Discrete Mathematics II

UP FAMNIT, Spring 2018–2019

These lecture notes are based on several sources [1–12].

1 Introduction

Historically (since Newton and Leibniz), almost the entire applied mathematics was based on **continuously varying** processes, motivated mostly by physics applications, and studied using analysis (differential calculus, integral calculus). With the growth of computers and other digital devices, **discrete mathematics** has become significantly more important. Discrete mathematics studies finite or countable discrete objects. It encompasses many areas of mathematics, including set theory, logic, combinatorics, graph theory, theoretical computer science, number theory, as well as (at least in part) algebra, operations research, game theory, probability, and statistics.

Besides computers, discrete mathematics finds many other **applications** in real life: arrangements of meetings, production and school teaching schedules, cryptography, design of codes, design of traffic, electrical, and communication networks, placing of people in jobs, design of voting schemes and auctions, design of experiments, applications in chemistry and biology (in particular in bioinformatics, in the study of the DNA sequences and phylogenetics), recreational mathematics (think, e.g., of the popular games such as Rubik's cube, Towers of Hanoi, Sudoku), etc.

In this course, we will study two important branches of discrete mathematics: **combinatorics** and **graph theory**. Two aspects that are generally important in mathematics will also play an important role in this course: **problem solving** and **proofs**.

1.1 What is Combinatorics?

Combinatorics is the art of arranging objects according to specified rules. If studies questions like: **Is a particular arrangement possible at all? If so, in how many different ways it can be done?** *If the rules are simple (like picking a football team from a class of schoolboys), the existence of an arrangement is clear, and we concentrate on the counting problem. But for more involved rules, it may not be clear whether the arrangement is possible at all. Examples are Euler's officers, described below.*

Sometimes an objective function might also be given, which measures how good an arrangement is. In that case, we are looking for **optimal solutions** with respect to the objective function (for example, find a schedule of a football tournament resulting in the least number of days of the tournament).

Sample problems

Derangements.

Given n letters and n addressed envelopes, in how many ways can the letters be placed in the envelopes so that no letter is in the correct envelope?

Discussion. The total number of ways of putting the letters in the envelopes is the number of *permutations* of n objects, which is $n!$. We will see that the fraction of these which are incorrectly addressed is very close to $1/e$, where $e = 2,71828\ldots$ is the base of natural logarithms—a surprising result at first sight. In fact, the exact number of ways of mis-addressing letters is the nearest integer to $n!/e$.

Exercise: For $n = 3, 4, 5$, calculate the number of ways of putting n letters in the envelopes so that every letter is incorrectly addressed. Calculate the ratio of this number to $n!$ in each case. ▲

Euler's officers.

Thirty-six officers are given, belonging to six regiments and holding six ranks (so that each combination of rank and regiment corresponds to just one officer). Can the officers be paraded in a 6×6 array so that, in any line (row or column) of the array, each regiment and each rank occurs precisely once?

Discussion. Euler posed this problem in 1782, he believed that the answer was 'no'. This was not proved until 1900, by Tarry. The problem can be generalized to n^2 officers, where the number of regiments, ranks, rows, and columns is n (we assume $n > 1$). There is no solution for $n = 2$. Euler knew solutions for all n not congruent to 2 modulo 4, and guessed that there was no solution for $n \equiv 2 \pmod 4$. However, he was wrong about that. Bose, Shrikhande, and Parker showed in 1960 that there is a solution for all n except $n = 2$ and $n = 6$.

Exercise: Solve Euler's problem for nine, sixteen, and twenty-five officers. Show that no solution is possible for four officers. ▲

A Ramsey game.

This two-player game requires a sheet of paper and pencils of two colors, say red and blue. Six points on the paper are chosen, with no three in a line. Now the players take a pencil each, and take turn drawing a line connecting two of the chosen points. The first player to complete a triangle of her own color loses. (Only triangles with vertices at the chosen points count.)

Can the game ever result in a draw?

Discussion. We'll see that a draw is not possible; one or other player will be forced to create a triangle. Ramsey proved a wide generalization of this fact. His theorem is sometimes stated in the form 'Complete disorder is impossible.'

Exercise: Test the assertion that the Ramsey game cannot end in a draw by playing it with a friend. Try to develop heuristic rules for successful play. ▲

1.2 Sets, Numbers, Functions, Relations, Revisited

In the course, we will assume knowledge of the following concepts as background knowledge:

Natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$, and their properties.
Every natural number has a successor.
The well-ordering principle (every nonempty set of natural numbers has the smallest element).

Principle of induction.
In its basic form: *"Let $P(n)$ be an assertion about the natural number n. Suppose that $P(1)$ is true. Suppose also that, if $P(n)$ is true, then $P(n+1)$ is also true. Then $P(n)$ is true for all natural numbers n."*

Example. Let f be a function satisfying $f(1) = 2$ and $f(n+1) = 2f(n)$. Then

$$f(2) = 4, f(3) = 8, \ldots, f(n) = 2^n\,.$$

The dots hide a proof by induction. (Do it!) ▲

Variations:

(1) Suppose that $P(n_0)$ holds and $P(n) \Rightarrow P(n+1)$. Then $P(n)$ holds for all $n \geq n_0$.

(2) "Principle of strong induction": Suppose that for all $n \in \mathbb{N}$, if $P(m)$ holds for all natural numbers m less than n, then $P(n)$ holds. Then $P(n)$ holds for all n.

(3) "Proof by Minimal Counterexample": Suppose that $P(n)$ is a proposition that does not hold for all natural n. Then there is a least natural number n for which $P(n)$ is false; in other words, $P(m)$ is true for all $m < n$ but $P(n)$ is false.

Sets. $x \in A$, $x \notin A$, $|A|$ = the number of elements in set A
the empty set – $\emptyset$, set operations: $A \cup B$, $A \cap B$, $A \setminus B$, binary relations on sets: $A \subseteq B$, $A = B$, the power set $\mathcal{P}(A)$: the set of all subsets of A.

$\{x : P\}$ – the set of all elements x having property P

Example. $\{n \in \mathbb{N} : (\exists k \in \mathbb{N})(k^2 = n)\}$. ▲

Extension of notation: $\{f(x) : P(x)\}$ where $f(x)$ is some function of x and P is a property of x that may either hold or not

Example. $\{p^2 : p \text{ is a prime number}\}$. ▲

$\{x, y\}$, (x, y) (ordered pair), $A \times B$ – Cartesian product of two sets, similarly for more factors; A^n = set of ordered n-tuples of elements of A

Functions. A function from A to B = a subset f of $A \times B$ such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$. If $(a, b) \in f$, we write $f(a) = b$.
Properties of functions: functions can be injective, surjective, bijective

If $A = \{a_1, \ldots, a_n\}$, then any function $f : A \to B$ can be specified by giving the n-tuple of values $(f(a_1), \ldots, f(a_n))$. Thus the number of functions from A to B is $|B|^{|A|}$. Motivated by this, the set of functions from A to B is sometimes written B^A, so that $|B^A| = |B|^{|A|}$.

Some useful functions:
factorial: $0! = 1$ and $n! = n \cdot (n-1)!$ for $n \in \mathbb{N}$
exponential and logarithm: $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \ldots$, for all $x \in \mathbb{R}$,
for $x > 0$, we have $\ln x = y$ if and only if $e^y = x$ (there is a unique such $y \in \mathbb{R}$),

Binary relations. Equivalence relation: transitive, reflexive, and symmetric binary relation. Equivalence classes. Partitions of a set.

2 Basic Combinatorial Principles

If we would like to count some objects with prescribed properties, this can be done in two steps: first we collect the objects of interest into a precisely described set, then we determine the cardinality of the set.

Definition. We say that a finite set X **contains** n **elements** if there exists a bijection from X into the set $\{1, 2, \ldots, n\}$. In this case, we write $|X| = n$ and say that the **cardinality** of set X is equal to n. In the special case of the empty set, we have $|\emptyset| = 0$.

In determining the cardinality of a given set, we often rely on a few simple principles.

The addition principle.

Theorem (The addition principle)**.** *If A and B are two finite disjoint sets, then*

$$|A \cup B| = |A| + |B|\,.$$

With the principle of mathematical induction the principle can be generalized to any number of sets:

If $A_1, \ldots, A_n$ are finite sets that are pairwise disjoint (i.e., $A_i \cap A_j = \emptyset$ whenever $i \neq j$), then the cardinality of their union is

$$|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n| = \sum_{i=1}^{n} |A_i|\,.$$

Example. *From city X to city Y one can travel by plane, by train, or by bus. There are 12 different flights from X to Y, 5 different trains, and 10 different buses. In how many different ways we can get from X to Y?*

We can only select one mode of transport and for every mode of transport we have a choice: $12 + 5 + 10 = 27$. ▲

Double counting (a.k.a. the Bookkeeper's Principle).

The following principle is deceptively simple yet enormously important:

Double Counting Principle: *If the same set is counted in two different ways, the answers are the same.*

This is analogous to finding the sum of all entries in a matrix by adding the row totals, and then checking the calculation by adding the column totals.

The principle has many applications. Here is one:

Lemma (Handshaking Lemma)**.** *At a convention, the number of delegates who shake hands an odd number of times is even.*

Proof. Let $D_1, \ldots, D_n$ be the delegates. We apply double counting to the set of ordered pairs (D_i, D_j) for which D_i and D_j shake hands with each other at the convention. Let x_i be the number of times that D_i shakes hands and y the total number of handshakes that occur. On the one hand, the number of pairs is $\sum_{i=1}^{n} x_i$ since for each D_i the number of choices of D_j is equal to x_i. On the other hand, each handshake gives rise to two pairs (D_i, D_j) and (D_j, D_i); so the total is $2y$. Thus $\sum_{i=1}^{n} x_i = 2y$. But, if the sum of n numbers is even, then evenly many of the numbers are odd. □

The principle is usually applied to counting ordered pairs. It can be formalized as follows:

Theorem. *Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ be sets and let $S \subseteq A \times B$. Suppose that, for $i = 1, \ldots, m$, the element a_i is the first component of x_i pairs in S, while, for $j = 1, \ldots, n$, the element b_j is the second component of y_j pairs in S. Then*

$$|S| = \sum_{i=1}^{m} x_i = \sum_{j=1}^{n} y_j \,.$$

Often it happens that x_i is constant (say x) and y_j is also constant (say y). Then we have $mx = ny$.

The multiplication principle.

A special case of the double counting principle is the multiplication principle, which says that the cardinality of the Cartesian product of two given sets equals the product of their cardinalities.

Theorem (The multiplication principle)**.** *If A and B are finite sets, then*

$$|A \times B| = |A| \cdot |B| \,.$$

Proof. Apply the previous theorem with A, B as in the theorem, $S = A \times B$, and $x_i = |B|$ for all $i = 1, \ldots, m$. Then $|S| = \sum_{i=1}^{m} x_i = |A| \cdot |B|$. □

With the principle of mathematical induction the principle can be generalized to any number of sets:

$$|A_1 \times \ldots \times A_n| = |A_1| \cdots |A_n| = \prod_{i=1}^{n} |A_i| \,.$$

Example. *How many 8-bit strings are there?*

8-bit strings are exactly the elements of the set $\{0,1\}^8$. Each of the eight bits may be selected in one of the two ways (0 or 1), from which, according to the multiplication principle, we infer that there are exactly $2^8 = 256$ strings of 8 bits. ▲

Example. *A restaurants serves three types of appetizers, six main courses, and five desserts. In how many ways can a three-course meal be chosen?*

A meal can be represented with an ordered triple, where the first component represents the appetizer, the second component the main course, and the third component the dessert. The meal can be chosen in $3 \times 6 \times 5 = 90$ ways. ▲

The equality principle.

It follows from the definition of the cardinality of a set that finite sets A and B have the same cardinality as soon as there exists a bijective mapping between them.

Theorem (The equality principle)**.** *If there exists a bijection between two finite sets A and B, then $|A| = |B|$.*

Example. *Let X be a set of n elements. How many subsets does the set X have?*

The problem asks about the cardinality of the power set $\mathcal{P}(X)$ of the set X. We will solve it by finding a bijection between the set $\mathcal{P}(X)$ and the set of all ordered n-tuples with elements from the set $\{0,1\}$. We denote the elements of X by $x_1, x_2, \ldots, x_n$. To an arbitrary subset $Y \in \mathcal{P}(X)$ we assign the **characteristic vector** $\chi(Y) = (y_1, \ldots, y_n) \in \{0,1\}^n$, defined by $y_i = 1$ if $x_i \in Y$ and $y_i = 0$, otherwise. In this way, we defined a mapping $\chi : \mathcal{P}(X) \to \{0,1\}^n$. It is not difficult to check that χ is bijective. Therefore, $|\mathcal{P}(X)| = |\{0,1\}^n| = 2^n$. In the latter equality we of course applied the multiplication principle. ▲

The pigeonhole principle (Dirichlet's principle).

Assume that a flock of pigeons flew in the pigeon house. The original version of Dirichlet's principle states the following: if there are more pigeons than pigeonholes, then some pigeonhole must contain two or more pigeons.

Theorem (Pigeonhole Principle)**.** *If $n+1$ or more objects are arranged in n boxes, then there is at least one box with at least two objects.*

Proof. By contradiction. Suppose that in each box there is at most one object. By the addition principle, the total number of objects is at most n, which is in contradiction with the assumption that there are at least $n+1$ objects. □

Examples. (i) *In each set of more than 12 people, there are two who have the birthday in the same month.*

(Boxes represent months.)

(ii) *In each set of more than* 366 *people, there are two who have the birthday on the same day.*

(Boxes represent days.)

(iii) *For every positive integer n there is a multiple of n that can be written only with digits* 0 *and* 1.

Let n be a positive integer. Consider the following sequence of n natural numbers:

$$1, 11, 111, \ldots, \underbrace{11\cdots1}_{n}\,.$$

If one of these n numbers is divisible by n, we are done. Otherwise, each of them gives one of $n-1$ possible remainders $1, 2, \ldots, n-1$. Since there are n numbers in the sequence and only $n-1$ remainders, the pigeonhole principle implies that two of the numbers in the sequence, say

$$\underbrace{11\cdots11}_{k} \quad \text{and} \quad \underbrace{11\cdots11}_{\ell}, \quad k < \ell\,,$$

give the same remainder when divided by n. But then their difference

$$\underbrace{11\cdots11}_{\ell-k}\underbrace{00\cdots00}_{k}$$

is divisible by n.

(iv) *In a group of two or more people there are always two with the same number of friends in this group. (It is assumed that the friendship relation is symmetric.)*

Suppose that the group consists of n people. Arrange people into rooms so that room i contains exactly those people who have exactly i friends. So we have n rooms marked with numbers $0, 1, \ldots, n-1$. At this moment we cannot use the pigeonhole principle since the number of rooms equals the number of people.

Notice that at least one of the rooms has to be empty. Indeed. Suppose that room $n-1$ is not empty. Then there is a person x who has $n-1$ friends. So each person is a friend with x, so there is no person who has 0 friends.

Therefore, the n people are arranged in $n-1$ rooms. By the pigeonhole principle, there are at least two people who are in the same room, that is, they have the same number of friends. ▲

Theorem (Generalized Pigeonhole Principle)**.** *If m objects are arranged into n boxes and $m > kn$, then there is at least one box with at least $k+1$ objects.*

Note that this is **best possible**: If $m = kn$ then each of the n boxes could contain precisely k objects.

Examples. (i) *At least how many cards we have to draw from a standard deck of* 52 *cards to assure that we will have at least four cards of the same suit (four spades, four hearts, four diamonds, or four clubs)?*

Suppose that we have four boxes, each reserved for a particular suit. When a card is drawn, we place it in the corresponding box. From the Generalized Pigeonhole Principle, we see that it is sufficient to extract at least 13 $(= 3 \cdot 4 + 1)$ cards to assure that we will have four cards of the same suit. ▲

(ii) *In every set of six people there are either three people who know each other or three people who do not know each other.*

Let a be an arbitrary person from the given set of six people. Divide the remaining five people into two rooms according to whether they know person a or not. Since $5 > 2 \cdot 2$, the Generalized Pigeonhole Principle implies that one of the two rooms contains at least three people. Suppose first that the first room contains people b, c, d. If two of them, say b and c, know each other, then $\{a, b, c\}$ is a subset of three people who know each other. Otherwise, no two people from the set $\{b, c, d\}$ know each other. The case when the second room contains three people is analyzed similarly. ▲

3 Elementary Combinatorics

3.1 Selections

Example. *In the lotto game run by Loterija Slovenije the drum contains* 39 *balls numbered* $1, \ldots, 39$. *The organizer of the game draws seven balls one after another from the drum. In how many ways this can be done?*

The answer depends on the interpretation of the word "way". The basic issues in understanding the problem are whether a ball that was pulled out at each step is returned back into the drum or not and whether the order of the extracted balls is important. The solution to the problem depends on the resolution of these two issues. ▲

Two basic characteristics of selections are:

Repetitiveness. Depending on whether we allow elements to repeat in a selection or not, we distinguish between *selections with repetition* and *selections without repetition.*

Order. Depending on whether the order of elements in a selection is important or not, we distinguish between *ordered selections (variations)* and *unordered selections (combinations).*

Ordered selections with repetition.

Suppose that the chosen balls are being **returned** back into the drum and that the **order** of the extracted balls **is important**.

Definition. Let N be a finite set and $k \in \mathbb{N}$. An ordered k-tuple $(a_1, \ldots, a_k)$ of elements of N is said to be an **ordered selection of order k over the set N**. (If we want to emphasize that some of the elements a_i might coincide, we call the k-tuple an "ordered selection with repetition".) The set of all of such selections is denoted by the symbol $\overline{V}(n, k)$.

Remark. An ordered k-tuple $(a_1, \ldots, a_k)$ of elements of N can be identified with a function from the set $\{1, \ldots, k\}$ to set N.

Since the set $\overline{V}(N,k)$ contains all ordered k-tuples of elements of the set N, it is equal to the k-fold Cartesian product of set N with itself:

$$\overline{V}(N,k) = \underbrace{N \times N \times \ldots \times N}_{k} .$$

From this equality and using the multiplication principle we infer the following.

Proposition. *Let N be an arbitrary set of n elements and $k \in \mathbb{N}$. Then, the set $\overline{V}(N,k)$ contains exactly n^k selections.*

Example. *Each weekend in February I can visit any of the three cinemas. How many different sequences of visits are possible, repeat visits of course being allowed?*

The number corresponds to the cardinality of the set $\overline{V}(C,4)$ where C is the set of three cinemas. $|\overline{V}(C,4)| = 3^4 = 81$. ▲

Ordered selections without repetition.

Suppose now that the **order** of the extracted balls **is important**, only that this time the selected balls will **not be returned** into the drum.

Definition. An ordered k-tuple $(a_1, \ldots, a_k)$ of pairwise distinct elements of set N is said to be an **ordered selection without repetition of order k over the set N**. The set of all such selections will be denoted by $V(N,k)$.

Remark. An ordered k-tuple $(a_1, \ldots, a_k)$ of pairwise distinct elements of N can be identified with an injective function from the set $\{1, \ldots, k\}$ to set N.

Of course, the number of ordered selections without repetition is smaller than the number of ordered selections with repetition.

Proposition. *Let N be an arbitrary set of n elements and $k \in \mathbb{N}$. Then, the set $V(N,k)$ contains exactly*

$$\prod_{i=0}^{k-1}(n-i) = n(n-1)\cdots(n-k+1)$$

selections.

Proof. If $n = 0$, then $N = \emptyset$ and $V(N,k) = \emptyset$. In this case, $|V(N,k)| = 0$ and the formula holds.

For $n \geq 1$, we use induction on k. If $k = 1$, then any selection is of the form (a) where $a \in N$. Therefore $|V(N,1)| = |N| = n$ and the formula holds.

Suppose that the formula holds for $k = r$ for some $r \geq 1$. We will show that it holds also for $k = r+1$. Let us denote the elements of N by $b_1, \ldots, b_n$. We can classify the selections from $V(N, r+1)$ into n groups, $R_1, \ldots, R_n$, where R_i contains exactly the selections with first coordinate b_i. If we remove the first coordinate from a selection $(b_i, x_1, \ldots, x_r)$ from R_i, we get the r-tuple $(x_1, \ldots, x_r)$, which is a selection of $V(N \setminus \{b_i\}, r)$. In doing so, each selection from $V(N \setminus \{b_i\}, r)$ occurs exactly once as a

"remainder" of a selection from R_i. Therefore, in each group R_i there are exactly as many selections as the selections in the set $V(N \setminus \{b_i\}, r)$, which, by the induction hypothesis, is of cardinality $(n-1)\cdots(n-r+1)(n-r)$. The number of selections in $V(N, r+1)$ is therefore $n(n-1)\cdots(n-r+1)(n-r) = n(n-1)\cdots(n-k+1)$. This proves the induction step. □

Unlike in the case of ordered selections with repetition, where the order of the selection can be arbitrary, in case of ordered selections without repetition the order is limited by the number of items we are selecting. In other words, if N is a finite set, then

$$V(N,k) = \emptyset, \qquad \text{as soon as } k > |N|\,.$$

Example. *In a presidential campaign a candidate must visit seven of the fifteen cities in Slovenia. In order to make the best possible impression, the candidate decided to end the campaign in Ljubljana. In how many ways can he visit the cities?*

Since the last city is already chosen, the candidate in fact chooses only the first six visited cities, from the remaining fourteen cities. Since the order is important, the number of such choices equals

$$14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 2162160\,.$$

▲

Permutations.

An ordered selection without repetition of maximum permissible order (that is, of order $k = |N|$) on a finite set N is said to be a **permutation** of N.

Corollary. *The number of permutations of a set of n elements is equal to*

$$n! = n(n-1)\cdots 1\,.$$

The symbol $n!$ is called n **factorial**. For the special case $n = 0$ we define $0! = 1$.

Remark. A permutation $(a_1, \ldots, a_n)$ of a set N can be identified with a bijective mapping from the set $\{1, \ldots, n\}$ to set N. If the elements of N are given in some order, we can identify a permutation $(a_1, \ldots, a_n)$ with the bijective mapping from the set N onto itself that maps the i-th element of N to a_i.

Unordered selections without repetition.

Suppose now that the **order** of the extracted balls **is not important** and that the selected balls are **not returned** into the drum.

Definition. Let N be a set of n elements and k a non-negative integer. A k-element subset of N will be called an **unordered selection without repetition of order k over the set N**. The set of all such selections will be denoted with the symbol $K(N, k)$.

Remark. The set of all k-element subset of N is often denoted also with $\binom{N}{k}$.

