MAT377 - Combinatorial Mathematics

Stefan H. M. van Zwam

Princeton University

Fall 2013
This version was prepared on April 24, 2014.

Contents

Acknowledgements

This course was run in the past by Benny Sudakov, Jan Vondrak, and Jacob Fox. I based these notes on their lecture notes, but added several new topics.

I thank Cosmin Pohoata for thoroughly reading the manuscript, correcting many errors, and adding some nice examples. Any remaining errors are, of course, only my responsibility.

—Stefan van Zwam. Princeton, April 2014.

CHAPTER 1

Introduction

1.1 What is combinatorics?

> It is difficult to find a definition of combinatorics that is both concise and complete, unless we are satisfied with the statement "Combinatorics is what combinatorialists do."
>
> W.T. Tutte (in Tutte, 1969, p. ix)

> Combinatorics is special.
>
> Peter Cameron (in Cameron, 1994, p. 1)

Combinatorics is a fascinating but very broad subject. This makes it hard to classify, but a common theme is that it deals with structures that are, in some sense, finite or discrete. What sets combinatorics apart from other branches of mathematics is that it focuses on *techniques* rather than results. The way you prove a theorem is of bigger importance than the statement of the theorem itself. Combinatorics is also characterized by what seems to be less depth than other fields. The statement of many results can be explained to anyone who has seen some elementary set theory. But this does not imply that combinatorics is shallow or easy: the techniques used for proving these results are ingenious and powerful.

Combinatorial problems can take on many shapes. In these notes, we focus mostly on the following three types:

Enumeration How many different structures of a given size are there?
Existence Does there exist a structure with my desired properties?
Extremal problems If I only look at structures with a specific property, how big can I make them?

Techniques for solving these are varied, and *anything is fair game*! In these notes we will see the eminently combinatorial tools of recursion, counting through bijection, generating functions, and the pigeonhole principle, but also probability theory, algebra, linear algebra (including eigenvalues), and even a little topology.

1.2 Some notation and terminology

If we use special notation, we normally explain it when it is first introduced. Some notation crops up often enough that we introduce it here:

$\mathbb{N}$	The set of nonnegative integers $\{0, 1, 2, \ldots\}$
$[n]$	The finite set of integers $\{1, 2, \ldots, n\}$
$\lvert X\rvert$	The size of the set X, i.e. the number of elements in it.
$\mathscr{P}(X)$	The power set of X, i.e. the set $\{Y : Y \subseteq X\}$.

Many of the structures we will study can be seen as *set systems*. A set system is a pair $(X, \mathscr{F})$, where X is a finite set and $\mathscr{F} \subseteq \mathscr{P}(X)$. We refer to $\mathscr{F}$ as a *set family*. Often we are interested in families with certain properties ("all sets have the same size"), or families whose members have certain intersections ("no two sets are disjoint"), or families that are closed under certain operations ("closed under taking supersets").

An important example, that comes with a little bit of extra terminology, is that of a *graph*:

1.2.1 DEFINITION. A *graph* G is a pair (V, E), where V is a finite set, and E is a collection of size-2 subsets of V.

The members of V are called *vertices*, the members of E *edges*. If $e = \{u, v\}$ is an edge, then u and v are the *endpoints*. We say u and v are *adjacent*, and that u and v are *incident* with e. One can think of a graph as a network with set of nodes V. The edges then denote which nodes are *connected*. Graphs are often visualized by drawing the vertices as points in the plane, and the edges as lines connecting two points.

1.2.2 DEFINITION. The *degree* of a vertex v, denoted $\deg(v)$, is the number of edges having v as endpoint. A vertex of degree 0 is called *isolated*.

If you have never encountered graphs before, an overview of the most basic concepts is given in Appendix A.

1.3 Elementary tools: double counting

Our first result can be phrased as an existential result: there is no graph with an odd number of odd-degree vertices. Phrased more positively, we get:

1.3.1 THEOREM. *Every graph has an even number of odd-degree vertices.*

Proof: Let $G = (V, E)$ be a graph. We find two ways to count the number of pairs (v, e), where $v \in V$, $e \in E$, and v is incident with e. First we observe that each edge gives rise to exactly two such pairs, one for each end. Second, each vertex appears in exactly one such pair for each edge it is incident with. So we find

$$2|E| = \sum_{v \in V} \deg(v).$$

Since the left-hand side is even, so is the right-hand side, and the result follows from this. ∎

The handshaking lemma is an example of a very useful combinatorial technique: double counting. By finding two ways to determine the size of a certain set (in this case the set of pairs (v,e)), we can deduce new information. A classical example is Euler's Formula (see Problem A.7.5)

1.4 Elementary tools: the Pigeonhole Principle

The Pigeonhole Principle is an extremely basic observation: if n pigeons are divided over strictly fewer than n holes, there will be a hole containing at least two pigeons. More formally,

1.4.1 LEMMA (Pigeonhole Principle). *Let N and K be finite sets and $f : N \to K$ a function. If $|N| > |K|$ then there exist $m, n \in N$ such that $f(m) = f(n)$.*

A proof by induction is easily constructed. We illustrate the use by an easy example:

1.4.2 THEOREM. *Let $G = (V,E)$ be a graph. There exist vertices $u, v \in V$ such that* $\deg(u) = \deg(v)$.

Proof: Suppose G is a graph for which the theorem fails. If G has a vertex v of degree 0 then $G - v$ is another such graph. Hence we assume no vertex has degree zero. If $|V| = n$, then the possible degrees are $\{1, 2, \ldots, n-1\}$. By the Pigeonhole Principle, applied to the function deg, there must be vertices u, v such that $\deg(u) = \deg(v)$. ∎

1.5 Where to go from here?

By design this course touches on a broad range of subjects, and for most manages only to scratch the surface. At the end of each chapter will be a section with references to textbooks that dive into the depths of the subject just treated. We will use this space in this chapter to list some texts with a broad scope.

- van Lint and Wilson (2001), *A Course in Combinatorics* is a very readable book containing 38 chapters on the most diverse topics. Notably missing from the treatment is the probabilistic method.
- Cameron (1994), *Combinatorics: Topics, Techniques, Algorithms* also doesn't feature the probabilistic method, has a similar (but smaller) range of topics, but includes more algorithmic results.
- Lovász (1993), *Combinatorial Problems and Exercises* is again a very broad treatment of combinatorics, but with a unique twist: the book is presented as a long list of problems. The second part contains hints for each problem, and the third a detailed solution.
- Jukna (2011), *Extremal Combinatorics* focuses mainly on extremal problems, but still covers a very wide range of techniques in doing so.
- Aigner and Ziegler (2010), *Proofs from THE BOOK* is a collection of the most beautiful proofs in mathematics. It has a significant section on combinatorics which is well worth reading.

Chapter 2

Counting

In this chapter we focus on enumerative combinatorics. This branch of combinatorics has, perhaps, the longest pedigree. It centers on the question "how many?" We will start by exploring what answering that question may mean.

2.1 Ways to report the count

Consider the following example:

2.1.1 Question. How many ways are there to write $n-1$ as an ordered sum of 1's and 2's?

This question illustrates the essence of enumeration: there is a set of objects (ordered sums of 1's and 2's), which is parametrized by an integer n (the total being $n-1$). What we are really looking for is a function $f : \mathbb{N} \to \mathbb{N}$, such that $f(n)$ is the correct answer for all n. For Question 2.1.1 we tabulated the first few values of $f(n)$ in Table 2.1.

n	sums totaling $n-1$	$f(n)$
0	-	0
1	0 (the empty sum)	1
2	1	1
3	2, 1+1	2
4	2+1, 1+2, 1+1+1	3
5	2+2, 2+1+1, 1+2+1, 1+1+2, 1+1+1+1	5

Table 2.1
Small values of $f(n)$ for Question 2.1.1

2.1.1 Recurrence relations

Often a first step towards solving a problem in enumerative combinatorics is to find a recurrence relation for the answer. In our example, we can divide the sums totaling n in two cases: those having 1 as last term, and those having 2 as last term. There are $f(n)$ different sums of the first kind (namely all sums totaling $n-1$, with a 1 added to the end of each), and $f(n-1)$ different sums of the second kind. So we find

$$f(n+1) = f(n) + f(n-1). \tag{2.1}$$

Together with the initial values $f(0) = 0$ and $f(1) = 1$ the sequence is uniquely determined.

With Equation (2.1) we have devised a straightforward way to compute $f(n)$ using roughly n additions. What we've gained is that we do not have to write down all the sums any more (as in the middle column of the table): only the numbers in the right column are needed, and in fact we need only remember the previous two rows to compute the next. So the recurrence relation gives us an *algorithm* to compute the answer for any value of n we want.

2.1.2 Generating function

Having the ability to compute a number does not mean we know all about it. Is the sequence monotone? How fast does it grow? For questions like these we have a very powerful tool, which at first sight may look like we are cheating: the *generating function*. A generating function is, initially, nothing but a formalism, a way to write down the sequence. We write down an infinite polynomial in x, where $f(n)$ is the coefficient of x^n:

$$F(x) := \sum_{n\geq 0} f(n)x^n.$$

Again, in spite of the notation, we do (for now) not see this as a function, just as a way to write down the sequence. In particular, we do not (yet) allow substitution of anything for x.

An interesting thing happens if we try to turn each side of the recurrence relation into a generating function. We multiply left and right by x^n, and sum over all values of n for which all terms are defined (in this case $n \geq 1$). This gives

$$\sum_{n\geq 1} f(n+1)x^n = \sum_{n\geq 1} f(n)x^n + \sum_{n\geq 1} f(n-1)x^n.$$

Next, we multiply both sides by x, and extract a factor of x from the last sum:

$$\sum_{n\geq 1} f(n+1)x^{n+1} = x\left(\sum_{n\geq 1} f(n)x^n + x\sum_{n\geq 1} f(n-1)x^{n-1}\right)$$

A change of variables in the first and third sum gives:

$$\sum_{m\geq 2} f(m)x^m = x\left(\sum_{n\geq 1} f(n)x^n + x\sum_{m\geq 0} f(m)x^m\right)$$

Finally we add terms to the sums to make all range from 0 to infinity:

$$\sum_{m\geq 0} f(m)x^m - f(0)x^0 - f(1)x^1 = x\left(\sum_{n\geq 0} f(n)x^n - f(0)x^0 + x\sum_{m\geq 0} f(m)x^m\right).$$

Now each of the sums equals $F(x)$. using what we know about $f(0)$ and $f(1)$ we find

$$F(x) - x = x(F(x) + xF(x))$$
$$F(x) = \frac{x}{1 - x - x^2},$$

where, in the last sequence, we could define $(1 - x - x^2)^{-1}$ to be "the generating function $G(x)$ such that $G(x)(1 - x - x^2) = 1$".

So far, we have only used the usual rules of polynomial addition and multiplication. But now we look at the expression on the right, and consider it a function over the real or complex numbers. There is an $\varepsilon > 0$ such that this function is defined for all $|x| < \varepsilon$, and it follows that $F(x)$ is actually the Taylor series of the function on the right around $x = 0$. Now we can use a huge range of tools to further analyze our function. In this case, we factor the denominator and use partial fraction expansion (we omit the details):

$$F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \tau_1 x)(1 - \tau_2 x)} = \frac{1}{\tau_1 - \tau_2}\left(\frac{1}{1 - \tau_1 x} - \frac{1}{1 - \tau_2 x}\right), \quad (2.2)$$

where

$$\tau_1 = \frac{1 + \sqrt{5}}{2}, \tau_2 = \frac{1 - \sqrt{5}}{2}.$$

The reason we went through all this trouble is because we want to express our generating function in terms of ones we "know". And the most famous generating function/Taylor series is of course the *geometric series:*

$$\frac{1}{1 - x} = \sum_{n \geq 0} x^n.$$

Applying this to the two terms on the right of Equation (2.2), we get

$$F(x) = \frac{1}{\tau_1 - \tau_2}\left(\sum_{n \geq 0} (\tau_1 x)^n - \sum_{n \geq 0} (\tau_2 x)^n\right) = \frac{1}{\sqrt{5}} \sum_{n \geq 0} (\tau_1^n - \tau_2^n) x^n,$$

which gives us a new and rather insightful expression for $f(n)$, almost for free!

2.1.3 Closed formula

Consider the following functions, each of which is the answer to a combinatorial counting problem:

$$f_1(n) = n^{n-2}$$
$$f_2(n) = n! \sum_{k=0}^{n} (-1)^k / k!$$
$$f_3(n) = \text{the nearest integer to } n!/e$$
$$f_4(n) = \frac{1}{\sqrt{5}}(\tau_1^n - \tau_2^n)$$

A function like f_1 is a completely satisfactory answer, but it is understandable that few problems admit solutions like this. We often need sums in the answer, as in f_2. This is still fairly acceptable, especially since (as we will see soon) the terms of the sum have combinatorial meaning: they correspond to certain partial counts! Formulas f_3 and f_4 are inherently non-combinatorial, since they involve terms that are not even rational numbers (let alone integers). However, such formulas can still be insightful, and may have a less cluttered appearance (case in point: $f_2 = f_3$).

We tend to refer to solutions that are pleasing as a solution in "closed form" or a "closed formula". We don't want to make that term precise, but definitely allowed are multiplication, division, addition, subtraction (each a finite number of times, independent of n), binomial coefficients with integers, exponentiation, and factorials. Sometimes (as in f_4), we are willing to accept arbitrary complex numbers.

While we don't consider f_2 to be a closed formula, it is still much more enlightening, and much easier to compute than listing all objects it counts (as we will see). For more convoluted sums, it becomes harder to see the value, and in fact it is possible to write sums so complicated that evaluating them is no better than listing all objects.

Closed formulas for generating functions may involve classical functions like sin, cos, exp, log, as well as exponentiation (including arbitrary real exponents) and multiplication, division, addition, subtraction.

2.1.4 Asymptotics

On occasion we are not interested in the exact count as much as we are interested in *asymptotics*. The quality of a formula for $f(n)$ can be tested by how easy it is to find its asymptotic behavior. Returning to our example, we see that $|\tau_2| < 1$, so the second term goes to zero. We write

$$f(n) \sim g(n)$$

to denote

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

So in our example,

$$f(n) \sim \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n.$$

It follows that $f(n)$ grows exponentially fast as a function of n.

2.2 Counting by bijection: spanning trees

The most satisfying way to count is to relate the objects you're counting to much simpler objects, or (ideally) to objects which you already know how to count. In this section we will see a classical example of this: Cayley's Theorem for counting the number of labeled spanning trees. That is, how many spanning trees are there on a fixed vertex set V? It is clear that the nature of the elements of V is not important: we may as well take $V = [n]$, so the answer only depends on the size of V. Denote the number by $t(n)$. As before, we start with a table. The way we generate the trees is by first (using ad-hoc

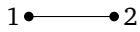
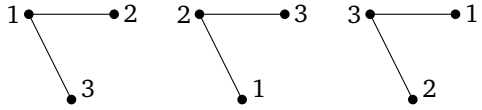
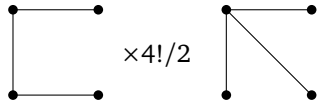
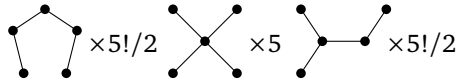
n	spanning trees	$t(n)$
1		1
2		1
3		3
4		16
5		125

TABLE 2.2
The number of labeled spanning trees for $n \leq 5$ vertices

methods) determining all possible *shapes* of trees ("unlabeled trees on n vertices"), and then finding all ways to assign the elements of V to their labels.

Interestingly, the numbers in the right are equal to n^{n-2}. Cayley proved that this is in fact true for all n:

2.2.1 THEOREM (Cayley's Theorem). *The number of spanning trees on a vertex set of size n is n^{n-2}.*

We will give two proofs of this important theorem. The first is a proof by bijection. We start by creating the *Prüfer code* $(y_1, \ldots, y_{n-1})$ of a tree T on vertex set $V = [n]$. This is done by recursively defining sequences $(x_1, \ldots, x_{n-1})$ and $(y_1, \ldots, y_{n-1})$ of vertices, and $(T_1, \ldots, T_{n-1})$ of trees, as follows:

- $T_1 := T$.
- For $1 \leq i \leq n-1$, let x_i be the degree-1 vertex of T_i having smallest index.
- For $1 \leq i \leq n-1$, let y_i be the neighbor of x_i in T_i.
- For $1 \leq i \leq n-2$, let $T_{i+1} := T_i - x_i$, that is, the tree obtained by removing vertex x_i and edge $\{x_i, y_i\}$.

2.2.2 EXAMPLE. Consider the tree in Figure 2.1. The sequence $(x_1, \ldots, x_9) = (3, 4, 2, 5, 6, 7, 1, 8, 9)$ and the sequence $(y_1, \ldots, y_9) = (2, 2, 1, 1, 7, 1, 10, 10, 10)$.

First proof of Theorem 2.2.1: Consider a Prüfer sequence $(y_1, \ldots, y_{n-1})$. Since each tree has at least two degree-1 vertices, vertex n will never be removed. Hence $y_{n-1} = n$. Pick $k \in \{1, \ldots, n-2\}$. Since only degree-1 vertices are removed, it follows that the degree of vertex v in tree T_k is one more than the number of occurrences of v among $(y_k, \ldots, y_{n-2})$. So the degree-1 vertices in T_k are precisely those vertices *not* occurring in

$$\{x_1, \ldots, x_{k-1}\} \cup \{y_k, \ldots, y_{n-2}\}. \tag{2.3}$$

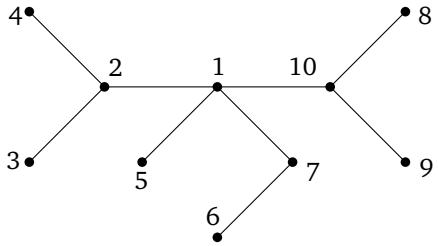


FIGURE 2.1
Labeled tree

Now x_k is the least element of $[n]$ not in the set (2.3). Note that such an element always exists, since set (2.3) has at most $n-2$ members. It follows that, from the sequence $(y_1,\ldots,y_{n-2})$, we can reconstruct

- $(y_1,\ldots,y_{n-1})$;
- $(x_1,\ldots,x_{n-1})$,

and therefore we can reconstruct $T_{n-1},\ldots,T_1 = T$ (in that order). Note that each tree gives a sequence, and each sequence allows us to reconstruct a unique tree (the process of re-attaching x_k to y_k is completely deterministic), so the number of sequences $(y_1,\ldots,y_{n-2})$ and the number of trees must be equal. The number of sequences is clearly n^{n-2}, since each y_i can take on n distinct values. ∎

The second proof is a clever construction that solves the problem through counting *more complicated* structures – a technique that comes up more often (even the handshake lemma can be seen as a simple instance of this). For digraphs and some basic facts regarding trees, see Appendix A. The proof is due to Pitman (1999), and the version below closely follows the one found in Aigner and Ziegler (2010).

Second proof of Theorem 2.2.1: A *rooted forest* is a set of trees, together with a marked vertex in each tree, called the *root* of that tree. Let $\mathscr{F}_{n,k}$ be the set of rooted forests on vertex set $[n]$ with precisely k trees. Pick a rooted forest F, let T be a tree of F with root r. For each vertex there is a unique path from the root to that vertex. It is not hard to see that the edges of T can be replaced by directed edges so that in the resulting digraph the root r is the only vertex without incoming edges. Moreover, this can be done in exactly one way, so we will identify the members of $\mathscr{F}_{n,k}$ with their directed counterparts. See Figure 2.2(a) for an example of a forest in $\mathscr{F}_{9,3}$.

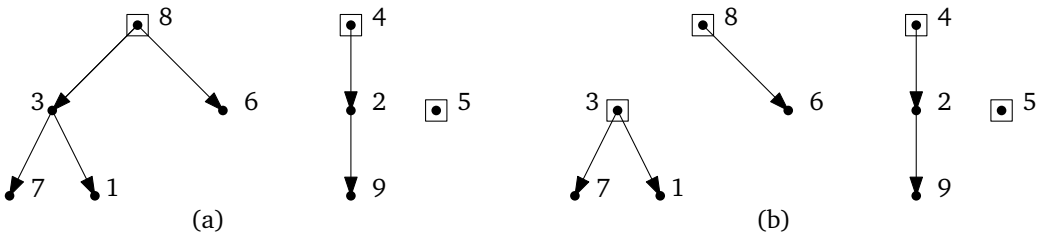


FIGURE 2.2
(a) A rooted forest with three trees and edges directed away from the roots; (b) A rooted forest with 4 trees contained in the rooted forest (a)

We say that a rooted forest F *contains* a rooted forest F' if F (seen as a digraph) contains F' (seen as a digraph). So all edges of F' are present in F, and directed the same way. In Figure 2.2, the rooted forest (a) contains the rooted forest (b). Now we define a *refining sequence* to be a sequence of rooted forests $(F_1, \ldots, F_k)$ such that $F_i \in \mathscr{F}_{n,i}$ (and therefore has i trees), and such that F_i contains F_{i+1}. For a fixed $F_k \in \mathscr{F}_{n,k}$ we define the following two counts:

- $t(F_k)$: the number of rooted trees containing F_k;
- $s(F_k)$: the number of refining sequences ending in F_k.

We are going to determine $s(F_k)$ by looking at a refining sequence from two sides: starting at F_k or starting at F_1. First, consider the set of rooted forests with $k-1$ trees that contain F_k. To obtain such a forest from F_k we must add a directed edge. This edge can start at any vertex v, but should end at a root r in a different tree from v. If r is in the same tree then we have introduced a cycle; if r is not a root then the containment relation fails since directions are not preserved. There are n choices for the start of this edge, and $(k-1)$ choices for the root in another tree. Hence there are $n(k-1)$ forests F_{k-1} containing F_k. For each such F_{k-1}, in turn, there are $n(k-2)$ forests F_{k-2} containing it. It follows that

$$s(F_k) = n^{k-1}(k-1)! \tag{2.4}$$

For the other direction, let F_1 be a fixed forest containing F_k. To produce a refining sequence starting in F_1 and ending in F_k, the edges in $E(F_1)\setminus E(F_k)$ need to be removed one by one. There are $k-1$ such edges, and every ordering gives a different refining sequence. There are $t(F_k)$ choices for F_1 by definition, so

$$s(F_k) = t(F_k)(k-1)! \tag{2.5}$$

By combining Equation (2.4) with (2.5) we find that $t(F_k) = n^{k-1}$.

To finish off, observe that $\mathscr{F}_{n,n}$ contains but a single member, F_n say: all trees in the forest are isolated vertices; and therefore all vertices are roots. It follows that $t(F_n)$ counts the number of rooted trees on n vertices. Since in each unrooted tree there are n choices for the root, we find that the number of trees is

$$t(F_n)/n = (n^{n-1})/n = n^{n-2}. \qquad \blacksquare$$

Different proofs yield different insights into a problem, and give different directions for generalizations. The proof using Prüfer codes can be refined, for instance, by restricting the allowable degrees of the vertices. The second proof can be used, without too much trouble, to find the number of forests with k trees:

2.2.3 THEOREM. *The number of forests with k trees on a vertex set of size n is kn^{n-k-1}.*

Proof: For a rooted forest $F_k \in \mathscr{F}_{n,k}$, define $s'(F_k)$ to be the number of refining sequences $(F_1, \ldots, F_n)$ having F_k as kth term. Each such sequence starts with a refining sequence $F_1, \ldots, F_k$ (of which there are $s(F_k) = n^{k-1}(k-1)!$, by the above), and each can be completed by deleting the remaining edges of F_k one by one. There are $(n-k)$ such edges, and they can be ordered in $(n-k)!$ ways. Hence $s'(F_k) = n^{k-1}(k-1)!(n-k)!$. Note that this number is the same for all F_k, so we find that

$$|\mathscr{F}_{n,k}| = \frac{\text{number of refining sequences } F_1, \ldots, F_n}{\text{number of refining sequences using } F_k} = \frac{s(F_n)}{s'(F_k)} = \binom{n}{k} kn^{n-1-k}.$$

By observing that the k roots can be chosen in $\binom{n}{k}$ ways, the number of unrooted forests with k trees on n vertices is kn^{n-k-1} as claimed*. ∎

We will see yet another proof of Cayley's formula in Section 5.6. As a teaser, compute the determinant of the $(n-1)\times(n-1)$ matrix

$$\begin{bmatrix} n-1 & -1 & \cdots & -1 \\ -1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & n-1 \end{bmatrix}.$$

2.3 The Principle of Inclusion/Exclusion

Given a set A and subsets A_1 and A_2, how many elements are in A but not in either of A_1 and A_2? The answer, which is easily obtained from a Venn diagram, is $|A| - |A_1| - |A_2| + |A_1 \cap A_2|$. The Principle of Inclusion/Exclusion (P.I.E.) is a generalization of this formula to n sets. It will be convenient to introduce some notation: for $V \subseteq [n]$, denote

$$A_V := \bigcap_{i\in V} A_i.$$

2.3.1 THEOREM (Principle of Inclusion/Exclusion). *Let A be a finite set, and $A_1,\ldots,A_n$ subsets of A. Then*

$$\left|A \setminus \left(\bigcup_{i=1}^{n} A_i\right)\right| = \sum_{V\subseteq[n]} (-1)^{|V|}|A_V|. \tag{2.6}$$

Proof: We take the right-hand side of (2.6) and rewrite it, thus showing it is equal to the left-hand side. Start by writing each set size as

$$|X| = \sum_{a\in X} 1.$$

In the right-hand side of (2.6), each element $a \in A$ will now contribute to a number of terms, sometimes with a plus sign, sometimes with a minus. We consider the contribution of a to each of the numbers $|A_V|$. Assume that a occurs in m of the sets A_i. Then $a \in A_V$ if and only if $a \in A_i$ for all $i \in V$. This can only happen if V is a subset of the m integers indexing sets containing a. There are precisely $\binom{m}{k}$ subsets of these indices with exactly k elements. It follows that the contribution of a to the sum is

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} = (1-1)^m = \begin{cases} 0 & \text{if } m > 0 \\ 1 & \text{if } m = 0, \end{cases}$$

where we used the binomial theorem and the fact that $0^0 = 1$. It follows that a contributes to the sum if and only if a is in none of the subsets A_i, and the result follows. ∎

*This last line is a bit subtle!

The Principle of Inclusion/Exclusion replaces the computation of the size of one set by a sum of lots of sizes of sets. To actually make progress in determining the count, it is essential to choose the sets A_i with care. This is best illustrated through a few examples.

2.3.2 PROBLEM (Derangements). Suppose n people pick up a random umbrella from the cloakroom. What is the probability that no person gets their own umbrella back?

More mathematically, we wish to determine the number of permutations $\pi : [n] \to [n]$ without a fixed point. A fixed point is an $x \in [n]$ such that $\pi(x) = x$.

Let $A := S_n$, the set of all permutations of $[n]$, and for each $i \in [n]$, define

$$A_i := \{\pi \in A : \pi(i) = i\}.$$

Clearly $|A| = n!$. For a permutation in A_i the image of i is fixed, but the remaining elements can be permuted arbitrarily, so $|A_i| = (n-1)!$. Similarly, $|A_V| = (n-|V|)!$. Note that we've parametrized so that we specify the image of certain members of A. This is important: the size of a set like "all permutations having precisely i fixed points" is as hard to determine as the original problem! Now we find

$$|A \setminus (A_1 \cup \cdots \cup A_n)| = \sum_{V \subseteq [n]} (-1)^{|V|}(n-|V|)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

where the first equality is the P.I.E., and the second uses the (commonly occurring) fact that $|A_V|$ depends only on the size of V, not on the specific elements in V. Then we use that there are exactly $\binom{n}{k}$ subsets V of size k. The final equality is just rearranging terms.

Now the probability that a random permutation is a derangement is

$$\sum_{k=0}^{n} \frac{(-1)^k}{k!} \xrightarrow[n\to\infty]{} \frac{1}{e}.$$

In fact, one can show that the number of derangements equals the closest integer to $n!/e$.

2.3.3 PROBLEM. Determine the number $T(n,k)$ of surjections $f : N \to K$ where $|N| = n$ and $|K| = k$.

A *surjection* is an expensive name for a function that is *onto*. For ease of notation, assume $N = [n]$ and $K = [k]$. Let's define A to be the set of all maps $N \to K$, and for $i \in [k]$ define

$$A_i := \{f \in A : \text{no element mapped to } i\}.$$

Then $|A| = k^n$, since each element of N can be mapped to any of the elements of K. If no element gets mapped to i, then only $k-1$ choices are left, so $|A_i| = (k-1)^n$; likewise $|A_V| = (k-|V|)^n$. This gives

$$T(n,k) = \sum_{V \subseteq [k]} (-1)^{|V|}(k-|V|)^n = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

We will look at these, and related, numbers later in this chapter.

For a third application of the Principle of Inclusion/Exclusion we refer to Section 2.6.

2.4 Generating functions

Generating functions form a powerful and versatile tool in enumerative combinatorics. In this overview course we barely scratch the surface of the field. We will mostly employ them for two purposes:

- Solve recurrence relations
- Decompose a counting problem into easier problems

We've seen an example of the first kind above, where we found an expression for the Fibonacci sequence. The second kind will lead to taking *products* of generating functions. We give another example.

2.4.1 EXAMPLE. In how many ways can change worth n cents be given using a combination of pennies and nickels?

Let a_n denote the number of ways to give change from n cents using only pennies. Let b_n be the number of ways to give change from n cents using only nickels. Clearly $a_n = 1$ for all $n \geq 0$, and $b_n = 1$ if n is divisible by 5, and 0 otherwise. Write

$$A(x) := \sum_{n\geq 0} a_n x^n = 1 + x + x^2 + \cdots = \frac{1}{1-x}.$$
$$B(x) := \sum_{n\geq 0} b_n x^n = 1 + x^5 + x^{10} + \cdots = \frac{1}{1-x^5}.$$

Now if we want to combine pennies and nickels, we could first allocate the number of pennies, say k, and use nickels for the remainder. So the desired answer will be $\sum_{k=0}^{n} a_k b_{n-k}$. If we look at the product of the generating functions, we get

$$A(x)B(x) = \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n,$$

so the coefficient of x^n contains exactly the right answer! Note that we can accommodate lots of extra side conditions in this method: use only an odd number of dimes, use up to twelve nickels, and so on.

This decomposition into simpler problems is usually most successful in an *unlabeled* context. For labeled problems often the *exponential generating function* is a better tool.

2.4.2 DEFINITION. Let $(f_0, f_1, \ldots)$ be a sequence of integers. The *exponential generating function* of this sequence is

$$\sum_{n\geq 0} f_n \frac{x^n}{n!}.$$

The most famous exponential generating function is the one with sequence $(1, 1, \ldots)$. We denote it by $\exp(x)$, or sometimes e^x.

Consider the product of two exponential generating functions $A(x)$ and $B(x)$:

$$A(x)B(x) = \sum_{n\geq 0}\left(\sum_{k=0}^{n}\frac{a_k}{k!}\frac{b_{n-k}}{(n-k)!}\right)x^n = \sum_{n\geq 0}\left(\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}\right)\frac{x^n}{n!}.$$

The term

$$\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}$$

can be interpreted as assigning values to *labeled* items using processes a and b. An example should make this more concrete:

2.4.3 EXAMPLE. How many strings of length n are there using the letters $\{a, b, c\}$, where
- a is used an odd number of times;
- b is used an even number of times;
- c is used any number of times?

The exponential generating function if we only use the symbol c is easy:

$$C(x) = \sum_{n\geq 0} 1\cdot\frac{x^n}{n!} = \exp(x).$$

If we use only the symbol b then we can do it in one way if the string length is even, and in no way if the length is odd:

$$B(x) = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots = \frac{\exp(x)+\exp(-x)}{2}$$

Similarly, if we use only a:

$$A(x) = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots = \frac{\exp(x)-\exp(-x)}{2}$$

Using both a's and b's, we can first select the positions in which we want the symbol a, and fill the remaining positions with the symbol b. This gives $\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}$ strings – precisely the coefficient of x^n in $A(x)B(x)$. This product gives

$$A(x)B(x) = \frac{\exp(x)^2 - \exp(-x)^2}{4}.$$

Similarly, if we use a's, b's, and c's, we first select where the a's and b's go, and fill the remaining positions with c's. We find

$$A(x)B(x)C(x) = \frac{\exp(3x)-\exp(-x)}{4},$$

from which we deduce easily that the answer is $(3^n - (-1)^n)/4$ strings.

This cursory treatment does little justice to the theory of generating functions. We hope the examples above, and several more that will appear below, suffice to get some feeling for the uses of this powerful tool, and that common mathematical sense will do the rest. At the end of this chapter we present some suggestions for further reading.

2.5 The Twelvefold Way

In this section we will consider a number of elementary counting problems that can be applied in a diverse set of contexts. Specifically, let N and K be finite sets, with sizes $|N| = n$ and $|K| = k$. We wish to count the number of functions $f : N \to K$, subject to a number of conditions:

- f can be unrestricted, or surjective (onto), or injective (one-to-one);
- N can consist of labeled/distinguishable objects, or of unlabeled objects;
- K can consist of labeled or unlabeled objects.

In the unlabeled case, formally we count *equivalence classes* of functions. For instance, if N is unlabeled, then two functions f, g are considered equivalent if there is a permutation π of N such that $f = g \circ \pi$ (where $\circ$ denotes function composition). More intuitively: we think of a labeled set N as a set of numbers, and of an unlabeled set as a set of eggs; we think of a labeled set K as a set of paint colors, and of an unlabeled set K as a set of identical jars (so shuffling them around does not change the function).

The combinations of these choices lead to twelve counting problems, which are known as The Twelvefold Way. The results are summarized in Table 2.3.

N	K	any f	injective f	surjective f
labeled	labeled	k^n	$(k)_n$	$k!S(n,k)$
unlabeled	labeled	$\binom{n+k-1}{k-1}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$
labeled	unlabeled	$S(n,1)+\cdots+S(n,k)$	$\begin{cases} 1 & \text{if } k \geq n \\ 0 & \text{if } k < n \end{cases}$	$S(n,k)$
unlabeled	unlabeled	$p_k(n+k)$	$\begin{cases} 1 & \text{if } k \geq n \\ 0 & \text{if } k < n \end{cases}$	$p_k(n)$

TABLE 2.3
The Twelvefold Way

We will work our way through them in decreasing order of satisfaction, as far as the answer is concerned. Table 2.4 shows in which subsection a result can be found. Along the way we will look at some related problems too.

N	K	any f	injective f	surjective f
labeled	labeled	2.5.1	2.5.1	2.5.3
unlabeled	labeled	2.5.2	2.5.1	2.5.2
labeled	unlabeled	2.5.3	2.5.1	2.5.3
unlabeled	unlabeled	2.5.4	2.5.1	2.5.4

TABLE 2.4
The Twelvefold Way: subsection reference

2.5.1 Easy cases

We start with both N and K labeled, and no restrictions on f. In that case there are k choices for the first element of N, then k choices for the second, and so on. The total number of functions is therefore k^n.

If f is injective, then each element of K can be the image of at most one element from N. This means we have k choices for the image of the first element of N, then $(k-1)$ choices for the second, and so on. The total number of injective functions is therefore

$$(k)_n := k(k-1)\cdots(k-n+1),$$

which is sometimes called the *falling factorial*.

Next, suppose f is still injective but N is unlabeled. Then – going with the eggs and paint analogy – all that matters is which paints get used: we get to paint at most one egg with each color anyway. This results in a number

$$\binom{k}{n}$$

of injective functions f. Note that, if we decide to label N after all, this can be done in $n!$ ways, which gives a combinatorial explanation of

$$\binom{k}{n} = \frac{(k)_n}{n!}.$$

If K is unlabeled and f injective, then – going with the jar analogy – we need to put each element of N into its own jar; since jars are indistinguishable, the only condition is that there are enough jars, in which case there is 1 such function; otherwise there are none. This completes the first entry of the table, as well as the second column.

2.5.2 Painting eggs

Now we finish off the row with unlabeled N and labeled K. This problem can be interpreted as painting n eggs with set of colors K. First we consider the case without restrictions on f. Let us call the number to be found $e(n,k)$ for the moment. In exploring this problem we can start once more with a table, hoping for inspiration: The first

$k\backslash n$	0	1	2	3	4	5
0	1	0	0	0	0	0
1	1	1	1	1	1	1
2	1	2	3	4	5	
3	1	3	6	10		
4	1	4	10			
5	1	5				
6	1					

TABLE 2.5
Painting eggs

column, as well as the first two rows, are easy to find. Further down the table seems to take on the shape of Pascal's triangle! This suggest the following recursion should be true:

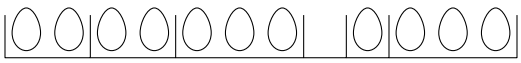
$$e(n,k) = e(n,k-1) + e(n-1,k).$$

This can be proven as follows: consider painting n eggs with k colors. How many times is the last color used? If it is not used at all, then we are painting n eggs with $k-1$ colors; if it is used at least once, then we can paint one egg with that color, put that egg aside, and continue painting the remaining $n-1$ eggs with k colors.

We now know that $e(n,k)$ is related to binomial coefficients, and it is not too hard to find

$$e(n,k) = \binom{n+k-1}{k-1}.$$

One can check that this satisfies both the recursion and the boundary conditions (the first row/column). But there is a more interesting and direct proof. We can imagine the colors as being boxes in which we put the eggs. The boxes are put in a fixed order, since the paints are distinguishable. A stylized picture of that situation is the following:



If we forget about the outermost lines (since they are always there anyway), and squint, we suddenly see something completely different:

0010010001101000

Here we have a string of $n+k-1$ symbols (n "eggs" and $k-1$ "walls"), of which $k-1$ symbols are "walls". And $e(n,k)$ is precisely the number of such objects!

Finally, let us look at surjective f. In that case each color is used at least once. Inspired by the way we arrived at the recursion, we can simply start by painting one egg with each color (this takes care of k eggs), and paint the remaining eggs arbitrarily. This gives

$$\binom{(n-k)+k-1}{k-1} = \binom{n-1}{k-1}$$

surjective functions. We note for use below that this number is equal to the number of solutions to

$$x_1 + x_2 + \cdots + x_k = n$$

in positive integers $x_1, \ldots, x_k$.

2.5.3 Stirling Numbers of the first and second kind

We have already determined the number $T(n,k)$ of surjections $N \to K$ in Section 2.3, but here is a different derivation using exponential generating functions. We write

$$F_k(x) = \sum_{n \geq 0} T(n,k) \frac{x^n}{n!}.$$

Again we interpret the problem as the number of ways to paint n integers using k colors, using each color at least once. If $k = 1$ then we can paint any set containing at least one element in exactly one way. So we find

$$F_1(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!} = \exp(x) - 1.$$

For $k = 2$, we can first pick i items from N to paint with color 2; all remaining items get painted with color 1. The number of ways to do this is

$$\sum_{i=1}^{n-1} \binom{n}{i} = \begin{cases} 2^n - 2 & \text{if } n > 0 \\ 0 & \text{else.} \end{cases}$$

Looking back at the multiplication formula for exponential generating functions, and remembering that the constant term of $F_1(x)$ is zero, we find

$$F_2(x) = F_1(x)F_1(x) = (\exp(x) - 1)^2.$$

Likewise,

$$F_k(x) = F_{k-1}(x)F_1(x) = (\exp(x) - 1)^k.$$

This can, in turn, be expanded to

$$F_k(x) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j \exp(x)^{k-j},$$

from which we read off

$$T(n,k) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j (k-j)^n$$

as before.

Next, what happens if K is *unlabeled*? Since each jar has at least one item from N in it, and those items are labeled, there are $k!$ different ways to put labels back on the jars for each function. So if we call the number we are looking for $S(n,k)$, then

$$S(n,k) = \frac{T(n,k)}{k!}.$$

As can be guessed from the way we filled Table 2.3, the numbers $S(n,k)$ are more fundamental than the $T(n,k)$. The $S(n,k)$ are known as *Stirling numbers of the second kind*. We note a few facts:

2.5.1 LEMMA. *The Stirling numbers of the second kind satisfy the following recursion:*

$$S(n,k) = kS(n-1,k) + S(n-1,k-1).$$

2.5.2 LEMMA. *The following holds for all integers $n, x \geq 0$:*

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k.$$

We leave the recursion as an exercise; to see the second lemma, count the functions $[n] \to [x]$ in two ways. Clearly there are x^n of them. Now count them, split up by the image of f. If this image equals Y for some set Y of size k, then there are $k!S(n,k)$ surjections $[n] \to Y$. Moreover, there are $\binom{x}{k}$ ways to choose such a set Y, giving

$$x^n = \sum_{k=0}^{n} \binom{x}{k} k!S(n,k)$$

from which the result follows.

This same idea can be used to fill up the entry corresponding to unrestricted functions $f : N \to K$ with K unlabeled: split the count up by the image of f. Since K is unlabeled, in this case only the size counts, immediately giving

$$S(n,1) + S(n,2) + \cdots + S(n,k).$$

Now let's look at the Stirling numbers of the *first* kind, which will be denoted by $s(n,k)$. We will start by determining a closely related set of numbers. Let $c(n,k)$ be the number of permutations with exactly k cycles[†]

Note that the total number of permutations is $n!$. We can determine without difficulty that

- $c(0,0) = 1$;
- $c(0,k) = 0$ for $k > 0$;
- $c(n,0) = 0$ for $n > 0$;
- $c(n,1) = (n-1)!$ for $n \geq 0$.

From the last line we conclude

$$\sum_{n\geq 0} c(n,1)\frac{x^n}{n!} = \sum_{n\geq 1} \frac{x^n}{n} = -\log(1-x).$$

Using the same reasoning as above for $F_k(x)$ (and correcting for the fact that cycles are unordered, i.e. unlabeled), we find

$$\sum_{n\geq 0} c(n,k)\frac{x^n}{n!} = \frac{1}{k!}(-\log(1-x))^k.$$

An interesting formula for these numbers is the following

2.5.3 LEMMA. *The number $c(n,k)$ of permutations of $[n]$ with exactly k cycles equals the coefficient of y^k in*

$$(y+n-1)(y+n-2)\cdots(y+1)y.$$

Sketch of proof: This is easy to obtain by exchanging sums in the expression

$$\sum_{m\geq 0} (-\log(1-x))^m \frac{y^m}{m!}.$$ ∎

[†]You may want to refresh your mind regarding cycle notation of permutations.

