Combinatorics and Graph Theory

Xavier Povill Clarós

December 21, 2021

Contents

1 Symbolic Enumeration

1.1 Combinatorial Classes

1.1.1 Basic definitions

We start with an overly technical definition that will allow us to frame every counting problem we encounter in the same terms.

Definition 1.1.1 (Combinatorial class)**.** A combinatorial class is a pair $(\mathcal{A}, |\cdot|)$ where $\mathcal{A}$ is a countable class of objects equipped with a size function $|\cdot| : \mathcal{A} \longrightarrow \mathbb{N}$ such that $\mathcal{A}_n := \{a \in \mathcal{A} : |a| = n\}$ is finite for every n.

Example 1.1.1.

1. We can take $\mathcal{A} = \mathbb{N}$, with $|n| = n$.
2. Words over an alphabet B, where $|w|$ is the length of the word.

Definition 1.1.2 (Generating function)**.** The generating function of a class $\mathcal{A}$ is

$$A(z) := \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} = \sum_{n \geq 0} a_n z^n, \quad \text{where } a_n = |\mathcal{A}_n|$$

Example 1.1.2. For the combinatorial class of the natural numbers, $\mathcal{A} = \mathbb{N}$ and $A(z) = z + z^2 + \cdots = \frac{z}{1-z}$.

Note that this last equality should be interpreted in algebraic terms, not as a function (because the series does not converge for $|z| \geq 1$).

There are in fact series like $\sum_{n \geq 1} n! z^n$ which do not converge anywhere in the complex plane but in $z = 0$. However, considering it as a formal power series, we can operate with it algebraically and obtain non-trivial results.

The *symbolic method* consists in translating formal operations with combinatorial classes into operations with their generating functions.

1.1.2 Operations on combinatorial classes

1. **Sum**: $\mathcal{C} = \mathcal{A} + \mathcal{B}$. It represents the union of the two classes (which are considered to be disjoint). Given $x \in \mathcal{C}$, if $x \in \mathcal{A}$ then we define $|x|_{\mathcal{C}} := |x|_{\mathcal{A}}$. Otherwise, $x \in \mathcal{B}$ and we define $|x|_{\mathcal{C}} := |x|_{\mathcal{B}}$. One might check that the resulting generating function is

$$C(z) = A(z) + B(z) = \sum_{n \geq 0} (a_n + b_n) z^n$$

2. **Product:** $\mathcal{C} = \mathcal{A} \times \mathcal{B} = \{(\alpha, \beta) : \alpha \in \mathcal{A},\ \beta \in \mathcal{B}\}$. The size is defined as the sum of both objects' sizes:

$$|(\alpha, \beta)|_{\mathcal{C}} := |\alpha|_{\mathcal{A}} + |\beta|_{\mathcal{B}}$$

   The resulting generating function is the product of both generating functions:

$$C(z) = \sum_{(\alpha,\beta) \in \mathcal{C}} z^{|(\alpha,\beta)|} = \sum_{\alpha \in \mathcal{A}, \beta \in \mathcal{B}} z^{|\alpha|+|\beta|} = \left(\sum_{\alpha \in \mathcal{A}} z^{|\alpha|} \right) \left(\sum_{\beta \in \mathcal{B}} z^{|\beta|} \right) = A(z) \cdot B(z)$$

3. **Sequence:** $\mathcal{C} = \mathrm{Seq}(\mathcal{A}) := \varepsilon + \mathcal{A} + \mathcal{A} \times \mathcal{A} + \cdots + \mathcal{A}^n + \ldots$, where ε is the combinatorial class with just one element of size zero.

   The resulting generating function is

$$C(z) = 1 + A(z) + A^2(z) + \cdots = \frac{1}{1 - A(z)}$$

1.2 Basic Examples

1.2.1 Integer compositions

Definition 1.2.1 (Class of integer compositions)**.** The class of integer compositions $\mathcal{I}$ is the one that has for objects the tuples $(a_1, a_2, \ldots, a_k) \in \bigcup_{m \geq 1} \mathbb{N}^m$, with size $|(a_1, a_2, \ldots, a_k)| := a_1 + \cdots + a_k$.

This class enables us to count the number of *compositions*, that is, the number of ways of expressing an integer $n \in \mathbb{N}$ as sum of other integers. Note that we care about the order so, for example, we consider $(1, 2)$ and $(2, 1)$ to be two different objects. This makes counting much easier.

Remember, that if $A(z) = \sum_{n \geq 0} a_n z^n$ is a generating function of the class $\mathcal{A}$, then $|\mathcal{A}_n| = a_n = [z^n]A(z)$ (that is, the coefficient of z^n in the series $A(z)$).

If $\mathbb{N}$ is the class of positive integers, $N(z) = z/(1-z)$. Then, we observe that $\mathcal{I} = \text{Seq}(\mathbb{N})$, so immediately we get its generating function:

$$I(z) = \frac{1}{1-N(z)} = \frac{1-z}{1-2z} = (1-z)\sum_{n\geq 0} 2^n z^n$$

In order to find the number of partitions of size n, we need to extract the n-th coefficient of the previous series:

$$I(z) = \sum_{n\geq 1}(2^n - 2^{n-1})z^n + 1 = 1 + \sum_{n\geq 1} 2^{n-1} z^n$$

Therefore, the number of partitions of a certain $n \geq 1$ is $I_n = [z^n]I(z) = 2^{n-1}$. As an exercise, try to derive this result using elementary methods.

The symbolic method is very powerful and it allows us to solve various versions of this problem. Let us consider the compositions of integers into parts in $\{1, 2\}$. In this case, instead of $\mathbb{N}$ we need to use the class $\mathcal{B} = \{1, 2\}$ with $|n| = n$. Then, $I_{1,2}(z) = \text{Seq}(\mathcal{B})$ so the generating function is

$$I_{1,2}(z) = \frac{1}{1-B(z)} = \frac{1}{1-z-z^2}$$

It can be seen that this is the generating function of the Fibonacci numbers, so the number of partitions of n into parts in $\{1, 2\}$ is the n-th Fibonacci number.

Let us consider next the compositions of numbers into odd parts. In this case we need to take the combinatorial class of odd integers $\mathcal{O} = \{1, 3, \dots\}$, which has the generating function

$$O(z) = z + z^3 + z^5 + \cdots = \frac{z}{1-z^2}$$

Therefore, $\mathcal{I}_{\text{odd}} = \text{Seq}(\mathcal{O})$ and

$$I_{\text{odd}}(z) = \frac{1}{1-O(z)} = \frac{1-z^2}{1-z-z^2}$$

which also ends up giving the Fibonacci numbers (moved one position to the right).

Finally, let us consider the composition of numbers into an even number of parts. Here we do not have any restriction in the numbers we can use, so we take $\mathbb{N}$ as the basic class. Then,

$$\mathcal{I}^{\text{even}} = \varepsilon + \mathbb{N}^2 + \mathbb{N}^4 + \cdots = \text{Seq}(\mathbb{N}^2)$$

So the generating function is

$$I^{\text{even}}(z) = \frac{1}{1-N(z)^2} = \frac{1}{1-(z/(1-z))^2}$$

1.2.2 Integer partitions

Definition 1.2.2 (Partition of a number)**.** A partition of n is a tuple of positive integers $(a_1, \dots, a_k)$ such that $n = a_1 + \cdots + a_k$ and $a_1 \leq \cdots \leq a_k$.

Observe that we consider $(1, 2)$ and $(2, 1)$ to be different compositions, but they both correspond to the same partition. This multiplicity makes the problem of counting partitions much more difficult.

Definition 1.2.3 (Class of partitions)**.** The class $\mathcal{P}$ of integer partitions is the class where the objects are k-tuples of positive integers such that $a_1 \leq a_2 \leq \cdots \leq a_k$, and their size is $|(a_1, \dots, a_k)| = \sum a_i$.

A symbolic description of this class is

$$\mathcal{P} = \text{Seq}(\{1\}) \times \text{Seq}(\{2\}) \times \dots$$

as any partition is defined by the number of ones, twos, threes, ... that it contains. Therefore, the generating function is

$$P(z) = \prod_{n \geq 1} \frac{1}{1 - z^n}$$

which is known as the *partition function*.

In order to find the number of partitions of n, we need to compute $[z^n]P(z)$, which is far from trivial. However, there are very sharp asymptotics, which are derived using complex analysis tools.

We will concern ourselves with simpler problems. For example, let us count the number of partitions with elements in $\{1, 2\}$. By the same argument as before,

$$\begin{aligned} P_{1,2}(z) = \frac{1}{1-z}\frac{1}{1-z^2} = \frac{1}{(1-z)^2}\frac{1}{1+z} = \frac{1}{4}\frac{1}{1-z} + \frac{1}{2}\frac{1}{(1-z)^2} + \frac{1}{4}\frac{1}{1+z} = \\ = \frac{1}{4}\sum_{n\geq 0} z^n + \frac{1}{2}\sum_{n\geq 0}(n+1)z^n + \frac{1}{4}\sum_{n\geq 0}(-1)^n z^n \end{aligned}$$

Therefore, the number of partitions of n is

$$[z^n]P_{1,2}(z) = \begin{cases} \frac{n+2}{2}, & n \text{ even} \\ \frac{n+1}{2}, & n \text{ odd} \end{cases}$$

Example 1.2.1. In the problem sheet we discuss Frobenius' change problem. The statement is the following. Given a finite number of coin values $T = \{b_1, \dots, b_k\}$, we want to find the number of ways of paying a quantity of n using those coins.

By using the previous result, the generating function is

$$P_T(n) = \frac{1}{1 - z^{b_1}} \cdots \frac{1}{1 - z^{b_k}}$$

This function is analytic inside the circle of radius 1, but it has poles at the b_i-roots of unity (for every $i \in [k]$). Therefore, if $\gcd(b_1, \dots, b_k) = 1$, there are no poles with multiplicity k except for $z = 1$. Then, it can be proved that

$$[z^n]P_T(z) \sim \frac{1}{b_1 \dots b_k} \frac{n^{k-1}}{(k-1)!}$$

Besides, for a finite set of b_i, one can find that the number of partitions and the number of compositions is asymptoptically related. We will find out more about this result in the exercises.

1.2.3 Partitions of sets

Let us consider the set $[n]$ (which may be used to represent any n-element set).

Definition 1.2.4 (Partition of a set)**.** A partition of a set is a collection of non-empty disjoint subsets such that every element is in some subset.

We are going to count the number of partitions of $[n]$ into k parts, which is known as the *Stirling number of second kind* and denoted by $\left\{ {n \atop k} \right\}$.

Let $\mathcal{B} = \{b_1, \dots, b_k\}$ be an alphabet with k letters. Then, each partition of $[n]$ corresponds to a word of length n using the alphabet $\mathcal{B}$ (assigning a letter to each part and writing for every $i \in [n]$ the letter corresponding to the part it belongs to). However, there are multiple words which correspond to the same partition, as the way in which we label the k parts is irrelevant.

One way to solve this issue is to order the parts by their minimum elements and assigning the labels $b_1, \dots, b_k$ by this order. Then, we get that $\min b_1 < \min b_2 < \dots < \min b_k$.

Now not all the words of length n as valid, as any symbol b_i can not appear before the first b_j symbol, where $j < i$. It can be easily seen that this procedure establishes a bijection. Therefore, the number of partitions of $[n]$ into k parts is the same as the number of words of n letters from an alphabet of size k and such that each letter b_i does not appear before the first letter b_{i-1}.

This results in the following symbolic description:

$$\mathcal{P} = \{b_1\} \times \mathrm{Seq}(\{b_1\}) \times \{b_2\} \times \mathrm{Seq}(\{b_1, b_2\}) \times \dots \times \{b_k\} \times \mathrm{Seq}(\{b_1, \dots, b_k\})$$

Therefore, the generating function of the number of partitions into k parts is

$$P_k(z) = z \cdot \frac{1}{1-z} \cdot z \cdot \frac{1}{1-2z} \dots z \cdot \frac{1}{1-kz} = z^k \prod_{i=1}^{k} \frac{1}{1-iz}$$

Let us decompose the product into partial fractions:

$$P_k(z) = z^k \sum_{i=1}^{k} \frac{A_i}{1-iz} = z^k \sum_{i=1}^{k} A_i \sum_{n \geq 0} i^n z^n$$

Computing A_i explicitly we get a formula for the Stirling numbers of the second kind:

$$\left\{ {n \atop k} \right\} = [z^n]P_k(z) = \frac{1}{k!} \sum_{j=1}^{k} \binom{k}{j} j^n (-1)^{k-j}$$

1.3 Formal Power Series

1.3.1 Definition

Consider the set of sequences $(a_0, a_1, \dots)$ of complex numbers. We can define the sum of two such sequences as

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) := (a_0 + b_0, a_1 + b_1, \dots)$$

which endows this set with the structure of an abelian group.

We can also define a product:

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (a_0 b_0, a_1 b_0 + a_0 b_1, \dots, \sum_{k=0}^{n} a_k b_{n-k}, \dots)$$

which is known as *convolution*.

With this two operations we obtain a ring of formal power series, which we denote by $\mathbb{C}[[z]]$, and where we identify the sequence $(a_0, a_1, \dots)$ with the power series $a_0 + a_1 z + \dots$.

The ring of formal power series is not a field, because not every element has a multiplicative inverse:

Proposition 1.3.1. *$A(z)$ is invertible (with respect to the product) if and only if $a_0 \neq 0$.*

Proof. If there is a $B(z)$ such that $B(z)A(z) = 1$, then $1 = [z^0]B(z)A(z) = a_0 b_0 \implies a_0 \neq 0$.

Reciprocally, if $a_0 \neq 0$, we can construct an inverse explicitly:

$$[z^0]A(z)B(z) = a_0 b_0 = 1 \implies b_0 := a_0^{-1}$$
$$[z^n]A(z)B(z) = \sum_{k=0}^{n} a_k b_{n-k} = 0 \implies b_n := a_0^{-1}\left(-\sum_{k=1}^{n} a_k b_{n-k}\right)$$

□

Example 1.3.1.

1. We have used that $1 + z + z^2 + \cdots = 1/(1-z)$. In terms of formal power series, this means that the series $1 - z$ is the inverse of $1 + z + z^2 + \dots$. We can check that indeed

$$[z^n](1-z)\sum_{n\geq 0} z^n = \begin{cases} 1 - 1 = 0, & \text{if } n \geq 1 \\ 1, & \text{if } n = 0 \end{cases}$$

   If we take the power of both sides, we get the equality

$$\frac{1}{(1-z)^m} = \left(\sum_{n\geq 0} z^n\right)^m = \sum_{n\geq 0} \binom{n+m-1}{n} z^n$$

   The reason why binomial coefficients appear is that $[z^n]\left(\sum_k z^k\right)^m$ is the number of ways of choosing m ordered non-negative integers that sum to n. We can picture this situation as

writing a word of $n+m-1$ characters where we have to place n ones and $m-1$ "separation tokens". There are $\binom{n+m-1}{n}$ possible words, and each word corresponds bijectively to one way of choosing the m summands.

2. We define the exponential series as

$$e^z := \sum_{n\geq 0} \frac{z^n}{n!}$$

and similarly

$$\log\left(\frac{1}{1-z}\right) := \sum_{n\geq 1} \frac{z^n}{n}$$

We can also define the *formal derivative* of a series:

$$A(z)' := \sum_{n\geq 1} n a_n z^{n-1}$$

This definition mimicks the analytic notion of derivative, and as such inherits most properties of the usual derivative (linearity, product rule, etc.).

Another operation we can perform with formal power series is *composition*:

$$A(B(z)) := \sum_{n\geq 0} a_n (B(z))^n$$

We need to be cautious because, following the definition given above, $[z^n]A(B(z))$ might not be finite for some $B(z)$ and therefore $A(B(z))$ would not be in the ring we previously defined.

We can solve this problem by only defining the composition for series with $b_0 = 0$. Then,

$$[z^n]A(B(z)) = [z^n](a_0 + a_1 B(z) + a_2 B(z)^2 + \cdots + a_n B(z)^n)$$

where we have left out the infinite tail of the series because $B(z)^m$ lowest term will be at least of the order of z^m.

Let's suppose we have a series with $a_0 = 0$, which can not be inverted. If we write it as

$$A(z) = z^k \underbrace{(a_k + a_{k+1}z + \dots)}_{A_1(z)}$$

where $a_k \neq 0$, then $A_1(z)$ can be inverted, giving another series $B(z)$. Then,

$$A^{-1}(z) = \frac{1}{z^k} B(z) = \frac{b_0}{z^k} + \frac{b_1}{z^{k-1}} + \cdots + b_k + b_{k+1}z + \dots$$

Therefore, if we consider also the formal power series with a finite number of terms with negative exponent, we get a field, which is called the field of *Laurent series*, or $\mathbb{C}((z))$.

1.3.2 Lagrange Inversion Formula

Definition 1.3.1 (Residue)**.** The coefficient of z^{-1} in a Laurent series is called its *residue*. We will denote it by $\text{Res}(A(z)) := [z^{-1}]A(z)$.

Proposition 1.3.2. *Let $A(z)$ be a formal power series with $a_0 = 0$ and $a_1 \neq 0$. Let $B(z)$ be its functional inverse in the field of Laurent series (that is, the $B(z)$ such that $B(A(z)) = z$). Then,*

$$b_n = [z^{-1}]\left(\frac{1}{nA(z)^n}\right)$$

Proof. We will need the following two lemmas:

Lemma 1.3.1. *If $A(z) \in \mathbb{C}((z))$, then $\text{Res}(A'(z)) = 0$.*

Proof: It can be checked by differentiating term by term. □

Lemma 1.3.2. *If $A(z) = \sum_{n \geq -k} a_n z^n$, then $\text{Res}(A'(z)/A(z)) = -k$.*

Proof: Left as exercise. □

We need to find $B(z)$ such that

$$B(A(z)) = b_0 + b_1 A(z) + b_2 (A(z))^2 + \cdots = z$$

For a fixed n, by differentiating the equality and dividing by $A(z)^n$, we get that

$$\frac{1}{A(z)^n} \sum_k k b_k A'(z)(A(z))^{k-1} = \frac{1}{A(z)^n}$$

We take the residue on both sides. By the definition, the residue is linear, so

$$\text{Res}\left(\frac{1}{A(z)^n} \sum_k k b_k A'(z)(A(z))^{k-1}\right) = \sum_k k b_k \,\text{Res}(A'(z)A(z)^{k-n-1}) = \text{Res}\left(\frac{1}{A(z)^n}\right)$$

The terms with $k \neq n$ are equal to a constant times the residue of the derivative of $A(z)^{k-n}$, so by lemma 1.3.1 they vanish. We are left with

$$n b_n \,\text{Res}\left(\frac{A'(z)}{A(z)}\right) = \text{Res}\left(\frac{1}{A(z)^n}\right)$$

It can be checked that the first non-zero term of $A'(z)/A(z)$ is the one with exponent 1, so using lemma 1.3.2 we get that $\text{Res}(A'(z)/A(z)) = 1$. Then the result follows. □

As a direct consequence of the previous proposition we have the Lagrange Inversion Formula, which we are going to use extensively:

Theorem 1.3.1 (Lagrange Inversion Formula)**.** *Let $\phi(z) = \sum_{n \geq 0} a_n z^n$, with $a_0 \neq 0$. Then, if $A(z) = z\phi(A(z))$, we have that*

$$[z^n]A(z) = \frac{1}{n}[z^{n-1}]\phi(z)^n$$

Proof. We have that

$$\frac{A(z)}{\phi(A(z))} = z$$

so $B(z) = z/\phi(z)$ is the functional inverse of $A(z)$. Therefore, by proposition 1.3.2,

$$[z^n]A(z) = \frac{1}{n}[z^{-1}]\frac{1}{B(z)^n} = \frac{1}{n}[z^{-1}]\left(\frac{\phi(z)}{z}\right)^n = \frac{1}{n}[z^{n-1}](\phi(z))^n$$

□

The Lagrange Inversion Formula is very useful because usually it is straightforward to derive a functional relation for the generating function of a combinatorial class, and then we can get the coefficients by applying this formula. There is an extension of the formula that we are also going to use:

Theorem 1.3.2 (Bürmann-Lagrange Inversion Formula)**.** *Let $\phi(z) = \sum_{n\geq 0} b_n z^n$, with $b_0 \neq 0$. Let $A(z)$ be a generating function satisfying the equation $A(z) = z\phi(A(z))$. Then, for any analytic function g,*

$$[z^n]g(A(z)) = \frac{1}{n}[z^{n-1}]\phi(z)^n g'(z)$$

For instance, if we are interested in knowing the coefficients of $A(z)^k$, we get that

$$[z^n]A(z)^k = \frac{1}{n}[z^{n-1}]\phi(z)^n k z^{k-1} = \frac{k}{n}[z^{n-k}]\phi(z)^n$$

1.4 Further examples

Now that we have seen the Lagrange Inversion Formula, let us examine a few more examples of the symbolic method where it is used.

1.4.1 Dyck Paths

Definition 1.4.1 (Dyck Path)**.** A *Dyck path* is a sequence of steps $(x, y) \to (x + 1, y + 1)$ or $(x, y) \to (x + 1, y - 1)$ in $\mathbb{Z}^2$ that starts at $(0, 0)$, ends at $(2n, 0)$, and never crosses the line $\{y = 0\}$.

If we denote by D_n the number of Dyck paths of length $2n$, then $D_1 = 1$, $D_2 = 2$ and $D_3 = 5$. For example, the 5 paths of length 6 are the following:

- ↗↗↗↘↘↘
- ↗↗↘↗↘↘
- ↗↗↘↘↗↘
- ↗↘↗↗↘↘
- ↗↘↗↘↗↘

We can define the combinatorial class of Dyck paths as the set

$$\mathcal{D} = \left\{ (x_1, \ldots, x_{2n}) : x_i \in \{1, -1\}, \sum_{i=1}^{2n} x_i = 0, \sum_{i=1}^{k} x_i \geq 0, \forall k \in [2n], n \in \mathbb{N} \right\}$$

where the size of a path is its length, $2n$.

We can find a symbolic description of this class by applying recursion. We notice that the first step must always be up. Then, we can divide the path into two Dyck paths: the one from the beggining until it first touches the $\{y = 0\}$ line again, and the one from there until the end (this second path can be an empty path). Therefore,

$$\mathcal{D} = \{\varepsilon\} + \{\nearrow\} \times \mathcal{D} \times \{\searrow\} \times \mathcal{D}$$

This recursive description yields a functional equality for the generating function:

$$D(z) = 1 + z \cdot D(z) \cdot z \cdot D(z) = 1 + z^2 D(z)^2$$

Let us rearrange the equation so we can use the Lagrange Inversion Formula. Let $V(z) := zD(z)$. Then,

$$V(z) = z + zV(z)^2 = z(1 + V(z)^2)$$

Applying the Lagrange Inversion Formula with $\phi(z) = 1 + z^2$, we get that the coefficients of $V(z)$ are

$$[z^n]V(z) = \frac{1}{n}[z^{n-1}](1 + z^2)^n = \frac{1}{n}[z^{n-1}] \sum_{k=0}^{n} \binom{n}{k} z^{2k}$$

We need $2k = n - 1$, so

$$[z^n]V(z) = \begin{cases} \frac{1}{n}\binom{n}{(n-1)/2}, & n \text{ odd} \\ 0, & n \text{ even} \end{cases}$$

We defined $V(z) = zD(z)$, so

$$[z^{2n}]D(z) = [z^{2n+1}]V(z) = \frac{1}{2n+1}\binom{2n+1}{n} = \frac{1}{n+1}\binom{2n}{n}$$

which is the n-th Catalan number, a sequence we will encounter in many other combinatorial problems.

