Discrete Mathematics

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Introduction

Mon 22 Feb

1 Counting

1.1 Finite sets

Let A be a finite set. We denote by $|A|$ the cardinality of A.

Definition 1 (First Numbers)
We denote by $[n]$ the set of n first natural numbers.

1.2 Bijections

Theorème 1
If there exists a bijection between finite sets A and B then $|A| = |B|$.

1.3 Operations with finite sets

— union
— intersection
— product
— exponentiation
— quotient

Definition 2 (Cartesion product)

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

Theorème 2

$$|A \times B| = |A||B|$$

Definition 3 (Disjoint union)
Define

$$A \sqcup B = A \times \{0\} \cup B \times \{1\}$$

Theorème 3

$$|A \sqcup B| = |A| + |B|$$

Definition 4 (Exponential object)

$$A^B = \{f | f \text{ is a function from } A \text{ to } B\}$$

Theorème 4

$$|A^B| = |A|^{|B|}$$

Definition 5 (Binomial coefficient)
A binomial coefficient $\binom{n}{k}$ *is the number of ways in which one can choose* k *objects out of* n *distinct objects assuming order doesn't matter.*

Proposition 5

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

Proposition 6
The following identities hold :

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

2. $\binom{n}{k}$ *is the* k*-th element in the* n*-th line of Pascal's triangle.*

Preuve
Each subset of $[n+1]$ *either contains* $n+1$ *or not.*
Number of $(k+1)$*-element subsets containing* $n+1$ *is* $\binom{n}{k}$
Number of $(k+1)$*-element subsets not containing* $n+1$ *is* $\binom{n}{k+1}$ □

Proposition 7
The number of subsets of an n*-element set is* 2^n*, since we have*

$$2^n = \sum \binom{n}{i}$$

Proposition 8
The number of subsets of even cardinality is the same as even cardinality : 2^{n-1}

Preuve
Consider

$$\phi : 2^{[n]} \to 2^{[n]}$$

defined by

$$\phi(A) = A\Delta\{1\} = \begin{cases} A \setminus \{1\}, & \text{if } 1 \in A \\ A \cup \{1\}, & \text{otherwise} \end{cases}$$

□

The cardinality of subsets A and $\phi(A)$ always have different parity.
Since $\phi \circ \phi = \mathrm{Id}$ we deduce that ϕ is a bijection between the set of odd and even subsets is the same.

Theorème 9

$$(1+x)^n = \sum \binom{n}{i} x^i$$

Preuve
In lecture notes. □

Proposition 10
Assume we have k identical objects and n different persons. Then ne number of ways in which one can distribute this k objects among the n persons equals

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

Equivalently, it is the number of solutions of the equation $x_1 + ... + x_n = k$

Preuve
Let $\mathcal{A}$ be the set of all solutions of the equation. Let $\mathcal{B}$ be the set of all subsets of cardinality $n-1$ in $k+n-1$.
we construct a bijection $\psi : \mathcal{A} \to \mathcal{B}$ in the following way

$$A = (x_1, \ldots, x_n) \mapsto B = \{x_1 + 1, x_1 + x_2 + 2 \ldots\}$$

It suffices to show that ψ is invertible. Let $B \in \mathcal{B}$. Suppose that $b_1 \ldots, b_{n-1}$ are the elements of B, ordered. Then the preimage is an n-tuple of integers $(x_1, \ldots)$ defined by

$$\begin{aligned} x_1 &= b_1 - 1 \\ x_i &= b_i - b_{i-1} \\ x_n &= k + n - 1 - b_{n-1} \end{aligned}$$

□

It is easy to see from these equations that the x_i are non-negative and their sums yield k.

Lecture 2: factorials and birthday paradox

Sat 27 Feb

Theorème 11 (Stirling's formula)

$$n! \ \sqrt{2\pi n} n^n e^{-n}$$

meaning the ration goes to 1.

Preuve

Euler's integral for $n!$ gives

$$n! = \int_0^\infty x^n e^{-x} dx$$

This is proven by induction on n.
The base case $n = 0$ simply gives 1.
For the integration step, we integrate by parts, giving

$$\int_0^\infty x^n e^{-x} = \int_0^\infty e^{-x} \frac{d}{dx} x^n dx$$

To prove Stirlings formula, we take

$$xt^n e^{-x} = \exp(n \log x - x)$$

We now taylor expand around the maximum, this yields

$$n \log x - x = n \log n - n - \frac{1}{2n}(x-n)^2 + \dots$$

□

integrating this gives the desired formula.