Now the Stirling numbers of the first kind are *signed* versions of the numbers $c(n,k)$:

$$s(n,k) := (-1)^{n+k} c(n,k).$$

The following results can be deduced (we omit the proofs):

2.5.4 LEMMA.

$$\sum_{n\geq 0} s(n,k)\frac{x^n}{n!} = \frac{1}{k!}(\log(1+x))^k.$$

2.5.5 LEMMA. *For all integers $n, x \geq 0$ we have*

$$\sum_{k=0}^{n} s(n,k)x^n = (x)_n.$$

Now by either substituting one exponential generating function into the other, or by substituting the result from one of Lemmas 2.5.5 and 2.5.2 into the other, we obtain the following

2.5.6 THEOREM. *Consider the infinite matrices A and B, where $A_{n,k} = S(n,k)$ and $B_{n,k} = s(n,k)$ for all $n,k \geq 0$. Then*

$$AB = BA = I_\infty,$$

where I_∞ is an infinite matrix with ones on the diagonal and zeroes elsewhere.

2.5.4 Partitions

Finally we arrive at the case where both N and K are unlabeled. This problem can be seen as *partitioning* a stack of eggs. Note that the parts are indistinguishable, so only the number of parts of a certain size counts. We denote by $\overline{p}_k(n)$ the number of partitions with at most k parts, and by $p_k(n)$ the number of partitions with *exactly* k parts. These numbers are related: if we set apart k eggs, one to be put in each part, then we can distribute the remaining eggs without restriction, so

$$p_k(n) = \overline{p}_k(n-k)$$
$$\overline{p}_k(n) = p_k(n+k).$$

A recursion for $p_k(n)$ can be found as follows: we distinguish whether there is a part of size one (in which case the remaining $n-1$ eggs are divided into $k-1$ parts) or not (in which case we can remove one egg from each part and still have k parts). This leads to

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k).$$

We can visualize a partition by a *Ferrers diagram* (see Figure 2.3), where each row corresponds to a part of the partition, and the rows are sorted in order of decreasing length. The *shape* of the diagram is the vector λ of row lengths.

We will determine the generating function of $\overline{p}_k(n)$. Note that $\overline{p}_k(n)$ counts the number of Ferrers diagrams with n dots and at most k rows. The key observation is that this is equal to the number of Ferrers diagrams with n dots and at most k dots

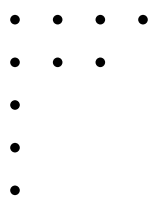


FIGURE 2.3
Ferrers diagram of shape $\lambda = (4,3,1,1,1)$.

per column! The Ferrers diagram is uniquely determined by specifying, for all i, the number α_i of columns of length i. Therefore $\overline{p}_k(n)$ is the number of solutions to

$$\alpha_1 + 2\alpha_2 + \cdots + k\alpha_k = n.$$

With this we find (by changing the order of summation around):

$$\begin{aligned}\sum_{n\geq 0}\overline{p}_k(n) &= \sum_{n\geq 0}\sum_{\substack{\alpha_1,\ldots,\alpha_k:\\ \alpha_1+\cdots+k\alpha_k=n}} 1\cdot x^n \\ &= \sum_{\alpha_1\geq 0}\sum_{\alpha_2\geq 0}\cdots\sum_{\alpha_k\geq 0} x^{\alpha_1+2\alpha_2+\cdots+k\alpha_k} \\ &= \left(\sum_{\alpha_1\geq 0} x^{\alpha_1}\right)\left(\sum_{\alpha_2\geq 0} x^{2\alpha_2}\right)\cdots\left(\sum_{\alpha_k\geq 0} x^{k\alpha_k}\right) \\ &= \prod_{i=1}^{k}\frac{1}{1-x^i}.\end{aligned}$$

Note that we can obtain a generating function for the number $p(n)$ of partitions of the integer n by letting k go to infinity:

$$\sum_{n\geq 0} p(n)x^n = \prod_{i=1}^{\infty}\frac{1}{1-x^i}.$$

Recall that we have $T(n,k) = k!S(n,k)$. No such relationship exists between $p_k(n)$ and $\binom{n-1}{k-1}$, but we can show that, if we fix k and let n grow, then asymptotically this is still close to being true:

2.5.7 THEOREM. *For fixed k,*

$$p_k(n) \sim \frac{n^{k-1}}{k!(k-1)!}.$$

Proof: We start by establishing a lower bound. If we impose an order on the parts of the partition, we get a solution of

$$x_1 + x_2 + \cdots + x_k = n$$

in positive integers. The number of solutions is equal to the number of surjections $N \to [k]$ with N unlabeled, so $\binom{n-1}{k-1}$. But if two parts have the same size, then this

solution is generated twice in the process of imposing an order on the partition, so we overcount:

$$k!p_k(n) \geq \binom{n-1}{k-1}. \tag{2.7}$$

For the converse we do a trick. Consider $p_k(n)$ as the number of solutions to

$$x_1 + x_2 + \cdots + x_k = n$$
$$x_1 \geq x_2 \geq \cdots \geq x_k \geq 1$$

Given such a solution, define

$$y_i := x_i + k - i.$$

We find that

$$y_{i+1} = x_{i+1} + k - i - 1 \leq x_i + k - i - 1 = y_i - 1,$$

so the y_i are all different. Clearly they add up to $n + \frac{k(k-1)}{2}$. It follows that each way to order the y_i gives a distinct solution to

$$y_1 + y_2 + \cdots + y_k = n + \frac{k(k-1)}{2}.$$

We know the total number of solutions to this equation, so we find

$$k!p_k(n) \leq \binom{n + \frac{k(k-1)}{2} - 1}{k-1}. \tag{2.8}$$

Both bounds (2.7) and (2.8) are dominated by the term $\frac{n^{k-1}}{(k-1)!}$, from which the result follows. ∎

2.6 Le problème des ménages

In this section we look at a very classical problem from combinatorics that can be solved using ideas introduced in this chapter. The problem is commonly known by its French name, "Le Problème des Ménages", and goes as follows:

> Des femmes, en nombre n, sont rangées autour d'une table dans un ordre déterminé; on demande quel est le nombre des manières de placer leurs maris respectifs, de telle sorte qu'un homme soit placé entre deux femmes sans se trouver à côté de la sienne?
>
> —Lucas (1891, p. 215)

In English, this can be recast as follows:

2.6.1 PROBLEM. A total of n couples (each consisting of a man and a woman) must be seated at a round table such that men and women alternate, women sit at odd-numbered positions, and no woman sits next to her partner. How many seating arrangements are possible?

Note that we have changed the problem slightly: Lucas has already seated the women and only asks in how many ways we can seat the men. The solution to Lucas' problem will be our solution to Problem 2.6.1 divided by $n!$. This change will, in fact, make the problem easier to deal with. We assume that the seats are distinguishable (i.e. they are numbered).

Let us start by giving names to things. Let $1, \ldots, n$ be the set of couples, and let A be the set of all seating arrangements in which women occupy the odd-numbered positions. We are looking at the members in A for which no couple is seated side-by-side, so it is natural to try the Principle of Inclusion/Exclusion. For $V \subseteq [n]$, denote by A_V the set of arrangements in which the couples in set V break the rule. By symmetry, the size $|A_V|$ depends only on the size of V, not on the specific choice of couples. So, if $|V| = k$, denote $a_k := |A_V|$. By the Principle of Inclusion/Exclusion we find that the number we want is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} a_k. \tag{2.9}$$

Next, denote by b_k the number of ways in which k disjoint pairs of side-by-side chairs can be picked. See Figure 2.4 for such an arrangement. Then

$$a_k = b_k k!(n-k)!(n-k)!, \tag{2.10}$$

since our k "bad" couples can be arranged over the bad pairs of seats in $k!$ ways; after that we can seat the remaining women in $(n-k)!$ ways, and the remaining men in $(n-k)!$ ways.

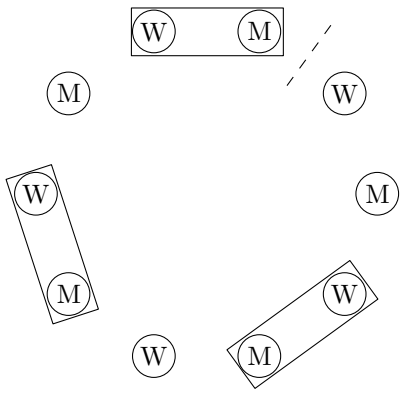
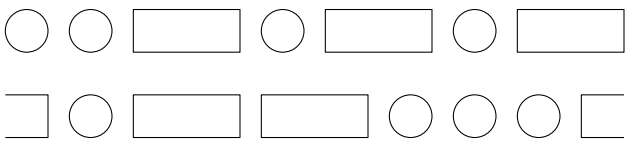


FIGURE 2.4
A seating arrangements with three known couples sitting side-by-side.

It remains to determine b_k. Cut the circle open at a fixed point. We can erase the letters in the circles (since they are fixed anyway), and the circles inside the rectangles (since there are two anyway) to get a picture of one of the following types:



In the first we have a sequence of $2n-k$ symbols, k of which are boxes, and the remaining being circles. There are, of course, $\binom{2n-k}{k}$ such sequences. In the second, ignoring the box split over the first and last position, we have $2n-k-1$ symbols, $k-1$ of which are boxes. It follows that

$$b_k = \binom{2n-k}{k} + \binom{2n-k-1}{k-1} = \binom{2n-k}{k} + \frac{k}{2n-k}\binom{2n-k}{k} = \frac{2n}{2n-k}\binom{2n-k}{k}. \tag{2.11}$$

Combining (2.11), (2.10) and (2.9) and simplifying a little, we get the solution

$$n!\sum_{k=0}^{n} \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!(-1)^k.$$

2.7 Young Tableaux

If we take a Ferrers diagram and replace the dots by squares, then we get a *Young diagram*. This change is interesting enough to warrant its own name, because new avenues open up: we get boxes that we can fill! In this section we will fill them in a very specific way:

2.7.1 DEFINITION. A *Young Tableau* of shape λ is

- a Young Diagram of shape λ...
- ... filled with the numbers 1 to n, each occurring once...
- ... such that each row and each column is increasing.

See Figure 2.5(a) for an example. Young Tableaux play an important role in the theory of representations of the symmetric group. In this section we will content ourselves with counting the number $f(n_1,\dots,n_m)$ of tableaux of a specific shape $\lambda = (n_1,\dots,n_m)$. We start by finding a recursion.

2.7.2 LEMMA. *f satisfies*

(i) $f(n_1,\dots,n_m) = 0$ *unless* $n_1 \geq n_2 \geq \cdots \geq n_m \geq 0$;

(ii) $f(n_1,\dots,n_m,0) = f(n_1,\dots,n_m)$;

(iii) $f(n_1,\dots,n_m) = f(n_1-1,n_2,\dots,n_m) + f(n_1,n_2-1,n_3,\dots,n_m) + \cdots + f(n_1,\dots,n_{m-1},n_m-1)$ *if* $n_1 \geq n_2 \geq \cdots \geq n_m \geq 0$;

(iv) $f(n) = 1$ *if* $n \geq 0$.

Moreover, these four properties uniquely determine f.

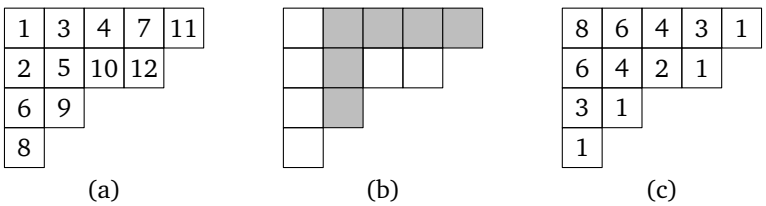


FIGURE 2.5
(a) A Young tableau; (b) A hook; (c) Hook lengths.

Proof: Properties (*i*), (*ii*) and (*iv*) are easily verified. For (*iii*), observe that the box containing the number n must be the last box in one of the rows. Removing that box gives the recursion (with terms being 0 if n is not also the last in its column). Clearly we can compute $f(n_1,\ldots,n_m)$ recursively from these conditions. ∎

There is a very nice description of f. It uses another definition:

2.7.3 DEFINITION. A *hook* of a Young tableau is a cell, together with all cells to the right of it, and all cells below it. The *hook length* is the number of cells in a hook.

See Figure 2.5(b) for an example of a hook; in Figure 2.5(c) the number in each cell denotes the length of the corresponding hook.

2.7.4 THEOREM (Hook Length Formula). *The number of Young tableaux of shape $\lambda = (n_1,\ldots,n_m)$, with total number of cells n, equals $n!$ divided by the product of all hook lengths.*

Our goal will be to prove this theorem. Unfortunately the best way to do this is by reformulating it in somewhat less attractive terms:

2.7.5 THEOREM.

$$f(n_1,\ldots,n_m) = \frac{\Delta(n_1+m-1, n_2+m-2,\ldots,n_m)\cdot n!}{(n_1+m-1)!(n_2+m-2)!\cdots n_m!}, \tag{2.12}$$

where

$$\Delta(x_1,\ldots,x_m) = \prod_{1\le i<j\le m}(x_i - x_j).$$

Proof that Theorem 2.7.5 implies Theorem 2.7.4: Consider a Young diagram with the hook length written in each cell. The first entry in the first row is n_1+m-1. The second entry in the first row would be n_1+m-2, except if the second column is shorter than the first. In fact, the first missing number will be $(n_1+m-1)-n_m$. After that the sequence continues until we run out of cells in row $m-1$, at which point the term $(n_1+m-1)-(n_{m-1}+1)$. We see that the first row contains the numbers $1,2,\ldots,n_1+m-1$, except for $(n_1+m-1)-(n_j+m-j)$ for $2\le j\le m$. This argument can be repeated for each row, showing the product of all hook lengths to be

$$\frac{(n_1+m-1)!(n_2+m-2)!\cdots n_m!}{\Delta(n_1+m-1, n_2+m-2,\ldots,n_m)},$$

from which the Hook Length Formula follows. ∎

The proof of Theorem 2.7.5 follows by showing that formula (2.12) satisfies all four properties of Lemma 2.7.2. For the third condition the following lemma will be very useful:

2.7.6 LEMMA. *Define*

$$g(x_1,\ldots,x_m;y) := x_1\Delta(x_1+y,x_2,\ldots,x_m) + x_2\Delta(x_1,x_2+y,\ldots,x_m) + \cdots + x_m\Delta(x_1,\ldots,x_m+y).$$

Then

$$g(x_1,\dots,x_m;y)=\left(x_1+\cdots+x_m+\binom{m}{2}y\right)\Delta(x_1,\dots,x_m).$$

Proof: Observe that g is a homogeneous polynomial of degree one more than the degree of $\Delta(x_1,\dots,x_m)$. Swapping x_i and x_j changes the sign of g (since Δ can be seen to be alternating). Hence if we substitute $x_i=x_j=x$ then g becomes 0. It follows that x_i-x_j divides g. Hence $\Delta(x_1,\dots,x_m)$ divides g. The result clearly holds if we substitute $y=0$, so it follows that we need to find a constant c such that

$$g(x_1,\dots,x_m;y)=(x_1+\cdots+x_m+cy)\Delta(x_1,\dots,x_m).$$

If we expand the polynomial and focus on the terms containing y, we find

$$\frac{x_iy}{x_i-x_j}\Delta(x_1,\dots,x_m)\qquad\text{and}\qquad\frac{-x_jy}{x_i-x_j}\Delta(x_1,\dots,x_m)$$

for $1\le i<j\le m$. Summing these gives the desired result. ∎

Proof of Theorem 2.7.5: As mentioned, we only need to show that formula (2.12) satisfies all four properties of Lemma 2.7.2. The first, second, and fourth properties are straightforward; for the third, use Lemma 2.7.6 with $x_1=n_1+m-1,\dots,x_m=n_m$ and $y=-1$. ∎

2.8 Where to go from here?

Enumerative combinatorics is one of the older branches of combinatorics, and as such there is a wealth of literature available. Moreover, most textbooks on combinatorics will contain at least some material on the subject. We mention a few more specialized books.

- Wilf (1994), *Generatingfunctionology* illustrates the versatility of generating functions in tackling combinatorial problems. It is available as a free download too!
- Flajolet and Sedgewick (2009), *Analytic Combinatorics* takes the analytic viewpoint of generating functions and runs with it.
- Stanley (1997), *Enumerative Combinatorics. Vol. 1* is an extensive treatment of the field of enumerative combinatorics. The text is aimed at graduate students.
- Goulden and Jackson (1983), *Combinatorial Enumeration* is another thorough, graduate-level text that starts with a formal development of the theory of generating functions. Both this volume and Stanley's books are considered classics.

Finally a resource that is not a book: the Online Encyclopedia of Integer Sequences is exactly what it says on the box. Input the first few terms of a sequence, hit the search button, and you will be presented with a list of all sequences in the database containing yours, together with a wealth of information and many references. This beautiful and useful resource was conceived and, until recently, maintained by Neil J.A. Sloane. Its current format is a moderated wiki.

- The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

CHAPTER 3

Ramsey Theory

RAMSEY THEORY can be summarized by the phrase "complete disorder is impossible". More precisely, no matter how chaotic a structure you come up with, if only it is large enough it will contain a highly regular substructure. The traditional example is the following:

3.0.1 PROBLEM. Prove that, among any group of six people, there is either a group of three, any two of whom are friends, or there is a group of three, no two of whom are friends.

More mathematically: in any graph on six vertices there is either a triangle or a set of three vertices with no edges between them. Ramsey's Theorem is a vast generalization of this.

3.1 Ramsey's Theorem for graphs

We will start with an "in-between" version of the theorem, which has an illustrative proof. Compared to the example in the introduction we are looking for complete subgraphs on l vertices, rather than triangles, and we are looking for s relations, rather than the two relations "friends" and "not friends". From now on we will refer to those relations as *colors*.

3.1.1 THEOREM. *Let $s \geq 1$ and $l \geq 2$ be integers. There exists a least integer $R(l;s)$ such that, for all $n \geq R(l;s)$, and for all colorings of the edges of K_n with s colors, there exists a complete subgraph on l vertices, all edges of which have the same color.*

We will refer to such a single-colored subgraph (as well as any configuration in this chapter that uses a single color) as *monochromatic*.

Proof: If $s = 1$ (i.e. all edges get the same color) then clearly $R(l;s) = l$. Hence we can assume $s \geq 2$. We will show that

$$R(l;s) \leq s^{(l-1)s+1}.$$

Pick an integer $n \geq s^{(l-1)s+1}$, and an s-coloring χ of the edges of K_n (so χ is a function $\chi : E(K_n) \to [s]$). Define a set $S_1 := [n]$, and recursively define vertices x_i, colors c_i, and sets S_{i+1} for $i = 1, 2, \ldots, (l-1)s$ as follows:

- Pick any vertex $x_i \in S_i$. Define

$$T_{i,j} := \{u \in S_i \setminus \{x_i\} : \chi(u, x_i) = j\}.$$

- Let j_0 be such that T_{i,j_0} is maximal. Let $S_{i+1} := T_{i,j_0}$ and $c_i := j_0$.

Note that the size of T_{i,j_0} must be at least the average size of the $T_{i,j}$, so

$$|S_{i+1}| \geq \frac{|S_i| - 1}{s}.$$

3.1.1.1 CLAIM. $|S_{i+1}| \geq s^{(l-1)s+1-i}$.

Proof: This is clearly true for $i = 0$. Assume it holds for S_i; then

$$|S_{i+1}| \geq \frac{|S_i| - 1}{s} \geq \frac{s^{(l-1)s+1-(i-1)} - 1}{s} = s^{(l-1)s+1-i} - \frac{1}{s}.$$

The claim follows since $|S_{i+1}|$ is an integer and $\frac{1}{s} < 1$. □

In particular, $|S_{(l-1)s+1}| \geq 1$, so our sequences are well-defined.

Consider the sequence of colors $(c_1, \ldots, c_{(l-1)s+1})$. Some color must occur at least l times, say in vertices

$$\{x_{i_1}, \ldots, x_{i_l}\}.$$

By our construction, the subgraph on these vertices is monochromatic. ■

An immediate consequence of Ramsey's Theorem is the following:

3.1.2 COROLLARY. *For each l there exists an n such that each graph on at least n vertices contains either a complete subgraph on l vertices or a stable set of size l.*

3.2 Ramsey's Theorem in general

Ramsey's Theorem in full can be obtained by generalizing the result above in the following directions:

- We let the size of the monochromatic subset depend on the color;
- Instead of coloring the edges of K_n (and therefore the size-2 subsets of $[n]$), we color the size-r subsets of $[n]$, for some fixed r.

This yields the following result:

3.2.1 THEOREM (Ramsey's Theorem). *Let $r, s \geq 1$ be integers, and let $q_i \geq r \quad (i = 1, \ldots, s)$ be integers. There exists a minimal positive integer $R_r(q_1, \ldots, q_s)$ with the following property. Suppose S is a set of size n, and the $\binom{n}{r}$ r-subsets of S have been colored with colors from $[s]$. If $n \geq R_r(q_1, \ldots, q_s)$ then there is an $i \in [s]$, and some q_i-size subset T of S, such that all r-subsets of T have color i.*

Our result from the last section can be recovered by taking $R(l;s) = R_2(\overbrace{l,l,\ldots,l}^{s \text{ terms}})$.

Proof: The proof is by induction on all the parameters. We split it in two parts, according to the value of s.

Case: $s = 2$**.** For ease of notation, write $(q_1, q_2) = (p, q)$. We distinguish a few base cases (check these to make sure you understand the theorem).

- If $r = 1$, then $R_1(p,q) = p + q - 1$.
- If $p = r$, then $R_r(p,q) = q$.
- If $q = r$, then $R_r(p,q) = p$.

Next, our induction hypothesis. Let $r \geq 2$, $p > r$ and $q > r$. We assume that we have proven the existence of the following integers:

- $R_{r-1}(p', q')$ for all $p', q' \geq r - 1$;
- $p_0 := R_r(p-1, q)$;
- $q_0 := R_r(p, q-1)$.

Choose a set S of size $|S| \geq 1 + R_{r-1}(p_0, q_0)$, and a coloring χ of its r-subsets with red and blue. Single out an element $a \in S$, and set $S' := S \setminus \{a\}$. Let χ^* be a coloring of the $(r-1)$-subsets of S' in red and blue, such that, for each $(r-1)$-subset $T \subseteq S'$,

$$\chi^*(T) = \chi(T \cup \{a\}).$$

By induction, one of the following holds:

- There exists $A \subseteq S'$, with $\chi^*(T) =$ red for all $T \subseteq A, |T| = r-1$, such that $|A| = p_0$;
- There exists $B \subseteq S'$, with $\chi^*(T) =$ blue for all $T \subseteq B, |T| = r-1$, such that $|B| = q_0$.

By symmetry, we may assume the first holds. Recall that $|A| = p_0 = R_r(p-1, q)$, so again by induction, A contains either a size-q subset, all of whose r-subsets are blue (under χ), or a size-$(p-1)$ subset A', all of whose size-r-subsets are red (under χ). In the former case we are done; in the latter it is easily checked that $A' \cup \{a\}$ is a monochromatic set of size p. Hence

$$R_r(p,q) \leq 1 + R_{r-1}\big(R_r(p-1,q), R_r(p,q-1)\big).$$

Case: $s > 2$**.** Now we apply induction on s. Choose a set S of size $|S| \geq R_r(q_1, \ldots, q_{s-2}, R_r(q_{s-1}, q_s))$, and let χ be a coloring of the size-r subsets of S with colors $[s]$. Construct a different coloring χ' of the size-r subsets with colors $[s-1]$ such that

$$\begin{aligned} \chi'(T) &= \chi(T) && \text{if } \chi(T) \in [s-2]; \\ \chi'(T) &= s-1 && \text{if } \chi(T) \in \{s-1, s\}. \end{aligned}$$

If there is an $i \in [s-2]$ such that S has a subset T of size q_i with all size-r subsets $T' \subseteq T$ having $\chi'(T') = i$, then we are done, so assume that is not the case. Then we know, by induction, that S has a subset T of size $R_r(q_{s-1}, q_s)$ with all r-subsets T' having $\chi'(T) = s-1$. Now the r-subsets of T were originally colored $s-1$ or s. By our choice of T and induction, we find that T has either a set of size q_{s-1}, all of whose r-subsets have color $s-1$, or a set of size q_s, all of whose r-subsets have color s. Hence we have established

$$R_r(q_1, \ldots, q_s) \leq R_r\big(q_1, \ldots, q_{s-2}, R_r(q_{s-1}, q_s)\big),$$

and our proof is complete. ∎

3.3 Applications

We will show that any large enough set of points in the plane, with no three on a line, will contain a big subset that forms a convex n-gon. First a small case:

3.3.1 LEMMA. *Let P be a set of five points in the plane, with no three on a line. Then some subset of four points of P forms a convex 4-gon.*

Proof: Exercise. ∎

3.3.2 LEMMA. *Let P be a set of n points in the plane, such that each 4-tuple forms a convex 4-gon. Then P forms a convex n-gon.*

Proof: Consider the smallest polygon containing all points. There must be $p, q \in P$ such that p is on the boundary of this polygon, and q is in the interior. Draw lines from p to all other points on the boundary. This will divide the polygon into triangles. Clearly q must be in one of the triangles, which contradicts that all 4-tuples are convex. ∎

3.3.3 THEOREM. *For all n there exists an integer N such that, if P is a set of at least N points in the plane, with no three points on a line, then P contains a convex n-gon.*

Proof: Take $N := R_4(n, 5)$. Let P be a set of points as in the theorem. Color the 4-subsets of P red if they form a convex set, and blue otherwise. By Lemma 3.3.1 there is no 5-subset for which all 4-subsets are blue. Hence Ramsey's Theorem implies that there must exist an n-subset all of whose 4-subsets are red! ∎

A second application is a "near-miss" of Fermat's Last Theorem. We start with *Schur's Theorem*:

3.3.4 THEOREM (Schur's Theorem). *Let s be an integer. If $N \geq R_2(\overbrace{3, 3, \ldots, 3}^{s \text{ terms}})$, and the integers $[N]$ are colored with s colors, then there exist $x, y, z \in [N]$ of the same color with*

$$x + y = z.$$

Proof: Let $\chi : [N] \to [s]$ be a coloring. Consider the graph K_N, with vertex set $[N]$, and define an edge coloring $\chi^* : E \to [s]$ as follows:

$$\chi^*(i, j) := \chi(|i - j|).$$

By Ramsey's Theorem there exist $i > j > k$ such that the subgraph indexed by these vertices is monochromatic. That is,

$$\chi^*(i, j) = \chi^*(j, k) = \chi^*(i, k)$$
$$\chi(i - j) = \chi(j - k) = \chi(i - k).$$

Now choose $x = i - j$, $y = j - k$, and $z = i - k$ to get the desired result. ∎

Schur applied his theorem to derive the following result:

3.3.5 THEOREM. *For every integer $m \geq 1$, there exists an integer p_0 such that, for all primes $p \geq p_0$, the congruence*

$$x^m + y^m \equiv z^m \pmod{p}$$

has a solution in positive x, y, z.

Proof: Pick a prime $p > R_2(\overbrace{3,3,\ldots,3}^{s \text{ terms}})$. Consider the multiplicative group $\mathbb{Z}_p^*$. This group is cyclic, so there is an element g, the *generator*, such that every $e \in \mathbb{Z}_p^*$ can be written uniquely as $e = g^a$ for some $a \in \{0, \ldots, p-2\}$. Write $e = g^{mb+c}$, with $0 \leq c < m$. We define a coloring $\chi : \mathbb{Z}_p^* \to \{0, \ldots, m-1\}$ by

$$\chi(e) = \chi(g^a) = a \pmod{m}.$$

By Schur's Theorem, we can find $x, y, z \in \mathbb{Z}_p^*$ such that $x + y = z$ and $\chi(x) = \chi(y) = \chi(z)$. We write $x = g^{a_x} = g^{mb_x+c}$. Similarly for y and z. We obtain

$$g^{mb_x+c} + g^{mb_y+c} = g^{mb_z+c}.$$

Dividing both sides by g^c we get the desired result. ∎

3.4 Van der Waerden's Theorem

A second cornerstone of Ramsey theory is *Van der Waerden's Theorem*. Instead of subsets we are now coloring integers.

3.4.1 DEFINITION. An *arithmetic progression* of length t is a set of integers of the form

$$\{a, a+l, a+2l, \ldots, a+(t-1)l\}.$$

3.4.2 THEOREM (Van der Waerden's Theorem). *For all integers $t, r \geq 1$, there exists a least integer $W(t,r)$ such that, if the integers $\{1, 2, \ldots, W(t,r)\}$ are colored with r colors, then one color class has an arithmetic progression of length t.*

A less combinatorial formulation is the following: If the positive integers are divided into k classes, then one class contains arbitrarily long arithmetic progressions.

In the next section we will derive Van der Waerden's Theorem from a very powerful result in Ramsey Theory. Here, following Graham, Rothschild, and Spencer (1990), we will only sketch a proof of the (rather bad) bound $W(3,2) \leq 325$, using ideas that can be extended to prove Theorem 3.4.2 directly.

First, note that $W(2,r) = r+1$. We color the integers $[325]$ red and blue. We partition them into 65 sets of length 5:

$$B_1 := \{1, \ldots, 5\}, \quad B_2 = \{6, \ldots, 10\}, \quad \ldots, \quad B_{65} = \{321, \ldots, 325\}.$$

Each block has a color pattern such as $rbrrb$. We can interpret this as the blocks being colored with $2^5 = 32$ colors. Hence two blocks among the first 33 must have the same color pattern. Assume, for the purposes of this illustration, that those blocks are B_{11}

and B_{26}. Within B_{11}, at least two of the first three entries have the same color. Let those entries be j and $j+d$ (where $d=1$ or 2, and if $d=2$ then j indexes the first element). Suppose this color is red. Now $j+2d$ is in B_{11}. If it is also red then $\{j, j+d, j+2d\}$ is our sequence; otherwise, suppose j' is the entry corresponding to j in B_{26}, and j'' is the entry corresponding to j in B_{41}. Then one of the sequences

$$\{j+2d, j'+2d, j''+2d\}$$
$$\{j, j'+d, j''+2d\}$$

is monochromatic. These options are illustrated in Figure 3.1.

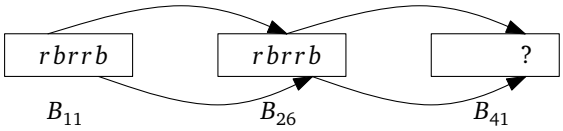


FIGURE 3.1
Two arithmetic progressions of length 3

3.5 The Hales-Jewett Theorem

The Hales-Jewett Theorem is the workhorse of Ramsey Theory. It gets to the core of Van der Waerden's Theorem, getting rid of the algebraic structure of the integers and replacing it by a purely combinatorial statement.

3.5.1 DEFINITION. Let A be a finite set of size t, and n an integer. Denote by A^n the set of all n-tuples of elements of A. A subset $L \subseteq A^n$ is a *combinatorial line* if there exist an index set $\emptyset \subsetneq I \subseteq [n]$, say $I = \{i_1, \ldots, i_k\}$, and elements $a_i \in A$ for $i \notin I$, such that

$$L = \{(x_1, \ldots, x_n) \in A^n : x_{i_1} = \cdots = x_{i_k} \text{ and } x_i = a_i \text{ for } i \notin I\}.$$

Think of the coordinates indexed by I as *moving*, and the remaining coordinates as *fixed*. The moving coordinates are synchronized, and take on all possible values. At least one coordinate is moving. We can describe such lines by introducing a new symbol, $*$, and considering n-tuples of $(A \cup \{*\})^n$. A *root* is an element $\tau \in (A \cup \{*\})^n$ using at least one $*$. Defining $I := \{i : \tau_i = *\}$ yields an easy bijection between roots and combinatorial lines.

3.5.2 EXAMPLE. Let $A^n = [3]^4$, let $I = \{2,4\}$, and let $a_1 = 1, a_3 = 2$. Then

$$L = \left\{ \begin{array}{l} \{\mathbf{1}, 1, \mathbf{2}, 1\} \\ \{\mathbf{1}, 2, \mathbf{2}, 2\} \\ \{\mathbf{1}, 3, \mathbf{2}, 3\} \end{array} \right\}.$$

The root of L is $1*2*$.

3.5.3 THEOREM (Hales-Jewett). *For all $t, r \in \mathbb{N}$ there is a least dimension $HJ(t,r)$ such that for all $n \geq HJ(t,r)$ and for all r-colorings of $[t]^n$, there exists a monochromatic combinatorial line.*

The main issue in understanding the proof is getting a grip on the many indices that are floating around. We will frequently look at products of spaces, and write $A^{n_1+n_2} = A^{n_1} \times A^{n_2}$. We will extend this notation to members of these spaces. For instance, if $A = \{1,2,3,4\}$, and $x, y \in A^2$, say $x = (1,3)$ and $y = (4,2)$, then we write $x \times y \in A^2 \times A^2$; in particular $x \times y = (1,3,4,2)$. One more piece of notation: if L is a combinatorial line, then $L(p)$ is the point on that line in which the moving coordinates are equal to p.

Proof: The proof is by induction. It is easy to see that $HJ(1,r) = 1$ for all r, giving us the base case of the induction. From now, assume that $t \geq 2$ and that the (finite) numbers $HJ(t-1,r)$ exist for all values of r. Fix r, and let $c_1, \ldots, c_r$ be a sequence of integers, $c_1 \ll c_2 \ll \cdots \ll c_r$, which we will specify later. Define $n := c_1 + \cdots + c_r$, and fix a coloring χ of $[t]^n$ with r colors. We will interpret

$$[t]^n = [t]^{c_1} \times [t]^{c_2} \times \cdots \times [t]^{c_r}.$$

Our starting point is to color the set $[t]^{c_r}$ with a huge number of colors: $r^{t^{n-c_r}}$ colors, to be precise. Let $\chi^{(r)}$ be this coloring of $[t]^{c_r}$, defined by

$$\chi^{(r)}(x) = (\chi(y_1 \times x), \chi(y_2 \times x), \ldots, \chi(y_{t^{n-c_r}} \times x)),$$

where $y_1, \ldots, y_{t^{n-c_r}}$ are the points of $[t]^{n-c_r} = [t]^{c_1} \times \cdots \times [t]^{c_{r-1}}$. We assume c_r was chosen so that $c_r \geq HJ(t-1, r^{t^{n-c_r}})$, and therefore we can find, in $[t-1]^{c_r}$, a monochromatic combinatorial line L_r' (with respect to coloring $\chi^{(r)}$). Let L_r be the extension of this line with the point in which the moving coordinates have value t; this may or may not be a monochromatic line, but the key observation is that, for fixed $y \in [t]^{n-c_r}$, the color $\chi(y \times L_r(i))$ only depends on whether or not $i = t$.

Now we restrict our attention to the subspace

$$[t]^{c_1} \times [t]^{c_2} \times \cdots \times [t]^{c_{r-1}}.$$

Construct a coloring $\chi^{(r-1)}$ of $[t]^{c_{r-1}}$, as follows:

$$\chi^{(r-1)}(x) = (\chi(y_1 \times x \times x_r), \ldots, \chi(y_{t^{n-c_r-c_{r-1}}} \times x \times x_r)),$$

where $y_1, \ldots, y_{t^{n-c_r-c_{r-1}}}$ are the points of $[t]^{n-c_r-c_{r-1}} = [t]^{c_1} \times \cdots \times [t]^{c_{r-2}}$, and x_r is any point of L_r in which the moving coordinate is not t (as we remarked earlier, we may as well choose $x_r = L_r(1)$). We assume c_{r-1} was chosen so that $c_{r-1} \geq HJ(t-1, r^{t^{n-c_r-c_{r-1}}})$, so again we find a monochromatic combinatorial line L_{r-1}' in $[t-1]^{c_{r-1}}$ (with respect to coloring $\chi^{(r-1)}$). Let L_{r-1} be the extension of this line with the point in which the moving coordinates have value t. Observe, similar to before, that for fixed $y \in [t]^{n-c_r-c_{r-1}}$, the color $\chi(y \times L_{r-1}(i) \times L_r(j))$ is independent of the choice of i, j (as long as $i, j < t$), and independent of j (if $i = t$ and $j < t$).

Proceeding in this way we find ourselves with a subspace $L_1 \times \cdots \times L_r$. Consider the $r+1$ points

$$\begin{aligned} &L_1(1) \times L_2(1) \times \cdots \times L_r(1), \\ &L_1(r) \times L_2(1) \times \cdots \times L_r(1), \\ &\cdots, \\ &L_1(r) \times L_2(r) \times \cdots \times L_r(r). \end{aligned}$$

Since we used only r colors, by the Pigeonhole Principle two of these must share the same color, say with last r in positions i and $j+1$ (where $j-1 > i$). Then the line L :=

$$\begin{aligned} \{&L_1(r) \times \cdots \times L_{i-1}(r) \times L_i(r) \times \cdots \times L_j(r) \times L_{j+1}(1) \times \cdots \times L_r(1), \\ &L_1(r) \times \cdots \times L_{i-1}(r) \times L_i(r-1) \times \cdots \times L_j(r-1) \times L_{j+1}(1) \times \cdots \times L_r(1), \\ &\cdots \\ &L_1(r) \times \cdots \times L_{i-1}(r) \times L_i(2) \times \cdots \times L_j(2) \times L_{j+1}(1) \times \cdots \times L_r(1) \\ &L_1(r) \times \cdots \times L_{i-1}(r) \times L_i(1) \times \cdots \times L_j(1) \times L_{j+1}(1) \times \cdots \times L_r(1)\} \end{aligned}$$

is monochromatic, for the following reasons:

(*i*) The points $L(1), \ldots, L(r-1)$ have the same color by our choice of L_i (compare the statement after choosing L_{r-1}).

(*ii*) The points $L(1)$ and $L(r)$ have the same color by our choice of i and j. ∎

3.5.1 Proof of Van der Waerden's Theorem

Proof of Theorem 3.4.2: We claim that $W(t,r) \leq t \cdot HJ(t,r)$. Let $n := HJ(t,r)$, and let $N := nt$. Define a function $f : [t]^n \to [N]$ by

$$f(x) = x_1 + \cdots + x_n.$$

Consider a coloring χ of the integers $[N]$ with r colors. We derive a coloring χ' of $[t]^n$ by

$$\chi'(x) = \chi(x_1 + \cdots + x_n).$$

By Theorem 3.5.3, $[t]^n$ contains a monochromatic combinatorial line L (under coloring χ'). By rearranging coordinates we may assume

$$L = \{(\underbrace{x, x, \ldots, x}_{b \text{ terms}}, a_{b+1}, \ldots, a_n) : x = 1, \ldots, t\}$$

for some fixed $a_{b+1}, \ldots, a_n$ and $b > 0$. Now set $a = b + a_{b+1} + \cdots + a_n$. Then

$$f(L) := \{f(y) : y \in L\} = \{a, a+b, a+2b, \ldots, a+(t-1)b\},$$

which by our construction is monochromatic. ∎

3.6 Bounds

An important question in Ramsey theory is what the exact value is of $R_r(q_1,\dots,q_s)$, $W(t,r)$, and $HJ(t,r)$. For the latter, for instance, the proof we gave yields truly awful bounds, because of the recursive nature, where $HJ(t,r)$ is bounded by *recursively* substituting parameters depending on $HJ(t-1,r)$ into $HJ(t-1,r)$ itself. For that reason, it was a breakthrough when Shelah (1988) found a proof of Theorem 3.5.3 that was *primitive recursive*, bringing the bound down to about

$$HJ(t,r) \leq \underbrace{r^{r^{\cdot^{\cdot^{\cdot^{r^{t^n}}}}}}}_{n \text{ times}}, \text{ where } n = HJ(t-1,r).$$

In this section we will restrict ourselves to Ramsey numbers for graphs, using two colors: the numbers $R(l;2)$. From the proof of Theorem 3.1.1, we know $R(l;2) \leq 2^{2l-1}$. How good is this bound? The following result shows that in terms of growth rate, the bound has the right behavior:

3.6.1 THEOREM. *For all $l \geq 2$, $R(l;2) \geq 2^{l/2}$.*

The proof uses a tool we will encounter again in a later chapter: the *probabilistic method*. Roughly, we show that a random coloring of a graph that's too small has a positive probability of not containing a size-l monochromatic clique:

Proof: First, observe that $R(2;2) = 2$ and $R(3;2) = 6$. Hence we may assume $l \geq 4$. Pick an integer $N < 2^{k/2}$, and consider a random coloring of the edges of K_N, with each edge independently receiving color red or blue with probability $1/2$. Hence each coloring of the full graph is equally likely, and has probability $2^{-\binom{N}{2}}$ of occurring.