Definition. Let n and k be non-negative integers. The **binomial coefficient** $\binom{n}{k}$ is defined to be the number of k-element subsets of a set of n elements. (The number obviously doesn't depend on which n-element set we use.)

$\binom{n}{k}$ is read "n choose k".

Theorem (Formula for binomial coefficients)**.** *For all pairs of non-negative integers n and k we have*

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}\,.$$

Proof. Let N be a set of n elements and let k be a non-negative integer. If $k = 0$ then $\binom{n}{k} = 1$ since $K(N,0) = \{\emptyset\}$. In this case, the numerator of the quotient $\frac{\prod_{i=0}^{k-1}(n-i)}{k!}$ involves the product of factors from the empty set, which is standardly defined as 1. Since also $0! = 1$, it follows that the value of the quotient is 1 and the formula holds.[1]

If $k > n$, then $\binom{n}{k} = 0$ and $\frac{\prod_{i=0}^{k-1}(n-i)}{k!} = 0$, hence the formula holds.

Now, let $1 \le k \le n$. We will prove the statement by a double counting of the set $V(N,k)$ of ordered selections without repetition. On the one hand, we have $|V(N,k)| = n(n-1)\cdots(n-k+1)$. On the other hand, let us define, for a set $A \in K(N,k)$ the following set of ordered selections without repetition:

$$R_A = \{(a_1,\ldots,a_k) : \{a_1,\ldots,a_k\} = A\}\,.$$

Note that R_A is exactly the set of all permutations of the set A, so $|R_A| = k!$. Since each selection from $V(n,k)$ appears in exactly one of the sets R_A (namely, in the one such that the set of all values of its components is equal to A), the total number of such selections is equal to: $|V(N,k)| = |K(N,k)|k!$. Putting it all together, we obtain

$$\binom{n}{k}\cdot k! = |K(N,k)|k! = n(n-1)\cdots(n-k+1)\,,$$

which implies the formula given by the theorem. □

Remark. Special values of the binomial coefficients: $\binom{n}{0} = 1$, $\binom{n}{1} = n$, and $\binom{n}{n} = 1$.

If $k > n$, then $\binom{n}{k} = 0$.

Remark. We can extend the definition of binomial coefficients to integers n, k such that $n < 0$ and $k \ge 0$ using the formula $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$.

Example. $\binom{-5}{3} = \frac{(-5)\cdot(-6)\cdot(-7)}{3!} = -35$. ▲

[1] Alternatively, note that

$$\frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n(n-1)\cdots(n-k+1)(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}\,,$$

which, for $k = 0$, evaluates to $n!/(0!n!) = 1$.

Example. *During the night a thief broke into the gallery with 20 works of art. He has space for exactly 3 items in his backpack. In how many ways can he select items to steal?*

The thief must make an unordered selection without repetition of order 3 over a set of 20 elements. The number of such selections is exactly

$$\binom{20}{3} = \frac{20 \cdot 19 \cdot 18}{3 \cdot 2 \cdot 1} = 1140\,.$$

▲

Lemma (Quotient representation)**.** *For any two non-negative integers n and k such that $0 \leq k \leq n$, we have*

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

Proof. The equality follows directly from the formula for binomial coefficients:

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\cdots(n-k+1)}{k!} \\ &= \frac{n(n-1)\cdots(n-k+1)(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}\,.\end{aligned}$$

□

Corollary (Symmetry of binomial coefficients)**.** *For all integers n and k with $0 \leq k \leq n$, we have*

$$\binom{n}{k} = \binom{n}{n-k}\,.$$

Algebraic proof. Immediate from the quotient representation:

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

□

Combinatorial proof. Let N be an arbitrary n-element set and consider the mapping that assigns to every set $A \in \binom{N}{k}$ its complement $\overline{A} \subseteq N$. This defines a bijection from the set $K(N,k) = \binom{N}{k}$ to the set $K(N,n-k) = \binom{N}{n-k}$. Therefore $\binom{n}{k} = |\binom{N}{k}| = |\binom{N}{n-k}| = \binom{n}{n-k}$. □

Unordered selections with repetition.

Finally, consider the problem where the **order** of the selected balls **is not important** and the chosen balls are **returned** into the drum.

The notion of a **multiset** is a generalization of the notion of a set, which differs from it in that it allows multiple occurrences of elements.

Definition. A **multiset** is an unordered collection of elements in which an element can appear multiple times. It is denoted with symbol $[\ldots]$ instead of $\{\ldots\}$.

Example. Expressions $\{1, 2\}$ and $\{1, 1, 2\}$ represent the same set, while expressions $[1, 2]$ and $[1, 1, 2]$ represent different multisets. However, as with sets, the order is irrelevant. For example, $[1, 1, 2] = [1, 2, 1]$. ▲

Formally, a multiset can be defined as a pair (N, χ) where N is a set and χ is a mapping from N to the set of non-negative integers. The quantity $\chi(a)$, $a \in N$, is said to be the **multiplicity** of element a. The **cardinality** of a multiset is the value of the sum $\sum_{a \in N} \chi(a)$.

Definition. Let N be a set with n elements. A multiset of cardinality k with elements in N is said to be an **unordered selection with repetition of order k over the set N**. The set of all such multisets is denoted by $\overline{K}(N, k)$.

Proposition. *For any set N with n elements and any non-negative integer k, we have*

$$|\overline{K}(N, k)| = \binom{n + k - 1}{k}.$$

Proof. If $n = 0$ then both sides of the equation equal 1 if $k = 0$ and 0, otherwise. So let $n > 0$. Notice that the number of unordered selections with repetition of order k on the set N is equal to the number of sequences assembled from k characters $*$ and $n - 1$ characters $|$. The $n-1$ characters $|$ delineate n spaces corresponding to the elements of N, each character $*$ indicates the selection of an element corresponding to the space where $*$ is located. The number of sequences consisting of k characters $*$ and $n - 1$ characters $|$ equals the number of unordered selections without repetition of order k, determining the positions for the characters $*$ from the set of all possible $n + k - 1$ positions. It follows that the number of selections for $\overline{K}(N, k)$ equals $\binom{n+k-1}{k}$. □

Example. *What is the number of solutions to the equation*

$$x_1 + \ldots + x_n = k\,,$$

where $x_1, \ldots, x_n$ are non-negative integers?

Let $N = \{1, \ldots, n\}$ and consider a solution $x = (x_1, \ldots, x_n)$ to the above equation. Assuming that x_i denotes the number (zero or more) of times element i is chosen from set N, we see that x corresponds to a unique unordered selection with repetition of order k over the set N. And conversely: every unordered selection with repetition of order k over the set N corresponds to a unique solution $(x_1, \ldots, x_n)$ to the above equation. Therefore, the number of solutions is exactly $\binom{n+k-1}{k}$. ▲

Example. *There are n books on a shelf. In how many ways can we choose k of them so that no two of the chosen books are next to each other?*

Consider a particular choice of k books as above. Let x_1 denote the number of books of the shelf that are before the first chosen book, x_i, $2 \leq i \leq k$, the number of books that are between the $(i-1)$-st and the i-th chosen book, and x_{k+1} the number of books that are placed after the k-th chosen book. Since numbers x_i denote the numbers of non-chosen books, we have

$$x_1 + \ldots + x_{k+1} = n - k\,.$$

On the other hand, since no two of the chosen books were next to each other on the shelf, we have $x_2, \ldots, x_k \geq 1$ and $x_1, x_{k+1} \geq 0$.

Let us introduce new variables y_i, for all $i \in \{1, \ldots, k+1\}$, using the rule

$$y_i = \begin{cases} x_i - 1, & \text{if } 2 \leq i \leq k; \\ x_i, & \text{if } i \in \{1, k+1\}. \end{cases}$$

Then, the y_i's are non-negative integers satisfying

$$y_1 + \ldots + y_{k+1} = (n-k) - (k-1) = n - 2k + 1\,.$$

Using the previous example, we get that the number of the solutions to this equation is equal to

$$\binom{k+1+(n-2k+1)-1}{n-2k+1} = \binom{n-k+1}{n-2k+1} = \binom{n-k+1}{k},$$

where the last equality follows from the symmetry property of binomial coefficients. Since the y_i's uniquely determine the x_i's, which in turn uniquely determine the choice of k books from the shelf so that no two of the chosen books are next to each other, this is also the solution to the initial question. ▲

Solution to the lotto game problem.

If the order of the selected balls matters and the chosen balls are returned into the drum, we count the ordered selections with repetition of order 7 over a set of cardinality 39. There are exactly

$$39^7 = 137.231.006.679$$

of them.

If the order of the selected balls matters and the chosen balls are not returned into the drum, we count the ordered selections without repetition of order 7 over a set of cardinality 39. There are exactly

$$39 \cdot 38 \cdot 37 \cdot 36 \cdot 35 \cdot 34 \cdot 33 = 77.519.922.480$$

of them.

If the order of the selected balls does not matter and the chosen balls are returned into the drum, we count the unordered selections with repetition of order 7 over a set of cardinality 39. There are exactly

$$\binom{39+7-1}{7} = \binom{45}{7} = 45.379.620$$

of them.

Finally, consider the interpretation of the problem corresponding to the actual game, that is, when the order of the selected balls is unimportant and the chosen balls are not returned into the drum. We count the unordered selections without repetition of order 7 over a set of cardinality 39. There are exactly

$$\binom{39}{7} = 15.380.937$$

of them.

Permutations with repetition.

The notion of a permutation of a set was already defined in the section on ordered selections. Sometimes we are interested in ordering the elements of a multiset.

Example. *How many different words can be formed by permuting the letters of the word ABRAKADABRA?*

Some of the 11 letters coincide, therefore the answer is **not** 11!. Now we have to count the permutations of the multiset with letters A, B, R, D, and K in which A appears 5 times, each of B and R twice, and each of D and K once. Such a permutation is determined once we know in which 5 positions of the word letter A appears, in which two positions letter B, etc. We can choose the 5 positions for A in $\binom{11}{5}$ ways, then we can choose the 2 positions for B out of the remaining 6 in $\binom{6}{2}$ ways. We are left with 4 positions, from which we can choose 2 for R in $\binom{4}{2}$ ways, and finally from the remaining 2 positions we can choose one for D in $\binom{2}{1}$ ways. We are then left with a unique position for letter K. Therefore, the required number of permutations is

$$\binom{11}{5} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{1} = 83160\,.$$

▲

Definition. Let M be a multiset of cardinality n with elements $x_1, \ldots, x_k$, where element x_i appears n_i times (and thus $n_1 + \ldots + n_k = n$). A **permutation of multiset** M is an ordered n-tuple $(a_1, \ldots, a_n)$ in which each element x_i appears n_i times.

The number of permutations of multisets will be given by the following generalization of binomial coefficients.

Definition. Let $k \in \mathbb{N}$, let $n_1, \ldots, n_k$ be non-negative integers and let $n = n_1 + n_2 + \cdots + n_k$. The **multinomial coefficient** $\binom{n}{n_1, \ldots, n_k}$ is defined as the number of permutations of a multiset M of cardinality n with elements $x_1, \ldots, x_k$, where element x_i appears n_i times.

Proposition. *For all $k \in \mathbb{N}$, non-negative integers $n_1, \ldots, n_k$ and $n = n_1 + n_2 + \cdots + n_k$, we have*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \cdots n_k!}\,.$$

Proof sketch. Similarly as in the example we can derive that the number of permutations equals

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\ldots-n_{k-2}}{n_{k-1}}\binom{n_k}{n_k}\,.$$

(A formal proof would use induction on k.) Next, we apply the quotient representation of binomial coefficients to each factor:

$$\begin{aligned}
\binom{n}{n_1, \ldots, n_k} &= \binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\ldots-n_{k-2}}{n_{k-1}}\binom{n_k}{n_k} \\
&= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!} \cdots \frac{(n-n_1-\ldots-n_{k-1})!}{n_k!(n-n_1-\ldots-n_k)!} \\
&= \frac{n!}{n_1! \cdots n_k!}\,.
\end{aligned}$$

(Also here, a more formal proof would use induction on k.) □

Example. Let us illustrate the above proposition on the previous example, with the word ABRAKADABRA.

Suppose first that all the letters in the word are pairwise distinct, for example by indexing the occurrences of the same letter: $A_1B_1R_1A_2K_1A_3D_1A_4B_2R_2A_5$. *Now we have* 11 *different letters, which we can permute in* 11! *different ways. Consider an arbitrary permutation of the "non-indexed" word ABRAKADABRA, for example BAKARADABAR. From how many "indexed" words can this word be obtained by removing the indices? The* 5 *indices of letter A can be permuted in* 5! *ways, independently of this we can permute the* 2 *indices of B in* 2! *ways, etc. Therefore, the word BAKARADABAR, just like any other obtained from the word ABRAKADABRA, can be indexed in* 5!2!2!1!1! *ways. The number of non-indexed words, which is also the solution to the problem, is therefore equal to*

$$\frac{11!}{5!2!2!1!1!}.$$

▲

Proposition. *The number of ways of placing* n *different objects into* k *boxes so that* n_i *objects are placed in box* i *for all* $1 \leq i \leq k$, *is equal to*

$$\binom{n}{n_1, \ldots, n_k}.$$

Proof. Suppose that the objects are placed in a sequence and the boxes are numbered $1, \ldots, k$. Then each distribution of objects into boxes corresponds to a unique permutation of the multiset M with elements $1, \ldots, k$, where element i appears exactly n_i times:

- given a distribution of objects into boxes, we obtain a permutation of the multiset by replacing each object in the sequence with the number of the box containing it;
- conversely, given a permutation of the multiset, we obtain a valid distribution of objects into boxes by placing the j-th object in the sequence into the box indexed by the j-th element of the permutation.

We thus found a bijective mapping from the set of all legal distributions of objects into boxes and the set of all permutations of multiset M. By the equality principle and the above proposition, the number of distributions is equal to $\binom{n}{n_1,\ldots,n_k}$. □

3.2 Properties of Binomial Coefficients

The binomial coefficient is one of the most important combinatorial notions. We will now analyze some of its interesting properties.

Lemma (Pascal's identity)**.** *For all integers* n *and* k *with* $1 \leq k \leq n-1$ *we have*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Algebraic proof.

$$\begin{aligned}\binom{n-1}{k}+\binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!}+\frac{(n-1)!}{(k-1)!(n-k)!}\\ &= \frac{((n-k)+k)(n-1)!}{k!(n-k)!}\\ &= \frac{n!}{k!(n-k)!}\\ &= \binom{n}{k}.\end{aligned}$$

□

Combinatorial proof. The left-hand side of the identity represents the number of all k-elements subsets of an n-element set, say N. Choose an arbitrary $a \in N$ and partition the k-subsets of N into two groups depending on whether they contain a or not. Those that do not contain a are exactly the sets in $\binom{N\setminus\{a\}}{k}$ and their number is exactly $\binom{n-1}{k}$. To any k-element subset $A \in \binom{N}{k}$ such that $a \in A$, we can associate a $(k-1)$-element set $A' = A \setminus \{a\}$. The mapping $A \mapsto A'$ is a bijection from the set $\{A \in \binom{N}{k} : a \in A\}$ and the set $\binom{A\setminus\{a\}}{k-1}$. Therefore the number of sets in $\binom{N}{k}$ containing a is exactly $\binom{n-1}{k-1}$. The addition principle now implies that the number of k-element subsets of N equals $\binom{n-1}{k}+\binom{n-1}{k-1}$. □

Pascal's identity allows us to compute the binomial coefficients recursively, using a scheme known as the Pascal's triangle:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & \vdots & & & & \vdots & & &
\end{array}$$

The scheme has the shape of an isosceles triangle that we start building from a top corner downwards by placing a 1 into the extremal positions of each row and filling up the interiors of the rows by writing into each empty position the sum of the numbers that are written in the row above, diagonally to the left and to the right from the position. Rows and positions within each row are counted from 0 on. Pascal's identity implies that the k-th entry of the n-th row contains the number $\binom{n}{k}$.

The next theorem gives one of the most important properties of binomial coefficients. A **binomial** is a polynomial with two terms. The binomial theorem states that, if a power of a binomial is expanded, the coefficients in the resulting polynomial are the binomial coefficients.

Theorem (Binomial Theorem)**.** *For an arbitrary non-negative integer n we have*

$$(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k \,.$$

Algebraic proof. We use induction on n. For $n = 0$ both sides of the equation equal 1. Suppose now that the result holds for some $n \geq 0$. Then

$$\begin{aligned}
(1+t)^{n+1} &= (1+t)^n(1+t) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} t^k\right)(1+t) \\
&= \sum_{k=0}^{n} \binom{n}{k} t^k + \sum_{k=0}^{n} \binom{n}{k} t^{k+1} \\
&= 1 + \sum_{k=1}^{n+1} \binom{n}{k} t^k + \sum_{j=1}^{n+1} \binom{n}{j-1} t^j \\
&= 1 + \sum_{k=1}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1}\right) t^k \\
&= 1 + \sum_{k=1}^{n+1} \binom{n+1}{k} t^k \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} t^k \,,
\end{aligned}$$

where the penultimate equality holds by Pascal's identity. □

Combinatorial proof. It's clear that $(1+t)^n$ is a polynomial in t of degree n. To find the coefficient of t^k, consider the product

$$\underbrace{(1+t)(1+t)\cdots(1+t)}_{n \text{ factors}} \,.$$

The expansion is obtained by choosing either 1 or t from each factor in all possible ways, multiplying the chosen terms, and summing up all the results. Formally,

$$(1+t)^n = \sum_{(a_1,\ldots,a_n)\in\{1,t\}^n} a_1 a_2 \cdots a_n \,.$$

A term t^k is obtained when t is chosen from k of the factors, and 1 from the other $n-k$ factors. There are $\binom{n}{k}$ ways of choosing these k factors; so the coefficient of t^k is $\binom{n}{k}$, as claimed. □

Corollary. *For an arbitrary non-negative integer n we have*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \,.$$

Proof. Let $x = ty$. Then

$$\begin{aligned}(x+y)^n &= y^n(1+t)^n \\ &= y^n\left(\sum_{k=0}^{n}\binom{n}{k}t^k\right) \\ &= \sum_{k=0}^{n}\binom{n}{k}(t^k y^k)y^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\,.\end{aligned}$$

□

Examples. (i) *Find the coefficient of $x^{10}y^{12}$ in the expansion of $(x+y)^{22}$.*

The corollary of the Binomial Theorem implies that the coefficient equals $\binom{22}{10} = 646646$.

▲

(ii) *Find the coefficient of $x^{10}y^{12}$ in the expansion of $(3x-2y)^{22}$.*

Applying the above corollary to $(3x+(-2y))^{22}$, we get

$$(3x+(-2y))^{22} = \sum_{k=0}^{22}\binom{22}{k}(3x)^k(-2y)^{22-k}\,.$$

We obtain the term $x^{10}y^{12}$ for $k = 10$ and the corresponding coefficient is $\binom{22}{10}3^{10}(-2)^{12} = 156.400.843.382.784$. ▲

Example. *A walk in the integer lattice is a walk starting in the origin $(0,0)$ and adding in each step one unit in one of the two coordinates. For positive integers m, n, in how many ways we can reach point (m,n) from point $(0,0)$?*

Each step can be represented with symbol x or y (depending on which coordinate is increased). Hence, the whole walk can be represented with a sequence of length $m+n$ consisting of m copies of symbol x and n copies of symbol y. Clearly, there are exactly $\binom{m+n}{m}$ such sequences. ▲

It follows that we can represent the number of selections without repetition of order k over an n-element set as:

(i) the binomial coefficient $\binom{n}{k}$ (that is, as the number of k-element subsets of an n-element set),

(ii) the coefficient of t^k in the expansion of $(1+t)^n$,

(iii) the number of sequences of length n consisting of k symbols x and $n-k$ symbols y.

Using the binomial theorem, the following interesting identities can be derived.

Proposition. *For every non-negative integer n, we have*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \,.$$

Algebraic proof. Plugging $t = 1$ into the binomial theorem, we get

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k = \sum_{k=0}^{n} \binom{n}{k} \,.$$

□

Combinatorial proof. Follows immediately from the fact that the number of all subsets of an n-element set is equal to 2^n. □

Proposition. *For every positive integer n, we have*

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

Proof. Plug $t = -1$ into the binomial theorem:

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

□

Example. *For non-negative integers n, m, k we have*

$$\sum_{j=0}^{k} \binom{m}{j} \binom{n}{k-j} = \binom{m+n}{k} \,.$$

Consider a class with $m+n$ students, of which m are boys and n are girls. The number of ways of choosing k students from the class is equal to $\binom{m+n}{k}$, the number on the right-hand side.

On the other hand, there are exactly $\binom{m}{j}\binom{n}{k-j}$ ways of choosing exactly j boys and exactly $k-j$ girls. It follows that the sum of all such products, which is the number on the right-hand side, equals the number on the right-hand side. ▲

Lemma. *For all non-negative integers n and k we have:*

$$\begin{aligned} \sum_{j=0}^{n} \binom{k+j}{j} &= \binom{n+k+1}{n} \,, \\ \sum_{j=0}^{n} \binom{j}{k} &= \binom{n+1}{k+1} \,. \end{aligned}$$

Proof. By induction on n and using Pascal's identity.

Let us first show the first identity. For $n = 0$ both sides are equal to 1. Suppose now that $\sum_{j=0}^{n-1} \binom{k+j}{j} = \binom{n+k}{n-1}$ holds for some positive integer n. Consider the sum $\sum_{j=0}^{n} \binom{k+j}{j}$. We have

$$\begin{aligned}\sum_{j=0}^{n} \binom{k+j}{j} &= \sum_{j=0}^{n-1} \binom{k+j}{j} + \binom{k+n}{n} \\ &= \binom{n+k}{n-1} + \binom{k+n}{n} \\ &= \binom{n+k+1}{n}.\end{aligned}$$

Let us now show the second identity. For $n = 0$ the left-hand side becomes $\binom{0}{k}$ and the right-hand side $\binom{1}{k+1}$. Both are 1 if $k = 0$ and 0, otherwise. Thus equality holds. Suppose now that $\sum_{j=0}^{n-1} \binom{j}{k} = \binom{n}{k+1}$ holds for some positive integer n and consider the sum $\sum_{j=0}^{n} \binom{j}{k}$. We have

$$\begin{aligned}\sum_{j=0}^{n} \binom{j}{k} &= \sum_{j=0}^{n-1} \binom{j}{k} + \binom{n}{k} \\ &= \binom{n}{k+1} + \binom{n}{k} \\ &= \binom{n+1}{k+1}.\end{aligned}$$

□

The second identity from the above lemma is used often. For example, for $k = 1$ we get the formula for the sum of the first n natural numbers:

$$\sum_{j=0}^{n} \binom{j}{1} = 0 + 1 + \ldots + n = \binom{n+1}{2} = \frac{(n+1)n}{2}.$$

Suppose that we would like to evaluate the sum $1^2 + \ldots + n^2$. Noting that $j^2 = 2\binom{j}{2} + \binom{j}{1}$, we get

$$\sum_{j=0}^{n} j^2 = 2\sum_{j=0}^{n} \binom{j}{2} + \sum_{j=0}^{n} \binom{j}{1} = 2\binom{n+1}{3} + \binom{n+1}{2}.$$

From this one can easily derive the well known identity:

$$1^2 + 2^2 + \ldots n^2 = \frac{n(n+1)(2n+1)}{6}.$$

3.3 Principle of Inclusion-Exclusion

The addition principle tells us that the cardinality of the union of pairwise disjoint sets is equal to the sum of their cardinalities. What if the sets are not pairwise disjoint?