Lecture 3: Inclusion-Exclusion and Induction

Sat 06 Mar

Let A, B be two sets, we want to compute $|A \cup B| = |A| + |B| - |A \cap B|$. What happens if we have n sets $A_1, \dots, A_n$.

Theorème 12 (Inclusion-Exclusion Formula)
Let $A_1, \dots, A_n$ be finite sets, then

$$|\bigcup A_i| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \dots$$

Let $B_1, \dots, B_m$ and $w_1 \dots, w_m$, then

$$\sum_i w_i |B_i| = \sum_i \sum_{b \in B_i} w_i = \sum_{b \in B} \sum_{indices\ i\ such\ that\ b \in B_i} w_i$$

where $B = \bigcup B_i$

Lecture 4: Combinatorial applications of polynomials and generating series

Sun 14 Mar

We note that arithmetic operations with finite sets have similarities.

$$(a+b)\cdot c = a\cdot c + b\cdot c$$

$$(A\cup B)\cap C = A\cap C \cup B\cap C$$

Exemple

Prove the identity

$$\sum \binom{n}{i}^2 = \binom{2}{n} n$$

Consider

$$(1+x)^n \cdot (1+x)^n = (1+x)^{2n}$$

By computing the coefficients of x^n*, we find the desired equality.*

Theorème 14 (Multinomial theorem)

$$(x_1 + \ldots + x_n)^k = \sum_{i_1,\ldots,\geq 0, i_1+i_2+\ldots=k} \frac{k!}{i_1!\ldots i_n!} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

Preuve

Note that

$$\frac{k!}{i_1!\ldots i_n!}$$

is the number of sequences of length k *from the letters "*$x_1, x_2, \ldots$*" such that* x_j *is used* i_j *times.* □

Definition 6 (Generating series)

Let a_n *be a sequence of complex numbers, then the generating series of this sequence is*

$$a(x) = \sum_{n=0}^{\infty} a_n x^n$$

Definition 7 (Formal power series)

A formal power series is an infinite sum

$$a(x) = \sum a_n x^n$$

where a_n *is a sequence of complex numbers and* x *is a formal variable.*

Proposition 15
Let $a(x) = \sum a_n x^n$ be a formal power series. Suppose that there exists a positive real number K such that $|a_n| < K^n$ for all n. Then the series converges absolutely for all $x \in]-\frac{1}{k}, \frac{1}{k}[$.
Moreover, the function $a(x)$ as derivatives of all orders at 0.

We can add and multiply formal power series.
However, in general, substitution is not well defined

$$a(b(x)) = \sum_{n=0}^{\infty} a_n b(x)^n = \sum_{n=0}^{\infty} a_n (\sum_{m=0}^{\infty} b_m x^m)^n$$

It is only well defined if $b_0 = 0$.
We can also differentiate, resp. integrate formal power series.

Theorème 16 (Generalized binomial theorem)
For every $r \in \mathbb{R}$, we have

$$(1+x)^r = \binom{r}{0} + \binom{r}{1} x \dots$$

where

$$\binom{r}{k} = \frac{r(r-1)\dots(r-k+1)}{k!}$$

Lecture 5: Binary trees

Sat 20 Mar

Definition 8 (Binary Tree)
A binary tree is either empty, or consists of one distinguished vertex called the root, plus an ordered pair of binary trees calle de left subtree and the right subtree.

We denote by b_n the number of binary trees with n vertices. We want to fin a closed formula for b_n The inductive definition yields

$$b_n = b_0 \cdot b_{n-1} + b_1 \cdot b_{n-2} + \dots + b_{n-1} \cdot b_0$$

Consider

$$b(x) = \sum b_n x^n$$

And we use

$$b_n = \sum b_k \cdot b_{n-k-1}$$

Now we use

$$\begin{aligned} b(x) \cdot b(x) &= \sum_{k=0}^{\infty} \left(\sum_{m=0}^{\infty} b_m b_{k-m} \right) x^k \\ &= \frac{1}{x} \left(\sum_{k=1}^{\infty} b_k x^k \right) = \frac{1}{x}(b(x) - b_0) \end{aligned}$$