From the equation $D(z) = 1 + z^2 D(z)^2$, we could also have proceeded with a purely algebraic approach, solving it as a second-degree equation:

$$z^2 D^2(z) - D(z) + 1 = 0 \implies D(z) = \frac{1 \pm \sqrt{1 - 4z^2}}{2z^2}$$

Using Newton's binomial formula, we get

$$(1 - 4z^2)^{1/2} = \sum_{n \geq 0} \binom{1/2}{n} (-1)^n 4^n z^{2n} = 1 - \frac{1}{2} 4z^2 + \ldots$$

where for this equality to make sense we need to define $\binom{\alpha}{n} := \alpha(\alpha-1)\dots(\alpha-n+1)/n!$, for arbitrary $\alpha \in \mathbb{C}$.

In order to get a proper generating function, we need to take the solution with the minus sign, which will give us the same generating function we obtained with the Lagrange Inversion Formula.

1.4.2 Plane trees

Definition 1.4.2 (Plane trees)**.** The combinatorial class of plane trees $\mathcal{T}$ is the class of rooted trees embedded in the plane, where the size of a tree is its number of vertices.

What we mean about the trees being embedded in the plane is that the order of the children matters, so we will consider two trees different if at some node they have two non-identical children subtrees in different order. Instead, if we considered the tree as an abstract object (not embedded in the plane), the order of the children subtrees would not matter for considering two trees equal.

We can express this class symbolically as

$$\mathcal{T} = \mathcal{N} \times \mathrm{Seq}(\mathcal{T})$$

where $\mathcal{N}$ is the class with one element of size 1. This gives the following equation for the generating function:

$$T(z) = z\frac{1}{1-T(z)}$$

Note that we do not admit a tree with no nodes as a valid tree.

In order to find its coefficients, we use the Lagrange Inversion Formula with $\phi(z) = 1/(1-z)$:

$$[z^n]T(z) = \frac{1}{n}[z^{n-1}]\phi(z)^n = \frac{1}{n}[z^{n-1}]\frac{1}{(1-z)^n} = \frac{1}{n}\binom{2(n-1)}{n-1} = C_{n-1}$$

We obtain that the number of plane trees with n vertices is the $(n-1)$-th Catalan number.

Seeing that there is the same number of plane trees with $n-1$ vertices as Dyck paths of length $2n$, one might wonder if we are able to construct an explicit bijection between both classes.

In this case, this can be easily done. Given a tree, we start at the root and travel along the edges (visiting the children of a node in order from left to right). When we go downwards, we add $\{\nearrow\}$ to the Dyck path, and when we go upwards we add $\{\searrow\}$ to the path.

We will never have more $\{\searrow\}$ steps than $\{\nearrow\}$ steps, because that would mean we are further up than the root. Besides, the traversal will end at the root, having done as many upward steps as downward ones. Therefore, the result will be a valid Dyck path.

The other direction of the bijection can also be constructed easily.

One of the advantages of the symbolic method is that it allows us to treat many variations of the problem in a very similar fashion:

- **Rooted plane trees in which every node has an even number of children**:

  The symbolic description is

  $$\mathcal{T} = \mathcal{N} \times \text{Seq}(\mathcal{T}^2)$$

  which gives the following equation for the generating function

  $$T(z) = z\frac{1}{1 - T(z)^2}$$

  In order to find the coefficients explicitly we would use once again the Lagrange Inversion Formula.

- **Rooted plane trees in which every node has 1 or 2 children**:

  The symbolic description is $\mathcal{T} = \mathcal{N} \times (\mathcal{T} + \mathcal{T}^2)$ which gives the following equality for the generating function:

  $$T(z) = z(T(z) + T(z)^2) \implies T(z) = -1 + 1/z$$

  This is not a valid generating function. Going back to the statement of the problem, we notice that a tree where every node has 1 or 2 children would not be finite, so it makes no sense to ask how many such trees of size n there are.

  This is another powerful characteristic of the generating functions. They sometimes allow us to see if we have made an error in the symbolic description.

- **Rooted plane trees where every node has 0 or 2 children**:

  These are usually called *binary trees*, and denoted by $\mathcal{B}$. There are two versions of this problem, depending on how we define the size of a tree. If we consider the size of a tree to be its number of vertices, then we would get the usual symbolic description

  $$\mathcal{B} = \mathcal{N} \times (\{\varepsilon\} + \mathcal{B}^2)$$

  Instead, if we consider the size of a tree to be the number of *internal* vertices it has (that is, vertices that are not leaves), then the symbolic description would be

  $$\mathcal{B} = \{\varepsilon\} + \mathcal{N} \times \mathcal{B}^2$$

  which gives the following equality for the generating function:

  $$B(z) = 1 + zB(z)^2$$

  In order to apply the Lagrange Inversion Formula, we first rearrange the equation:

  $$B(z) - 1 = z((B(z) - 1) + 1)^2$$

  Taking $\phi(z) = (z + 1)^2$ and $V(z) = B(z) - 1$ we get

  $$[z^n]V(z) = \frac{1}{n}[z^{n-1}](z + 1)^{2n} = \frac{1}{n}\binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n} = C_n$$

So the number of binary trees with n internal nodes is

$$b_n = \begin{cases} 1, & n = 0 \\ C_n, & n \geq 1 \end{cases}$$

Therefore, we have seen that $b_n = t_{n+1}$. There is indeed an explicit bijection between plane trees with $n + 1$ vertices and binary trees with n internal vertices, but it is quite complicated. Instead, it is easier to construct a bijection between binary trees and Dyck paths, and then use the bijection we have seen between Dyck paths and plane trees.

This example allows us to illustrate that the size function we take is a conscious choice. Usually, it is obvious what size function we must take given the nature of the object we want to count, but in some cases it might be useful to take a non-standard size function in order to count something more easily.

2 Labeled Classes

2.1 EGFs and Labeled Classes

2.1.1 Exponential Generating Functions

For studying labeled classes we are going to use a different kind of generating functions:

Definition 2.1.1 (Exponential generating functions)**.** Let $a = (a_0, a_1, \dots,)$ be a sequence. We define the exponential generating function (EGF) of a as

$$A(z) = \sum_{n\geq 0} \frac{a_n}{n!} z^n$$

- **Sum:** If $A(z)$ and $B(z)$ are EGF's of a and b, then $C(z) = A(z) + B(z)$ is the EGF of $a + b$.
- **Product:** If we do the product of two EGF's we obtain

$$C(z) = A(z)B(z) = \sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_k b_{n-k}}{k!(n-k)!} z^n = \sum_{n\geq 0} \frac{1}{n!} \left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \right) z^n$$

  which is the EGF of the sequence c with terms

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

  This special kind of product is the reason we use EGF's when working with labeled classes.

If $A(z)$ is the EGF of sequence a, then we can obtain the terms of the sequence as $a_n = n![z^n]A(z)$.

2.1.2 Labeled classes

Definition 2.1.2 (Labeled class)**.** We say that a combinatorial class is *labeled* if the objects are graphs with labeled nodes (from 1 up to n). The size of an object is defined as its number of nodes.

Example 2.1.1.

1. **Class of urns:** The class of urns $\mathcal{U}$ is the class of edgeless labeled graphs:

   $$\mathcal{U} = \{\varepsilon,\ \textcircled{1}\ ,\ \textcircled{1}\ \textcircled{2}\ ,\ \dots\}$$

   For each n, there is a unique labeled edgeless graph of size n, so $U_n = 1$. Therefore, the EGF is $U(z) = \sum_{n\geq 0} z^n/n! = e^z$.

2. **Permutations:** The class of permutations $\mathcal{P}$ is the class of directed paths:

   $$\mathcal{P} = \{\varepsilon,\ \textcircled{1}\ ,\ \textcircled{1}\!\!\longrightarrow\!\!\textcircled{2}, \textcircled{2}\!\!\longrightarrow\!\!\textcircled{1},\ \dots\}$$

   There are $n!$ labeled directed paths of size n, so the coefficients are $P_n = n!$ and the EGF of the class of permutations is $P(z) = \sum_{n\geq 0} z^n = 1/(1-z)$.

3. **Cycles:** The class of cycles is the class that has directed cycles as objects:

   $$\mathcal{C} = \left\{ \textcircled{1}\!\circlearrowright\ ,\ \textcircled{1}\rightleftarrows\textcircled{2},\ \textcircled{1}\!\to\!\textcircled{2}\!\to\!\textcircled{3}\!\to\!\textcircled{1},\ \textcircled{1}\rightleftarrows\textcircled{2}\rightleftarrows\textcircled{3}\rightleftarrows\textcircled{1},\ \dots \right\}$$

   The number of labeled directed cycles of size n is $(n-1)!$, so the EGF is

   $$C(z) = \sum_{n\geq 1} \frac{z^n}{n} = -\log(1-z)$$

2.2 Operations on labeled classes

- **Sum:** $\mathcal{C} = \mathcal{A} + \mathcal{B}$. We take the disjoint union of the objects of $\mathcal{A}$ and $\mathcal{B}$. The resulting EGF is $C(z) = A(z) + B(z)$.
- **Labeled Product:** $\mathcal{C} = \mathcal{A} * \mathcal{B}$. The objects of $\mathcal{C}$ are pairs $(\alpha, \beta) \in \mathcal{A} \times \mathcal{B}$. In order to define the operation properly, we need to decide how to label the elements of $\mathcal{C}$.

  For a sequence of n distinct integers $(a_1, \dots, a_n)$, we denote its *reduction* $\rho(a_1, \dots, a_n)$ as the unique permutation $\sigma \in S_n$ that is order-preserving (i.e. $a_i < a_j \iff \sigma_i < \sigma_j$). For example, $\rho(6, 9, 7, 5) = (2, 4, 3, 1)$.

  Then we define the labeling of $\mathcal{C}$ as follows:

  $$\alpha * \beta = \left\{ (\alpha', \beta') : \begin{array}{c} \alpha' \text{ is labeled with } |\alpha| \text{ numbers in } [|\alpha| + |\beta|] \text{ and } \beta' \text{ is labeled with} \\ |\beta| \text{ numbers in } [|\alpha| + |\beta|] \text{ such that } \rho(\alpha') = \alpha \text{ and } \rho(\beta') = \beta \end{array} \right\}$$

For example,

$$(1,2) * (1,3,2) = \{((1,2),(3,5,4)),((1,3),(2,5,4)),\dots\}$$

Therefore, $|\alpha * \beta| = \binom{|\alpha|+|\beta|}{|\alpha|}$. We will later see in the examples why this definition of product is the natural one when working with labeled classes.

The EGF of the product is

$$\begin{aligned} C(z) &= \sum_{\alpha\in\mathcal{A},\beta\in\mathcal{B}} \sum_{(\alpha',\beta')\in\alpha*\beta} \frac{z^{|\alpha|+|\beta|}}{(|\alpha|+|\beta|)!} = \sum_{\alpha\in\mathcal{A},\beta\in\mathcal{B}} \frac{z^{|\alpha|+|\beta|}}{|\alpha|!\ |\beta|!} = \left(\sum_{\alpha\in\mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!}\right)\cdot\left(\sum_{\beta\in\mathcal{B}} \frac{z^{|\beta|}}{|\beta|!}\right) \\ &= A(z)B(z) \end{aligned}$$

- **Sequence:** $\operatorname{Seq}(A) = \varepsilon + \mathcal{A} + \mathcal{A} * \mathcal{A} + \cdots + \mathcal{A}^k + \dots$. The generating function will be

$$C(z) = 1 + A(z) + A(z)^2 + \cdots = \frac{1}{1-A(z)}$$

- **Set:** The class of sets of $\mathcal{A}$ with cardinality k is $\operatorname{SET}(\mathcal{A}, \operatorname{card} = k) = \overbrace{\mathcal{A} * \cdots * \mathcal{A}}^{k} / \sim$, where $\sim$ is the equivalence relation that identifies two objects with the same elements (despite being in a different order). As the objects are labeled, they are distinguishable, so every equivalence class has $k!$ elements. This makes this operation much more useful than in the non-labeled setting.

  We also define the class of sets of $\mathcal{A}$ as the class of sets of any cardinality: $\operatorname{SET}(\mathcal{A}) := \sum_{k\geq 0} \operatorname{SET}(\mathcal{A}, \operatorname{card} = k)$. The generating function of the resulting class is

$$C(z) = 1 + A(z) + \frac{A(z)^2}{2!} + \frac{A(z)^3}{3!} + \cdots = e^{A(z)}$$

There exist other operations with labeled classes but these are the ones we are going to use.

2.3 Examples

2.3.1 Permutations

We know that a permutation of $[n]$ can be expressed uniquely as a product of cycles. For example, 3125764 is expressed as $(123)(457)(6)$. Therefore, the class of permutations can be expressed symbolically as $\mathcal{P} = \operatorname{SET}(\mathcal{C})$. We can check that the EGF given by this relation is

$$P(z) = e^{C(z)} = e^{-\log(1-z)} = \frac{1}{1-z}$$

which is the EGF of the class of permutations.

We already knew the EGF of the class of permutations, but this symbolic description is very useful because it allows us to count many classes related to permutations:

Derangements

Definition 2.3.1 (Derangement)**.** A *derangement* is a permutation without any fixed points.

If we denote the class of derangements as $\mathcal{D}$, we see that $\mathcal{D} = \text{SET}(\mathcal{C} - \mathcal{C}_1)$, where $\mathcal{C}_1$ is the class of cycles of length 1 (which only has one element). Then, the EGF is

$$D(z) = \exp\left(\log\frac{1}{1-z} - z\right) = \frac{e^{-z}}{1-z}$$

So the number of derangements of size n is

$$d_n = n![z^n]D(z) = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} \sim \frac{n!}{e}$$

This problem could also be solved by the inclusion-exclusion principle, but the solution using the symbolic method is much more straight-forward.

Involutions

Definition 2.3.2 (Involution)**.** An *involution* is a permutation $\sigma \in S_n$ such that $\sigma^2 = \text{Id}$.

A permutation σ can only be an involution if it is decomposed in cycles of length 1 and 2. Therefore, we can express the class of involutions as $\mathcal{I} = \text{SET}(\mathcal{C}_1 + \mathcal{C}_2)$. Then, the EGF of this class is

$$I(z) = \exp(z + z^2/2) = e^z e^{z^2/2}$$

From here we obtain a formula for the number of involutions of size n:

$$I_n = n![z^n]I(z) = n![z^n]\left(\sum_{k\geq 0}\frac{z^k}{k!}\right)\left(\sum_{m\geq 0}\frac{z^{2m}}{m!2^m}\right) = \sum_{\ell=0}^{\lfloor n/2\rfloor}\frac{n!}{\ell!(n-2\ell)!2^\ell}$$

Permutations with k cycles

Let us count now the number of permutations with exactly k cycles. We will denote this class as $\mathcal{P}^{(k)}$. A symbolic description is given by $\mathcal{P}^{(k)} = \text{SET}(\mathcal{C}, \text{card} = k)$. This gives us the following EGF

$$P^{(k)}(z) = \frac{1}{k!}C(z)^k = \frac{1}{k!}\left(\log\frac{1}{1-z}\right)^k$$

The n-th coefficient can be expressed as

$$P_n^{(k)} = n![z^n]P^{(k)}(z) = \frac{n!}{k!}\sum_{\substack{i_1+\cdots+i_k=n\\ i_j\geq 1}}\frac{1}{i_1\cdots i_k} = \begin{bmatrix} n \\ k \end{bmatrix}$$

The coefficients $\begin{bmatrix} n \\ k \end{bmatrix}$ are called *Stirling numbers of the first kind* or *Stirling permutation numbers*, and they were originally defined as

$$\begin{bmatrix} n \\ k \end{bmatrix} := [z^k] z(z+1)\dots(z+n-1)$$

which can be proved by induction using the following recursive relation:

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = n \begin{bmatrix} n \\ k \end{bmatrix} + \begin{bmatrix} n \\ k-1 \end{bmatrix}$$

This formula comes from the fact that the permutations of $n+1$ elements with k cycles can be expressed as the disjoint union of the permutations of n elements with $k-1$ cycles (which we extend to a permutation of $[n+1]$ by adding the $(n+1)$-th element as a fixed point), and the permutations of n elements with k cycles (where we add the element $n+1$ in one of the n available positions inside the existing cycles).

By convention we take $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$, and $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ n \end{bmatrix} = 0$.

From the combinatorial definition it is easy to see that

$$\sum_{k=1}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$$

because there are $n!$ permutations of size n, and they can not have more than n cycles.

2.3.2 Partitions of sets

Let $\mathcal{P}$ be the class of partitions of sets where each element is labeled (and we don't allow empty subsets). We have already seen how to count them using unlabeled classes, but this problem is more naturally approached using labeled classes.

We observe that we can express a partition of a set as a set of labeled sets (which we had called urns). Therefore, $\mathcal{P} = \mathrm{SET}(\mathcal{U} - \varepsilon)$, so

$$P(z) = e^{U(z)-1} = e^{e^z - 1}$$

The coefficients of this EGF are called *Bell numbers*, and are given by

$$B_n = n![z^n]e^{e^z-1} = \frac{n!}{e}[z^n] \sum_{k\geq 0} \frac{e^{kz}}{k!} = \frac{n!}{e} \sum_{k\geq 0} \frac{1}{k!}[z^n] \sum_{m\geq 0} \frac{(kz)^m}{m!} = \frac{1}{e} \sum_{k\geq 0} \frac{k^n}{k!}$$

Let us suppose now that we are only interested in partitions of $[n]$ into k parts. We can express this class as

$$\mathcal{P}^{(k)} = \mathrm{SET}(\mathcal{U} - \varepsilon, \mathrm{card} = k) = (\mathcal{U} - \varepsilon)^k / \sim$$

which gives rise to the EGF

$$P^{(k)}(z) = \frac{(e^z - 1)^k}{k!}$$

The n-th coefficient will be

$$P_n^{(k)} = n![z^n]P^{(k)}(z) = \frac{n!}{k!}[z^n](e^z-1)^k = \cdots = \left\{ {n \atop k} \right\}$$

A result we had already seen in the first chapter.

2.3.3 Words

A word of length n in an alphabet $A = \{a_1, \ldots, a_r\}$ can be described as a sequence of pairwise disjoint sets $(f^{-1}(a_1), \ldots, f^{-1}(a_r))$, where $f : [n] \longrightarrow A$ is the function that gives the letter appearing at each position. For example, the word $a_1a_2a_1a_3a_2a_1$ in the alphabet $A = \{a_1, a_2, a_3, a_4\}$ would correspond to the sequence $(\{1,3,6\}, \{2,5\}, \{4\}, \{\emptyset\})$.

Therefore, we can represent the class of words symbolically as $\mathcal{W} = \mathcal{U}^r$, where $\mathcal{U}$ is the class of urns. The exponential generating function of the class of words is

$$W(z) = U(z)^r = e^{zr}$$

and the number of words of length n is

$$w_n = n![z^n]e^{rz} = r^n$$

Again, we could have reached this result by simpler methods, but having a symbolic description of the class allows us to easily count many related classes. For example, suppose we want to count the number of maps from $[n]$ to $[r]$ such that every element of $[r]$ has at least 2 preimages. This corresponds to the number of words formed by a sequence of sets of size at least 2. Then,

$$\mathcal{W}^{\geq 2} = (\mathcal{U} - \varepsilon - \mathcal{U}_1)^r$$

and the EGF is

$$W^{\geq 2}(z) = (e^z - 1 - z)^r$$

If we wanted to count the number of words where a_1 appears ≥ 3 times, a_2 appears ≤ 3 times and $a_3, \ldots, a_r$ appear an arbitrary number of times, then the symbolic description would be

$$\mathcal{W} = (\mathcal{U} - \varepsilon - \mathcal{U}_1 - \mathcal{U}_2) * (\varepsilon + \mathcal{U}_1 + \mathcal{U}_2 + \mathcal{U}_3) * \mathcal{U}^{r-2}$$

2.3.4 Labeled trees

Let $\mathcal{T}$ be the class of rooted labeled trees (trees where each vertex has a label, the root is specified, and the order of children of a node does not matter). According to this specifications, we can describe a tree as a node together with a set of trees:

$$\mathcal{T} = \mathcal{N} \times \mathrm{SET}(\mathcal{T})$$

Therefore, the EGF satisfies the following equation

$$T(z) = ze^{T(z)}$$

By the Lagrange Inversion Formula, the number of rooted labeled trees with n vertices is

$$t_n = n! \left(\frac{1}{n} [z^{n-1}](e^z)^n \right) = n^{n-1}$$

Cayley's Formula tells us that the number of labeled trees of n vertices is n^{n-2}. This agrees with our result, as the number of rooted trees of n vertices is the number of unrooted trees multiplied by n.

3

Enumeration with symmetries

Suppose you want to count the number of graphs with 4 vertices. If we work with labelled classes, we would obtain 6 different graphs that have only 1 edge, but all of them are essentially the same (up to isomorphism). In this chapter we will see Polya's theorem, a result that will enable us to take this kind of symmetries into account.

Another example of the kind of problems we will be able to solve is to count the number of positions of a Rubik's cube by describing its group of symmetries.

3.1 Group actions

Definition 3.1.1 (Group)**.** A group is a set equipped with an associative binary operation that has an identity element id such that $\sigma(\mathrm{id}) = \mathrm{id}(\sigma) = \sigma$ for all $\sigma \in G$, and every element $\tau \in G$ has an inverse τ^{-1} such that $\tau^{-1}\tau = \tau\tau^{-1} = \mathrm{id}$.

From here on we will suppose all groups we work with are finite.

Example 3.1.1. A basic example of a group is the set of permutations $G = \{\mathrm{id}, (123), (132)\} \subset S_3$, where we take composition as the binary operation.

Definition 3.1.2 (Subgroup)**.** A *subgroup* H is a subset of G which is in itself a group.

Definition 3.1.3 (Left coset)**.** A *left coset* of a subgroup H is $\sigma H = \{\sigma h : h \in H\}$ for some $\sigma \in G$.

Proposition 3.1.1. *Let H be a subgroup of G. Then, $|H|$ divides $|G|$.*

Proof. We observe that $\sigma \in \sigma H$, so any element of G is included in some coset of H. Besides, two cosets of the same subgroup are either the same or completely disjoint. This is because if

$a \in \sigma H$ and $a \in \tau H$, then $\sigma = \tau h_2 h_1^{-1}$ for some $h_1, h_2 \in H$, so $\sigma H \subset \tau H$ (due to the closure of H). The other inclusion is analogously proved.

Therefore, we can partition G into disjoint cosets of H. All the cosets have size $|\sigma H| = |H|$ (if $\sigma(x) = \sigma(y)$, then $x = \sigma^{-1}\sigma(x) = \sigma^{-1}\sigma(y) = y$), so $|H|$ must divide $|G|$. □

Definition 3.1.4 (Group action)**.** Let X be a set. We say that G acts on X if for all $\sigma \in G$ there exists a map $X \longrightarrow X$ such that $\mathrm{id}(x) = x$ and $\sigma(\tau(x)) = (\sigma \cdot \tau)(x)$ for every $x \in X$ and every $\sigma, \tau \in G$.

Remark. Notice that if $\sigma(x) = \sigma(y)$ for some $x, y \in X$, then applying σ^{-1} we get that $\sigma^{-1}(\sigma(x)) = (\sigma^{-1}\sigma)(x) = \mathrm{id}(x) = x$, so $x = y$.

Therefore, an action of a group G on a set X can be thought of as a group homomorphism from G to $\mathrm{Sym}(X)$ (the group of permutations of the elements in X).

Example 3.1.2. Let $G = \mathrm{Sym}(4)$ be the group of permutations of $\{1, 2, 3, 4\}$. Then, we can construct an action of G on the vertices of the undirected graph K_4 (assigning vertex i to vertex $\sigma(i)$), but we can also consider that G acts on the set of edges of K_4, assigning $\{i, j\}$ to $\{\sigma(i), \sigma(j)\}$.

When we have a group G acting on a set X, we will denote the map $X \longrightarrow X$ corresponding to $\sigma \in G$ by σ itself. This is a slight abuse of notation, as we are using the same symbol for the group element and the map $X \longrightarrow X$, but it will make notation easier.