Then, clearly, the cardinality of the union is strictly smaller than the sum of the cardinalities of the individual sets, since when adding up these cardinalities each of the elements that appears in more than one set is counted more than once. The Principle of Inclusion-Exclusion gives a relation between the cardinality of the union and the cardinalities of the individual sets and their intersections.

Union of two sets.

Let us start with a simple example of the union of two sets A and B. If we first count the elements of A and then the elements of B, we will have counted all the elements of the union $A \cup B$, counting every element in the intersection $A \cap B$ twice. We thus get the well known formula:

$$|A \cup B| = |A| + |B| - |A \cap B| \,.$$

Union of arbitrarily many sets.

A similar argument shows that in the case of three sets A, B, and C we get

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \,.$$

More generally, for n finite sets $A_1, \ldots, A_n$ we get

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \left|\bigcap_{i \in I} A_i\right| \,.$$

Equivalently:

Theorem (Principle of Inclusion-Exclusion (PIE))**.** *For finite sets $A_1, \ldots, A_n$ we have*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right| \,.$$

Algebraic proof. We use induction on n. For $n \in \{1, 2\}$ equality holds. Suppose that it holds for an arbitrary collection of $n-1$ finite sets, for some $n \geq 3$. Then

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} A_i\right| &= \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| \\
&= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right| \\
&= \sum_{\emptyset \neq I \subseteq \{1,\ldots,n-1\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right| + |A_n| - \sum_{\emptyset \neq I \subseteq \{1,\ldots,n-1\}} (-1)^{|I|-1} \left|\cap_{i \in I \cup \{n\}} A_i\right| \,.
\end{aligned}$$

In the first term we are summing up, with appropriate signs, the cardinalities of all intersections of families of sets that do not contain set A_n. In the last term the

cardinalities of all intersections of k sets appear that do contain set A_n (set A_n and $k-1$ sets among $A_1, \ldots, A_{n-1}$), with signs $-(-1)^{(k-1)-1} = (-1)^{(k-1)}$. The last term does not include $|A_n|$, but this appears as a term on its own. Thus, the cardinality of the intersection of any k sets among $A_1, \ldots, A_n$ appears exactly one in the above expression, with sign $(-1)^{k-1}$. This completes the inductive step. □

Combinatorial proof. We claim that every element $x \in \cup_{i=1}^{n} A_i$ is counted exactly once in the above formula. Suppose that x is contained in exactly m sets A_i. Without loss of generality, we may assume (by renaming the sets if necessary) that x is contained in $A_1, \ldots, A_m$. Then, x is contained in any intersection of $k \geq 1$ sets among $A_1, \ldots, A_m$ and in no other intersection. Since the number of k-element subsets of an m-element set is $\binom{m}{k}$, element x appears in exactly $\binom{m}{k}$ intersections of exactly k sets. This means that for each k element x contributes exactly $(-1)^{k-1}\binom{m}{k}$ to the sum. Altogether its contribution is

$$\sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} = 1 + \sum_{k=0}^{m} (-1)^{k-1} \binom{m}{k} = 1\,,$$

where the last equality follows from one of the consequences of the Binomial Theorem. □

Example. *A cruise ship arrives to Koper. Passengers on the ship speak English, German, and Italian. Any of these languages is spoken by at most* 60 *passengers. For every pair of languages there exist at least* 10 *passengers speaking both languages. There exist exactly four passengers who speak all three languages. What is the maximum number of passengers on the ship?*

Let E, G, and I denote the sets of passengers speaking English, German, and Italian, respectively. Then $|E|, |G|, |I| \leq 60$, $|E \cap G|, |E \cap I|, |G \cap I| \geq 10$, and $|E \cap G \cap I| = 4$. It follows that the number of passengers is

$$|E \cup G \cup I| = |E| + |G| + |I| - |E \cap G| - |E \cap I| - |G \cap I| + |E \cap G \cap I| \leq 3 \cdot 60 - 3 \cdot 10 + 4 = 154\,.$$

(It can be verified that this upper bound can indeed be achieved.) ▲

Example. *Derangements. Recall the question from the first class: Given n letters and n addressed envelopes, in how many ways can the letters be placed in the envelopes so that no letter is ins the correct envelope?*

Assume an ordering of the letters and envelopes such that the i-th letter corresponds to the i-th envelope, for all $i = 1, \ldots, n$. Every placement of letters into envelopes can be described by a permutation $(a_1, \ldots, a_n)$ of the set $\{1, \ldots, n\}$, where a_i is the number of the envelope in which the i-th letter is placed. Therefore, there are exactly $n!$ possible placements. The placements such that no letter is in the correct envelope correspond exactly to permutations $(a_1, \ldots, a_n)$ such that $a_i \neq i$ for all $i = 1, \ldots, n$.

For all $i \in \{1, \ldots, n\}$, let A_i be the set of all permutations $(a_1, \ldots, a_n)$ such that $a_i = i$. We say that elements of A_i **fix** element i. The union $\cup_{i=1}^{n} A_i$ is exactly the set of all permutation that fix at least one element. We are interested in the quantity

$$d(n) = n! - |\cup_{i=1}^{n} A_i|\,.$$

Consider an arbitrary non-empty set $I \subseteq \{1, \ldots, n\}$ and let $k = |I|$. Let us determine the cardinality $|\cap_{i\in I} A_i|$. The elements of this intersection are exactly the permutations $(a_1, \ldots, a_n)$ that fix all elements in I. That is, $a_i = i$ for all $i \in I$, and in the remaining positions $\{1, \ldots, n\}\setminus I$ there is an arbitrary permutation of the set $\{1, \ldots, n\} \setminus I$. Therefore, the cardinality of the intersection $|\cap_{i\in I} A_i|$ is equal to $(n - |I|)! = (n - k)!$.

By the Inclusion-Exclusion principle, we have

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{I\subseteq\{1,\ldots,n\}\\ |I|=k}} \left|\bigcap_{i\in I} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}\,.$$

The quantity $d(n)$ is therefore equal to

$$d(n) = n! - \frac{n!}{1!} + \frac{n!}{2!} - \ldots + (-1)^n \frac{n!}{n!}\,.$$

Note: A permutation without fixed points is called a **derangement**. This explains the notation $d(n)$.

Let us write

$$d(n) = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right)\,.$$

Note that $\frac{d(n)}{n!}$ converges to e^{-1}, therefore $d(n) \approx n!/e$. ▲

Example. *How many surjective mappings from an n-element set X to an m-element set Y are there?*

We already know that the number of all mappings from X to Y is m^n. Let us compute the number of all mappings that are not surjective. The number of all surjective mappings will then equal the difference between the number of all mappings, m^n, and the number of those that are not surjective.

Without loss of generality we may assume that $Y = \{1, \ldots, m\}$. Let A_i denote the set of all mappings from X to Y that do not take value i. Then, a mapping is **not** surjective if and only if it belongs to the union $\cup_{i=1}^{m} A_i$.

Consider an arbitrary non-empty subset $I \subseteq \{1, \ldots, m\}$, let $k = |I|$ and let us determine the cardinality of the intersection $|\cap_{i\in I} A_i|$. Set $\cap_{i\in I} A_i$ consists of all mappings from X to Y that do not take any value from I. These are exactly the mappings from X to $Y \setminus I$; their number is $(m - k)^n$. By the Inclusion-Exclusion Principle, we get

$$\left|\bigcup_{i=1}^{m} A_i\right| = \sum_{k=1}^{m} (-1)^{k-1} \sum_{\substack{I\subseteq\{1,\ldots,m\}\\ |I|=k}} \left|\bigcap_{i\in I} A_i\right| = \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n\,.$$

Consequently, the number of all surjective maps is

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

▲

4 Recurrence Relations

A **recurrence relation** expresses the value of a function f at a natural number n in terms of its values at smaller natural numbers.

Examples. 1. Let $F(0) = 1$ and $F(n) = n \cdot F(n-1)$ for $n \geq 1$. Then $F(n) = n!$ holds for all non-negative integers n.

2. Any sequence $(a_1, a_2, \ldots)$ of real numbers such that the difference of two consecutive numbers is constantly equal to d is said to be an **arithmetic progression**. Since $d = a_{n+1} - a_n$, the following recurrence relation holds for $F(n) = a_n$:

$$F(n+1) = F(n) + d\,.$$

It can be shown using induction on n that $F(n) = F(1) + (n-1)d$ holds for all $n \in \mathbb{N}$.

3. Any sequence $(a_1, a_2, \ldots)$ of real numbers such that the quotient of two consecutive numbers is constantly equal to q is said to be a **geometric progression**. Since $q = \frac{a_{n+1}}{a_n}$, the following recurrence relation holds for $F(n) = a_n$:

$$F(n+1) = q \cdot F(n)\,.$$

It can be shown using induction on n that $F(n) = F(1) \cdot q^{n-1}$ holds for all $n \in \mathbb{N}$. ▲

Example. Let $F(n)$ denote the number of subsets of an n-element set. Then

$$F(n+1) = 2F(n)\,.$$

This is because we can find all subsets of $\{1, \ldots, n+1\}$ by taking all subsets of $\{1, \ldots, n\}$ and extending each in the two possible ways — either do nothing, or add the element $n+1$. Moreover, $F(0) = 1$. The relations $F(n+1) = 2F(n)$ and $F(0) = 1$ determine the value of F for every non-negative integer.

Induction on n can be used to show that $F(n) = 2^n$. ▲

An important technique, often associated with recurrence relations, is that of **generating functions**. These are power series whose coefficients form the number sequence in question. We will show how generating functions can be used to solve recurrence relations.

Example. Let $F(n)$ denote the number of subsets of an n-element set. We will show that $F(n) = 2^n$ with yet another method. Set

$$\phi(t) = \sum_{n=0}^{\infty} F(n) t^n\,.$$

Such an expression is called a **power series**, also called a **generating function** of the sequence $(F(n))_{n\geq 0}$.[2] Now

$$\begin{aligned} 2t\phi(t) &= \sum_{n=0}^{\infty} 2F(n)t^{n+1} \\ &= \sum_{n=0}^{\infty} F(n+1)t^{n+1} \\ &= \phi(t) - 1\,, \end{aligned}$$

the last equality holding because the sum is identical with the definition of $\phi(t)$ (with $n+1$ replacing n) except that the first term $F(0)t^0 = 1$ is missing. Thus

$$\phi(t) = \frac{1}{1-2t}\,.$$

The right-hand side is the sum of a geometric progression:

$$\phi(t) = \sum_{n=0}^{\infty} (2t)^n\,.$$

[Recall: $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$ for all x with $|x| < 1$.] Comparing this with the original series, we conclude that $F(n) = 2^n$. (If two power series are equal, then all their coefficients coincide.)[3] ▲

4.1 Fibonacci Numbers

Problem. *In how many ways can a non-negative integer n be written as a sum of ones and twos (in order)?*

Let F_n be this number. Then, for example, $F_4 = 5$, since

$$4 = 1+1+1+1 = 2+1+1 = 1+2+1 = 1+1+2 = 2+2\,.$$

Similarly, we find that $F_1 = 1$, $F_2 = 2$, $F_3 = 3$. By convention, we take $F_0 = 1$: the only solution for $n = 0$ is the empty sequence.

Suppose that $n \geq 2$. Any expression for n as a sum of ones and twos must end with either a 1 or a 2. If it ends with a 1, then the preceding terms sum to $n-1$; if it ends with a 2, then the preceding terms sum to $n-2$. So we have

$$F_n = F_{n-1} + F_{n-2}\,.$$

The numbers $F_0, F_1, F_2, \ldots$ are called the **Fibonacci numbers**.

[2] Students of the Mathematics program will learn about power series in more detail in the Analysis II course.

[3] The above reasoning also shows that the power series converges for all t with $|t| < 1/2$; so our manipulations are justified by analysis.

Remark. The original formulation involved rabbits. *Rabbits take two months to reach maturity. A mature pair of rabbits produces another pair of rabbits each month. If you start with one pair of newly born rabbits, how many pairs you will have after n months?*

If F_n denotes the number of rabbit pairs after n months, then $F_0 = 1$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. ▲

This is an example of a **recurrence relation**, more specifically, a three-term linear recurrence relation with constant coefficients. More generally:

- a $(k+1)$**-term recurrence relation** expresses any value $F(n)$ of a function in terms of the k preceding values $F(n-1)$, $F(n-2), \ldots, F(n-k)$;
- it is **linear** if it has the form

$$F(n) = a_1(n)F(n-1) + a_2(n)F(n-2) + \ldots + a_k(n)F(n-k)\,,$$

  where $a_1, \ldots, a_k$ are functions of n; and
- it is **linear with constant coefficients** if $a_1, \ldots, a_k$ are constants.

FACT: *A function satisfying a $(k+1)$-term recurrence relation is uniquely determined by its values on the first k natural numbers.*

(The first k natural numbers could be $0, \ldots, k-1$ or $1 \ldots, k$, depending on the context.)

Indeed: if we know $F(1), \ldots, F(k)$ (say), then these values determine $F(k+1)$, and then the values $F(2), \ldots, F(k+1)$ determine $F(k+2)$, and so on.

Formally, if two functions F and G satisfy the same $(k+1)$-term recurrence relation and agree on the first k natural numbers, then one proves by induction that they agree everywhere.[4]

We turn to methods for solving the recurrence relation:

Fibonacci Reccurence Relation
For $n \geq 2$, $$F_n = F_{n-1} + F_{n-2}\,.$$

Two methods will be given; both of them generalize.

First Method. Since the recurrence relation is linear, if we can find any solutions, we can take linear combinations of them to generate new solutions. Specifically, let F and G satisfy the recurrence relation above, and let $H_n = aF_n + bG_n$. Then

$$\begin{aligned} H_n &= aF_n + bG_n \\ &= a(F_{n-1} + F_{n-2}) + b(G_{n-1} + G_{n-2}) \\ &= (aF_{n-1} + bG_{n-1}) + (aF_{n-2} + bG_{n-2}) \\ &= H_{n-1} + H_{n-2}\,. \end{aligned}$$

[4] A similar situation occurs with differential equations, where we expect a kth order differential equation and k initial conditions to determine a solution uniquely. You can learn about differential equations in the elective course Differential Equations; some basics are also discussed in the 3rd year course Mathematical Modeling. A numerical treatment of differential equations is given in the Masters course "Selected Topics in Numerical Mathematics".

We try to fit the initial conditions by choice of a and b.

Try a solution of the form $F_n = \alpha^n$. (The justification for this will be that it works!) We require

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2}\,,$$
$$\alpha^{n-2}(\alpha^2 - \alpha - 1) = 0\,.$$

So, if $\alpha^2 - \alpha - 1 = 0$, the recurrence holds for all n. The roots of this equation are $\alpha = \frac{1}{2}\left(1+\sqrt{5}\right)$, $\beta = \frac{1}{2}\left(1-\sqrt{5}\right)$. So we have a general solution of the form

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

To fit the initial conditions (which are $F_0 = 1$, $F_1 = 1$ in our case), we require

$$\begin{aligned} a+b &= 1\,,\\ a\left(\frac{1+\sqrt{5}}{2}\right) + b\left(\frac{1-\sqrt{5}}{2}\right) &= 1\,, \end{aligned}$$

which is equivalent to $a+b=1$, $a-b=1/\sqrt{5}$, giving

$$a = \frac{\sqrt{5}+1}{2\sqrt{5}}, \quad b = \frac{\sqrt{5}-1}{2\sqrt{5}}$$

and so:

Fibonacci Numbers

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

Remarks. 1. $\frac{1+\sqrt{5}}{2} \approx 1,618...$, and $\frac{1-\sqrt{5}}{2} \approx -0,618...$ So the function grows exponentially; for large n, its value is the nearest integer to $\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n$.
2. We could easily find the values of a and b to fit any given initial values.
3. For computational purposes, the explicit formula is less useful than the recurrence relation. ▲

Second Method. We now solve the recurrence relation using the technique of generating functions. We let $\phi(t)$ be the power series

$$\phi(t) = \sum_{n\geq 0} F_n t^n\,,$$

where t is an indeterminate. We have

$$\begin{aligned} t\phi(t) &= \sum_{n\geq 0} F_n t^{n+1} = \sum_{n\geq 1} F_{n-1} t^n \,, \\ t^2\phi(t) &= \sum_{n\geq 0} F_n t^{n+2} = \sum_{n\geq 2} F_{n-2} t^n \,. \end{aligned}$$

Now $F_n = F_{n-1} + F_{n-2}$ so it is 'almost true' that $\phi(t) = (t + t^2)\phi(t)$. Certainly, the coefficients of t^2 and all higher powers will be the same on both sides of this equation, but we might have to adjust the constant term and the term in t. Remember that $F_0 = 1$, $F_1 = 1$.

The coefficient of t is F_1 on the left and F_0 on the right, so these agree. The constant term is F_0 on the left and 0 on the right, so we have to add 1 to the right-hand side to obtain equality. Thus,

$$\phi(t) = 1 + (t + t^2)\phi(t)$$

and so

$$\phi(t) = \frac{1}{1 - t - t^2} \,.$$

Now the value of F_n is the coefficient of t^n in the Taylor series for this function. This is most easily found by a **partial fraction expansion**. Let $1 - t - t^2 = (1 - \alpha t)(1 - \beta t)$. Thus, α and β are roots of $x^2 - x - 1 = 0$; so $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$. If we let

$$\frac{1}{(1 - \alpha t)(1 - \beta t)} = \frac{a}{1 - \alpha t} + \frac{b}{1 - \beta t} \,,$$

then

$$1 = a(1 - \beta t) + b(1 - \alpha t) \,,$$

so $a + b = 1$, $a\beta + b\alpha = 0$. These equations can be solved for a and b (with the same solution as before). Now

$$\begin{aligned} \phi(t) &= \frac{a}{1 - \alpha t} + \frac{b}{1 - \beta t} \\ &= a(1 + \alpha t + \alpha^2 t^2 + \ldots) + b(1 + \beta t + \beta^2 t^2 + \ldots) \,; \end{aligned}$$

equating coefficients at t^n, we find that

$$F_n = a\alpha^n + b\beta^n \,.$$

4.2 Linear Recurrence Relations with Constant Coefficients

The procedure for solving a general linear recurrence relation with constant coefficients is similar to that in the Fibonacci case. Consider the recurrence

$$F(n) = a_1 F(n-1) + a_2 F(n-2) + \ldots + a_k F(n-k) \,.$$

Using the first method, we try a solution of the form $F(n) = \alpha^n$; we find that α must be a solution to the equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \ldots + a_k \,.$$

- If this **characteristic equation** (which is a polynomial equation of degree k) has all its roots distinct, then we obtain k independent solutions of the recurrence relation, say $F_i(n)$ for $i = 1, \ldots, k$. We need to find a linear combination of these, $\sum_{i=1}^{k} \lambda_i F_i(n)$, which fits the k initial values of F. We get k linear equations in k unknowns; these equations have a unique solution $(\lambda_1, \ldots, \lambda_k)$. So the solution to the recurrence equation (with the given initial values) is $\sum_{i=1}^{k} \lambda_i F_i(n)$.

- However, if the **characteristic polynomial**

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

has repeated roots, then we don't obtain enough solutions. In this case, suppose that α is a root of the characteristic polynomial with multiplicity d. Then it can be verified that the d functions $\alpha^n, n\alpha^n, \ldots, n^{d-1}\alpha^n$, are all solutions of the recurrence relation. Doing this for every root, we again find enough independent solutions that k initial values can be fitted.

The justification of this is the fact that the solutions claimed can be substituted in the recurrence relation and the truth verified.

Example. *Solve the recurrence relation*

$$F(n) = 2F(n-1) - F(n-2)$$

with initial values $F(0) = 1$, $F(1) = 2$.

The characteristic equation is $x^2 = 2x - 1$, with the multiset of solutions $x \in [1, 1]$. So the general solution of the recurrence relation is

$$F(n) = an + b\,.$$

To fit the initial conditions, we require $a = b = 1$, so the solution is $F(n) = n + 1$ for all $n \geq 0$. ▲

Example. *Solve the recurrence relation*

$$F(n) = 3F(n-2) - 2F(n-3)$$

with initial values $F(0) = 3$, $F(1) = 1$, $F(2) = 8$.

The characteristic equation is $x^3 = 3x - 2$, with the multiset of solutions $x \in [1, 1, -2]$. So the general solution of the recurrence relation is

$$F(n) = a(-2)^n + bn + c\,.$$

To fit the initial conditions, we require $a = b = 1$, $c = 2$, so the solution is $F(n) = (-2)^n + n + 2$. ▲

The above method is only applicable in the case of linear recurrence relations with constant coefficients. When this fails, we use the technique of generating functions.

Example. *Solve the recurrence relation*

$$F(n) = 3F(n-1) + 2$$

with initial value $F(0) = 0$.

Let $\phi(t) = \sum_{n\geq 0} F(n)t^n$. Then

$$\begin{aligned}\sum_{n\geq 1} F(n)t^n &= 3\sum_{n\geq 1} F(n-1)t^n + 2\sum_{n\geq 1} t^n \\ &= 3t\sum_{n\geq 0} F(n)t^n + 2\left(\frac{1}{1-t} - 1\right),\end{aligned}$$

hence

$$\phi(t) = 3t\phi(t) + \frac{2t}{1-t},$$

that is,

$$\phi(t) = \frac{2t}{(1-3t)(1-t)}.$$

We apply the partial fraction expansion: setting

$$\frac{2t}{(1-3t)(1-t)} = \frac{a}{1-3t} + \frac{b}{1-t}$$

yields $a + b = 0$ and $-a - 3b = 2$, which has a unique solution $a = 1$, $b = -1$. Therefore

$$\phi(t) = \frac{1}{1-3t} - \frac{1}{1-t}.$$

Since $\frac{1}{1-3t} = \sum_{n\geq 0}(3t)^n$ and $\frac{1}{1-t} = \sum_{n\geq 0} t^n$, we get

$$\phi(t) = \sum_{n\geq 0} (3^n - 1)\, t^n,$$

that is, $F(n) = 3^n - 1$ for all $n \geq 0$. ▲

4.3 Derangements, Revisited

For linear recurrences with non-constant coefficients, or for non-linear recurrences, there is no general method which always works. Sometimes it is possible to solve such relations, either by guessing the solution (and verifying that it works), or by some other method. We give an example of the former principle.