Denote by A_R the event that subset A of vertices induces an all-red subgraph (i.e. all edges with both ends in A are red). If $|A| = k$, this probability is $2^{-\binom{l}{2}}$. Let p_R be the probability that *some* subset of size l induces an all-red subgraph. Then

$$p_R = \Pr\left(\bigcup_{|A|=l} A_R\right) \leq \sum_{A:|A|=l} \Pr(A_R) = \binom{N}{l} 2^{-\binom{l}{2}}.$$

The inequality uses the *union bound*, to be discussed later. Now

$$\binom{N}{l} 2^{-\binom{l}{2}} \leq \frac{N^l}{l!} 2^{-\binom{l}{2}} \leq \frac{N^l}{2^{l-1}} 2^{-\binom{l}{2}} < \frac{(2^{l/2})^l}{2^{l-1}} 2^{-\binom{l}{2}} = 2^{l^2/2+1-l-\frac{1}{2}l(l-1)} = 2^{1-l/2} \leq 1/2,$$

where the strict inequality uses the choice of N. Hence we have $p_R < 1/2$. Similarly, $p_B < 1/2$. But then $p_R + p_B < 1$, so there is a positive probability that a random coloring has *no* monochromatic l-subset. Hence such a coloring must exist! ∎

3.7 Density versions

All results in Ramsey theory state that *some* color class exhibits the desired behavior. What can we do if we insist that the *red* color class having the property? At first sight,

not much: there are colorings that don't use red at all! But some of the most powerful results in combinatorics state that, if only we use red often enough, the desired conclusion *still* holds. The first theorem of this kind was the following:

3.7.1 THEOREM (Szemerédi). *For all real numbers $\varepsilon > 0$ and integers $k \geq 3$, there exists an integer n_0 such that, for any $n \geq n_0$, and any $S \subseteq [n]$ with $|S| \geq \varepsilon n$, the set S contains an arithmetic progression of length k.*

Note that we can make the fraction of points that is red as small as we want, as long as we increase the total number of points enough. Furstenberg and Katznelson generalized Szemerédi's result to the following:

3.7.2 THEOREM (Density Hales-Jewett). *For every integer $t > 0$ and for every real number $\varepsilon > 0$, there exists an integer $DHJ(t, \varepsilon)$ such that, if $n \geq DHJ(t, \varepsilon)$ and $A \subseteq [t]^n$ has density[*] at least ε, then A contains a combinatorial line.*

The proofs of these results were originally non-combinatorial, using ergodic theory instead. Recently, a "polymath" project found a combinatorial proof of the Density Hales-Jewett Theorem. Gowers and Tao managed to use Szemerédi's Theorem to show the existence of arbitrarily long arithmetic progressions in the set of primes.

3.8 Where to go from here?

Ramsey theory is an important branch of combinatorics, but textbooks devoted exclusively to the subject are hard to find. The classical text is still

- Graham et al. (1990), *Ramsey Theory*.

Most books mentioned in Section 1.5 contain at least one chapter on Ramsey theory. In particular,

- Jukna (2011), *Extremal Combinatorics*

contains Shelah's proof of the Hales-Jewett Theorem.

[*]This means $|A| \geq \varepsilon t^n$.

CHAPTER 4

Extremal combinatorics

EXTREMAL combinatorics deals with questions that go roughly as follows: "how many objects of a certain type can I pack together before a certain property is violated?" A concrete example is the following:

4.0.1 QUESTION. How many edges can a graph on n vertices have, if it has no triangles?

After some thought you might come up with the class of *bipartite graphs*. The highest number of edges is achieved when the color classes are roughly equal in size, which gives a family of graphs without triangles, and whose number of edges equal to $\lfloor \frac{1}{4}n^2 \rfloor$. So our upper bound needs to exceed this number. *Mantel's Theorem* from 1907 tells us that this is tight:

4.0.2 THEOREM. *If an n-vertex graph G has more than $\lfloor \frac{1}{4}n^2 \rfloor$ edges, then G contains a triangle.*

We will prove a more general theorem in the next section.

4.1 Extremal graph theory

Another way to look at Theorem 4.0.2 is as a density version of Ramsey's Theorem (cf. Szemerédi's Theorem and the Density Hales-Jewett Theorem mentioned in the previous chapter). We ask how often we can use the color red without creating a red triangle. As such it makes sense to generalize this result to arbitrary complete graphs. To describe the extremal graphs (those to which no more edges can be added) we use the notion of a *k-partite graph*: a graph whose vertex set is partitioned into sets $V_1, \ldots, V_k$, and no edge has both endpoints inside a set V_i. The *complete k-partite graphs* are those in which all such edges are present. If $|V_i| = n_i$ for $i \in [k]$, then this complete k-partite graph is denoted by $K_{n_1,\ldots,n_k}$. Moreover, $n = n_1 + \cdots + n_k$, and if $|n_i - n_j| \leq 1$ for all $i, j \in [k]$, then we denote the unique (up to vertex labeling) such graph by $T_{n,k}$.

4.1.1 EXERCISE. Show that $T_{n,k}$ has $\lfloor \frac{1}{2}(1 - \frac{1}{k})n^2 \rfloor$ edges.

The following is a generalization of Mantel's Theorem:

4.1.2 THEOREM (Turán's Theorem). *Among all graphs with no K_{k+1}-subgraph, $T_{n,k}$ has the most edges.*

We give two proofs, with a decidedly different flavor.

Proof 1: Let G be a graph on n vertices without K_{k+1}-subgraph, and with $|E|$ maximum under all such graphs.

4.1.2.1 CLAIM. *G has no triple u, v, w of vertices with $vw \in E$ yet $uv, uw \notin E$.*

Proof: Suppose it does. We try to modify the graph to improve the number of edges; we distinguish three cases.

I. If $\deg(u) < \deg(v)$, then we construct a new graph, G', as follows from G. Delete all edges incident with u, and create new edges so that the set of neighbors of u, denoted by $N(u)$, satisfies $N(u) = N(v)$. Note that u and v are not adjacent in G', so if G' has a K_{k+1}-subgraph, then it uses at most one of u and v. But both $G' - u$ and $G' - v$ are isomorphic to subgraphs of G, and therefore have no K_{k+1}. Hence G' has none; and the number of edges satisfies

$$|E(G')| = |E(G)| - \deg(u) + \deg(v) > |E(G)|,$$

contradicting our choice of G.

II. $\deg(u) < \deg(w)$ follows from (I) by symmetry.

III. If $\deg(u) \geq \deg(v)$ and $\deg(u) \geq \deg(w)$, then we construct a new graph, G', as follows from G. Delete all edges incident with v, and all edges incident with w. Then make both v and w adjacent to all neighbors of u. Again we can see that G' has no K_{k+1}-subgraph. Moreover,

$$|E(G')| = |E(G)| - \deg(v) - \deg(w) + 1 + 2\deg(u) > |E(G)|,$$

where the $+1$ follows from double-counting the edge vw. □

Now we define an equivalence relation $\sim$ such that $u \sim v$ if and only if u is *not* incident to v. By the claim, this is an equivalence relation. Hence our graph G is isomorphic to $K_{n_1,\ldots,n_t}$ for some t. We leave as an exercise to prove that this is optimal precisely for $T_{n,k}$. ■

Proof 2: We will only prove the bound, not the structure. This proof turns the question into an *optimization problem*. Let G be a graph with no K_{k+1} subgraph. We introduce real numbers w_v for each $v \in V(G)$. Our goal is:

$$\begin{aligned} \text{maximize} \quad & f(\mathbf{w}) := \sum_{uv \in E(G)} w_u w_v \\ \text{subject to} \quad & w_v \geq 0 \qquad\qquad \text{for all } v \in V(G) \\ & \sum_{v \in V(G)} w_v = 1. \end{aligned}$$

Let $\mathbf{w}$ be an optimal solution, and suppose i, j are nonadjacent vertices with $w_i, w_j > 0$. Let s_i be the sum of the weights of the neighbors of i, and s_j the sum of the weights of the neighbors of j. Define $\mathbf{w}'$ by

$$\begin{aligned} w'_j &= 0 \\ w'_i &= w_i + w_j \\ w'_k = w_k \qquad &\text{for all } k \in V \setminus \{i, j\}. \end{aligned}$$

Then

$$f(\mathbf{w}') = f(\mathbf{w}) + w_j s_i - w_j s_j \geq f(\mathbf{w}),$$

so there exists a maximizer having positive weights only on the vertices of a clique, say of size k. Let $\mathbf{w}$ be such an optimizer.

Now assume that there exist vertices i, j in this clique with $w_i > w_j > 0$. Pick an $\varepsilon : 0 < \varepsilon < w_i - w_j$, and define $\mathbf{w}'$ by

$$\begin{aligned} w'_j &= w_j + \varepsilon \\ w'_i &= w_i - \varepsilon \\ w'_k = w_k \qquad &\text{for all } k \in V \setminus \{i, j\}. \end{aligned}$$

Then

$$f(\mathbf{w}') = f(\mathbf{w}) + \varepsilon w_i - \varepsilon w_j - \varepsilon^2 > f(\mathbf{w}).$$

We conclude that, if f takes on nonzero values on a clique of size k, then f is maximized when $w_i = 1/k$ if i is in the clique, and $w_i = 0$ otherwise. This gives

$$f(\mathbf{w}) = \binom{k}{2} \frac{1}{k} \frac{1}{k} = \frac{1}{2}(1 - \frac{1}{k}).$$

This function is increasing in k, so it is largest when $k = p - 1$, which gives the upper bound $f(\mathbf{w}) \leq \frac{1}{2}(1 - \frac{1}{p-1})$ for *any* vector w. Now we choose the vector $w_i = \frac{1}{n}$ for all i. The function value of this one is

$$f(\mathbf{w}) = |E| \frac{1}{n} \frac{1}{n} \leq \frac{1}{2}(1 - \frac{1}{p-1}), \tag{4.1}$$

from which the result follows. ∎

4.2 Intersecting sets

For the next while we will be studying questions of the following form:

4.2.1 PROBLEM. Let $\mathscr{F}$ be a set of subsets of the finite set $[n]$, such that *[insert property here]* is satisfied. How large can $\mathscr{F}$ be?

To let our sentences flow more smoothly, we will speak of *families* of subsets from now on. Our first property is the following:

4.2.2 DEFINITION. Let $\mathscr{F}$ be a family of subsets of $[n]$. We say $\mathscr{F}$ is *intersecting* if $A \cap B \neq \emptyset$ for all $A, B \in \mathscr{F}$.

An example of an intersecting family would be the family of all subsets containing element 1. There are 2^{n-1} of them, and the next result shows we cannot do better:

4.2.3 THEOREM. *If $\mathscr{F}$ is an intersecting family of subsets of $[n]$, then $|\mathscr{F}| \leq 2^{n-1}$.*

Proof: Let $S := [n]$, and $A \subseteq S$. At most one of $A, S \setminus A$ is in $\mathscr{F}$, so $|\mathscr{F}| \leq \frac{1}{2}2^n$. ∎

Things get slightly more interesting if we insist that all sets in $\mathscr{F}$ have the same size, say k. It is easy to find a family of size $\binom{n-1}{k-1}$, and if $n \geq 2k$ then this is best possible (if not, we can take $\binom{n}{k}$ subsets).

4.2.4 THEOREM (Erdős-Ko-Rado). *Let n, k be integers, $n \geq 2k$. If $\mathscr{F}$ is an intersecting family of size-k subsets of $[n]$, then $|\mathscr{F}| \leq \binom{n-1}{k-1}$.*

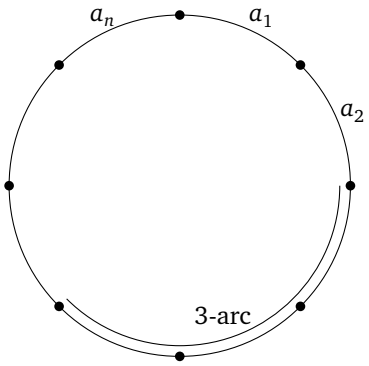


FIGURE 4.1
Illustration of the proof of the Erdős-Ko-Rado Theorem.

Proof: Let n, k be integers with $n \geq 2k$. A *k-arc* is a set $\{i, i+1, \ldots, i+k\}$, where the integers are taken modulo n. Imagine the elements of a k-arc as k consecutive circle segments, connecting the points i and $i+k \pmod{n}$ on a circle (see Figure 4.1). We say arcs A and A' *intersect* if they share a circle segment; meeting in just a point is not considered an intersection.

4.2.4.1 CLAIM. *A family $\{A_1, \ldots, A_t\}$ of pairwise intersecting k-arcs of $[n]$ has size $t \leq k$.*

Proof: Each point i is an endpoint of two arcs: one where i is the first point, and one where it is the last. These arcs have no overlap, so at most one of them is in the family. Moreover, given arc A_1, all other arcs must have one of the interior points of A_1 as an endpoint, of which there are $k-1$. □

Now consider a permutation of $[n]$ of the form $(a_1, \ldots, a_n)$, i.e. the permutation consists of a single cycle. Label the circle segments by the a_i, as in Figure 4.1. Some sets of $\mathscr{F}$ may appear as k-arcs in this permutation, but by the claim that holds for at most k

of them. Summing over all cyclic permutations, we count at most $k(n-1)!$ sets. How often does a specific set appear? There are $k!$ ways to sort set A_i, and $(n-k)!$ ways to sort its complement; finally, there is only a single way to combine these on a cycle. Hence

$$|\mathscr{F}|k!(n-k)! \leq k(n-1)!$$
$$|\mathscr{F}| \leq \frac{k(n-1)!}{k!(n-k)!} = \binom{n-1}{k-1}.$$ ∎

4.3 Sunflowers

The sets that attained the bounds in the previous section had a pretty nice structure. You might imagine that it is useful to give up a few sets, if a structure like that arises as a reward. In this section we prove a result showing that we can do this.

4.3.1 DEFINITION. A *sunflower* with k *petals* and *core* Y is a family $\mathscr{F}$ of sets, along with a set Y, such that $|\mathscr{F}| = k$, and for all $A, B \in \mathscr{F}$ with $A \neq B$ we have $A \cap B = Y$. Moreover, the sets $A \setminus Y$, which we call the petals, are nonempty.

4.3.2 LEMMA (Sunflower Lemma). *Let $\mathscr{F}$ be a family of sets, each of size s. If $|\mathscr{F}| > s!(k-1)^s$ then $\mathscr{F}$ contains a sunflower with k petals.*

Proof: We prove the result by induction on s. If $s = 1$ then $|\mathscr{F}| > k-1$, so $\mathscr{F}$ contains at least k size-1 sets. These form a sunflower (with $Y = \emptyset$).

Fix $s \geq 2$, and suppose the result holds for all smaller values of s. Let $\{A_1, \ldots, A_t\}$ be a maximal collection of pairwise disjoint subsets contained in $\mathscr{F}$. If $t \geq k$ then any k of these form a sunflower, so assume $t < k$. Let $B := A_1 \cup \cdots \cup A_t$. Then $|B| \leq s(k-1)$. No set in $\mathscr{F}$ is disjoint from B (by maximality of $A_1, \ldots, A_t$), so by the pigeonhole principle, some element $x \in B$ must be in at least

$$\frac{|\mathscr{F}|}{|B|} > \frac{s!(k-1)^s}{s(k-1)} = (s-1)!(k-1)^{s-1}$$

sets. Consider $\mathscr{F}_x := \{A \setminus \{x\} : A \in \mathscr{F}, x \in A\}$. By induction we find a sunflower with k petals in this family. Adding x to each member gives the desired sunflower of $\mathscr{F}$. ∎

The Sunflower Lemma has found a number of applications in computer science.

As we did in the chapter on Ramsey theory, we may wonder what the best possible bound is that guarantees a sunflower with k petals. Denote this number by $f(s,k)$. We have

$$(k-1)^s < f(s,k) \leq s!(k-1)^s + 1.$$

The upper bound was just proven; for the lower bound, consider the family $\mathscr{F}$ of SDRs of a collection of s pairwise disjoint size-$(k-1)$ sets $A_1, \ldots, A_s$. A sunflower with k petals in $\mathscr{F}$ must contain two petals using the same element $x \in A_1$. But each element is in either none, exactly one, or all of the members of the sunflower. It follows that all petals use x. Since we are looking at SDRs, no other element of A_1 is used by the sunflower. This can be repeated for all A_i, and we can only conclude that the sunflower has but one petal!

4.4 Hall's Marriage Theorem

The result in this section does not exactly fit the chapter title. However, it is a central result that is frequently used in combinatorics, and we'll need it in the next section. If you've taken a course in graph theory, you may have seen it formulated in terms of bipartite graphs, in close connection with Kőnig's Theorem. Here we stick to a formulation in terms of set systems.

4.4.1 DEFINITION. Let $A_1, \ldots, A_n$ be finite sets. An n-tuple $(x_1, \ldots, x_n)$ is a *system of distinct representatives* (SDR) if

- $x_i \in A_i$ for $i \in [n]$;
- $x_i \neq x_j$ for $i, j \in [n]$ with $i \neq j$.

The question we wish to answer is: when does a set system $A_1, \ldots, A_n$ have an SDR? Clearly each A_i needs to contain an element, and $A_1 \cup \cdots \cup A_n$ needs to contain n elements. Write, for $J \subseteq [n]$, $A(J) := \cup_{i \in J} A_i$. A more general necessary condition, which is equally obvious, is *Hall's Condition*:

$$|A(J)| \geq |J| \qquad \text{for all } J \subseteq N. \tag{HC}$$

As it turns out, this condition is not only necessary but also sufficient:

4.4.2 THEOREM (Hall's Marriage Theorem). *The finite sets $A_1, \ldots, A_n$ have an SDR if and only if* (HC) *holds.*

Proof: If the sets have an SDR, then clearly (HC) holds. For the converse, suppose (HC) holds. We prove the result by induction on n, the case $n = 1$ being obvious. Say a subset $J \subseteq [n]$ is *critical* if $|A(J)| = |J|$.

Case I. Suppose only $J = \emptyset$ and (possibly) $J = [n]$ are critical. Pick any $x_n \in A_n$, and let $A_i' := A_i \setminus \{x_n\}$ for $i \in [n-1]$. For $J \subseteq [n-1]$ with $J \neq \emptyset$ we have

$$|A'(J)| \geq |A(J)| - 1 \geq |J|,$$

since we removed only x_n from $A(J)$, and J is not critical. Hence (HC) holds for the A_i', and by induction the sets $A_1', \ldots, A_{n-1}'$ have an SDR $(x_1, \ldots, x_{n-1})$. Then $(x_1, \ldots, x_n)$ is an SDR for the original problem.

Case II. Suppose there is a nontrivial critical set. Pick J a minimum-size, nonempty critical set. By induction, $\{A_j : j \in J\}$ has an SDR X. Now define $A_i' := A_i \setminus A(J)$ for $i \notin J$. For $K \subseteq [n] \setminus J$ we find

$$|A'(K)| = |A(J \cup K)| - |A(J)| \geq |J \cup K| - |A(J)| = |J \cup K| - |J| = |K|,$$

so (HC) holds for the A_i'. By induction, there is an SDR Y for those sets. The union of X and Y then forms an SDR for the original problem. ∎

The name of the theorem derives from the following interpretation: men $\{1, \ldots, n\}$ are trying to find a spouse; the set A_i denotes the eligible women for man i. Can all men be married off?

4.5 The De Bruijn-Erdős Theorem

In this section we prove the following result:

4.5.1 THEOREM (De Bruijn-Erdős). *Let $n > 0$ be an integer, and let $\mathscr{F}$ be a family of subsets of $[n]$ such that $|A \cap B| = 1$ for all $A, B \in \mathscr{F}$ with $A \neq B$. Then $|\mathscr{F}| \leq n$. If $|\mathscr{F}| = n$, say $\mathscr{F} = \{A_1, \ldots, A_n\}$, then one of the following holds:*

(i) Up to relabeling, $A_i = \{i, n\}$ (so $A_n = \{n\}$);
(ii) Up to relabeling, $A_i = \{i, n\}$ for $i \in [n-1]$, and $A_n = [n-1]$;
(iii) There exists an integer $q > 0$ such that $n = q^2 + q + 1$. Each A_i has $q+1$ elements, and each element is in $q+1$ of the A_i.

This result is usually framed in terms of *incidence geometry*. We think of $[n]$ as a set of points, and of $\mathscr{F}$ as a set of lines through these points. The lines obey the classical rules of projective geometry: every two lines intersect in exactly one point. The three outcomes of the theorem are illustrated in Figure 4.2.

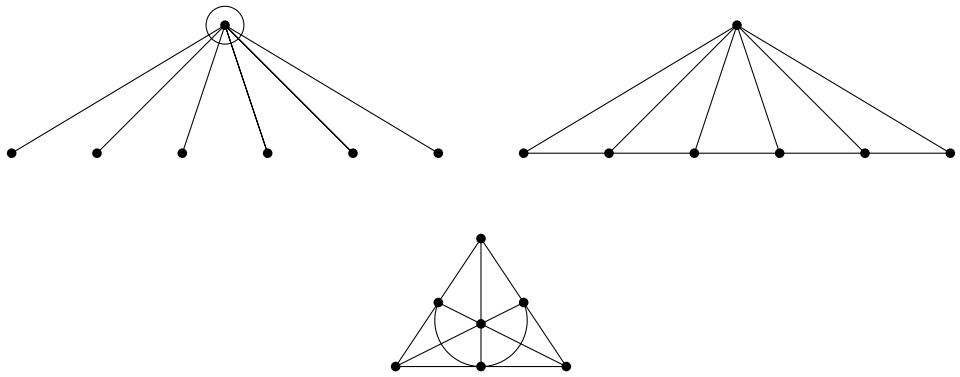


FIGURE 4.2
Illustration of the outcomes of the De Bruijn-Erdős Theorem for $n = 7$.

Proof: We omit the analysis for $n \leq 2$, and will assume $n \geq 3$. Let $\mathscr{F} = \{A_1, \ldots, A_n\}$ be a family of subsets of $[n]$ such that $|A_i \cap A_j| = 1$ for all $i \neq j$. We will analyze the structure of this family, and along the way show that no further sets can be added without violating the property. First some trivialities:

- If $A_i = \emptyset$ for some i then $\mathscr{F} = \{\emptyset\}$.
- If $A_i = \{x\}$ for some i and x, then $x \in A_j$ for all $j \in [n]$. This will be the unique point of intersection, so at most $n-1$ more sets can be added to A_i, and we have situation (*i*).
- If $A_i = [n]$ for some i, then a second set A_j intersects A_i in a singleton, so has size 1. A third set must intersect A_i *and* A_j in a singleton, which is impossible. So $|\mathscr{F}| \leq 2$.

Hence we may assume that $2 \leq |A_i| < n$ for all $i \in [n]$. Define the following:

$$B_i := [n] \setminus A_i$$
$$k_i := |A_i|$$
$$r_x := |\{j : x \in A_j\}|.$$

4.5.1.1 CLAIM. *If $x \notin A_i$ then $r_x \leq k_i$.*

Proof: Let A_j be a set containing x. Then A_j meets A_i in a single element y. If A_k is another set containing x, then A_k meets A_i in a point distinct from y (otherwise $A_j \cap A_k \supseteq \{x, y\}$). It follows that there can be no more sets containing x than points on A_i. □

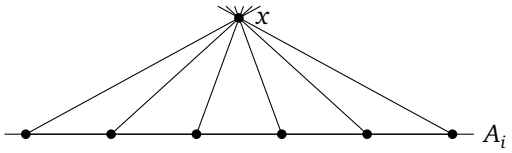


FIGURE 4.3
Illustration of Claim 1

4.5.1.2 CLAIM. *The sets $B_1, \ldots, B_n$ satisfy Hall's Condition* (HC).

Proof: The cases $|J| = 1$ and $|J| = n$ are clear by our assumptions on the sizes of the A_i. If $|J| > 1$ then, since $B_i \cup B_j = [n] \setminus (A_i \cap A_j)$, we have $|B(J)| \geq n - 1$. The claim follows. □

Fix an SDR of $B_1, \ldots, B_n$, and relabel the elements so that element i is the representative of B_i (so $i \notin A_i$). We count the pairs (i, A_j) with $i \in A_j$. This yields

$$\sum_{i=1}^{n} r_i = \sum_{j=1}^{n} k_j.$$

Since $r_i \leq k_i$ for all i (by Claim 1), it follows that for all $i \in [n]$ we have

$$r_i = k_i.$$

4.5.1.3 CLAIM. *We may assume that if J is critical then $J = \emptyset$ or $J = [n]$.*

Proof: If a set J with $|J| = 1$ is critical, then there is an i such that $|A_i| = n - 1$. This leads quickly to the second conclusion of the theorem. If a set J with $|J| = n - 1$ is critical, then $n - 1$ of the A_i meet a single point, which again leads to the second conclusion. We omit the easy details. □

It follows, as in the proof of Hall's Marriage Theorem, that we can choose the representative for one of the sets B_j at will.

4.5.1.4 CLAIM. *If $x, y \in [n]$ then there exists an $A_i \in \mathcal{F}$ such that $x, y \in A_i$.*

Proof: Pick an index j such that $y \in A_j$ and $x \in B_j$. We may choose x as representative in the SDR. This gives $r_x = k_j$, and the conclusion follows. □

Now every pair of elements is in a *unique* member of $\mathscr{F}$, so no more sets can be added!

To finish our analysis of the outcomes, observe that if $x \notin A_j$ then $r_x = k_j$, by the same argument as in the last claim. Suppose there exist $x, y \in [n]$ with $r_x \neq r_y$. Up to relabeling, suppose there is a $z \in [n]$, $z \neq y$, with $r_x \neq r_z$. We have:

- Every set contains one of x and y;
- Every set contains one of x and z;
- Exactly *one* set contains y and z.

The first two statements follow because $r_u = r_v = k_j$ for all $u, v \notin A_j$. Hence all but one of the sets contain x, which again leads to the second outcome.

It follows that, for all $x, y \in [n]$, we have $r_x = r_y = q+1$ for some q. Since $r_i = k_i$, it follows that $|A_i| = q+1$. By looking at the $q+1$ lines through x, each of which contains q points besides x, we find that $n = (q+1)q + 1 = q^2 + q + 1$, and we are done. ∎

An important problem, which has not been settled completely, is the following:

4.5.2 PROBLEM. For which values of q can the third possibility occur?

We will return to this problem later.

4.6 Sperner families

Let us look at a milder restriction on our subsets:

4.6.1 DEFINITION. A family $\mathscr{F}$ of sets is a *Sperner family* (or *antichain*, or *clutter*) if, for all $A, B \in \mathscr{F}$ with $A \neq B$ we have $A \not\subset B$ and $B \not\subset A$.

This condition is easy to satisfy: take $\mathscr{F}$ to be the collection of all size-k subsets of $[n]$. This gives a family of size $\binom{n}{k}$, and the size of the family is maximal for $k = \lfloor n/2 \rfloor$. Sperner proved that we cannot, in fact, do better:

4.6.2 THEOREM (Sperner). *If $\mathscr{F}$ is a Sperner family of subsets of $[n]$, then $|\mathscr{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

Sperner's Theorem is an easy consequence of the following result, known as the LYM inequality, named after Lubell, Meshalkin, and Yamamoto who each independently discovered it.

4.6.3 THEOREM (LYM inequality). *If $\mathscr{F}$ is a Sperner family of subsets of $[n]$, then*

$$\sum_{A \in \mathscr{F}} \binom{n}{|A|}^{-1} \leq 1.$$

Proof of Sperner's Theorem using the LYM inequality: As seen above, $\binom{n}{k}$ is maximal when $k = \lfloor n/2 \rfloor$. Hence

$$1 \geq \sum_{A \in \mathscr{F}} \binom{n}{|A|}^{-1} \geq \sum_{A \in \mathscr{F}} \binom{n}{\lfloor n/2 \rfloor}^{-1} = |\mathscr{F}| \binom{n}{\lfloor n/2 \rfloor}^{-1}.$$ ∎

The LYM inequality can be proven in various ways. This is a quick proof:

Proof of the LYM inequality: Consider chains

$$\emptyset = C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_n = [n].$$

There are $n!$ such chains, and for every chain $\mathscr{C}$ we have $|\mathscr{C} \cap \mathscr{F}| \leq 1$ (why?).

Pick $A \in \mathscr{F}$ with $|A| = k$. All chains that contain A must have $A = C_k$. By looking at all orderings of the elements, it follows that there are $k!(n-k)!$ chains containing A. Hence the number of chains meeting $\mathscr{F}$ is

$$\sum_{A \in \mathscr{F}} (|A|)!(n - |A|)! \leq n!$$

from which the result follows. ∎

An alternative approach is to derive the LYM inequality from a more general theorem by Bollobás. First a special case:

4.6.4 THEOREM (Bollobás, special case). *Let $A_1, \ldots, A_m$ be sets of size a, and $B_1, \ldots, B_m$ sets of size b, such that $A_i \cap B_j = \emptyset$ if and only if $i = j$. Then $m \leq \binom{a+b}{a}$.*

This theorem, in turn, can be generalized as follows (also due to Bollobás):

4.6.5 THEOREM (Bollobás). *Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ be sets. Let $a_i := |A_i|$ and $b_i := |B_i|$ for all $i \in [m]$. Suppose $A_i \cap B_j = \emptyset$ if and only if $i = j$. Then*

$$\sum_{i=1}^{m} \binom{a_i + b_i}{a_i}^{-1} \leq 1. \tag{4.2}$$

Let us work our way back:

First proof of Theorem 4.6.5: Let $\mathscr{F} := \{(A_1, B_1), \ldots, (A_m, B_m)\}$ be a collection of pairs of sets satisfying the conditions of the theorem. Let $X := \bigcup_{i=1}^{m} (A_i \cup B_i)$. We will prove the result by induction on $|X|$, the case $|X| = 1$ being easily verified.

Suppose the claim holds for $|X| = n-1$, and assume $|X| = n$. For each $x \in X$, define

$$\mathscr{F}_x := \{(A_i, B_i \setminus \{x\}) : (A_i, B_i) \in \mathscr{F}, x \notin A_i\}.$$

By induction, (4.2) holds for each $\mathscr{F}_x$. Sum the n left-hand sides of (4.2). We consider the contribution of a set (A_i, B_i). For $n - a_i - b_i$ elements $x \in X$ we have $x \notin A_i \cup B_i$, so the contribution is $\binom{a_i+b_i}{a_i}^{-1}$. For b_i elements $x \in X$ we have $x \in B_i$ (and hence $x \notin A_i$). The contribution in this case is $\binom{a_i+b_i-1}{a_i}$. This gives

$$\sum_{i=1}^{m} \left((n - a_i - b_i) \binom{a_i + b_i}{a_i}^{-1} + b_i \binom{a_i + b_i - 1}{a_i}^{-1} \right) \leq n.$$

Note that

$$\binom{a_i + b_i - 1}{a_i} = \frac{b_i}{a_i + b_i} \binom{a_i + b_i}{a_i},$$

from which we find

$$\sum_{i=1}^{m} n \binom{a_i + b_i}{a_i}^{-1} \leq n,$$

and the result follows. ∎

We will see another beautiful proof of Bollobás' Theorem using the probabilistic method in Section 6.4.

Proof of Theorem 4.6.4 using Bollobás' Theorem: Just substitute $a_i = a$ and $b_i = b$ for all i. ∎

Proof of the LYM inequality using Bollobás Theorem: Let $\mathscr{F} = \{A_1, \ldots, A_m\}$ and define $B_i := [n] \setminus A_i$. Since now $b_i = n - a_i$, we find

$$\sum_{i=1}^{m} \binom{n}{a_i}^{-1} = \sum_{i=1}^{m} \binom{a_i + b_i}{a_i}^{-1} \leq 1,$$

where the inequality is Bollobás' Theorem. ∎

4.7 Dilworth's Theorem

The first proof of the LYM inequality used the existence of a relation between Sperner families and *chains* of subsets. This relation is more explicit in a result by Dilworth. Dilworth's theorem holds for more general structures than subsets: we can prove it for arbitrary *partial orders*.

4.7.1 DEFINITION. A *partially ordered set* (or *poset*) is a pair $(P, \leq)$ such that $\leq$ is a subset of $P \times P$ (we denote the fact that (x, y) is in this subset by $x \leq y$), satisfying for all $x, y, z \in P$:
Reflexivity: $x \leq x$;
Antisymmetry: If $x \leq y$ and $y \leq x$ then $x = y$;
Transitivity: If $x \leq y$ and $y \leq z$ then $x \leq z$.

A key example of a poset is when P is a collection of sets, and $\leq$ is set inclusion: $X \leq Y$ iff $X \subseteq Y$.

4.7.2 DEFINITION. A *chain* in a poset is an ordered tuple $(x_1, \ldots, x_k)$ of distinct elements such that $x_1 \leq x_2 \leq \cdots \leq x_k$. An *antichain* is a subset F such that, for all distinct $x, y \in F$ we have neither $x \leq y$ nor $y \leq x$.

We study the problems of partitioning a poset into disjoint chains, or into disjoint antichains. The following is easy to see, since a chain and an antichain intersect in at most one element:

4.7.3 LEMMA. *Let $(P, \leq)$ be a poset.*
(i) If P has a chain of size r, then P cannot be partitioned into fewer than r antichains;

(ii) If P has an antichain of size r, then P cannot be partitioned into fewer than r chains.

We will prove that the bound of r is tight in both cases. First, a partition into chains:

4.7.4 THEOREM. *Suppose the longest chain in a poset $(P,\leq)$ has size r. Then we can partition P into r antichains.*

Proof: For $x \in P$, define the *height* of x as the longest chain ending in x. Let A_i be the set of elements of height i, for $i \in [r]$. Then clearly $P = A_1 \cup \cdots \cup A_r$. We show that each A_i is an antichain. Consider $x, y \in A_i$ and suppose $x \leq y$. By definition there exists a chain

$$x_1 \leq x_2 \leq \cdots \leq x_i = x.$$

We can add y to this chain obtaining a chain of length $i+1$ ending in y, a contradiction. ∎

The converse is a little more difficult to prove.

4.7.5 THEOREM (Dilworth). *Suppose the longest antichain in a poset $(P,\leq)$ has size r. Then P can be partitioned into r chains.*

Proof: The proof is by induction on $|P|$, the case $|P| = 0$ being trivial. Let C be a maximal chain in P. If $P \setminus C$ has only antichains up to size $r-1$ then we find a partition into $r-1$ chains, to which C can be added for a partition of P. Hence we may assume $P \setminus C$ has an antichain $a_1, \ldots, a_r$. Clearly this is also a maximal antichain of P. We define two subsets of P:

$$S^- := \{x \in P : x \leq a_i \text{ for some } i\},$$
$$S^+ := \{x \in P : a_i \leq x \text{ for some } i\}.$$

Note:

- Each item of P is in one of S^-, S^+; otherwise a larger antichain would exist.
- $S^- \cap S^+ = \{a_1, \ldots, a_r\}$.
- The start of C is not in S^+.
- The end of C is not in S^-.
- The elements $a_1, \ldots, a_r$ are maximal in S^-.
- The elements $a_1, \ldots, a_r$ are minimal in S^+.

For the fifth item, suppose $a_i \leq y$ for some $y \in S^-$. Then there exists an index j such that $a_i \leq y \leq a_j$, so $a_i = y = a_j$.

Now, since S^- and S^+ are strict subsets of P, each with an antichain of size r, these sets can be partitioned, by induction, into r chains. The chains of S^- end in the a_i, and the chains in S^+ start with the a_i. Joining them up gives the desired partition of P. ∎

4.7.6 EXERCISE. Prove Hall's Marriage Theorem using Dilworth's Theorem.

4.8 Where to go from here?

An excellent book on extremal combinatorics, which was mentioned before, is

- Jukna (2011), *Extremal Combinatorics*.

It contains much more material than these notes, and references to even more material. The following books are devoted exclusively to extremal set theory:

- Anderson (1987), *Combinatorial Set Theory* is a very readable textbook.
- Engel (1997), *Sperner Theory* is an advanced text dealing with Sperner systems.

In the next chapter we will use a powerful method to prove more results from extremal combinatorics.

CHAPTER 5

Linear algebra in combinatorics

LINEAR algebra can be a powerful tool in combinatorics. In this chapter we will see a number of examples of this phenomenon. In the first half we will focus again on extremal results in set theory. In the second half, starting with Section 5.5 we will shift our focus to some combinatorial uses for determinants.

5.1 The clubs of Oddtown

In an effort to cut costs, the town council of Oddtown tries to limit the number of clubs the citizens can form. They hire two consulting firms, who come up with the following rules for clubs. Both firms agree on the first two rules, but have a different version of the third.

(*i*) No two clubs can have the same set of members;
(*ii*) Every two distinct clubs must have an *even* number of common members;
(*iii*) a) Each club has an *even* number of members;
b) Each club has an *odd* number of members.

If clubs have even size, a collection of clubs of size $2^{\lfloor n/2 \rfloor}$ is easily constructed: divide the citizens into pairs, and let each club be a union of pairs. If clubs have odd size, it is harder to come up with a large construction, and you'll struggle to do better than $\{1\}, \ldots, \{n\}$. There is a reason for the struggle:

5.1.1 THEOREM (Oddtown). *Let $\mathscr{F}$ be a family of subsets of $[n]$ such that, for all $A, B \in \mathscr{F}$ with $A \neq B$, we have $|A \cap B|$ is even and $|A|$ is odd. Then $|\mathscr{F}| \leq n$.*

Proof: Let $\mathscr{F} = \{A_1, \ldots, A_m\}$. For each A_i define a vector $a_i \in \mathbb{Z}_2^n$ by

$$(a_i)_j = \begin{cases} 1 & \text{if } j \in A_i \\ 0 & \text{otherwise.} \end{cases}$$

Consider the inner product $\langle a_i, a_j \rangle$.

$$\langle a_i, a_j \rangle = \sum_{x \in [n]} (a_i)_x (a_j)_x = \sum_{x \in A_i \cap A_j} 1 \pmod 2 = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}$$

If we collect the vectors a_i as the rows of an $m \times n$ matrix A, then

$$AA^T = I_m,$$

where I_m denotes the $m \times m$ identity matrix. Since each column of AA^T is a linear combination of the columns of A, we have

$$m = \mathrm{rk}(AA^T) \leq \mathrm{rk}(A) \leq n,$$

and the result follows. ∎

Effectively, what we have done is shown that the vectors a_i are linearly independent in $\mathbb{Z}_2^n$. Since $\dim(Z_2^n) = n$, there are at most n of the a_i.

To prove that our construction in the case of even-size clubs is optimal, we use the following definition and lemma from linear algebra:

5.1.2 DEFINITION. Let W be a vector space with inner product $\langle \cdot, \cdot \rangle$. Let V be a linear subspace of W. The *orthogonal complement* of V is

$$V^\perp := \{w \in W : \langle v, w \rangle = 0 \text{ for all } v \in V\}.$$

It is easily seen that $V^\perp$ is a vector space, and that $(V^\perp)^\perp = V$. Moreover, we have the following:

5.1.3 LEMMA. *Let V be a subspace of an n-dimensional vector space W. Then*

$$\dim(V) + \dim(V^\perp) = n.$$

If V happened to be the rowspace of a matrix A, then this is a reformulation of the *rank-nullity theorem*.

5.1.4 THEOREM. *Let $\mathscr{F}$ be a family of subsets of $[n]$ such that, for all $A, B \in \mathscr{F}$ with $A \neq B$, we have $|A \cap B|$ is even and $|A|$ is even. Then $|\mathscr{F}| \leq 2^{\lfloor n/2 \rfloor}$.*

Proof: Construct vectors a_i as before. Note that now $\langle a_i, a_j \rangle = 0$ for all $i, j \in [m]$. Moreover, $\langle a_i + a_j, a_k \rangle = 0$, so we conclude that the vectors a_i are contained in the linear subspace

$$V := \{v \in \mathbb{Z}_2^n : \langle v, a_i \rangle = 0 \text{ for all } i \in [m]\}.$$

The key observation* here is that $V \subseteq V^\perp$. Now we use the dimension formula:

$$n = \dim(V) + \dim(V^\perp) \geq \dim(V) + \dim(V),$$

so $\dim(V) \leq n/2$, and hence V has at most $2^{\lfloor n/2 \rfloor}$ vectors. The a_i are among these, so the result follows. ∎

*This may look weird, and would never happen in vector spaces over $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ unless $V = \{0\}$. But finite fields are different: a nonzero vector can be orthogonal to itself, for starters.

5.2 Fisher's Inequality

We prove the following generalization of the De Bruijn-Erdős Theorem (though we make no attempt to classify the extremal cases):

5.2.1 THEOREM (Fisher's Inequality). *Let k be an integer, and let $\mathscr{F}$ be a family of subsets of $[n]$ such that $|A \cap B| = k$ for all $A, B \in \mathscr{F}$ with $A \neq B$. Then $|\mathscr{F}| \leq n$.*

Proof: Suppose $\mathscr{F} = \{A_1, \ldots, A_m\}$. Associate to each A_i a vector $a_i \in \mathbb{R}^n$ as follows (note that we use a different field from before!):

$$(a_i)_j = \begin{cases} 1 & \text{if } j \in A_i \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$\langle a_i, a_j \rangle = \begin{cases} |A_i| & \text{if } i = j \\ k & \text{if } i \neq j. \end{cases}$$

We will show that the a_i are linearly independent. Suppose not. Then there exist $\alpha_1, \ldots, \alpha_m$, not all zero, such that

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

Note that at least two of the α_i must be nonzero. Now

$$0 = \left\langle \sum_{i=1}^{m} \alpha_i a_i, \sum_{j=1}^{m} \alpha_j a_j \right\rangle = \sum_{i=1}^{m} \alpha_i^2 \langle a_i, a_i \rangle + \sum_{i \neq j} \alpha_i \alpha_j \langle a_i, a_j \rangle$$
$$= \sum_{i=1}^{m} \alpha_i^2 |A_i| + \sum_{i \neq j} k \alpha_i \alpha_j = \sum_{i=1}^{m} \alpha_i^2 (|A_i| - k) + k \left(\sum_{i=1}^{m} \alpha_i \right)^2.$$

Note that $|A_i| \geq k$ for all i, and that we can have $|A_i| = k$ at most once. Since $\alpha_i \neq 0$ for at least two of the coefficients, the right-hand side of this equation is strictly greater than zero, a contradiction.

Hence the a_i are linearly independent. They are vectors in $\mathbb{R}^n$, so there are at most n of them. ∎

5.3 The vector space of polynomials

We obtained our results so far by associating a vector to each member of the structure, and showing that these vectors are linearly independent, thus bounding the size of the structure. In this section we will repeat this trick, but with a twist: our vectors are now *functions*.