Example 3.1.3. The notion of group action is more restrictive than it might seem at first glance. For example, let $G = \{\mathrm{Id}, \sigma, \sigma^2\}$ be a group acting on $X = \{a, b\}$. Let us suppose $\sigma(a) = b$. Then, since group actions act as a permutation, $\sigma(b) = a$. Therefore, $\sigma^2(a) = a$. By applying σ again to both sides, $\sigma^3(a) = \sigma(a) = b$. The only group of size 3 is the cyclic group, so $\sigma^3(a) = \mathrm{Id}(a) = a$. Therefore, we reach the contradiction $a = b$.

Thus, in this case the only admissible action is the one where all the elements of G act on X like the identity.

Definition 3.1.5. We say that G acts *faithfully* if the only element of G that acts as the identity is the identity itself.

Definition 3.1.6 (Orbit)**.** Let G be a group acting on X. For each $x \in X$, we define the *orbit* of x as the set

$$\mathrm{orb}(x) = \{y \in X : \exists \sigma \in G \text{ such that } \sigma(x) = y\} = \{\sigma(x) : \sigma \in G\}$$

Definition 3.1.7. We say that G acts *transitively* on X if there is just one orbit.

Example 3.1.4. Let $G = C_4 = \{\mathrm{id}, (1234), (13)(24), (1432)\}$ be the cyclic group of 4 elements. The action of G on the vertices of K_4 is transitive, but on the edges it has 2 orbits:

$\{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}\}$ and $\{\{1, 3\}, \{2, 4\}\}$.

Definition 3.1.8. For each $x \in X$ we define the *stabilizer subgroup* as the set of elements from the group which fix x: $G_x = \{\sigma \in G : \sigma(x) = x\}$.

Lemma 3.1.1. *If G acts transitively on X then, for any $x \in X$, $|G_x|\,|X| = |G|$.*

Proof. Let us fix an $x \in X$. We know that G_x is a subgroup, so we can partition G into left cosets of G_x. Let $\sigma, \tau \in G$ such that $\tau G_x = \sigma G_x$. Then, we have that $(\sigma^{-1}\tau)G_x = G_x$. As $\mathrm{Id} \in G_x$, $\sigma^{-1}\tau \in G_x$, so $\sigma(x) = \tau(x)$. The converse is also true: if $\sigma(x) = \tau(x)$, then $\tau^{-1}\sigma \in G_x$, so $\sigma = \tau(\tau^{-1}\sigma) \in \tau G_x$. As σ is trivially in σG_x, that means that σG_x and τG_x are not disjoint, so they must be equal.

The action is transitive by hypothesis, so for each $y \in X$, there exists some $\sigma \in G$ such that $\sigma(x) = y$. Therefore, we can assign to every element $y \in X$ the coset σG_x, where $\sigma \in G$ is such that $\sigma(x) = y$. We know that these cosets will partition G, because an arbitrary $\tau \in G$ will belong to the coset assigned to $\tau(x)$. Besides, all cosets will be different and there will be $|X|$ of them.

We know that all left cosets of a subgroup will have the same size, so $|\sigma G_x| = |G_x|$ for every $\sigma \in G$. Then, the previous partition of G into $|X|$ cosets of G_x implies that $|G_x|\,|X| = |G|$. □

Definition 3.1.9. For $\sigma \in G$, we define $\mathrm{fix}(\sigma) := \{x \in X : \sigma(x) = x\}$.

Lemma 3.1.2 (Orbit counting lemma)**.** *The number of orbits of G acting on X is*

$$\frac{1}{|G|}\sum_{\sigma \in G} |\mathrm{fix}(\sigma)|$$

Proof. Suppose G acts transitively. Then, we can count the pairs (σ, x) such that $\sigma(x) = x$ as $\sum_{\sigma \in G} |\mathrm{fix}(\sigma)|$.
On the other hand, the pairs can also be counted as $\sum_{x \in X} |G_x|$. By applying the lemma, we get the equality we wanted to prove. falta.

If G is not transitive, suppose it has orbits $X_1, \ldots, X_t$. Then, we define

$$\mathrm{fix}_i(\sigma) = \{x \in X_i : \sigma(x) = x\}$$

Since G is transitive on X_i,

$$\sum_{\sigma \in G} |\mathrm{fix}_i(\sigma)| = |G| \implies \sum_{i=1}^{t}\sum_{\sigma \in G} |\mathrm{fix}_i(\sigma)| = t\,|G|$$

By switching the sums and applying $\sum_i |\mathrm{fix}_i(\sigma)| = |\mathrm{fix}(\sigma)|$, we have that

$$t\,|G| = \sum_{\sigma \in G} |\mathrm{fix}(\sigma)|$$

□

Example 3.1.5. Let $G = \{\mathrm{id}, (1234), (13)(24), (1432)\}$ be the cyclic group acting on the edges of K_4. id fixes all 6 edges, while (1234) and (1432) fix none and (13)(24) fixes 2. Therefore, the number of orbits of the action of G is $8/4 = 2$.

Example 3.1.6. If we expand G to the dihedral group by adding the reflexions (12)(34), (14)(23), (1)(3)(24) and (2)(4)(13), we get in addition 2 edges fixed by each of (12)(34), (14)(23), (1)(3)(24) and (2)(4)(13). Therefore, the number of orbits is still $16/8 = 2$.

3.2 Group actions on functions

Example 3.2.1. Suppose we want to count the number of ways of colouring the vertices of C_6 with 2 colours under the action of the cyclic group C_6.

In order to do it by hand, we can count the number of colourings with i blue vertices C_i, with i ranging from 0 to 6. We observe that $C_0 = 1$, $C_1 = 1$, $C_2 = 3$ and $C_3 = 4$. Then, by the symmetry of the problem, $C_4 = 3$, $C_5 = 1$ and $C_6 = 1$. The total number of 2-colourings is thus 14.

If we considered the dihedral group D_6 (C_6 plus the 6 reflections that leave an hexagon invariant). Again, let us define D_i as the number of ways of colouring C_6 with i blue vertices that are different under the action of D_6. We observe that $D_0 = 1$, $D_1 = 1$, $D_2 = 3$ and $D_3 = 3$, so the total number of 2-colourings is 13.

We will come back later to this problem.

Suppose G acts on X. Let C be a finite set of colours. Let us denote the set of functions $X \longrightarrow C$ as C^X. We want to define an action from G to C^X, because this will allow us to apply the counting lemma to our colouring problem.

For $\sigma \in G$ and $f \in C^X$, we define $\sigma(f)$ as the function

$$\sigma(f)(x) := f(\sigma^{-1}(x))$$

To prove that this is a well-defined action, we need to show that $\tau(\sigma(f)) = (\tau\sigma)(f)$. Let $x \in X$ be an arbitrary element. Then,

$$\tau(\sigma(f))(x) = \sigma(f)(\tau^{-1}(x)) = f(\sigma^{-1}\tau^{-1}(x)) = f((\tau\sigma)^{-1}(x)) = \tau\sigma(f)(x)$$

Example 3.2.2. Let $X = C_6$ be the cyclic graph with 6 vertices, and let f be the function that colours vertices 1, 2 and 3 blue and 4, 5, 6 green. Let $\tau = (135)(246)$. Then,

$$\begin{aligned}
\tau(f)(1) &= f(\tau^{-1}(1)) = f(5) = \text{ green} \\
\tau(f)(2) &= f(\tau^{-1}(2)) = f(6) = \text{ green} \\
\tau(f)(3) &= f(\tau^{-1}(3)) = f(1) = \text{ blue} \\
\tau(f)(4) &= f(\tau^{-1}(4)) = f(2) = \text{ blue} \\
\tau(f)(5) &= f(\tau^{-1}(5)) = f(3) = \text{ blue} \\
\tau(f)(6) &= f(\tau^{-1}(6)) = f(4) = \text{ green}
\end{aligned}$$

3.3 The cycle-index polynomial

Let G be a group acting on X. For each $\sigma \in G$, its action σ can be looked at as a permutation of the elements of X, so it has a cycle decomposition on the elements of X.

Example 3.3.1. Let $G = C_4$ and $X = K_4$. If we consider G acting on the vertices, then Id corresponds to (.)(.)(.)(.), (1234) corresponds to (....), (13)(24) corresponds to (..)(..) and (1432)

corresponds to (....). (We write points instead of labeling the elements of X because we will see later that we are only interested in the size of the cycles.)

So far, this looks trivial, but if we consider the action on the edges of X, the cyclic decomposition gets more interesting. Id corresponds to (.)(.)(.)(.)(.)(.), (1234) corresponds to (....)(..), (13)(24) corresponds to (..)(..)(.)(.), and (1432) corresponds to (....)(..).

Definition 3.3.1. Let $c_i^X(\sigma)$ be the number of i-cycles in the cyclic decomposition of σ acting on X, and let $c^X(\sigma)$ be the total number of cycles.

Then, we define the *cycle-index polynomial* of the action as

$$Z_G^X(X_1, \ldots, X_n) = \frac{1}{|G|} \sum_{\sigma \in G} \prod_{i=1}^{n} X_i^{c_i^X(\sigma)}$$

Example 3.3.2. Let us consider again C_4 acting on the vertices of K_4. The cyclic-index polynomial of this action is

$$Z_G^X(X_1, \ldots, X_4) = \frac{1}{4}\left(X_1^4 + X_2^2 + 2X_4\right)$$

Considering the action on the edges, we get the polynomial

$$Z_G^X(X_1, \ldots, X_4) = \frac{1}{4}\left(X_1^6 + X_1^2X_2^2 + 2X_2X_4\right)$$

Theorem 3.3.1 (Polya's Theorem)**.** *Let G be a group acting on X. Let C be a set of r colours. Then, the number of orbits of G acting on C^X (i.e. the number of r-colourings of X which are distinct under the symmetries in G) is*

$$Z_G^X(r, \ldots, r) = \frac{1}{|G|} \sum_{\sigma \in G} r^{C^X(\sigma)}$$

Proof. A colouring is fixed by σ if, and only if, all the elements of X on the same cycle (in the cycle decomposition of σ) are painted with the same colour. This can be done in $r^{C^X(\sigma)}$ ways.

Therefore, considering the action of G on C^X,

$$|\mathrm{fix}(\sigma)| = r^{C^X(\sigma)}$$

Now we apply the orbit-counting lemma, and we get that

$$\#\text{orbits} = \frac{1}{|G|} \sum_{\sigma \in G} |\mathrm{fix}(\sigma)| = \frac{1}{|G|} \sum_{\sigma \in G} \left| r^{C^X(\sigma)} \right|$$

□

Example 3.3.3. In the previous example of C_4 acting on the edges of K_4, we saw that

$$Z_G^X(X_1, \ldots, X_4) = \frac{1}{4}\left(X_1^6 + X_1^2X_2^2 + 2X_2X_4\right)$$

Therefore, the number of r-colourings of edges distinct under rotations is

$$\frac{1}{4}\left(r^6 + r^4 + 2r^2\right)$$

which for $r = 2$ gives a total of 22.

Example 3.3.4. Let us consider C_6 (the group) acting on the vertices of C_6 (the graph). The cycle-index polynomial of this action is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{6}\left(X_1^6 + X_2^3 + 2X_3^2 + 2X_6\right)$$

so the number of 2-colourings of C_6 which are distinct under rotations is

$$\frac{1}{6}\left(2^6 + 2^3 + 2\cdot 2^2 + 2\cdot 2\right) = \frac{84}{6} = 14$$

which is the result we arrived at previously by brute-force.

Extending the group to D_6, we get 6 new elements, and it can be checked that the cyclic-index polynomial of this action is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{12}\left(X_1^6 + X_2^3 + 2X_3^2 + 2X_6 + 3X_2^3 + 3X_1^2X_2^2\right)$$

so the number of 2-colourings rotationally distinct is

$$Z_G^X(2,\dots,2) = \frac{14}{2} + \frac{1}{12}(24+48) = 13$$

3.4 Rotational group of the cube

Falten apunts en paper

We can prove that there are no more symmetries by using lemma 3.1.1, where we take X to be the set of faces of the cube. It is easy to see that $|G_x| = 4$ (there are 4 symmetries that fix a given face x), so $|G| = |X|\cdot|G_x| = 24$.

Cyclic decompostions for G acting on the set of faces of the cube:

- Id: leaves every face fixed: (.)(.)(.)(.)(.)(.)
- face $180^{\underline{o}}$: two faces are fixed (the ones the axis cross) and the other 4 exchange positions in pairs: (.)(.)(..)(..)
- face 90: two faces are fixed and the other 4 move in a cycle: (.)(.)(....)
- edge: all faces exchange positions in pairs: (..)(..)(..)
- vertex: resting the cube on a vertex, the 3 upper faces and the 3 lower faces move in a cycle: (...)(...)

Therefore, the cycle-index polynomial is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{24}\left(X_1^6 + 3X_1^2X_2^2 + 6X_1^2X_4 + 6X_2^3 + 8X_3^2\right)$$

Using Polya's theorem, we get that the number of 2-colouring of faces of the cube is

$$Z_G^X(2,\dots,2) = \frac{1}{24}(64+48+48+48+32) = \frac{240}{24} = 10$$

Let's take now X to be the set of edges of the cube. Now the cyclic decompositions are:

- Id: (.)(.)(.)(.)(.)(.)(.)(.)(.)(.)(.)(.)
- face 180º: (..)(..)(..)(..)(..)(..)
- face 90: (....)(....)(....)
- edge: (.)(.)(..)(..)(..)(..)(..)
- vertex: the rotation has order 3 so it can only have 1-cycles or 3-cycles. There are no edges fixed, so we have: (...)(...)(...)(...)

The cycle-index polynomial is now

$$Z_G^X(X_1,\dots,X_{12}) = \frac{1}{24}\left(X_1^{12} + 3X_2^6 + 6X_4^3 + 6X_1^2X_2^5 + 8X_3^4\right)$$

Once again, using Polya's theorem we get that the number of 2-colourings of the edges is $Z_G^X(2,\dots,2) = 218$.

3.5 The number of non-isomorphic graphs

In order to count the number of non-isomorphic graphs on n vertices, we need to count the number of 2-colourings of the edges of K_n which are distinct under the action of the full symmetric group $\mathrm{Sym}(n)$.

For example, for $n = 4$, we need to work out the action on the edges of all the elements of $\mathrm{Sym}(4)$. Let us count first the number of non-isomorphic graphs manually, so we can later check the result.

With 0 and 1 edges there is just 1 graph, for 2 edges there are 2, and for 3 edges there are 3, so in total we have $1+1+2+3+2+1+1 = 11$ different non-isomorphic graphs.

Falta taula

The corresponding cycle-index polynomial is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{24}\left(X_1^6 + 6X_1^2X_2^2 + 8X_3^2 + 3X_1^2X_2^2 + 6X_2X_4\right)$$

Substituting $X_1 = \cdots = X_6 = 2$, we get that there are 11 non-isomorphic graphs with 4 vertices.

If we wanted to count the number of directed graphs, we would need to compute the action on ordered pairs. For example, for $n = 3$ we have the cycle decomposition:

Falta

so the cycle-index polynomial is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{6}\left(X_1^6 + 3X_2^3 + 2X_3^2\right)$$

so the number of directed graphs in 3 vertices is $Z_G^X(2,\dots,2) = 96/6 = 16$.

3.6 General version of Polya's Theorem

Let us go back to the example where we calculated the number of 2-colourings of the vertices of C_6 distinct under D_6 (rotations and reflections). The cycle-index polynomial we obtained is

$$Z_G^X(X_1,\dots,X_6) = \frac{1}{12}\left(X_1^6 + 4X_2^3 + 2X_3^2 + 2X_6 + 3X_1^2X_2^2\right)$$

where we substituted $X_1 = \cdots = X_6 = 2$ in order to get the total number of 2-colourings. Instead, if we wanted to calculate the number of 2-colourings with k blue vertices, we just need to substitute $X_1 = t_1 + t_2$, $X_2 = t_1^2 + t_2^2$, $\dots$, $X_6 = t_1^6 + t_2^6$ and extract the k-th coefficient of t_1.

This is what we will call the general version of Polya's Theorem.

Let G be a group acting on a set X, and let $f \in C^X$, where C is a set of r colours. Let ω be a map from C^X to $\mathbb{Z}[t_1,\dots,t_r]$, where $t_1,\dots,t_r$ are indeterminates. Let $m_i(f)$ be the number of elements from X that map to the i-th colour. We define ω as

$$\omega(f) = \prod_{i=1}^{r} t_i^{m_i(f)} = \prod_{x\in X} h(f(x))$$

where h maps the i-th colour to t_i.

Example 3.6.1. Let $\tau = (124)(356)$. Let f be a 2-colouring that assigns either blue (b) or red (r) to each vertex. The functions f which are fixed by τ are:

- f = bbbbbb, which gives $\omega(f) = t_1^6$
- f = bbrbrr, which gives $\omega(f) = t_1^3t_2^3$
- f = rrbrbb, which gives $\omega(f) = t_1^3t_2^3$
- f = rrrrrr, which gives $\omega(f) = t_2^6$

so

$$\sum_{f\in \mathrm{fix}(\tau)} \omega(f) = t_1^6 + 2t_1^3t_2^3 + t_2^6 = (t_1^3 + t_2^3)^2$$

Example 3.6.2. Let us take $G = \mathrm{Sym}(6)$ acting on $X = [6]$. Let us consider $C = \{b, r, w\}$ and $\tau = (123)(45)(6)$. The number of f fixed by τ is now 27 (as we need to colour all the vertices in a cycle with the same colour). We have that,

$$\sum_{f\in \mathrm{fix}(\tau)} \omega(f) = (t_1^3 + t_2^3 + t_3^3)(t_1^2 + t_2^2 + t_3^2)(t_1 + t_2 + t_3)$$

That's because each term in the product will correspond to a way of choosing a colour for the cycle of length 1, a colour for the cycle of length 2 and a colour for the cycle of length 3.

In general, this computation depends on the cyclic decomposition of τ acting on X. Let $c_i^X(\tau)$ be the number of i-cycles in the cycle decomposition of τ acting on X. Then,

$$\sum_{f\in \text{fix}(\tau)} \omega(f) = (t_1 + \cdots + t_r)^{c_1^X(\tau)} \cdots (t_1^n + \cdots + t_r^n)^{c_n^X(r)}$$

The cycle-index polynomial is

$$Z_G^X(X_1, \ldots, X_n) = \frac{1}{|G|} \sum_{\sigma\in G} \prod_{i=1}^{n} X_i^{c_i^X(\sigma)}$$

Hence,

$$|G| \cdot Z_G^X(t_1 + \cdots + t_r, \ldots, t_1^n + \cdots + t_r^n) = \sum_{\sigma\in G} \sum_{f\in \text{fix}(\sigma)} \omega(f)$$

Theorem 3.6.1 (Polya's general theorem)**.** *Let R be a set of representatives of the orbits of the action of G on C^X. Then,*

$$Z_G^X(t_1 + \cdots + t_r, \ldots, t_1^n + \cdots + t_r^n) = \sum_{f\in R} \omega(f)$$

Remark. Notice that if we substitute $t_i = 1$ for all $i \in [r]$, then the theorem reduces to the special case of Polya's Theorem we proved earlier:

$$Z_G^X(r, \ldots, r) = |R| = \#\text{ r-colourings of } X \text{ distinct under } G$$

Besides, notice that the theorem statement does not deppend on the representatives of R taken: Suppose $g \in \text{orb}(f)$. Then, $\exists\sigma \in G$ such that $g = \sigma(f)$. Therefore,

$$\omega(g) = \prod_{x\in X} h(g(x)) = \prod_{x\in X} h(\sigma(f)(x)) = \prod_{x\in X} h(f(\sigma^{-1}(x))) = \prod_{x\in X} h(f(x)) = \omega(f)$$

Proof. Observe that

$$\sum_{\sigma\in G} \sum_{f\in \text{fix}(\sigma)} \omega(f) = \sum_{f\in C^x} \sum_{\sigma\in S_f} \omega(f)$$

where S_f is the stabiliser subgroup of f in G.
By lemma 3.1.1, since G is transitive on $\text{orb}(f)$,

$$|G| = |S_f| \cdot |\text{orb}(f)|$$

Therefore,

$$\sum_{f\in C^X} \sum_{\sigma\in S_f} \omega(f) = \sum_{f\in C^X} |S_f|\,\omega(f) = \sum_{f\in C^X} |G|\,\frac{\omega(f)}{|\text{orb}(f)|} = \sum_{f\in R} |G|\,\omega(f)$$

since $\omega(f) = \omega(g)$ if $g \in \text{orb}(f)$. Substituting back in, we get the equality we wanted to prove:

$$Z_G^X(t_1 + \cdots + t_r, \ldots, t_1^n + \cdots + t_r^n) = \sum_{f\in R} \omega(f)$$

□

Example 3.6.3. Going back to the example of $G = \mathrm{Sym}(4)$ acting on the edges of K_4, we calculated that the cycle-index polynomial was

$$Z_G^X(X_1, \ldots, X_6) = \frac{1}{24}\left(X_1^6 + 9X_1^2X_2^2 + 8X_3^2 + 6X_2X_4\right)$$

Hence,

$$Z_G^X(t_1 + t_2, \ldots, t_1^6 + t_2^6) = \cdots = t_1^6 + t_1^5t_2 + 2t_1^4t_2^2 + 3t_1^2t_2^3 + 2t_1^2t_2^4 + t_1t_2^5 + t_2^6$$

which tells us for example that there are 3 different 4-vertex graphs with 3 edges.

In general, the coefficient of $t_1^{k_1} \ldots t_r^{k_r}$ is the number of distinct r-colourings with k_i elements coloured with colour c_i.

4

Finite geometries & Latin squares

4.1 System of distinct representatives (SDR)

Definition 4.1.1. Let $A_1, \ldots, A_n$ be a set of subsets of a set X. We say that $\{a_1, \ldots, a_n\}$ is an *SDR* if $a_i \in A_i$ for all $i \in [n]$ and the a_i are distinct pair-wise.

Example 4.1.1. Let $A_1 = \{x_1, x_3, x_4\}$, $A_2 = \{x_1, x_3\}$, $A_3 = \{x_2, x_4\}$ and $A_4 = \{x_2, x_3\}$. Then, $a_1 = x_1$, $a_2 = x_3$, $a_3 = x_4$ and $a_4 = x_2$ is an SDR.

Example 4.1.2. Let $X = [7] := \{1, \ldots, 7\}$. Let $A_1 = \{1, 2\}$, $A_2 = \{1, 3, 4\}$, $A_3 = \{1, 2, 5, 7\}$, $A_4 = \{1, 4, 6, 7\}$, $A_5 = \{1, 3\}$, $A_6 = \{2, 3, 4\}$ and $A_7 = \{1, 4\}$. We observe that $A_1 \cup A_2 \cup A_5 \cup A_6 \cup A_7 = \{1, 2, 3, 4\}$. Therefore, there can not be an SDR, as we would need 5 distinct elements from these subsets.

This example illustrates a particular case of Hall's Theorem:

Theorem 4.1.1 (Hall)**.** *Let $A(J) := \bigcup_{j \in J} A_j$, where $J \subseteq [n]$. Then, $A_1, \ldots, A_n$ has an SDR if, and only if, $|A(J)| \geq |J|$ for all $J \subseteq [n]$.*

Proof. The forward direction is direct. When we restrict the SDR to $A(J)$, we observe that it must contain at least an element for every A_j, so $|A(J)| \geq |J|$.

The inverse direction is not so obvious. Let us prove it by induction on n (the number of subsets A_i). The base case is $n = 1$. Taking $|J| = \{1\}$, we have that $|A_1| \geq 1$, so we can construct an SDR formed by an element of A_1.