Derangements. *Recall that a derangement of* $\{1, \ldots, n\}$ *is a permutation* $(a_1, \ldots, a_n)$ *of this set which leaves no point fixed (that is,* $a_i \neq i$ *for all* i*). We computed the general formula for the number of derangements using the Principle of Inclusion-Exclusion. Now we will do the same using recurrence relations.*

Let $d(n)$ be the number of derangements of $\{1, 2, \ldots, n\}$. Any derangement $(a_1, \ldots, a_n)$ has $a_n = i$ for some $i < n$. Clearly, the same number of derangements is obtained for each value of i from 1 to $n-1$; so we will find $d(n)$ by computing the number of derangements such that $a_n = i$ and multiplying by $n - 1$.

Let $a = (a_1, \ldots, a_n)$ be a derangement with $a_n = i$. There are two cases:

Case 1. $a_i = n$. In other words, a (viewed as a bijective mapping of the set $\{1, \ldots, n\}$ to itself) interchanges i and n. Now it operates on the remaining $n-2$ points as a derangement. Furthermore, given any derangement of the points different from i and n, we may extend it to interchange i and n, and obtain a derangement of the entire set. So the number of derangements of this type is $d(n-2)$.

Case 2. $a_i \neq n$. Then $a_j = n$ for some $j \neq i$. Define a permutation a' of $\{1, \ldots, n-1\}$ by the rule

$$a'_k = \begin{cases} a_k, & \text{if } k \neq j; \\ i, & \text{if } k = j. \end{cases}$$

Then a' is a derangement. Any derangement of $\{1, \ldots, n-1\}$ can be 'extended' to a derangement of $\{1, \ldots, n\}$, by reversing the construction. So there are $d(n-1)$ derangements under this case.

So we obtain

$$d(n) = (n-1)(d(n-1) + d(n-2))\,.$$

This is a three-term recurrence relation. The initial values are given by $d(0) = 1$, $d(1) = 0$.

We already know that

$$d(n) = n! \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right).$$

We give an alternative proof by showing that the two sides of the equation satisfy the same recurrence relation and have the same initial values. So let $f(n) = n! \sum_{k=0}^{n} (-1)^k/k!$. Then

$$f(0) = 1 = d(0), \quad f(1) = 0 = d(1)\,.$$

Also

$$\begin{aligned}
& (n-1)(f(n-1) + f(n-2)) \\
= \; & (n-1)(n-1)! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} + (n-1)(n-2)! \sum_{k=0}^{n-2} \frac{(-1)^k}{k!} \\
= \; & ((n-1)(n-1)! + (n-1)(n-2)!) \sum_{k=0}^{n-2} \frac{(-1)^k}{k!} + (-1)^{n-1}(n-1) \\
= \; & n! \sum_{k=0}^{n-2} \frac{(-1)^k}{k!} + (-1)^{n-1} \frac{n!}{(n-1)!} + (-1)^n \frac{n!}{n!} \\
= \; & n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \\
= \; & f(n)\,,
\end{aligned}$$

since $n - 1 = n!/(n-1)! - n!/n!$. So the equality is established.

5 Distributions

A **distribution** is a way of placing the elements of a given set X into a given number of cells (boxes). There are various types of distributions, depending on:

(i) whether the elements and/or the cells are **distinguishable** (or: **labeled**) or not,

(ii) whether or not we allow some of the cells to be **empty**.

Example. The set $X = \{a, b, c, d\}$ has exactly the following distributions of its elements into two non-empty unlabeled cells:

$$\{\{a\}, \{b, c, d\}\}, \{\{b\}, \{a, c, d\}\}, \{\{c\}, \{a, b, d\}\}, \{\{d\}, \{a, b, c\}\},$$
$$\{\{a, b\}, \{c, d\}\}, \{\{a, c\}, \{b, d\}\}, \{\{a, d\}, \{b, c\}\}\,.$$

There are 7 in total. In case of labeled cells, there would be 14. ▲

Distributing labeled elements into unlabeled cells

Consider first the case when all the cells must be **non-empty**. In this case we can view a distribution of labeled elements into unlabeled non-empty cells as a partition of a set into a given number of parts.

Definition. The number of all partitions of an n-element set into k non-empty subsets is the **Stirling number of the second kind**, denoted by $S(n, k)$.

The previous example implies that $S(4, 2) = 7$.

The following holds:

$$S(n, k) = 0 \quad \text{for all } k > n\,, \quad S(n, n) = 1\,, \quad \text{and } S(n, 1) = 1\,.$$

Additionally, let us define $S(n, 0) = 0$ for all $n \geq 1$ and $S(0, 0) = 1$.

The Stirling numbers of the second kind can be computed recursively.

Proposition. *For all positive integers n and k with $n \geq k \geq 1$ we have*

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

Proof. Let $X = \{x_1, \ldots, x_n\}$ be an arbitrary n-element set, R the set of all partitions of X into k non-empty parts, R_0 the set of all partitions from R containing $\{x_n\}$ as a part, and $R_1 = R \setminus R_0$. Consider an arbitrary partition $P = \{X_1, \ldots, X_k\} \in R$. Removing x_n from X, partition P becomes partition $P' = \{X_1 \setminus \{x_n\}, \ldots, X_k \setminus \{x_n\}\}$ of the set $X \setminus \{x_n\}$.

If $P \in R_0$, then one of the sets in P' is empty and we can remove it, thus obtaining a partition of the $(n-1)$-element set $X \setminus \{x_n\}$ into $k-1$ non-empty sets. And conversely, every partition $T = \{X'_1, \ldots, X'_{k-1}\}$ of the set $X \setminus \{x_n\}$ into $k-1$ non-empty sets can be turned into a partition $P = \{X'_1, \ldots, X'_{k-1}, \{x_n\}\}$ of set X into k non-empty sets. Partition P is the only partition from R_0 such that $P' = T$. The equality principle implies $|R_0| = S(n-1, k-1)$.

If $P \in R_1$, then none of the sets in P' is empty, which means that P' is a partition of $X \setminus \{x_n\}$ into k non-empty parts. For any partition $T = \{X'_1, \ldots, X'_k\}$ of the set $X \setminus \{x_n\}$ into k non-empty parts, adding x_n to one of the parts X'_i results in a partition P from R_1 such that $P' = T$. Moreover, the so obtained partitions are the only ones from R_1 for which $P' = T$, which means that the number of partitions from R_1 is exactly k times the number of partitions of the $(n-1)$-element set $X \setminus \{x_n\}$ into k non-empty parts, that is, $kS(n-1, k)$. We conclude that $|R_1| = kS(n-1, k)$.

The proposition now follows from the addition principle: $|R| = |R_0| + |R_1| = S(n - 1, k - 1) + kS(n - 1, k)$. □

Using the recursive formula we can compute the Stirling numbers of the second kind similarly as the binomial coefficients. We obtain a two-dimensional table where the entry in the n-th row and k-th column contains the number $S(n,k)$:

$n \setminus k$	0	1	2	3	4	5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	0	1	1	0	0	0
3	0	1	3	1	0	0
4	0	1	7	6	1	0
5	0	1	15	25	10	1

It follows from the initial conditions that all values above the main diagonal are zeros, all values on the main diagonal are ones, and the first column contains all zeros except for the first element, which is one. We obtain a number $S(n,k)$ in the table by summing the number diagonally to the left above it and the number immediately above it, multiplied by k.

Example. $S(5,3) = S(4,2) + 3 \cdot S(4,3) = 7 + 3 \cdot 6 = 25$. ▲

Suppose now that we **allow empty cells**. Suppose that out of k cells exactly j are non-empty. We then distribute the n elements into j non-empty cells, which can be done in $S(n,j)$ ways. Since the number of non-empty cells can be $1, \ldots, k$, the number of distributions equals

$$\sum_{j=1}^{k} S(n,j)\,.$$

A similar reasoning shows that the number of partitions of an n-element set equals

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

This number is called the **Bell number**. (The case of $k = 0$ is included only because of $n = 0$.)

Distributing labeled elements into labeled cells

Now we would like to distribute the elements of an n-element set X into k labeled cells. If the cells are allowed to be empty, then we can place any element into any cell. In this case, the multiplication rule implies that the number of distributions is

$$k^n\,.$$

If we require that the cells are **non-empty**, then we first distribute the elements into k unlabeled cells in $S(n,k)$ ways. We can label (order) the cells in $k!$ ways. The multiplication rule implies that the number of distributions is

$$k! \cdot S(n,k)\,.$$

Remark. We can view a distribution of elements of a set of cardinality n into k labeled cells so that all of the cells are non-empty as a surjective mapping from an n-element set into a k-element set. So the number of such mappings is $k! \cdot S(n,k)$. On the other hand, we know that the number of all surjective maps is

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

It follows that

$$S(n,k) = \frac{1}{k!}\sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j}j^n\,.$$

Distributing unlabeled elements into unlabeled cells.

Consider first the case when the cells are required to be **non-empty**. Any distribution of n unlabeled elements into k unlabeled cells such that none of the cells is empty can be seen as a sequence of positive integers $n_1 \le n_2 \le \ldots \le n_k$ summing up to n.

Definition. A sequence of positive integers $n_1 \le n_2 \le \ldots \le n_k$ summing up to n is a **partition of n of order k**. The number of all such partitions is denoted by $p_k(n)$.

For example, $p_2(4) = 2$, since $4 = 1+3 = 2+2$.

Clearly, we have

$$p_k(n) = 0 \quad \text{for } k > n\,.$$

Additionally, we define $p_0(0) = 1$ and $p_0(n) = 0$ for all $n > 0$.

Proposition. *For all positive integers n and k with $n \ge k \ge 1$, we have*

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

Proof. Let R_0 and R_1 consist of all partitions $(n_1,\ldots,n_k)$ of n of order k such that $n_1 = 1$ and $n_1 > 1$, respectively. Removing the first element $n_1 = 1$ from a partition in R_0 produces a partition of $n-1$ of order $k-1$. The process can be reversed, hence $|R_0| = p_{k-1}(n-1)$.

Reducing each summand of a partition from R_1 by one produces a partition of $n-k$ of order k. Since each partition of $n-k$ of order k arises exactly once this way, we have $|R_1| = p_k(n-k)$. The addition principle now implies $p_k(n) = |R_0| + |R_1| = p_{k-1}(n-1) + p_k(n-k)$. □

Using the recursive formula, we obtain a two-dimensional table where the entry in the n-th row and k-th column contains the number $p_k(n)$. The initial conditions imply that all values above the main diagonal are zeros, all values on the main diagonal are ones, and the first column contains all zeros except for the first element, which is one. We obtain a number $p_k(n)$ in the table by summing the number diagonally to the left above it and the number k units above it.

$n \setminus k$	0	1	2	3	4	5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	0	1	1	0	0	0
3	0	1	1	1	0	0
4	0	1	2	1	1	0
5	0	1	2	2	1	1

Suppose now that we allow empty cells. Suppose that out of k cells exactly j are non-empty. We then distribute the n unlabeled elements into j non-empty unlabeled cells, which can be done in $p_j(n)$ ways. Since the number of non-empty cells can be $1, \ldots, k$, the number of such distributions equals

$$\sum_{j=1}^{k} p_j(n)\,.$$

A similar reasoning shows that the number of all partitions of positive integer n equals

$$p(n) = \sum_{k=1}^{n} p_k(n)\,.$$

Distributing unlabeled elements into labeled cells

[Recall the example from the section on unordered selections with repetition: the number of solutions to the equation $x_1 + \ldots + x_n = k$, where $x_1, \ldots, x_n$ are non-negative integers, is exactly $\binom{n+k-1}{k}$.]

Consider first the case when the cells are required to be non-empty. In this case, a distribution of n unlabeled elements into k labeled cells so that none of the cells is empty can be seen as an sequence $x_1, \ldots, x_k$ of positive integers with sum n, that is, as an integer solution of the equation $x_1 + \ldots + x_k = n$ with $x_1, \ldots, x_k \geq 1$. The number of such solutions is the same as the number of non-negative solutions to $y_1 + \ldots + y_k = n - k$, which is $\binom{n-k+k-1}{n-k} = \binom{n-1}{k-1}$.

If empty cells are allowed, then the number of such distributions equals the number of non-negative integer solutions to the equation $x_1 + \ldots + x_k = n$, which is $\binom{n+k-1}{n}$.

6 Introduction to Designs

We introduce the idea of a balanced incomplete block design – a highly regular family of finite sets – and look at some special families of such designs, namely finite projective planes, affine planes, and Steiner triple systems.

Example. *Seven golfers are to spend a week's holiday at a seaside town which has two splendid golf courses. They decide that each should play a round of golf on each of the seven days. They also decide that on each day they should split into two groups, one of size 3 to play on one course and the other of size 4 to play on the other course. Can the*

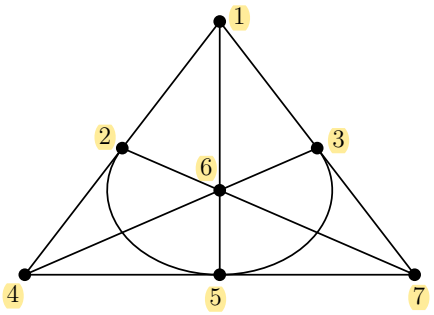
groups be arranged so that each pair of golfers plays together in a group of 3 *the same number of times, and each pair plays together in a group of* 4 *the same number of times?*

Here is one solution: the groups for each day are shown. It can be easily checked that each pair plays together once in a group of 3 and twice in a group of 4.

Day 1	$\{1,2,4\}$	$\{3,5,6,7\}$
Day 2	$\{2,3,5\}$	$\{4,6,7,1\}$
Day 3	$\{3,4,6\}$	$\{5,7,1,2\}$
Day 4	$\{4,5,7\}$	$\{6,1,2,3\}$
Day 5	$\{5,6,1\}$	$\{7,2,3,4\}$
Day 6	$\{6,7,2\}$	$\{1,3,4,5\}$
Day 7	$\{7,1,3\}$	$\{2,4,5,6\}$

▲

What we have done in the above example is to make use of the configuration known as the **Fano plane** (or the **seven-point plane**):



There are seven points and seven lines, with each line containing three points, and each pair of points being in exactly one line. The groups of size 4 are the **complements** of the lines of this configuration.

Example. The following subsets of $\{1,\ldots,6\}$ have the property that each subset has 3 elements and each pair of elements occurs in two of the subsets:

$$\{1,2,3\},\{1,2,4\},\{1,3,5\},\{1,4,6\},\{1,5,6\},$$

$$\{2,3,6\},\{2,4,5\},\{2,5,6\},\{3,4,5\},\{3,4,6\}.$$

This example was given by the statistician Frank Yates in 1936 in a paper which discussed the use of balanced designs in the construction of agricultural experiments. ▲

Definition. A (v,k,λ) **design** is a collection of k-element subsets (called **blocks**) of a v-element set S, where $k<v$, such that each pair of elements of S occur together in exactly λ blocks. Such a design is also known as a **balanced incomplete block design** (BIBD).

The adjective "balanced" refers to the existence of λ, and "incomplete" refers to the requirement that $k < v$ (so that no block contains all the elements).

Examples of balanced designs:

1. The Fano plane is a $(7, 3, 1)$ design.
2. The last example above is a $(6, 3, 2)$ design.
3. League schedules. The games of a league schedule for $2n$ teams form a $(2n, 2, 1)$ design; if each team plays each other twice in a season, the games form a $(2n, 2, 2)$ design.
4. An affine plane of order n is a $(n^2, n, 1)$ design.

Definition. An **affine plane of order** n is a collection of $n(n+1)$ subsets (blocks) of a set of size n^2 such that:

(i) each block contains n elements,

(ii) each element is in $n+1$ blocks,

(iii) each pair of elements lies in exactly one block,

(iv) each pair of blocks intersect in at most one element.

Compare the elements with points, and the blocks with lines in ordinary geometry. Property (iii) corresponds to the fact that any two points determine a unique line, and (iv) corresponds to the fact that any two lines intersect in at most one point.

In particular, an affine plane of order 3 is a $(9, 3, 1)$ design. It consists of 12 blocks of size 3 such that every pair of elements occur together once in a block:

$$\{1,2,3\},\{4,5,6\},\{7,8,9\},$$
$$\{1,4,7\},\{2,5,8\},\{3,6,9\},$$
$$\{1,6,8\},\{2,4,9\},\{3,5,7\},$$
$$\{1,5,9\},\{2,6,7\},\{3,4,8\}.$$

Block designs with $k = 3$ and $\lambda = 1$ were among the first designs to be studied.

Definition. A $(v, 3, 1)$ design is called a **Steiner triple system** (STS) of order v and is denoted by STS(v).

Examples. The Fano plane is an STS(7).

There are trivial Steiner triple systems of order 0 (no points or triples), 1 (a single point, no triples), and 3 (three points forming a triple).

The affine plane of order 3 is an STS(9).

Kirkman's schoolgirls.

> *Fifteen schoolgirls walk each day in five groups of three. Arrange the girls' walks for a week so that, in that time, each pair of girls walks together in a group just once.*

DISCUSSION. If it is possible at all, seven days will be required. For any given girl must walk once with each of the other fourteen; and each day she walks with two others. However, showing that the walks are actually possible requires more argument. The question was posed and solved by Kirkman in 1850. The same question could be asked for other numbers of girls. Only in 1967 did Ray-Chauduri and Wilson show that solutions exist for any number of girls congruent to 3 modulo 6.

It is easy to see that STS(9) solves Kirkman's problem for nine schoolgirls, walking for four days. *(Nine schoolgirls walk each day in three groups of three. Arrange the girls' walks for four days so that, in that time, each pair of girls walks together in a group just once.) The walking scheme is:*

$$\begin{aligned} \textit{Day 1}: &\quad \{1,2,3\},\{4,5,6\},\{7,8,9\}\,,\\ \textit{Day 2}: &\quad \{1,4,7\},\{2,5,8\},\{3,6,9\}\,,\\ \textit{Day 3}: &\quad \{1,6,8\},\{2,4,9\},\{3,5,7\}\,,\\ \textit{Day 4}: &\quad \{1,5,9\},\{2,6,7\},\{3,4,8\}\,. \end{aligned}$$

▲

Exercise: Verify that there are no Steiner triple systems of orders 2, 4, 5, or 6.

To prove, more generally, that Steiner triple systems can exist only for certain orders, we first obtain the following general result.

Theorem. *Suppose that a (v,k,λ) design with $k>1$ has b blocks. Then each element occurs in precisely r blocks, where*

$$\lambda(v-1)=r(k-1) \quad \textit{and} \quad bk=vr\,.$$

Proof. Choose any element x, and suppose it occurs in r blocks. In each of these r blocks x makes a pair with $k-1$ other elements; so altogether there are $r(k-1)$ pairs in the blocks involving x. But x is paired with each of the $v-1$ other elements λ times, so the number of pairs involving x is also $\lambda(v-1)$. So $\lambda(v-1)=r(k-1)$. This shows that r is independent of the choice of x, since it is uniquely determined by v, k, and λ.

To prove that $bk=vr$, note first that each block has k elements, and so the b blocks contain bk elements altogether (including repetitions). But each element x occurs r times in the blocks, so we must have $bk=vr$. □

Example. In an affine plane of order n, i.e., a $(n^2,n,1)$ design, we have $1\cdot(n^2-1)=(n-1)r$, so $r=n+1$. Also, $bn=n^2r$, so $b=n(n+1)=n^2+n$. ▲

Example. No $(11,6,2)$ design can exist, since it would require $2(11-1)=5r$, i.e., $r=4$, and $6b=44$, which is clearly impossible. ▲

Theorem. *A STS(v) can exist only if $v \equiv 1$ or $3 \pmod 6$.*

Proof. Suppose a $(v, 3, 1)$ design exists. Then $v - 1 = 2r$ and $3b = vr$, so that $v = 2r + 1$ (which is odd) and $b = \frac{1}{6}v(v-1)$. If $v = 6u + 5$, then $b = \frac{1}{6}(6u+5)(6u+4)$, which is not an integer; so we must have $v \equiv 1$ or $3 \pmod 6$. □

Note that $v = 7$ and 9, already dealt with, are of this form. *Steiner systems are so named because Steiner discussed them in an 1853 paper, having come across them in a geometrical setting. But it had already been shown by Kirkman in 1847 that not only was the condition $v \equiv 1$ or $3 \pmod 6$ necessary, but it was also sufficient. So STS(v) exists if and only if $v \equiv 1$ or $3 \pmod 6$. (Contrary to the special cases of STS's, there is no hope of deciding the values of the parameters (v, k, λ) for which a (v, k, λ) design exists.)*

Example. The sets

$$\{1, 2, 5\}, \{2, 3, 6\}, \ldots, \{9, 10, 13\}, \{10, 11, 1\}, \ldots, \{13, 1, 4\}$$

and

$$\{1, 3, 9\}, \{2, 4, 10\}, \ldots, \{5, 7, 13\}, \{6, 8, 1\}, \ldots, \{13, 2, 8\}$$

form a STS(13). Note that the blocks are obtained from $\{1, 2, 5\}$ and $\{1, 3, 9\}$ by adding 1 successively to each element, and working modulo 13. This is similar to the STS(7) (the Fano plane), which is obtained from the initial block $\{1, 2, 4\}$ and working modulo 7. (The unifying concepts behind all these examples are the so-called **difference sets**.) ▲

Further progress on designs is assisted by the representation of designs by matrices.

Definition. The **incidence matrix** of a (v, k, λ) design with b blocks is the $b \times v$ matrix $A = (a_{ij})$ defined by

$$a_{ij} = \begin{cases} 1, & \text{if the } i\text{th block contains the } j\text{th element;} \\ 0, & \text{otherwise.} \end{cases}$$

For example, the incidence matrix of the Fano plane is:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The first row has 1 in positions 1, 2, 4 since the first block is $\{1, 2, 4\}$. Note that the rows correspond to the blocks and the columns correspond to elements. Note also that the matrix A depends on the order in which the blocks and the elements are taken. However, it turns out that the important properties of A do not depend on the particular orders chosen.