Let Ω be any set, and $\mathbb{F}$ a field. We denote the space of all functions $f : \Omega \to \mathbb{F}$ by $\mathbb{F}^\Omega$. It is easy to verify that this is indeed a vector space. Our key lemma is the following:

5.3.1 LEMMA (Independence Criterion). *Let $f_1, \dots, f_m$ be functions in $\mathbb{F}^\Omega$, and let $v_1, \dots, v_m \in \Omega$ be such that*

- *$f_i(v_i) \neq 0$ for all i;*
- *$f_i(v_j) = 0$ for all $j < i$.*

Then $f_1, \dots, f_m$ are linearly independent.

Proof: Suppose not. Then there exist $\lambda_1, \dots, \lambda_m \in \mathbb{F}$, not all zero, such that

$$g := \lambda_1 f_1 + \cdots + \lambda_m f_m = 0.$$

Let $j \in [m]$ be the least index such that $\lambda_j \neq 0$. Write

$$0 = g(v_j) = \sum_{i \leq j} \lambda_i f_i(v_j) + \sum_{j<i} \lambda_i f_i(v_j) = \lambda_j f_j(v_j) \neq 0,$$

a contradiction. ∎

As a first application, consider the following problem:

5.3.2 PROBLEM. Let $c, d \in \mathbb{R}$, and let $A \subset \mathbb{R}^n$ be a set of vectors such that $\|x - y\| \in \{c, d\}$ for all $x, y \in A$. How large can A be?

We call A a *two-distance set*.

If $c = d$, that is, if A is a one-distance set, then it is not hard to show that $|A| \leq n+1$. For two distances it is not very hard to do better:

5.3.3 EXERCISE. Show that there exists a two-distance set of size $\binom{n}{2}$.

Interestingly, that number is nearly tight!

5.3.4 THEOREM. *Every two-distance set in $\mathbb{R}^n$ has at most $\frac{1}{2}(n+1)(n+4)$ points.*

Proof: Suppose $A = \{a_1, \dots, a_m\}$ is a two-distance set with distances c, d. Define, for $i \in [m]$,

$$f_i(x) := \left(\|x - a_i\|^2 - c^2\right)\left(\|x - a_i\|^2 - d^2\right).$$

Then $f_i(a_i) = c^2 d^2 \neq 0$, and $f_i(a_j) = 0$ for $i \neq j$, so by Lemma 5.3.1 the f_i are linearly independent. To bound m, then, it suffices to find a low-dimensional space containing all of the f_i. If we look at the expansion, we see that each f_i is a linear combination of

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

Hence $f_1, \dots, f_m \subseteq V$ for some vector space V of dimension at most $1 + n + \frac{1}{2}n(n+1) + n + 1 = \frac{1}{2}(n+1)(n+4)$, and therefore $m \leq \frac{1}{2}(n+1)(n+4)$. ∎

Note that a better bound, due to Blokhuis (1984), is $\frac{1}{2}(n+1)(n+2)$. The key is to see that the functions $x_1, x_2, \dots, x_n, 1$ can be added to $f_1, \dots, f_m$, and the result *still* forms a linearly independent set!

Our second application is a generalization of the De Bruijn-Erdős Theorem in a slightly different direction:

5.3.5 DEFINITION. Let $L \subset \{0,1,\ldots,n\}$. A family $\mathscr{F}$ of subsets of $[n]$ is *L-intersecting* if $|A \cap B| \in L$ for all $A, B \in \mathscr{F}$ with $A \neq B$.

We wish to bound the size of an L-intersecting family. If $L = \{0,1,\ldots,l-1\}$ then a simple idea is to take $\mathscr{F} = \{X \in [n] : |X| \leq l\}$. As it turns out, no family can beat this construction, regardless of the choice of L:

5.3.6 THEOREM. *Let $L \subset \{0,1,\ldots,n\}$, and let $\mathscr{F}$ be an L-intersecting family of subsets of $[n]$. Then*

$$|\mathscr{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}.$$

Proof: Let $\mathscr{F} = \{A_1,\ldots,A_m\}$, and suppose the sets are sorted so that $|A_i| \leq |A_j|$ if $i < j$. Let $a_i := (a_{i1},\ldots,a_{in})$ be the incidence vector:

$$a_{ij} = \begin{cases} 1 & \text{if } j \in A_i \\ 0 & \text{otherwise.} \end{cases}$$

For $i \in [m]$, define $f_i : \mathbb{R}^n \to \mathbb{R}$ by

$$f_i(x) := \prod_{l \in L : l < |A_i|} \left(\langle a_i, x \rangle - l \right).$$

Note that

$$f_i(a_i) = \prod_{l \in L : l < |A_i|} \left(|A_i| - l \right) > 0,$$
$$f_i(a_j) = 0 \qquad \text{for } j < i,$$

since $\langle a_i, a_j \rangle = |A_i \cap A_j| < |A_i|$.

It follows that the f_i are linearly independent, and again we must find a small-dimensional subspace containing them all. The degree of each f_i is at most $|L|$, but a trick gets us better results. Note that all deductions above remain true if we interpret the f_i as functions $\{0,1\}^n \to \mathbb{R}$. This allows us to replace each term x_i^k by x_i itself! So each term in the expansion of f_i will be a monomial in which each x_j occurs at most once. There are precisely

$$\sum_{k=0}^{|L|} \binom{n}{k}$$

such monomials. ∎

Finally, we sketch a "modular version" of the theorem:

5.3.7 THEOREM. *Let p be a prime, let $L \subset \mathbb{Z}_p$, and suppose $\mathscr{F}$ is such that*

- *$|A| \notin L \pmod p$ for all $A \in \mathscr{F}$;*
- *$|A \cap B| \in L \pmod p$ for all $A, B \in \mathscr{F}$ with $A \neq B$.*

Then

$$|\mathscr{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}.$$

Sketch of proof: Define the polynomials $f_i : \mathbb{Z}_p^n \to \mathbb{Z}_p$ by

$$f_i(x) := \prod_{l \in L} \left(\langle a_i, x \rangle - l \right).$$

Follow the proof of the previous theorem. ∎

5.4 Some applications

We study some applications of the linear algebra method in general, starting with a few applications of the various theorems proven so far.

5.4.1 Lines in $\mathbb{R}^2$

Our first application deals with classical geometry in the plane. For any two points in the plane there is a unique line meeting those points.

5.4.1 THEOREM. *Let $\mathscr{P}$ be a set of n points in $\mathbb{R}^2$, such that not all points lie on a single line. Then these points determine at least n lines.*

Proof: Let $\mathscr{L}$ be the set of lines determined by the points $\mathscr{P}$. For each $x \in \mathscr{P}$, let $A_x := \{l \in \mathscr{L} : x \in l\}$. Note that $|A_x| \geq 2$ (otherwise all points would lie on a single line), $A_x \neq A_y$ if $x \neq y$ (since two lines determine a point), and $|A_x \cap A_y| = 1$ (since two points define a unique line). It follows from Theorem 5.2.1, applied to the sets A_x, that $|\mathscr{P}| \leq |\mathscr{L}|$. ∎

Note that, since we used only the most elementary facts about lines, the proof holds for any projective or affine plane. As an aside we cannot resist mentioning a classical theorem that *does* require the plane to be Euclidean:

5.4.2 THEOREM (Sylvester-Gallai). *Let $\mathscr{P}$ be a set of n points in $\mathbb{R}^2$, not all on a line. Then some line contains exactly two of the points.*

Proof: Let $\mathscr{L}$ be the set of lines determined by $\mathscr{P}$. Consider the set of pairs (x, l) with $x \in \mathscr{P}$, $l \in \mathscr{L}$, and $x \notin l$. Pick a pair (x_0, l_0) minimizing the distance $d(x, l)$ between the point and the line. Let q be the point on l_0 closest to x_0. See Figure 5.1. If l_0 contains three points, at least two of them will not be separated by q. Say these are y, z, labeled so $d(y, q) < d(z, q)$. Now let l_1 be the line through x_0 and z. Then $d(y, l_1) < d(x_0, l_0)$, a contradiction. So l_0 contains only two points. ∎

5.4.2 Explicit Ramsey graphs

We consider Corollary 3.1.2, which states that every sufficiently large graph contains either a big clique or a big stable set. But how large, precisely, is "sufficiently large"?

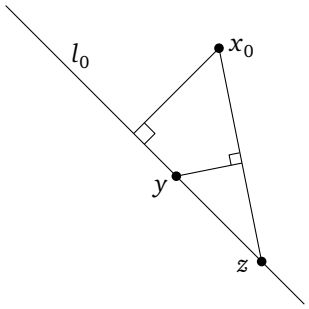


FIGURE 5.1
The proof of the Sylvester-Gallai Theorem

To answer that, we need to construct the largest possible graphs *without* a big clique and *without* a big stable set. Let's call such graphs *Ramsey graphs*. We have seen (in Theorem 3.6.1) that $R(k;2) \geq 2^{k/2}$. However, the proof does not tell us how to construct graphs attaining that bound. Since such graphs can be useful, it is worthwhile looking at constructions.

5.4.3 THEOREM. *Let k be an integer, and let G be a graph having as vertex set all size-3 subsets of $[k]$. Two vertices A and B are adjacent if and only if $|A \cap B| = 1$. Then G has neither a clique nor an stable set of size more than k.*

Since G has roughly k^3 edges, it follows that $R(k;2) = \Omega(k^3)$.

Proof: Let Q be a clique. By Theorem 5.2.1 we have $|Q| \leq k$. Let Q be a stable set. By Theorem 5.1.1 we have $|Q| \leq k$. ∎

We can, in fact, show a stronger lower bound using similar ideas:

5.4.4 THEOREM. *For every prime p, there exists a graph G on $\binom{p^3}{p^2-1}$ vertices such that each clique and each independent set has size at most*

$$\sum_{i=0}^{p-1} \binom{p^3}{i}.$$

This graph has about p^{p^2} vertices, and the largest clique and stable set have size about p^p, so $R(k;2) = \Omega(k^p) = \Omega(k^{\log k/\log\log k})$.

Proof: Let G be a graph having as vertex set all size-(p^2-1) subsets of $[p^3]$. Two vertices A and B are adjacent if and only if $|A \cap B| \neq p-1 \pmod p$.

If $A_1, \ldots, A_k$ is a clique, then choose $L = \{0, 1, \ldots, p-2\}$. Theorem 5.3.7 then implies $k \leq \sum_{i=0}^{p-1} \binom{p^3}{i}$.

If $A_1, \ldots, A_k$ is a stable set, then choose $L = \{p-1, 2p-1, \ldots, p^2-p-1\}$. Now we apply Theorem 5.3.6 to conclude again that $k \leq \sum_{i=0}^{p-1} \binom{p^3}{i}$. ∎

5.4.3 Borsuk's Conjecture refuted

In 1932, Borsuk conjectured the following:

5.4.5 CONJECTURE. *Every set $S \subset \mathbb{R}^d$ of bounded diameter $\sup\{\|x-y\| : x, y \in S\}$ can be split into $d+1$ parts, each of which has smaller diameter.*

It is easy to prove that d parts don't suffice (do this!), and the conjecture was proven in some special cases: $d = 2, 3$, any d when S is smooth, and so on.

It came as a shock, then, that Kahn and Kalai *disproved* the conjecture in 1993!

5.4.6 THEOREM. *For sufficiently large d there exists a set $S \subset \mathbb{R}^d$ of bounded diameter, such that any partition of S into fewer than $1.2^{\sqrt{d}}$ parts contains some part of the same diameter as S.*

We start with a lemma:

5.4.7 LEMMA. *For p prime, there are $\frac{1}{2}\binom{4p}{2p}$ vectors $F \subseteq \{-1,1\}^{4p}$ such that every subset of $2\binom{4p}{p-1}$ of them contains an orthogonal pair.*

Proof: Let $\mathscr{F}$ be the size-$2p$ subsets of $[4p]$ containing 1. For each $A \in \mathscr{F}$ define a vector a by $a_i = 1$ if $i \in A$ and $a_i = -1$ otherwise. Let F be this set of vectors, and pick $a, b \in F$. Now

$$\langle a, b\rangle = \sum a_i b_i = 0 \text{ if and only if } |A \cap B| = p.$$

This is because positive and negative terms need to cancel, so $|A \triangle B| = 2p$, which implies $|A \cap B| = p$. Since $1 \le |A \cap B| \le 2p-1$, we have that $\langle a, b\rangle = 0$ if and only if $|A \cap B| = 0 \pmod p$.

Now consider a subset $G \subseteq F$ without orthogonal pair. Then the corresponding subset family $\mathscr{G}$ satisfies $|A| = 0 \pmod p$ for all $A \in \mathscr{G}$, and $|A \cap B| \in \{1, 2, \ldots, p-1\} \pmod p$. It follows from Theorem 5.3.7 that

$$|\mathscr{G}| \le \sum_{k=0}^{p-1} \binom{4p}{k} < 2\binom{4p}{p-1}. \qquad \blacksquare$$

Proof of Theorem 5.4.6: We can find hard-to-avoid orthogonal pairs using the previous lemma; our next task is to turn these into maximum-distance pairs of vectors in a set S. We use tensors for this purpose. Given a set $F \subseteq \mathbb{R}^{4p}$ as defined by the lemma, we define

$$S := \{v \otimes v : v \in F\} \subseteq \mathbb{R}^{n^2}.$$

Here an element $w = v \otimes v \in S$ is defined by $w_{ij} = v_i \cdot v_j$. We have the following properties (which are not hard to verify) for $w, w' \in S$ with $w = v \otimes v$ and $w' = v' \otimes v'$:

(*i*) $w \in \{-1,1\}^{n^2}$;
(*ii*) $\|w\| = \sqrt{n^2} = n$;
(*iii*) $\langle w, w'\rangle = \langle v, v'\rangle^2 \ge 0$;

(*iv*) w, w' are orthogonal if and only if v, v' are orthogonal;

(*v*) $\|w-w'\|^2 = \|w\|^2+\|w'\|^2-2\langle w,w'\rangle = 2n^2-2\langle v,v'\rangle^2 \leq 2n^2$, which is maximized when w, w' are orthogonal.

If we wish to partition S into subsets of strictly smaller diameter, each of those subsets has to have size less than $2\binom{4p}{p-1}$ by our lemma. Hence the number of subsets needs to be at least

$$\frac{|S|}{2\binom{4p}{p-1}} = \frac{\frac{1}{2}\binom{4p}{2p}}{2\binom{4p}{p-1}} = \frac{(3p+1)(3p)(3p-1)\cdots(2p+2)(2p+1)}{4(2p)(2p-1)\cdots(p+1)(p)} \geq \left(\frac{3}{2}\right)^{p-1}.$$

Since the dimension $d = n^2 = (4p)^2$, it follows that the number of parts must be at least $(3/2)^{\sqrt{d}/4-1}$. The actual bound stated in the theorem requires a slightly more careful analysis. ∎

5.5 Gessel-Viennot and Cauchy-Binet

Let M be an $n \times n$ matrix with entries m_{ij}. The *determinant* of M is

$$\det(M) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) m_{1\sigma(1)} m_{2\sigma(2)} \cdots m_{n\sigma(n)},$$

where S_n is the set of all permutations of $[n]$, and $\operatorname{sgn}(\sigma)$ is the sign: $+1$ for *even* permutations and -1 for *odd* permutations, where even and odd refer to the number of two-cycles when we write σ as a product of (non-disjoint) two-cycles. To refresh your memory: if $\sigma = \{5,2,1,3,4\}$ (i.e. 1 gets mapped to 5, 2 to 2, and so on), then, for instance,

$$\sigma = (1,5)(3,5)(4,5),$$

so $\operatorname{sgn}(\sigma) = -1$ (and this is independent of the particular 2-cycles, or transpositions, we use).

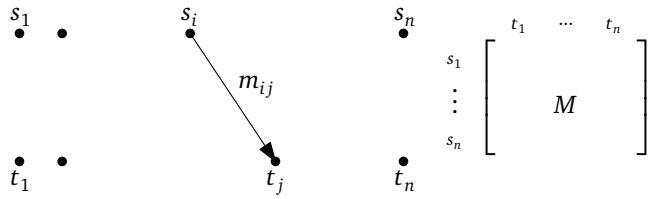


FIGURE 5.2
From a matrix to a directed graph

We will go through some lengths to reformulate this in terms of directed graphs. Indeed: consider a directed graph $D = (V,A)$ with $V = \{s_1, \ldots s_n, t_1, \ldots, t_n\}$ and $A = \{(s_i, t_j) : i, j \in [n]\}$. We assign to each directed edge (s_i, t_j) a number, which we call its *weight*. Let the weight of (s_i, t_j) in D be equal to m_{ij}. A *path system* is a collection of directed paths $\mathscr{P}_\sigma := \{s_1 \to t_{\sigma(1)}, \ldots, s_n \to t_{\sigma(n)}\}$. Note that each path consists of a

single directed edge. The *weight* of a path system is the product of the weights of the paths, and is denoted by $w(\mathscr{P}_\sigma)$. Now

$$\det(M) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) w(\mathscr{P}_\sigma).$$

The observation of Gessel and Viennot was that we can do essentially the same for other directed graphs! We generalize our definitions. In what follows, $D = (V,A)$ will be an *acyclic* directed graph, and $w : E \to \mathbb{R}$ a function assigning a weight to each directed edge. Denote by $P : s \to t$ the fact that P is a directed path starting in s and ending in t. The weight of a path is

$$w(P) := \prod_{e \in P} w(e),$$

so if $s = t$ then $w(P) = 1$. Now let $S = \{s_1, \ldots s_n\}$ and $T = \{t_1, \ldots, t_n\}$ be sets of vertices of D.

5.5.1 DEFINITION. A *path system* $\mathscr{P}$ is a collection $\{P_1, \ldots, P_n\}$ of directed paths in D such that, for some permutation σ of $[n]$, we have $P_i : s_i \to t_{\sigma(i)}$ for all $i \in [n]$. The *sign* of a path system is $\operatorname{sgn}(\mathscr{P}) = \operatorname{sgn}(\sigma)$.

The *weight* of a path system is

$$w(\mathscr{P}) := \prod_{i=1}^{n} w(P_i).$$

Define a matrix $M = (m_{ij})$ by

$$m_{ij} := \sum_{P : s_i \to t_j} w(P),$$

i.e. the sum of the weights of all directed $s_i \to t_j$ paths. Then we have

5.5.2 LEMMA (Gessel-Viennot).

$$\det(M) = \sum_{\mathscr{P}} \operatorname{sgn}(\mathscr{P}) w(\mathscr{P}),$$

where the sum ranges over all path systems where the paths are pairwise vertex-disjoint.

The fact that the sum is only over vertex-disjoint paths is what makes the lemma so useful, as we will see in the two applications we'll discuss.

Proof: Plugging the definition of m_{ij} into the determinant formula, we get

$$\begin{aligned}\det(M) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(\sum_{P_1 : s_1 \to t_{\sigma(1)}} w(P_1) \right) \left(\sum_{P_2 : s_2 \to t_{\sigma(2)}} w(P_2) \right) \cdots \left(\sum_{P_n : s_n \to t_{\sigma(n)}} w(P_n) \right) \\ &= \sum_{\mathscr{P}} \operatorname{sgn}(\mathscr{P}) w(\mathscr{P}),\end{aligned}$$

where the sum in the second line is over *all* path systems, including the non-disjoint ones! Let N be the set of all non-vertex-disjoint path systems. The result follows if we can show

$$\sum_{\mathscr{P}\in N} \operatorname{sgn}(\mathscr{P})w(\mathscr{P}) = 0.$$

To that end we will show that there is an involution $\pi : N \to N$ without fixed points, such that for $\mathscr{P}$ and $\pi(\mathscr{P})$ we have

$$w(\mathscr{P}) = w(\pi(\mathscr{P})) \qquad \text{and} \qquad \operatorname{sgn}(\mathscr{P}) = -\operatorname{sgn}(\pi(\mathscr{P})).$$

We construct π as follows. Pick any $\mathscr{P} \in N$. Let i_0 be the least index i such that path P_i meets another path P_j. Let v be the first vertex on P_{i_0} shared by another path, and let j_0 be the least index larger than i_0 such that P_{j_0} meets v. Now we define

$$\pi(\mathscr{P}) = (P'_1, \ldots, P'_n)$$

by

- $P'_k = P_k$ for $k \neq i_0, j_0$;
- P'_{i_0} is the path $s_{i_0} \to t_{\sigma(j_0)}$ following P_{i_0} until v and P_{j_0} from v;
- P'_{j_0} is the path $s_{j_0} \to t_{\sigma(i_0)}$ following P_{j_0} until v and P_{i_0} from v.

Since v exists and is not one of the t_i, we have that $\pi(\mathscr{P}) \neq \mathscr{P}$. Moreover, $\operatorname{sgn}(\pi(\mathscr{P})) = -\operatorname{sgn}(\mathscr{P})$ (since the new permutation was obtained from the old by one extra transposition), and $\pi(\pi(\mathscr{P})) = \mathscr{P}$. Finally, the two path systems have the same set of edges, so $w(\pi(\mathscr{P})) = w(\mathscr{P})$. The result follows. ∎

5.5.1 Lattice paths

As a first application, consider the following problem, which first led Gessel and Viennot to their lemma:

5.5.3 PROBLEM. Given positive integers $a_1 < a_2 < \cdots < a_n$ and $b_1 < b_2 < \cdots < b_n$, what is

$$\det \begin{bmatrix} \binom{a_1}{b_1} & \cdots & \binom{a_1}{b_n} \\ \vdots & & \vdots \\ \binom{a_n}{b_1} & \cdots & \binom{a_n}{b_n} \end{bmatrix}?$$

We place points $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$ on the 2-dimensional grid, with s_i at position $(0, -a_i)$ and t_j at $(b_j, -b_j)$. We direct the lattice edges north and east. The number of $s_i \to t_j$ paths is

$$\binom{b_j + (a_i - b_j)}{b_j} = \binom{a_i}{b_j},$$

precisely the entry (i, j) of our matrix. Note that the graph is planar, so vertex-disjoint paths cannot cross. Hence the only option for a vertex-disjoint path system is to have the identity permutation. From our lemma we now have

$$\det\left(\binom{a_i}{b_j}\right) = \text{number of vertex-disjoint path systems } \{s_1 \to t_1, \ldots, s_n \to t_n\}.$$

It follows in particular that this determinant is nonnegative, and zero precisely when $a_i < b_i$ for some i.

5.5.2 The Cauchy-Binet Formula

A second result, which has a number of different proofs and many applications, is the following.

5.5.4 THEOREM (Cauchy-Binet). *Let A be an $r \times n$ matrix, and B an $n \times r$ matrix, where $n \geq r$. Then*

$$\det(AB) = \sum_{X \subseteq [n]:|X|=r} (\det(A_X))(\det(B_X)),$$

where A_X is the $r \times r$ submatrix of A with columns indexed by X ,and B_X is the $r \times r$ submatrix of B with rows indexed by X.

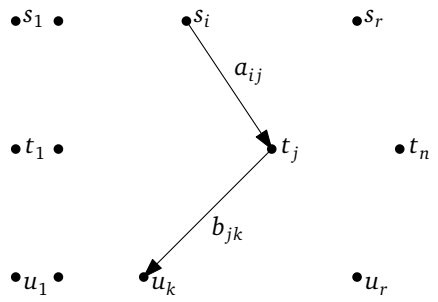


FIGURE 5.3
Proof of the Cauchy-Binet formula, detail

Proof: Index the rows of A by a set S and the columns by a set T. Index the rows of B by T again, and the columns of B by a set U. Construct, for each matrix, a bipartite graph as at the start of Section 5.5, and identify the vertex set T of one with the vertex set T of the other. See Figure 5.3.

The path matrix of this directed graph has entries

$$m_{ij} = \sum_{k=1}^{n} a_{ij} b_{jk}$$

so $M = AB$. By the Gessel-Viennot Lemma,

$$\det(AB) = \det(M) = \sum_{\mathscr{P}} \operatorname{sgn}(\mathscr{P}) w(\mathscr{P}).$$

Now it is just a matter of observing that each path system $S \to U$ breaks up into a path system $S \to X$ and a path system $X \to U$, where $X \subseteq T$ has size r. For fixed X, we need the additional observation that $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. Summing over all these pairs yields the result. ∎

5.6 Kirchhoff's Matrix-Tree Theorem

We will use the theory from the previous section, in particular the Cauchy-Binet formula, to solve a counting problem:

5.6.1 PROBLEM. Given a connected graph G, determine the number of spanning trees of G.

Since we don't know in advance what G is, the answer should be an *algorithm*. A slow algorithm would be the following recursion:

- Given a forest F, find an edge e not spanned by F;
- Count:
  - The number of trees that extend $F \cup \{e\}$;
  - The number of trees that extend F and do not use e.
- Return the sum of the two.

The desired number is then the count obtained by starting with an edgeless forest F.

The algorithm just described takes, in the worst case, about $2^{|E|}$ steps, which quickly becomes impractical. While it is still useful for theoretical purposes (see Section 11.2), we would like a more efficient algorithm. And the following result, due to Kirchhoff (of circuit law fame), gives just that:

5.6.2 THEOREM (Kirchhoff). *Let $G = (V, E, \iota)$ be a connected multigraph without loops, having $V = [n]$. Let $F = (a_{ij})$ be the adjacency matrix of G, given by*

$$a_{ij} = \textit{the number of edges from } i \textit{ to } j.$$

Let $D = (d_{ij})$ be the diagonal matrix such that $d_{ii} = \deg(i)$.

Let Q be any $(n-1) \times (n-1)$ principal submatrix of $D - F$. Then $\det(Q)$ equals the number of spanning trees of G.

Note that building Q from a given graph takes (depending on the data structure) roughly $O(n^2)$ steps, and computing the determinant roughly $O(n^3)$ steps. This is a huge improvement over our first algorithm! We need a few lemmas:

5.6.3 LEMMA. *$D - F = AA^T$, where A is the signed incidence matrix of G. That is, A is an $[n] \times E$ matrix (i.e. rows are labeled by the set $[n] = V$ and columns by the set E) with entries*

$$a_{ve} = \begin{cases} -1 & \text{if } e = uv, \text{ and } v < u \\ 1 & \text{if } e = uv, \text{ and } v > u \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Consider a diagonal entry of $R := AA^T$. Then

$$R_{vv} = \sum_{e \in E} a_{ve}^2 = \sum_{e \text{ incident with } v} 1 = \deg(v).$$

And an off-diagonal entry:

$$R_{uv} = \sum_{e \in E} a_{ue} a_{ve} = \sum_{e \in E : e = uv} (-1) \cdot 1.$$

■

Note that the result remains valid if we scale some columns of A by -1. Hence we may reorder the vertices if we feel so inclined.

5.6.4 LEMMA. *A subset $X \subseteq E$ of columns of A is linearly independent if and only if X contains no cycle (in G).*

Proof: Consider a submatrix corresponding to a cycle. After reordering the vertices and edges, and scaling some of the columns, this matrix looks like

$$\begin{bmatrix} -1 & & & & & 1 \\ 1 & -1 & & & & \\ & 1 & -1 & & & \\ & & 1 & -1 & & \\ & & & 1 & -1 & \\ 0 & & \cdots & & 0 & \\ \vdots & & & & \vdots & \\ 0 & & \cdots & & 0 & \end{bmatrix},$$

where omitted entries are 0. Since the columns add up to the all-zero vector, this set of columns is linearly dependent.

For the converse, we argue by induction on $|X|$, the case $|X| = 0$ being trivial. Otherwise, since the subgraph corresponding to X is a forest, there must be some vertex v of degree 1. The submatrix then looks like

$$\begin{array}{c} \\ v \end{array} \overset{e}{\left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline -1 & & & \\ & & H & \\ & & & \end{array}\right]},$$

and it is singular if and only if the submatrix H corresponding to $X \setminus \{e\}$ is singular. ■

5.6.5 LEMMA. *If H is a square submatrix of A then* $\det(H) \in \{-1, 0, 1\}$.

Proof: Suppose not. Let H be a square submatrix with different determinant, and choose H as small as possible. Then H has no all-zero rows. If a row has exactly one nonzero entry, then that entry is 1 or -1, and by developing with respect to this row we find a smaller violating submatrix, a contradiction. Hence each row (and by symmetry each column) has at least two nonzero entries. But each column has at most two nonzero entries, so this number must be exact. By counting the total number of nonzero entries, also each row must have exactly two. But then the corresponding subgraph is a union of cycles, and hence $\det(H) = 0$, by the previous lemma. ■

Proof of the Matrix-Tree Theorem: Let A' be the matrix obtained from A by removing the row corresponding to vertex i. Note that since the sum of all rows of A is zero, we can recover this row uniquely. We know from Lemma 5.6.4 that a subset $X \subseteq E : |X| = n-1$ indexes an independent subset of columns if and only if the corresponding subgraph is a spanning tree. By the Cauchy-Binet formula we find

$$\begin{aligned} \det(A'(A')^T) &= \sum_{X \subseteq E : |X| = n-1} \det(A'_X) \det((A'_X)^T) = \sum_{X \subseteq E : |X| = n-1} \det(A'_X)^2 \\ &= \sum_{\substack{X \subseteq E : |X| = n-1 \\ X \text{ spanning tree}}} 1, \end{aligned}$$

where the last equality uses that $\det(A'_X) \in \{-1,0,1\}$, and is nonzero if and only if X is a spanning tree. The result follows by noting that $Q = A'(A')^T$. ∎

We conclude this section with the advertised (third) proof of Cayley's theorem.

Third proof of Theorem 2.2.1: Any tree on n vertices is a spanning tree of the complete graph K_n, so we can apply the Matrix-Tree Theorem. We get that the number of spanning trees of K_n is equal with $\frac{1}{n}\lambda_1 \dots \lambda_{n-1}$, where $\lambda_1, \dots, \lambda_{n-1}$ are the non-zero eigenvalues of the Laplacian matrix

$$L = \begin{bmatrix} n-1 & -1 & \cdots & -1 \\ -1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & n-1 \end{bmatrix} = nI - J,$$

where J is the $n \times n$ matrix of ones.

Note that J has the ones vector as one of its eigenvectors. The remaining $n-1$ eigenvectors are of the form

$$\begin{bmatrix} \vdots \\ 1 \\ -1 \\ \vdots \end{bmatrix}$$

so J has eigenvalues $n, 0, \dots, 0$, with 0 having multiplicity $n-1$. This implies that L has eigenvalues $0, n, \dots, n$, with n having multiplicity $n-1$. So, the number of spanning trees of K_n equals $n^{n-1}/n = n^{n-2}$. ∎

5.7 Totally unimodular matrices

The signed incidence matrix of a graph is an example of a class of very special matrices with interesting combinatorial properties:

5.7.1 DEFINITION. A matrix A is *totally unimodular* (TU) if, for every square submatrix D of A, we have $\det(D) \in \{-1,0,1\}$.

In this section we will give a characterization of these matrices in a way that is similar to Kuratowski's Theorem for graphs (Theorem A.7.7):

5.7.2 THEOREM. *Let A be a $\{0,1\}$-matrix. The following are equivalent:*

(i) A has a TU signing;

(ii) A cannot be transformed to

$$M(F_7) = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

by repeatedly carrying out the following operations:

- *deleting rows, columns*

- *permuting rows, columns*
- *transposing the matrix*
- *pivoting over* $\mathbb{Z}_2$.

Two terms in this theorem need explaining. A matrix has a *TU signing* if we can change some 1s into (-1)s to obtain a TU matrix.

The operation of a *pivot* does the following (where (x, y) can index an arbitrary entry, but for the sake of simplicity we assume it has been brought to the top left by row and column swaps):

$$\begin{array}{c} \\ x \end{array}\!\!\begin{array}{c} \begin{array}{cc} y & \end{array} \\ \left[\begin{array}{c|c} \alpha & c \\ \hline b & D \end{array}\right] \end{array} \to \begin{array}{c} \\ y \end{array}\!\!\begin{array}{c} \begin{array}{cc} x & \end{array} \\ \left[\begin{array}{c|c} \alpha^{-1} & \alpha^{-1}c \\ \hline -b\alpha^{-1} & D-\alpha^{-1}bc \end{array}\right] \end{array}.$$

This operation will look weird at first. A less opaque description is the following: we prepend an identity column to the matrix (which we index by x), then row-reduce the column indexed by y, and finally delete the column indexed by y:

$$\begin{array}{c} \begin{array}{ccc} x & y & \end{array} \\ \left[\begin{array}{c|c|c} 1 & \alpha & c \\ \hline 0 & b & D \end{array}\right] \end{array} \to \begin{array}{c} \begin{array}{ccc} x & y & \end{array} \\ \left[\begin{array}{c|c|c} \alpha^{-1} & 1 & \alpha^{-1}c \\ \hline 0 & b & D \end{array}\right] \end{array} \to$$

$$\to \begin{array}{c} \begin{array}{ccc} x & y & \end{array} \\ \left[\begin{array}{c|c|c} \alpha^{-1} & 1 & \alpha^{-1}c \\ \hline -b\alpha^{-1} & 0 & D-\alpha^{-1}bc \end{array}\right] \end{array}.$$

The reason to do this is the following. It is easy to show that a matrix A is TU if and only if $[I\ A]$ is TU. We implicitly keep an identity matrix in front of A in mind, with columns indexed by the rows of A.

Note that the definition of pivoting is valid for any field (and, in fact, for any ring – commutative or not). The theorem specifies pivoting over $\mathbb{Z}_2$.

Theorem 5.7.2 is due to Tutte, who gave an intricate proof. A very clean and beautiful proof was given by Gerards (1989). We can do no better than refer to that paper for the proof, which takes up only a few pages.

5.8 Where to go from here?

- Jukna (2011), *Extremal Combinatorics* should, once again, be your first stop.
- Matoušek (2010), *Thirty-three miniatures* is a small but beautiful book, containing thirty-three lecture-size chapters on applications of linear algebra, mostly in combinatorics.
- Aigner and Ziegler (2010), *Proofs from THE BOOK* is the source of our treatment of Kirchhoff's Matrix-Tree Theorem.

Totally unimodular matrices play a key role in combinatorial optimization, as well as in the field of matroid theory. We will introduce matroids in the next chapter. A good book introducing combinatorial optimization is

- Cook, Cunningham, Pulleyblank, and Schrijver (1998), *Combinatorial Optimization*,

but there are many others.

CHAPTER 6

The probabilistic method

We have already seen an example of the probabilistic method, a powerful technique in combinatorics, which is most useful to show the existence of certain combinatorial objects. In Theorem 3.6.1 we found a lower bound on Ramsey numbers by establishing the existence of large graphs with a "wrong" coloring. In this chapter we will put the technique on firmer footing.

6.1 Probability basics: spaces and events

Let us start with defining the basic tools of probability.

6.1.1 DEFINITION. A *probability space* is a pair $(\Omega, \Pr)$ of a finite set Ω, the *universe*, and a map $\Pr : \Omega \to \mathbb{R}$, the *measure*, satisfying

- $\Pr(\omega) \geq 0$ for all $\omega \in \Omega$;
- $\sum_{\omega \in \Omega} \Pr(\omega) = 1$.

Note that the notion of a probability space, as well as all definitions below, can be extended to infinite spaces through measure theory. We don't need these complications, so we will stick with finite spaces.

6.1.2 DEFINITION. An *event* is a subset $A \subseteq \Omega$. We write $\Pr(A) := \sum_{\omega \in A} \Pr(\omega)$.

6.1.3 EXAMPLE. Consider a sequence of n coin flips. After each flip we write down an H if the result is heads, and a T if the result is tails. The universe is the set of potential outcomes: strings of Hs and Ts of length n, i.e. $\Omega = \{H, T\}^n$. Since each flip produces heads and tails with equal probability $\frac{1}{2}$, we have that $\Pr(\omega) = 1/2^n$ for all $\omega \in \Omega$.

An example of an event is "The first flip is heads". This event would be the set $\{(HHH\cdots H), (HTH\cdots H), \ldots, (HTT\cdots T)\}$.

6.1.4 DEFINITION. The *complement* of an event A is

$$\overline{A} := \Omega \setminus A.$$

6.1.5 DEFINITION. Events A and B are *independent* if $\Pr(A \cap B) = \Pr(A)\Pr(B)$.

An example of independent events would be "the first flip is heads" and "the last flip is tails", provided $n > 1$. The following is an easy exercise:

6.1.6 LEMMA. *If A and B are independent, then A and $\overline{B}$ are independent.*

6.1.7 DEFINITION. If $\Pr(B) > 0$, then the *conditional probability* of A given B is

$$\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}.$$

Note that $\Pr(\,\cdot \mid B)$ is, itself, a probability measure.

An example would be "heads comes up five times" given "heads comes up the first time". The following three lemmas, whose easy proofs are skipped, will be useful:

6.1.8 LEMMA. *Events A and B are independent if and only if* $\Pr(A \mid B) = \Pr(A)$.

6.1.9 LEMMA. *If A, B, and C are events, then*

$$\Pr(A \mid B \cap C) = \frac{\Pr(A \cap B \mid C)}{\Pr(B \mid C)}.$$

6.1.10 LEMMA. $\Pr(A \cap B \cap C) = \Pr(A \mid B \cap C) \cdot \Pr(B \mid C) \cdot \Pr(C)$.

The tool we used in Theorem 3.6.1 is the following:

6.1.11 THEOREM (Union bound). *Let $A_1, \ldots, A_k$ be events. Then*

$$\Pr(A_1 \cup \cdots \cup A_k) \leq \sum_{i=1}^{k} \Pr(A_i).$$

Proof: Easy exercise. ∎

6.2 Applications

Two-colorability of set systems. Let $H = ([n], \mathscr{F})$ be a collection of subsets of $[n]$, and $\chi : [n] \to \{\text{red, blue}\}$ a coloring. We say χ is a *proper* 2-coloring of H if each $X \in \mathscr{F}$ has elements of both colors. In other words, there exist $u, v \in X$ such that $\chi(u) \neq \chi(v)$. If there exists a proper 2-coloring for H then H is said to be *2-colorable*. We study the following problem:

6.2.1 PROBLEM. Let $H = ([n], \mathscr{F})$ be a set system with $|X| = r$ for all $X \in \mathscr{F}$. Find the maximum value of $|\mathscr{F}|$ such that H is guaranteed to be 2-colorable.

Note that n is not an important parameter here, since increasing it without changing $\mathscr{F}$ will not change the problem. Hence we are looking for an answer in terms of r. Denote this value by $m(r)$. It is easy to obtain an upper bound. If $n \geq 2r - 1$, then the collection of *all* r-subsets is not 2-colorable: by the Pigeonhole Principle, one color is

used at least r times. This shows that

$$m(r) \leq \binom{2r-1}{r} \equiv \frac{4^r}{\sqrt{r}}.$$

For a lower bound on $m(r)$, we use the probabilistic method.

6.2.2 THEOREM. *If $H = ([n], \mathscr{F})$ is a set system with $|X| = r$ for all $X \in \mathscr{F}$, and $|\mathscr{F}| < 2^{r-1}$, then H is 2-colorable.*

Proof: Suppose $|\mathscr{F}| < 2^{r-1}$. Independently color each element red or blue with probability $1/2$. Pick an $X \in \mathscr{F}$. We have

$$\Pr(X \text{ monochromatic}) = \frac{1}{2^r} + \frac{1}{2^r} = \frac{1}{2^{r-1}}.$$

By the union bound we find

$$\Pr(\text{some } X \text{ monochromatic}) \leq \sum_{X \in \mathscr{F}} \Pr(X \text{ monochromatic}) = \frac{|\mathscr{F}|}{2^{r-1}} < 1.$$

Since there is a positive probability that no X is monochromatic, it follows that H must be 2-colorable. ∎

Hence we have

$$2^{r-1} < m(r) \leq 4^r/\sqrt{r},$$

showing that $m(r)$ grows exponentially in r. A typical feature of proofs using the probabilistic method is that a gap is left between the lower and upper bounds.

Winners in tournaments. A tournament is a complete graph in which each edge has been given a direction (see also Definition A.8.2). We can interpret these edges as outcomes of matches between teams, with the edge pointing from the winner to the loser of that match. We write $x \to y$ if team x beats team y. How can we determine an overall winner?

A clear winner would be a team that beats all others, but those situations are rare. A different option is to define a *set* of winners, as follows: a subset X of the vertices is a winning set if each team outside X was beaten by at least one team in X. This gives a lot more flexibility, so one might wonder if there is a value k so that any tournament has a winning set of size k. The following result refutes this:

6.2.3 THEOREM. *For all $k \geq 1$ there exists a tournament $T = (V, A)$ such that, for every subset X of k vertices, there exists a vertex $y \in V \setminus X$ such that y beats all $x \in X$.*

Proof: Observe that we may as well prove this for large values of k only, since the result for smaller values follows from it.

For fixed k, set $n = |V| = k + k^2 2^k$. Pick a tournament on n vertices uniformly at random, i.e. for each unordered pair $\{x, y\}$ of vertices, pick one of $x \to y$ and $y \to x$, each with probability $1/2$.

Fix a subset X of size k, and a vertex y outside X. Clearly,

$$\Pr(\text{for all } x \in X, y \to x) = \frac{1}{2^k},$$

so, conversely,

$$\Pr(\text{there exists } x \in X, x \to y) = 1 - \frac{1}{2^k}.$$

For distinct vertices y and y', the events "y beats all members of X" and "y' beats all members of X" are independent (since the edges are disjoint). So it follows that

$$\Pr(\text{for all } y \in V \setminus X \text{ there exists } x \in X : x \to y) = \left(1 - \frac{1}{2^k}\right)^{n-k} = \left(1 - \frac{1}{2^k}\right)^{2^k k^2} \leq e^{-k^2}.$$

Now we apply the union bound to all sets X:

$$\begin{aligned}\Pr(\text{there exists } X \text{ such that no team beats all members of } X) &\leq \binom{n}{k} e^{-k^2} \\ &= \binom{k + 2^k k^2}{k} e^{-k^2} \leq (k^2 2^k)^k e^{-k^2} = \left(\frac{k^2 2^k}{e^k}\right)^k,\end{aligned}$$

which is strictly less than 1 for sufficiently large k. Hence a tournament as desired does exist. ∎

Note that such a tournament needs to be big: if $n = k$ then the tournament clearly has a winning set. How big? It has been shown that one must have $n > ck2^k$ for some constant c.