For the inductive step we are going to consider two cases. Let us suppose that $\nexists J \neq \emptyset$ and $J \neq [n]$ such that $|A(J)| = |J|$. We know that $|A_n| \neq 0$ by Hall's condition, so $\exists a_n \in A_n$. Taking that element for our SDR and defining $A'_j := A_j \setminus \{a_n\}$, we claim that Hall's condition once again holds for $A'_1, \ldots, A'_{n-1}$. Indeed,

$$\left|A'(J)\right| \geq |A(J)| - 1 \leq |J|$$

since we remove at most one element from $A(J)$ to construct $A'(J)$ and $|A(J)| > |J|$. By induction, there exists an SDR for $A'_1, \dots, A'_{n-1}$, which we can expand to an SDR of $A_1, \dots, A_n$ by adding a_n.

Let us now consider the second case, in which there exists a non-empty subset $J \subsetneq [n]$ such that $\cdot|J| = |A(J)|$. For $i \in I = [n] \setminus J$, let us define $A'_i := A_i \setminus A(J)$. Then we claim that $\{A_i\}_{iI}$ satisfies Hall's condition.

Indeed, let $K \subset I$. We have that

$$|A'(K)| = \left|\bigcup_{i\in K} A'_i\right| = \left|\bigcup_{i\in K} (A_i \setminus A(J))\right| = \left|\Big(\bigcup_{i\in K} A_i\Big) \setminus \Big(\bigcup_{j\in J} A_j\Big)\right| = \left|\bigcup_{i\in K\cup J} A_i \setminus \Big(\bigcup_{j\in J} A_j\Big)\right| =$$

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

Therefore, by induction there exists an SDR for A'_i, $i \in I = [n] \setminus J$ which is a subset of $X \setminus A(J)$. We also apply induction to find an SDR for A_j, $j \in J$, which will be disjoint from the other one, as it is contained in $A(J)$. Then, the union of both forms a SDR of A_i, $i \in [n]$. □

Under an extra condition, Hall's theorem not only guarantees the existence of an SDR, but of many:

Theorem 4.1.2 (Hall's extended theorem)**.** *Suppose $A_1, \dots, A_n$ satisfy Hall's condition, and that $|A_i| \geq r$ for all $i \in [n]$. Then there exist at least $r!$ distinct SDR's.*

Proof. We are going to prove it by induction on n and r. If $r = 1$, we apply the standard Hall Theorem. If $n = r$, then $|A_i| \geq n$ for every $i \in [n]$, so we can take a different element from each one greedily.

Suppose we are in case 1 from the previous proof. Then, $A'_1, \dots, A'_{n-1}$ are subsets of $X \setminus \{a_n\}$ of size $r - 1$, so by induction there exist at least $(r-1)!$ SDR's, and we could have taken at least r choices of a_n, so we can extend them to $r!$ SDR's of $A_1, \dots, A_n$.

If we are in case 2, then there exists a non-empty proper subset J such that $|A(J)| = |J|$ and $r \leq |J| \leq n$. By induction, the A_j $(j \in J)$ have at least $r!$ SDRs, and we can extend each one of them to an SDR of the whole family of sets (by the same argument as in last theorem). □

The following theorem gives us a sufficient condition for Hall's condition to hold.

Theorem 4.1.3. *Suppose $A_1, \dots, A_n$ is a set of subsets of X such that $|A_i| = r$ and each element $x \in X$ is contained in at most r of these subsets. Then, $A_1, \dots, A_n$ satisfy Hall's condition.*

Proof. We are going to apply double counting to the pairs (x, j) where $x \in A_j$, for every subset $J \subseteq [n]$. Counting j first, we get at most r choices for $x \in A_j$ and $|J|$ choices for j, so the total number of pairs is at least $r\,|J|$. revisar canvis del Fèlix

Counting x first, we have that each x is contained in exactly r sets A_i $(i \in [n])$, so it is contained in at most r sets A_i $(i \in J)$. Then, there are $|A(J)|$ choices for x why?, so there are at least $r\,|A(J)|$ pairs. Hence, $r\,|A(J)| \geq r\,|J|$, so Hall's condition holds. □

4.2 Latin squares

Definition 4.2.1 (Latin square)**.** Let X be a set of size n (that we usually assume to be $[n]$). A *Latin square* is an $n \times n$ array such that every row and column contains each element of X exactly once.

Example 4.2.1. Let G be a group of size n, with elements $\{g_1, \dots, g_n\}$ and binary operation $\circ$. Then, the matrix $(g_i \circ g_j)_{ij}$ forms a Latin square, since $g_i \circ g_j = g_i \circ g_k \implies g_j = g_k$ due to the existence of g_i^{-1}.

We can also look at it the other way. Given a Latin square, we can define a binary operation on X by labelling the rows and columns with elements of X and treating it as a multiplication table. This gives us a structure of *quasigroup*. However, as the following example shows, this does not always give us a group.

Example 4.2.2. The following Latin square does not give us a group, as there is no identity and the operation is not associative: $(1 \circ 1) \circ 1 = 2 \circ 1 = 0$ but $1 \circ (1 \circ 1) = 1 \circ 2 = 3$.

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	3	0	1	2
3	2	3	0	1

Definition 4.2.2 (Latin rectangle)**.** A *Latin rectangle* is an $r \times n$ array in which every row contains every element of X exactly once, and each column contains every element of X at most once.

Example 4.2.3. An example of a 2×4 Latin rectangle is the following:

2	1	4	3
3	2	1	4

Given an $r \times n$ Latin rectangle, let A_i be the set of elements of X not appearing in the i-th column. Clearly, $|A_i| = n - r$ (since the elements in the column can not be repeated) and each element of X appears in $A_1, \dots, A_n$ exactly $n - r$ times.

Applying Hall's extended theorem, we get the following lemma:

Lemma 4.2.1. *An $r \times n$ Latin rectangle can be extended to a $(r+1) \times n$ Latin rectangle in $\geq (n-r)!$ ways.*

Proof. Each way of extending the Latin rectangle is associated bijectively to an SDR of $A_1, \dots, A_n$, since we have to choose n pair-wise different elements, one from each set. The bound is then given by Hall's extended theorem. □

We can use this result to get a lower bound on $L(n)$, the number of Latin squares of size n. The argument is the following:

For the first row, we have $n!$ possible choices, as all permutations are valid. For the i-th row, having fixed rows $1, \dots, i-1$, the previous lemma tells us that we have at least $(n-i)!$ possible choices. Therefore, the total number of Latin squares is at least

$$L(n) \geq \prod_{k=1}^{n} k!$$

Example 4.2.4. We can check that $L(2) = 2$ and $L(3) = 12 = 3!2!$, so the bound is tight for $n = 2$ and $n = 3$. However, it is easy to see that the bound is not tight for $n \geq 4$. Suppose wlog that the first row is $(123 \dots n)$, and let the second row be $(\sigma(1)\sigma(2) \dots \sigma(n))$. This will give a Latin rectangle if, and only if, σ is a derangement (that is, it has no 1-cycle). Then, the number of choices for the second row is

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

where the last inequality holds for $n \geq 4$.

Given an $n \times n$ Latin rectangle, we can construct an $n \times n$ matrix where $m_{ij} = 1$ if $i \in A_j$ and $m_{ij} = 0$ otherwise.

Example 4.2.5. The Latin rectangle

1	2	3	4
2	3	4	1

corresponds to the matrix

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

Observe that we can check if a permutation σ gives an SDR by computing $\prod_{i=1}^{n} m_{i\sigma(i)}$ and checking if it gives 1. Then, the total number of SDRs is given by

$$\operatorname{Perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} m_{i\sigma(i)}$$

which is called the *permanent* of the matrix M.

The permanent is an interesting operation, because its definition is very similar to the one of determinants, but calculating permanents turns out to be very difficult in practice, while there are very efficient algorithms for computing the determinant of a matrix.

Theorem 4.2.1. *Let M be a matrix of 0's and 1's with r 1's in each column. Then,*

$$\mathrm{Perm}(M) \leq (r!)^{n/r}$$

This theorem gives us an upper bound for the number of Latin squares of size n, $L(n)$:

Corollary 4.2.1. *The number of Latin squares of size n is bounded by*

$$L(n) \leq \prod_{r=0}^{n-1} ((n-r)!)^{n/(n-r)}$$

Proof. Given a Latin rectangle of size $r \times n$, the associated matrix M will have $n-r$ ones in each column, so there are at most $(n-r)!^{n/(n-r)}$ ways to extend it to a Latin rectangle of size $r+1 \times n$. Applying this process n times, we get

$$L(n) \leq \prod_{r=0}^{n-1} ((n-r)!)^{n/(n-r)}$$

□

Theorem 4.2.2. *Let M be an $n \times n$ matrix of non-negative real numbers whose rows and columns sum to 1. Then,*

$$\mathrm{Perm}(M) \geq \frac{n!}{n^n}$$

Remark. An easy way to remember this lower bound is to think of the matrix where each element is $1/n$.

Corollary 4.2.2. *The number of Latin squares of size n is bounded by*

$$L(n) \geq \frac{(n!)^{2n}}{n^{n^2}}$$

Proof. Given an $r \times n$ Latin rectangle, the matrix $\frac{1}{n-r}M$ satisfies the hypothesis of the theorem. Hence,

$$\mathrm{Perm}\left(\frac{1}{n-r}M\right) \geq \frac{n!}{n^n} \implies \mathrm{Perm}(M) \geq n! \left(\frac{n-r}{n}\right)^n$$

Applying this bound n times, we get that

$$L(n) \geq \prod_{r=0}^{n-1} \frac{n!(n-r)^n}{n^n} = \frac{(n!)^{2n}}{n^{n^2}}$$

□

We have seen an upper bound and a lower bound for the number of Latin squares. Now, we are going to see that the logarithms of those bounds are not very far away (at least asymptotically). Let us recall Stirling's approximation:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

Using this approximation, the upper bound becomes

$$\log\left(\frac{(n!)^{2n}}{n^{n^2}}\right) = 2n\log(n!) - n^2\log n \sim n^2\log n - 2n^2\log e$$

The lower bound gives the same asymptotics:

$$\log\prod_r((n-r)!)^{n/(n-r)} = \sum_r \frac{n}{n-r}\log(n-r)! = \sum_k \frac{n}{k}\log k! \sim \cdots \sim n^2\log n - 2n^2\log e$$

So the gap between them is relatively small (compared to the actual number of Latin squares).

4.3 Mutually orthogonal Latin squares (MOLS)

Definition 4.3.1 (MOLS)**.** We say that two Latin squares or quasigroups $(G, \circ)$ and $(H, \star)$ are *mutually orthogonal* if the superposition of both gives each element of $G \times H$ exactly once.

Example 4.3.1. The following two Latin squares are mutually orthogonal:

$\circ$			
	0	1	2
	2	0	1
	1	2	0

$\star$			
	A	C	B
	C	B	A
	B	A	C

The task of finding two MOLS of order n is a classical problem in combinatorics, usually presented as arranging n^2 soldiers from n different regiments and n different ranks such that each column and row has a soldier from every regiment and rank. In order to study this problem we are going to make use of finite fields.

Refresher of finite fields

We denote by $\mathbb{F}_p$ the finite field of p elements, which is unique up to isomorphism when p is prime, and is usually represented by $\mathbb{Z}/p\mathbb{Z}$. For $q = p^h$ a power of a prime (with $h \geq 2$), $\mathbb{F}_q$ is also unique up to isomorphism, but now it is not isomorphic to $\mathbb{Z}/q\mathbb{Z}$, but to $(\mathbb{Z}/p\mathbb{Z})[X]/(f)$, where (f) is the ideal generated by some irreducible polynomial of degree h.

For example, $\mathbb{F}_4$ is the finite field of order $4 = 2^2$, which is isomorphic to the quotient of $(\mathbb{Z}/2\mathbb{Z})[x]$ with respect to the ideal (x^2+x+1) (or any other irreducible polynomial of degree 2 for that matter). Then one can check that $\mathbb{F}_4 = \{0, 1, x, x^2\}$, which is closed under sums and products. For example: $x^2 + x = (x^2 + x + 1) + 1 = 1$ and $x^2 \cdot x = x^3 = (x^2 + x + 1)(x + 1) + 1 = 1$.

For a given $m \in \mathbb{F}_q \setminus \{0\}$, $g \star_m h := g + mh$ defines a binary operation on $\mathbb{F}_q$. For $q = 4$, taking $\mathbb{F}_4 = (\mathbb{Z}/2\mathbb{Z}[e])/(e^2 + e + 1) = \{0, 1, e, e^2\}$, we get the following three multiplication tables:

Falten taules

By labeling the elements of F_4, one can check that these three tables are pair-wise mutually orthogonal Latin squares of order 4.

Lemma 4.3.1. *Let $G = \mathbb{F}_q$. Then, the quasigroups $(G, \star_m)$ and $(G, \star_j)$ are MOLS for $j \neq m \in G$.*

Proof. If not, there exists a pair $(x, x') \in G^2$ that appears twice. So there exist h_1, h_2 and g_1, g_2 such that $x = g_1 \star_m h_1 = g_2 \star_m h_2$ and $x' = g_1 \star_j h_1 = g_2 \star_j h_2$. This implies that

$$m = \frac{g_1 - g_2}{h_1 - h_2} = j$$

reaching a contradiction. □

The previous discussion guarantees the existence of $n-1$ pair-wise MOLS for every order of the form $n = p^k$, where p is a prime. This result is optimal:

Theorem 4.3.1. *There are at most $n - 1$ MOLS of order n.*

Proof. Supose the elements of the Latin squares are all from the set X, of size n. Permuting the elements of a Latin squares gives us another Latin square, and the permutation of two MOLS gives us another pair of MOLS. Then, suppose we have N MOLS of order n. In each we can permute the elements of X such that the $(1, 1)$ cell is a certain $x \in X$.

Notice that in the subsquare formed by removing the first row and column, x must appear in different positions in all the N Latin squares (otherwise they would not be mutually orthogonal). We have to place $n - 1$ x's in each of the N Latin squares, so $(n-1)N \leq (n-1)^2 \implies N \leq n - 1$. □

Let us suppose $(G, \star)$ and $(H, \circ)$ are Latin squares. Then, we can define its product $(G \times H, \star\circ)$ as the Latin square given by the operation $(g_1, h_1) \star\circ (g_2, h_2) := (g_1 \star g_2,\ h_1 \circ h_2)$.

Lemma 4.3.2. *$(G \times H, \star\circ)$ is a Latin square.*

Proof. Let us suppose we have two equal elements in the same row (the same argument works for columns). Then, we have g_1, g_2, g_3 and h_1, h_2, h_3 such that

$$(g_1, h_1) \star \circ (g_2, h_2) = (g_1, h_1) \star \circ (g_3, h_3)$$

By definition of the operation $\star\circ$, that implies that $g_1 \star g_2 = g_1 \star g_3$, so $(G, \star)$ would not be a Latin square, reaching a contradiction. □

Theorem 4.3.2. *Suppose $(G, \cdot)$ and $(G, \star)$ are MOLS, and $(H, \circ)$ and $(H, *)$ are also MOLS. Then, $(G \times H, \cdot\circ)$ and $(G \times H, \star *)$ are MOLS.*

Proof. Falta □

The previous theorem tells us that, given 2 MOLS of order n and 2 MOLS of order m, we can construct 2 MOLS of order mn.

We proved that there exist at least $n - 1$ MOLS of order n, where $n = p^k$ for some prime k. Therefore, for $n = p^k \geq 3$, there are at least 2 MOLS of order n. This implies that for any integer n that can be decomposed as a product of odd primes and 2^k, with $k \geq 2$, we will be able to construct a pair of MOLS of order n using the previous procedure.

Euler conjectured that in the rest of cases, when $n \equiv 2 \mod 4$, there exist no pair of MOLS of order n. This is indeed the case for $n = 2$ and $n = 6$, but it is not true for $n \geq 10$.

Example 4.3.2. One of the ways to construct a pair of MOLS of order 10, due to Ernest Parker, is the following:

6	1	3	5	0	2	4	7	8	9
5	0	2	4	6	1	3	9	7	8
3	5	0	2	4	6	1	8	9	7
7	8	1	9	3	4	5	6	0	2
8	6	9	1	2	3	7	4	5	0
4	9	6	0	1	7	8	2	3	5
9	4	5	6	7	8	2	0	1	3
2	3	4	7	8	0	9	5	6	1
1	2	7	8	5	9	0	3	4	6
0	7	8	3	9	5	6	1	2	4

4	2	0	5	3	1	6	7	8	9
1	6	4	2	0	5	3	8	9	7
2	0	5	3	1	6	4	9	7	8
3	4	9	6	8	7	2	5	1	0
6	9	1	8	7	4	5	0	3	2
9	3	8	7	6	0	1	2	5	4
5	8	7	1	2	3	9	4	0	6
8	7	3	4	5	9	0	6	2	1
7	5	6	0	9	2	8	1	4	3
0	1	2	9	4	8	7	3	6	5

Figure 4.1: Two 10×10 MOLS found by Ernest Parker

4.4 Linear spaces

Definition 4.4.1 (Incidence structure)**.** An *incidence structure* $\Gamma = (P, L)$ is a set of points P and a set of lines L, which are non-empty subsets of P.

Given an incidence structure (P, L), we can also define the *dual structure*, $\Gamma^* = (L, M)$. In the dual structure, the points are the lines of the original structure, and the lines $m_x \in M$ are the subsets of L formed by the $\ell \in L$ such that $\ell \in m_x$ iff $x \in \ell$.

Example 4.4.1. Falta dibuix

Definition 4.4.2 (Linear space)**.** A *linear space* is an incidence structure such that any 2 points are joined by a line, and this line is unique.

Theorem 4.4.1 (Erdös - de Bruijn)**.** *Let (P, L) be a linear space for which there is no line containing all the points. Then, $|L| \geq |P|$.*

Proof. For each $x \in P$, let r_x be the number of lines incident with x, and for each $l \in L$ let k_l be the number of points incident with l. Suppose we have a non-incident point-line pair (x, l) (that is, $x \in P$, $l \in L$ but $x \notin l$). Then, for any point $y \in l$ there must be another line joining x and y (and these lines must be pair-wise different because otherwise two points in l would be joined too by a line $l' \neq l$, so we would not be in a linear space). Therefore, $r_x \geq k_l$.

Let us suppose $|P| \geq |L|$. Then,

$$\begin{gathered} |P|\, r_x \geq |L|\, k_\ell \\ |L|\,|P| - |L|\, k_\ell \geq |L|\,|P| - |P|\, r_x \\ \frac{1}{|P|\,(|L| - r_x)} \geq \frac{1}{|L|\,(|P| - k_\ell)} \end{gathered}$$

Summing both sides over all non-incident point-line pairs (x, ℓ), the LHS is

$$\sum_{x \in P} \sum_{\ell : x \notin \ell} \frac{1}{|P|\,(|L| - r_x)} = \sum_{x \in P} \frac{1}{|P|} = 1$$

because the term $|P|\,(|L| - r_x)$ does not depend on ℓ and there are exactly $|L| - r_x$ lines not incident to x. Similarly,

$$\sum_{\ell \in L} \sum_{x \notin \ell} \frac{1}{|L|\,(|P| - k_\ell)} = \sum_{\ell \in L} \frac{1}{|L|} = 1$$

Therefore we have an equality, so all the intermediate steps are also an equality, which implies that $|P| = |L|$. □

Remark. If $|P| = |L|$, the proof of the theorem also gives us that $r_x = k_\ell$ for any non-incident (x, ℓ). Then, if $x, y \in P$ such that $r_x \neq r_y$, and if $z \in P \setminus \{x, y\}$ (wlog we can suppose $r_x \neq r_z$), we get that every line must be incident with x or with y (otherwise $r_x = k_\ell = r_y$), and every line must be incident with x or with z (for the same reason). Then, there can be at most one line not incident with x (as otherwise there would be two lines joining y and z). Thus, we get a degenerate projective plane.

In the other case, when $|P| = |L|$ and $r_x = r_y$ for every $x, y \in P$, we get constructions like the Fano plane, which we will study in the next sections.

Definition 4.4.3 (Projective plane)**.** A linear space Γ is called a *projective plane* if Γ^* is also a linear space. Furthermore, a projective plane is called *non-degenerate* if it contains 4 points with no 3 collinear.

Example 4.4.2. Let P be the set of one-dimensional subspaces of $\mathbb{F}_q^3$ and let L be the set of two-dimensional subspaces of F_q^3. Then, (P, L) is a projective plane, as any two different one-dimensional subspaces span a two-dimensional subspace, and any two different two-dimensional subspaces intersect in a one-dimensional subspace. This projective plane is denoted by $\mathrm{PG}(2, q)$.

Let (x_1, x_2, x_3) be a vector from $\mathbb{F}_q^3$. Every vector except the 0 vector spans a one-dimensional subspace, and each one-dimensional subspace is spanned by $(q-1)$ different non-zero vectors, so the number of points in the projective plane is $|P| = (q^3 - 1)/(q - 1) = q^2 + q + 1$.

This formula for the number of points holds in the general case. Let (P, L) be a projective plane of order n (that is, $r_x = k_\ell = n + 1$ for every $x \in P$ and $\ell \in L$). Then, fixing one point, there are $n+1$ lines that go through that point, each one containing n points (and there are no other points, as all pairs of points are joined by a line), so $|P| = n(n + 1) + 1 = n^2 + n + 1$.

With the previous example we constructed projective planes of order $q = p^k$, for all p prime and $k \geq 1$. It is conjectured that there are no projective planes of other orders:

Conjecture 4.4.1. *All finite projective planes have prime power order.*

Theorem 4.4.2. *If $n \equiv 1$ or $2 \mod 4$ and there exists a projective plane of order n, then n is the sum of two squares.*

Proof. Let A be a $m \times m$ matrix whose rows are indexed by the points of the projective plane, and whose columns are indexed by the lines ($m = n^2 + n + 1$). Let $A_{ij} = 1$ if $x_i \in \ell_j$ and 0 otherwise. Then, $AA^T = J + n\mathrm{Id}_m$, where J is the matrix with all 1's.

Let $A = (a_{ij})$, and let $(z_1, \ldots, Z_m) = (x_1, \ldots, x_m)A$. Then,

$$(x_1, \ldots, x_m)AA^T(x_1, \ldots, x_m)^T = (z_1, \ldots, z_m)(z_1, \ldots, z_m)^T = z_1^2 + \cdots + z_m^2$$

but in the other hand, using the expression found earlier for AA^T,

$$(x_1, \ldots, x_m)AA^T(x_1, \ldots, x_m)^T = (x_1 + \cdots + x_m)^2 + n(x_1^2 + \cdots + x_m^2)$$

By Lagrange 4 squares theorem, there exist a_1, a_2, a_3, a_4 such that $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Plugging this in, we get that

$$(a_1^2 + \cdots + a_4^2)(x_1^2 + \cdots + x_m^2) = c_1^2 + \cdots + c_4^2$$

where c_1, c_2, c_3 and c_4 are certain coefficients that can be expressed in function of the a_i's and x_i's.

(...)

We have obtained a system of m equations in $m+1$ variables, which must have a non-trivial solution over the rationals. Therefore, $nx_{m+1}^2 = \omega^2 + c_{m+1}^2$, and if $x_{m+1} \neq 0$, that means that n is the sum of two rational squares, which implies that n is the sum of two integer squares.

If $x_{m+1} = 0$, Falta completar (veure llibre de Cameron)

□

4.5 Affine planes

Definition 4.5.1 (Affine plane)**.** An *affine plane* is a linear space (P, L) with the property that there exists a unique line $m \in L$ such that $x \in m$ and $m \cap \ell = \emptyset$ for all non-incident line pairs (x, ℓ).

This property is usually called the *parallel axiom*.

We can define a relation on the set of lines such that $\ell \sim m \iff l = m$ or $l \cap m = \emptyset$.