Lemma. *If A is the incidence matrix of a (v, k, λ) design, then*

$$A^T A = (r - \lambda)I + \lambda J\,,$$

where r is the number of blocks containing a given point, I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix with every entry equal to 1.

Proof. The (i, j)th entry of $A^T A$ is the dot product of the ith row of A^T and the jth column of A, that is, of the ith and jth columns of A. Thus the (i, i) diagonal entry is the dot product of the ith column of A with itself, and so is the number of 1s in the ith column. But this is just the number of blocks containing the ith element, which is r.

If $i \neq j$, the dot product of the ith and jth columns of A is just the number of places in which both columns have a 1. This is the number of blocks containing both the ith and the jth elements, which is λ. So all diagonal entries of $A^T A$ are r, and all non-diagonal entries of $A^T A$ are λ. This property also holds for the matrix $(r - \lambda)I + \lambda J$. □

An important consequence of this result is the fact that a (v, k, λ) design contains at least as many blocks as elements. This result was first obtained by the statistician R. A. Fisher in 1940.

Remark: Historically, the notion of designs first arose in statistical design. Imagine that we are testing a number v of varieties of fertilizer. In each experimental trial, we can take k of these varieties and compare them. In order to evaluate the results, it is desirable that each pair of varieties should be compared in the same number (say, λ) of trials. So the experimental design should be a (v, k, λ) design. Fisher's result brings bad news for statisticians: it shows that, to achieve balance between treatments, at least as many trials are required as the number of variables being tested.

Theorem (Fisher's Inequality)**.** *In every (v, k, λ) design with b blocks, we have $b \geq v$.*

Proof. We give a matrix proof, using the above lemma and basic properties of determinants. (Purely combinatorial proofs are also known.)

Let A be the incidence matrix of the design. Then, denoting the determinant of a matrix M by $|M|$, we have:

$$\left|A^T A\right| = \begin{vmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \vdots & & & & \\ \lambda & \lambda & \lambda & \dots & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda - r & r - \lambda & 0 & \dots & 0 \\ \lambda - r & 0 & r - \lambda & \dots & 0 \\ \vdots & & & & \\ \lambda - r & 0 & 0 & \dots & r - \lambda \end{vmatrix},$$

by subtracting the first row from each of the other rows. We now add to the first column the sum of all the other columns to obtain

$$\begin{aligned} \left|A^T A\right| &= \begin{vmatrix} r + (v-1)\lambda & \lambda & \lambda & \dots & \lambda \\ 0 & r - \lambda & 0 & \dots & 0 \\ 0 & 0 & r - \lambda & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & r - \lambda \end{vmatrix} \\ &= (r + (v-1)\lambda)(r - \lambda)^{v-1} \\ &= rk(r - \lambda)^{v-1}\,, \end{aligned}$$

since $r + (v-1)\lambda = r + r(k-1) = rk$. The inequality $k < v$ implies $r > \lambda$, since $(v-1)\lambda = (k-1)r$, and so $|A^TA| \neq 0$. Thus, A^TA is an invertible $v \times v$ matrix and its rank $r(A^TA)$ must be v. But $r(A^TA) \leq r(A)$ and since A has b rows, we have $r(A) \leq b$. It follows that $v \leq b$, as required. □

Example. No $(25, 10, 3)$ design can exist. If it did, then $24 \cdot 3 = 9 \cdot r$ and $10b = 25r$, hence $r = 8$ and $b = 20$. But this gives $b < v$. ▲

7 Graphs

Graphs describe the connectedness of systems; typically, they model transport or communication systems, electrical networks, etc. Graphs can also be used to model 'incompatibility', to model problems such as the following one:

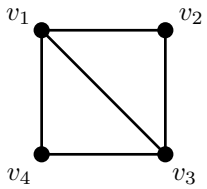
Suppose that radio frequencies are being allocated to a number of transmitters. Some pairs of transmitters are so close that their transmissions would interfere, and they must be allocated different frequencies. How many frequencies are required?

Remark. This chapter is based on Chapters 11 and 18 of Cameron [5], with occasional additions from Anderson [3]. There are some slight terminological differences from Cameron's exposition, as he uses some non-standard terminology.[5]

7.1 Definitions

A **(simple) graph** is a pair (V, E) where V is a set of **vertices** and E is a set of 2-element subsets of V called **edges**.

Example.
$V = \{v_1, v_2, v_3, v_4\}$, $E = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_3, v_4\}\}$.



▲

Sometimes it is necessary to broaden the definition. We may want to allow:

- **loops**, which are edges joining a vertex to itself,
- **multiple edges**, more than one edge between the same pair of vertices, and

[5] The differences are in the definition of: a closed walk (he requires it to have an edge), a path (he allows it to be a closed walk). What we call a cycle he calls a circuit. Also he uses the term *valency* for the degree of a vertex, *edge-cover* for a vertex cover, and *coclique* for independent set.

- **directed edges**, which have an orientation so that they go **from** one vertex **to** another. (Directed edges could arise in modeling traffic flow in a town with some one-way streets, for example.)

A graph with some or all of these features is called a **(general) graph**. If a graph has directed edges, it is a **directed graph** or **digraph**. If a graph is allowed to have multiple edges, it is a **multigraph**. Directed edges are easily represented as ordered pairs rather than 2-subsets of vertices.

In terms of relations:

- a simple graph with vertex set V = an irreflexive and symmetric binary relation on V (called the 'adjacency' relation);

  relaxing these two conditions allows loops and directed edges, respectively,

- a directed graph = a binary relation on a set V.

We will mostly consider only undirected graphs without loops. Sometimes we will need to allow multiple edges and in two sections we will study digraphs.

In a simple graph, we say that vertices x and y are **adjacent** if $\{x, y\}$ is an edge, otherwise, they are **non-adjacent**. Adjacent vertices x and y are **endpoints** of edge $\{x, y\}$.

For a graph G with vertex set V and edge set E, we will write $G = (V, E)$ and denote by $V(G)$ the vertex set and by $E(G)$ the edge set of G.

An important family of graphs are **complete graphs**, graphs in which every pair of vertices is an edge. The complete graph on n vertices will be denoted by K_n.

Note that K_n has exactly $\binom{n}{2}$ edges.

A **subgraph** of a graph $G = (V, E)$ is a graph $G' = (V', E')$ such that $V' \subseteq V$ and $E' \subseteq E$. Note that, in this case, for every edge $e \in E'$, it must hold that both vertices of e lie in V'. Two kinds of subgraphs are particularly important:

- An **induced subgraph** of G is a subgraph $G' = (V', E')$ whose edge set consists of *all* the edges of G that have both endpoints in V'. We say that G' is the **subgraph of G induced by V'** and write $G' = G[V']$.

- A **spanning subgraph** of G is one whose vertex set is the same as that of G.

Thus, for example, every graph with at most n vertices is a subgraph of K_n, and every graph with exactly n vertices is a spanning subgraph of K_n; but the only induced subgraphs of K_n are complete graphs.

Now we have to consider various kinds of routes in graphs. A **walk** in a graph is a sequence

$$(v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$$

where e_i is the edge $\{v_{i-1}, v_i\}$ for $i = 1, \ldots, n$. We say that it is a walk **from** v_0 **to** v_n. The **length** of the walk is the number n of edges in the sequence (or one less than the

number of vertices). A walk is **closed** if $v_n = v_0$. Note that there are no restrictions; when walking, we may retrace our steps arbitrarily.

In a simple graph, the edges in a walk are uniquely determined by the vertices; so we often speak of the walk $(v_0, v_1, \ldots, v_n)$, defined by the condition that v_{i-1} and v_i are adjacent for $i = 1, \ldots, n$.

A **trail** is a walk with all its edges distinct; a **path** is a walk with all its vertices distinct. A **cycle** is a closed walk with $n > 0$, all its vertices distinct (except for $v_n = v_0$) and all its edges distinct.

Proposition. *For any two vertices x, y of a graph G, the conditions that there exists a walk, trail, or path from x to y are all equivalent.*

Proof. Since a path is a trail and a trail is a walk, we only need to prove that the existence of a walk from x to y implies the existence of a path from x to y. Let W be a shortest walk from x to y. If W is a path, there is nothing to prove. Otherwise, W has a repeated vertex. But then, W has a subsequence $(v, \ldots, v)$, which can be replaced by a single v to obtain a shorter walk, contradicting the choice of W. □

Now define a relation $\equiv$ on the vertex set V by the rule: $x \equiv y$ if there is a path (or trail, or walk) from x to y. Then, $\equiv$ is an equivalence relation on V:

- it is reflexive since there is a walk of length 0 from x to x,
- it is symmetric since reversing a walk from x to y gives a walk from y to x,
- it is transitive since following a walk from x to y and a walk from y to z gives a walk from x to z.

The equivalence relation, of course, defines a partition of the vertex set of G. We define the **connected components** (or, for short, the **components**) of G to be the subgraphs induced by the equivalence classes of the relation $\equiv$. Note that no edge joins vertices of different equivalence classes; so the edge set of G is partitioned into edge sets of its components.

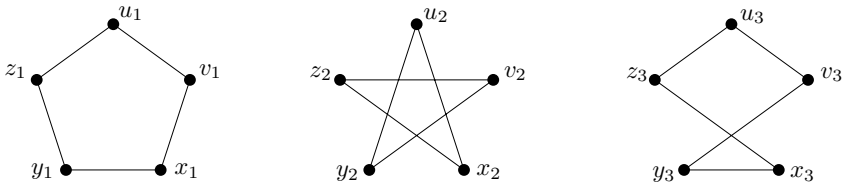
A graph is **connected** if it has just one component. Note that any connected component of G is a connected graph.

The **degree** of a vertex x in a graph G is the number of edges containing x. In a directed graph, we have to distinguish between the **out-degree** of a vertex (the number of directed edges starting at that vertex) and its **in-degree** (the number of edges ending there). If every vertex of the graph has the same degree, the graph is called **regular**; if the common degree is d, the graph is **d-regular**.

Often we will modify a graph G by removing a vertex v and all edges containing it, or by removing an edge e, or by adding an edge e joining two vertices not previously joined. We use the shorthand notations $G - v$, $G - e$, $G + e$ for the results of these operations.

7.2 Isomorphism of graphs

Suppose you are asked to give an example of three graphs with 5 vertices and 5 edges. Would the following three graphs be an acceptable answer to this question?



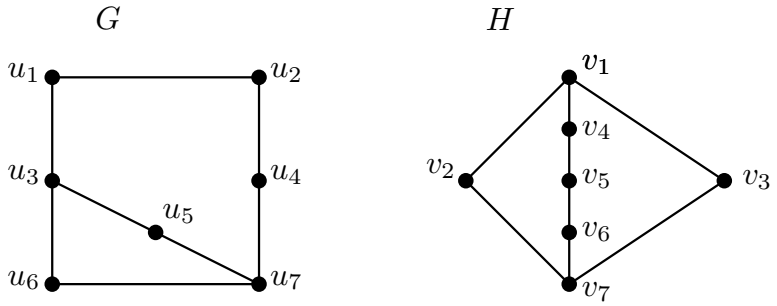
Probably not, as the graphs differ only in the way they are labeled.

Two (simple) graphs $G = (V, E)$ and $G' = (V', E')$ are said to be **isomorphic** (to each other) if there is a bijection $f : V \to V'$ such that

$$\{x, y\} \in E \quad \text{if and only if} \quad \{f(x), f(y)\} \in E'$$

holds for all $x, y \in V$, $x \neq y$. Such an f is called an **isomorphism** from G to G'. The fact that G and G' are isomorphic is written $G \cong G'$.

Example. The following two graphs are isomorphic.



An isomorphism f from G to H is given by

$$f(u_1) = v_4, \quad f(u_2) = v_5, \quad f(u_3) = v_1,$$

$$f(u_4) = v_6, \quad f(u_5) = v_2, \quad f(u_6) = v_3, \quad f(u_7) = v_7.$$

▲

An isomorphism is required to map adjacent vertex pairs to adjacent vertex pairs and nonadjacent vertex pairs to nonadjacent vertex pairs – it can be thought of as "renaming the vertices" of a graph.

The isomorphism relation $\cong$ is an equivalence relation, on any set of graphs.

In general, it is not easy to determine if two graphs are isomorphic. Some necessary conditions are easy to obtain.

Theorem. *If two graphs $G = (V, E)$ and $G' = (V', E')$ are isomorphic, then $|V| = |V'|$, $|E| = |E'|$, and the multisets of vertex degrees of G and of G' are the same.*

Proof. Let $f : V \to V'$ be an isomorphism from G to G'. Since f is bijective, we have $|V| = |V'|$. To see that $|E| = |E'|$, note that the mapping g, defined by setting

$$g(\{x, y\}) = \{f(x), f(y)\}$$

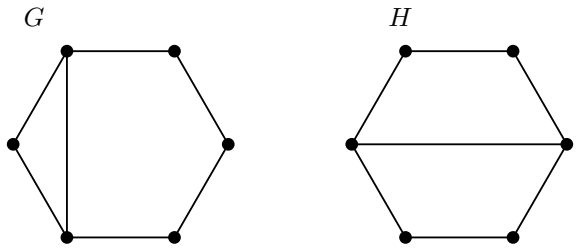
for all $\{x, y\} \in E$, is a bijection from E to E'.

Finally, let x be a vertex of G and let $k = d_G(v)$. Then x is adjacent to k vertices, say $x_1, \ldots, x_k$. But then $f(x)$ is adjacent to $f(x_1), \ldots, f(x_k)$ and non-adjacent to any other vertex of G'. It follows that $d_{G'}(f(x)) = d_G(x)$. □

Example. The graphs from the figure above both have 7 vertices, 8 edges, and multiset of vertex degrees $[3, 3, 2, 2, 2, 2, 2]$. ▲

However, if two graphs have the same multisets of vertex degrees, they are not necessarily isomorphic.

Example. Consider the graphs in the following figure.



They have vertex degrees $[3, 3, 2, 2, 2, 2]$. But they are not isomorphic. Graph G contains a cycle of length 3, while graph H does not contain such a cycle. ▲

We can prove that two graphs are isomorphic by showing an isomorphism from one to the other.

We can prove that two graphs are not isomorphic by exhibiting some structural property in which they differ.

7.3 Trees and Forests

A **tree** is a connected graph without cycles. A graph without cycles is called a **forest**. (Its connected components are trees.)

We might expect that a connected graph has 'many' edges, and a graph without cycles has 'few'. The next result shows that trees are extremal for both properties.

Theorem. *(a) A connected graph with n vertices has at least $n - 1$ edges, with equality if and only if it is a tree.*

(b) A forest with n vertices and k components has $n - k$ edges. Thus, a forest has at most $n - 1$ edges, with equality if and only if it is a tree.

Proof. We show first that a tree has $n - 1$ edges. This is proved by induction; it is clear for $n = 1$. The inductive step depends on the following fact:

A tree with more than one vertex has a vertex of degree 1.

Since a tree is connected, it has no vertices of degree 0 (if $n > 1$), so, arguing by contradiction, we can assume that every vertex has degree at least 2. We can now form a walk of length n in which any two consecutive edges are distinct. Such a walk must return to a vertex it has visited previously; so there is a cycle, and we have arrived at a contradiction. The assertion is proved.

Now let v be a vertex in the tree T such that v has degree 1. Then, $T - v$ has $n - 1$ vertices and contains no cycles. We claim that $T - v$ is connected. This holds because a path in T between two vertices $x, y \neq v$ cannot pass through v. Thus $T - v$ is a tree. By the induction hypothesis, it has $n - 2$ edges; so T has $n - 1$ edges.

Now part (b) of the theorem follows easily. For let F be a forest with n vertices and k components $T_1, \ldots, T_k$, with $a_1, \ldots, a_k$ vertices respectively. Then $\sum_{i=1}^{k} a_i = n$. Now T_i is a tree, and so has $a_i - 1$ edges. So F has $\sum_{i=1}^{k}(a_i - 1) = n - k$ edges.

To prove (a), let G be any connected graph with n vertices and suppose that G is not a tree. Then G contains a cycle C. Let e be an edge in this cycle and $G' = G - e$ the graph obtained by removing e. Then G' is still connected. For, if a path from x to y in G uses the edge e, then there is a walk from x to y not using e. (Instead of using e, we traverse the cycle the other way.) Repeating this procedure, we must reach a tree after, say r, steps. Since $r \geq 1$ edges are removed, G has $n - 1 + r$ edges altogether. □

Let G be a graph. A **spanning forest** is a spanning subgraph of G (consisting of all the vertices and some of the edges of G) that is a forest. A **spanning tree** is defined similarly.

Corollary. *Every connected graph has a spanning tree.*

This follows from the argument for part (a) of the theorem above; by removing edges from G, we can obtain a spanning tree.

There is a great deal of freedom in creating spanning trees. The following theorem establishes the number of spanning trees in a complete graph.

Theorem (Cayley's Theorem, 1889)**.** *The complete graph K_n with vertex set $\{1, \ldots, n\}$ has n^{n-2} spanning trees.*

Equivalently: there are n^{n-2} trees with vertex set $\{1, \ldots, n\}$.
(We omit the proof. See [5, p. 38-39].)

7.4 Minimum Spanning Trees

Suppose that n towns are to be linked by a telecommunication network. For each pair of towns, the cost of installing the cable between these two towns is known. What is the most economical way of connecting all the towns?

This is known as the **minimum connector** problem. The data can be regarded as an edge-weighted graph. (As described, the graph G in question is complete, but this is not essential. We could suppose that, for various reasons, it is impossible or uneconomic to connect certain pairs of towns directly.)

The solution to the problem will be a connected spanning subgraph H of the graph G of minimum total weight (that is, the sum of the weights of the edges of H is as small

as possible). Clearly, H must be a tree; if not, then edges could be deleted, reducing the weight without disconnecting it. The problem is solved by a simple algorithm called the **greedy algorithm**, which says: at each stage, build the cheapest link that joins two towns not already connected by a path. Formally:

Greedy Algorithm for minimum connector

Let $G = (V, E)$ be a connected graph, w a non-negative weight function on E.
Set $S = \emptyset$.
WHILE (V, S) is not connected, choose an edge e of minimal weight subject to joining vertices in different components, and add e to S.
RETURN (V, S).

Theorem (Kruskal, 1956)**.** *The Greedy Algorithm produces a minimum-weight spanning tree of G.*

Proof. First we show that the algorithm produces a spanning tree. To this end, we argue that the choice of e is always possible and its addition creates no cycle. Let Y be the vertex set of a connected component of (V, S) and $Z = V \setminus Y$. Choose vertices $y \in Y$ and $z \in Z$. In G, there is a path from y to z; some edge in this path must cross from Y to Z, and this is a suitable choice for e. Consider now such an edge and suppose that $(V, S) + e$ contains a cycle. If we start, say in Y, and follow this cycle, at some moment we cross into Z by using the edge e; then there is no way to return to Y to complete the cycle without reusing e; a contradiction.

It remains to show that the tree T produced by the algorithm has minimum weight. Let $e_1, \ldots, e_{n-1}$ be the edges in S, in the order in which the Greedy Algorithm chooses them. Note that

$$w(e_1) \leq \ldots \leq w(e_{n-1}) \,,$$

since if $w(e_j) < w(e_i)$ for $j > i$, then at the i^{th} stage, e_j would join vertices in different components, and should have been chosen in preference to e_i.

Suppose, for a contradiction, that there is a spanning tree of smaller weight, with edges $f_1, \ldots, f_{n-1}$, ordered so that $w(f_1) \leq \ldots \leq w(f_{n-1})$. Thus,

$$\sum_{i=1}^{n-1} w(f_i) < \sum_{i=1}^{n-1} w(e_i) \,.$$

Choose k as small as possible such that

$$\sum_{i=1}^{k} w(f_i) < \sum_{i=1}^{k} w(e_i) \,.$$

Note that $k > 1$ since the greedy algorithm chooses first an edge of smallest weight. Then we have

$$\sum_{i=1}^{k-1} w(f_i) \geq \sum_{i=1}^{k-1} w(e_i) \,,$$

hence

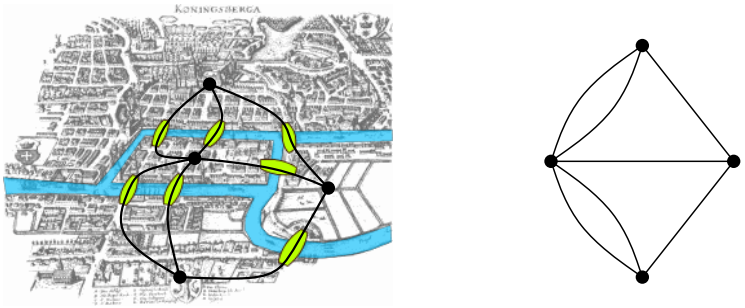
$$w(f_1) \leq \ldots \leq w(f_k) < w(e_k)\,.$$

(If $w(f_k) \geq w(e_k)$, then we would have $\sum_{i=1}^{k} w(f_i) \geq \sum_{i=1}^{k} w(e_i)$.) Now, at stage k, the greedy algorithm chooses e_k, and not any of the edges $f_1, \ldots, f_k$ of strictly smaller weight; so all of these edges must fail the condition that they join vertices in different components of (V, S) where $S = \{e_1, \ldots, e_{k-1}\}$. It follows that the vertex sets of connected components of (V, S'), where $S' = \{f_1, \ldots, f_k\}$, are subsets of those of (V, S); in particular, (V, S') has at least as many components as (V, S). But this is a contradiction, since both (V, S) and (V, S') are forests, and their numbers of components are $n-(k-1)$ and $n-k$, respectively. □

In general, the **greedy algorithm** refers to any algorithm for constructing an object in stages, where at each stage we make the choice that locally optimizes some 'objective function', subject to the condition that we move closer to our final goal. Obviously, this short-sighted local optimization does not usually produce the best overall solution. It is quite remarkable that it does so in this case!

7.5 Eulerian Graphs

One's first encounter with graph theory often takes the form of the familiar puzzle 'trace this figure without taking your pencil off the paper'. Euler's experience was similar. He showed that it was not possible to walk around the town of Königsberg crossing each of its seven bridges just once. This demonstration is commonly taken as the starting point of graph theory.



Source: wikipedia

In problems of this sort, we are required to traverse every edge of a graph once, but we may revisit a vertex. So the appropriate type of route is a trail. We define an **Eulerian trail** in a graph to be a trail that includes every edge. An **Eulerian circuit** is a closed Eulerian trail. Clearly an **isolated vertex** (lying on no edges) has no effect, and may be deleted. Also, it is convenient here to work with **multigraphs**, where two vertices may be joined by more than one edge. Euler's result can be stated as follows:

Theorem (Euler's Theorem). *(a) A multigraph with no isolated vertices has an Eulerian circuit if and only if it is connected and every vertex has even degree.*

(b) A multigraph with no isolated vertices has a non-closed Eulerian trail if and only if it is connected and has exactly two vertices of odd degree.

