) = A(\pm\lambda x) = \lambda^2 x,$$

so x is an eigenvector of A and therefore $S_{A^2}(\lambda^2)$ has dimension at least $\dim(S_A(\lambda)) + \dim(S_A(-\lambda))$ due to Proposition 4.32 and this is exactly the sum of multiplicities of λ and $-\lambda$ by Proposition 4.33. Since this holds for every eigenvalue and the sum of multiplicities is n, this is also an upper bound, so we are done. □

The next result shows how to calculate the minimal polynomial of a symmetric matrix, if the eigenvalues are known.

Proposition 4.36. *Let A be an $n\times n$ symmetric matrix over $\mathbb{R}$. Then $m_A(x) = (x-\mu_1)\cdot\ldots\cdot(x-\mu_t)$ where $\{\mu_1,\ldots,\mu_t\} = \{\lambda_1,\ldots,\lambda_n\}$ is the set of eigenvalues of A, without multiplicities.*

Proof. Let $f(x) = (x-\mu_1)\cdot\ldots\cdot(x-\mu_t)$. Since A is symmetric it is also diagonalizable, so we have that $A = P^{-1}DA$ for some invertible matrix P and $D = \operatorname{diag}(\lambda_1,\ldots,\lambda_n)$. Note that $f(D) = 0$ and therefore $f(A) = f(P^{-1}DP) = P^{-1}f(D)P = 0$. Thanks to Lemma 4.26 we conclude that f is the minimal polynomial such that $f(A) = 0$, so by definition $m_A = f$ and we are done. □

Remark 4.37. It can be seen from the proof of the previous proposition that the same claim holds for the larger class of diagonalizable matrices.