6.3 Markov's inequality

It is often useful to work with data *derived* from events. To that end, we introduce

6.3.1 DEFINITION. A *random variable* is a function $X : \Omega \to \mathbb{R}$. We write

$$\Pr(X = x) := \sum_{\omega \in \Omega : X(\omega) = x} \Pr(\omega).$$

In this definition, we can consider "$X = x$" to be an event in the derived probability space $\{X(\omega) : \omega \in \Omega\}$.

As an example, consider the random variable "total number of heads". Another example is the random variable that is 1 if the first flip comes up heads, and 0 if it comes up tails.

6.3.2 DEFINITION. The *expectation* or *expected value* of a random variable X is

$$\mathbb{E}[X] := \sum_{\omega \in \Omega} X(\omega) \Pr(\omega) = \sum_x x \Pr(X = x),$$

where the latter sum is defined since $\mathrm{im}(X)$ has only a finite set of elements.

One last definition:

6.3.3 DEFINITION. Random variables X and Y are *independent* if, for all $x, y \in \mathbb{R}$,

$$\Pr(X = x \text{ and } Y = y) = \Pr(X = x)\Pr(Y = y).$$

An important tool is the following:

6.3.4 THEOREM (Linearity of expectation). *Let $X_1, \ldots, X_k$ be random variables. Then*

$$\mathbb{E}[X_1 + \cdots + X_k] = \sum_{i=1}^{k} \mathbb{E}[X_i].$$

Proof: Easy exercise. ∎

Note that in the result above, as well as in the union bound, *no assumptions* were made regarding independence. The following result, by contrast, *only* holds for independent random variables:

6.3.5 THEOREM. *Let X and Y be independent random variables. Then*

$$\mathbb{E}[XY] = \mathbb{E}[X]\,\mathbb{E}[Y]. \tag{6.1}$$

Proof: Another easy exercise. It is illustrative to do the exercise, and figure out why independence is important here but not in the previous proofs. ∎

Finally, we state an important inequality:

6.3.6 THEOREM (Markov's Inequality). *Let X be a nonnegative random variable, and $t \geq 0$. Then*

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

Proof:

$$\mathbb{E}[X] = \sum_{a \geq 0} a \Pr(X = a) \geq \sum_{a \geq t} a \Pr(X = a) \geq \sum_{a \geq t} t \Pr(X = a) = t \Pr(X \geq t).$$ ∎

6.4 Applications

Sum-free sets. Our first application concerns sum-free sets.

6.4.1 DEFINITION. A set $B \subseteq \mathbb{Z}$ is *sum-free* if $x + y \notin B$ for all $x, y \in B$.

6.4.2 PROBLEM. Let A be a finite set of integers. How large a sum-free set does A contain?

For example, if $A = [2n]$ then we can pick $B = \{n+1, n+2, \ldots, 2n\}$, or $\{1, 3, 5, \ldots, 2n-1\}$. In both cases $|B| = \frac{1}{2}|A|$. As it turns out, we cannot always find a sum-free subset

that contains half the elements of A, but the following theorem shows we can achieve a third:

6.4.3 THEOREM. *For every set A of nonzero integers, there exists a sum-free subset $B \subseteq A$ with $|B| \geq \frac{1}{3}|A|$.*

Proof: Pick a prime p such that $p > |a|$ for all $a \in A$. In $\mathbb{Z}_p$, define the set

$$S := \{\lceil p/3 \rceil, \ldots, \lfloor 2p/3 \rfloor\}.$$

Note that $|S| \geq \frac{1}{3}(p-1)$, and that S is a sum-free subset in the ring $\mathbb{Z}_p$.

We pick an $x \in \mathbb{Z}_p \setminus \{0\}$ uniformly at random. For this x, define

$$A_x := \{a \in A : ax \pmod p \in S\}.$$

If $a, b \in A_x$ then, since $ax \pmod p + bx \pmod p = (a+b)x \pmod p$ and S is sum-free, we cannot have $a + b \in A_x$. Hence A_x is sum-free. Consider the random variable $X := |A_x|$. We define

$$\chi_x(a) := \begin{cases} 1 & \text{if } a \in A_x \\ 0 & \text{if } a \notin A_x. \end{cases}$$

With this we can compute the expected value

$$\mathbb{E}[X] = \mathbb{E}[|A_x|] = \mathbb{E}\left[\sum_{a \in A} \chi_x(a)\right] = \sum_{a \in A} \mathbb{E}[\chi_x(a)] = \sum_{a \in A} \Pr(ax \pmod p \in S) \geq \frac{1}{3}|A|,$$

where we use that $\Pr(ax \pmod p \in S) = |S|/(p-1) \geq 1/3$. It follows that there must exist a value of x for which $|A_x| \geq \frac{1}{3}|A|$. ∎

It is unknown what the best possible fraction c is such that every set A of nonzero integers has a sum-free subset B with $|B| \geq c|A|$. The following set can be checked to have no sum-free sets of size more than four, giving an upper bound of $\frac{4}{10}$ on c:

$$\{1, 2, 3, 4, 5, 6, 8, 9, 10, 18\}.$$

A bigger example is known which gives $c \leq \frac{11}{28}$.

Another less classical example from additive combinatorics is the following result from a past International Mathematics Olympiad Shortlist.

6.4.4 THEOREM. *For every subset $A \subset \mathbb{Z}/n^2\mathbb{Z}$ with n elements, there exists a subset $B \subset \mathbb{Z}/n^2\mathbb{Z}$ with n elements such that $|A+B| \geq \frac{n^2}{2}$.*

Proof: Pick a random collection of n elements of $\mathbb{Z}/n^2\mathbb{Z}$, each of the n elements being taken with probability $1/n^2$ and all choices being independent. Put the distinct elements among the n chosen ones in a set B, which may have less than n elements. Consider the random variable $X = |A+B|$. As

$$X = \sum_{i \in \mathbb{Z}/n^2\mathbb{Z}} 1_{i \in A+B},$$

we have by linearity of expectation

$$\mathbb{E}[X] = \sum_{i \in \mathbb{Z}/n^2\mathbb{Z}} \Pr(i \in A+B).$$

On the other hand, the probability that $i \notin A+B$ is clearly the $n-$th power of the probability that a given integer is not in A, that is

$$\Pr(i \in A+B) = 1 - \left(1 - \frac{|A|}{n^2}\right)^n = 1 - \left(1 - \frac{1}{n}\right)^n.$$

We deduce that

$$\mathbb{E}[X] = n^2 \left(1 - \left(1 - \frac{1}{n}\right)^n\right)$$

and the result follows from the inequality $(1 - \frac{1}{n})^n < \frac{1}{2}$. ∎

Graphs with high girth and high chromatic number.

6.4.5 DEFINITION. A k-coloring of a graph $G = (V, E)$ is a map $c : V \to [k]$ such that $c(u) \neq c(v)$ for all $uv \in E$. The *chromatic number* $\chi(G)$ is the least k for which there exists a k-coloring.

6.4.6 DEFINITION. The *girth* of a graph is the length of the shortest cycle.

Note that trees have infinite girth, and chromatic number 2. Since graphs with high girth look like trees locally, one might wonder if $\chi(G)$ is small for such graphs. But this is not so:

6.4.7 THEOREM. *For all positive integers k, l there exists a graph G with $\chi(G) \geq k$ and girth at least l.*

Proof: A *random graph* $G_{n,p}$ is a graph on n vertices in which each edge appears independently with probability p. Fix a value n (we will decide on a value later), pick some $\lambda \in (0, 1/l)$, and define $p := n^{\lambda-1}$. Let X be the random variable denoting the number of cycles of length at most l in $G_{n,p}$. Each cycle is determined by its (ordered) vertex set. A rough estimate is that there are fewer than n^j ordered vertex sets of size j, and each vertex set j forms a cycle with probability p^j. By linearity of expectation, therefore,

$$\mathbb{E}[X] \leq \sum_{j=3}^{l} n^j p^j = \sum_{j=3}^{l} n^{\lambda j} \leq \frac{n^{\lambda l}}{1 - n^{-\lambda}}.$$

Note that $\lambda l < 1$, so if we choose n sufficiently large then we will have $\mathbb{E}[X] < n/4$. Now Markov's Inequality gives

$$\Pr(X \geq \frac{n}{2}) < \frac{n/4}{n/2} = \frac{1}{2}.$$

Note that some small cycles may still exist! We will deal with those at the end of the proof.

Next, consider the chromatic number of $G_{n,p}$. In fact, we will look at the *stable set number* $\alpha(G)$, where $S \subseteq V$ is *stable* if no edge has both endpoints in S. Each color class is clearly a stable set, so we have

$$\chi(G) \geq \frac{|V(G)|}{\alpha(G)}.$$

Pick the number $a := \lceil \frac{3}{p} \ln n \rceil$, and consider the event that there is an independent set of size a. By the union bound, we find

$$\Pr(\alpha(G) \geq a) \leq \binom{n}{a}(1-p)^{\binom{a}{2}} \leq n^a e^{-pa(a-1)/2} \leq n^a n^{-3(a-1)/2},$$

where we used $(1 - 1/x) \leq e^{-x}$ and the definition of a. For n large enough this probability will be less than $1/2$. One more application of the union bound gives

$$\Pr(X \geq n/2 \text{ or } \alpha(G) \geq a) < 1,$$

so there exists a graph G with less than $n/2$ short cycles and $\alpha(G) < a$. We delete an arbitrary vertex from each of the short cycles. Note that this does not increase the stable set number. Let G' be the resulting graph. Then

$$\chi(G') \geq \frac{|V(G')|}{\alpha(G')} \geq \frac{n/2}{3n^{1-\lambda}\ln n} = \frac{n^\lambda}{6\ln n}.$$

Again, choosing n large enough will ensure $\chi(G') \geq k$. ∎

We end this section with the probabilistic proof of Theorem 4.6.5.

Second proof of Theorem 4.6.5: Define $X = \cup_i (A_i \cup B_i)$ and consider a random order π of X and let X_i be the event that in this order all the elements of A_i precede all those of B_i.

To compute the probability of X_i note that there are $(a_i + b_i)!$ possible orders of the elements in $A_i \cup B_i$ and the number of such orders in which all the elements of A_i precede all those of B_i is exactly $a_i!b_i!$. Therefore

$$\Pr(X_i) = \frac{a_i!b_i!}{(a_i+b_i)!} = \binom{a_i+b_i}{a_i}^{-1}.$$

We claim that events X_i are pairwise disjoint. Indeed, suppose that there is an order of X in which all the elements of A_i precede those of B_i and all the elements of A_j precede all those of B_j. WLOG, assume that the last element of A_i appears before the last element of A_j. Then, all the elements of A_i precede all those of B_j, contradicting the fact that $A_i \cap B_j \neq \emptyset$. Therefore, the events X_i are pairwise disjoint.

It follows that

$$1 \geq \sum_{i=1}^{m} \Pr(X_i) = \sum_{i=1}^{m} \binom{a_i+b_i}{a_i}^{-1}.$$

We end this section with a digression about a second very important inequality involving random variables.

6.4.8 THEOREM. *Let X be a random variable and let $t > 0$. Then*

$$\Pr(|X - \mathbb{E}[X]| \geq t) \leq \frac{\mathbb{E}[X^2] - \mathbb{E}[X]^2}{t^2}.$$

Proof: We use Markov's Inequality. Namely, we write that

$$\Pr(|X - \mathbb{E}[X]| \geq t) = \Pr(|X - \mathbb{E}[X]|^2 \geq t^2) \leq \frac{\mathbb{E}[X^2] - \mathbb{E}[X]^2}{t^2},$$

and an easy computation using lineary of expectation yields the result. ∎

In fact, the quantity $\mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$ turns out to be the second most vital statistic for a random variable after its expectation. It is called the *variance* of random variable X and it has a lot of applications. We include one from the topic of random graphs.

6.4.9 THEOREM. *Let G_n be a random graph on n vertices where each of the $\binom{n}{2}$ possible edges is included in the edge set with probability $1/2$, independently of the other edges. Then, with high probability, G_n contains a clique of size $0.5 \log_2 n$.*

Sketch of proof: We will solve the problem by lower bounding the probability for the existence of a clique of size $0.5 \log_2 n$ (i.e. finding a lower bound that goes to 1 as n goes to infinity). First, note that this probability is equal with $Pr(X > 0)$ where X is the random variable counting the number of $0.5 \log_2 n$ cliques. Clearly, we have that

$$E(X) = \binom{n}{0.5 \log_2 n} \left(\frac{1}{2}\right)^{\binom{0.5 \log_2 n}{2}}$$

We now show that $E(X^2)$ is $\binom{n}{0.5 \log_2 n}^2 \left(\frac{1}{2}\right)^{2\binom{0.5 \log_2 n}{2}} + \epsilon$ with

$$\epsilon << \binom{n}{0.5 \log_2 n}^2 \left(\frac{1}{2}\right)^{2\binom{0.5 \log_2 n}{2}},$$

so that $Var(X) = E(X^2) - (E(X))^2 = \epsilon$ is smaller than $\binom{n}{0.5 \log_2 n}^2 \left(\frac{1}{2}\right)^{2\binom{0.5 \log_2 n}{2}}$. In this case, by Chebyshev's inequality, we get that X is concentrated about the mean (when n goes to infinity), so we are done, since the $E(X)$ clearly goes to infinity, when $n \to \infty$. (!)

Now, to compute $E(X^2)$. Let X_i be the indicator variable for the event that the i-th subset of size $k = 0.5 \log_2 n$ forms a clique. We have that $X = X_1 + \ldots + X_n$, so

$$\begin{aligned} E(X^2) &= \sum_{i,j} E(X_i X_j) = \sum_i \sum_{t=0}^{k} \sum_{j:|S_i \cap S_j| = t} E(X_i X_j) \\ &= \binom{n}{k} \sum_{t=0}^{k} f(t), \end{aligned}$$

where

$$f(t) = \sum_{j:|S_i \cap S_j| = t} E(X_i X_j) = \binom{k}{t} \binom{n-k}{k-t} 2^{-k(k-1)+t(t-1)/2}$$

and by S_i we denote the i-th subset of vertices (in our arbitrary indexation).

But

$$\binom{n}{k} \cdot \sum_{t=0}^{k} \binom{k}{t}\binom{n-k}{k-t} 2^{-k(k-1)+t(t-1)/2} = \binom{n}{k} 2^{-k(k-1)} \cdot \sum_{t=0}^{k} \binom{k}{t}\binom{n-k}{k-t} 2^{t(t-1)/2}$$

which is $\binom{n}{k}^2 2^{-k(k-1)} + \epsilon = \binom{n}{k}^2 \left(\frac{1}{2}\right)^{2\binom{k}{2}} + \epsilon$ for some $\epsilon << \binom{n}{k}^2 \left(\frac{1}{2}\right)^{2\binom{k}{2}}$, as one can easily check. This proves the result, since we saw that this is enough (in (!)). ∎

We leave it as an exercise to prove that, with high probability, G_n does not contain a clique of size $3\log_2 n$.

6.5 The Lovász Local Lemma

Suppose we have a probability space with a number of "bad" events. The probabilistic method instructs us to show that, with positive probability, none of the bad events happen. Our basic tool, the union bound, gives

$$\Pr(A \cup B) \leq \Pr(A) + \Pr(B),$$

so as long as each of the probabilities on the right-hand side is small enough, there is a positive probability that none of them happen. If A and B are independent events then, writing $\overline{A}$ for the *complement* of A, we can conclude:

$$\Pr(\overline{A} \cap \overline{B}) = \Pr(\overline{A}) \Pr(\overline{B}),$$

so we only need to show that each of the probabilities on the right-hand side is positive. Of course, this is a useless observation if these events are not independent. But it turns out that we can still say something if the dependencies between events are limited.

6.5.1 DEFINITION. An event A is *mutually independent* of $B_1, \ldots, B_k$ if, for all $I \subseteq [k]$, event A is independent of $\bigcap_{i \in I} B_i$.

Take our example of coin flips. Let A be the event "the first flip and last flip are the same", let B_1 be the event "the first flip comes up heads", and let B_2 be the event "the last flip comes up heads". Then $\Pr(A \mid B_1) = \Pr(A \mid B_2) = \Pr(A) = 1/2$, but $\Pr(A \mid B_1 \cap B_2) = 1$. Hence A is *not* mutually independent of B_1 and B_2.

6.5.2 LEMMA (Lovász Local Lemma). *Let $A_1, \ldots, A_n$ be events, such that each A_i is mutually independent of all but at most d of the remaining A_j. Suppose $\Pr(A_i) \leq p$ for all i. if $4pd \leq 1$ then*

$$\Pr\left(\bigcap_{i=1}^{n} \overline{A_i}\right) > 0.$$

Proof: Our main ingredient is the following

6.5.2.1 CLAIM. *For all integers m, and for all subsets of m events (say $A_1,\dots,A_m$, after relabeling), we have*

$$\Pr(A_1 \mid \overline{A_2} \cap \cdots \cap \overline{A_m}) \le 2p.$$

Proof: We prove the claim by induction on m, the case $m = 1$ being trivial. Suppose the events $A_2,\dots,A_m$ were sorted so that A_1 is mutually independent of $A_{k+1},\dots,A_m$ for some k. Note that we can always find an ordering and a k so that $k-1 \le d$. By Lemma 6.1.9,

$$\Pr\left(A_1 \mid \overline{A_2} \cap \cdots \cap \overline{A_m}\right) = \frac{\Pr\left(A_1 \cap \overline{A_2} \cap \cdots \cap \overline{A_k} \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right)}{\Pr\left(\overline{A_2} \cap \cdots \cap \overline{A_k} \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right)}.$$

The numerator can be bounded as follows:

$$\Pr\left(A_1 \cap \overline{A_2} \cap \cdots \cap \overline{A_k} \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right) \le \Pr\left(A_1 \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right) = \Pr(A_1) \le p.$$

For the denominator, we use the union bound and the induction hypothesis:

$$\begin{aligned}\Pr\left(\overline{A_2} \cap \cdots \cap \overline{A_k} \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right) &= 1 - \Pr\left(A_2 \cup \cdots \cup A_k \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right) \\ &\ge 1 - \sum_{i=2}^{k} \Pr\left(A_i \mid \overline{A_{k+1}} \cap \cdots \cap \overline{A_m}\right) \\ &\ge 1 - (k-1)2p \ge 1 - 2pd \ge 1/2.\end{aligned}$$

Hence

$$\Pr\left(A_1 \mid \overline{A_2} \cap \cdots \cap \overline{A_m}\right) \le \frac{p}{1/2} = 2p. \qquad \square$$

By Lemma 6.1.10,

$$\Pr\left(\overline{A_1} \cap \cdots \cap \overline{A_n}\right) = \prod_{i=1}^{n} \Pr\left(\overline{A_i} \mid \overline{A_1} \cap \cdots \cap \overline{A_{i-1}}\right) \ge (1-2p)^n > 0. \qquad \blacksquare$$

Note that, with some extra work, we can weaken the conditions in the lemma to $ep(d+1) \le 1$, where e is the base of the natural logarithm. There are further strengthenings of the result that weaken the condition $\Pr(A_i) \le p$, and that do not require symmetry: some events are allowed to have more dependencies than others.

Another important observation is that the lemma does not restrict the *number* of events, as long as their interactions are limited. This in particular makes it much more powerful than the union bound.

6.6 Applications

Two-colorability of set systems. We return to the subject of our first application (Theorem 6.2.2), namely to find conditions guaranteeing that a set system is 2-colorable. The next result shows that a system will be 2-colorable if we restrict the intersections of the sets:

6.6.1 THEOREM. *Let $H = ([n], \mathscr{F})$ be a set system such that $|X| = r$ for all $X \in \mathscr{F}$. If each $X \in \mathscr{F}$ intersects at most 2^{r-3} other members of $\mathscr{F}$, then H is 2-colorable.*

Proof: Let $\mathscr{F} = \{X_1, \ldots, X_k\}$. Randomly color the elements $[n]$ red and blue. Let A_i be the event that X_i is monochromatic. Then $\Pr(A_i) = 1/2^{r-1}$ as before. Pick $p := 1/2^{r-1}$.

The event A_i is mutually independent of all A_j such that $X_i \cap X_j = \emptyset$. Note that X_i has nonempty intersection with at most 2^{r-3} of the remaining X_j. Pick $d := 2^{r-3}$. Now

$$4dp = 4 \cdot 2^{r-3} \cdot 2^{1-r} = 1,$$

so by the Lovász Local Lemma

$$\Pr(\text{no edge monochromatic}) = \Pr(\overline{A_1} \cap \cdots \cap \overline{A_k}) > 0. \qquad \blacksquare$$

Directed cycles (mod k). It is easy to construct a directed graph that avoids an odd cycle: make sure the underlying graph is bipartite. But can we avoid an even cycle? Or, more generally, a cycle whose length is a multiple of k for some k? The next result gives a condition under which such a cycle cannot be avoided:

6.6.2 THEOREM. *Let $D = (V, A)$ be a digraph with minimum outdegree δ and maximum indegree Δ. If $4\Delta\delta(1 - 1/k)^{\delta} \leq 1$ then D contains a directed cycle of length $0 \pmod{k}$.*

Proof: Let D be such a digraph. First note that the conditions do not change if we remove arc coming out of a vertex of outdegree more than δ. Hence we may assume each vertex has outdegree exactly δ. Let $f : V \to \{0, 1, \ldots, k-1\}$ be a random coloring of V. Let A_v be the event that there is no $u \in V$ with $(v, u) \in A$ and $f(u) \equiv f(v) + 1 \pmod{k}$. Clearly

$$\Pr(A_v) = \left(1 - \frac{1}{k}\right)^{\delta}.$$

Define $N^+(v) := \{w \in V : (v, w) \in A\}$. Note that A_v is independent of all events that do not involve $N^+(v)$; specifically, A_v is mutually independent of all A_u except those with

$$N^+(v) \cap (\{u\} \cup N^+(u)) \neq \emptyset.$$

Each vertex in $N^+(v)$ has at most $\Delta - 1$ arcs pointing to it from vertices other than v, so v is mutually independent from all but at most $\delta(1 + (\Delta - 1)) = \delta\Delta$ vertices u. By the Lovász Local Lemma, with $p = \left(1 - \frac{1}{k}\right)^{\delta}$ and $d = \delta\Delta$, we find that

$$\Pr\left(\bigcap_{v \in V} \overline{A_v}\right) > 0,$$

so there is a coloring such that, for all $v \in V$ there exists $u \in V$ with $f(u) \equiv f(v) + 1 \pmod{k}$.

Now start at any vertex v_1, and find a sequence $v_1, v_2, v_3, \ldots$ of vertices so that $(v_i, v_{i+1}) \in A$ and $f(v_{i+1}) \equiv f_(v_i) + 1 \pmod{k}$ for all i. Since V is a finite set, some

vertex must repeat. Pick j and l such that $l < j$, $v_l = v_j$, and $j - l$ minimal. Then $v_l v_{l+1} \cdots v_j$ is a cycle, and

$$f(v_j) \equiv f(v_l) + (j - l - 1) \pmod{k}.$$

Since $f(v_j) = f(v_l)$, it follows that $j - l - 1 \equiv 0 \pmod{k}$. But $j - l - 1$ is precisely the length of the cycle! ∎

6.7 Where to go from here?

We list two books:

- Alon and Spencer (2008), *The Probabilistic Method* is a beautiful, readable, and comprehensive book on the subject. After each chapter an intermezzo titled "The probabilistic lens" gives a particularly striking application of the theory just discussed.
- Jukna (2011), *Extremal Combinatorics* devotes several chapters to the probabilistic method.

CHAPTER 7

Spectral Graph Theory

> The founders of Google computed the Perron-Frobenius eigenvector of the web graph and became billionaires.
>
> Brouwer and Haemers (2012)

ALGEBRAIC graph theory is a field of combinatorics in which tools from algebra are used to study graph properties. The rank polynomial (to be discussed in Chapter 11) may be counted as such an algebraic tool. In this chapter we will focus on a specific tool: the set of *eigenvalues* associated with a graph (also called the *spectrum*).

7.1 Eigenvalues of graphs

7.1.1 Eigenvalues of symmetric matrices

We start with a quick refresher on eigenvalues. The proofs of the standard results are omitted.

7.1.1 DEFINITION. Let A be an $n \times n$ matrix (over $\mathbb{C}$, say). If $\lambda \in \mathbb{C}$ and $v \in \mathbb{C}^n$, $v \neq 0$, are such that $Av = \lambda v$ then λ is an *eigenvalue* of A and v is the corresponding *eigenvector*.

The *spectrum* of A is the list of eigenvalues, together with their multiplicities (i.e. the dimension of the space of eigenvectors associated with that eigenvalue).

7.1.2 LEMMA. *Let A be an $n \times n$ matrix, and r a positive integer. The eigenvalues of A^r are precisely the rth powers of the eigenvalues of A.*

7.1.3 DEFINITION. The *characteristic polynomial* of A is

$$\varphi(A, x) := \det(xI - A).$$

7.1.4 LEMMA. *The eigenvalues of A are the roots of $\varphi(A, x)$.*

7.1.5 DEFINITION. The *trace* of an $n \times n$ matrix A is

$$\operatorname{tr}(A) := \sum_{i=1}^{n} A_{ii}.$$

7.1.6 LEMMA. *If A is an $n \times n$ matrix, then $\operatorname{tr}(A)$ equals the sum of the eigenvalues of A.*

We continue with a few facts that are particular to symmetric, real matrices. For completeness we give the proofs of these.

7.1.7 LEMMA. *Let A be an $n \times n$ symmetric matrix over $\mathbb{R}$. Let u, v be eigenvectors of A with distinct eigenvalues. Then u is orthogonal to v.*

Proof: Suppose $Au = \lambda u$ and $Av = \tau v$ with $\lambda \neq \tau$. Then

$$u^T \tau v = u^T(Av) = u^T Av = u^T A^T v = (u^T A^T)v = (Au)^T v = u^T \lambda v.$$

Since $\lambda \neq \tau$, it follows that $u^T v = \langle u, v \rangle = 0$. ∎

7.1.8 LEMMA. *Let A be an $n \times n$ symmetric matrix over $\mathbb{R}$. Then all eigenvalues of A are real.*

Proof: Suppose $Au = \lambda u$. Taking complex conjugates we find $A\overline{u} = \overline{\lambda}\overline{u}$. So

$$\overline{\lambda}\overline{u}^T u = \overline{u}^T Au = \lambda \overline{u}^T u.$$

Since $u \neq 0$ by definition, we have $\overline{u}^T u = \|u\|^2 > 0$, and therefore $\overline{\lambda} = \lambda$. ∎

The following result, a strengthening of Lemma 7.1.7, will prove very useful:

7.1.9 THEOREM. *Let A be an $n \times n$ symmetric matrix over $\mathbb{R}$. Then $\mathbb{R}^n$ has an orthonormal basis of eigenvectors.*

Proof: We start with the following:

7.1.9.1 CLAIM. *Let U be a subspace of $\mathbb{R}^n$ such that $AU \subseteq U$. Then $AU^\perp \subseteq U^\perp$.*

Proof: Consider $u \in U$ and $v \in U^\perp$, so $\langle u, v \rangle = 0$. Then $v^T Au = v^T u'$ for some $u' \in U$. By definition of $U^\perp$ we have $v^T u' = 0$, so $(Av)^T u = 0$ for all $u \in U$, so $Av \in U^\perp$. □

7.1.9.2 CLAIM. *A has at least one real eigenvector.*

Proof: Note that $\varphi(A, x)$ has at least one root (over $\mathbb{C}$), say θ. This root is real by Lemma 7.1.8. Now $\varphi(A, \theta) = \det(\theta I - A) = 0$, so $\ker(\theta I - A) \neq \emptyset$ (over $\mathbb{R}$). Any vector in that kernel is an eigenvector with eigenvalue θ. □

In fact, we can find such an eigenvector in a more restricted space:

7.1.9.3 CLAIM. *Let U be a subspace of $\mathbb{R}^n$ such that $AU \subseteq U$. Then U contains a real eigenvector of A.*

Proof: Let $\{r_1, \ldots, r_k\}$ be an orthonormal basis of U, and let R be a matrix whose ith column is r_i. We now have that

$$AR = RB$$

for some square matrix B. Note that

$$R^T AR = R^T RB = B,$$

from which we conclude that B is real and symmetric (since $R^T AR$ is). By the previous claim, B has a real eigenvector v, say with eigenvalue λ. Now

$$ARv = RBv = \lambda Rv,$$

so Rv is an eigenvector of A with eigenvalue λ. □

Now the result follows easily by induction. ■

Finally, a useful interpretation of the largest eigenvalue:

7.1.10 LEMMA. *Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of a symmetric, real, $n \times n$ matrix A. Then $\lambda_1 = \max\{\langle v, Av\rangle : v \in \mathbb{R}^n, \|v\| = 1\}$.*

Proof: Exercise. ■

7.1.2 Eigenvectors of graphs

7.1.11 DEFINITION. Let G be a graph. The *eigenvalues*, *eigenvectors*, and *spectrum* of G are those of the *adjacency matrix* $A(G)$, given by

$$(A(G))_{i,j} = \begin{cases} 1 & \text{if } ij \in E(G) \\ 0 & \text{otherwise.} \end{cases}$$

A key property, that we will use time and again, is the following:

7.1.12 LEMMA. *Let $A = A(G)$ for a graph G. Then $(A^r)_{uv}$ is the number of walks from u to v of length r.*

7.1.13 COROLLARY. *We have the following:*

- $\mathrm{tr}(A(G)) = 0$
- $\mathrm{tr}(A(G)^2) = 2|E(G)|$
- $\mathrm{tr}(A(G)^3) = 6t$, *where t is the number of triangles of G.*

Note that those values are determined by the spectrum of G. However, the spectrum does not determine the graph uniquely: one can check that both graphs in Figure 7.1 have spectrum $\{-2, -1^{(2)}, 1^{(2)}, 1 - \sqrt{7}, 1 + \sqrt{7}\}$. Here the superscript $^{(2)}$ denotes the multiplicity of the eigenvalue.

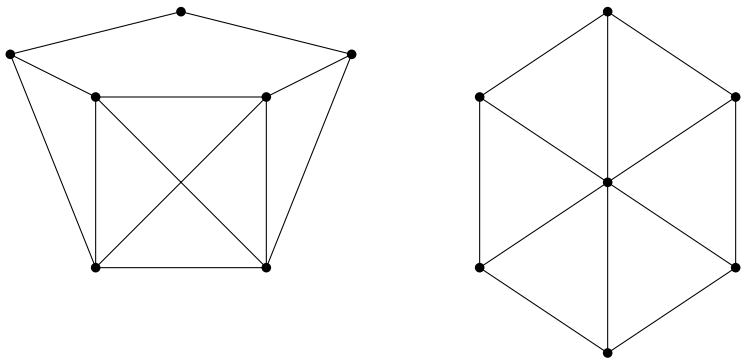


FIGURE 7.1
Two cospectral graphs

7.1.3 Finding eigenvalues

It is often better to look for eigenvectors first, rather than trying to find roots of the characteristic polynomial. If A is the adjacency matrix of G, then we can interpret an eigenvector v as a function $v : V(G) \to \mathbb{R}$. If λ is the eigenvalue of v then we have, for all vertices $u \in V(G)$,

$$\sum_{uw \in E(G)} v(w) = \lambda v(u).$$

One particular eigenvector is often useful:

7.1.14 LEMMA. *The all-ones vector* $\mathbf{1}$ *is an eigenvalue of* G *if and only if* G *is* k*-regular for some* k*.*

Proof: This follows directly from

$$A\mathbf{1} = \begin{bmatrix} \deg(v_1) \\ \deg(v_2) \\ \vdots \\ \deg(v_n) \end{bmatrix}. \qquad \blacksquare$$

7.2 The Hoffman-Singleton Theorem

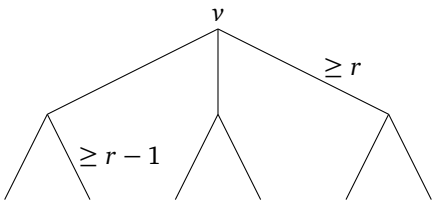
We look at graphs with specified girth and minimum degree.

7.2.1 LEMMA. *Let* $g = 2k+1$ *be an odd integer, and* r *a positive integer. If* G *is a graph with girth* g *and minimum degree* r*, then* G *has at least*

$$1 + r + r(r-1) + r(r-1)^2 + \cdots + r(r-1)^{k-1}$$

vertices.

Sketch of proof: Start drawing the graph from an arbitrary single vertex v, in a tree-like fashion: all neighbors of v are one level below v, all *their* neighbors are below that, and so on for k levels. Since the graph has no cycles of length at most $2k$, these vertices are necessarily distinct.



■

We ask ourselves whether this bound is ever attained. Such graphs are called *Moore graphs*. The following result almost settles the question for girth five:

7.2.2 THEOREM. *Moore graphs with $g = 5$ exist for $r = 2, 3, 7$, and maybe 57.*

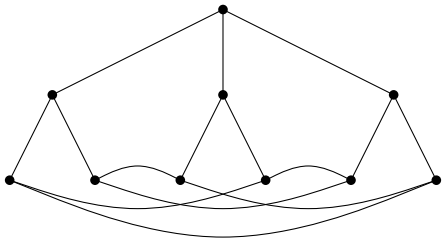


FIGURE 7.2
The Petersen graph, drawn as a Moore graph. Note that Moore graphs must look like this for every *choice of top vertex!*

Proof: The case $r = 2$ is the five-cycle, so assume $r \geq 3$. Let G be an r-regular Moore graph, and let $A := A(G)$. Note that the number of vertices is $n = 1+r+r(r-1) = r^2+1$.

Consider $B := A^2$. Then B_{ij} equals the number of neighbors common to vertices i and j. Note that, since G has but $1 + r + r(r-1)$ vertices, no pair of vertices can have distance more than 2 (by adapting the argument from the previous lemma). From this we conclude

$$B_{ij} = \begin{cases} r & \text{if } i = j \\ 0 & \text{if } i \neq j, ij \in E(G) \\ 1 & \text{if } i \neq j, ij \notin E(G). \end{cases}$$

So for $i \neq j$ we have $B_{ij} = 1 - A_{ij}$. Hence we can write

$$A^2 = rI + J - I - A,$$

where J is the $n \times n$ all-ones matrix. We will use this relation to help determining the eigenvalues of A. Since A is regular, the vector $\mathbf{1}$ is an eigenvector with eigenvalue r. We may assume that all remaining eigenvectors v are orthogonal to $\mathbf{1}$. It follows that

$Jv = 0$. Now

$$A^2 v = \lambda^2 v$$
$$(rI + J - I - A)v = (r - 1 - \lambda)v$$

so $\lambda^2 + \lambda - (r-1) = 0$. This gives two more eigenvalues:

$$\rho_1 = \frac{-1 - \sqrt{4r-3}}{2}, \qquad \rho_2 = \frac{-1 + \sqrt{4r-3}}{2}$$

with multiplicities m_1, m_2. Using that the sum of the multiplicities is n, and the sum of the eigenvalues is $\mathrm{tr}(A) = 0$, we find

$$m_1 + m_2 = n - 1 = r^2$$
$$\rho_1 m_1 + \rho_2 m_2 + r = 0.$$

We substitute our expressions for ρ_1, ρ_2 in the second equation, and use the first to simplify it. This gives us

$$(m_2 - m_1)\sqrt{4r-3} = r^2 - 2r. \tag{7.1}$$

Note that m_1, m_2, and r are integers. If $\sqrt{4r-3}$ is not integral, then we had better have $m_1 = m_2$, and therefore $r^2 = 2r$. This has no solutions for $r \geq 3$. Hence we may assume $\sqrt{4r-3}$ is integral, i.e. $4r - 3 = s^2$ for some integer s. It follows that $r = (s^2+3)/4$. Substituting this into (7.1) and rearranging, we obtain

$$s^4 - 2s^2 - 16(m_1 - m_2)s = 15.$$

Hence s must be a divisor of 15, so $s \in \{1, 3, 5, 15\}$. But then $r \in \{1, 3, 7, 57\}$. We assumed $r \geq 3$ so, adding the case $r = 2$, the result follows. ∎

Note that the case $r = 2$ is the 5-cycle, the case $r = 3$ is the Petersen graph, and the case $r = 7$ is a graph known as the *Hoffman-Singleton graph*. It is an open problem whether a Moore graph with $r = 57$ exists.

7.3 The Friendship Theorem and Strongly Regular graphs

The following result is proven using similar ideas to the proof of the Hoffman-Singleton Theorem.

7.3.1 THEOREM (Friendship Theorem). *If $G = (V, E)$ is such that every pair of vertices has exactly one common neighbor, then G contains a vertex adjacent to all others.*

In other words: in a group of people, if any two share exactly one common friend, then there must be a "politician" who is friends with all.

Proof: Suppose the result if false, and let $G = (V, E)$ be a friendship graph without politician.

7.3.1.1 CLAIM. *G is regular.*

Proof: Pick nonadjacent vertices u and v, such that $\deg(v) \leq \deg(u)$. Let $w_1, \ldots, w_k$ be the neighbors of u, and let w_1 be the neighbor shared with v. Each of the w_i, $i > 1$, has a common neighbor with v, say z_i. No two of the z_i can be the same, because if $z_i = z_j$ then w_i and w_j are common neighbors of both u and z_i, contradicting the assumption of the theorem. Hence $\deg(v) \geq \deg(u)$, and therefore the degrees are equal.

Now if $w \notin \{u, v, w_1\}$, then w is adjacent to at most one of u and v, and by the previous argument $\deg(w) = \deg(u) = \deg(v)$. Finally, by our assumption there is some vertex w such that w_1 is not adjacent to w. It follows that also $\deg(w_1) = \deg(w)$. □

Consider the adjacency matrix $A := A(G)$. This time,

$$A^2 = J + (k-1)I.$$

A again has eigenvalue k (with eigenvector $\mathbf{1}$). Consider an eigenvector v orthogonal to $\mathbf{1}$, having eigenvalue λ. Then

$$A^2 v = \lambda^2 v$$
$$(J + (k-1)I)v = (k-1)v,$$

so $\lambda = \pm\sqrt{k-1}$. Let the multiplicities of these eigenvalues be m_+, m_-. Since $\mathrm{tr}(A) = 0$ is the sum of the eigenvalues, we have

$$k + (m_+ - m_-)\sqrt{k-1} = 0.$$

Bringing k to the other side and squaring, we find

$$k^2 = (m_- - m_+)^2(k-1),$$

so we conclude that $k-1$ divides k^2. Since $k-1$ also divides $k^2 - 1 = (k-1)(k+1)$, we must have $k-1 \in \{0,1\}$, or $k \in \{1,2\}$. If $k = 1$ then G is a single edge, and if $k = 2$ then G is a triangle. Both of these have a vertex adjacent to all others. ■

The key properties of the counterexample studied in the proof can be generalized as follows:

7.3.2 DEFINITION. A graph $G = (V, E)$ is *strongly regular* with parameters (n, k, a, c) if G has n vertices, G is k-regular, every pair of adjacent vertices has a common neighbors, and every pair of nonadjacent vertices has c common neighbors.

It follows that the Moore graphs are $(r^2+1, r, 0, 1)$-strongly regular, and the graph in the proof above is $(k^2-k+1, k, 1, 1)$-strongly regular. A difficult problem is to determine the parameter sets for which strongly regular graphs exist (as is evidenced by the open problem whether a $(3250, 57, 0, 1)$-strongly regular graph exists). The parameters are not independent. We state a few easily checked facts:

7.3.3 LEMMA. *Let G be an (n, k, a, c)-strongly regular graph with $n > k+1$. The following are equivalent:*

- *G is not connected;*
- $c = 0$*;*
- $a = k - 1$*;*
- *G is isomorphic to* mK_{k+1} *for some* $m > 1$.

As an example, the graph $5K_3$ consists of five disjoint triangles.

7.3.4 LEMMA. *Let G be an* (n,k,a,c)*-strongly regular graph. Then* $k(k-a-1) = (n-k-1)c$.

Sketch of proof: Count the number of edges between a neighbor and a non-neighbor of a vertex v in two ways. ∎

7.4 Bounding the stable set number

Things get interesting when the eigenvalues appear in the *statement* of the theorem. Recall that $\alpha(G)$ is the *stable set number*: the size of a largest subset of vertices such that no edge has both ends in this set.

7.4.1 THEOREM. *Let* $G = (V,E)$ *be a k-regular graph on n vertices, with eigenvalues* $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$*. Then*

$$\alpha(G) \leq \frac{n}{1 - \lambda_1/\lambda_n}.$$

Proof: Consider an independent set S, define $\alpha := |S|$, and define a vector x_S by

$$(x_S)_v = \begin{cases} 1 & \text{if } v \in S \\ 0 & \text{otherwise.} \end{cases}$$

Consider an orthonormal basis of eigenvectors $B = \{v_1, \ldots, v_n\}$, where $v_1 = \frac{1}{\sqrt{n}}\mathbf{1}$. Now we can find constants $a_1, \ldots, a_n$ so that

$$x_S = \sum_{i=1}^{n} a_i v_i.$$

Since B is orthonormal,

$$\langle x_S, v_1 \rangle = \frac{\alpha}{\sqrt{n}} = a_1.$$

For the same reason,

$$\langle x_S, x_S \rangle = \alpha = \sum_{i=1}^{n} a_i^2.$$

Furthermore

$$\langle x_S, Ax_S \rangle = x_S^T A x_S = \sum_{x,y \in S} A_{xy} = 0,$$

since no edge is contained in S. Combining these, we see

$$0 = \langle x_S, Ax_S \rangle = \sum_{i=1}^{n} \lambda_i a_i^2 \geq \lambda_1 a_1^2 + \lambda_n \sum_{i=2}^{n} a_i^2 = \lambda_1 \frac{\alpha^2}{n} + \lambda_n \left(\alpha - \frac{\alpha^2}{n} \right).$$

Hence

$$\begin{aligned} (\lambda_1 - \lambda_n)\frac{\alpha^2}{n} &\leq -\alpha\lambda_n \\ \alpha &\leq \frac{-n\lambda_n}{\lambda_1 - \lambda_n} = \frac{n}{1 - \lambda_1/\lambda_n}. \end{aligned}$$

■

We leave it as an exercise to prove that x_S is an eigenvector if equality holds.