Proof. Necessity. It is obvious that a graph with an Eulerian trail must be connected if no vertex is isolated. The other conditions are also necessary. For consider a graph with an Eulerian circuit. As we follow the circuit, each time we reach a vertex by an edge, we must leave it by a different edge, using up two edges through that vertex. Since every edge is used, the degree must be even. The same applies at the initial vertex of an Eulerian circuit, since the first and the last edge of the circuit play the same role. For a non-closed Eulerian trail, however, the degrees of the first and the last vertices are odd, since the first and last edges are 'unpaired'.

Remark: recall the Handshaking Lemma from the section on the Double Counting principle: "At a convention, the number of delegates who shake hands an odd number of times is even." In terms of multigraphs, the number of vertices of odd degree in a graph is even. So, if there is a vertex of odd degree, then there are at least two.

Sufficiency. We have to construct Eulerian trails in graphs satisfying the conditions. The argument is, in some sense, algorithmic.

Se let $G = (V, E)$ be a graph satisfying the condition of either (a) or (b). In case (a), let v be any vertex; in (b), let v be one of the vertices of odd degree. Now follow a trail from v, never reusing an edge, for as long as possible. Let S be the set of edges in this trail.

For any vertex x other than v (in case (a)) or the other vertex of odd degree (in case (b)), whenever the trail reaches x, there are an odd number of edges through x not yet used. This is because we reached x along an edge, and previous visits accounted for an even number of edges (except for v, where previous visits accounted for an odd number of edges). Thus, we don't get stuck at x since there is always an edge by which we can leave. So the trail must end at v (in case (a)) or the other vertex of odd degree (in case (b)).

If $S = E$, we have constructed an Eulerian trail, and we are finished. So suppose not. There must be a vertex u lying on both an edge in S and an edge not in S. For otherwise, the sets X and Y of vertices lying on edges in S and on edges not in S respectively, form a partition of V; and no edge joins vertices in different parts, contradicting connectedness.

Moreover, in the graph $(V, E \setminus S)$, every vertex has even degree. So, starting at u and using only edges of $E \setminus S$, we can find a closed trail, by the same argument as before. Now we can 'splice in' this trail to produce a longer one: start at v and follow the old trail to u; then traverse the new trail; then continue along the old trail.

After a finite number of applications of this construction, we must arrive at an Eulerian trail of the type desired. □

Note that, in case (b), any Eulerian trail must start at one vertex of odd degree and finish at the other–a fact well known to anyone who has tried a 'trace without lifting the pencil' puzzle.

The map of Königsberg is easily converted into a multigraph whose edges are the bridges. All four vertices have odd degree, so there is no Eulerian trail.

7.6 Hamiltonian Graphs

There are natural analogues of Eulerian trails and circuits for vertices:

- A **Hamiltonian path** is a path that passes through each vertex.
- A **Hamiltonian cycle** is a cycle that passes through each vertex.

A graph possessing a Hamiltonian cycle is said to be **Hamiltonian**. Since multiple edges are irrelevant here, we assume all graphs in this section to be simple.

For $n > 2$, there is a unique connected 2-regular graph on n vertices. This is the so-called **n-cycle**, C_n. It can be represented as the vertices and edges of an n-gon. A graph is Hamiltonian if and only if it has a cycle as a spanning subgraph.

Hamiltonian graphs are much harder to deal with than Eulerian ones. There is no simple necessary and sufficient condition for a graph to be Hamiltonian, and it is notoriously difficult to decide this question for a given graph of even moderate size. A lot of effort has gone into proving *sufficient conditions*. As an example, we prove one of the simplest of these conditions.

Theorem (Ore's Theorem)**.** *Let G be a graph with $n \geq 3$ vertices, and suppose that, for any two non-adjacent vertices x and y in G, the sum of their degrees is at least n. Then G is Hamiltonian.*

Proof. (In contrast with Euler's Theorem, the proof is non-constructive.) Arguing by contradiction, suppose that G is a graph that satisfies the hypothesis of Ore's Theorem but is not Hamiltonian. We may also suppose that G is *maximal* with these properties, that is, that the addition of any edge to G produces a Hamiltonian graph. We achieve this by adding new edges joining previously non-adjacent vertices as long as G remains non-Hamiltonian. Adding an edge does not decrease the degree of any vertex and does not create any new non-adjacent pair of vertices, so the degree condition remains true.

Since $n \geq 3$ and G is not Hamiltonian, G is not complete, so it has a non-adjacent pair of vertices x and y. Since G is maximal non-Hamiltonian, the graph obtained by adding the edge $e = \{x, y\}$ is Hamiltonian; and a Hamiltonian cycle in the graph must contain e. So G itself contains a Hamiltonian path

$$(x = v_1, e_2, v_2, \ldots, v_n = y)\,.$$

Now let A be the set of vertices of G adjacent to x; and let

$$B = \{v_i : v_{i-1} \text{ is adjacent to } y\}\,.$$

By assumption, $|A| + |B| \geq n$. But the vertex $v_1 = x$ doesn't belong to either A or B; so $|A \cup B| \leq n - 1$. It follows that $|A \cap B| \geq 1$ and so there is a vertex v_i lying in both A and B.

Now we obtain a contradiction by constructing a Hamiltonian cycle in G. Starting at $x = v_1$, we follow the path $v_2, v_3, \ldots$ until v_{i-1}. Now v_{i-1} is adjacent to y (since $v_i \in B$), so we go to $y = v_n$ as the next step. Then we follow the path backwards through v_{n-1} until v_i and then back to v_1 (this edge exists since $v_i \in A$). □

The result is best possible in some sense. Consider the graph with $2m+1$ vertices $x_1, \ldots, x_m, y_1, \ldots, y_{m+1}$, and having as edges all pairs $\{x_i, y_j\}$. (This is a **complete bipartite graph**.) It is not Hamiltonian: any edge crosses between sets $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_{m+1}\}$, so any cycle of odd length starting in X would have to finish in Y, therefore it would never close. But two non-adjacent vertices are both in X or both in Y, and the sum of their degrees is $2m+2 = n+1$ or $2m = n-1$ respectively.

7.7 Briefly about Digraphs

The most important variant of graphs consists of **directed graphs** or **digraphs**, where the edges are ordered pairs of vertices (rather than unordered pairs). Each edge (x, y) has an **initial vertex** (or: **tail**) x and a **terminal vertex** (or: **head**) y. Note that (x, y) and (y, x) are different edges.

With any digraph D is associated an ordinary (undirected) graph, the **underlying graph**: it has the same vertex set as D, and its edges are those of D without the order (that is, $\{x, y\}$ for each edge (x, y) of D). The underlying graph will fail to be simple if D contains two oppositely-directed edges (such as (x, y) and (y, x)). If the underlying graph is simple, then D is called an **oriented graph**.

The definitions of various types of routes in a digraph are the same as in a graph, with the important exception that the edges must be traversed in the correct direction: so, if

$$(v_0, e_1, v_1, \ldots, e_n, v_n)$$

is a walk, trail, or path, then e_i is the edge (v_{i-1}, v_i) for $i = 1, \ldots, n$. Just like in graphs, for any two distinct vertices x, y of a digraph, the conditions that there exists a walk, trail, or path from x to y are all equivalent.

The situation with connected components is different, however. If, as before, we let R be the relation defined by the rule that $(x, y) \in R$ if and only if there is a path (or a trail, or a walk) from x to y, then the relation R is reflexive and transitive, but not necessarily symmetric. Accordingly, we define two types of connectedness:

- the digraph D is **(weakly) connected** if its underlying graph is connected;
- D is **strongly connected** if, for any two vertices x and y, there is a path from x to y.

It is clear that a strongly connected digraph is weakly connected. The converse is false. (Examples?)

The definitions of Eulerian trail and circuit and of Hamiltonian path and cycle are just what you would expect. A digraph possessing a Hamiltonian cycle is obviously strongly connected; one with a Hamiltonian path is weakly (but not necessarily strongly) connected. Similar statements hold for Eulerian trails and circuits.

The analogue of Euler's theorem is the following:

Theorem. *A digraph with no isolated vertices has an Eulerian circuit if and only if it is weakly connected and the in-degree and the out-degree of any vertex are equal.*

Exercise:

1) Prove the above theorem.

2) Formulate and prove a necessary and sufficient condition for the existence of a non-closed Eulerian trail.

7.8 Hall's Theorem

In this section we will learn an important theorem, Hall's Theorem. The theorem is about *matchings in bipartite graphs*.

A graph $G = (V, E)$ is **bipartite** if there is a partition of the vertex set into two parts X and Y such that every edge has one end in X and one end in Y. Any such partition $\{X, Y\}$ is called a **bipartition** of G; sets X and Y are called **partite sets** (or simply **parts**).

Certainly not every graph is bipartite. For example, the 5-cycle C_5, with a cyclic order of vertices $v_1, \ldots, v_5$, is not bipartite. If C_5 were bipartite, then it would have a bipartition $\{X, Y\}$. Vertex v_1 must belong to either X or Y, say $v_1 \in X$. Since $\{v_1, v_2\}$ is an edge of C_5, it follows that $v_2 \in Y$. Since $\{v_2, v_3\}$ is an edge of C_5, it follows that $v_3 \in X$. Similarly, $v_4 \in Y$ and $v_5 \in X$. However, $v_1, v_5 \in X$ and $\{v_1, v_5\}$ is an edge of C_5. This is a contradiction.

In fact, no odd cycle (that is, C_n with n odd) is bipartite. More generally, any graph that contains an odd cycle is not bipartite. The converse is true as well: A graph is bipartite if and only if it contains no odd cycle.

To introduce the notion of a matching, consider the following situation.

The department has acquired 12 books on a variety of subjects to award 10 students who placed best at the University Programming Marathon (one book to each successful student). However, some of the students already have copies of some books and there are some books that certain students have no need for. The question is this: Is there a way of distributing 10 of the 12 books to the 10 students so that each student receives one of the books that he or she would like to have?

The answer to this problem may be 'no' even though there are more books than students. For example, there may be three or more books that no student wants. Also, perhaps there are four students only interested in the same three books, in which case it would be impossible to distribute four books to these four students.

This situation can be modeled by a graph G whose vertices are the students, say $s_1, \ldots, s_{10}$, and the books, say $b_1, \ldots, b_{12}$, where two vertices of G are adjacent if one of these vertices is a student and the other is a book that this student would like to have. Thus, G is a bipartite graph with parts S and B where $S = \{s_1, \ldots, s_{10}\}$ and $B = \{b_1, \ldots, b_{12}\}$. What we are seeking then is a set M of 10 edges in the graph G, no two of which have an endpoint in common. If such a set M exists, then each vertex s_i is an endpoint of exactly one edge in M.

There is a related mathematical question here. Let X and Y be two sets such that $|X| = 10$ and $|Y| = 12$. Does there exist an injective function $f : X \to Y$? Clearly,

the answer is yes. However, what if the image of each element of X cannot be just any element of Y? The image of each element of X is required to be an element of some prescribed subset of Y. Consequently, what we are asking is that if we know the sets of possible images of the elements of X, is there an injective function $f : X \to Y$ that satisfies these conditions?

Definition. In a graph G, a **matching** is a set of pairwise disjoint edges. The vertices that are endpoints of the edges of a matching M are **M-saturated**.

Thus the above problem asks whether a particular bipartite graph contains a matching saturating one part of the bipartition.

Given two vertices x and y in a graph G, we say that y is a **neighbor** of x if y is adjacent to x.

Let G be a bipartite graph with parts X and Y. A matching in G is a set $M = \{e_1, \ldots, e_k\}$ of edges, where $e_i = \{x_i, y_i\}$ for $1 \leq i \leq k$, such that $x_1, \ldots, x_k$ are k distinct vertices of X and $y_1, \ldots, y_k$ are k distinct vertices of Y. We say that M **matches** the set $\{x_1, \ldots, x_k\}$ to the set $\{y_1, \ldots, y_k\}$.

If a matching M saturates X, then for every $S \subseteq X$ there must be at least $|S|$ vertices that have neighbors in S, because the vertices matched to S must be chosen from that set. We use $N(S)$ to denote the set of vertices having a neighbor in S. Thus $|N(S)| \geq |S|$ is a necessary condition.

The graph G is said to satisfy **Hall's condition** if $|N(S)| \geq |S|$ for all $S \subseteq X$. Hall proved that this obvious necessary condition is also sufficient.

Theorem (Hall's Theorem - P. Hall, 1935)**.** *A bipartite graph G with parts X and Y has a matching that saturates X if and only if $|N(S)| \geq |S|$ for all $S \subseteq X$.*

Proof. Necessity. The $|S|$ vertices matched to S must lie in $N(S)$.

Sufficiency. We prove sufficiency using the principle of strong induction on the cardinality of X. Suppose first that Hall's condition is satisfied and $|X| = 1$. Since $|N(X)| \geq |X| = 1$, there is a vertex in Y adjacent to the vertex in X and so X can be matched to a subset of Y.

Assume, for an integer $k \geq 2$, that if G' is any bipartite graph with parts X' and Y' where $1 \leq |X'| < k$, that satisfies Hall's condition, then X' can be matched to a subset of Y'. Let G be a bipartite graph with parts X and Y, where $|X| = k$, such that Hall's condition is satisfied. We show that X can be matched to a subset of Y. We consider two cases.

Case 1. For every subset $S \subseteq X$ such that $1 \leq |S| < |X|$, we have $|N(S)| > |S|$.

Let $x \in X$. By assumption, x is adjacent to two or more vertices of Y. Let y be a vertex adjacent to x. Now let H be the bipartite induced subgraph of G with parts $X \setminus \{x\}$ and $Y \setminus \{y\}$. Then, for each subset S of $X \setminus \{x\}$, we have $|N(S)| \geq |S|$ in H. By the induction hypothesis, $X \setminus \{x\}$ can be matched to a subset of $Y \setminus \{y\}$. This matching together with the edge $\{x, y\}$ shows that X can be matched to a subset of Y in G.

Case 2. There exists a subset $S \subseteq X$ such that $1 \leq |S| < |X|$ and $|N(S)| = |S|$.

Let F be the bipartite induced subgraph of G with parts S and $N(S)$. Since Hall's condition is satisfied in F, it follows by the induction hypothesis that S can be matched

to a subset of $N(S)$. In fact, since $|N(S)| = |S|$, the set S must be matched to $N(S)$. Let M' be such a matching.

Next, consider the bipartite induced subgraph H of G with parts $X \setminus S$ and $Y \setminus N(S)$. Let T be a subset of $X \setminus S$ and let

$$T' = N(T) \cap (Y \setminus N(S)) .$$

We show that $|T| \leq |T|$. By assumption, $|N(S \cup T)| \geq |S \cup T|$. Hence

$$|N(S)| + |T'| = |N(S \cup T)| \geq |S| + |T| .$$

Since $|N(S)| = |S|$, it follows that $|T'| \geq |T|$. Thus Hall's condition is satisfied in H and so there is a matching M'' from $X \setminus S$ to $Y \setminus N(S)$. Therefore, $M' \cup M''$ is a matching saturating X in G. □

The original statement of Hall's Theorem was stated in the language of sets.

Let $A_1, \ldots, A_n$ be sets. A **system of distinct representatives** (SDR) for these sets is an n-tuple $(x_1, \ldots, x_n)$ of elements such that:

(a) $x_i \in A_i$ for $i = 1, \ldots, n$ (i.e., representatives);

(b) $x_i \neq x_j$ for $i \neq j$ (i.e., distinct).

For any set $J \subseteq \{1, \ldots, n\}$ of indices, we define

$$A(J) = \bigcup_{j \in J} A_j .$$

If the sets $A_1, \ldots, A_n$ have an SDR, then necessarily $|A(J)| \geq |J|$ for every set $J \subseteq \{1, \ldots, n\}$, since $A(J)$ contains the representative x_j of each set A_j for $j \in J$, and these representatives are all distinct. Hall's Theorem says that this necessary condition is also sufficient.

Theorem (Hall's Marriage Theorem)**.** *A family $(A_1, \ldots, A_n)$ of finite sets has a system of distinct representatives if and only if $|A(J)| \geq |J|$ for all $J \subseteq \{1, \ldots, n\}$.*

The name of the theorem is due to the following interpretation. Given a set of boys and a set of girls, each girl knowing a specified set of boys, it is possible for all the girls to marry boys if and only if any set of k girls know altogether at least k boys.

Proof. Let $\mathcal{F} = (A_1, \ldots, A_n)$ be a family of subsets of $\{1, \ldots, m\}$. We define the **incidence graph** G of $\mathcal{F}$ as follows. This is a bipartite graph with parts $X = \{A_1, \ldots, A_n\}$ and $Y = \{1, \ldots, m\}$; vertices $A_i \in X$ and $j \in Y$ are joined by an edge if and only if $j \in A_i$.

A matching in G is a set of pairwise disjoint edges $\{A_i, j\}$; thus, each element j lies in its corresponding set A_i, and the elements are all distinct, as are the sets. This is just a system of distinct representatives for a subfamily of $\mathcal{F}$. So $\mathcal{F}$ has an SDR if and only if there is a matching saturating X. Let $S \subseteq X$. Taking $J = \{j \in \{1, \ldots, n\} : A_j \in S\}$, we have $S = \{A_j : j \in J\}$. Moreover, $N(S) = \cup_{j \in J} A_j = A(J)$. Therefore, the condition $|A(J)| \geq |J|$ is equivalent to the condition $|N(S)| \geq |S|$, and the theorem follows from Hall's theorem for graphs. □

Corollary. *Let $\mathcal{F} = (A_1, \ldots, A_n)$ be a family of subsets of a set S such that, for some k:*

(i) $|A_i| = k$ for each i,

(ii) each element of S occurs in exactly k of the A_is.

Then $\mathcal{F}$ has an SDR.

Proof. Let $J \subseteq \{1, \ldots, n\}$ and let $p = |J|$. Including repetitions, the union $A(J)$ contains pk elements. But, by (ii), no element can occur in this union more than k times; so the number of distinct elements of the union is at least $\frac{pk}{k} = p = |J|$. Thus, the condition from Hall's Marriage Theorem is satisfied. □

7.9 A Detour to Latin Squares

A **Latin square of order** n is an $n \times n$ array in which each row and each column contains each of the n given symbols exactly once. For example, here is a Latin square of order 4 over the set $\{1, 2, 3, 4\}$:

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}.$$

The above construction generalizes, so the existence is not a problem. Latin squares are useful in statistical experimental designs but they are also used in many different areas of mathematics. (For example, a group table (= multiplication table of a finite group) is a Latin square.)

Latin squares can be constructed one row at the time. Given the first row, the second row has to be a derangement of the first; but, in general, if the first r rows of a hoped-for $n \times n$ Latin square have been constructed, is it always possible to find a suitable $(r+1)$-st row?

Definition. If $r \leq n$, an $r \times n$ **Latin rectangle** over an n-element set S is an $r \times n$ array of elements of S such that no element occurs more than once in any row or column.

Theorem. *For $r < n$, any $r \times n$ Latin rectangle can be extended to an $(r+1) \times n$ Latin rectangle.*

Proof. Let L be an $r \times n$ Latin rectangle on $\{1, \ldots, n\}$. For each $i \leq n$, let A_i denote the set of elements of $\{1, \ldots, n\}$ that do not occur in the ith column of L. Then $|A_i| = n - r$ for each i. Furthermore, for each $j \leq n$, element j occurs in each row of L and hence has appeared in r of the columns; so j must occur in precisely $n - r$ of the A_is. Thus we can take $k = n - r$ in the above corollary and conclude that the sets A_i possess an SDR, which can be taken as the $(r+1)$-st row of the required rectangle. □

Many applications of Latin squares make use of the concept of **orthogonality**, an idea going back to Euler and his "thirty-six officers" problem from 1779.

Recall the problem: **Euler's officers.**

> *Thirty-six officers are given, belonging to six regiments and holding six ranks (so that each combination of rank and regiment corresponds to just one officer). Can the officers be paraded in a 6×6 array so that, in any line (row or column) of the array, each regiment and each rank occurs precisely once?*

In a solution to Euler's problem, if the officer's ranks are numbered from 1 to 6, they are arranged in a Latin square, and similarly for the regiments.

Definition. If $A = (a_{ij})$ and $B = (b_{ij})$ are $n \times n$ arrays, the **join** (A, B) of A and B is the $n \times n$ array whose (i, j)th entry is the pair (a_{ij}, b_{ij}). Two Latin squares A, B over $\{1, \ldots, n\}$ are **orthogonal** if all the entries of their join (A, B) are distinct. (Equivalently: each of the n^2 possible pairs occurs exactly once.)

Example. The join of $L_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$ and $L_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$ is

$$(L_1, L_2) = \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}.$$

The two Latin squares L_1 and L_2 are orthogonal. ▲

Euler's officer problem has a solution if and only if there exist two orthogonal Latin squares of order 6. Tarry proved in 1900 that no such squares exist.

More generally, a set $\{L_1, \ldots, L_r\}$ of Latin squares of order n is called a set of **mutually orthogonal** Latin squares (MOLS) if any two squares in the set are orthogonal. For a given n, let $f(n)$ denote the maximum number of MOLS of order n. We state without proof the following interesting theorem about sets of MOLS.

Theorem. *For all $n \geq 2$, we have $f(n) \leq n - 1$, with equality if and only if there exists an affine plane of order n.*

7.10 Graph Colorings

Graph colorings can be used to model 'incompatibility', to address problems such as:

- the frequency assignment problem from the beginning of Chapter 7,

  [Suppose that radio frequencies are being allocated to a number of transmitters. Some pairs of transmitters are so close that their transmissions would interfere, and they must be allocated different frequencies. How many frequencies are required?]

- the more classical *map coloring* problem:

  Countries sharing a common frontier must be given different colors on a map. How many colors does the cartographer need?

We define a **vertex coloring** of a graph $G = (V, E)$ to be a function c from V to a set of **colors** such that, for any edge $\{x, y\} \in E$, we have $c(x) \neq c(y)$. In the frequency assignment problem, the transmitters are the vertices, and the incompatible pairs edges, of a graph G; a legitimate frequency assignment is a vertex coloring of G. Similar remarks apply to the map coloring problem. In each case, we are interested in the smallest number of colors for which a coloring exists.

A graph G is **k-colorable** if it has a vertex coloring with k colors.