Hence, $b(x)$ satisfies

$$xb^2(x) - b(x) + 1 = 0$$

Hence

$$b(x) = \frac{1 + \sqrt{1-4x}}{2x} \text{ and } b(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

are solutions.
Note that the first solution is not bounded around 0.
However, the second solution is smooth around 0 because

$$\tilde{b}(x) := \frac{1 - \sqrt{1-4x}}{2x} = \frac{2}{1 + \sqrt{1-4x}}$$

Hence, $\tilde{b}(x)$has derivatives of all orders.
We want to establish the connection between $\tilde{b}$ and b.
Consider the taylor expansion of $\tilde{b}$

$$\tilde{b}(x) = \sum_{n=0}^{\infty} \tilde{b}_n \cdot x^n$$

Still, $\tilde{b}$ satisfies the quadratic equation, we want to show

$$\tilde{b}_n = \sum \tilde{b}_k \cdot \tilde{b}_{n-k-1}$$

By taylors theorem

$$\tilde{b}(x) = \tilde{b}_0 + \tilde{b}_1 x + \ldots + O(x^{n+1})$$

We substitute this into the quadratic equation, which yields

$$x(\tilde{b}_0 + \ldots \tilde{b}_n x^n + O(x^{n+1}))^2 - (\tilde{b}_0 + \ldots + \tilde{b}_n x^n + O(x^{n+1})) + 1 = 0$$

Solving for $\tilde{b}_n$ yields the desired equation.
Applying the generalized binomial theorem gives a closed form for b_n

$$b_n = -\frac{1}{2}(-4)^{n+1}\binom{\frac{1}{2}}{n+1}$$

We define the b_n 's as Catalans number.

Lecture 6: Fibonacci Numbers

Sat 27 Mar

Definition 9 (Fibonacci Sequence)
The sequence is defined by

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}$$

Theorème 17

$$\lim_{n\to+\infty}\frac{F_{n+1}}{F_n}=\phi$$

Preuve

Consider

$$F(x)=\sum F_i x^i$$

Hence

$$F(x)-xF(x)-X^2F(x)=\sum_{n=0}^{\infty}F_nx^n-\sum_{n=1}^{\infty}F_{n-1}x^n-\sum_{n=2}^{\infty}F_{n-2}x^n=x$$

Hence

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

Hence F as derivatives of all orderes at 0, writing the taylor expansion yields

$$\sum_{n=1}^{\infty}\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)x^n$$

□

Lecture 7: Linear Recurrence Relations

Sat 27 Mar

Definition 10 (Linear Recurrence)

A sequence of complex numbers satisfy a linear recurrence relation if there existe numbers $c_0,\ldots,c_{k-1}$ such that

$$a_{n+k}=c_0a_n+c_1a_{n+1}+\ldots+c_{k-1}a_{n+k-1}$$

forall $n\in\mathbb{Z}$

Lemme 18

Let $f=\frac{P}{Q}$ the ratio of two polynomials with $\deg Q>\deg P$.
Suppose that $Q(x)=(x-\mu_1)^{l_1}\ldots(x-\mu_t)^{l_t}$ for some $\mu_1,\ldots,$ then there exist $A_{j,m}$ such that

$$f(x)=\sum_{j=1}^{t}\sum_{m=1}^{l_j}\frac{A_{j,m}}{(x-\mu_j)^m}$$

Theorème 19

Suppose that a sequence a_n satisfies a linear recurrence relation

$$a_{n+k}=c_0a_n+c_1a_{n+1}+\ldots,+c_{k-1}a_{n+k-1}$$

Let $\lambda_1, \ldots, \lambda_s$ be the complex roots of the polynomial

$$x^k - c^{k-1}x^{k-1} - \ldots - c_0 = 0$$

where λ_i as multiplicity k_i.
Then there exist polynomials $P_1, \ldots, P_s$ of degree $k_i - 1$ such that

$$a_n = \sum_{i=1}^{s} P_i(n)\lambda_i^n, \quad n \in \mathbb{N}$$

Preuve
Suppose that a sequence a_n satisfies a linear recurrence relation as above.
Let $a(x) = \sum a_i x^i$, the recurrence relation implies

$$\begin{aligned} 0 &= \sum_{n=0}^{\infty} \left(a_{n+k} - c_{k-1}a_{n+k-1} - \ldots - c_0 a_n\right) x^n \\ &= \sum_{n=k}^{\infty} a_n x^{n-k} - c_{k-1} \sum_{n=k-1}^{\infty} a_n x^{n-k+1} - \ldots \end{aligned}$$

Rewriting this expression yields

$$a(x)(x^{-k} - c_{k-1}x^{-k+1} - \ldots) = \sum_{n=1}^{k} b_n x^{-n}$$

where b_n is linearly dependent with the initial terms. Dividing, this yields

$$a(x) = \frac{b_1 x^{-1} + \ldots + b_k x^{-k}}{x^{-k} - c^{k-1}x^{-k+1} - \ldots}$$