7.4.2 EXAMPLE. The Petersen graph has eigenvalues

$$\left\{ 3, \frac{-1+\sqrt{9}}{2}, \frac{-1-\sqrt{9}}{2} \right\} = \{3, 1, -2\}.$$

Hence

$$\alpha(G) \leq \frac{10}{1 - 3/(-2)} = 4,$$

which is tight.

We end this section with a lower bound for the stable set number due to Caro and Wei.

7.4.3 THEOREM. *Let $d_1, \ldots, d_n$ be the degrees of the vertices of a graph. Prove that*

$$\alpha(G) \geq \frac{1}{d_1 + 1} + \ldots + \frac{1}{d_n + 1} \geq \frac{|V(G)|^2}{2|E(G)| + |V(G)|}$$

The proof uses the probabilistic method and is very surprising.

Proof: Consider a random permutation σ of the vertices of our graph, all permutations having equal probability $1/n!$. Let A_i be the event that $\sigma(i) < \sigma(j)$ for any neighbor j of i. We claim that

$$\Pr(A_i) = \frac{1}{d_i + 1}.$$

Indeed, we need to find the number of permutations σ of the vertices such that $\sigma(i) < \sigma(j)$ for any neighbor j of i. If $y_1, \ldots, y_{d_i}$ are the neighbors of i, there are $\binom{n}{d_i+1}$ possibilities for the set

$$\left\{ \sigma(i), \sigma(y_1), \ldots, \sigma(y_{d_i}) \right\},$$

$d_i!$ ways to permute the elements of this set, and $(n - d_i - 1)!$ ways to permute the remaining vertices. So

$$\Pr(A_i) = \binom{n}{d_i + 1} \cdot \frac{(n - d_i - 1)! d_i!}{n!} = \frac{1}{d_i + 1},$$

as claimed. Let X now be the random variable

$$X(\sigma) = \sum_{i=1}^{n} 1_{\sigma \in A_i}.$$

By linearity of expectation, we have that

$$\mathbb{E}[X] = \sum_{i=1}^{n} \Pr(A_i) = \sum_{i=1}^{n} \frac{1}{d_i + 1}.$$

Hence one can find σ such that

$$X(\sigma) \geq \sum_{i=1}^{n} \frac{1}{d_i + 1}.$$

It is clear that the set of vertices i such that $\sigma \in A_i$ satisfies both properties. This proves the first inequality.

The second inequality is just a simple application of the Cauchy-Schwarz Inequality. ∎

One of the most popular uses of the Caro-Wei theorem is a really quick proof of Theorem 4.1.2. We leave this deduction as an exercise.

7.5 Expanders

Strongly regular graphs (with $c > 0$) have the property that each pair of vertices has distance at most 2. Moore graphs of girth $g = 2k + 1$ have distance at most k. Graphs in which the *diameter* (maximum distance between vertices) is small have many applications in computer science, in particular when the number of edges is not too large. However, as we have seen in the proof of the Hoffman-Singleton theorem, they may be hard to come by. In this section we will study families of graphs with similarly good properties: *expander graphs*. Qualitatively, expander graphs are

- Highly connected (i.e. one can find many different paths between pairs of vertices), and
- Sparse (i.e. the number of edges is small compared to the complete graph on the same vertex set).

For a subset S of the vertices of a graph G, define the *neighbor set* $N(S) := \{v \in V(G) \backslash S : uv \in E(G) \text{ for some } u \in S\}$.

7.5.1 DEFINITION. Let n, d be positive integers and $c > 0$ a real number. A graph $G = (V, E)$ is an (n, d, c)-*expander* if $n = |V|$, if G is d-regular, and if, for all $S \subseteq V$ with $|S| \leq n/2$ we have

$$|N(S)| \geq c|S|.$$

This definition states that, starting from a certain set, if we repeatedly add all neighbors of that set, then in each step we will add a fair number of new vertices – at least until we have reached half of all vertices. Without proof we state the following:

7.5.2 PROPOSITION. *An (n, d, c)-expander has diameter at most $2(k + 1)$, where*

$$k > \log_{1+c} \frac{n}{2(1 + d)}.$$

7.5.1 Spectral gap bound

Verifying whether a given graph is an expander is a difficult task when working from the definition: one must compute $|N(S)|/|S|$ for exponentially many subsets. Luckily eigenvalues come to the rescue!

7.5.3 THEOREM. *Let G be a d-regular graph on n vertices with eigenvalues $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Then G is an (n, d, c)-expander for*

$$c = \frac{\lambda_1 - \lambda_2}{2\lambda_1}.$$

As a first step in our proof we look at the edges sticking of a set S, rather than the neighbor set.

7.5.4 DEFINITION. If $S, T \subseteq V(G)$ are disjoint, then

$$e(S,T) := |\{uv \in E(G) : u \in S, v \in T\}|.$$

7.5.5 LEMMA. *Let G be a d-regular graph on n vertices with eigenvalues $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Let $S \subseteq V(G)$ and $T := V(G) \setminus S$. Then*

$$e(S,T) \geq \frac{(\lambda_1 - \lambda_2)|S||T|}{n}$$

Proof: Let $G = (V, E)$, S, and T be as stated, and define $s := |S|$ and $t := |T| = n - s$. We consider the matrix $D - A$, where $D = dI$ is the diagonal matrix with d on the diagonal, and $A = A(G)$ (cf. Theorem 5.6.2). Note that $D - A$ has the same eigenvectors as A, with eigenvalues $d - \lambda_i$ for $i \in [n]$. Let $\{v_1, \ldots, v_n\}$ be an orthogonal basis of eigenvectors with $v_1 = \mathbf{1}$. For all $x \in \mathbb{R}^n$, we have

$$\langle (D-A)x, x\rangle = \sum_{u \in V} \left(d x_u^2 - \sum_{v \in V : uv \in E} x_u x_v \right) = d \sum_{u \in V} x_u^2 - 2 \sum_{uv \in E} x_u x_v = \sum_{uv \in E} (x_u - x_v)^2.$$

Now pick x such that

$$x_u = \begin{cases} -t & \text{if } u \in S \\ s & \text{if } u \in T. \end{cases}$$

Note that $\langle x, \mathbf{1}\rangle = 0$, so x is a linear combination of the remaining eigenvectors $v_2, \ldots, v_n$. Since $d - \lambda_2$ is the second smallest eigenvalue of $D - A$, we find

$$\langle (D-A)x, x\rangle \geq (d - \lambda_2)\langle x, x\rangle = (d - \lambda_2)(st^2 + ts^2) = (d - \lambda_2)stn.$$

On the other hand,

$$\langle (D-A)x, x\rangle = \sum_{uv \in E} (x_u - x_v)^2 = e(S,T) \cdot (s+t)^2 = e(S,T) \cdot n^2,$$

so indeed

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

■

Proof of Theorem 7.5.3: Consider a subset $S \subseteq V(G)$ with $|S| = s \leq n/2$. By the theorem, there are at least

$$\frac{(\lambda_1 - \lambda_2)s(n-s)}{n} \geq \frac{(\lambda_1 - \lambda_2)s}{2}$$

edges from S to $V(G) \setminus S$. No vertex in $V(G) \setminus S$ is incident with more than d of these vertices (since G is d-regular), so

$$|N(S)| \geq \frac{(\lambda_1 - \lambda_2)s}{2d},$$

and the result follows. ∎

7.5.2 Random graphs are good expanders

Although we can now recognize expanders, we still don't know how to find them. In particular, we want to solve the following problem. Choose a value of d, and pick some constant c depending on d. Then find infinitely many values n for which there exists an (n, d, c)-expander. In fact, it is not clear that such infinite families exist! Luckily, random graphs come to the rescue. We follow most textbooks and prove the result only for a different notion of expander graph:

7.5.6 DEFINITION. A bipartite graph G with color classes L and R of size n each is a (d, β)-*expander* if the degrees in L are d and any set $S \subset L$ of at most n/d vertices has at least $\beta|S|$ neighbors (in R).

7.5.7 THEOREM. *Let $d \geq 4$, and let G be a random bipartite graph with color classes L and R of size n each, obtained by connecting each vertex in L to d vertices in R chosen uniformly at random. Then*

$$\Pr(G \text{ is a } (d, d/4)\text{-expander}) > 0.$$

Proof: For $S \subseteq L$ and $T \subseteq R$, let $A_{S,T}$ denote the event that all neighbors of S are in T. Using the union bound, this probability is bounded by

$$\Pr(A_{S,T}) \leq \left(\frac{|T|}{n}\right)^{d|S|}.$$

Now let $\beta := d/4 \geq 1$. By the union bound again, and using that $\binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$, we find

$$\begin{aligned}
&\Pr\Big(\text{There are } S \subseteq L, T \subseteq R \text{ with } |S| \leq \frac{n}{d}, |T| < \beta|S|\Big) \\
&\qquad \leq \sum_{s=1}^{n/d} \binom{n}{s}\binom{n}{\beta s}\left(\frac{\beta s}{n}\right)^{ds} \leq \sum_{s=1}^{n/d} \binom{n}{\beta s}^2 \left(\frac{\beta s}{n}\right)^{ds} \\
&\qquad \leq \sum_{s=1}^{n/d} \left(\frac{ne}{\beta s}\right)^{2\beta s}\left(\frac{\beta s}{n}\right)^{ds} = \sum_{s=1}^{n/d} \left(\frac{4ne}{ds}\right)^{ds/2}\left(\frac{ds}{4n}\right)^{ds} \\
&\qquad = \sum_{s=1}^{n/d} \left(\frac{eds}{4n}\right)^{ds/2} \leq \sum_{s=1}^{n/d} \left(\frac{e}{4}\right)^{ds/2} \\
&\qquad \leq \sum_{s=1}^{\infty} \left(\frac{e}{4}\right)^{ds/2} = \frac{(e/4)^{d/2}}{1-(e/4)^{d/2}} < 1. \qquad \blacksquare
\end{aligned}$$

Several uses of expander graphs rely on the fact that we can turn this statement on its head: expanders can be good approximations of random graphs, i.e. they are *pseudorandom*. This, however, is beyond the scope of these notes.

7.5.3 Explicit constructions

In spite of a more relaxed condition compared to strongly regular graphs, expander graphs are still not easy to construct. Most constructions rely on algebraic relations or even on deep results from number theory. We sketch two examples, skipping the — involved — proofs.

7.5.8 THEOREM (Margulis' expanders). *Let $V = \mathbb{Z}_n \times \mathbb{Z}_n$ and define an 8-regular multigraph $G = (V, E, \iota)$ (i.e. potentially having multiple edges and loops) as follows. Let*

$$T_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \quad e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Each vertex $v \in \mathbb{Z}_n \times \mathbb{Z}_n$ is adjacent to $T_1 v, T_2 v, T_1 v + e_1, T_2 v + e_2$, and the four inverses. Then G is is an $(n, 8, 0.46)$-expander.

7.5.9 THEOREM. *Let p be prime, and let $V = \mathbb{Z}_p$. Define the multigraph $G = (V, E)$ having edge set $\{\{x, x+1\} : x \in \mathbb{Z}_p\} \cup \{\{x, x^{-1}\} : x \in \mathbb{Z}_p\}$ (taking $0^{-1} = 0$). Then G is a $(p, 3, \varepsilon)$-expander for some $\varepsilon > 0$ independent of p.*

7.5.4 Ramanujan graphs

It is known that the second largest eigenvalue λ_2 of a d-regular graph G can only be slightly smaller than $2\sqrt{d-1}$. Graphs with $\lambda_2 \leq 2\sqrt{d-1}$ are called *Ramanujan graphs*. The examples in the previous section are *not* Ramanujan graphs. The following construction does yield Ramanujan graphs, but at the cost of sacrificing constant degree:

7.5.10 THEOREM. *Let $G = (V, E)$ be a multigraph, defined by picking a prime p, setting $V = (\mathbb{Z}_p \setminus \{0\}) \times \mathbb{Z}_p$, and joining vertices (a, b) and (c, d) by an edge if and only if $ac = b + d$*

(mod p). *Then G is $(p-1)$-regular. Moreover, if $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of G, then $\lambda_2 < \sqrt{3p}$.*

Sketch of proof: One can show that
(*i*) (a,b) and (c,d) have no common neighbor if $a=c$ or $b=d$ (but not both);
(*ii*) (a,b) and (c,d) have exactly one common neighbor otherwise.
If we take A to be the adjacency matrix (with a 1 on the diagonal for each loop), then once again A^2 has the degrees on the diagonal, and the number of length-2 walks from u to v off the diagonal. Then

$$A^2 = J + (p-2)I - B,$$

where B is the adjacency matrix of the "error" graph H with an edge between (a,b) and (c,d) if and only if $a=c$ or $b=d$ (but not both). Note that H is $(2p-3)$-regular.

Let v be an eigenvector of G orthogonal to $\mathbf{1}$, and let λ be the corresponding eigenvalue. Then

$$\lambda^2 v = (p-2)v - Bv,$$

so v is an eigenvector of B with eigenvalue $p-2-\lambda^2$. The degree $2p-3$ of H is an upper bound on the absolute value of any eigenvalue of H, so

$$p-2-\lambda^2 \geq -2p+3, \tag{7.2}$$

and therefore $\lambda < \sqrt{3p}$. ∎

7.6 Where to go from here?

Textbook writers in this field have been prolific. We list a few, ranging from accessible to advanced.

- Godsil and Royle (2001), *Algebraic Graph Theory* focuses on the connections between algebra (including linear algebra) and graphs.
- Bollobás (1998), *Modern Graph Theory* contains many topics not found in the usual texts on graph theory, including spectral graph theory and random graphs.
- Brouwer and Haemers (2012), *Spectra of Graphs* is the most specialized text in this list, but at the same time the most thorough treatment of the subject.
- Brualdi (2011), *The mutually beneficial relationship of graphs and matrices* describes just what it says: it looks at applications of matrix theory in graph theory, but also the other way. Based on a series of 10 lectures, so not too long.
- Brouwer, Cohen, and Neumaier (1989), *Distance-regular Graphs* discusses a family of graphs generalizing strongly regular graphs. There are deep connections with many corners of algebraic combinatorics. Sadly out of print.
- Lubotzky (2012), *Expander Graphs in Pure and Applied Mathematics* is a detailed survey of the theory of expander graphs.
- Tao (2012), *254B - Expansion in Groups* is a set of lecture notes on the subject, focusing on constructions. Contains a good introduction and many hyperlinks and references.

CHAPTER 8

Combinatorics versus topology

THERE is a deep and fruitful interaction between combinatorics and topology. Sometimes combinatorial reasoning provides an elegant proof of a topological fact; sometimes topology helps to prove a result in combinatorics. In this chapter we will see examples of both.

8.1 The Borsuk-Ulam Theorem

We start our exploration with an important topological result, the *Borsuk-Ulam Theorem*.

8.1.1 DEFINITION. The *n-dimensional sphere* (or simply *n-sphere*) is

$$\mathscr{S}^n := \left\{ x \in \mathbb{R}^{n+1} : \|x\| = 1 \right\}.$$

8.1.2 THEOREM. *For every continuous function $f : \mathscr{S}^n \to \mathbb{R}^n$, there exists a point $x \in \mathscr{S}^n$ such that $f(-x) = f(x)$.*

In the case $n = 2$, this can be interpreted as "at any time there exist two antipodal points on earth with the same temperature and the same atmospheric pressure." In our application we will use the following corollary:

8.1.3 COROLLARY. *Let $U_0, U_1, \ldots, U_n$ be subsets of $\mathscr{S}^n$, each of which is either open or closed, such that their union covers the sphere $\mathscr{S}^n$. Then there exist an inde $i \in \{0, \ldots, n\}$ and an $x \in \mathscr{S}^n$ such that $x, -x \in U_i$.*

Sketch of proof: We prove the case where all U_i are closed. Define a function $f : \mathscr{S}^n \to \mathbb{R}^n$ by

$$f(x) := \big(\operatorname{dist}(x, U_1), \ldots, \operatorname{dist}(x, U_n)\big),$$

where $\operatorname{dist}(x, U) := \min_{y \in U} \|x - y\|$ is the infimum of the distance between x and any point in U. By the Borsuk-Ulam Theorem, there exists an $x \in \mathscr{S}^n$ such that $\operatorname{dist}(x, U_i) = \operatorname{dist}(-x, U_i)$ for all $i \in \{1, \ldots, n\}$. If $\operatorname{dist}(x, U_i) = 0$ for any such i then we are done, since then $x, -x \in U_i$ (as U_i is closed). Otherwise, since $U_0, \ldots, U_n$ is a cover and $x, -x \notin U_1 \cup \cdots \cup U_n$, we must have $x, -x \in U_0$. ∎

8.2 The chromatic number of Kneser graphs

We apply the Borsuk-Ulam Theorem to compute the chromatic number of a famous family of graphs.

8.2.1 DEFINITION. The *Kneser graph* $\mathrm{KG}_{n,k}$ is the graph with as vertex set the collection of all subsets of $[n]$ of size k, and as edge set

$$E(\mathrm{KG}_{n,k}) = \{\{A,B\} : A,B \in V(\mathrm{KG}_{n,k}), A \cap B = \emptyset\}.$$

See Figure 8.1 for $\mathrm{KG}_{5,2}$.

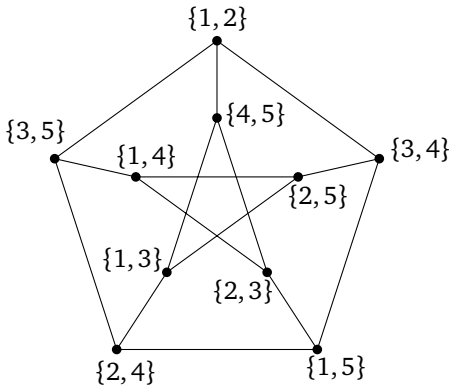


FIGURE 8.1
The Kneser graph $\mathrm{KG}_{5,2}$.

Let us first take a look at the stable set number of $\mathrm{KG}_{n,k}$. If $k \leq n/2$ then it follows from the Erdős-Ko-Rado Theorem (4.2.4) that

$$\alpha(\mathrm{KG}_{n,k}) = \binom{n-1}{k-1} = \frac{k}{n}|V(\mathrm{KG}_{n,k})|.$$

Next, the chromatic number. As in the proof of Theorem 6.4.7, an easy bound is

$$\chi(\mathrm{KG}_{n,k}) \geq \frac{|V(\mathrm{KG}_{n,k})}{\alpha(\mathrm{KG}_{n,k})}.$$

However, unlike the situation in that theorem, this bound is *not* tight. Take, for instance, the case $n = 3k-1$. Then the bound states that $\chi(\mathrm{KG}_{n,k}) \geq 3$. The next theorem states that this can be far off. In fact, the chromatic number *grows* as a function of n.

8.2.2 THEOREM. *For all integers $k \geq 0$ and $n \geq 2k-1$, we have $\chi(\mathrm{KG}_{n,k}) = n-2k+2$.*

Proof: First we show that a coloring with $n-2k+2$ colors exists, by explicitly constructing one. Remember that vertices correspond to k-subsets, and we will use the terms interchangeably. Start by coloring all k-subsets of $\{1,2,\ldots,2k-1\}$ with color 1. Then color each remaining k-subset by its maximal element. This uses

$$1 + n - (2k-1) = n - 2k + 2$$

colors.

Next, we show that there is no coloring with $d = n - 2k + 1$ colors. Suppose, for a contradiction, that there is a d-coloring of $\mathrm{KG}_{n,k}$. Let X be a set of n points of $\mathscr{S}^d$ that lie in *general position*, i.e. no $d+1$ of them lie in a d-dimensional hyperplane through the origin. Pick an arbitrary bijection $X \to [n]$. Then each k-subset of X corresponds to a vertex of $\mathrm{KG}_{n,k}$. For $i \in [d]$, let $\mathscr{A}_i$ be the family of k-subsets of X whose vertex is colored i. We use these to find a covering $U_0, \ldots, U_d$ of the sphere $\mathscr{S}^d$, as follows. For $i \in [d]$ (so $i > 0$) and $x \in \mathscr{S}^d$ we say

$$x \in U_i \text{ if there exists } A \in \mathscr{A}_i \text{ such that, for all } y \in A : \langle y, x \rangle > 0. \tag{8.1}$$

In words, all points of A lie in the open hemisphere with pole x. Finally, $U_0 := \mathscr{S}^d \setminus (U_1 \cup \cdots \cup U_d)$.

Note that $U_1, \ldots, U_d$ are open sets, whereas U_0 is closed. By Corollary 8.1.3, there exist an index i and point x such that $x, -x \in U_i$. We distinguish two cases:

Case $i = 0$. By the definition of the U_i, no k-subset is contained in either the hemisphere centered around x, and no k-subset is contained in the hemisphere centered around $-x$. Indeed: such a k-subset would have a color, i say, and then x or $-x$ would be in U_i (and therefore not in U_0). But X contains n points, so there must be at least $n - 2k + 2 \geq d + 1$ points on the equator, i.e. lying in neither of the open hemispheres. This is contradicts the fact that the points of X are in general position.

Case $i > 0$. Now there must be a k-subset A, fully contained in the open hemisphere centered around x, having color i. Likewise, there must be a k-subset B, fully contained in the open hemisphere centered around $-x$, having color i. But now A and B are disjoint, so $\{A, B\}$ is an edge of $\mathrm{KG}_{n,k}$, so A and B cannot both receive color i, a contradiction. ∎

Kneser graphs know many variants and generalizations. An obvious one is to look at arbitrary set families.

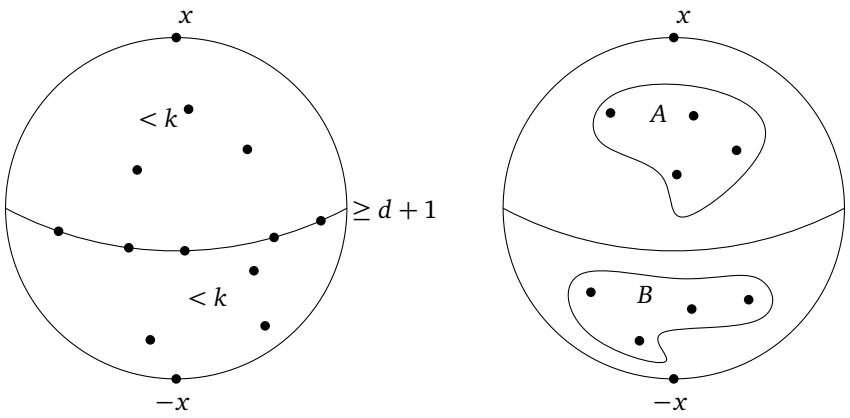


FIGURE 8.2
Detail of the proof of Theorem 8.2.2, case $i = 0$ (left) and case $i > 0$ (right).

8.2.3 DEFINITION. Let $\mathscr{F}$ be a family of sets. Then $\mathrm{KG}(\mathscr{F})$ is the graph with vertex set $\mathscr{F}$ and as edge set

$$E(\mathrm{KG}(\mathscr{F})) = \{\{A,B\} : A,B \in \mathscr{F}, A \cap B = \emptyset\}.$$

Recall, from Sections 6.2 and 6.6, that a set system $\mathscr{F}$ is 2-colorable if the elements of the underlying ground set can be 2-colored so that each member of $\mathscr{F}$ contains elements of each color.

8.2.4 DEFINITION. The *2-colorability defect* $\mathrm{cd}_2(\mathscr{F})$ of a set family $\mathscr{F}$ is the smallest number of elements X such that the family

$$\{A \in \mathscr{F} : A \cap X = \emptyset\}$$

is 2-colorable.

8.2.5 EXAMPLE. Consider the collection of all k-subsets of $[n]$. Delete any $n-2k+2 elements$. The remaining subsets are all subsets of a set with $2k-2$ elements. A 2-coloring is easily found. It follows that $\mathrm{cd}_2(\mathscr{F}) \leq n-2k+2$.

There is a surprising connection between the two very different coloring concepts discussed in this section, captured by the following result:

8.2.6 THEOREM. *For every set family $\mathscr{F}$ we have $\chi(\mathrm{KG}(\mathscr{F})) \geq \mathrm{cd}_2(\mathscr{F})$.*

We omit the proof, which is again topological and similar to that of 8.2.2.

8.3 Sperner's Lemma and Brouwer's Theorem

In this section we will see how a very combinatorial statement leads to a result in topology. We start with some terminology.

8.3.1 DEFINITION. A subset $S \subseteq \mathbb{R}^n$ is *convex* if, for all $x, y \in S$ and $\lambda \in \mathbb{R}$ with $0 \leq \lambda \leq 1$ we have $\lambda x + (1-\lambda)y \in S$.

8.3.2 DEFINITION. Given a set S, the *convex hull* is the smallest convex set containing all of S.

8.3.3 DEFINITION. An n-dimensional *simplex* is the convex hull of $n+1$ points in general position in $\mathbb{R}^n$. If $x_0, \ldots, x_n$ is this list of points, then the corresponding simplex is

$$\Delta(x_0, \ldots, x_n) := \{\lambda_0 x_0 + \cdots + \lambda_n x_n : \lambda_0, \ldots, \lambda_n \geq 0,\ \lambda_0 + \cdots + \lambda_n = 1\}.$$

8.3.4 DEFINITION. The *face* of a simplex Δ is the convex hull of a subset of the points defining the simplex. A *vertex* is a face consisting of a single point.

The main objects we will study are the following:

8.3.5 DEFINITION. A *simplicial subdivision* of an n-dimensional simplex S is a collection $\Delta_1, \ldots, \Delta_k$ of n-dimensional simplices, called "cells", satisfying

- $\bigcup_{i=1}^{k} \Delta_i = S$;
- $\Delta_i \cap \Delta_j = \emptyset$ or $\Delta_i \cap \Delta_j$ is a face of both Δ_i and Δ_j for all $i, j \in [k]$.

In Figure 8.3 a simplicial subdivision of a 2-simplex is shown.

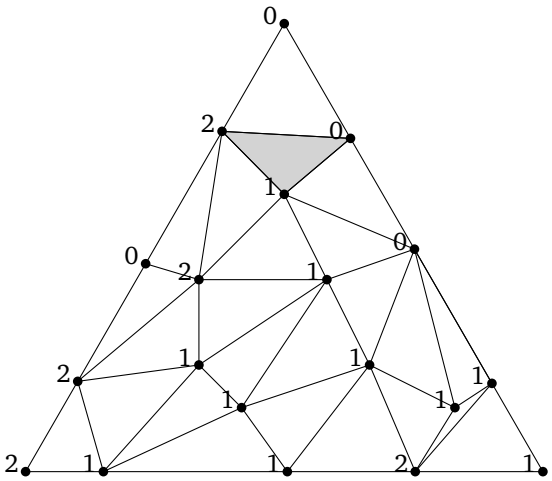


FIGURE 8.3
Simplicial subdivision of a 2-simplex. Two of the (small) simplices can be disjoint, meet in a vertex, or have a common side. A legal coloring is shown, as well as a rainbow cell.

8.3.6 DEFINITION. For each point $v = \lambda_0 x_0 + \cdots + \lambda_n x_n$, define $l(v) := \{i : \lambda_i > 0\}$. Let V be the union of the vertices of the Δ_i. A *legal coloring* of the simplicial subdivision is a map $c : V \to \{0, \ldots, n\}$ such that

$$c(v) \in l(v) \text{ for all } v \in V.$$

Now we can state our combinatorial result, known as *Sperner's Lemma*:

8.3.7 LEMMA (Sperner). *There is a cell Δ_i whose vertices all have different colors.*

Such a cell will be called a *rainbow cell*. Figure 8.3 shows a legal coloring and a rainbow cell.

Proof: We will prove a stronger statement: the number of rainbow cells is odd! We will proceed by induction on the dimension n.

Case $n = 1$. The simplex in this case is a line segment, the simplicial subdivision is a subdivision into shorter line segments, and a legal coloring is an assignment of zeroes and ones to the vertices such that the leftmost vertex has color 0 and the rightmost vertex has color 1. If we follow the line segment from left to right, we encounter an odd number of color changes. Each color change corresponds to a rainbow cell.

Case $n = 2$. In principle this case can be skipped, and the argument for general n can be followed instead. But the case gives much insight. The proof is by double counting,

where we count the pairs (Δ, e), with Δ a cell and e an edge of Δ that uses both color 0 and 1.

- Let X be the number of boundary edges having both color 0 and 1;
- Let Y be the number of interior edges having both color 0 and 1;
- Let Q be the number of non-rainbow cells containing an edge having both color 0 and 1;
- Let R be the number of rainbow cells (which always contain an edge having both color 0 and 1).

Each boundary edge is in one cell; each internal edge is in two cells. Each non-rainbow cell containing a $0-1$-edge, will have exactly two such edges. Each rainbow cell has exactly one $0-1$-edge. It follows that

$$2Q + R = X + 2Y.$$

From the case $n = 1$ we know that X is odd. But then R has to be odd too!

Case $n > 2$. We generalize the previous argument. We count the pairs (Δ, f), with Δ a cell and f an $(n-1)$-dimensional face of Δ that uses all of the colors $\{0, 1, \ldots, n-1\}$.

- Let X be the number of $(n-1)$-dimensional faces on the boundary using all of the colors $\{0, 1, \ldots, n-1\}$;
- Let Y be the number of $(n-1)$-dimensional faces in the interior using all of the colors $\{0, 1, \ldots, n-1\}$;
- Let Q be the number of non-rainbow cells using all of the colors $\{0, 1, \ldots, n-1\}$;
- Let R be the number of rainbow cells.

Again, each boundary face is in one cell; each internal face is in two cells. And again, each rainbow cell has exactly one such face. Each non-rainbow cell has two: drop either one of the two vertices whose color appears twice. So

$$2Q + R = X + 2Y.$$

Now X is odd by induction (since each such face is a rainbow cell in the $(n-1)$-simplex that is the boundary), and therefore R must be odd. ∎

Our applications of Sperner's Lemma come from topology. The first one is a proof of the famous *Brouwer's Fixed Point Theorem*.

8.3.8 DEFINITION. The *n-dimensional ball* is

$$\mathscr{B}^n := \{x \in \mathbb{R}^n : \|x\| \leq 1\}.$$

8.3.9 THEOREM (Brouwer's Fixed Point Theorem). *Let $f : \mathscr{B}^n \to \mathscr{B}^n$ be continuous. Then there exists $x \in \mathscr{B}^n$ with $f(x) = x$.*

Proof: First we note that the ball $\mathscr{B}^n$ is homeomorphic to the simplex (i.e. there is a continuous bijection whose inverse is again continuous). So it suffices to prove the result for the n-dimensional simplex $S := \Delta(e_1, \ldots, e_{n+1}) \subseteq \mathbb{R}^{n+1}$, where e_i is the ith standard basis vector (i.e. $(e_i)_j = 1$ for $i = j$ and 0 elsewhere). Let $f : S \to S$ be a continuous function, and assume f has no fixed point.

Consider a sequence $\mathscr{S}_1, \mathscr{S}_2, \ldots$ of simplicial subdivisions of S such that the length of the longest edge in the subdivision tends to 0.

Define a coloring $c_i : V(\mathscr{S}_i) \to \{1, \ldots, n+1\}$ by

$$c_i(x) = k \tag{8.2}$$

if k is the least coordinate in which $f(x_k) < x_k$. Since $f(x) \neq x$ and

$$\sum_{l=1}^{n+1} x_l = \sum_{l=1}^{n+1} f(x)_l = 1,$$

the index k exists, and therefore the coloring is well-defined.

8.3.9.1 CLAIM. *The coloring c_i is a legal coloring of the simplicial subdivision $\mathscr{S}_i$.*

Proof: Consider a vertex $v = \lambda_1 e_1 + \cdots + \lambda_{n+1} e_{n+1}$, and recall $l(v) = \{i : \lambda_i > 0\}$. Since $f(v)_i \geq 0$ for all i, the index k such that $f(v)_k < v_k$ must be among the indices in $l(v)$, that is, $c_i(v) \in l(v)$. □

It follows that we have an infinite sequence $\Delta_1, \Delta_2, \ldots$ of rainbow cells, with $\Delta_i \in \mathscr{S}_i$, such that the longest edge length tends to 0. The simplex S is closed and bounded, so the 1-colored vertices in the Δ_i have a convergent subsequence $x_{1,1}, x_{1,2}, \ldots$. Let x^* be the limit.

Now the 2-colored vertices in this subsequence converge to x^* as well, and so do the i-colored vertices for $i \in \{3, \ldots, n+1\}$. Note that, for each i, we have

$$f(x_{i,1})_i < (x_{i,1})_i, \quad f(x_{i,2})_i < (x_{i,2})_i, \quad \ldots$$

so $f(x^*)_i \leq x^*_i$ for all i. But $f(x^*) \neq x^*$, so $f(x^*)_i > x^*_i$ for at least one index i, a contradiction. ■

The next application, from Pohoata (2013), is a proof for a true Borsuk theorem - weaker than the claim from 5.4.5, yet still interesting.

8.3.10 THEOREM (Borsuk's Theorem). *Given any covering of $\mathbb{R}^n$ with uniformly bounded open sets, there exist $n+1$ of these sets that have a non-trivial intersection.*

Proof: Let S be an n-dimensional simplex in $\mathbb{R}^n$, with main vertices $v_1, \ldots, v_{n+1}$, whose sides are so large that none of the open sets in the cover cut all faces of S. For each i from $\{1, \ldots, n+1\}$, let U_i be the union of those open sets in the cover which do not intersect the face of S containing v_i. Now, the sets $\{U_i \cap S\}_i$ represent an open cover of S. We can then find a closed cover $\{V_i\}_{1 \leq i \leq n+1}$ of S such that the complements F_i of the sets V_i are contained in the U_i's for all $1 \leq i \leq n+1$. Since V_i contains v_i, but U_i does not intersect the face of S not containing v_i, F_i cuts precisely those faces of S which contain v_i. >> Now consider a triangulation of S. For each vertex of this triangulation, choose one of the sets F_i which contain the vertex, and label the vertex with the etiquette i. The observation made above that F_i cuts precisely those faces of S which contain v_i implies that this labelling is actually a Sperner coloring, and so the Sperner Lemma yields that one of the elementary n-simplices simplices in the triangulation has vertices

of different labels. Because the simplices in the triangulation can be made arbitrarily small, the compactness of the sets F_i easily implies that $\bigcap_{i=1}^{n+1} F_i \neq \emptyset$. This proves the theorem. ■

Fixed-point theorems play a major role in the theory of Nash equilibria, an important concept in game theory.

8.4 Where to go from here?

A well-written text on the combinatorial implications of the Borsuk-Ulam theorem is

- Matoušek (2003), *Using the Borsuk-Ulam Theorem. Lectures on Topological Methods in Combinatorics and Geometry*.

CHAPTER 9

Designs

DESIGN THEORY is the study of a family of combinatorial structures rich in symmetries. Designs have their origins in experiment design, a branch of statistics, but have since found applications in other areas, such as computer science.

9.1 Definition and basic properties

We start with a generalization of the notion of set system:

9.1.1 DEFINITION. An *incidence structure* is a triple $(\mathscr{P}, \mathscr{B}, I)$, where
- $\mathscr{P}$ is a finite set; its elements are called *points*.
- $\mathscr{B}$ is a finite set; its elements are called *blocks*.
- $I \subseteq \mathscr{P} \times \mathscr{B}$; I is called an *incidence relation*

Instead of writing $(p, B) \in I$ we will use the shorthand $p \in B$. We say p and B are *incident*. If no two blocks have the same set of incidences, we say the incidence structure is *simple*. In that case we can consider the blocks as subsets of $\mathscr{P}$, and identify the incidence structure with a set system $(\mathscr{P}, \mathscr{B})$.

9.1.2 DEFINITION. Let $v \geq k \geq t \geq 0$ and $\lambda \geq 1$ be integers. A $t-(v,k,\lambda)$ *design* (or a t-*design on v points with block size k and index λ*) is an incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B}, I)$ with
- $|\mathscr{P}| = v$
- $|B| = k$ for all $B \in \mathscr{B}$
- For every subset T of t points, exactly λ blocks are incident with all points of T.

The main question in design theory is the following:

9.1.3 QUESTION. For which values of the parameters do (simple, nontrivial) $t-(v,k,\lambda)$ designs exist?

Trivial designs are the following:

- There is one block, and it contains all points. This is a $t-(v,v,1)$ design for all $t \leq v$.

- $\mathscr{B}$ is the collection of *all* size-k subsets. This is a $t-(v,k,\lambda)$ design for all $t \leq k$ and appropriate λ.

From now on, unless indicated otherwise, we will use the following

9.1.3.1 ASSUMPTION. $v > k > t$.

A famous design question is the following problem:

9.1.4 EXERCISE (Kirkman's Schoolgirls). Fifteen girls walk to school each day in 5 groups of 3. Arrange a schedule so that, in a week, each pair walks side by side only once.

In our language, this asks for a $2-(15,3,1)$ design, with the additional property that the set of 45 blocks gets partitioned into seven groups of 5.

One can associate more parameters with designs. One notable parameter is the number of blocks (45 in the example just discussed). But it turns out this number is determined by the other parameters:

9.1.5 LEMMA. *Let b be the number of blocks of a $t-(v,k,\lambda)$ design. Then*

$$b = \lambda \binom{v}{t} \Big/ \binom{k}{t}.$$

Proof: Count the pairs (T,B) where B is a block and T a size-t subset contained in B in two ways. ∎

We can get more detailed:

9.1.6 LEMMA. *For $0 \leq i \leq t$, let b_i be the number of blocks containing a fixed size-i subset S of points. Then*

$$b_i = \lambda \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i}.$$

In particular, this number does not depend on the choice of S. Hence each $t-(v,k,\lambda)$ design is also an $i-(v,k,b_i)$ design.

The number b_1, the number of blocks containing a fixed element, is also called the *replication number*, denoted by r. We have

9.1.7 LEMMA. *For a design with $t = 2$ we have*

$$bk = vr,$$
$$\lambda(v-1) = r(k-1).$$

An obvious necessary condition for a design to exist, is that all numbers we've seen are integers. But this is not always sufficient. For instance, does a $10-(72,16,1)$ design exist? If we look at the b_i, for instance by running the following code through the SAGE computer algebra system,

```
[binomial(72-i, 10-i) / binomial(16-i, 10-i) for i in range(11)]
```

we see that all b_i are integers. But the following result still rules out the existence of a corresponding design:

9.1.8 THEOREM (Tits). *For any nontrivial $t-(v,k,1)$ design, we have*

$$v \geq (t+1)(k-t+1).$$

Proof: Note that $\lambda = 1$, so any two blocks overlap in at most $t-1$ elements. Pick a set S of $t+1$ elements so that S is not contained in any block. (*Exercise:* why does S exist?)

For each $T \subseteq S$, with $|T| = t$, there is a unique block B_T containing T. Now B_T has $k-t$ other elements, and since $|B_T \cap B_{T'}| = t-1$ for $T' \neq T$, $T' \subseteq S$ with $|T'| = t$, each element of $\mathscr{P} \setminus S$ is in at most one set B_T. Hence

$$v \geq |S| + (t+1)(k-t) = (t+1) + (t+1)(k-t). \qquad \blacksquare$$

Finally, here is a reformulation of a result we've seen before, namely Theorem 5.4.1.

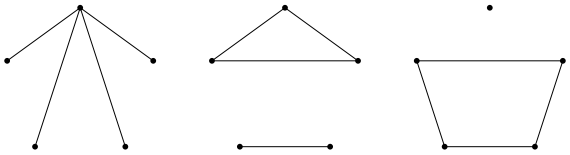
9.1.9 THEOREM (Fisher's Inequality). *In a $2-(v,k,\lambda)$ design with b blocks, and $v > k$, we have*

$$b \geq v.$$

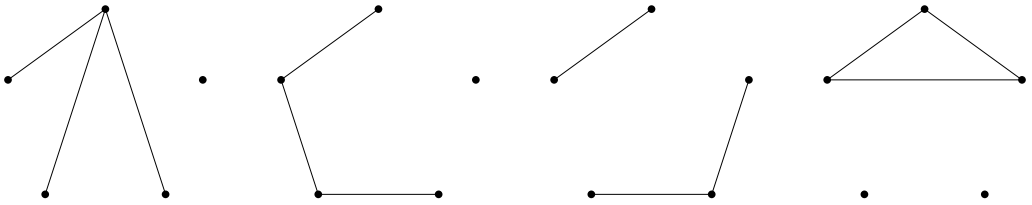
9.2 Some constructions

Our first design is a bit of a novelty item.

9.2.1 EXAMPLE. Let $\mathscr{P} := E(K_5)$, the edge set of the complete graph on 5 vertices. The blocks of the design will be the size-4 subsets of edges such that the subgraph has one of the following shapes:



There are $5 + 10 + 15 = 30$ blocks. Next, consider a triple of edges. The corresponding subgraph can take on one of the following shapes:



Note that each triple can be completed in a unique way into one of the blocks. It follows that we have found a $3-(10,4,1)$ design.

Next we consider an infinite family. These are based on the third outcome of the De Bruijn-Erdős Theorem (Theorem 4.5.1).

9.2.2 EXAMPLE. A *projective plane of order q* is a configuration of q^2+q+1 points and q^2+q+1 lines such that

- Every two points determine a unique line.
- Every two lines meet in a unique point.
- Every line has $q+1$ points.
- Every point is on $q+1$ lines.

If we take the lines as our blocks, this gives a $2-(q^2+q+1, q+1, 1)$ design.