Note that the only 1-colorable graphs are the edgeless graphs. A graph is 2-colorable if and only if it is bipartite. (The color classes form a bipartition and vice versa.)

A **clique** in a graph G is a set of vertices, any pair joined by an edge (so that the induced subgraph is complete), and an **independent set** is a set of vertices containing no edges (so that the induced subgraph is edgeless). So, in a vertex coloring, each color class is an independent set.

The **chromatic number** of a graph $G = (V, E)$, written $\chi(G)$, is the least number k of colors such that G is k-colorable. Equivalently, it is the least k such that V can be partitioned into k independent sets. While this invariant has many applications, its computation is difficult.

For a graph G, we denote by $\omega(G)$ its **clique number**, that is, the maximum size of a clique in G. Note that if G has a clique of size c, then all vertices of this clique must receive different colors in any vertex coloring; so the chromatic number is at least c.

Proposition. *For every graph G, we have $\chi(G) \geq \omega(G)$.*

The following simple upper bound in terms of $\Delta(G)$, the **maximum degree** of a vertex in G, holds.

Proposition. *For every graph G, we have $\chi(G) \leq \Delta(G) + 1$.*

Proof. Let d be the maximum degree of G. To see that G can be colored with $d + 1$ colors, consider the vertices one at a time. Each vertex v has at most d neighbors, to which at most d colors have been applied; so there is an unused color available at v. □

The above upper bound is sharp, for two reasons:

- if G is the complete graph K_n, then $\chi(G) = n$ and $\Delta(G) = n - 1$;
- if G is a cycle of odd length (C_{2k+1} for $k \geq 1$), then G is 2-regular but not bipartite (that is, not 2-colorable).

Brooks' Theorem asserts that among connected graphs, these graphs are the only exceptions.

Theorem (Brooks' Theorem)**.** *For every connected graph G that is neither complete nor an odd cycle, $\chi(G) \leq \Delta(G)$.*

For a proof, see [5, p. 296]

A counting problem for graphs

For a graph G and a positive integer k, a **k-coloring** of G is a coloring of G with colors $\{1, \ldots, k\}$. We denote by $\chi(G, k)$ the **number** of k-colorings of G.

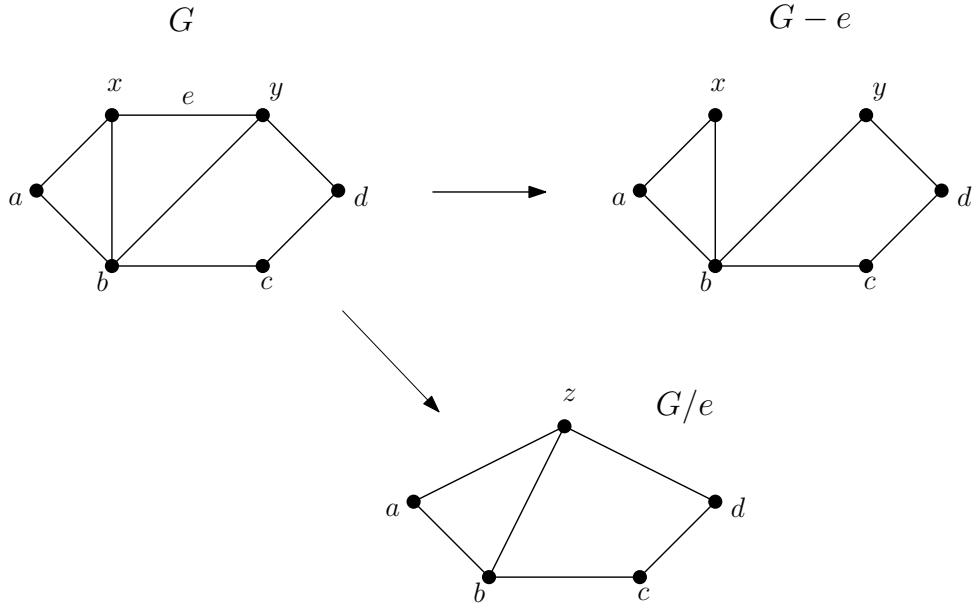
Examples:

- Let $\overline{K_n}$ denote the edgeless graph with n vertices. Then $\chi(\overline{K_n}, k) = k^n$
  (= the number of all functions from $V(\overline{K_n})$ to the set $\{1, \ldots, k\}$ of colors).
- $\chi(K_n, k) = n(n-1)\ldots(n-k+1)$
  (= the number of all injective functions from $V(K_n)$ to $\{1, \ldots, k\}$).

Given a graph $G = (V, E)$ and an integer k, how can we compute $\chi(G, k)$? Let $e = \{x, y\}$ be an edge of G. We define two operations on G:

- *Deletion* of e yields the graph $G - e = (V, E \setminus \{e\})$.
- *Contraction* of e: replace x and y by a new vertex z, with an edge $\{v, z\}$ whenever $\{v, x\} \in E$ or $\{v, y\} \in E$. Denote the resulting graph by G/e.

Example:



We can compute the value of $\chi(G, k)$ recursively.

Lemma. *If G is a graph and $e \in E(G)$, then*

$$\chi(G, k) = \chi(G - e, k) - \chi(G/e, k)\,.$$

Proof. Let $e = \{x, y\}$. Let c be a k-coloring of $G - e$.

If $c(x) \neq c(y)$, then c is a k-coloring of G.

If $c(x) = c(y)$, then c induces a coloring of G/e: color the contracted edge with color $c(x) = c(y)$, and the other vertices as in $G - e$.

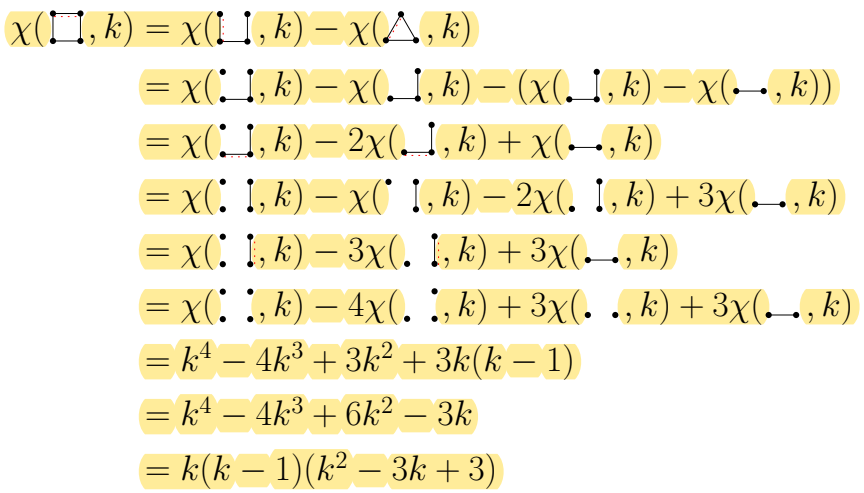
This gives a function

$$\{k\text{-colorings of } G-e\} \to \{k\text{-colorings of } G\} \cup \{k\text{-colorings of } G/e\}\,.$$

This process is reversible, so the function has an inverse. Thus, it is a bijection. So $\chi(G-e,k) = \chi(G,k) + \chi(G/e,k)$, as required. □

Now, if G is given and e is an edge of G, both $G-e$ and G/e have fewer edges than G. Assuming inductively that the values of $\chi(G-e,k)$ and $\chi(G/e,k)$ are known, the value of $\chi(G,k)$ can be computed. The induction begins with graphs without edges, for which we calculated the number of colorings already.

Example:



▲

Theorem (Chromatic Polynomial Theorem)**.** *For every graph G, $\chi(G,k)$ is a polynomial in k with integer coefficients.*

Proof. We use strong induction on $m = |E(G)|$. If $m = 0$, then $\chi(G,k) = k^{|V(G)|}$.

For the inductive step, suppose that the statement is true for all graphs with fewer edges than G. In particular, the statement is true for $G-e$ and for G/e. By the above lemma, $\chi(G,k) = \chi(G-e,k) - \chi(G/e,k)$, and the difference of integer polynomials is an integer polynomial. □

$\chi(G,\cdot)$ is called the **chromatic polynomial** of G. From now on, we will write it with variable t, as $\chi(G,t)$.

Example: the chromatic polynomial of a 6-vertex path, P_6, with vertices $\{v_1,\ldots,v_6\}$ in order, is $\chi(P_6,t) = t(t-1)^5$. Color the vertices of the path one by one. For the first vertex, we have t choices, and for each other one, we have $t-1$ choices since one neighbor of it is already colored.

Similarly, we see that the chromatic polynomial of an n-vertex path is $t(t-1)^{n-1}$. More generally:

Theorem. *If G is a tree on n vertices, then*

$$\chi(G,t) = t(t-1)^{n-1}.$$

Proof. We use induction on n.

If $n = 1$, then $G \cong K_1$ and $\chi(K_1, t) = t$.

For the inductive step, let $n \geq 2$ and assume that the statement holds for all trees with $n-1$ vertices. Let G be a tree with n vertices. Since $n \geq 2$, the tree G has a vertex v of degree 1. The graph $G - v$ is a tree with $n-1$ vertices. By the induction hypothesis, we have $\chi(G-v,t) = t(t-1)^{n-2}$. A t-coloring of G is uniquely determined by a t-coloring of $G - v$ together with assigning one of the $t-1$ available colors to v (any of the colors other than the color of the unique neighbor of v). Therefore, $\chi(G,t) = \chi(G-v,t) \cdot (t-1) = t(t-1)^{n-1}$. □

What can we say about the degree of the chromatic polynomial?

Lemma. *If G is a graph with n vertices, then the degree of $\chi(G,t)$ is n.*

Proof. We use strong induction on $m = |E(G)|$.

If $m = 0$, then $G = \overline{K_n}$ and $\chi(G,t) = t^n$.

For the inductive step, suppose that the statement is true for all graphs with fewer edges than G, where G is a graph with n vertices. Then $\chi(G-e,t)$ is of degree n and $\chi(G/e,t)$ is of degree $n-1$. Since $\chi(G,t) = \chi(G-e,t) - \chi(G/e,t)$, the degree of $\chi(G,t)$ is n, as claimed. □

Recall examples:

- $\chi(C_4,t) = t^4 - 4t^3 + 6t^2 - 3t$.
- If G is an n-vertex tree, then

$$\chi(G,t) = t(t-1)^{n-1} = t\sum_{k=0}^{n-1}\binom{n-1}{k}t^k(-1)^{n-1-k}$$

(by the Binomial Theorem).

For example, if $n = 4$, then $\chi(G,t) = t(t^3 - 3t^2 + 3t - 1) = t^4 - 3t^4 + 3t^2 - t$.

We state without proof some further properties of the chromatic polynomial.

Theorem. *For every graph G on n vertices and c connected components, we have:*

i) $\chi(G,t)$ is a polynomial in t of degree n, with coefficient at t^n equal to 1.

ii) t^c divides $\chi(G,t)$.

iii) Between t^n and t^c, the coefficients alternate in sign (and are $\neq 0$).

Read conjectured in 1968 that the absolute values of the coefficients of every chromatic polynomial are strictly increasing at first, then become strictly decreasing and remain so. This was proved by Huh in 2012.

Perfect Graphs (briefly)

We have seen that for any graph G, we have $\chi(G) \geq \omega(G)$. What are the graphs in which equality holds? Claude Berge realized that, to obtain a manageable theory, we should require the condition also for all induced subgraphs of G. Thus, a graph is **perfect** if for every induced subgraph H of G, the chromatic number and the clique number of H are equal. A number of interesting graph classes are perfect.

Theorem. *Bipartite graphs are perfect.*

Proof. Let G be a bipartite graph, with parts X and Y, and let H be an induced subgraph of G. Then, H is bipartite, too (with parts $X \cap V(H)$ and $Y \cap V(Y)$). The clique number and chromatic number of H are equal: both numbers are 2 unless the graph is edgeless (in which case they are 1). Thus, G is perfect. □

If n is odd and $n > 3$, then the n-cycle C_n is not perfect: it has clique number 2 and chromatic number 3.

The **complement** $\overline{G}$ of a graph G has the same vertex set as G; two distinct vertices are adjacent in $\overline{G}$ if and only if they are not adjacent in G. The cliques of $\overline{G}$ are the independent set of G, and vice versa. So the clique number of $\overline{G}$ is equal to the **independence number** of G (the maximum size of an independent set), and the chromatic number of $\overline{G}$ is the **clique cover number** of G (the smallest number of cliques the union of which is $V(G)$).

If n is odd and $n > 3$, then the complement of C_n also fails to be perfect: the independence number of C_n is $(n-1)/2$, while it is not possible to cover all n vertices of C_n with $(n-1)/2$ cliques (as they are all of size at most 2).

Thus a graph that contains either C_n or $\overline{C_n}$ as induced subgraph for n odd and $n > 3$ also fails to be perfect. Such subgraphs are called **odd holes** and **odd antiholes**, respectively.

Berge conjectured in the 1960s that these are the only obstructions to perfection. In 2002, Chudnovsky, Robertson, Seymour, and Thomas turned this so-called Strong Perfect Graph Conjecture into a theorem.

Theorem. *A graph is perfect if and only if it contains no odd hole and no odd antihole.*

Homomorphisms

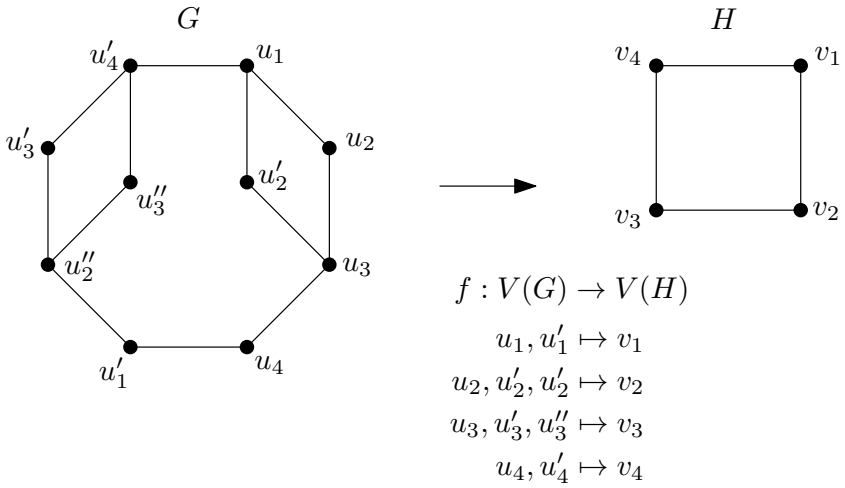
A **homomorphism** from a graph G to a graph H is a map $f : V(G) \to V(H)$ which takes edges to edges, that is,

$$\text{if} \quad \{x, y\} \in E(G) \quad \text{then} \quad \{f(x), f(y)\} \in E(H)$$

holds for all $x, y \in V(G)$, $x \neq y$. (It may map a non-edge to a single vertex, a non-edge, or an edge.) Notation: $f : G \to H$.

Clearly, every isomorphism is a homomorphism. But in the case of a homomorphism, the mapping is not necessarily bijective: an independent set of vertices may be mapped to the same vertex.

Example. A homomorphism.



We can check that edges are mapped to edges. ▲

Homomorphisms are a generalization of graph colorings. A homomorphism from the graph G to the complete graph K_r is exactly the same as a coloring of G with r colors (where the color of a vertex is its image under the homomorphism), since adjacent vertices map to distinct vertices of the complete graph.

Example. If G is a bipartite graph, with parts X and Y, and H is the complete graph with $V(H) = \{1, 2\}$, then $f : V(G) \to \{1, 2\}$, given by $f(x) = 1$ for all $x \in X$ and $f(y) = 2$ for all $y \in Y$, is a homomorphism. ▲

Example: Scheduling exams.

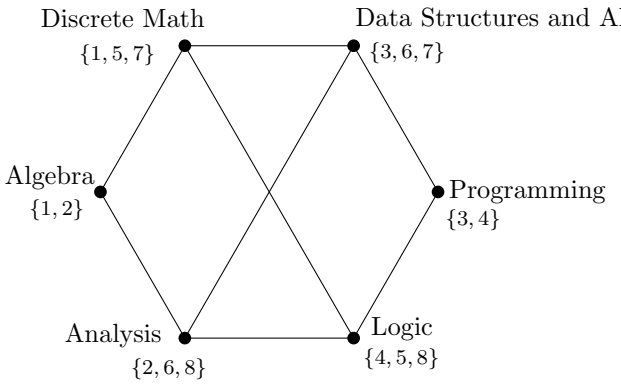
How to schedule the exams in the smallest number of periods?

Two exams taken by the same student cannot be scheduled at the same time. So make a graph G whose vertices are the exams, two vertices joined by an edge if some student is taking both exams. Then an exam schedule in k periods exists if and only if the graph is k-colorable, that is, there is a homomorphism from G to the complete graph K_k.

Now suppose that a student is not permitted to take exams in consecutive periods. Let H_k be the complete graph on k vertices with the $k-1$ edges of a spanning path removed. Then the exams can be scheduled in k periods if and only if there is a homomorphism from G to H_k.

For example, suppose we have 8 student groups labeled $1, \ldots, 8$. We also have 6 courses in which these students have to take exams: Algebra (student groups 1 and 2), Analysis (student groups $2, 6, 8$), Data Structures and Algorithms (student groups $3, 6, 7$), Discrete Math (student groups $1, 5, 7$), Logic (student groups $4, 5, 8$), Programming (student groups 3 and 4).

The following graph G represents the conflicts between exams:



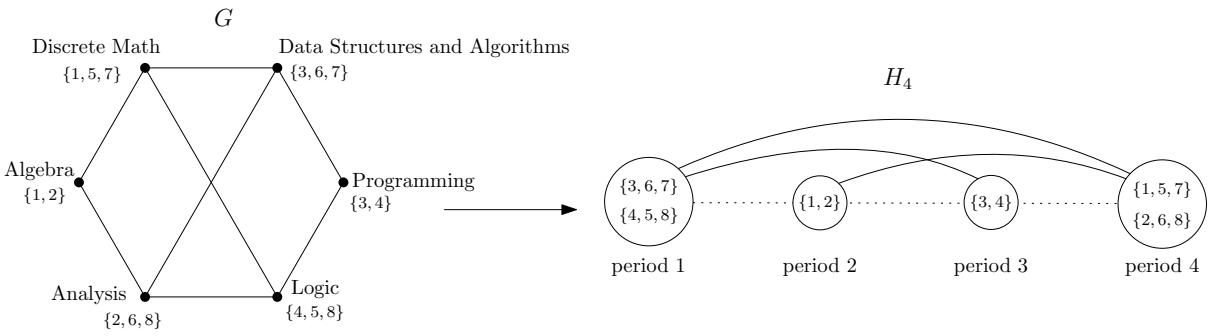
The graph is bipartite, so we could schedule exams in two periods only:

period 1: Algebra, Data Structures and Algorithms, Logic
period 2: Analysis, Discrete Math, Programming

But what if a student is not permitted to take exams in consecutive periods? Then we can schedule the exams in four periods, as follows:

period 1: Data Structures and Algorithms (3,6,7), Logic (4,5,8)
period 2: Algebra (1,2)
period 3: Programming (3,4)
period 4: Analysis (1,5,7), Discrete Math (2,6,8)

This represents a homomorphism from the graph G to the graph H_4:



7.11 Edge Colorings

An **edge coloring** of a graph $G = (V, E)$ is a map c from E to a set of **colors** such that two edges sharing a vertex have different colors. Every color class in an edge coloring is a matching. The **chromatic index** of G is denoted by $\chi'(G)$ and defined to be the least number of colors required for an edge coloring of G.

The **line graph** of a graph $G = (V, E)$ is defined as follows. The vertex set of $L(G)$ is E; two vertices e_1, e_2 are joined in $L(G)$ if and only if (as edges of G) they have a common vertex. An edge coloring of a graph is exactly the same thing as a vertex coloring of its

line graph. So, in a sense, the theory of edge colorings is a part of the theory of vertex colorings; but it has its own particular style and results.

In an edge coloring, all the edges which meet at a vertex must have different colors. So the chromatic index of G cannot be smaller than its maximum degree. The following theorem of Vizing restricts the chromatic index to two possible values:

Theorem. *If a graph has maximum degree d, then it has an edge coloring with $d+1$ colors.*

So the chromatic index is either d or $d+1$. Accordingly, the class of all graphs can be divided into two parts. A graph belongs to **Class 1** if its chromatic index is equal to its maximum degree, and to **Class 2**, otherwise.

As the next result shows, every bipartite graph is Class 1.

Theorem. *Let G be a bipartite graph with maximum degree d. Then $\chi'(G) = d$.*

Proof. We already justified the inequality $\chi'(G) \geq d$. The proof of the inequality $\chi'(G) \leq d$ is by induction on the number of edges. As usual, starting the induction ($d = 0$) is trivial. So assume that the theorem holds for graphs with fewer edges than G. Let $\{X, Y\}$ be a bipartition of G and $e = \{x, y\}$ an edge of G, with $x \in X$ and $y \in Y$. Then the edges of $G - e$ can be partitioned into d matchings. It is easier to visualize the edges as being colored with d colors $1, \ldots, d$ so that a vertex lies on at most one edge of each color.

Since x and y have degree less than d in $G - e$, at least one color does not occur on the edges at each of them. If the same color is missing at both x and y, we can use it to color the edge e. So we may suppose that color 1 is missing at x, and color 2 at y.

Set $x = u_1$, and define $v_1, u_2, v_2, \ldots$ by the rule that $\{u_i, v_i\}$ has color 2 and $\{v_i, u_{i+1}\}$ has color 1, as long as such edges exist. Note that all vertices u_i belong to X and all v_i to Y. The sequence cannot revisit any vertex, so it must terminate; by assumption, it cannot terminate at either x or y (for example, $y \neq v_n$ since y lies on no edge of color 2). Now we can interchange the colors 1 and 2 on the edges of this path without violating the condition that no two edges of the same color meet at a vertex. As a result, color 2 is no longer used on an edge through x, and we can give this color to e. □

Edge colorings of K_n. Consider a sports league of n teams, where in a course of a season, every team plays against every other team exactly once. If there are n teams in the competition, what is the least number of rounds required to play the matches? The number of matches to be played is $\binom{n}{2} = \frac{n(n-1)}{2}$. If n is even, then $n/2$ matches can be played in every round, so we need at least $n-1$ rounds. If n is odd, then only $(n-1)/2$ matches can be played in a round, with one team having a bye; so n rounds are required. A **tournament schedule** of n teams is an arrangement of all pairs of teams into rounds.