Lemma 4.5.1. *The previous relation is an equivalence relation.*

Proof. Symmetry and reflexivity follow immediately. Let's prove transitivity. Suppose there exist $\ell \sim \ell'$ and $\ell' \sim \ell''$ such that $\ell \not\sim \ell''$. Let $x \in \ell \cap \ell''$. We know that $x \notin \ell'$, but then we have two lines (ℓ and ℓ'') which are incident to x and not intersecting ℓ', contradicting the parallel axiom. □

Let E be the set of equivalence classes given by the previous relation. For $\ell \in L$, we define $\ell^* := \ell \cup \{e\}$, where $e \in E$ is the equivalence class containing ℓ. We can then expand our affine space, defining $P^* := P \cup E$ and $L^* := \{\ell^* : \ell \in L\} \cup \{\ell_\infty\}$, where we take $\ell_\infty := E$.

Theorem 4.5.1. (P^*, L^*) *is a projective plane.*

Proof. Since (P, L) is a linear space,so each pair of points $x, y \in P$ are connected by a unique line. Let $x \in P$ and $e \in E$. By the parallel axiom, the lines of e cover all the points in P. Therefore, there exists $m \in e$ such that $x \in m$, so $x, e \in m^*$. Thus, (P^*, L^*) is a linear space.

Now let's check that the dual is a linear space too. Let $\ell, m \in L$. If $l \cap m = \emptyset$, then $\ell^* \cap m^* = \{e\}$, where e is the equivalence class connecting l and m, so the dual of (P^*, L^*) is a linear space.

Repassar i explicar millor demo □

Corollary 4.5.1. *A finite affine plane has an order n such that each line is incident with n points and each point is incident with $n+1$ lines.*

$$|P^*| = n^2 + n + 1 \implies |P| = n^2$$
$$|L^*| = n^2 + n + 1 \implies |L| = n^2 + n$$

Què vol dir amb les equacions? És demo o part del corol·lari?

Theorem 4.5.2. *If we delete a line ℓ_∞ and all its points from a projective plane, we obtain an affine plane.*

Proof. Let $x \in P$ and $\ell \in L$, with $x \notin \ell$. In the projective plane, the line m joining x to $e \in \ell \cap \ell_\infty$ is unique, and this line will be the parallel line to ℓ going through x in the affine plane. □

Let A_1 and A_2 be two MOLS of order 3, such as

1	2	3
3	1	2
2	3	1

1	2	3
3	1	2
2	3	1

Let's define the line ℓ_{ij} as the positions in the i-th of the MOLS where we have element j (we will number the rows starting from the bottom). Then,

$$\begin{aligned}
\ell_{11} &= \{(3,1),(2,3),(1,2)\} \\
\ell_{12} &= \{(3,2),(2,1),(1,3)\} \\
\ell_{13} &= \{(3,3),(2,1),(1,3)\} \\
\ell_{21} &= \{(3,1),(2,2),(1,3)\} \\
\ell_{22} &= \{(3,2),(2,3),(1,1)\} \\
\ell_{23} &= \{(3,3),(2,1),(1,2)\}
\end{aligned}$$

Adding the vertical and horizontal lines, we obtain an affine plane of order 3. This procedure is valid in general:

Theorem 4.5.3. *Given a set of $n-1$ MOLS of order n, we can construct an affine plane of order n by setting $P = [n] \times [n]$ and defining the following lines:*

$$\begin{aligned}
h_j &= \{(j,x) : x \in [n]\}, \quad \forall j \in [n] \\
v_j &= \{(x,j) : x \in [n]\}, \quad \forall j \in [n] \\
\ell_{mk} &= \{(i,j) : A^m_{(i,j)} = k, m \in [n-1]\}, \forall k \in [n]
\end{aligned}$$

where $A^1, \ldots, A^{n-1}$ is the set of MOLS.

Proof. Suppose that (i,j) and (i',j') are joined by two lines ℓ_{mk} and $\ell m'k'$. Then, $A^m_{ij} = k = A^m_{i'j'}$ and $A^{m'}_{ij} = k' = A^{m'}_{i'j'}$, contradicting the orthogonality of the Latin squares A^m and $A^{m'}$. It is easy to see also that no two horizontal or vertical lines can join the same pair of points, and that no horizontal (or vertical) line can join a pair of points that a certain ℓ_{mk} joins (as then it would not be a Latin square). Therefore, two points are not joined by more than one line.

Let's now show that this line always exists. We just have to count the tuples (x,y,ℓ) where x and y are incident with ℓ. Since $|L| = n^2+n$ and each line is incident with n points, the number of tuples of that form is

$$N = (n^2+n)\binom{n}{2} = \frac{n^2(n^2-1)}{2} = \binom{n^2}{2}$$

Since $|P| = n^2$, this implies that any 2 points must be joined by a line. Repassar argument

Lastly, let's show that the parallel axiom holds. If $m \neq m'$, then ℓ_{mk} and $\ell m'k'$ intersect, since by the orthogonality of A^m and $A^{m'}$ there exists a position (i,j) such that $A^m_{ij} = k$ and $A^{m'}_{ij} = k'$. Suppose $x = (i,j) \notin \ell_{mk}$. Let $k' = A^m_{ij}$. Then, $\ell_{mk'}$ is the parallel line to ℓmk that passes though x. For horizontal and vertical lines, the existence of parallel lines going through every other point is direct, so the parallel axiom holds. □

Remark. It can be shown that all affine planes of order q constructed with this procedure conform $\mathrm{AG}(2,q) \simeq \mathrm{PG}(2,q) \setminus \ell$.

4.6 Projective spaces

We can define a geommetry of points, lines, planes, etc. where a i-dimensional subspace is a $i+1$-dimensional subspace of $\mathbb{F}_q^n$. This geommetry is denoted by $\mathrm{PG}(n-1,q)$.

For example, for $n = 4$ and $q = 2$ we get a geommetry with 15 points (corresponding to the non-zero vectors of $\mathbb{F}_2^4$), 35 lines (corresponding to the 35 2-dimensional subspaces of $\mathbb{F}_2^4$, and so on.

If we multiply by a change of basis matrix, then the subspace structure of $\mathbb{F}_q^n$ is preserved, so $\mathrm{PG}(n-1,q)$ will have a large group of symmetries.

Lemma 4.6.1. *The number of k-tuples of linearly independent vectors in $\mathbb{F}_q^n$ is $(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$.*

Proof. Let $(v_1,\ldots,v_k)$ be a k-tuple of linearly independent vectors. We can choose v_1 to be any non-zero vectors, so we have q^n-1 choices. v_2 must not be in the 1-dimensional space spanned by v_1, which contains q vectors, so we have q^n-q choices for v_2. Iterating this argument we see that we have q^n-q^{i-1} choices for v_i, which gives the desired result. □

Theorem 4.6.1. *The number of k-dimensional subspaces of $\mathbb{F}_q^n$ (equal to the number of $(k-1)$-dimensional subspaces of $PG(n-1,q)$) is $\begin{bmatrix} n \\ k \end{bmatrix}_q$.*

Proof. The number of k-dimensional subspaces is the number of k-tuples of vectors in $\mathbb{F}_q^n$ that are linearly independent divided by the number of k-tuples of vectors in $\mathbb{F}_q^k$ which are linearly independent. repassar

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$$

We can get a nicer expression by using the *q-analogue of the binommial coefficient*, defined as Falta □

Let X and Y be two triangles "in perspective", that is, such that there exists a point z with x_i, y_i and z are collinear (for $i = 1,2,3$). Let $z_{12} := (y_1 \oplus y_2) \cap (x_1 \oplus x_2)$. Counting dimensions (using Grassman's formula), and using that in a projective plane two lines always meet in a point, we get that z_{12} must be a single point. Then, defining analogously z_{13} and z_{23}, we get the following result:

Theorem 4.6.2 (Desargues)**.** *Let X and Y be two triangles "in perspective". Then, the previously defined z_{12}, z_{13} and z_{23} are collinear.*

Proof. Suppose the whole structure is not contained in a plane. Then, it is contained in a 3-dimensional subspace, so π_x and π_y are distinct planes (where we define $\pi_x := x_1 \oplus x_2 \oplus x_3$ and $\pi_y := y_1 \oplus y_2 \oplus y_3$).

By Grassmann's formula, $3 + 3 - 4 = 2$, so $\pi_x \cap \pi_y$ is a line ℓ. Since, $z_{ij} \in \pi_x$ and $z_{ij} \in \pi_y$, we get that all z_{ij} are contained in line ℓ, so they are collinear.

If the whole structure is contained in a plane π, we can not apply the previous argument, as now $\dim(\pi_x \cup \pi_y) = \dim \pi = 3$. So in that case we choose another line ℓ_4 incident with z and not contained in π. Choosing arbitrary x_4 and y_4 in ℓ_4, and applying the first argument, the points z_{12}, z_{14} and z_{24} are collinear. Similarly, z_{13}, z_{14} and z_{34} are collinear, and z_{23}, z_{24} and $z34$ are collinear.

This implies that z_{12}, z_{13} and z_{23} are contained in $\pi_4 = z_{14} \oplus z_{24} \oplus z_{34}$, but they are also in π. We now that π_4 and π span a 3-dimensional space, so applying once again Grassmann's formula, $\dim \pi_4 \cap \pi = 3 + 3 - 4 = 2$, so z_{12}, z_{13} and z_{23} lie in a common line. □

Definition 4.6.1 (Spread)**.** A *spread* of $\mathbb{F}_q^{2t}$ is a set of t-dimensional subspaces which partition the non-zero vectors of $\mathbb{F}_q^{2t}$.

Example 4.6.1. Let $q = p^k$, where $p > 2$ and $k \geq 2$. Let η be a non-square of $\mathbb{F}_q$. For any $a, b \in \mathbb{F}_q$, we define

$$U_{ab} := \langle (1, 0, a, b), (0, 1, b, \eta a^p) \rangle$$
$$U_\infty = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle$$

We then claim that $\{U_{ab} : a, b \in \mathbb{F}_q\} \cup \{U_\infty\}$ is a spread of F_q^4.

Notice that $U_{ab} = \{(x, y, ax + by, bx + \eta a^p y) : x, y \in \mathbb{F}_q, x \neq 0 \text{ or } y \neq 0\}$, so it suffices to prove that these are different for every pair (a, b), that is, that

$$(ax + by, bx + \eta a^p y) \neq (a'x + b'y, , b'x + \eta (a')^p y)$$

Assume they are equal for some values of a, b, a', b', x, y. Then, in matricial form,

$$\begin{pmatrix} a & b \\ b & \eta a^p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a' & b' \\ b' & \eta (a')^p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

so the determinant of the substraction of both matrices bust be zero, and that implies that

$$\eta(a - a')(a^p - a'^p) = (b - b')^2 \implies \eta(a - a')^{p+1} = (b - b')^2$$

since the characteristic of the field is p, so $(x + y)^p = x^p + y^p$. Therefore, the product of η with a square gives another square, so η itself must be a square, reaching a contradiction.

Theorem 4.6.3. *Let S be a spread of $\mathbb{F}_q^{2t}$. Let P be the set of vectors of F_q^{2t} and let L be the set of cosets of subspaces of S. Then, (P, L) is an affine plane of order q^t.*

Proof. For $u, v \in P$, let U be the unique element of S containing $u - v$. Then, $v \in U + v$ (taking $0 \in U$) and $u \in U + v$ (taking $u - v \in U$), so u and v are joined by a line. It can proved that this line is indeed unique, so (P, L) is a linear space.

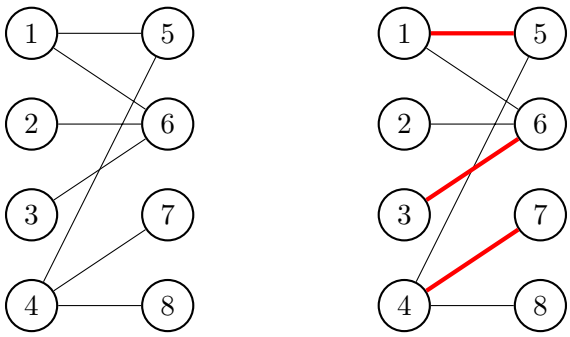
The lines which are cosets of the same subspace form a parallel set of lines. And it can be checked that we end up getting a projective plane not satisfying Desargues theorem. □

5 Matchings

5.1 Basic definitions

Definition 5.1.1 (Matching)**.** A *matching* is a set of non-intersecting edges in a graph. Given a graph Γ, we define $\mathrm{m}(\Gamma)$ as the maximum size of a matching in Γ.

Example 5.1.1. One can check that $\mathrm{m}(\Gamma) = 3$ for the following graph. An example of a maximum matching is given in red.



Definition 5.1.2 (Vertex cover)**.** A *vertex cover* is a set of vertices that cover all the edges (that is, a set of vertices such that every edge incides on at least one of these vertices).

Given a graph Γ, we define $\mathrm{vc}(\Gamma)$ as the minimum size of a vertex cover of Γ.

Example 5.1.2. In the graph from the previous example, $\mathrm{vc}(\Gamma) = 3$, which is equal to $\mathrm{m}(\Gamma)$. However, notice that by adding an edge between vertices 7 and 8, the minimum vertex cover increases by one while the maximum matching size does not change. The following theorem tells us that this can only happen because the graph is not bipartite now.

Theorem 5.1.1 (König)**.** *Let Γ be a bipartite graph. Then,* $\mathrm{m}(\Gamma) = \mathrm{vc}(\Gamma)$.

Proof. If all vertices have degree ≤ 2, then Γ is the union of disjoint even cycles and paths. In a path of length n, both the maximum matching and the minimum vertex cover are of size $\lfloor n/2 \rfloor$. In a cycle of length $2n$, both the maximum matching and the minimum vertex cover are of size n. Therefore, by adding all together, we get that $\mathrm{m}(\Gamma) = \mathrm{vc}(\Gamma)$ in the whole graph.

Note that in a cycle of odd length such as C_3, we have that $\mathrm{m}(C_3) = 1 \neq 2 = \mathrm{vc}(C_3)$. Thus, this result is only valid for bipartite graphs.

Let us assume u is a vertex of degree ≥ 3. Let v be a neighbour of u. Suppose that Γ is the graph with the least number of vertices (and among these, the graph with the least number of edges) such that $\mathrm{m}(\Gamma) \neq \mathrm{vc}(\Gamma)$.

We will divide the proof in two cases. First, suppose all matchings of size $\mathrm{m}(\Gamma)$ cover v. Then, $\mathrm{m}(\Gamma \setminus \{v\}) < \mathrm{m}(\Gamma)$, and in $\Gamma \setminus \{v\}$ we have erased at most one edge of every matching, so $\mathrm{m}(\Gamma \setminus \{v\}) = \mathrm{m}(\Gamma) - 1$. Then, by the minimality assumption on Γ, $\mathrm{vc}(\Gamma \setminus \{v\}) = \mathrm{m}(\Gamma \setminus \{v\}) = \mathrm{m}(\Gamma) - 1$.

Clearly, for any graph, $\mathrm{m}(\Gamma) \leq \mathrm{vc}(\Gamma)$, since every edge in the matching must be covered and they are non-intersecting. In our particular case, we have that $\mathrm{vc}(\Gamma) \leq \mathrm{m}(\Gamma)$, since $\mathrm{vc}(\Gamma \setminus \{v\}) = \mathrm{m}(\Gamma) - 1$ and we can extend it to a cover of Γ by adding the vertex v. Therefore, $\mathrm{m}(\Gamma) = \mathrm{vc}(\Gamma)$, reaching a contradiction.

The other case is when there is a matching M of size $\mathrm{m}(\Gamma)$ that does not cover v. We know that u has degree at least 3, so it has at least 2 edges not incident with v. Only one of these can be in M, so we have an edge e incident to u (and not v) such that $e \notin M$.

Then, M is a matching of $\Gamma \setminus e$, so by the minimality of Γ, there exists a vertex cover W of $\Gamma \setminus e$ of the same size. A vertex can not cover more than 2 edges from M, so every vertex from W must cover an edge in M. Hence, $v \notin W$, and thus, since W is a vertex cover of $\Gamma \setminus e$, it must contain u.

As e was incident to u, W will also be a vertex cover of Γ, so $\mathrm{vc}(\Gamma) \leq \mathrm{m}(\Gamma) \implies \mathrm{vc}(\Gamma) = \mathrm{m}(\Gamma)$, reaching once again a contradiction. □

5.2 Hall's Theorem

Definition 5.2.1 (Alternating path)**.** An *alternating path* with respect to a matching M is a path that alternates between edges in M and edges not in M, and that starts in an unmatched vertex.

We say that an alternating path is *augmenting* if the last vertex is unmatched (that is, not incident to any edge in M).

Notice that an augmenting alternating path gives rise to a larger matching, since switching all the edges in the path (from $\in M$ to $\notin M$ and viceversa) still gives a valid matching, whose size has increased by one.

Definition 5.2.2 (Hall's condition)**.** Let $A \cup X$ be a bipartite graph. For any subset $J \subseteq A$, let $N(J)$ be the subset of vertices of X that are joined to some vertex in J.

We say that the graph follows *Hall's condition* if $|N(J)| \geq |J|$ for any $J \subseteq A$.

Theorem 5.2.1 (Hall)**.** *If Hall's condition holds in the bipartite graph $A \cup X$, then there exists a matching covering all vertices in A.*

Remark. We already saw this theorem when working with SDRs. There, the A_i correspond to $N(a_i)$ and $a_i x_i$ was an edge if $x_i \in SDR$. repassar

Proof. Let M be a matching that does not cover $a_1 \in A$. By Hall's condition, there exists a $x_1 \in X$ such that $a_1 x_1$ is an edge of the graph. Suppose x_1 is covered by a certain $x_1 a_2 \in M$. Then, applying Hall's condition on $\{a_1, a_2\}$, we get an $x_2 \neq x_1$ neighbour of a_2 or a_1. We can continue this process until we get to a x_k that is not covered by any edge in M. (That must happen at some point, since a_1 is not covered by M and $|X| \geq |A|$.)

Now, starting from x_k, we can find an augmenting alternating path that ends at a_1. The process is the following: from x_j we go to an a_i with $i \leq j$ such that $a_i x_j$ is an edge of the graph (it exists because of the definition of x_j). From a_i (if $i > 1$), we go to x_{i-1} (we know $x_{i-1} a_i \in M$ by definition of a_i). When we reach a_1, we stop. Notice that the path we obtain is augmenting because it alternates between edges $\in M$ and $\notin M$, and the first and last vertices (a_1 and x_k) are not incident to any edge in M.

As described earlier, we can switch all the edges from the alternating path to get a bigger matching, so M is not maximal. Hence, in any maximal matching, all vertices of A must be covered. □

Definition 5.2.3 (Perfect matching)**.** A *perfect matching* is a matching that covers all the vertices.

Theorem 5.2.2. *A k-regular bipartite graph has a perfect matching.*

Proof. Let $J \subseteq A$. Counting the pairs (a, x) with $a \in J$ and where ax is an edge, we get that we have $|J|$ options for a and k options for x (fixing a). Therefore, the number of pairs is $|J|\,k$.

Counting x first, we get that at most there are $|N(J)|\,k$ pairs, so we get the inequality of Hall's condition: $|N(J)| \geq |J|$. Then, by Hall's theorem, there exists a perfect matching (since $|A| = |X|$). repassar □

Definition 5.2.4 (k-factor)**.** Given a graph Γ, a k-factor is a k-regular subgraph which contains all the vertices in Γ.

Observe that, according to this definition, a perfect matching is a 1-factor and a cycle decomposition is a 2-factor.

A *k-factorization* is a decomposition of the edges of Γ into k-factors.

Corollary 5.2.1. *A k-regular bipartite graph has a 1-factorization (that is, a decomposition into perfect matchings).*

Proof. By theorem 5.2.2 we have a perfect matching, and removing it we obtain a $k-1$-regular bipartite graph (as every vertex is covered by exactly one edge of a perfect matching). We can repeat this process until reaching a graph with no edges. The k perfect matchings we have found will form a 1-factorization of the original graph. □

5.3 Stable matchings

In this section we will suppose that every vertex has a preference order on its neighbours. This will enable us to measure how "good" and how "stable" is a matching.

Definition 5.3.1 (Unstable edge)**.** Let M be a matching of Γ. Let xy be an edge of $\Gamma \setminus M$. Suppose that x is matched with y' and y is matched with x'. We say that the edge xy is *unstable* if x prefers y to y' and y prefers x to x'. We will consider that a vertex always prefers any matching to being unmatched.

Definition 5.3.2 (Stable matching)**.** A matching M is *stable* if there are no unstable edges in Γ with respect to M.

This last definition implies that a stable matching is maximal (that is, it can not be extended further), because otherwise the edge xy that extends it would be unstable (as both vertices are not currently covered by M, and being unmatched is always last in order of preference).

Theorem 5.3.1. *Every bipartite graph has a stable matching.*

Proof. Suppose $A \cup B$ is the vertex partition of our graph. We will describe an iterative algorithm that reaches a stable matching.

We start with each vertex in A proposing to its most preferred neighbour. If a vertex in B receives ≥ 2 proposals, then it rejects all of them but the most preferred (and the other edges are deleted). This process is repeated until no vertex in B receives ≥ 2 proposals.

Notice that some vertices in A might end up not being matched, but we claim that the resulting matching M is stable. Suppose there's a unstable edge ab with respect to M. We will divide the proof in 4 cases:

- If a and b are unmatched, then b can not have had any proposal, but then the edge ab is not deleted so a should have proposed to b in the last iteration (it can not have been rejected in the last iteration because of the termination condition).
- Suppose a is unmatched and b is matched. The edge is unstable, so b must prefer a to its current match a'. But then, a would have proposed to b at some point and then a' would have been rejected, so this case can not occur.
- Suppose a is matched, and b is unmatched. The edge is unstable, so a prefers b to its current match b'. b can not have been proposed to ever, but a should have proposed to b before b', so this case is also impossible.
- Suppose a and b are both matched. Then a prefers b to its current match b' and b prefers a to its current match a'. By the order of preference, a must have proposed to b before b', and this proposal has been rejected, so the match of b must be more preferred than a, so it must also have rejected a', reaching a contradiction.

□

Corollary 5.3.1. *$K_{n,n}$ has a perfect stable matching.*

5.4 Tutte's Theorem

Given a graph, we can define an equivalence relation on the set of vertices such that $v \sim v'$ if they can be joined by a path. The equivalence classes of this relation are the *connected components* of the graph. In this section we will be interested in *odd components*, that is, connected components with an odd number of vertices.

Let $\mathrm{oc}(\Gamma)$ be the number of odd components of the graph Γ. Recall that a perfect matching is a matching that covers all the vertices. The following theorem tells us that these two notions are related:

Theorem 5.4.1 (Tutte)**.** *A graph Γ has a perfect matching iff $\mathrm{oc}(\Gamma \setminus S) \leq |S|$ for all subsets S of the vertices of Γ.*

Proof. $\boxed{\Longrightarrow}$ Let Γ be a graph with a perfect matching M. Let $S \subset V(\Gamma)$. Every odd component of $\Gamma \setminus S$ will have a vertex that is "left out" by the matching with other vertices in the same component, so it must be connected to a vertex in S. Therefore, for every odd component there must be at least a vertex in S connected to it, and these vertices must be pair-wise different (otherwise it would not be a matching). Then, $|S| \geq \mathrm{oc}(\Gamma \setminus S)$.

$\boxed{\Longleftarrow}$ Suppose Γ does not have a perfect matching. Let's add arbitrary edges to Γ until adding any other edge would give us a graph with a perfect matching. Let Γ^* be this new graph.

Notice that by adding edges we can not increase the number of odd components. Therefore, the condition $\mathrm{oc}(\Gamma^* \setminus S) \leq |S|$ still holds for every subset S of the vertices in Γ^*.

Let K be the set of vertices of Γ^* that are joined to all the other vertices.