In Problem 4.5.2 we raised the question for which values of q a projective plane exists. The following theorem gives a sufficient condition.

9.2.3 THEOREM. *For each prime power q there exists a projective plane of order q.*

Proof: Consider the vector space $\mathrm{GF}(q)^3$. Let the points be the 1-dimensional subspaces, and the lines be the 2-dimensional subspaces.

Each nonzero vector v spans a unique 1-dimensional subspace $\langle v\rangle$. This subspace contains $(0,0,0)$ and all nonzero multiples of v, of which there are $q-1$. It follows that there are

$$\frac{q^3-1}{q-1} = q^2+q+1$$

1-dimensional subspaces, i.e. points. Each pair of points spans a unique 2-dimensional subspace; all other properties can be derived from here. ∎

9.3 Large values of t

We can find designs for a wide range of parameters once we allow repeated blocks:

9.3.1 THEOREM. *Let t,k,v be given with $t<k<v-t$. If repeated blocks are allowed, then there exists a $t-(v,k,\lambda)$ design for some λ.*

Proof: Let $\mathscr{P} := [v]$ be a set of points. Define a $\binom{v}{t}\times\binom{v}{k}$ matrix M, with rows indexed by the size-t subsets of $\mathscr{P}$ and columns indexed by the size-k subsets of $\mathscr{P}$, and entries

$$M_{T,K} = \begin{cases} 1 & \text{if } T\subseteq K \\ 0 & \text{otherwise.}\end{cases}$$

Since $t<k<v-t$, the matrix M has more columns than rows, so the columns are linearly dependent over $\mathbb{Q}$. That is, we can find coefficients α_K, not all zero, such that

$$\sum_{K\subseteq\mathscr{P}:|K|=k} \alpha_K M_{T,K} = 0$$

for all $T\subseteq\mathscr{P}$ with $|T|=t$. Possibly after scaling we may assume $\alpha_K\in\mathbb{Z}$ for all K. Let d be an integer such that $\alpha_K+d\geq 0$ for all K, and $\alpha_K+d=0$ for some K. Consider

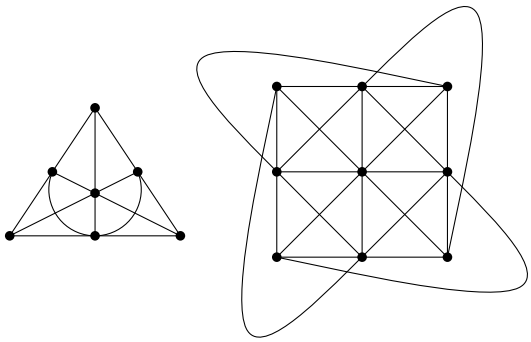


FIGURE 9.1
An STS(7) *and an* STS(9).

the incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B}, I)$ in which each block K is repeated $\alpha_K + d$ times. We claim that this is the desired design.

To see this, pick any subset T of size t, and count the number of blocks containing T. This is

$$\sum_K M_{T,K}(\alpha_K + d) = \sum_K M_{T,K} d = d\binom{v-t}{k-t} d.$$

Clearly this number does not depend on our choice of T, so $\mathscr{D}$ is a $t-(v,k,d\binom{v-t}{k-t})$ design. ∎

A more difficult question is for which values of t designs exist without repeated blocks. A result by Teirlinck shows that we can still find designs for all values of t, but the parameters v and k can no longer be chosen freely, and will in fact be very large relative to t.

If, in addition, we demand that $\lambda = 1$, then our knowledge shrinks dramatically. We know of a finite number of designs with $t \geq 4$, and of *no* designs with $t > 6$.

9.4 Steiner Triple Systems

For at least one class of designs, the existence problem has been settled completely (but not the uniqueness problem!). In this section we will look at those designs.

9.4.1 DEFINITION. A *Steiner triple system* of order v (denoted STS(v)) is a $2-(v,3,1)$ design.

In Figure 9.1 two small Steiner triple systems are shown. We will show the following:

9.4.2 THEOREM. *There exists an* STS(v) *if and only if* $v = 0$ *or* $v \equiv 1 \pmod 6$ *or* $v \equiv 3 \pmod 6$.

Proof of necessity: Necessity follows easily from Lemma 9.1.7: we have

$$3b = vr$$
$$v - 1 = 2r.$$

Since r is an integer, the second equation implies that v is odd, i.e. $v \equiv 1, 3$, or $5 \pmod 6$. Substituting the second equation in the first gives

$$b = \frac{v(v-1)}{6},$$

and it is easily checked that $v = 6x + 5$ doesn't work. ∎

To prove sufficiency, we need to construct designs. Our first construction is the following:

9.4.3 LEMMA. *Let $n = 2m + 1$ and $\mathscr{P} := \mathbb{Z}_n \times \mathbb{Z}_3$. Consider the set $\mathscr{B}$ consisting of*

- *All triples of the form $\{(x,0),(x,1),(x,2)\}$ for $x \in \mathbb{Z}_n$;*
- *All triples of the form $\{(x,i),(y,i),(z,i+1)\}$ for $x, y, z \in \mathbb{Z}_n$ such that $x \neq y$ and $2z = x + y$, and for all $i \in \mathbb{Z}_3$.*

Then $(\mathscr{P}, \mathscr{B})$ is an STS$(3n) =$ STS$(6m + 3)$.

Sketch of proof: Note that, for fixed x, y, there is a unique value of z with $x + y = 2z$. This is because 2 has a multiplicative inverse in $\mathbb{Z}_n$. It follows that the number of blocks is

$$n + 3\binom{n}{2} = \frac{3n(3n-1)}{6},$$

as expected. We leave it as an exercise to show that each pair of points is in a unique block. ∎

While direct constructions for STS$(6m + 1)$ also exist, we will instead look at a recursive construction, building new designs by gluing together smaller ones.

9.4.4 DEFINITION. If $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ is a Steiner Triple System, and $\mathscr{P}' \subseteq \mathscr{P}$ is such that any triple from $\mathscr{B}$ with two points in $\mathscr{P}'$ is fully contained in $\mathscr{P}'$, then we say $(\mathscr{P}', \mathscr{B}')$ is a *subsystem*, where $\mathscr{B}'$ is the restriction of $\mathscr{B}$ to those sets fully contained in $\mathscr{P}'$.

9.4.5 THEOREM. *Let $\mathscr{D}$ be an* STS(v) *having an* STS(u) *subsystem. Let $\mathscr{D}'$ be an* STS(w). *Then there exists an* STS$(u + w(v - u))$.

If $w > 0$ then this new system has $\mathscr{D}$ as a subsystem.

If $0 < u < v$ and $w > 1$ then the new system may be chosen such that it has an STS(7) *subsystem.*

Proof: Label the points of $\mathscr{D}$ as $\mathscr{P} = \{a_1, \ldots, a_u\} \cup \{b_i : i \in \mathbb{Z}_m\}$, where $\{a_1, \ldots, a_u\}$ are the points of the subsystem, and $m = v - u$. Label the points of $\mathscr{D}'$ as $\{1, \ldots, w\}$.

We construct our new design as follows: take w disjoint copies of $\mathscr{D}$. Identify the points $\{a_1, \ldots, a_u\}$ and add new blocks according to $\mathscr{D}'$. Figure 9.2 illustrates the process. We now give the construction in detail.

Define the set of points $\mathscr{Q} := \{a_1, \ldots, a_u\} \cup \{d_{p,i} : p = 1, \ldots, w; i \in \mathbb{Z}_m\}$. We define w maps from the design $\mathscr{D}$ to the "pages" of the new construction:

$$\varphi_p : \mathscr{P} \to \mathscr{Q}, \text{ defined by } \varphi_p(a_i) = a_i \text{ and } \varphi_p(b_i) = d_{p,i}.$$

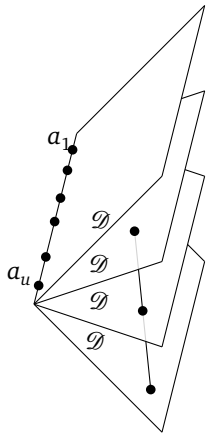


FIGURE 9.2
Gluing together Steiner Triple Systems

The blocks of the new design are of two kinds. First, there are the blocks of $\mathscr{D}$, copied to each page:

$$\varphi_1(\mathscr{B}) \cup \cdots \cup \varphi_w(\mathscr{B}).$$

Second, there are all triples of the form $\{d_{p_1,i_1}, d_{p_2,i_2}, d_{p_3,i_3}\}$ such that

- $\{p_1, p_2, p_3\}$ is a block of $\mathscr{D}'$;
- $i_1 + i_2 + i_3 \equiv 0 \pmod{m}$.

Again, we leave it as an exercise that each pair is in a unique triple.

The second claim in the theorem is obvious from the construction: any page is isomorphic to the original $\mathscr{D}$.

For the last claim, pick any $a \in \mathscr{P}'$. Note that $m = v - u$ is even and nonzero. Number the b_i such that $\{a, b_0, b_{m/2}\}$ is a triple of $\mathscr{D}$. Label the elements of $\mathscr{D}'$ such that $\{1, 2, 3\}$ is a triple of $\mathscr{D}'$. Then it can be checked that the newly constructed design contains a configuration as illustrated in Figure 9.3. ∎

To prove Theorem 9.4.2, we need to check that the construction suffices to create Steiner Triple systems of all desired orders. This is a bit of a puzzle, of which we omit the details. Note that, in addition to the Steiner triple systems already discussed, we also need an STS(13).

9.5 A different construction: Hadamard matrices

We take a short detour into another family of highly regular mathematical structures: *Hadamard matrices.* These matrices were named in honor of Hadamard, who proved the following theorem:

9.5.1 THEOREM. *Let A be an $n \times n$ real matrix with $|a_{ij}| \leq 1$ for all $i, j \in [n]$. Then $|\det(A)| \leq n^{n/2}$. Equality holds if and only if*

- *$a_{ij} = \pm 1$ for all $i, j \in [n]$, and*
- *$AA^T = nI$.*

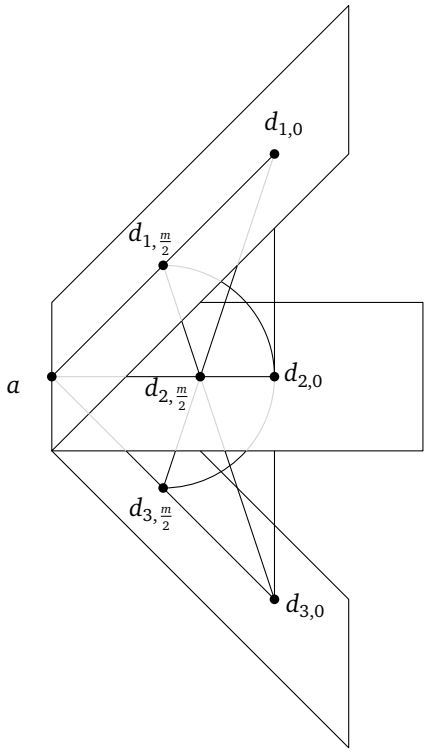


FIGURE 9.3
An STS(7) *as subsystem of the recursive construction.*

Sketch of proof: We use a geometric interpretation of the determinant. Let P be the parallelepiped in $\mathbb{R}^n$ whose sides are defined by the rows of A. Then $\text{vol}(P) = |\det(A)|$. See Figure 9.4 for an example where $n = 2$. Note that $\|a_i\| \leq \sqrt{n}$, and $\text{vol}(P) \leq \prod_{i=1}^{n} \|a_i\| \leq (\sqrt{n})^n$. For equality to hold in the theorem, we must therefore have

- $\|a_i\| = \sqrt{n}$;
- $\langle a_i, a_j \rangle = 0$, i.e. the vectors are pairwise orthogonal.

These conditions yield the desired result. ∎

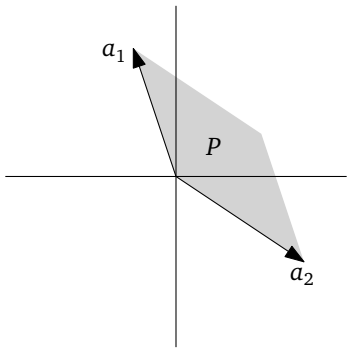


FIGURE 9.4
Relation between determinant and parallelepiped volume

9.5.2 DEFINITION. An $n \times n$ matrix $A = (a_{ij})$ is a *Hadamard matrix* if

$$a_{ij} = \pm 1 \text{ for all } i, j \in [n];$$
$$AA^T = nI.$$

The main question, as usual, is whether Hadamard matrices exist. It is not hard to find the first few examples:

$$\begin{bmatrix} 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

For $n = 3$, we get that $\langle a_i, a_j \rangle = \pm 1 \pm 1 \pm 1$ which is never 0. Generalizing this argument leads us to conclude that n had better be even if $n > 1$. But we can do a little better:

9.5.3 THEOREM. *If a Hadamard matrix of order n exists, then $n = 1, 2$, or $n \equiv 0 \pmod 4$.*

Proof: Consider a Hadamard matrix A with at least three rows. We can do a number of things to A without changing its properties. Notably we can swap rows, swap columns, and multiply rows and columns by -1 (*check this!*). Hence we can assume that the first three rows look like this (we denote entries equal to 1 by a $+$ and equal to -1 by a $-$):

$$\begin{array}{cccc} \overbrace{+\cdots+}^{a} & \overbrace{+\cdots+}^{b} & \overbrace{+\cdots+}^{c} & \overbrace{+\cdots+}^{d} \\ +\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\ +\cdots+ & -\cdots- & +\cdots+ & -\cdots- \end{array}$$

where a, b, c, d denote the number of columns of each kind. Since the inner product between each pair needs to be 0, we derive the following relations:

$$\begin{aligned} a + b &= c + d \\ a + c &= b + d \\ a + d &= b + c \\ a + b + c + d &= n, \end{aligned}$$

and we conclude that $a = b = c = d = n/4$, from which the result follows. ∎

The major open problem in this area is the following:

9.5.4 CONJECTURE. *If $n \equiv 0 \pmod 4$, then there exists an $n \times n$ Hadamard matrix.*

For $n \leq 1000$, the conjecture has verified for all orders but $668,716,892$.

Hadamard matrices have many attractive properties showing a high degree of balance or regularity. We give one example.

9.5.5 THEOREM. *The absolute value of the sum of the entries of any $a \times b$ submatrix of an $n \times n$ Hadamard matrix does not exceed $\sqrt{abn}$.*

Proof: Let D be an $a \times b$ submatrix of the $n \times n$ Hadamard matrix A. By permuting rows and columns we may as well assume that D consists of the first a rows and b columns. Let α be the sum of the entries of D.

Define $v_1, \ldots, v_a$ to be the first a rows of A, and let $y := v_1 + \cdots + v_a$. Let x be a vector of length n whose first b entries are 1 and whose remaining $n - b$ entries are 0. Then $\alpha = \langle x, y \rangle$, and so

$$\alpha^2 = \langle x, y \rangle^2 \leq \|x\|^2 \cdot \|y\|^2 = b\|y\|^2 = b \sum_{i=1}^{a} \langle v_i, v_i \rangle = abn. \qquad \blacksquare$$

9.5.1 Constructions

We will look at two constructions. The first builds new Hadamard matrices out of old through the *tensor product*: given matrices $A = (a_{ij})$ and B, define

$$A \otimes B := \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{bmatrix}.$$

9.5.6 LEMMA. *If A and B are Hadamard matrices, then so is $A \otimes B$.*

Sketch of proof: Let A be $n \times n$ and B be $m \times m$. Using some easy to verify properties of the tensor product, we see

$$(A \otimes B)(A \otimes B)^T = AA^T \otimes BB^T = nI_n \otimes mI_m = nmI_{nm}. \qquad \blacksquare$$

By starting with a 2×2 Hadamard matrix, we conclude that there exist Hadamard matrices for all $n = 2^k, k \in \mathbb{N}$. These are called Hadamard matrices of *Sylvester type*.

Our second example relies on some basic number theory.

9.5.7 THEOREM. *Suppose $q \equiv -1 \pmod 4$ is a prime power. Let $P(q) = (p_{ij})$ be a $(q+1) \times (q+1)$ matrix with rows and columns indexed by $\mathrm{GF}(q) \cup \{\infty\}$, and entries*

$$p_{ij} = \begin{cases} +1 & \text{if } i = \infty \text{ or } j = \infty \\ -1 & \text{if } i = j \neq \infty \\ +1 & \text{if } i - j \text{ is nonzero square in } \mathrm{GF}(q) \\ -1 & \text{if } i - j \text{ is nonzero non-square in } \mathrm{GF}(q). \end{cases}$$

Then $P(q)$ is a Hadamard matrix.

Sketch of proof: Define the following function (also known as the *Legendre symbol*):

$$\chi(x) := \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is nonzero square} \\ -1 & \text{if } x \text{ is nonzero non-square.} \end{cases}$$

Note that each finite field $\mathrm{GF}(q)$ is *cyclic*: there is a generator $g \in \mathrm{GF}(q)$ such that $x = g^r$ for some $r \in \{0, \ldots, q-2\}$, for all $x \in \mathrm{GF}(q) \setminus \{0\}$. Since exactly half the values of r are even, exactly half the nonzero elements of $\mathrm{GF}(q)$ are squares. Moreover, we have $\chi(xy) = \chi(x)\chi(y)$.

9.5.7.1 CLAIM. *If $c \neq 0$, then we have*

$$\sum_{b \in \mathrm{GF}(q)} \chi(b)\chi(b+c) = -1.$$

Proof: To see this, write, for $b \neq 0$, $\chi(b+c) = \chi(b)\chi(1+cb^{-1})$. The sum now becomes

$$\sum_{b \neq 0} \chi(b)^2 \chi(1+cb^{-1}).$$

It is clear that $1+cb^{-1}$ takes on all nonzero values but 1 (just look at the inverses). The result follows since exactly half the nonzero values get mapped to -1. □

Now consider the inner product between two of the rows (where we assume neither row is indexed by ∞, which is an easy case anyway):

$$\langle p_i, p_k \rangle = \sum_{j \in \mathrm{GF}(q) \cup \infty} p_{ij} p_{kj} = 1 + \sum_{j \in \mathrm{GF}(q)} \chi(i-j)\chi(k-j).$$

The result now follows by an easy substitution. ■

9.5.2 Designs from Hadamard matrices

The reason we introduced Hadamard matrices, aside from their intrinsic interest, is to create some more designs.

9.5.8 EXAMPLE. Let A be a Hadamard matrix of order $4k$, scaled so the first row and first column have only positive entries. Delete the first row and column. Let $\mathscr{P}$ be the set of remaining rows, $\mathscr{B}$ the set of remaining columns, and set $p \in B$ if $A_{pB} = +1$. If we pick any pair of rows and carry out the sorting argument from the proof of Theorem 9.5.3, we see that they have exactly $k-1$ positive entries in common. Hence we have constructed a $2-(4k-1, 2k-1, k-1)$ design.

9.5.9 EXERCISE. Use a similar technique to find a $3-(4k, 2k, k-1)$ design.

9.6 Where to go from here?

Design theory is a vast subject. A good place to get started is

- http://www.designtheory.org/

and in particular the bibliography at

- http://designtheory.org/library/encyc/biblio/

CHAPTER 10

Coding Theory

ERROR-correcting codes are one of the hidden success stories of mathematics. They enable reliable communication over noisy channels (which include airwaves). The Mars explorers use them to send us their pictures, CD players use them to compensate for scratches, and your cell phone uses them to send your voice to the receiving party.

10.1 Codes

The key to error correction is to introduce *redundancy* to the signal. We do this as follows.

10.1.1 DEFINITION. Let S be a finite set, and $n \geq 0$ an integer. A *code* C is a subset of S^n, the collection of n-tuples from S.

The elements of C are called *codewords*. We usually think of them as row vectors. A typical choice for S is a finite field $\mathrm{GF}(q)$, with $\mathrm{GF}(2) = \{0, 1\}$ being the most common. We define a *metric* on S^n:

10.1.2 DEFINITION. The *Hamming distance* between $x, y \in S^n$ is

$$d(x, y) := |\{i : x_i \neq y_i\}|.$$

It's easy to check the following properties (the second one is the triangle inequality):

10.1.3 LEMMA. *For all $x, y, z \in S^n$ we have*

- $d(x, y) = d(y, x)$*, and*
- $d(x, y) + d(y, z) \geq d(x, z)$*.*

The idea behind error correction is the following:

- The sender transmits an element $c \in C$;
- The receiver receives an element $y \in S^n$;
- The receiver finds the element $c^* \in C$ such that $d(c^*, y)$ is minimized, and assumes that c^* was the submitted codeword.

In order for this to work (at least most of the time), we must ensure that, with high probability, $c^* = c$. In most situations it is likelier that few coordinates have changed, than that many coordinates have changed. Hence a useful measure for this probability is the number of errors that can still be corrected.

10.1.4 LEMMA. *If $d := \min_{x,y\in C} d(x,y) \geq 2e+1$, then up to e errors can be corrected.*

Proof: Suppose not. Then there exist $y \in S^n$ and $x, z \in C$ such that $d(x,y) \leq e$ and $d(z,y) \leq e$. But then

$$2e+1 \leq d(x,z) \leq d(x,y) + d(y,z) \leq 2e,$$

a contradiction. ∎

When communicating, each transmission has a cost, so we want to convey as much information as possible. This means that we look for codes with a large number of codewords. Clearly this goal clashes with the goal of achieving a large minimum distance. We consider three bounds on the size of a code with minimum distance d, a lower bound and two upper bounds.

10.1.5 THEOREM. *Let S be a finite set with q elements. There exists a code C over S^n with minimum distance d and*

$$|C| \geq q^n \Bigg/ \left(\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \right).$$

Proof: Suppose $|C| = k$, and fix some $c \in C$. The number of elements of S^n having distance less than d to a codeword is $\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$. Clearly C can contain none of these points except c itself. But as long as $k \cdot \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i < q^n$, there is an element $c' \in S^n$ that can be added to C while keeping the minimum distance at least d. ∎

In other words, we are trying to *cover* S^n with spheres of radius $d-1$.

10.1.6 THEOREM (Hamming bound). *Let S be a finite set with q elements. There exists an e-error correcting code C over S^n with*

$$|C| \leq q^n \Bigg/ \left(\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \right).$$

Proof: The number of elements of S^n having distance at most e to a codeword x is $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$. Note that each element in that neighborhood can have distance $\leq e$ to at most one codeword, otherwise the code is not e-error correcting. Hence these neighborhoods need to be disjoint, and the result follows. ∎

In other words, we are trying to *pack* spheres of radius e in S^n. A code attaining the bound is called a *perfect code*.

10.1.7 THEOREM (Singleton bound). *With the same setup as before, $|C| \leq q^{n-d+1}$.*

Proof: Pick $d-1$ coordinates and delete them from all codewords. The resulting words are still all different, since the minimum distance is at least d. Clearly there are at most $q^{n-(d-1)}$ possible words left. ∎

A code attaining the Singleton bound is called a *Maximum-distance separable (MDS) code*.

10.2 Linear codes

In this section we study an important class of codes with extra structure. This structure opens the way to more advanced analysis, and to efficient encoding/decoding algorithms.

10.2.1 DEFINITION. A code C is *linear* if $S = \mathrm{GF}(q)$ is a finite field, and for all $x, y \in C$ and $\alpha \in \mathrm{GF}(q)$ we have

$$x + y \in C$$
$$\alpha x \in C.$$

In other words, C is a *linear subspace* of $\mathrm{GF}(q)^n$. If $\dim(C) = k$ then we say C is a *q-ary $[n,k,d]$ code*. The fraction k/n is the *code rate*.

10.2.2 DEFINITION. The *weight* of a codeword x, denoted by $\mathrm{wt}(x)$, is the number of nonzero coordinates. In other words,

$$\mathrm{wt}(x) = d(x,0).$$

Since $d(x,y) = d(x-y,0)$, we have the following:

10.2.3 LEMMA. *If C is a linear code, then $d = \min_{x \in C} \mathrm{wt}(x)$.*

With each linear code we can associate a second code:

10.2.4 DEFINITION. If C is a q-ary linear $[n,k,d]$ code, then the *dual code* is

$$C^\perp := \{u \in \mathrm{GF}(q)^n : \langle u, v \rangle = 0 \text{ for all } v \in C\}.$$

Note that $C^\perp$ is the orthogonal complement of the linear subspace C, and therefore it is a linear $[n, n-k, d']$ code for some d'.

Since linear codes are linear subspaces, they are fully specified by a basis:

10.2.5 DEFINITION. Let C be a q-ary linear $[n,k,d]$ code. A *generator matrix* for C is a $k \times n$ matrix G such that $C = \mathrm{rowspan}(G)$. A generator matrix H for $C^\perp$ is called a *(parity) check matrix* of G.

The name "parity check" derives from the fact that c is a codeword in C if and only if $cH^T = 0$. Given matrices G and H, the encoding/decoding process now looks as follows:

Encoding: Given $x \in \mathrm{GF}(q)^k$, compute and send $c := xG$.

Decoding: On receiving $y \in \mathrm{GF}(q)^n$, compute the *syndrome* yH^T. This is zero if and only if y is a codeword. What happens next depends on how cleverly G and H were constructed, and falls beyond the scope of this course.

The check matrix of a code can help with determining the minimum distance:

10.2.6 THEOREM. *A linear code C with check matrix H has minimum weight at least d if and only if any $d-1$ columns of H are linearly independent.*

Proof: Suppose there is a set of $d-1$ linearly dependent columns. This implies there is a word c with $\mathrm{wt}(c) \leq d-1$ such that $cH^T = 0$. Hence the minimum distance of C is at most $\mathrm{wt}(c) \leq d-1$. The converse follows by reversing the argument. ∎

10.2.1 Hamming codes

Let us look at an example.

10.2.7 DEFINITION. Take all vectors in $\mathrm{GF}(q)^r$, but remove multiples of previously chosen vectors. This gives a $r \times \left(\frac{q^r-1}{q-1}\right)$ matrix H. The code C with check matrix H is called a *Hamming code*.

10.2.8 THEOREM. *A Hamming code over* $\mathrm{GF}(q)$ *has parameters* $[n, n-r, 3]$, *where* $n = \frac{q^r-1}{q-1}$.

Proof: The first two parameters follow directly from duality; the third follows since any two columns in H are linearly independent. ∎

10.2.9 THEOREM. *Hamming codes are perfect, 1-error-correcting codes.*

Proof: We already know Hamming codes are 1-error-correcting; let us show they are perfect. This follows almost immediately:

$$|C| = q^{n-r} = \frac{q^n}{q^r} = \frac{q^n}{1+n(q-1)}.$$ ∎

10.2.2 MDS codes

Next, let us take a closer look at MDS codes. Linear MDS codes have the following relationship between their parameters:

10.2.10 LEMMA. *If C is a q-ary linear $[n,k,d]$ code, then $k = n-d+1$, and $d = n-k+1$.*

Proof: $|C| = q^k = q^{n-d+1}$. ∎

The dual of a linear MDS code is again an MDS code, as is shown by the following result:

10.2.11 THEOREM. *Let C be a q-ary linear $[n,k,d]$ code with generator matrix $G = [I_k \; D]$ and check matrix $H = [-D^T I_{n-k}]$, such that $d = n-k+1$. The following are equivalent:*

(i) C is an MDS code;

(ii) Every $d-1 (= n-k)$ columns of H are linearly independent;

(iii) Every square submatrix of D is nonsingular;
(iv) Every k columns of G are linearly independent;
(v) $C^\perp$ is an MDS code.

Proof: The fact (*i*) $\Rightarrow$ (*ii*) is Theorem 10.2.6. From (*ii*) it follows that every $(n-k)\times(n-k)$ submatrix of H is nonsingular. Every submatrix of D can be augmented to an $(n-k)\times(n-k)$ matrix using columns from the identity submatrix of H, and the determinant of that augmented matrix is $\pm$ the determinant of the submatrix of D. Hence (*iii*) follows from (*ii*). From there (*iv*) can be readily deduced, and using Theorem 10.2.6 we conclude that (*v*) holds.

The reverse implications follow by swapping C and $C^\perp$. ∎

The main question surrounding MDS codes, and in fact one of the major open problems in coding theory, is the following:

10.2.12 QUESTION. Given k, what is the largest n such that there is a q-ary $[n,k,d]$ linear MDS code?

Let us start by considering an example of a construction. The main ingredient is the following:

10.2.13 DEFINITION. A *Vandermonde matrix* is an $n\times n$ matrix of the form

$$V_n = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}.$$

Without proof we state the following:

10.2.14 LEMMA. *If V_n is a Vandermonde matrix, then*

$$\det(V_n) = \prod_{1\le i<j\le n} (x_j - x_i).$$

Note that this formula is valid over any field, and for any $x_1,\ldots,x_n$ from that field. This is a really beautiful result that comes to aid in very surprising contexts. Before passing to our construction, we make a detour with an example from elementary number theory that is connected with the determinants from Section ?

10.2.15 EXAMPLE. For any sequence of positive integers $(a_n)_{n\ge1}$, we have that $\prod_{1\le i<j\le n}(j-i)$ divides $\prod_{1\le i<j\le n}(a_j-a_i)$.

In other words, the product

$$\prod_{1\le i<j\le n} \frac{a_j - a_i}{j-i}$$

is an integer. In this form, the result reminds of the Vandermonde determinant, namely Lemma 10.2.14.

Sketch of proof: By Lemma 10.2.14, we can write that

$$\prod_{1\le i<j\le n} \frac{a_j - a_i}{j-i} = \frac{1}{1!\cdot 2!\cdot \ldots (n-1)!}\cdot \det(V),$$

where

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix}.$$

Elementary row operations then lead to

$$\frac{1}{1!\cdot 2!\cdot \ldots (n-1)!}\cdot \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix} = \det \begin{bmatrix} 1 & \cdots & 1 \\ \binom{a_1}{1} & \cdots & \binom{a_n}{1} \\ \vdots & & \vdots \\ \binom{a_1}{n-1} & \cdots & \binom{a_n}{n-1} \end{bmatrix},$$

which proves that

$$\prod_{1\le i<j\le n} \frac{a_j - a_i}{j-i}$$

is an integer, since the latter determinant is an integer (all entries are integers). ∎

We return to our construction.

10.2.16 DEFINITION. Suppose q is a prime power and $k \le q$. The q-ary *Reed-Solomon code* is the linear code with generator matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ x_1 & x_2 & \cdots & x_q & 0 \\ x_1^2 & x_2^2 & \cdots & x_q^2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_q^{k-1} & 1 \end{bmatrix},$$

where $x_1, \ldots, x_q$ are the q distinct elements of GF(q).

10.2.17 THEOREM. *The Reed-Solomon code is an MDS code.*

Proof: It follows easily from Lemma 10.2.14 that the determinant of every $k \times k$ submatrix is nonzero, and hence that the corresponding k columns are independent. This is condition 10.2.11(*iv*). ∎

It is conjectured that this construction is, in fact, almost always best possible:

10.2.18 CONJECTURE (MDS Conjecture). *Let q be a prime power, and $k \le q$ an integer. A q-ary linear $[n,k,d]$ MDS code has $n \le q+1$, except if $q = 2^h$ for some $h \ge 1$, and $k \in \{3, q-1\}$. In those cases $n \le q+2$.*

This conjecture was almost completely open for decades, but not too long ago a major step was made:

10.2.19 THEOREM (Ball 2011). *The MDS Conjecture holds if q is a prime number.*

10.3 The weight enumerator

We return to the theme from Chapter 2 and collect some information about codes in polynomials. There are some differences: these are actual, finite polynomials (as opposed to generating functions).

10.3.1 DEFINITION. The *weight enumerator* of a code C is

$$W_C(x,y) := \sum_{c\in C} x^{\mathrm{wt}(c)} y^{n-\mathrm{wt}(c)}.$$

Equivalently, if n_i denotes the number of codewords of weight i, then

$$W_C(x,y) = \sum_{i=0}^{n} n_i x^i y^{n-i}.$$

The weight enumerator carries a lot of information about the code (and arguably the key information), and it is invariant under permutations of the columns and scaling of the columns. For those, and many other, reasons coding theorists often use the weight enumerator in their studies of codes. A particularly important result is the following:

10.3.2 THEOREM (MacWilliams relations). *Let C be a q-ary, linear code. Then*

$$W_{C^\perp}(x,y) = q^{-k} W_C(y-x, y+(q-1)x).$$

While it is clear that the dual code is determined uniquely by the code itself, it is still surprising to see such a clean relationship between the two weight enumerators. We will see a proof of this equation in the next chapter, where it will be deduced as a special case of a much more general result.

10.3.1 Application: the nonexistence of certain projective planes

To see the power of the MacWilliams relations, let us look at an application. We will prove the following result, restricting the number of open cases in Problem 4.5.2:

10.3.3 THEOREM. *There exists no projective plane of order* $6 \pmod 8$.

Our proof follows a short paper by Assmus and Maher (1978). That paper also shows the nonexistence of certain so-called biplanes. Some terminology: a $t-(v,k,\lambda)$ design is *symmetric* if the number of blocks equals the number of points (i.e. equality holds in Fisher's Inequality). The *incidence matrix* of the design is a matrix A with rows indexed by blocks, columns by points, and

$$A_{ij} = \begin{cases} 1 & \text{if point } j \text{ is in block } i \\ 0 & \text{otherwise.} \end{cases}$$

Note that the incidence matrix of a symmetric design is *not necessarily symmetric!* The term "symmetric" only implies that the matrix is *square*.

By looking at AA^T we can deduce the following two lemmas:

10.3.4 LEMMA. *In a symmetric $2-(v,k,\lambda)$ design we have $b=v$ and $k=r$. Every two blocks intersect in precisely λ points. Also,*

$$k(k-1)=(v-1)\lambda.$$

10.3.5 LEMMA. *Let A be the incidence matrix of a symmetric $2-(v,k,\lambda)$ design. Then $\det(A)=k(k-\lambda)^{(v-1)/2}$.*

We will use the following linear algebra result, which is a special case of the *Smith Normal Form*:

10.3.6 THEOREM. *Let A be an $n\times n$ nonsingular matrix over $\mathbb{Z}$. There exist integer matrices M and N such that $\det(M)=\det(N)=1$ and $MAN=D$, where D is a diagonal matrix with diagonal entries $d_1,\ldots,d_n$ such that $d_i|d_{i+1}$ for all $i\in[n-1]$.*

Next, consider the matrix A_+, obtained from A by adding an all-ones column. We interpret A_+ as a matrix over GF(2).

10.3.7 LEMMA. *Let A be the incidence matrix of a symmetric $2-(v,k,\lambda)$ design, let A_+ be as above, and let C be the linear code generated by the rows of A. If k is odd, $k-\lambda$ is even, but $k-\lambda$ is not a multiple of 4, then C is a $(v+1,(v+1)/2,d)$ code for some d, such that $C=C^\perp$.*

Proof: Let M,N be as in Theorem 10.3.6. Then $d_1d_2\cdots d_n=\det(MAN)=\det(A)=k(k-\lambda)^{(v-1)/2}$. Note that k is odd, and each term $(k-\lambda)$ has exactly one factor 2. Hence no more than $(v-1)/2$ of the diagonal entries are divisible by 2, and $\dim(C)=\mathrm{rk}(A_+)\geq\mathrm{rk}_{\mathrm{GF}(2)}(A)\geq\mathrm{rk}_{\mathrm{GF}(2)}(MAN)\geq(v+1)/2$.

Next, let a and b be rows of A_+. Then $\langle a,a\rangle=k+\lambda\equiv 0 \pmod 2$. Also, $\langle a,b\rangle=\lambda+1\equiv 0 \pmod 2$. It follows that $C\subseteq C^\perp$. Since $\dim(C)+\dim(C^\perp)=v+1$, we have that $\dim(C)\leq(v+1)/2$. Hence equality must hold, and the result follows. ∎

Call a code *doubly even* if all weights are multiples of 4.

10.3.8 LEMMA. *If C is a binary, linear $[v+1,(v+1)/2,d]$ code that is doubly even, and $C^\perp=C$, then $8|(v+1)$.*

Proof: For a binary code, the MacWilliams relations specialize to

$$W_{C^\perp}(x,y)=2^{-k}W_C(y-x,y+x)=2^{n/2-k}W_C((x,y)\sigma),$$

where σ is the linear transformation

$$\frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}.$$

If C is self-dual, then then $W_C(x,y)$ is invariant under σ. If C is doubly even, then $W_C(x,y)$ is also invariant under

$$\pi = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix},$$

where $i \in \mathbb{C}$ is such that $i^2 = -1$. But now $W_C(x,y)$ must be invariant under the group generated by π and σ, and in particular under

$$(\pi\sigma)^3 = \frac{1+i}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

which multiplies each of x and y by a primitive eighth root of unity. The result follows.■

Proof of Theorem 10.3.3: Suppose a projective plane of order $q \equiv 6 \pmod 8$ exists. Consider the corresponding $2-(q^2+q+1, q+1, 1)$ design. Let A be its incidence matrix, and C the binary, linear code of A_+ as above. By Lemma 10.3.7, C is self-dual. Each row of C has $q+2$ nonzero entries, and in particular weight $0 \pmod 4$. By Lemma 10.3.8, then, $v+1 = q^2+q+2$ is divisible by 8, which contradicts that $q \equiv 6 \pmod 8$.■

The weight enumerator also played a crucial role in establishing the nonexistence of a projective plane of order 10, by reducing the number of cases to be checked by a computer to a manageable level. The most general result establishing nonexistence of projective planes is

10.3.9 THEOREM (Bruck-Ryser-Chowla). *If a projective plane of order q exists, and $q \equiv 1$ or $2 \pmod 4$, then q is the sum of two squares.*

10.4 Where to go from here?

The literature on coding theory is immense. Here are a few pointers.

- Lam (1991), *The Search for a Finite Projective Plane of Order 10* recounts the resolution of the existence of a projective plane of order 10 (spoiler: it doesn't exist). The MacWilliams relations play a key part, as does an extensive computer search.
- MacWilliams and Sloane (1977), *The Theory of Error-Correcting Codes* is a classical textbook on coding theory.
- Welsh (1988), *Codes and Cryptography* is more accessible.
- van Lint (1998), *Introduction to Coding Theory* is an excellent textbook too.

CHAPTER 11

Matroid theory

1935 was the year in which the word "matroid" was first printed. It was a time when building an axiomatic foundation of mathematics was a popular pursuit. Whitney (1935), in his paper *On the abstract properties of linear dependence*, attempts just that: try to capture linear independence using a few simple axioms. Whitney's axioms capture a much broader class of structures, though, with many interesting properties. Matroid theory was born. Today the subject thrives, having deep links to graph theory, coding theory, and finite geometry.

11.1 Matroids

Let us start with the definition.

11.1.1 DEFINITION. A *matroid* is a pair (E, r), where E is a finite set and $r : \mathscr{P}(E) \to \mathbb{Z}$ a function satisfying the following:

(*i*) (Monotonicity) For all $A \subseteq B \subseteq E$ then $r(A) \leq r(B)$.

(*ii*) (Submodularity) For all $A, B \subseteq E$,

$$r(A) + r(B) \geq r(A \cup B) + r(A \cap B). \tag{11.1}$$

(*iii*) (Unit increase) For all $A \subseteq E$, $0 \leq r(A) \leq |A|$.

Any function satisfying (*i*) — (*iii*) is called a *rank function*. Let us look at two examples. In fact, these examples are what motivated Whitney to write his paper.

11.1.2 EXAMPLE. Let E be a finite set of vectors in a vector space V. Let $r(A) := \dim(\text{span}(A))$ for each $A \subseteq E$. Then (E, r) is a matroid.

Proof: It is easy to verify (*i*) and (*iii*). For submodularity, we use the following relation for subspaces U, W of a vector space V:

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W).$$

Taking $U := \text{span}(A)$ and $W := \text{span}(B)$, we see that $U + W = \text{span}(A \cup B)$. However, although $A \cap B \subseteq U \cap W$, the dimension of $\text{span}(A \cap B)$ can be strictly smaller than $\dim(U \cap W)$. In fact, the intersection of the subspaces can be large while the finite sets A and B are disjoint! Still, this suffices to conclude submodularity. ∎

11.1.3 EXAMPLE. Let $G = (V, E)$ be a graph. For an edge subset $A \subseteq E$, let $c(A)$ be the number of components of the subgraph (V, A). Define $r(A) := c(A)$. Then (E, r) is a matroid, called the *cycle matroid* of G.

Proof: This result is easiest proven through a detour. Consider the $V \times E$ incidence matrix A of G (as we did in Lemma 5.6.3). Let r_1 be the rank function of the previous example, where E is now the set of columns of A. We will show that $r_1 = r$.

Consider a set $A \subseteq E$. Let F be a maximal spanning forest contained in A. Each edge connects two components, so $c(F) = |V| - |F|$. By Lemma 5.6.4, the vectors corresponding to F are linearly independent, so $r_1(F) = |F| = |V| - (|V| - |F|) = r(F)$.

Next, we add the remaining edges from A one by one. Each $e \in A$ closes a cycle when added to F (by maximality of $|F|$), so each e is linearly dependent on F (again by Lemma 5.6.4), so $r_1(A) = r_1(F)$ and $r(A) = r(F)$, completing the proof. ∎

Some more terminology:

11.1.4 DEFINITION. Let $M = (E, r)$ be a matroid. A set $A \subseteq E$ is *independent* if $r(A) = |A|$. A set $A \subseteq E$ is *spanning* if $r(A) = r(E)$.

A striking feature of matroids is that there are many different characterizations. They can be defined in terms of any of the following, and more besides. In each case there is a list of two to four simple axioms.

- Independent sets
- Inclusionwise maximal independent sets (called *bases*)
- Inclusionwise minimal dependent sets (called *circuits*)
- *Closures* (the closure of a set A is the inclusionwise maximal set B such that $A \subseteq B$ and $r(A) = r(B)$)
- *Hyperplanes* (closed sets of rank $r(E) - 1$).