Consider the complete graph K_n where the teams are the vertices and the edges represent the matches between the teams. An edge coloring of K_n is the same thing as a tournament schedule for n teams: the rounds of the tournament are the colors of the edges.

Proposition. *The complete graph K_n belongs to Class 1 if n is even, and to Class 2 if n is odd.*

Proof. Since the maximum degree of K_n is $n-1$, the statement is equivalent to proving that $\chi'(K_n) = n$ if n is odd and $\chi'(K_n) = n-1$ if n is even. We already argued above that n and $n-1$ are the lower bounds on the chromatic index. There is a simple construction achieving the bounds.

First, consider the case when n is odd. Draw a regular n-gon in the plane, and number its vertices $0, 1, \ldots, n-1$ corresponding to the teams (these numbers are regarded as belonging to the integers mod n). For each edge of the n-gon, there are $(n-3)/2$ diagonals parallel to this edge; this parallel class determines the matches in a round, with the team corresponding to the vertex opposite the chosen edge having a bye.

For n even, we temporarily remove one team from the competition, and construct a tournament schedule with $n-1$ rounds as above. Then we decree that, in each round, the extra team will play the team which would otherwise have had a bye in that round. □

7.12 Planar Graphs

Although graphs are abstract objects, geometrically representing them using 'dots' and 'lines' may help our intuition. But so far we have been studying properties of graphs not related to their drawings, and the role of drawings was purely auxiliary. In this chapter the subject of analysis will be the drawing of graphs itself and we will mainly investigate **graphs that can be drawn in the plane without edge crossings**. Such graphs are called planar.

More generally, we choose some familiar geometric or topological space as a drawing board and represent vertices by distinct points of the space; each edge is represented by a line or curve whose endpoints correspond to its vertices.

The question **'What is a curve?'** is a difficult one, which took mathematicians nearly a century to resolve. Peano, for example, constructed a continuous curve passing through every point of the unit square. But such curves don't aid intuition. We assume that an edge is represented by a *piecewise smooth* curve (one having a continuously varying tangent everywhere except perhaps a finite number of 'corners'). A **curve** in the plane is a subset α of the plane of the form

$$\alpha = \gamma([0,1]) = \{\gamma(x) : x \in [0,1]\},$$

where $\gamma : [0,1] \to \mathbb{R}^2$ is an injective continuous map of the closed interval $[0,1]$ to the plane. The points $\gamma(0)$ and $\gamma(1)$ are called the **endpoints** of the curve α.

For applications such as road layouts and map coloring, we impose a further condition:

The curves representing two edges are disjoint except at their common endpoints (if any).

We call a drawing of G satisfying this condition an **embedding** of G in the plane. Embeddings in other spaces are defined similarly.

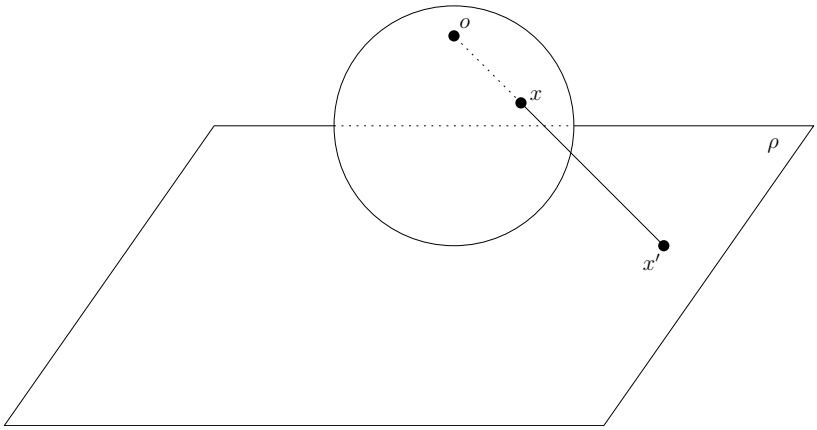
It is not clear whether a given a graph can be embedded in a given space. In three dimensions, there is no restriction:

Proposition. *Any graph can be embedded in $\mathbb{R}^3$.*

Proof. Take a line L and represent vertices by points on L. For each edge e, take a plane Π_e through L (all these planes distinct), and join the vertices of e by a semicircle in Π_e (by a circle if e is a loop). □

In two dimensions, the situation is very different. We call a graph **planar** if it is embeddable in the Euclidean plane. The complete graph K_5 and the complete bipartite graph $K_{3,3}$ are non-planar. We will see that this is a consequence of a theorem of Euler.

Embedding in the plane and in the surface of a sphere are 'equivalent' concepts. This is because of the so-called **stereographic projection**. We place the sphere in the 3-dimensional space in such a way that it touches the considered plane ρ. Let o denote the point of the sphere lying farthest from ρ (the "north pole"):



The stereographic projection maps each point $x \neq o$ of the sphere to a point x' in the plane, where x' is the intersection of the line ox with the plane ρ. (For the point o, the projection is undefined.) This defines a bijection between the sphere without the point o and the plane. Given an embedding of G in the sphere, where the point o lies on no curve of the drawing (which we may assume by a suitable choice of o), the stereographic projection yields a planar drawing of G. Conversely, from a planar drawing we get a drawing on the sphere by the inverse projection.

Now let G be a connected graph. Given an embedding of G in the plane or sphere, the removal of the image of the embedding leaves a finite number of connected pieces called **faces**. In the case of the plane, just one face — the **infinite face** — is unbounded. The boundary of a face is a closed curve made up of a finite number of vertices and the same number of edges (possibly with repetitions), corresponding to a closed walk in G. (The connectedness of the face boundary depends on that of G.) The face itself is topologically equivalent to a disc (the interior of a circle), except in the case of the infinite face in the plane.

Theorem (Euler's Theorem)**.** *Let an embedding of a connected graph G in the plane have n vertices, e edges, and f faces. Then*

$$n - e + f = 2\,.$$

Proof. We use induction on e. A connected graph with no edge has one vertex and one face, and satisfies the theorem.

Suppose that there is an edge e' such that $G - e'$ is connected. Then $G - e'$ has n vertices, $e - 1$ edges, and $f - 1$ faces, since, when e' is removed, the two faces on either side of it coalesce. (We have to show that these two faces are different. Suppose not; let f' be this face. There is a curve in f' from one side of e' to the other. When e' is removed, this becomes a simple closed curve in f'. By the Jordan Curve Theorem,[6] this curve divides the plane into two components, each of which contains a vertex of e'; so $G - e'$ is not connected.) So $n - (e - 1) + (f - 1) = 2$, and we are done.

So we may assume that there is no such edge. Then G is a tree. (Since G is connected, it has a spanning tree, say T. If $G \neq T$, then the removal of an edge outside T leaves a connected graph.) Since an n-vertex tree has $n - 1$ edges, we have $e = n - 1$. Moreover, $f = 1$. So $n - e + f = 2$, as required. □

If you find that proof a bit unsatisfactory in its appeals to geometrical or physical intuition, you should read Imre Lakatos' **Proofs and Refutations** *(1976). Euler's Theorem is used as a test case for an investigation of mathematical rigor, and plausible 'counterexamples' are used to refine and make more precise both the statement of the theorem and the arguments used in the proof. (If you are happy with the above proof, then there is even more reason for you to read the book!)*

Corollary. *K_5 and $K_{3,3}$ are non-planar.*

Proof. (a) K_5 has 5 vertices and 10 edges, so an embedding would have 7 faces. But each face has at least three edges (a face with 1 or 2 edges can only occur if there are loops or parallel edges in the graph), while each edge bounds at most two faces. Double-counting the number N of incident edge-face pairs shows that the number of faces is at most $20/3$ (since $3f \leq N \leq 2e = 20$), a contradiction.

(b) $K_{3,3}$ has 6 vertices and 9 edges, so 5 faces (if embedded in the plane). Now each face has at least four edges: the graph is simple and bipartite and has no closed walk of odd length. The same argument as before the shows that there are at most $9/2$ faces, a contradiction. □

From this result, we can give further examples of non-planar graphs.

A **subdivision** of a graph G is obtained by repeated application of the operation 'insert a vertex into an edge': replace the edge $\{x, y\}$ by two edges $\{x, v\}$ and $\{v, y\}$, where v is a new vertex.

This operation does not affect embeddability in any space: choose any point on the curve from x to y to represent v, and let the two 'halves' of this curve represent $\{x, v\}$ and $\{v, y\}$. This operation reverses, so any subdivision of K_5 or $K_{3,3}$ is non-planar, as is any graph containing a subgraph of this form.

[6]The **Jordan Curve Theorem** asserts that a simple (non-intersecting) closed plane curve has an 'inside' and an 'outside'; that is, its complement has two connected components, exactly one of which is unbounded.

Remarkably, the converse is true:

Theorem (Kuratowski's Theorem)**.** *A graph G is planar if and only if G contains no subdivision of K_5 or $K_{3,3}$.*

For later use, let us derive the following consequence of Euler's theorem.

Proposition. *Every planar graph contains a vertex of degree at most 5.*

Proof. Let G be a planar graph. We may assume that G is connected (otherwise, we consider only one of its connected components) and embedded in the plane. Let G have n vertices, of which n_i have degree i; let there be e edges and f faces.

As in the proof of the fact that K_5 is non-planar, we have $2e \geq 3f$. Counting vertices and incident vertex-edge pairs, we have

$$\begin{aligned} \sum n_i &= n\,, \\ \sum i n_i &= 2e\,. \end{aligned}$$

From Euler's Theorem, we conclude that

$$\sum_i (6-i)n_i \geq 12\,.$$

The left-hand side of this inequality must be positive; so $n_i \geq 0$ for some $i < 6$. This means that graph contains a vertex of degree at most 5, as desired. □

One of the main areas of interest in topological graph theory is the connection with coloring problems. Any plane map can be described by a graph whose vertices are the countries, with edges joining countries that share a boundary. (If two countries share several unconnected segments of boundary, use multiple edges.) Now coloring a map is the same as a vertex coloring of the graph. The famous **four-color problem** was resolved in 1976 by Appel and Haken, with the help of extensive computation:

Theorem (Appel-Haken Theorem, or the Four-color Theorem)**.** *Every planar graph has a vertex coloring with four colors.*

It is impossible to summarize here the techniques used. We will prove that five colors suffice; the proof illustrates the basic ideas which grew into the Appel-Haken proof. The argument is due to Kempe, who thought (incorrectly) that he had proved the Four-color conjecture.

Let us first give a very simple argument of why 6 colors suffice.

Proposition. *Every planar graph has a vertex coloring with six colors.*

Proof. The proof is by induction on the number of vertices. Let G be a planar graph. We assume the result for graphs with fewer vertices than G. By the previous proposition, G has a vertex of degree at most 5. Let v be such a vertex. By induction, $G - v$ has a coloring with six colors. Since v has at most 5 neighbors, there is a color available for coloring v. It follows that G is 6-colorable. □

Theorem (The Five-color Theorem, Heawood 1890)**.** *Every planar graph has a vertex coloring with five colors.*

Proof. The proof is by induction on the number of vertices. Let G be a planar graph. We assume the result for graphs with fewer vertices than G. We also assume that G is drawn in the plane.

Let v be a vertex of degree at most 5 in G. By induction, $G - v$ has a coloring with five colors 1, 2, 3, 4, 5. If not all colors are used on the neighbors of v, then there is a free color which can be applied to v. So we may assume that v has degree 5 and that all its neighbors have different colors. Let the neighbors be $z_1, \ldots, z_5$ in clockwise order, where we may assume that z_i has color i.

Let S be the set of all vertices that can be reached from z_1 by a path using vertices with colors 1 and 3 only. Then we can legitimately interchange colors 1 and 3 throughout the set S, without affecting the property that adjacent vertices have different colors. If $z_3 \notin S$, then after this interchange no neighbor of v has color 1, and we can use this color for v. So we may assume that $z_3 \in S$. Thus, there is a path $z_1, x_1, \ldots, x_k, z_3$ consisting of vertices with colors 1 and 3. Adjoining v to this path, we obtain a simple closed curve C.

By the Jordan Curve Theorem, C divides the plane into two parts, and clearly z_2 and z_4 lie in different parts; suppose that z_2 is inside C. Let T be the set of vertices that can be reached from z_2 by a path using vertices with colors 2 and 4 only. No such path can cross C, so T lies wholly inside C, and $z_4 \notin T$. Then we can interchange colors 2 and 4 throughout T, freeing color 2 to use on v. □

7.13 Ramsey's Theorem

Recall the **Ramsey game question** from the opening lecture:

> *This two-player game requires a sheet of paper and pencils of two colors, say red and blue. Six points on the paper are chosen, with no three in a line. Now the players take a pencil each, and take turn drawing a line connecting two of the chosen points. The first player to complete a triangle of her own color loses. (Only triangles with vertices at the chosen points count.)*
>
> Note that the game is finite, since at most $\binom{6}{2} = 15$ lines can be drawn.
>
> *Can the game ever result in a draw?*

The answer, as we will see, is NO: there will always be a red triangle or a blue triangle.

The question is a special case of the following question on graphs:
Is it true that for every coloring of the edges of the complete graph K_6 with two colors, there is a monochromatic subgraph K_3? (A subgraph is **monochromatic** if all its edges have the same color.)

In this section, the edge colorings do not have to satisfy the condition that adjacent edges get different colors. The graph K_6 has 15 edges, so there are $2^{15} = 32,768$ red-blue colorings of $E(K_6)$.

Theorem (Ramsey's Theorem, 1930)**.** *Given $a, b \geq 2$, there exists a least integer $R(a,b)$ with the following property: Every red-blue coloring of the edges of the complete graph on $R(a,b)$ vertices yields a red K_a or a blue K_b. Furthermore,*

$$R(a,b) \leq R(a-1,b) + R(a,b-1)$$

for all $a, b \geq 3$.

Proof. We use a "double induction" – induction on a and b.

The basis of the induction consists of the statements $R(a,2) = a$ and $R(2,b) = b$:

- In the first assertion, if we two-color K_a and any edge is blue, then we obtain a blue K_2, while if no edge is blue, we obtain a red K_a. Thus $R(a,2) \leq a$. Equality follows from the fact that an all red coloring of $E(K_{a-1})$ contains neither red K_a nor a blue K_2.
- The second assertion is proved similarly.

Now, assuming the existence of $R(a-1,b)$ and $R(a,b-1)$ for some $a, b \geq 3$, we will show that $R(a,b)$ exists. Let G be the complete graph on $R(a-1,b)+R(a,b-1)$ vertices and let v be an arbitrary vertex of G. Then, at least $R(a-1,b)$ red edges or at least $R(a,b-1)$ blue edges emanate from v. (Indeed, if this is not the case, then v would have at most $(R(a-1,b)-1)+(R(a,b-1)-1) < R(a-1,b)+R(a,b-1)-1$ neighbors, contrary to the fact that G is complete.)

Without loss of generality, suppose that v is joined by red edges to a complete subgraph on $R(a-1,b)$ vertices. By definition of $R(a-1,b)$, this subgraph must contain a red K_{a-1} or a blue K_b. In the former case, the red K_{a-1} and v, and all the edges between the two, constitute a red K_a. Therefore, G contains a red K_a or a blue K_b. This shows that $R(a,b)$ exists and satisfies $R(a,b) \leq R(a-1,b) + R(a,b-1)$. □

Note that Ramsey's Theorem can be formulated equivalently in terms of graphs and their complements, as follows:

Given $a, b \geq 2$, there exists a least integer $R(a,b)$ such that every graph on $R(a,b)$ vertices contains either a clique of size a or an independent set of size b.

Here is an application of Ramsey's Theorem.

Proposition. *There is a function $f(m,n)$ with the following property. If $(x_1, \ldots, x_N)$ is any finite sequence of distinct real numbers with $N > f(m,n)$, then there is either an increasing subsequence of length $> m$ or a decreasing subsequence of length $> n$.*

Example: in the following sequence $(7,4,1,8,5,2,9,6,3,0)$ there is an increasing subsequence of length 3, for example $(1,2,6)$, as well as a decreasing subsequence of length 4, for example $(7,5,3,0)$.

Proof of the proposition. Let $f(m,n) = R(m+1,n+1)-1$. Suppose that $N > f(m,n)$, and we are given a sequence of N distinct real numbers. Take $X = \{1, \ldots, N\}$, and color the edges of the complete graph with vertex set X as follows: given a pair $\{i,j\}$ with $i < j$, color it red if $x_i < x_j$, and blue if $x_i > x_j$. Since $|X| = N \geq R(m+1,n+1)$, there is either a red K_{m+1} or a blue K_{n+1}. But a red set indexes an increasing subsequence: if the vertices of a red K_{m+1} are $\{i_1, \ldots, i_{m+1}\}$ with $i_1 < \ldots < i_{m+1}$, then $x_{i_1} < \ldots x_{i_{m+1}}$. Similarly, a blue set indexes a decreasing subsequence. □

Remark: a direct proof of the above proposition using the Pigeonhole Principle shows that we can take $f(m,n) = mn$.

The integers $R(a,b)$ are called **Ramsey numbers**. Very few of them are known. (The fact that we have determined their existence but we don't know their values illustrates one disadvantage of existential proofs.)

Since the roles of the variables a and b are symmetric, we have $R(a,b) = R(b,a)$ for all $a, b \geq 2$. The values $R(a,a)$ are called **diagonal Ramsey numbers** because they appear on the main diagonal of a table of Ramsey numbers.

We have showed above that $R(a,2) = a$ and $R(2,b) = b$ for all $a, b \geq 2$. Moreover, we have $R(3,3) = 6$:

- $R(3,3) \leq R(2,3) + R(3,2) = 3 + 3 = 6$.
- $R(3,3) > 5$ since there is a two-coloring of the edges of K_5 not having a monochromatic K_3 (each color class forms a 5-cycle).

Some known or partially known Ramsey numbers (only the part of the table above the diagonal is shown):

$a \setminus b$	2	3	4	5	6
2	2	3	4	5	6
3		6	9	14	18
4			18	25	36-41
5				43-48	58-87
6					102-165

Ramsey numbers can be bounded from above as follows.

Theorem. *For all $a, b \geq 2$,*

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

Proof. We use induction on a and b, noting that $R(a,2) = a = \binom{a}{a-1}$ and $R(2,b) = b = \binom{b}{1}$.

Suppose that the upper bound holds for $R(a-1,b)$ and $R(a,b-1)$, for some $a, b \geq 3$. Then

$$\begin{aligned} R(a,b) &\leq R(a-1,b) + R(a,b-1) \\ &\leq \binom{a+b-3}{a-2} + \binom{a+b-3}{a-1} \\ &= \binom{a+b-2}{a-1} \qquad \text{(by Pascal's identity)} \end{aligned}$$

and the upper bound is established. □

Open problems:

- Determine a formula for $R(n,n)$.
- Determine the value of the limit $\lim_{n\to\infty} R(n,n)^{1/n}$ (if it exists; if it exists, then it is somewhere between $\sqrt{2}$ and 4).

Ramsey's Theorem generalizes to larger subsets (not necessarily edges) and to more colors. More generally, a theorem of **Ramsey theory** says that any structure of a certain type, no matter how 'disordered', contains a much more ordered substructure of the same type *("Complete disorder is impossible").*

Theorem (Ramsey's Theorem – a more general version)**.** *Given positive integers r, k, ℓ, there exists a least positive integer $n = R(r, k, \ell)$ with the following property. If the k-subsets of an n-set are colored with r colors, then there is a monochromatic ℓ-subset, that is, one all of whose k-subsets have the same color.*

Here is an application of Ramsey's Theorem to geometry.

A set of points in the Euclidean plane is **convex** if it contains the line segment joining any two of its points. The **convex hull** of a set S of points is the smallest convex set containing S. A **convex n-gon** is a set of n points in the plane, none of which lies in the convex hull of the others (equivalently, each of the points lies on a line such that all other points are on the same side of the line).

Theorem (Erdős-Szekeres)**.** *Let n be a positive integer. Then there exists a least integer $ES(n)$ such that if there are $N \geq ES(n)$ points given in the plane, no three of which are collinear, then we can choose n of them that form a convex n-gon.*

For example, $ES(4) = 5$.

Proof. We claim that $R(2, 3, n)$ will always be such a positive integer (not necessarily the minimal one). Take a set of $R(2, 3, n)$ points in the plane. Color the triangles (= 3-sets) red or blue according to the following rule. Number the points from 1 to $R(2, 3, n)$, and color a triangle red if the path from the smallest number via the middle one to the largest one is clockwise. Color a triangle blue if that path is counterclockwise.

By Ramsey's Theorem, there is a monochromatic n-set, say S. We claim that points in S form a convex n-gon. To see this, it suffices to show that there are no four points in S such that one of them is within the triangle spanned by the other three. Suppose that this is not the case, and let ABC be a triangle containing a fourth point D where $A, B, C, D \in S$. We may assume without loss of generality that all the triangles in S are red and that $A < B < C$. Since the triangle ACD is red, we infer that $A < D$ and $D < C$. Since the triangle ABD is red, we have that $B < D$. But now, the triangle BCD is blue, a contradiction. □

References

[1] R. B. J. T. Allenby and A. Slomson. *How to Count: An Introduction to Combinatorics.* Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, second edition, 2011.

[2] I. Anderson. *A First Course in Combinatorial Mathematics.* Oxford Applied Mathematics and Computing Science Series. The Clarendon Press, Oxford University Press, New York, second edition, 1989.

[3] I. Anderson. *A First Course in Discrete Mathematics*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 2001.

[4] M. Bóna. *A Walk Through Combinatorics*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, second edition, 2006.

[5] P. J. Cameron. *Combinatorics: Topics, Techniques, Algorithms*. Cambridge University Press, Cambridge, 1994.

[6] M. J. Erickson. *Introduction to Combinatorics*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., New York, 1996.

[7] M. Juvan and P. Potočnik. *Teorija grafov in kombinatorika*. DMFA – Založništvo, Ljubljana, 2000.

[8] L. Lovász, J. Pelikán, and K. Vesztergombi. *Discrete Mathematics: Elementary and Beyond*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2003.

[9] J. Matoušek and J. Nešetřil. *Invitation to Discrete Mathematics*. Oxford University Press, Oxford, second edition, 2009.

[10] R. Požar. *Unpublished notes on combinatorics (in Slovene, for the course Diskretna Matematika II, 2015/2016)*. UP FAMNIT.

[11] D. Stevanović, V. Baltić, M. Ćirić, and S. Simić. *Diskretna Matematika. Osnove kombinatorike i teorije grafova*. Prirodno-matematički fakultet u Nišu, 2007.

[12] R. Woodroofe. *Unpublished notes on chromatic polynomial, 2015/2016*. UP FAMNIT.