- If $\Gamma^* \setminus K$ has only complete components (i.e., all components are isomorphic to a complete graph), then in the even components we can pair up the vertices to get a perfect matching, while in the odd components we can pair up all the vertices but one. The remaining vertex of each odd component can be paired with a vertex in K, as $\mathrm{oc}(\Gamma^* \setminus K) \leq |K|$.

  We have paired every vertex except perhaps some vertices from K. If there was an odd number of vertices left, then we would not be able to extend this to a perfect matching. However, this can not happen. Taking $S = \emptyset$, we get that $\mathrm{oc}(\Gamma^*) \leq 0$, so Γ^* must have an even number of vertices. Therefore, the number of remaining vertices in K after pairing all the odd components must be even, so we can join them two by two.

- The other case to check is when $\Gamma^* \setminus K$ does not decompose into complete components. That means there exists a connected component that lacks at least one edge. This component must have at least 3 vertices (in order to stay connected), and it is easy to see that it must have 3 vertices a, b and c such that a and c have an edge with b but not with each other.

  Let M_{ac} be the perfect matching obtained by adding the edge (ac) (it exists because of the maximality condition of Γ^*). Notice that there must also be a vertex $d \in \Gamma^* \setminus K$ such that (bd) is not an edge (otherwise $b \in K$). Let M_{bd} be the matching obtained by adding the edge (bd) to Γ^*. Now we'll construct a path P starting with $b \to d$ and alternating between edges in M_{bd} and M_{ac}. (Notice that $(bd) \in M_{\mathrm{bd}}$ because Γ^* had no perfect matching.)

Notice that there can not be an edge in this path both in M_{bd} and M_{ac}, as then it will create a conflict with the previous edge (and the path has length at least 2, because $(bd) \notin M_{\text{ac}}$, so vertex d must be covered by some edge in M_{ac}). Therefore, we will always find an edge to continue the path (as both M_{ac} and M_{bd} are perfect matchings) unless we cycle back to b.

Now we branch into two more subcases:

- If the path P gets to a before b (wlog first a than c, because both vertices are equivalent), then we can modify M_{bd} by discarding the edges in $M_{\text{bd}} \cap P$ and choosing the edges in $M_{\text{ac}} \cap P$ together with (ab). This would give a perfect matching of $\Gamma^* \cup \{ac\}$ and also of Γ^*, since (ac) is not in the path P up until that point. Therefore, we reach a contradiction.
- If the path P cycles back to b without going through a or c, then we can modify M_{bd} by replacing the edges in $M_{\text{bd}} \cap P$ by the edges in $M_{\text{ac}} \cap P$, obtaining a perfect matching of Γ^* (since a and c are not visited in P, so $(ac) \notin P$). Again, this contradicts our assumptions.

□

Corollary 5.4.1 (Berge)**.** *Let* $d = \max_{S \subseteq V(\Gamma)} \{\text{oc}(\Gamma \setminus S) - |S|\}$. *Then there is a matching covering all but at most* d *vertices of* Γ.

Proof. We will modify the graph Γ so we can apply Tutte's theorem. Let Γ^* be the graph obtained from Γ by adding d vertices joined to all the other vertices. We claim that Γ^* satisfies Tutte's condition.

Let S^* be a subset of the vertices of Γ^*, and let K be the set of vertices we have added. We will split the proof into three cases:

- Suppose $S^* = \emptyset$. We need to show that $\text{oc}(\Gamma^*) = 0$. Since Γ^* is connected (due to the new vertices we have added), we have to show that it has an even number of vertices. By construction, $|V(\Gamma^*)| = |V(\Gamma)| + \text{oc}(\Gamma \setminus S) - |S|$ for some subset $S \subseteq V(\Gamma)$. Notice that the parity of $\text{oc}(\Gamma \setminus S)$ is equal to the parity of $|V(\Gamma \setminus S)|$, and $|V(\Gamma \setminus S)| = |V(\Gamma)| - |S|$, so by the previous formula $|V(\Gamma^*)|$ must be even.
- Suppose $S^* \neq \emptyset$ and $K \not\subseteq S^*$. Then, at least one of the vertices in K remains, and these are connected to everything else, so $\Gamma^* \setminus S^*$ is connected. Therefore, $\text{oc}(\Gamma^* \setminus S^*) \leq 1$ but $S^* \neq \emptyset$, so $|S^*| \geq 1$. Hence, Tutte's condition must hold.
- Suppose $K \subseteq S^*$. Let $S = S^* \setminus K$. Notice that $S \subseteq V(\Gamma)$, and $\Gamma^* \setminus S^* = \Gamma \setminus S$. Therefore,

  $$\text{oc}(\Gamma^* \setminus S^*) = \text{oc}(\Gamma \setminus S) \leq d + |S|$$

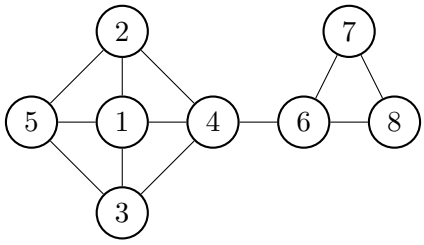
  by definition of d. And $|K| = d$, so $|S^*| = d + |S|$. Putting it all together, we get that $\text{oc}(\Gamma^* \setminus S^*) \leq |S^*|$, so Tutte's condition holds.

Once we know Γ^* satisfies Tutte's condition, then it must have a perfect matching, which induces a matching in Γ where at most d vertices are left unmatched. □

Definition 5.4.1 (Cubic graph)**.** A *cubic graph* is a graph in which all vertices ahve degree 3.

Definition 5.4.2 (Bridge)**.** A *bridge* is an edge of a graph whose deletion increases the number of connected components.

Example 5.4.1. The edge $\{4, 6\}$ of the following graph is a bridge, as it increases the number of connected components to 2, while the edge $\{6, 7\}$ is not.



Corollary 5.4.2. *Any bridgeless cubic graph has a perfect matching.*

Proof. It is enough to prove the result for a connected graph, since then one can find a perfect matching for every connected component.

Let S be a subset of vertices, and suppose D is an odd component of $\Gamma \setminus S$. Since D is an odd component and every vertex has degree 3 in Γ, then there must be an odd number of edges from D to S (otherwise the sum of the internal degrees in D would be even, but there is an odd number of vertices with odd degree). However, there can not be only one edge from D to S (as this edge would be a bridge of Γ), so there are at least 3.

Therefore, there are at least $3 \cdot \mathrm{oc}(\Gamma \setminus S)$ edges going into S, and S has at most $3\,|S|$ edges coming in, so $\mathrm{oc}(\Gamma \setminus S) \leq |S|$. Hence, by Tutte's theorem, Γ must have a perfect matching. □

5.5 Coverings and independent sets

Definition 5.5.1 (Independent set)**.** An *independent set* I is a subset of vertices such that there is no edge joining two vertices in I.

We define $\mathrm{is}(\Gamma)$ as the maximum size of an independent set in Γ.

Recall that we defined $\mathrm{vc}(\Gamma)$ as the minimum size of a vertex cover of Γ. This quantity is related to $\mathrm{is}(\Gamma)$:

Lemma 5.5.1. $\mathrm{is}(\Gamma)+\mathrm{vc}(\Gamma) = |V(\Gamma)|$

Proof. Let U be any vertex cover. Then, $\Gamma \setminus U$ is an independent set, since every edge is incident to some vertex in U.

Conversely, let I be an independent set. Then, $\Gamma \setminus I$ is a vertex cover, since there is no edge between two vertices in I, so every edge must be covered by some vertex in $\Gamma \setminus I$.

Hence we have the two inequalities:

falta □

Definition 5.5.2 (Edge-covering)**.** An *edge-covering* is a subset of the edges which covers all the vertices. We define $\mathrm{ec}(\Gamma)$ as the minimum size of an edge-covering.

Recall that we defined $\mathrm{m}(\Gamma)$ as the maximum size of a matching in Γ. Just as before, these two quantities are related:

Theorem 5.5.1. $\mathrm{ec}(\Gamma) + \mathrm{m}(\Gamma) = |V(\Gamma)|$

Proof. Let L be an edge-covering of minimum size $\mathrm{ec}(\Gamma)$. Then L can not conatin any path of length 3 (as dropping the middle edge would still give an edge-covering. Therefore, L is the union of some number of disjoint stars.

Let k be the number of connected components of L, and let ℓ_i be the number of edges of the i-th component. Then,

$$\sum_{i=1}^{k}(\ell_i + 1) = |V(\Gamma)|$$

since a star with ℓ_i edges covers $\ell_i + 1$ vertices, so $|L| + k = |V(\Gamma)| \implies \mathrm{ec}(\Gamma) + k = |V(\Gamma)|$.

Taking an edge from each star we get a valid matching of size k, so $k \leq \mathrm{m}(\Gamma)$, and $\mathrm{ec}(\Gamma)+\mathrm{m}(\Gamma) \geq |V(\Gamma)|$.

Now we will prove the reverse inequality. Let M be a matching of size $\mathrm{m}(\Gamma)$. There are $|V(\Gamma)| - 2\mathrm{m}(\Gamma)$ vertices not covered by M. Choosing an edge for each of these vertices, we find an each covering with at most $|V(\Gamma)| - 2\mathrm{m}(\Gamma) + \mathrm{m}(\Gamma)$ edges, so

$$|V(\Gamma)| - \mathrm{m}(\Gamma) \geq \mathrm{ec}(\Gamma) \implies \mathrm{ec}(\Gamma) + \mathrm{m}(\Gamma) \leq |V(\Gamma)|$$

□

6 Graph Connectivity

6.1 Basic Definitions

Definition 6.1.1 (Connected graph)**.** We say that a graph $G = (V, E)$ is *connected* if, for every pair $x, y \in V$, there is a path in G connecting them.

Definition 6.1.2 (Connected component)**.** A *connected component* of a graph G is a maximal subgraph which is connected. Note that the maximality refers both to adding vertices and edges.

Definition 6.1.3 (Tree)**.** A *tree* T is a graph which is connected and acyclic.

Proposition 6.1.1. *The following are equivalent:*

(i) T *is a tree.*

(ii) T *is an edge-minimal connected graph (we can not remove any edge while keeping* T *connected).*

(iii) T *is an edge-maximal acyclic graph (we can not add any edge while keeping* T *acyclic).*

(iv) $|V(T)| = |E(T)| + 1$ *and either* T *is connected or acyclic.*

Definition 6.1.4 (Spanning tree)**.** We say that T is a *spanning tree* of graph G if T is a tree subgraph of G with the same vertices.

Proposition 6.1.2. *A graph is connected if, and only if, it contains a spanning tree.*

Proof. We claim that G is connected if, and only if, for all subsets $X \subsetneq V$ there exists an edge $e \in E$ incident to exactly one vertex of X. Then, in order to prove the proposition, we start with some $x_1 \in V$ and let x_2 be the vertex at the other end of the edge joining $\{x_1\}$ with $V \setminus \{x_1\}$.

Recursively, if $X_i = \{x_1, \ldots, x_i\}$, we find an edge joining X_i with $V \setminus X_i$, and add the vertex at the other end to form X_{i+1}.

At the end we get a connected graph with $|V|$ vertices and $|V|-1$ edges, so it must be a spanning tree of G. □

Definition 6.1.5 (Leaf)**.** We say that a vertex of a tree is a *leaf* if it has degree 1.

Lemma 6.1.1. *Every tree has at least* 2 *leaves.*

Proof. Due to the handshaking lemma, $2|E| = \sum d(x)$. As we are in a tree, $|E| = n - 1$, where n is the number of vertices, so

$$2(n-1) = \sum_{x \in V} d(x) = |L| + \sum_{\substack{x \in V \\ d(x) \geq 2}} d(x) \geq |L| + 2(n - |L|) = 2n - |L|$$

and therefore $|L| \geq 2$. □

Intuitively, some graphs are "more connected" than others, as removing some edges doesn't affect its connectivity. We will quantify this notion with the following definition:

Definition 6.1.6 (k-connected)**.** We say that a graph G (with $|V| \geq k+1$) is k-connected, for some $k \geq 0$, if it is the complete graph of $k+1$ vertices, or if we need to remove at least k vertices in order to disconnect it.

We can also state the definition in terms of separators:

Definition 6.1.7 (Separator)**.** Let $G = (V, E)$ be a graph. A subset $S \subset V$ is a *separator* if the subgraph induced by $V \setminus S$, $G[V \setminus S]$, is not connected.

With this definition, a graph G with $|V(G)| \geq k+1$ is k-connected if G is the complete graph on $k+1$ vertices or if every separator S has size $|S| \geq k$.

Example 6.1.1.

i A tree is 0-connected and 1-connected, but it is not 2-connected, as we can break it into two connected components by removing just a vertex.

ii A cycle is 2-connected, as removing just one vertex gives a path, but it is not 3-connected, as we can disconnect it by removing 2 vertices. Notice that by the technicalities of the definition, K_3 is 2-connected by default.

Definition 6.1.8 (Connectivity)**.** The *connectivity* of graph G is the maximum $k \geq 0$ such that G is k-connected. We will denote it by $k(G)$.

6.2 Structure of k-connected graphs

We will now try to understand the structure of graphs with connectivty k for small values of k. Notice that we have already characterized the graphs with connectivity 1 as trees.

6.2.1 Structure of 2-connected graphs

Definition 6.2.1 (Block)**.** A *block* of a graph is a maximal 2-connected subgraph. Technically, we will also consider a graph with either a single vertex or two vertices joined by an edge as a block.

Notice that two different blocks of a graph can intersect at most in one vertex. Otherwise, it can be seen that the union would be a block, as we would need to remove at least two vertices in order to break it.

Definition 6.2.2 (Articulation point)**.** A vertex in the intersection of two different blocks is called an *articulation point*.

Example 6.2.1. The following graph can be divided in 4 blocks, marked by the dotted lines. Notice that some of these blocks intersect in articulation points 4 and 7. Falta graf

Proposition 6.2.1. *Let G be a connected graph. Let $A \subseteq V(G)$ be the set of articulation points of G, and let $\mathcal{B}$ be the set of blocks of G. Then the bipartite graph H with vertices $A \cup \mathcal{B}$ and edges $(a, B) \in A \times \mathcal{B}$ such that $a \in B$, is a tree.*

Example 6.2.2. This is the tree constructed from the graph of the previous example: Falta dibuix

Proof. We need to prove that H is connected and acyclic. We will just give an informal sketch of the proof:

The fact that it is connected comes from FALTA

Suppose that we had a cycle in H. Then, the union of the blocks in that cycle would make a 2-connected component of G, contradicting their maximality. Therefore, H is acyclic. □

Proposition 6.2.2. *Every 2-connected graph G admits a sequence $G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$, where G_0 is a cycle and G_i is obtained from G_{i-1} by adding a path connecting two distinct vertices.*

Proof. If the sequence exists, it is clear that every vertex in G is contained in a cycle, so G is at least 2-connected. Reciprocally, if G is 2-connected, it has to contain a cycle (an acyclic graph is either disconnected or a tree). Therefore, starting with that cycle, we define $G' \subseteq G$ as the maximal subgraph constructed according to the above procedure. We need to show that this construction gives G, that is, that $G' = G$.

By maximality, $G' = G[V(G')]$, as otherwise we can add an extra edge to G'. If $G' \neq G$, that means that there is a $v \in V(G) \setminus V(G')$. By 2-connectedness, there must be at least two disjoint paths joining v with $V(G')$. Then, concatenating this two paths, we get a path from $V(G')$ to $V(G')$, contradicting once again the maximality of G'. □

6.2.2 Structure of 3-connected graphs

Definition 6.2.3 (Contraction)**.** Given a graph G, the *contraction* of an edge $e \in E(G)$ is the graph G/e resulting from identifying the end vertices of e and identifying any resulting multiple edges.

Example 6.2.3. Contracting the red edge in the graph in the left gives as a result the graph on the right.

Falta dibuix

Lemma 6.2.1. *If G is 3-connected, then there is an edge $e \in E(G)$ such that G/e is also 3-connected.*

Remark. Note that there can be some edges whose contraction decreases the connectivity of the graph (think for example of two K_n separated by a triangle, we can not contract the edges of the triangle without creating a bridge). However, what the lemma tells us is that there exists some edge whose contraction still retains the 3-connectivity.

Proof. Suppose that G/e is not 3-connected. Let v_{xy} be the vertex resulting from the contraction of $e = xy$. Note that every minimum separator S of G/e must contain v_{xy} (otherwise it would also separate the original graph G). Therefore, when decontracting e, S is still a minimum separator, that can have at most 3 vertices.

We have seen that the assumption that G/e is not 3-connected implies that G/e is 2-connected, and every minimum separator of G/e must contain the contracted vertex v_{xy}. Now, if G/e is not 3-connected for every $e \in E(G)$, then for every edge $e = xy \in E(G)$ we can choose a third point z_{xy} such that v_{xy} and z_{xy} separate G/e (and hence $\{x, y, z\}$ separate G).

Let C be the smallest connected component of $G[V \setminus \{x, y, z\}]$ (in number of vertices), among all possible choices of $e = xy$ and z.

Remark. If S is a minimum separator of G, then every vertex in S is adjacent to every connected component of $G[V \setminus S]$. That's because, if for a $x \in S$ there was a component of $G[V \setminus S]$ not incident to it, then $S \setminus \{x\}$ would still be a separator of the graph.

The previous remark tells us that z must have a neigbour $u \in C$. Let $e' = uz$, and consider the separator $\{u, z, z'\}$, for some z'. Notice that u can not be connected to any other vertex in the graph except those in C and maybe x or y. Consider a connected component C' not containing x and y. Vertex u must be adjacent to C', so $C' \subset C \setminus \{u\}$, contradicting our choice of C. □

Theorem 6.2.1 (Tutte)**.** *A graph G is 3-connected if, and only if, there is a sequence $G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ such that $G_0 = K_4$ and every G_{i+1} has an edge $e = xy$ such that $G_i = G_{i+1}/e$ and $d(x), d(y) \geq 3$ in G_{i+1}.*

Proof. $\boxed{\Longrightarrow}$ If G is 3-connected, than there exists an edge $e \in E(G)$ such that G/e is 3-connected. By contracting this edge and repeating the same procedure, we eventually reach a 3-connected graph with just 4 vertices, and the only one is K_4.

$\boxed{\Longleftarrow}$ Given a sequence of graphs following the hypothesis, we will show that G_i 3-connected implies that G_{i+1} is 3-connected. As $G_0 = K_4$ is 3-connected, that implies that $G = G_n$ is 3-connected.

Suppose G_{i+1} is not 3-connected but G_i is. Let $e = xy$ be an edge such that $G_i = G_{i+1}/e$. Let S be a minimum separator of G_{i+1}. We have assumed that $|S| \leq 2$. Notice that S can not contain both x and y, since then G_i would be 1-connected. Similarly, S can not be disjoint from $\{x, y\}$, as then S would separate G_i so G_i would be 2-connected.

We can suppose then without loss of generality that $S \cap \{x, y\} = \{x\}$. That implies that the connected component of $G_{i+1}[V \setminus S]$ containing y consists only of $\{y\}$. But then $d_{G_{i+1}}(y) < 3$, reaching a contradiction. Repassar □

For $k \geq 4$, the characterization of k-connected graphs is much more involved, so we will not consider it in this course.

6.3 Menger's Theorem

Another natural notion of k-connectivity is that a graph is k-connected if for every pair of vertices x and y, there exist at least k paths from x to y that are vertex-disjoint (except for their endpoints). It is easy to see that if this condition holds, then every separator must have at least k vertices (as we can take a pair x, y in opposite sides of the partition and we need a separating vertex for every such path). Menger's theorem tells us that the reciprocal is also true.

First we will introduce a few definitions:

Definition 6.3.1 (AB-separator)**.** Let $A, B \subseteq V(G)$. An *AB-separator* is a set S such that there are no paths from A to B that are contained in $G[V \setminus S]$.

Notice that paths of length zero are allowed, so every AB-separator must contain the vertices in $A \cap B$.

Definition 6.3.2 (AB-connector)**.** An *AB-connector* is a graph $C \subseteq G$ such that all of its components are paths from a vertex in A to a vertex in B. Here we also allow paths of length zero.

We define the size of a connector C as its number of paths.

Theorem 6.3.1 (Menger)**.** *Let G be a graph and let $A, B \subseteq V(G)$. Then, the minimum cardinality of an AB-separator equals the maximum cardinality of an AB-connector.*

Remark. This theorem is related to the min-max theorem, that might be familiar to those interested in linear programming.

Proof. We will prove it by induction on $m = E(G)$. As we have mentioned before, one of the directions is trivial. Let S be a minimum AB-separator with $|S| = s$, and let C be a maximum AB-connector with $|C| = c$. The, $s \geq c$, as S must contain a vertex of every path in C, which are vertex-disjoint.

We will prove that $c \geq s$ by induction on m. If $m = 0$, there are no edges, so $s = |A \cap B| = c$. Now we assume that $m > 0$, and that the theorem holds for $m - 1$. Take an edge $e = xy$ and remove it from G (keeping its end-vertices), obtaining G'.

Let S' be a minimum AB-separator of G'. If $|S'| = s$, then we are done, because every AB-connector in G' is also a connector in G, so $c \geq c' = s$. Suppose then that $|S'| < s$. Then, $S_1 := S' \cup \{x\}$ and $S_2 := S' \cup \{y\}$ are both AB-separators of G, so $|S'| = s - 1$.

Let S'' be an AS_1-separator of G'. Notice that S'' is also an AB-separator in G, because in order to go from A to B we need to cross S_1 at some point, so an AS_1-separator is also a AB-separator.

Therefore, $|S''| \geq s$, so by the induction hypothesis there must be an AS_1-connector with at least s paths. Similarly, there exists an S_2B-connector with s paths. This paths are disjoint, and S_1 and S_2 have size s, so each vertex in S_1 and S_2 must be contained in one of the paths in the respective separator. Besides, there is an edge between x and y, so we can construct an AB-connector in G of size s by concatenating the paths of the AS_1-connector and the S_2B-connector (and adding the edge xy). Then, $c \geq s$. □

The other statement of Menger's theorem follows directly from this one:

Theorem 6.3.2 (Menger)**.** *Let G be a k-connected graph. Then, for every $x, y \in V(G)$ with $x \neq y$, there are k internally disjoint paths connecting x and y.*

Proof. Let $A = N(x)$ and $B = N(y)$ be the set of neighbours of x and y. Every AB-separator S must have size $\geq k$ (as the graph is k-connected), so there exists an AB-connector with k paths. These paths are disjoint, so extending the paths by adding x to the beggining and y to the end will give us k internally disjoint paths between x and y. □

Let us recall the definition of transversal or SDR:

Definition 6.3.3 (Transversal)**.** A *transversal* (or *system of distinct representatives*) of a family of sets $\mathcal{A} = \{A_1, \ldots, A_m\}$, with $A_i \subseteq [n]$, is a m-tuple $(x_1, \ldots, x_m)$ of distinct elements such that $x_i \in A_i$.

Definition 6.3.4 (Common transversal)**.** Given two families of sets $\mathcal{A} = \{A_1, \ldots, A_m\}$ and $\mathcal{B} = \{B_1, \ldots, B_m\}$, with $A_i, B_i \subseteq [n]$, we define a *common transversal* as a m-tuple $(x_1, \ldots, x_n)$ of distinct elements that is both a transversal of $\mathcal{A}$ and of a reordering of $\mathcal{B}$ (that is, such that $x_i \in A_i \cap B_\sigma(i)$ for some $\sigma \in S_m$).

Theorem 6.3.3 (Ford and Fulkerson)**.** *There is a common transversal to $\mathcal{A}$ and $\mathcal{B}$ if, and only if, for all $I, J \subseteq [m]$, we have that*

$$\left| \left(\bigcup_{i \in I} A_i \right) \cap \left(\bigcup_{j \in J} B_i \right) \right| \geq |I| + |J| - m$$

Proof. We will use Menger's theorem on graph G with vertices $V(G) = \{s\} \cup \mathcal{A} \cup [n] \cup \mathcal{B} \cup \{t\}$ and edges $E(G) = \{\{s, A_i\} : i \in [m]\} \cup \{\{t, B_j\} : j \in [m]\} \cup \{\{x, A_i\} \in [n] \times \mathcal{A}\} : x \in A_i\}$.