The following lemmas can be proven without difficulty from the axioms:

11.1.5 LEMMA. *Let $M = (E, r)$ be a matroid. All maximal independent subsets of E have size $r(E)$.*

11.1.6 LEMMA. *Let $M = (E, r)$ be a matroid.* $\max\{|A| : A \text{ independent}\} = \min\{|A| : A \text{ spanning}\}$.

11.1.1 Duality

With each matroid we associated a new matroid, its *dual*, as follows.

11.1.7 DEFINITION. The *dual matroid* of $M = (E, r)$ is $M^* = (E, r^*)$, where

$$r^*(A) = |A| + r(E \setminus A) - r(E).$$

11.1.8 THEOREM. *M^* is a matroid.*

Proof: We have to show that r^* obeys the rank axioms. We denote $\overline{A} := E \setminus A$ and, for a function f, we write $\overline{f}(A) := f(\overline{A})$.

11.1.8.1 CLAIM. *If f is a submodular function, then so is $\overline{f}$.*

Proof:

$$\begin{aligned}\overline{f}(A)+\overline{f}(B) &= f(\overline{A})+f(\overline{B}) \geq f(\overline{A}\cap\overline{B})+f(\overline{A}\cup\overline{B}) \\ &= f(\overline{A\cup B})+f(\overline{A\cap B}) = \overline{f}(A\cup B)+\overline{f}(A\cap B).\end{aligned}$$ □

It is easy to check that $|\cdot|$ is a submodular function, as is the (constant) function $-r(E)$. Summing submodular functions gives a submodular function, so $|A|+\overline{r}(A)-r(E)$ is submodular.

Next, let $A\subseteq B\subseteq E$. Then

$$r(\overline{A}) = r(\overline{B}\cup(B\setminus A)) \leq r(\overline{B})+r(B\setminus A) \leq r(\overline{B})+|B\setminus A|,$$

where the inequality follows from submodularity, and the last equality from 11.1.1(*iii*). It follows that

$$\overline{r}(A)+|A| \leq \overline{r}(B)+|B\setminus A|+|A| = \overline{r}(B)+|B|,$$

and hence r^* satisfies monotonicity.

Finally, note that submodularity implies $r(E)\leq r(A)+r(\overline{A})$, so $0\leq r(E)-r(\overline{A})\leq r(A)\leq |A|$. Hence

$$r^*(A) = |A|-(r(E)-r(\overline{A}))$$

satisfies 11.1.1(*iii*) too. ■

It is easy to check the following properties:

11.1.9 THEOREM. *Let $M=(E,r)$ be a matroid. The following are true:*
(i) *B is a basis of M if and only if $E\setminus B$ is a basis of M^*.*
(ii) *$(M^*)^* = M$.*
(iii) *$r^*(E) = |E|-r(E)$.*

11.1.10 EXAMPLE. Let M be the cycle matroid of a graph G, which we assume to be connected. We wish to describe the dependent sets of M^*. Such an edge set F cannot be contained in the complement of any spanning tree, since the complement of a spanning tree is a basis of M^*. Hence F meets every spanning tree, i.e. F is an *edge cut*: $G\setminus F$ has more components than G. The minimal dependent sets of M^* are the minimal edge cuts. These are sometimes called *bonds*, and M^* is known as the *bond matroid* of G.

Note that there are deep connections with planar graph duality.

11.1.2 Minors

A key concept in matroid theory is that of a *minor*. The definition takes three steps:

11.1.11 DEFINITION. Let $M=(E,r)$ be a matroid and $e\in E$. We define $M\setminus e := (E\setminus\{e\}, r)$. We say $M\setminus e$ was obtained from M by *deleting* e.

11.1.12 DEFINITION. Let $M=(E,r)$ be a matroid and $e\in E$. We define $M/e := (E\setminus\{e\}, r')$, where

$$r'(A) := r(A\cup\{e\})-r(\{e\}).$$

We say M/e was obtained from M by *contracting* e.

11.1.13 DEFINITION. Let M be a matroid. We say N is a *minor* of M if N can be obtained by repeatedly deleting and/or contracting elements from M.

Matroid minors generalize graph minors. It is easy to see that deleting an element corresponds to deleting an edge. Contraction specializes to the following:

11.1.14 EXAMPLE. Let $G = (V, E, \iota)$ be a multigraph, and $e \in E$, not a loop, with endpoints u, v. The graph G/e is $(V', E \setminus \{e\}, \iota')$, where $V' := V \setminus \{u, v\} \cup \{uv\}$, and $\iota'(uv, f) = \min\{\iota(u, f) + \iota(v, f), 1\}$, and $\iota'(w, f) = \iota(w, f)$ for all $f \in E \setminus \{e\}$ and $w \in V' \setminus \{uv\}$. In words: we delete e and identify the endpoints. See Figure 11.1.

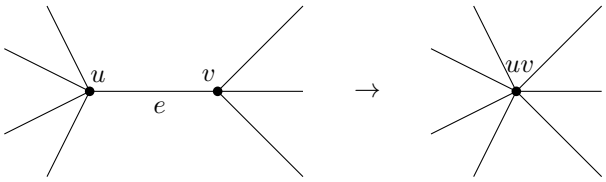


FIGURE 11.1
Contraction of an edge

We skip the proof of the following:

11.1.15 LEMMA. *If M is the cycle matroid of G, and e is a non-loop edge of G, then M/e is the cycle matroid of G/e.*

11.2 The Tutte polynomial

Before presenting the main theory of this section, let us consider a few examples. The main theme will be *deletion-contraction formulas*. Our first example is our favorite pastime: counting trees.

11.2.1 PROPOSITION. *Let $G = (V, E, \varphi)$ be a connected graph, and let $\tau(G)$ denote the number of spanning trees of G. If $e \in E$ then*

$$\tau(G) = \begin{cases} \tau(G \setminus e) & \text{if } e \text{ is a loop} \\ \tau(G/e) & \text{if } e \text{ is a cut-edge} \\ \tau(G \setminus e) + \tau(G/e) & \text{otherwise.} \end{cases}$$

Proof: We observe that $\tau(G)$ is the number of trees using edge e plus the number of trees not using e. It is easily checked that each tree of G/e corresponds to exactly one tree of G using e. Hence, if e is not a loop, then $\tau(G/e)$ is the number of spanning trees using e. The result now follows easily. ∎

Next up, colorings.

11.2.2 DEFINITION. The *chromatic polynomial* $P(G, t)$ is the number of proper colorings of G with t colors.

For instance, $P((V,\emptyset),t) = t^{|V|}$, and $P(K_n,t) = t(t-1)\cdots(t-n+1)$. We call $P(G,t)$ a polynomial, but is it always?

11.2.3 PROPOSITION. *$P(G,t)$ is indeed a polynomial in t.*

Proof: We will show that $P(G,t)$ satisfies the following recursion. Let $e \in E(G)$.

$$P(G,t) = \begin{cases} 0 & \text{if } G \text{ contains a loop} \\ P(G\backslash e,t) - P(G/e,t) & \text{otherwise.} \end{cases}$$

From this it is clear that $P(G,t)$ is a polynomial.

Clearly if G has a loop, then any coloring will have an edge whose endpoints receive the same color. Otherwise, consider the proper colorings of $G\backslash e$. Those come in two types: ones where the endpoints of e receive different colors (those correspond to proper colorings of G) and ones where the endpoints of e receive the same color (those do *not* correspond to proper colorings of G). But the latter are in a 1-to-1 correspondence with colorings of G/e. ∎

Our third example concerns connectivity when edges may randomly disappear:

11.2.4 DEFINITION. The *reliability polynomial* $C(G,p)$ is the probability that, if each edge is independently deleted with probability p, then the remaining graph has the same number of components as G.

11.2.5 THEOREM. *$C(G,p)$ is a polynomial in p.*

Proof: Again we prove a recursion. Let $e \in E(G)$.

$$C(G,p) = \begin{cases} C(G\backslash e,p) & \text{if } e \text{ is a loop} \\ (1-p)C(G/e,p) & \text{if } e \text{ is a cut-edge} \\ pC(G\backslash e,p) + (1-p)C(G/e,p) & \text{otherwise.} \end{cases}$$

The loop case is clear; the rest is easily deduced by using conditional probability:

$$\begin{aligned} \Pr(G \text{ survives}) = \Pr(e \text{ survives})\Pr(G \text{ survives}|e \text{ survives}) + \\ \Pr(e \text{ dies})\Pr(G \text{ survives}|e \text{ dies}). \end{aligned}$$

∎

All examples have a similar recurrence relation, because all examples above are evaluations of a more generic polynomial, the *rank polynomial*. We define it for matroids:

11.2.6 DEFINITION. Let $M = (E,r)$ be a matroid, and let r^* denote the rank function of M^*. The *rank polynomial* of M is

$$R(M;x,y) := \sum_{A\subseteq E} x^{r(E)-r(A)} y^{r^*(E)-r^*(E\backslash A)}.$$

The following facts are easily checked:

11.2.7 LEMMA.

$$R(M;x,y) = R(M^*;y,x), \tag{11.2}$$

$$R(M;x,y) = \sum_{A\subseteq E} x^{r(E)-r(A)} y^{|A|-r(A)}, \tag{11.3}$$

$$R(M;x,y) = \sum_{A\subseteq E} x^{|E\setminus A|-r^*(E\setminus A)} y^{r^*(E)-r^*(E\setminus A)}. \tag{11.4}$$

Equation (11.3) shows that $R(M;x,y)$ is something like a generating function for the number of sets of size i and rank j, but with remapped exponents. The rank polynomial satisfies a recurrence relation:

11.2.8 THEOREM. *Let $M=(E,r)$ be a matroid, and let $e\in E$. Then*

$$R(M;x,y) = \begin{cases} (1+y)R(M\setminus e;x,y) & \text{if } r(e)=0 \\ (1+x)R(M/e;x,y) & \text{if } r^*(e)=0 \\ R(M\setminus e;x,y)+R(M/e;x,y) & \text{otherwise.} \end{cases}$$

Proof: We split the sum up into the terms containing e and the terms not containing e. If $r(e)=0$ (the technical term is "e is a loop"), then $r(A\cup\{e\})=r(A)$ for all sets A. Looking at (11.3), the only effect of adding e to a set is to increase $|A|$, and therefore an extra factor y is obtained. The first case follows.

The second case follows by duality, using (11.2) and the first case.

For the third case, it is an easy exercise in using the rank axioms to conclude that $r(E\setminus\{e\})=r(E)$ (and hence $r^*(E\setminus\{e\})=r^*(E)$). The sets not containing e contribute the following to the sum:

$$\sum_{A\subseteq E\setminus\{e\}} x^{r(E)-r(A)} y^{|A|-r(A)} = R(M\setminus e;x,y).$$

The sets containing e contribute the following to the sum, using (11.4) and (11.2):

$$\sum_{A\subseteq E:e\in A} x^{|E\setminus A|-r^*(E\setminus A)} y^{r^*(E)-r^*(E\setminus A)} = R(M^*\setminus e;y,x) = R(M/e;x,y).$$

The result follows. ∎

Our main result in this section is the following:

11.2.9 THEOREM. *For each matroid $M=(E,r)$, and each $e\in E$, let $f(M;x,y)$ be given by*

$$f(M;x,y) = \begin{cases} a(1+y)f(M\setminus e;x,y) & \text{if } r(e)=0 \\ b(1+x)f(M/e;x,y) & \text{if } r^*(e)=0 \\ af(M\setminus e;x,y)+bf(M/e;x,y) & \text{otherwise.} \end{cases}$$

If, moreover, $f(\emptyset;x,y)=1$, then

$$f(M;x,y) = a^{|E|-r(E)} b^{r(E)} R(M;x,y).$$

We will omit the proof, which is a not too difficult exercise in bookkeeping.

11.2.10 PROPOSITION. *Let $G = (V, E, \iota)$ be a graph with n vertices, m edges, and c components, and let M be the corresponding cycle matroid. Then the following hold:*

$$\begin{aligned} \tau(G) &= R(M;0,0) && \text{(provided } G \text{ is connected)};\\ P(G,t) &= (-1)^{n-c}t^c R(M;-t,-1);\\ C(G,p) &= (1-p)^{n-c}p^{m-n+c}R\left(M;0,\frac{1-p}{p}\right). \end{aligned}$$

Sketch of proof: The first equation is a simple substitution, coupled with the observation that bases correspond to sets with $|A| = r(A) = r(E)$. Hence the contribution of a basis is $0^0 0^0 = 1$, whereas the contribution of any other set is 0.

For the second, apply Theorem 11.2.9 to $t^{-c}P(G,t)$. We need to figure out the relation in case e is a cut-edge. Consider a partition (H_1, H_2) of $V(G)$ such that e is the only edge having one end u in H_1 and one end v in H_2. Let c_i be the number of colorings of H_1 with t colors, such that u has color i, and let c'_i be the corresponding number for H_2. Since there is symmetry between the colors, we have $c_i = c$ and $c'_i = c'$ for some c, c' and for all $i \in [t]$. Now

$$\begin{aligned} P(G\backslash e, t) &= \prod_{i,j\in[t]} c_i c'_j = t^2 cc'\\ P(G/e, t) &= \prod_{i\in[t]} c_i c'_i = tcc'. \end{aligned}$$

Hence $P(G\backslash e, t) = tP(G/e, t)$. Now if we plug $t^{-c}P(G,t)$ into Theorem 11.2.9, we find

$$\begin{aligned} a(1+y) &= 0\\ b(1+x) &= t-1\\ a &= 1\\ b &= -1, \end{aligned}$$

from which the result follows.

The third equation is proven similarly, and left as an exercise. ∎

The rank polynomial has many other connections, such as the Ising and Potts models in statistical mechanics, the Jones polynomial in knot theory, and, indeed, the weight enumerator we saw in the last chapter.

One question remains: what is the Tutte polynomial from the section title?

11.2.11 DEFINITION. The *Tutte polynomial* of a matroid is

$$T(M;x,y) := R(M;x-1,y-1).$$

Tutte defined his polynomial in a different way, and it took a number of years before people realized that it was so closely related to the rank polynomial.

11.2.1 Proof of the MacWilliams Relations

All proofs in this section are left as exercises.

Let C be a q-ary linear $[n,k,d]$ code with generator matrix G. Let M be the vector matroid (cf. Example 11.1.2) whose elements are the columns of G. Note that M does not change when we do row operations on G. Therefore M depends only on the code C, and we can write $M = M(C)$. The next result shows that linear code duality is a special case of matroid duality:

11.2.12 THEOREM. $M(C)^* = M(C^\perp)$.

Deletion and contraction can be defined for codes too:

11.2.13 DEFINITION. We say the *punctured code* at coordinate i, denoted $C\backslash i$, is the code obtained from C by removing the ith coordinate from each word.

11.2.14 THEOREM. $M(C\backslash i) = M(C)\backslash i$.

11.2.15 DEFINITION. We say the *shortened code* at coordinate i, denoted C/i, is the code obtained from C by restricting the code to those words having a 0 in the ith coordinate, and then removing the ith coordinate from each remaining word.

11.2.16 THEOREM. $M(C/i) = M(C)/i$.

Now to prove the MacWilliams relations, we need to show that the weight enumerator $W_C(x,y)$ is determined by the rank polynomial $R(M(C);x',y')$ and use $R(M^*;y',x') = R(M;x',y')$.

11.3 Where to go from here?

We have seen only one aspect of matroids. The following books have more:

- Oxley (2011), *Matroid Theory*, is the standard textbook. It is thorough but accessible with many examples and many exercises. However, this chapter is instead based on the treatment from
- Godsil and Royle (2001), *Algebraic Graph Theory*, since the book by Oxley does not discuss the Tutte polynomial.
- Welsh (1976), *Matroid Theory*, was the first textbook on matroid theory. It is available as a low-cost reprint, and valuable since it contains a number of results that Oxley omitted from his text.

APPENDIX A

Graph theory

Graph theory is a cornerstone of combinatorics. Not only are there an abundance of beautiful results and intriguing open problems, but there are also countless practical applications. While these lecture notes do not center on graph theory, still many results and examples involve graphs. This appendix gives an overview of the basic concepts. Many results are stated as problems. The proofs are typically not difficult, and can be useful exercises. The content of this appendix is, in part, inspired by Schrijver (ca. 2000).

A.1 Graphs and multigraphs

In these lecture notes we will use the following definition:

A.1.1 DEFINITION. A *graph* G is a pair (V, E), where V is a finite set, and E is a collection of size-2 subsets of V.

The members of V are called *vertices*, the members of E *edges*. If $e = \{u, v\}$ is an edge, then u and v are the *endpoints*. We say u and v are *adjacent*, and that u and v are *incident* with e. One can think of a graph as a network with set of nodes V. The edges then denote which nodes are *connected*. Graphs are often visualized by drawing the vertices as points in the plane, and the edges as lines connecting two points.

A.1.2 PROBLEM. Determine the number of graphs with $V = [n]$.

A.1.3 DEFINITION. The *degree* of a vertex v, denoted $\deg(v)$, is the number of edges having v as endpoint. A vertex of degree 0 is called *isolated*.

A.1.4 PROBLEM. Prove that every graph has an even number of odd-degree vertices.

A.1.5 DEFINITION. A graph is *k-regular* if all vertices have degree k, and *regular* if it is k-regular for some k. A 3-regular graph is sometimes called *cubic*.

A.1.6 PROBLEM. How many edges does a k-regular graph on n vertices have?

A.1.7 PROBLEM. Determine the number of cubic graphs with $V = [6]$.

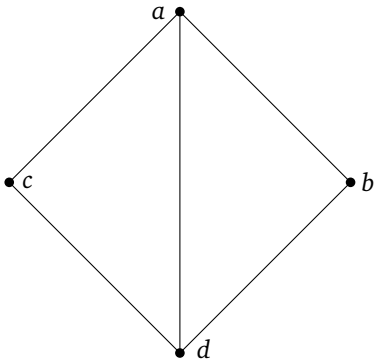


FIGURE A.1
The graph $G = (V, E)$, where $V = \{a, b, c, d\}$, and $E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, d\}, \{c, d\}\}$.

A.1.8 DEFINITION. A *complete graph* on n vertices is a graph with $|V| = n$, such that all pairs of vertices are connected. We denote this graph by K_n (leaving the set V implicit).

A.1.9 PROBLEM. Show that G is a complete graph if and only if G is $(n-1)$-regular.

A.1.10 DEFINITION. A graph $G = (V, E)$ is *bipartite* if V can be partitioned into disjoint sets U, W such that, for each $e \in E$ we have $e = \{u, w\}$ for some $u \in U$, $w \in W$. The sets U, W are sometimes called the *color classes*.

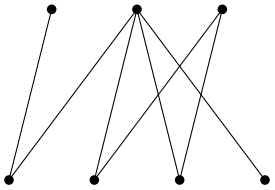


FIGURE A.2
A bipartite graph with $|U| = 3$ and $|W| = 4$.

A.1.11 DEFINITION. A *complete bipartite graph* $K_{m,n}$ is a bipartite graph with color classes U and W, where $|U| = m, |W| = n$, and with edge set $E = \{\{u, w\} : u \in U, w \in W\}$.

A.1.12 PROBLEM.
(*i*) How many edges does $K_{m,n}$ have?
(*ii*) For which values of m, n is $K_{m,n}$ regular?
(*iii*) How many bipartite graphs are there with $V = [n]$?

Sometimes we need a more general structure than Definition A.1.1.

A.1.13 DEFINITION. A *multigraph* is a triple (V, E, ι), where V and E are finite sets, and $\iota : V \times E \to \{0, 1\}$ a function such that, for each $e \in E$, we have $\iota(v, e) = 1$ for either one or two members $v \in V$.

The advantage of multigraphs is that they can contain *loops* (edges whose endpoints are identical) and *multiple edges* (two or more edges sharing the same endpoints). Figure A.3 shows the multigraph in which $\iota(v,e)$ is given by the (v,e) entry of the following matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array} \tag{A.1}$$

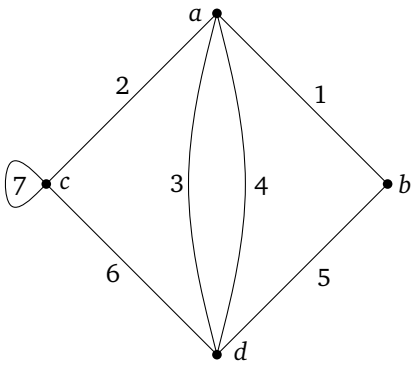


FIGURE A.3
The multigraph $G = (V, E, \iota)$ with $V = \{a, b, c, d\}$, $E = \{1, 2, 3, 4, 5\}$, and ι as defined by matrix (A.1)

Multiple edges are also referred to as parallel edges. Two loops can be in parallel too. A loop contributes 2 to the degree of a vertex.

Note. Many authors refer to an object as defined in Definition A.1.13 as a *graph*. An object as in Definition A.1.1 is then called a *simple graph*.

A.2 Complement, subgraphs, *morphisms

A.2.1 DEFINITION. Let $G = (V, E)$ be a graph, and let $K = (V, F)$ be the complete graph on vertex set V. Then the *complement* of G is the graph $\overline{G} := (V, F \setminus E)$.

We will see the complement again when we discuss coloring.

A.2.2 DEFINITION. Let $G = (V, E)$ be a graph. A graph $G' = (V', E')$ is a *subgraph* of G if $V' \subseteq V$ and $E' \subseteq E$. We say G' is an *induced* subgraph if, whenever $u, v \in V'$ and $\{u, v\} \in E$, then $\{u, v\} \in E'$.

Typically, homomorphisms are maps that preserve a certain property. Graph homomorphisms preserve connectivity between vertices:

A.2.3 DEFINITION. Let $G = (V, E)$ and $H = (W, F)$ be graphs. A *graph homomorphism* is a map $\varphi : V \to W$ such that, for all $\{u, v\} \in E$, we have $\{\varphi(u), \varphi(v) \in F\}$.

A.2.4 DEFINITION. A graph homomorphism φ is an *isomorphism* if it is a bijection between the two vertex sets, and its inverse is also a homomorphism. An *automorphism* is an isomorphism between G and itself.

A.2.5 PROBLEM. Determine the automorphism groups of the following graphs:

(*i*) The graph in Figure A.1

(*ii*) The unique cubic graph on 10 vertices, such that every two nonadjacent vertices have a common neighbor.
Hint: This graph is usually called the *Petersen graph*. Determining its automorphism group is somewhat tedious. Use of a computer could help.

Note that vertices of graphs *always* have labels, even if these are omitted in a drawing. If we are interested in structures within the graph irrespective of labels, we can say that we want them "up to isomorphism" or "up to relabeling".

A.3 Walks, paths, cycles

A.3.1 DEFINITION. Let $G = (V, E, \iota)$ be a multigraph. A *walk* is a sequence $(v_0, e_0, v_1, e_1, \ldots, v_{n-1}, e_{n-1}, v_n)$, where $v_0, \ldots, v_n \in V$, and $e_0, \ldots, e_{n-1} \in E$, and e_i has endpoints v_i, v_{i+1} for $i = 0, \ldots, n-1$.

The *length* of a walk is the number of edges in it.

A.3.2 DEFINITION. Let $G = (V, E, \iota)$ be a multigraph, and $W = (v_0, e_0, \ldots, e_{n-1}, v_n)$ a walk of G. We say that

(*i*) W is a *path* if no vertex occurs twice;

(*ii*) W is a *closed walk* if $v_0 = v_n$;

(*iii*) W is a *cycle* if $v_0 = v_n$, and no other vertex occurs twice.

A.3.3 PROBLEM. How many paths are there in the complete graph on 4 vertices? How many cycles? How many of each up to isomorphism?

We will often be imprecise and refer to either the sequence $(e_0, \ldots, e_{n-1})$ or the sequence $(v_0, \ldots, v_n)$ as the walk. For (simple) graphs, no information is lost.

A.3.4 PROBLEM. Show that, if there is a walk from v_0 to v_n, then there is also a path from v_0 to v_n.

A.3.5 PROBLEM. (*i*) Show that, if each vertex in a graph has degree at least k, then the graph contains a path of length k.

(*ii*) Show that, if each vertex in a nonempty graph has degree at least 2, then the graph contains a cycle.

A cycle of length 3 is often called a *triangle*.

A.4 Connectivity, components

A.4.1 DEFINITION. We say two vertices u, v are *connected* if there exists a walk starting in u and ending in v. The length of a shortest such walk is the *distance* between u and v.

A.4.2 DEFINITION. A graph is *connected* if every two vertices are connected.

A.4.3 PROBLEM.

(*i*) Show that, for each n, there exists a connected n-vertex graph with $n-1$ edges.
(*ii*) Show that each connected, n-vertex graph has at least $n-1$ edges.
(*iii*) Show that, for each n, there exists a disconnected, n-vertex graph having $\frac{1}{2}(n-1)(n-2)$ edges.
(*iv*) Show that every disconnected, n-vertex graph has at most $\frac{1}{2}(n-1)(n-2)$ edges.

A.4.4 DEFINITION. A *component* of G is an inclusionwise maximal connected subgraph. That is: if G' is connected, and G' is a subgraph of a connected graph G'', then $G' = G''$.

A.4.5 PROBLEM. Prove the following:

(*i*) If $C_1 = (V_1, E_1)$ and $C_2 = (V_2, E_2)$ are distinct components of a graph, then $V_1 \cap V_2 = \emptyset$.
(*ii*) Each vertex is contained in exactly one component.
(*iii*) Vertices u and v belong to the same component of G if and only if there is a path from u to v.
(*iv*) $G = (V, E)$ has at least $|V| - |E|$ components.
(*v*) If G has exactly two vertices of odd degree, then there is a path between them.

A.4.6 DEFINITION. An *Euler-tour* is a closed walk that uses each edge exactly once. A graph is *Eulerian* if it has an Euler-tour.

The following is, perhaps, the oldest result in graph theory:

A.4.7 THEOREM (Euler, 1736). *A graph $G = (V, E)$ without isolated vertices is Eulerian if and only if it is connected and all degrees are even.*

Proof: First, assume G is an Eulerian graph, with Euler tour $(v_0, e_0, \ldots, e_{n-1}, v_n)$. Pick vertices u and w. Let i be the first index such that $v_i \in \{u, w\}$, and let $j > i$ be such that $v_j \in \{u, w\} \setminus \{v_i\}$. Then $(v_i, e_i, \ldots, v_{j-1}, e_j, v_j)$ is a path from u to w. It follows that G is connected. Pick a vertex v. Let $i_1, \ldots, i_k$ be the indices such that $v_{i_j} = v$ for all $j \in [k]$. First suppose $i_1 > 0$. Then $i_k < n$, since $v_0 = v_n$ (the tour is closed). Since each edge occurs exactly once in the tour, the edges $e_{i_1-1}, \ldots, e_{i_k+1}$ are distinct (since G is simple, by assumption), and these are all edges incident with v. It follows that $\deg(v) = 2k$. If $i_1 = 0$ then a similar argument shows $\deg(v) = 2k - 2$.

Suppose the converse does not hold. Let G be a connected graph without isolated vertices, with all degrees even, but with no Euler-tour. Suppose that, among all such graphs, G was chosen to have as few edges as possible. Let $W = (v_0, e_0, \ldots, e_{n-1}, v_n)$ be a closed walk of maximum length that uses each edge at most once, and let H be the graph obtained from G by removing the edges of W. Since W meets each vertex in an even number of edges, H has all degrees even. This graph may have isolated vertices,

but since W does not cover all edges of G, at least one component C of H contains an edge. Pick C such that C has at least one vertex in common with W (*Exercise:* Why does such C exist?) Every degree of C is even, and C is connected, so by induction C has an Euler tour $(w_0, f_0, \ldots, f_{k-1}, w_k)$. We can let the tours start in such a way that $v_n = w_0$. But then $(v_0, e_0, \ldots, e_{n-1}, v_n, f_0, w_1, \ldots, f_{k-1}, w_k)$ is another closed walk without repeated edges, and this tour is longer than W, a contradiction our choice of W as a maximum-length walk. ∎

A.5 Forests, trees

A.5.1 DEFINITION. A *forest* is a graph without cycles. A *tree* is a connected forest.

A.5.2 PROBLEM. Prove the following:

(*i*) Between every two vertices of a tree there is exactly one path.
(*ii*) Every tree with at least two vertices, has at least two vertices of degree 1.
(*iii*) Every tree with a vertex of degree k, has at least k vertices of degree 1.
(*iv*) Every tree with exactly 2 vertices of degree 1, is a path.
(*v*) Every tree with n vertices has exactly $n-1$ edges.
(*vi*) Every forest with k components has exactly $n-k$ edges.

A.5.3 DEFINITION. Let $G = (V, E)$ be a connected graph. A subgraph $T = (V, F)$ is a *spanning tree* if T is a connected graph and a tree.

A.5.4 PROBLEM. Let T_1 and T_2 be distinct spanning trees of the connected graph G. Show that, for every edge $e \in E(T_1) \setminus E(T_2)$, there is an edge $f \in E(T_2) \setminus E(T_1)$ such that the subgraph obtained from T_2 by adding e and removing f is again a spanning tree.

A.6 Matchings, stable sets, colorings

Below, we say that an edge *covers* a vertex v if one of its ends equals v. Conversely, a vertex v *covers* an edge if it covers one of the ends of that edge.

A.6.1 DEFINITION. Let $G = (V, E)$ be a graph.

(*i*) A *vertex cover* is a subset $U \subseteq V$ such that each edge is covered by at least one vertex of U. The minimum size of a vertex cover is denoted by $\tau(G)$.
(*ii*) An *edge cover* is a subset $F \subseteq E$ such that each vertex is covered by at least one edge of F. The minimum size of an edge cover is denoted by $\rho(G)$.

A.6.2 DEFINITION. Let $G = (V, E)$ be a graph.

(*i*) A *matching* is a subset $M \subseteq E$ such that no vertex is incident with more than one edge in M. A matching is *perfect* if it covers all vertices. The maximum size of a matching is denoted by $\nu(G)$.
(*ii*) A *stable set* (sometimes called *independent set*) is a subset $U \subseteq V$ such that no edge has both ends in U. The maximum size of a stable set is denoted by $\alpha(G)$.

A.6.3 PROBLEM. Show that $\alpha(G) \leq \rho(G)$ and $\nu(G) \leq \tau(G)$.

The following result is harder to prove:

A.6.4 THEOREM (Gallai's Theorem). *Let $G = (V, E)$ be a graph without isolated vertices. Then*

$$\alpha(G) + \tau(G) = |V| = \nu(G) + \rho(G).$$

A.6.5 DEFINITION. A (vertex) *coloring* of $G = (V, E)$ with k colors is a map $c : V \to [k]$. A coloring is *proper* if, for each $e \in E$, $e = \{u, v\}$, we have $c(u) \neq c(v)$. The least k for which G has a proper k-coloring is denoted by $\chi(G)$, the *chromatic number* of G.

Note that we may assume implicitly that a coloring is proper.

A.6.6 PROBLEM. Let $\Delta(G)$ denote the maximum degree of G. Show that $\chi(G) \leq \Delta(G) + 1$.

A.6.7 PROBLEM. Show that $\chi(G) \geq \alpha(\overline{G})$, where $\overline{G}$ denotes the complement of G.

A.6.8 PROBLEM. What is the connection between proper k-colorings of G and homomorphisms $G \to K_k$?

We can also color edges:

A.6.9 DEFINITION. An *edge-coloring* of $G = (V, E)$ with k colors is a map $c : E \to [k]$. An edge-coloring is *proper* if, for each $v \in V$, and for every pair e, f of edges incident with v, $c(e) \neq c(f)$.

The *edge coloring number* $\chi'(G)$ is defined analogously to $\chi(G)$.

A.6.10 PROBLEM. Let $G = (V, E)$ be a graph with maximum degree $\Delta(G)$. Show that $\chi'(G) \geq \Delta(G)$.

The following is harder to prove, and possibly the hardest theorem quoted in this section:

A.6.11 THEOREM (Vizing's Theorem). *Every graph has an edge coloring with at most $\Delta(G) + 1$ colors.*

A.7 Planar graphs, minors

A.7.1 DEFINITION. A graph is *planar* if it can be drawn in the plane so that no two edges cross (and they can meet only in their endpoints).

There is a rich theory of planar graphs, which is beyond the scope of these notes.

A.7.2 DEFINITION. Let $G = (V, E, \iota)$ be a multigraph, and let $e \in E$ be an edge of G with endpoints u, v. We say that H is obtained from G by *contracting* edge e if $H = (V', E', \iota')$

with $V' = (V \setminus \{u,v\}) \cup \{uv\}$, $E' = E \setminus \{e\}$, and

$$\iota'(x,f) = \begin{cases} 1 & \text{if } x = uv \text{ and } \iota(u,f) = 1 \text{ or } \iota(v,f) = 1 \\ 0 & \text{if } x = uv \text{ and } \iota(u,f) = \iota(v,f) = 0 \\ \iota(x,f) & \text{otherwise.} \end{cases}$$

This is denoted by $H = G/e$.

In other words, we delete the edge e and *identify its endpoints*. Deleting an edge is denoted by $H = G \setminus e$.

A.7.3 DEFINITION. A graph H is a *minor* of G if H can be obtained from G by a series of edge deletions, edge contractions, and deletions of isolated vertices.

A.7.4 PROBLEM. Show that, if G is a planar multigraph, and H is a minor of G, then H is a planar graph.

A.7.5 PROBLEM (Euler's Formula.). Consider a drawing of a planar (multi)graph. We call such a drawing a *plane embedding*. If we remove this plane embedding from the plane, the plane is cut up into a number of connected parts, called *faces*.

Let $G = (V,E)$ be a planar graph, and let F be the set of faces of a fixed embedding of G. Show that

$$|V| - |E| + |F| = 2.$$

A.7.6 PROBLEM. Show that, if G is a simple planar graph with at least one cycle, then $|E| \leq 3|V| - 6$. Conclude that K_5 is not a planar graph.

The following is Wagner's reformulation of Kuratowski's Theorem, which characterizes planar graphs:

A.7.7 THEOREM (Kuratowski). *A multigraph G is planar if and only if it does not contain any of K_5 and $K_{3,3}$ as a minor.*

A.8 Directed graphs, hypergraphs

A.8.1 DEFINITION. A *directed graph* or *digraph* is a pair $D = (V,A)$, where V is a finite set, and $A \subseteq V \times V$ a set of ordered pairs of vertices, called the *arcs*. If (u,v) is an arc, then u is the *tail* and v is the *head*.

A directed graph is often represented by using arrows for the arcs, pointing from tail to head. A directed graph can have loops, and between each pair of vertices two arcs can be placed, one in each direction. See Figure A.4. One can define a directed multigraph analogously.

A.8.2 DEFINITION. A *tournament* is a digraph $D = (V,A)$ such that, for every pair u,v of vertices, exactly one of (u,v) and (v,u) is in A.

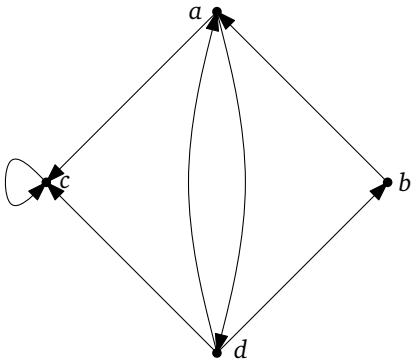


FIGURE A.4
A digraph $D = (V,A)$ *with* $V = \{a,b,c,d\}$ *and*
$A = \{(a,c),(a,d),(b,a),(c,c),(d,a),(d,b),(d,c)\}$

One can define *indegree* and *outdegree* in obvious ways, as well as *directed* walks, paths, and cycles.

A.8.3 DEFINITION. A *hypergraph* is a pair (V,E), with E a collection of subsets of V. A hypergraph is *k-uniform* if $|X| = k$ for all $X \in E$.

Bibliography

M. Aigner and G. M. Ziegler (2010). Proofs from The Book, 4th edition, Springer-Verlag. Cited on pp. 3, 10, and 68.

N. Alon and J. H. Spencer (2008). The probabilistic method, 3rd edition, John Wiley & Sons Inc. Cited on p. 83.

I. Anderson (1987). Combinatorics of finite sets, Oxford University Press; reprinted by Dover, New York. Cited on p. 51.

E. F. Assmus, Jr. and D. P. Maher (1978). Nonexistence proofs for projective designs, *Amer. Math. Monthly*, volume 85, no. 2, pp. 110–112. Cited on p. 125.

A. Blokhuis (1984). Few-distance sets, volume 7 of *CWI Tract*, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, ISBN 90-1636-273-0. Cited on p. 56.

B. Bollobás (1998). Modern graph theory, Springer-Verlag, New York. Cited on p. 98.

A. E. Brouwer, A. M. Cohen, and A. Neumaier (1989). Distance-regular graphs, Springer-Verlag, Berlin. Cited on p. 98.

A. E. Brouwer and W. H. Haemers (2012). Spectra of graphs, Universitext, Springer, New York, ISBN 978-1-4614-1938-9, doi:10.1007/978-1-4614-1939-6. Cited on pp. 85 and 98.

R. A. Brualdi (2011). The mutually beneficial relationship of graphs and matrices, volume 115 of *CBMS Regional Conference Series in Mathematics*, American Mathematical Society, Providence, RI, ISBN 978-0-8218-5315-3. Cited on p. 98.

P. J. Cameron (1994). Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press. Cited on pp. 1 and 3.

W. J. Cook, W. H. Cunningham, W. R. Pulleyblank, and A. Schrijver (1998). Combinatorial optimization, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Inc., New York, ISBN 0-471-55894-X. A Wiley-Interscience Publication. Cited on p. 69.

K. Engel (1997). Sperner theory, volume 65 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge. Cited on p. 51.

P. Flajolet and R. Sedgewick (2009). Analytic combinatorics, Cambridge University Press, Cambridge. Cited on p. 27.

A. M. H. Gerards (1989). A short proof of Tutte's characterization of totally unimodular matrices, *Linear Algebra Appl.*, volume 114/115, pp. 207–212, doi:10.1016/0024-3795(89)90461-8. Cited on p. 68.

C. Godsil and G. Royle (2001). Algebraic graph theory, Springer-Verlag, New York. Cited on pp. 98 and 136.

I. P. Goulden and D. M. Jackson (1983). Combinatorial enumeration, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, ISBN 0-471-86654-7. With a foreword by Gian-Carlo Rota, Wiley-Interscience Series in Discrete Mathematics. Cited on p. 27.

R. L. GRAHAM, B. L. ROTHSCHILD, and J. H. SPENCER (1990). Ramsey theory, 2nd edition, John Wiley & Sons Inc., New York. Cited on pp. 33 and 38.

S. JUKNA (2011). Extremal combinatorics, 2nd edition, Springer, ISBN 978-3-642-17363-9. With applications in computer science. Cited on pp. 3, 38, 51, 68, and 83.

C. LAM (1991). The search for a finite projective plane of order 10, *American Mathematical Monthly*, volume 4, pp. 305–318. Cited on p. 127.

J. H. VAN LINT (1998). Introduction to Coding Theory, 3rd edition, Springer, Berlin. Cited on p. 127.

J. H. VAN LINT and R. M. WILSON (2001). A course in combinatorics, 2nd edition, Cambridge University Press. Cited on p. 3.

L. LOVÁSZ (1993). Combinatorial problems and exercises, 2nd edition, North-Holland Publishing Co. Cited on p. 3.

A. LUBOTZKY (2012). Expander graphs in pure and applied mathematics, *Bull. Amer. Math. Soc. (N.S.)*, volume 49, no. 1, pp. 113–162, doi:10.1090/S0273-0979-2011-01359-3. Cited on p. 98.

E. LUCAS (1891). Théorie des Nombres, Gauthier-Villars et Fils, Paris. Cited on p. 23.

F. J. MACWILLIAMS and N. J. A. SLOANE (1977). The theory of error-correcting codes, North-Holland Publishing Co., Amsterdam. Cited on p. 127.

J. MATOUŠEK (2003). Using the Borsuk-Ulam Theorem, Springer. Lectures on Topological Methods in Combinatorics and Geometry. Cited on p. 106.

J. MATOUŠEK (2010). Thirty-three miniatures, volume 53 of *Student Mathematical Library*, American Mathematical Society, Providence, RI. Mathematical and algorithmic applications of linear algebra. Cited on p. 68.

J. OXLEY (2011). Matroid Theory, Second Edition, Oxford University Press. Cited on p. 136.

J. PITMAN (1999). Coalescent random forests, *J. Combin. Theory Ser. A*, volume 85, no. 2, pp. 165–193. Cited on p. 10.

C. POHOATA (2013). Around sperner's lemma, Fall Junior Paper, Princeton University.

A. SCHRIJVER (ca. 2000). Grafen: Kleuren en routeren. Lecture notes (in Dutch). Cited on p. 137.

S. SHELAH (1988). Primitive recursive bounds for van der Waerden numbers, *J. Amer. Math. Soc.*, volume 1, no. 3, pp. 683–697. Cited on p. 37.

R. P. STANLEY (1997). Enumerative combinatorics. Vol. 1, Cambridge University Press, Cambridge. Cited on p. 27.

T. TAO (2012). Lecture notes for 254b — expansion in groups. Online at http://terrytao.wordpress.com/2011/12/02/245b-notes-1-basic-theory-of-expander-graphs/. Cited on p. 98.

W. TUTTE (editor) (1969). Recent progress in combinatorics, Proceedings of the Third Waterloo Conference on Combinatorics, May 1968., Academic Press. Cited on p. 1.

D. WELSH (1976). Matroid Theory, Oxford University Press; reprinted by Dover, New York. Cited on p. 136.

D. WELSH (1988). Codes and Cryptography, Oxford University Press, Oxford. Cited on p. 127.

H. WHITNEY (1935). On the abstract properties of linear dependence, *Amer. J. Math.*, volume 57, no. 3, pp. 509–533. Cited on p. 129.

H. S. WILF (1994). generatingfunctionology, 2nd edition, Academic Press Inc., Boston, MA. Downloadable from http://www.math.upenn.edu/~wilf/DownldGF.html. Cited on p. 27.