In order to make sense of the previous construction, note that we are adding a source vertex s and a sink vertex t, together with a set of n vertices labelled by the elements of $[n]$. Then, we are connecting the source vertex to all sets in $\mathcal{A}$, the sink vertex to all sets in $\mathcal{B}$, and every set in $\mathcal{A}$ or $\mathcal{B}$ to the elements in $[n]$ that it contains.

We now claim that there is a common transversal of $\mathcal{A}$ and $\mathcal{B}$ if, and only if, there are m internally disjoint paths joining s and t in G. By Menger's theorem, this is equivalent to the condition that every separator S of $\{s\}$ and $\{t\}$ has $|S| \geq m$.

It only remains to show that the condition that every separator of $\{s\}$ and $\{t\}$ has size at least m is equivalent to the condition given in the statement of the theorem.

That's because if S is a separator, and we take $I = \{i \in [m] : A_i \notin S\}$ and $J = \{j \in [m] : B_j \notin S\}$, then

$$\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_i\right) \subseteq S \cap [n]$$

so, by looking at their cardinalities,

$$\left|\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_i\right)\right| \leq |S \cap [n]| = |S| - (m - |I|) - (m - |J|) = |I| + |J| - m + (|S| - m)$$

But by the condition in the statement of the theorem, the LHS is at least $|I| + |J| - m$, so $|S| - m \geq 0 \implies |S| \geq m$.

This has proved one of the directions: if the condition in the statement of the theorem holds, then there exists a transversal. But if there exists a transversal, then every separator S of s and t must have size $|S| \geq m$, and from here it can be seen by contradiction that the condition must hold. The details are left to the reader (sorry). □

6.4 Edge-connectivity

So far when we talked about connectivity we were referring to vertex-connectivity. In this section we will see how connectivity can also be defined in terms of the removal of edges.

Definition 6.4.1 (Edge-separator)**.** An *edge-separator* of a graph $G = (V, E)$ is a set of edges $E' \subseteq E$ such that $G - E' := (V, E \setminus E')$ is not connected.

Definition 6.4.2 (k-edge-connected)**.** We say that a graph G is *k-edge-connected* if every edge-separator has cardinality at least k.

Definition 6.4.3 (Edge-connectivity)**.** The *edge-connectivity* of graph G is the maximum non-negative integer $\lambda(G)$ such that G is $\lambda(G)$-edge-connected.

Proposition 6.4.1.

1. *For any graph with minimum degree $\delta(G)$, $k(G) \leq \lambda(G) \leq \delta(G)$.*
2. *If $\tilde{E}$ is a subset of edges of size $\lambda(G)$, then $G - \tilde{E}$ has at most 2 connected components.*

Proof. We will not concern ourselves with the full details, but just give an idea of why both statements are true.

1. If removing a certain set of edges disconnects the graph, then removing one vertex for each of these edges will also disconnect the graph, so $k(G) \leq \lambda(G)$. We have to be a little bit careful, as maybe if we remove a vertex from every edge in the separator, one of the two remaining connected components of the graph becomes empty. However, in that case it can be shown that we can choose the opposite vertex for some of the edges so that both connected components are not empty.

2. The idea is that by adding an edge from $\tilde{E}$ to $G - \tilde{E}$ we decrease the number of connected components by at most one. Therefore, if $G - \tilde{E}$ had more than 2 connected components, then $G - (\tilde{E} \setminus \{e\})$ would still be disconnected, so $\tilde{E} \setminus \{e\}$ would be an edge-separator with less than $\lambda(G)$ edges.

□

There is an analogue of Menger's theorem for edge-connectivity:

Theorem 6.4.1 (Menger)**.** *If G is k-edge connected, then for all $x \neq y \in V(G)$ there exist k edge-disjoint paths joining x and y.*

Proof. We will use Menger's theorem for vertex connectivity in the line graph (that is, the graph $L(G)$ where $V(L(G)) = E(G)$ and $E(L(G)) = \{\{e, e'\} : |e \cap e'| \neq \emptyset\}$).

It can be seen that $k(L(G)) = \lambda(G)$, so by taking two arbitrary edges incident to x and y (respectively), we know that there exist k vertex-disjoint paths in the line graph, and it can be shown that these paths correspond to edge-disjoint paths joining x and y. □

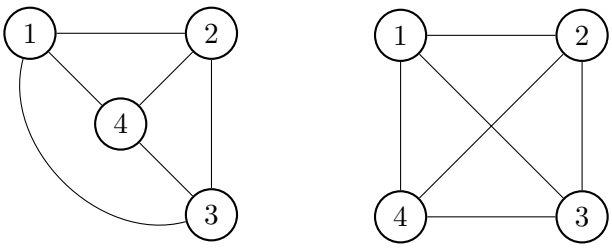
That's why edge-connectivity is not so widely studied as vertex-connectivity: because we can reduce edge-connectivity to vertex-connectivity by taking the line graph.

7 Planarity

7.1

Definition 7.1.1 (Planar graph)**.** We say that a graph G is *planar* if there is an embedding of the vertices of G in the plane $f : V(G) \longrightarrow \mathbb{R}^2$, such that for every edge $\{x, y\} \in E(G)$ we can draw a simple curve $\sigma_e : [0, 1] \longrightarrow \mathbb{R}^2$ that only intersects V in its endpoints ($\sigma_e(0) = x$, $\sigma_e(1) = y$, $\sigma(t) \notin V$ for all $t \in (0, 1)$) and such that no two edges intersect (except perhaps at their endpoint vertices).

Example 7.1.1. The graph K_4 is planar, as shown by the embedding on the left, but that does not mean that any embedding is valid. For example, the embedding on the right is not a valid plane embedding, as the edges 13 and 24 intersect.



Definition 7.1.2 (Plane graph)**.** A *plane graph* is a planar graph embedded in the plane with an embedding that satisfies the planarity conditions (a *plane embedding*). For example, only the K_4 on the left is a plane graph in the previous example, despite the fact that K_4 as a graph is planar.

Proposition 7.1.1. *If G is planar, then there is a plane embedding in which every edge in the embedding is a polygonal line (that is, piece-wise linear).*

Proof. We will polygonalize the edges one by one. Suppose we have the edge xy, with its corresponding curve σ_{xy}. We start at x, and find the circle with center in x of biggest radius such that it does not intersect any other vertices of the graph. (what about other edges?). Then we draw the line from x to the intersection of that circle with σ_{xy}, and start again from that point.

As the number of vertices is finite, it can be seen that this process reaches y in a finite number of steps (This needs better justification). Then, we will have obtained a polygonal line joining x and y. □

Theorem 7.1.1 (Jordan's curve theorem)**.** *Let C be a closed simple polygonal curve in the plane. Then, $\mathbb{R}^2 \setminus C$ consists of 2 arc-connected components, one bounded and the other unbounded.*

Remark. The previous theorem is also true for general simple curves, but the proof is much more involved.

Proof. (not rigourous)

Let C be a closed simple polygonal curve in the plane. C must have a finite number of segments, so we can rotate it slightly such that no segments are horizontal. Now, for every $x \in \mathbb{R}^2$, we draw an horizontal ray (either to the right or to the left, it is indifferent) and we define $\pi(x)$ to be the number of segments this ray crosses mod 2.

Let a, b and c be 3 points in the plane. By the pidgeonhole principle, at least 2 of them must have the same $\pi(x)$, and it can be shown that the two points with the same value of $\pi(x)$ can be joined by a curve. Therefore, there can not be more than 2 arc-connected components (as otherwise there would be 3 points no pair of which could be joined by a curve).

Besides, any horizontal line that crosses at least a segment of the curve will have both points with $\pi(x) = 0$ and with $\pi(x) = 1$, so at least there are 2 arc-connected components. And lastly, it can be seen that the component with $\pi(x) = 0$ is unbounded while the component with $\pi(x) = 1$ is bounded, completing the proof. □

Apart from vertices and edges, in plane graphs we have a third kind of "object":

Definition 7.1.3 (Face)**.** A *face* of a plane graph is an arc-connected component of $\mathbb{R}^2 - G$ (ie, $\mathbb{R}^2$ after removing the vertices and edges of G).

It is easy to see that a tree is a planar graph. One way to formalize it is by induction on the number of vertices. It is clear that the tree with 2 vertices is planar, and if we have a tree with n vertices, we can remove a leaf to get a tree with $n-1$ vertices, which by hypothesis is planar. Now we just need to find a point to place the new vertex such that it can be joined to its parent, and in fact any point in $\mathbb{R}^2 \setminus G$ is valid.

Besides, any planar embedding of a tree will only have a unique connected component. This can be proved again by induction, and we will use it to prove the following theorem:

Theorem 7.1.2 (Euler)**.** *Let G be a connected planar graph with n vertices and m edges. Then, every planar embedding of G has f faces, where*

$$n - m + f = 2$$

Proof. We will fix n and prove it by induction on m. The least amount of edges a connected graph with n vertices can have is $n-1$. In that case, the graph is a tree, so $f = 1$ and the formula holds.

Now suppose $m > n-1$. As G is connected but it's not a tree, we know that G must have a cycle C (remember trees can be characterized either as connected graphs with $n-1$ edges or as connected acyclic graphs). By removing one edge e in C, we get the graph $G-e$, which is still connected and planar. By induction it must satisfy Euler's formula, so

$$n-(m-1)+(f-1)=2 \implies n-m+f=2$$

Where we have used that removing e removes a face (as it joins a face from inside the cycle with a face from outside the cycle). This argument could be formalized further, but we will not concern ourselves with topological pathologies here. □

Proposition 7.1.2. *Let G be a plane graph. If G is 2-connected, then every bounded face has by boundary a cycle of G.*

Proof. If G is a cycle, then this follows from Jordan's curve theorem. If G is not a cycle, then there is a sequence of graphs

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_t = G$$

where G_0 is a cycle and every G_{i+1} is obtained from adding a path joining two vertices in G_i (that's the characterization we gave for 2-connected graphs).

By induction on t, if $t > 0$, we have that every face of G_{t-1} is bounded by a cycle of G_{t-1}. When we add a path to G_{t-1}, all the vertices in the path must belong to the same face. Therefore, every face in G_t is either contained in a cycle of G_{t-1}, or it is the face that has been split in two by the new path. And it is clear that this two new faces are bounded by a cycle containing the path together with some vertices from G_{t-1}. □

Theorem 7.1.3 (Tutte)**.** *Let G be a 3-connected plane graph. A cycle C in G is the boundary of a face f if, and only if, C is an induced cycle (a cycle without any chord) and a non-separating cycle (a cycle such that $G-C$ is still connected).*

Proof. If C is an induced cycle, then it is the boundary of a face (by Jordan's curve theorem). Notice that we need 2-connectedness for this to hold, as otherwise we could have a subtree hanging inside the cycle.

For the other direction, suppose that C is the boundary of a face. Then, C can not have any "internal chords", as they would be part of the boundary of the face, so we just need to rule out external chords. Suppose that there exist two vertices $x, y \in C$ that are not adjacent in the cycle but are joined by an edge. Let a and b be the two vertices on both sides of x in the cycle C. By 3-connectedness, there must be a path joining a and b which is internally-disjoint from the path $a-x-b$. However, this path can not go inside the cycle (again because the boundary of the face is just C), so it must be on the outside, intersecting the edge $x-y$. Therefore, G is not planar, reaching a contradiction.

In order to see that $G - C$ is connected, let $x, y \in V(G - C)$ be any pair of vertices. We know that in G there are 3 internally-disjoint paths going from x to y (by 3-connectedness). These 3 paths separate the plane into 3 arc-connected components. Notice that every face of G must be confined in one of these components, so by removing the edges of the cycle C we can only affect at most 2 of these paths. Therefore, there is still a path from x to y in $G - C$. □

This theorem tells us that we can characterize the faces of a 3-connected graph just from combinatorial properties of the graph, so they do not depend on the specific plane embedding we choose. In fact, later on we'll see that all plane embeddings of a 3-connected graph are essentially equivalent.

7.2 Kuratowski Theorem

Proposition 7.2.1. *A planar graph G on n vertices has at most $3n-6$ edges, and equality only holds if G is a triangulation (that is, all faces are triangles).*

Proof. Let F be the set of faces of a plane embedding of G, and let $H = (E \cup F, E')$ be the bipartite graph where $ef \in E'$ iff e is incident to face f. Notice that every edge is adjacent to at most 2 faces, and every face is adjacent to at least 3 edges.

Therefore, by double counting, we get that $|E'| \leq 2|E|$ and $|E'| \geq 3|F|$, so $2|E| \geq 3|F|$. Plugging this into Euler's formula, we get the bound we wanted to prove:

$$2 = |V| - |E| + |F| \leq |V| - \frac{1}{3}|E|$$
$$|E| \leq 3|V| - 6$$

Equality holds if every face is adjacent to exactly 3 edges, that is, if every face is a triangle. □

Corollary 7.2.1. *The graph K_5 is not planar.*

Proof. The graph K_5 has 5 vertices and 10 edges, and $3 \cdot 5 - 6 = 9 < 10$. □

Proposition 7.2.2. *A planar bipartite graph G with n vertices has $m \leq 2n - 4$, and equality only holds if G is a quadrangulation (all faces are quadrilateral shapes).*

Corollary 7.2.2. *The graph $K_{3,3}$ is not planar.*

Proof. The graph $K_{3,3}$ has 9 edges and 6 vertices, but $2 * 6 - 4 = 8 < 9$. □

These two corollaries are important, because the graphs K_5 and $K_{3,3}$ allow us to characterize planarity. However, we must first define a weaker notion of what it means for a graph to contain another graph.

Definition 7.2.1 (Subdivision)**.** A *subdivision* of an edge $xy \in E(G)$ is the replacement of e by a path joining x and y (such that all internal vertices are of degree 2, so they are not connected to anything else).

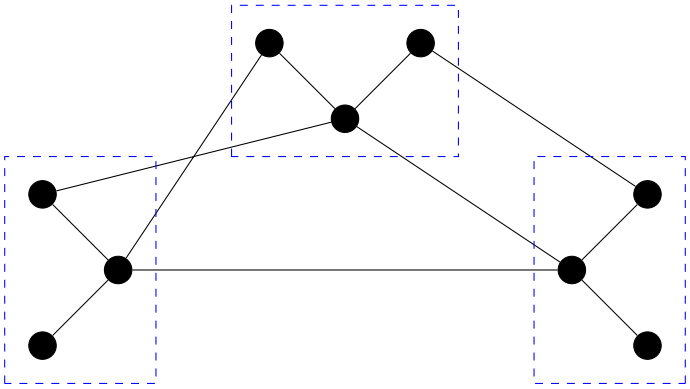
We say that H is a *subdivision* of graph G if it can be obtained by the subdivision of some of its edges.

Definition 7.2.2 (Topological minor)**.** We say that graph H is a *topological minor* of G if G contains a subdivision of H as a subgraph. In that case, we write $H \leq_T G$.

Remark. The previous notation for topological minors comes from the fact that $\leq_T$ defines a partial order in the class of graphs. It is interesting to see that planarity is "inherited" by this relation, so if G is planar, and $H \leq_T G$, then H is planar.

Definition 7.2.3 (Minor)**.** A graph H is a *minor* of G if G contains a subgraph from which H can be obtained by the contraction of some edges. In that case we write $H \leq G$.

Example 7.2.1. The triangle K_3 is a minor of the following graph, as we can contract all the edges in the dotted parts, leaving only K_3.



Remark. The relation $\leq$ defines a partial quasiorder in the class of graphs, which is a refinement of $\leq_T$. Again, it can be seen that planarity is inherited by minors, so $H \leq G$ and G planar implies that H is planar.

Theorem 7.2.1 (Kuratowski)**.** *A graph G is planar if, and only if, it does not contain a subdivision of K_5 or $K_{3,3}$ (that is, $K_5 \not\leq_T G$ and $K_{3,3} \not\leq_T G$).*

Remark. This theorem is an instance of a more general theorem called Graph Minor Theorem, that states that every minor-closed class of graphs can be defined as the set of graphs that do not contain a certain finite set of minors.

Proof. It is clear that if $K_5 \leq_T G$ or $K_{3,3} \leq_T G$, then G can not be planar (otherwise all their topological minors would also be planar). Hence, we just have to prove that if a graph does not contain K_5 and $K_{3,3}$ as topological minors, then it is planar. We will first prove the following proposition:

Proposition 7.2.3. *Let G be a 3-connected graph such that $K_5 \not\leq_T G$ and $K_{3,3} \not\leq_T G$. Then G admits a convex plane embedding (an embedding where all faces are convex polygons).*

Proof. We will prove it by induction on $n = |V(G)|$. The base case is $n = 4$, and it is clear that K_4 (the only 3-connected graph with 4 vertices) admits an embedding where all faces are

convex. Note that we are also considering the exterior face here. In order to do so, we can consider embeddings on a sphere, instead of in the plane, in which the outer face can also be convex.

For $n > 4$, we take an edge $e = xy$ such that G/e is also 3-connected (we know it exists by previous results). As $G/e \leq G$, we know that it does not contain K_5 or $K_{3,3}$ as topological minors. Therefore, by the induction hypothesis we know that G/e admits a convex plane embedding.

Let v_{xy} be the vertex resulting from the contraction of edge xy. $G/e - v_{xy}$ is 2-connected, so all faces are bounded by cycles. Let f be the face of $G/e - v_{xy}$ containing v_{xy} in its interior. Decontracting the edge, we get x and y inside that face. Let $x_1, \ldots, x_k$ be the neighbours of x (in clockwise order). We will now consider 4 cases.

1. $N(y) \subseteq \{x\} \cap P_{x_i x_{i+1}}$ If all neigbours of y are contained in the path between two neighbours of x, then by placing x in the position of v_{xy} and inserting y in the triangle formed by x, x_i and x_{i+1}, we obtain a convex embedding of G.

2. y has 3 neigbours x_i, x_j and x_k in common with x Then, we would have $K_5 \leq_T G$, as vertices x_i, x_j and x_k are adjacent via paths on the cycle and x and y are adjacent to all of them. Therefore, this case is not possible.

3. y is adjacent to x_i and x_j, which are not consecutive (otherwise we are in case 1) Then we can build a $K_{3,3}$ with vertices x, x_i, x_j on one side and vertices y, x_{i+1}, x_{j+1} on the other side. Therefore, $K_{3,3} \leq_T G$, reaching once again a contradiction.

4. y has one neighbour z in the interior of path $x_i x_{i+1}$ and another z' in $x_j x_{j+1}$, with $i \neq j$

   Again, we find that $K_{3,3}$ is a topological minor of G, taking vertices x, z, z' on one side and vertices y, x_i, x_{i+1} on the other side. Note that the proof also works if $z' = x_j$, so this also covers the case when y is adjacent to a vertex in the interior of a path and a vertex in $N(x)$.

   There are no more cases because, due to the 3-connectivity, y needs at least 3 neigbours.

□

Note that it is enough to prove the statement for G edge-maximal planar (no edge can be added while keeping G planar). That's because if the theorem is true for edge-maximal planar graphs, then removing a few edges will not create a subdivision of K_5 or $K_{3,3}$ out of nowhere. That allows us to use the following lemma:

Lemma 7.2.1. *If G is an edge-maximal graph such that K_5, $K_{3,3} \not\leq_T G$, then G is either 3-connected or K_n for $n \leq 3$.*

Proof. We will prove it by induction on $n = |V(G)|$. If $n = 4$, it can not have K_5 or $K_{3,3}$ as topological minors, so the only edge-maximal graph with respect to this condition is K_4, and the lemma holds.

For $n > 4$, let S be a minimum separating set of G. We need to prove that $|S| \geq 3$, so we will consider $|S| < 3$ and reach a contradiction. If $|S| = 0$, that means G is disconnected, but then G

can not be edge-maximal (in fact, we can add any edge in between two connected components without creating K_5 or $K_{3,3}$, as neither of these graphs has a bridge).

If $|S| = 1$, let $u \in S$. Let $G = G_1 \cup \{u\} \cup G_2$, where G_1 and G_2 are the two connected components of $G \setminus \{u\}$ (if it has more than 2 connected components, the argument works too). Let $x \in G_1$ be any vertex adjacent to u and $y \in G_2$ adjacent to u. Then it can be seen that $G + xy$ can not have K_5 or $K_{3,3}$ as minors, so G is non-maximal.

Remark. In order to prove that, we can use that if Y is a subdivision of a 3-connected graph X, then any 2 "branching vertices" are joined by 3 independent paths (where a branching vertex is a vertex of Y that after reducing the paths corresponds to a vertex of the minor).

Using this remark, we see that all branching vertices must be fully contained in G_1 or G_2 (as there are only two disjoint paths that cross from G_1 to G_2), and then any path of a topological minor in $G + xy$ using the edge xy must come back through u, so we can replace it by the edge xu or yu, obtaining the same topological minor in G.

The last case to check is $|S| = 2$. Let $u, v \in S$. If $uv \notin E(G)$, then G would not be edge-maximal, as $G + uv$ does not contain K_5 or $K_{3,3}$ as topological minors. Again, that's because all branching vertices must be in one of the two sides, and if a path uses the edge uv, then it can be replaced by $u - x - y - v$, where x and y are some neighbours of u and v in the other connected component (notice that if $x = y$ the same argument still holds, and if x did not exist, then $\{v\}$ alone would be a separator, contradicting the assumption that $|S| = 2$).

Therefore, we just need to check the case with $uv \in E(G)$. In this case, it can be seen that both G_1 and G_2 are edge-maximal (with respect to not containing K_5 or $K_{3,3}$ as topological minors).

By induction, G_1 and G_2 are either 3-connected or K_n with $n \leq 3$. By the previous proposition, both G_1 and G_2 admit a convex plane embedding. Recall that we can consider embeddings on the plane as embeddings on the sphere (by the stereographic projection for example). Therefore, we can take any face as the exterior face. We will take convex plane embeddings of G_1 and G_2 such that uv belongs to the boundary of the exterior face in both of them.

Let x be the neighbour of u in the boundary of the exterior face of graph G_1, and let y be the equivalent in graph G_2. Notice that we can join x and y with an edge that is contained in the exterior face, so $G + xy$ is still planar. Therefore, it can not have K_5 or $K_{3,3}$ as topological minors (we have already proved this direction), so G was not edge-maximal with respect to that condition. □

Using the previous lemma, the proof is now trivial. Let G be a graph such that $K_5 \not\leq_T G$ and $K_{3,3} \not\leq_T G$. If G is not edge-maximal, we add edges until it is. Then, by 7.2.1 it is either 3-connected or K_n for $n \leq 3$. All K_n for $n \geq 3$ are planar, and by 7.2.3 it admits a plane embedding. Then, removing the edges we added, we get a plane embedding of G, so G is planar. □

We can extend Kuratowski's theorem to ordinary minors:

Theorem 7.2.2 (Wagner)**.** *A graph G is planar if, and only if, $K_5, K_{3,3} \not\leq G$*

Proof. If G is planar, then $K_5, K_{3,3} \not\leq_T G$, so $K_5, K_{3,3} \not\leq G$. We will now prove the opposite direction. We will do it by proving that $K_{3,3} \leq G \implies K_{3,3} \leq_T G$ and $K_5 \leq G \implies K_5 \leq_T G$

or $K_{3,3} \leq_T G$.

- $\boxed{K_{3,3} \leq G \implies K_{3,3} \leq_T G}$

  All vertices in $K_{3,3}$ have degree 3, so this follows directly from the following lemma:

  Lemma 7.2.2. *Let H be a graph with maximum degree $\Delta(H) \leq 3$. Then, $H \leq G \implies H \leq_T G$*

  Proof. Suppose $H \leq G$. Then, there exists a vertex partition of G $X_1, \ldots, X_h \subseteq V(G)$ with $h = |H|$ and such that each $G[X_i]$ is connected and contracts to a vertex in H.

  Let G' be a minimal subgraph of G with respect to the condition that $H \leq G'$. Then, $G[X_i]$ is a tree (otherwise we can remove an edge) and it has at most 3 leaves (otherwise there exists a leaf not connected to another X_j, since $\Delta(H) \leq 3$, and then this leaf can be removed too).

  Depending on whether there's 1, 2 or 3 vertices in X_i connected to the rest of G, we can reduce the tree to one of the following topological minors, where the vertices in X_i are the ones inside the blue rectangle. By contracting the red vertices, we see that the first graph is a topological minor of the other two, so we can reduce every X_i down to one vertex, getting H as a topological minor of G.

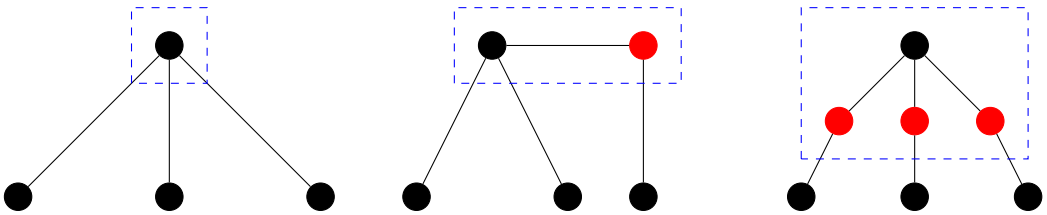
  

  Figure 7.1

  □

- $\boxed{K_5 \leq G \implies K_5 \leq_T G \text{ or } K_{3,3} \leq_T G}$

  □

8 Colorings

8.1

Definition 8.1.1 (Coloring)**.** A *vertex-k-coloring* of a graph $G = (V, E)$ is a map $\chi : V \longrightarrow [k]$. We say that the coloring is *proper* if $\chi(x) \neq \chi(y)$ for every edge $xy \in E(G)$.

Definition 8.1.2 (Chromatic number)**.** Let G be a graph. The *chromatic number* $\chi(G)$ is the minimum k such that G admits a proper k-coloring.

Example 8.1.1.

1. The chromatic number of the complete graph is $\chi(K_n) = n$, as we need to paint each vertex with a different color.
2. The chromatic number of a cycle with n vertices depends on the parity of n:
$$\chi(C_n) = \begin{cases} 2, & n \text{ even} \\ 3, & n \text{ odd} \end{cases}$$
3. Falta

Computing the chromatic number of a general graph is a very difficult task, so we will try to find bounds for it. The following proposition gives two elementary lower bounds which, however, are not always close to the real value.

Proposition 8.1.1. *Let $\alpha(G)$ be the stability number of G (the maximum size of a subgraph with no edges) and let $\omega(G)$ be the clique number of G (the maximum size of a subgraph that is complete). Then,*
$$\chi(G) \geq \max\left\{\omega(G), \frac{n}{\alpha(G)}\right\}$$

Proof. Falta, i també falta discussió de quan són o no tight □

The following theorem gives a tighter bound:

Theorem 8.1.1 (Szekeres-Wilf)**.** $\chi(G) \leq \max_{H \subseteq G} \delta(H) + 1$

Proof. The proof is based on ordering the vertices in such a way that the greedy algorithm always produces a proper coloring with the desired number of colours.
Falta □

The greedy algorithm that appeared in the proof can sometimes give a very bad upper bound for the chromatic number, but it can be seen that for every graph there exists some ordering of the vertices in which the greedy algorithm gives a colouring with the minimum number of colours.

Corollary 8.1.1. *Let $\Delta(G)$ be the maximum degree of a vertex in G. Then, $\chi(G) \leq \Delta(G) + 1$.*

Proof. Let H be subgraph of G. The degree of a vertex in H is smaller or equal than the degree of the vertex in G, so $\max_{H \subseteq G} \delta(H) \leq \Delta(G)$. □

In fact, this bound can be reduced by one (except in two extremal cases):

Theorem 8.1.2 (Brooks)**.** *Let G be a connected graph. If $G \neq K_n, C_{2m+1}$, then $\chi(G) \leq \Delta(G)$.*

Remark. Notice that we could assume G not connected and then ask for none of its connected components to be K_n or C_{2m+1}.

Proof. Let $\Delta := \Delta(G)$. We may assume that the graph G is Δ-regular, and $\Delta \leq 3$. That's because we can always add some vertices and edges in order to produce a Δ-regular graph, and this addition might make $\chi(G)$ get bigger, but never smaller. We restrict oursleves to $\Delta \geq 3$, because if $\Delta = 2$ then the graph is a collection of cycles, which have $\chi(G) = 2$ if they are all even.

We will divide the prove in cases:

1. G is 3-connected Choose a vertex x and two of its neighbours x_1, x_2, such that $x_1 \neq x_2$. (Notice that there always exists some choice of x with two non-incident neighbours, as $G \neq K_n$.) We know that $G - \{x_1, x_2\}$ is connected. Therefore, we define an ordering of the vertices, starting at $x_n := x$, and for each $i \in \{3, \ldots, n-1\}$ choosing a vertex x_i such that it has a neighbour in $\{x_{i+1}, \ldots, x_n\}$. Notice that there always exists some choice due to the fact that the graph is connected.

   Now we use the greedy algorithm in this order. For every $i \in \{1, \ldots, n-1\}$, we know that it has a neighbour to the right, so it has at most $\Delta - 1$ edges to the left. Therefore, the greedy algorithm will color the first $n-1$ vertices with not more than Δ colours. How to colour the last vertex? We know that $x_n = x$ is adjacent to x_1 and x_2, which are not neighbours, so the algorithm will have colored them both with colour 1. Then, the Δ neighbours of x_n can have at most $\Delta - 1$ different colours, so we can colour x_n with one of the remaining colours.

2. G is 2-connected We pick a separating set $\{x, y\}$, and consider the graph $G - \{y\}$, which has to be connected. Thus, $G - \{y\}$ admits a decomposition into a tree in which every component is a 2-connected subgraph.

   This tree has more than 1 vertex (otherwise $\{x, y\}$ is not a separator), so we can take two different leaves. Notice that y has to be connected to some vertex in every leaf component. Then, choose x_1 and x_2 from two different leaves such that both were connected to y in G. These vertices are not adjacent (why?).

   Therefore, we have found a vertex x connected to x_1 and x_2 such that $G - \{x_1, x_2\}$ is still connected and x_1 and x_2 are not adjacent. Then, we can apply the procedure from case 1, obtaining a coloring with no more than Δ colors.

3. G is 1-connected We choose a vertex v that separates G, and break the graph by that point (duplicating v). Then we can colour each piece independently and join them again (permuting the colours of one of the pieces so that both copies of v have the same colour). Since $\Delta(H) \leq \Delta(G)$ for any $H \subseteq G$, by induction the colouring on each of the two pieces will have no more than $\Delta(G)$ colours, so the union will not have more than $\Delta(G)$ colours either.

   There could be a problem with this argument if one of the two pieces was a complete graph of a cycle (then we can not apply the theorem inductively), but that's not possible. That's because we can assume that $\Delta \geq 3$, so none of the pieces can be a cycle, and the graph is Δ-regular, so if one of the pieces was a $K_{\Delta+1}$, then v could have no neighbours in the other side.

□

8.2 Coloring planar graphs

Theorem 8.2.1 (4 color theorem)**.** *If G is planar, then $\chi(G) \leq 4$.*

The only known proof is based on dividing the theorem in a lot of cases and checking each one with the aid of a computer. We will not discuss this proof here, and we will focus on a weaker result:

Theorem 8.2.2 (Heawood)**.** *If G is planar, then $\chi(G) \leq 5$.*

Proof. We will prove it by induction on n. We can assume that G is maximally planar (that is, a triangulation of the sphere), since the addition of edges can not decrease $\chi(G)$. We will also assume that $n > 4$ (the cases $n = 3, 4$ can be checked by hand).

Suppose $\delta(G) \leq 4$. Then, let v be a vertex with $\deg(v) \leq 4$. Removing the vertex from the graph, we obtain a graph with $n - 1$ vertices, which by the inductive hypothesis is 5-colorable. Therefore, $\chi(G) \leq 5$, since we can extend the previous colouring to a colouring of G by painting v with one of the colours not appearing in its neighbours (it has only 4 neighbours at most).

Therefore, we can assume $\delta(G) \geq 5$. Let v be an arbitrary vertex. Let's take a 5-colouring of $G - v$, which exists by the inductive hypothesis. Notice that the neighbours of v must be painted with the 5 colours (otherwise we paint v with the missing colour).

Let x_i be a neighbour of v painted with colour i, and let H_{13} be the subgraph induced by vertices colored 1 and 3. We will suppose the colours are ordered in such a way that the x_i are ordered when we go around v.

1. x_1 and x_3 are in different components of H_{13}

   Then we can interchange the colours in the connected component of x_1, so that $\chi(x_1) = 3$, and then we can take $\chi(v) = 1$.

2. x_1 and x_3 are in the same connected component

   There is a path in H_{13} joining x_1 and x_3. This path separates x_2 and x_4, so every path joining x_2 and x_4 in $G - v$ must have a vertex with colour 1 or 3. Therefore, x_2 and x_4 are in different components of H_{24}, so we apply case 1.

□

8.3 Planar graphs with low chromatic number

Proposition 8.3.1. *Let G be a planar graph. Then, $\chi(G) = 2$ if, and only if, all the faces have an even number of edges in their boundary.*

Proof. It is one of the exercises seen in class. □

Theorem 8.3.1 (Heawood)**.** *A maximal planar graph has $\chi(G) = 3$ if, and only if, G is Eulerian (ie. all the degrees are even).*

Proof. Suppose G contains a vertex v of odd degree. Since G is a triangulation, the neighbours of v are connected forming a wheel (a cycle together with a central vertex connected to everything). Since $\chi(C_{2m+1}) = 3$, we need at least 4 colours to colour an odd wheel, reaching a contradiction.

For the opposite direction, we will prove a stronger statement:

Lemma 8.3.1. *If G is a near-triangulation (all faces but the external face are triangular) and all inner vertices (not adjacent with the external face) have even degree, then $\chi(G) \leq 3$.*

Proof. We will use induction on the number of inner faces. Let $e = xy \in E(G)$ in the boundary of the external face. Let z be the third vertex of the triangular face containing e.

1. z is also in the external face boundary Then, y has degree 2. Then we can remove y, keeping the graph a near-triangulation. By the inductive hypothesis, $\chi(G - y) \leq 3$, and y only has 2 neighbours, so $\chi(G) \leq 3$.

2. z is an inner vertex By induction, $G - e$ admits a 3-coloring. Since z has even degree by hypothesis, x and y have to be colored with different colors (all the inner faces are triangles, so the neighbours of z form an even cycle, with x and y adjacent). Therefore, the coloring of $G - e$ is still proper in G.

□

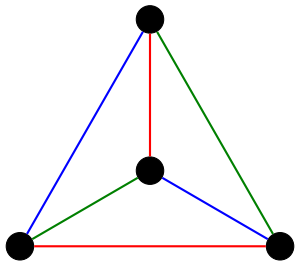
□

8.4 Edge-coloring

Definition 8.4.1 (Edge-coloring)**.** An *edge-coloring* is a map $\chi : E(G) \longrightarrow [k]$ for some integer $k \geq 1$. We say that the edge-coloring is *proper* if $\chi(e) \neq \chi(e')$ for all incident e, e'.

Definition 8.4.2 (Edge chromatic number)**.** The *edge chromatic number* is the minimum k such that there exists a proper coloring $\chi : E(G) \longrightarrow [k]$. We denote it by $\chi'(G)$.

Example 8.4.1. The edge chromatic number of K_4 is $\chi'(K_4) = 3$, as the following coloration shows:



Remark. Notice that,

- $\chi'(G) \geq \Delta(G)$
- The collection of edges painted with a colour in some edge-coloring forms a matching, as they can not be pair-wise incident.
- $\chi'(G) = \chi(L(G))$, where $L(G)$ represents the line graph (where vertices are edges of G and edges are vertices of G).

The following theorem strongly restricts the value of the edge chromatic number (in contrast to the usual chromatic number).

Theorem 8.4.1 (Vizing)**.** *The edge chromatic number is bounded by*

$$\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$$

Remark. It is easy to see that the two bounds can be achieved, taking the class of cycles. Since $L(C_n) = C_n$, $\chi'(C_n) = \chi(C_n) = 2$ or 3, depending on the parity of n. Thus, for odd cycles $\chi'(C_n) = 3 = \Delta(C_n) + 1$ and for even cycles $\chi'(C_n) = 2 = \Delta(C_n)$.

Proof. We have already seen the lower bound, so we will prove the upper bound. We fix a value for Δ. Then, we will use induction on $m = |E(G)|$, restricting ourselves to the class of graphs with maximum degree $\Delta(G) = \Delta$.

If $m = \Delta$, then the only possible graph is a star with Δ leaves together with some isolated vertices. Then, $\chi'(G) = \chi'(K_{1,\Delta}) = \Delta \leq \Delta + 1$.

If $m > \Delta$, let x_0 be a vertex of degree Δ, and let $e = x_0y_0 \in E(G)$. By induction, $G-e$ admits a $\Delta+1$-edge-colouring. Let χ be such a colouring. Then, for every vertex x, let $\beta(x)$ be the set of colours not used in edges incident to x. Notice that $\beta(x) \neq \emptyset$ for every x, as $\Delta(G) = \Delta < \Delta+1$.

If $\beta(x_0) \cap \beta(y_0) \neq \emptyset$, then χ can be extended to G by choosing a colour in the intersection. Therefore, we may assume that $\beta(x_0) \cap \beta(y_0) = \emptyset$. Now, we will build a sequence $y_0, y_1, \ldots, y_k$. We start by choosing a colour $c_0 \in \beta(y_0)$, and choosing y_1 to be a neigbour of x_0 such that $\chi(x_0y_1) = c_0$. We know that such an y_1 exists, as otherwise $c_0 \in \beta(x_0) \cap \beta(y_0)$.

If $\beta(x_0) \cap \beta(y_1) \neq \emptyset$, we recolor x_0y_1 with some $\alpha \in \beta(x_0) \cap \beta(y_1)$ and now $c_0 \in \beta(x_0)$, so we can color the edge x_0y_0 with c_0. Otherwise, we repeat the same strategy, picking a $c_1 \in \beta(y_1)$ and choosing a y_2 neighbour of x_0 such that x_0y_2 is painted with colour c_1. We iterate this process until there exists no $c_k \in \beta(y_k)$ that has not been picked before.

By maximality of the sequence, either we have stopped because $\beta(x_0) \cap \beta(y_{k+1}) \neq \emptyset$ (in which case we can color x_0y_{k+1} with some $\alpha \in \beta(x_0) \cap \beta(y_{k+1})$, x_0y_k with c_k, $\ldots$, x_0y_1 with c_1 and x_0y_0 with c_0), or we have stopped because $c_k = c_j$ for some $j < k$. In that case, we set $\chi(x_0y_i) = c_i$ for $0 \leq i \leq j$, just as before, and pick some $\alpha \in \beta(x_0)$.

We now consider the subgraph $H \subseteq G$ induced by colours α and c_j. Since no edges with the same colour are incident, $\Delta(H) \leq 2$, so the connected components of H are either paths or cycles. Notice that, under the new coloring, $d_H(y_k) = d_H(y_{j+1}) = d_H(x_0) = 1$.

A path has at most 2 vertices of degree 1, so x_0, y_{j+1} and y_k have to be in different connected components of H. Then, x_0, y_k or x_0, y_{j+1} are in different connected components. If x_0 and y_{j+1} are in different connected components, we switch c_j and α in the connected component containing y_{j+1}, and after this change we can paint x_0y_{j+1} with color α.

Otherwise, if x_0 and y_k are in different connected components, we again switch c_j and α in the component containing y_k and paint the edge x_0y_k with colour α. Now we can push back the colours, setting $\chi(x_0y_i) = c_i$ for $j+1 \leq i \leq k-1$, and we have coloured all the edges. □

8.5 List coloring

So far we have defined colorings in graphs as functions from $V(G)$ (or $E(G)$) to $[k]$, where the image of each vertex represents its colour. However, we might also consider colorings in which each vertex also has k available colours, but these colours migh not always be the same. This is what we call a list coloring.

Definition 8.5.1 (List assignment)**.** Let G be a graph, and let V be its vertex set. Then, we define a *list assignment* of G as a function that assigns a finite subset of the natural numbers to each vertex:

$$\begin{aligned} L : V &\longrightarrow 2^{[n]} \\ v &\longmapsto L(v) \subseteq \mathbb{N} \end{aligned}$$

where $n \in \mathbb{N}$.

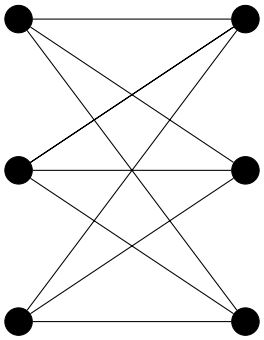
Definition 8.5.2 (list coloring)**.** Let L be a list assignment on graph G. We define a *list coloring* or *L-coloring* of G as a proper coloring χ such that $\chi(v) \in L(v)$ for any $v \in V(G)$.

Definition 8.5.3 (List chromatic number)**.** Let G be a graph together with a list assignment L. We define the *list chromatic number* of G as

$$\chi_L(G) := \min\left\{k : \forall L : V \longrightarrow 2^{\mathbb{N}} \text{ st } (v) \geq k, \ \ G \text{ admits an } L\text{-coloring}\right\}$$

In particular, taking $L : V \longrightarrow 2^{\mathbb{N}}$ to be $L(v) = [k]$, we see that $\chi_L(G) \geq \chi(G)$. It might seem at first that these two numbers are always equal, since intuitively one might think that the most restrictive list assignment is that in which all vertices share the same colour. However, the following example shows that this is not the case.

Example 8.5.1. Let us take $G = K_{3,3}$. We know that all bipartite graphs are 2-colorable, so $\chi(G) = 2$. However, as the following list assignment shows, $\chi_L(G) > 2$, since it is impossible to pick a proper coloring for this assignment. Falta afegir assignment



While the 4-colour theorem is such a complicated problem in usual vertex-coloring, it is quite easy to prove a tight bound on the list chromatic number of planar graphs:

Theorem 8.5.1 (Thomassen)**.** *If G is planar, then $\chi_L(G) \leq 5$, and the bound is tight.*

Proof. We will prove the stronger statement that for every near-triangulation G and for every list assignment L satisfying

- $|L(v)| \geq 5$ for every inner vertex v
- $|L(v)| \geq 3$ for every vertex in the boundary except two certain vertices x,y joined by an edge
- $|L(x)| = |L(y)| = 1$ and $L(x) \neq L(y)$

then G admits an L-coloring. □

Falten els apunts del dilluns 20 de Desembre

9 Extremal Graph Theory

Theorem 9.0.1 (Mantel)**.** *Let G be a triangle-free graph. Then,*

$$|E(G)| \leq \frac{|V(G)|^2}{4}$$

Proof. Let S be a maximum independent set of S. Since every edge has an endpoint outside of S, we have that the number of edges is bounded by the sum of degrees in $V(G) \setminus S$:

$$m \leq \sum_{x \in V \setminus S} d(x)$$

Now notice that, since the graph has no triangles, $d(x) \leq |S|$ for any $x \in V(G)$ (otherwise, the neighbours of x would form an independent set larger than S). Therefore,

$$\sum_{x \in V \setminus S} d(x) \leq \sum_{x \in V \setminus S} |S| = |S| \cdot |V \setminus S| \leq \left(\frac{|S| + |V \setminus S|}{2} \right)^2 = \frac{n^2}{4}$$

where the last inequality is a direct application of the AM-GM inequality to $|S|$ and $|V \setminus S|$. □

Remark. Suppose n is even. In the previous proof, we know that equality holds in AM-GM iff $|S| = |V \setminus S|$. Therefore, for a triangle-free graph G to have $n^2/4$ edges, we would need $|S| = n/2$ and $d(x) = |S| = n/2$ for every $x \in V \setminus S$. Then, the graph is $K_{n/2,n/2}$.

Similarly, if n is odd, one can check that the only graph that achieves the upper bound on edges is $K_{(n-1)/2,(n+1)/2}$.

This theorem was the starting point for the theory of extremal graphs. In extremal combinatorics, we look for the maximum value of a certain quantity (in this case edges) in a class of objects (in this case triangle-free graphs), and we aim to characterize the objects that maximize or minimize this quantity.

Definition 9.0.1 (Extremal function)**.** Let H be a fixed graph. We define the *extremal function* of H as

$$\mathrm{ex}(n, H) := \max\left\{ |E(G)| \,:\, G \text{ is } H\text{-free and } |V(G)| = n \right\}$$

Example 9.0.1. Mantel's theorem tells us that $\mathrm{ex}(n, K_3) = \lfloor n^2/4 \rfloor$.

Theorem 9.0.2 (Turán)**.** *For any integer $r \geq 2$, $\mathrm{ex}(n, K_{r+1})$ is the Turán number $t_{n,r} = |E(T_{n,r})|$, and the extremal graph is the Turán graph $T_{n,r}$, which is the complete r-partite graph with parts of size $\lfloor n/r \rfloor$ or $\lceil n/r \rceil$.*

Proof. We will use the following lemma:

Lemma 9.0.1. *If G is extremal for K_{r+1}, then $x \not\sim y$ and $x \not\sim z$ implies that $y \not\sim z$.*

Proof. Suppose $yz \in E(G)$. We will consider the following cases:

1. $\boxed{d(x) < d(y))}$ We delete x and duplicate y, creating vertex y'. The number of vertices of the new graph G' is still n, but the number of edges is $m' = m - d(x) + d(y) > m$.

   This new graph G' has to be triangle-free, as any copy of K_{r+1} can only contain either y or y' (because they are not neighbours), so it also exists in G. Therefore, G is not the extremal graph, reaching a contradiction.

   Notice that the same argument holds if $d(x) < d(z)$.

2. $\boxed{d(x) \geq d(y), d(z)}$ We delete y and z and add two copies of x, called x' and x''. We obtain a graph with the same number of vertices and $m' = m-(d(y)+d(z)-1)+2d(x) > m$ edges. Therefore, we just need to prove that G' is K_{r+1}-free in order to obtain a contradiction.

   But that can be done by the same argument as before: if G' contains a copy of K_{r+1}, then this K_{r+1} can only contain one of x, x' and x'' (since they are not neighbours), so it will also be present in the original graph G.

□

The previous lemma tells us that non-adjacency is transitive. Since it is trivially reflexive and symmetric, we know that $\not\sim$ is an equivalence relation in $V(G)$, so G can be split in equivalence classes with respect to that relation (partition of vertices such that two vertices from the same class are not neighbours and such that two vertices from different classes are always neighbours).

Therefore, G is complete-multipartite. That means that the number of classes is at most r (otherwise taking a vertex from each class we would get a K_{r+1}). Let $n_1, \ldots, n_r$ be the cardinalities of the classes (notice that we allow $n_i = 0$ for some indices i). The number of edges of G is

$$m = \sum_{i=1}^{r} n_i(n - n_i) = n^2 - \sum_{i=1}^{r} n_i^2$$

The maximum number of edges is obtained by minimizing $\sum_{i=1}^{r} n_i^2$ subject to $n_1 + \cdots + n_r = n$, and it can be seen that the optimal solution has some $n_i = \lfloor n/r \rfloor$ ans some others equal to $\lceil n/r \rceil$ (the number of each type depends on the value of $n \mod r$). □

Remark. There is a similar result obtained by replacing K_{r+1} with any other graph with $\chi(G) = r + 1$, except in this case the result only holds asymptotically.