Therefore $a(x) = x\frac{P(x)}{Q(x)}$.
Suppose $Q(x) = (x - \mu_1)^{l_1} \ldots$
By the lemma

$$a(x) = x \sum_{j=1}^{t} \sum_{m=1}^{l_j} \frac{A_{j,m}}{(x - \mu_j)^m}$$

Observe that if λ_j is a root of

$$x^k - c_{k-1}x^{k-1} - \ldots - c_0$$

then $\mu_j^{-1} = \lambda_j$, also, if m is fixed, n can be considered as a variable and then

$$-n(n-1)\ldots(n-m+1)$$

is a polynomial of degree m. □

1.4 Linear recurrences in matrix form

Let a_n be a linearly recursive series, for each $n \geq 0$ we consider the vector

$$a_n = \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-1} \end{pmatrix}.$$

Then the recurrence relation can be written as

$$\begin{pmatrix} a_{n+1} \\ a_{n+1} \\ \vdots \\ a_{n+k} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ c_0 & c_1 & c_2 & \dots & c_{k-1} \end{pmatrix} \cdot \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-1} \end{pmatrix}$$

and more generally, we have

$$a_n = C^n \cdot a_0$$

Lecture 8: Moebios inversion formula

Sat 17 Apr

2 Moebius inversion formulas

2.1 Moebf

Let $f : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ be a function, we define a new function $F : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ by

$$F(n) \coloneqq \sum_{d|n} f(d), n \in \mathbb{Z}_{\geq 1}$$

Exemple
Let $f(n) = 1$ for all $n \in \mathbb{Z}_{\geq 1}$, then $F(n) = \sum_{d|n} 1$ which is the number of divisors of n.

Question

Suppose that we know F. How do we recover f ?

Definition 11 (Moebius function)

$$\mu : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$$

is defined as follows.
Suppose that $n \in \mathbb{Z}_{\geq 1}$ has the prime factorization

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

then

$$\mu(n) \coloneqq \begin{cases} 1 \text{ for } n = 1 \\ 0 \text{ if some } e_i > 1 \\ (-1)^r \text{ if } e_1 = e_2 = \ldots = 1 \end{cases}$$

Lemme 21
For $n \in \mathbb{Z}_{\geq 1}$ we have

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

Preuve
By induction, we check that

$$\sum_{d|1} \mu(d) = \mu(1) = 1$$

Now suppose that $n \in \mathbb{Z}_{\geq 1}$ has the prime factorization

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

Set $n^* \coloneqq \prod p_i$, the square free part of n.
If $d|n$ and $d \not| n*$, then d has a prime divisor of multiplicity > 1, then $\mu(d) = 0$.
Hence

$$\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d)$$

Now can easily compute

$$\begin{aligned} \sum_{d|n^*} \mu(d) &= \sum_{d|p_1 \ldots p_r} \mu(d) & &= \sum_{I \subset \{1,\ldots,r\}} \mu(\prod_{i \in I} p_i) \\ &= \sum_{I \subset \{1,\ldots,r\}} (-1)^{|I|} \\ &= \sum_{k=0}^{r} (-1)^k \binom{r}{k} = (1-1)^r = 0 \end{aligned}$$

□

Theorème 22 (Moebius inversion formula)
Let $f, F : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ be such that

$$F(n) = \sum_{d|n} f(d), \quad n \in \mathbb{Z}_{\geq 1} \tag{1}$$

Then

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) \tag{2}$$

Moreover, (2) *implies* (1)

Preuve

Let d *and* n *be positive integers such that* $d|n$.
Then $F(\frac{n}{d}) = \sum_{d'|\frac{n}{d}} f(d')$, *therefore*

$$\sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d')$$

Consider the set S_n *of all pairs* $(d, d') \in \mathbb{Z}_{\geq 1}$ *such that*

$$d|n \text{ and } d'|\frac{n}{d}$$

If n *and its divisor* d' *are fixe, then* d *runs over all divisors of* $\frac{n}{d'}$.
Hence, we can change the order of summation

$$\begin{aligned}\sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) f(d') &= \sum_{(d,d') \in S_n} \mu(d) f(d') \\ &= \sum_{d'|n} \sum_{d|\frac{n}{d'}} f(d') \mu(d)\end{aligned}$$

Using the lemma above, we get

$$\begin{aligned}\sum_{d'|n} \sum_{d|\frac{n}{d'}} f(d') \mu(d) &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= f(n)\end{aligned}$$

We now show the other implication, namely
Let $F : \mathbb{Z}_{\geq 0} \to \mathbb{C}$ *be any function.*
Set $f(n) \coloneqq \sum_{d|n} \mu(d) F(\frac{n}{d})$, *then for* $n \in \mathbb{Z}_{\geq 1}$

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{d'|d} \mu(d') F(\frac{d}{d'})$$

we make the change of variables

$$\{(d, d') | d|n, d'|d\} \to \left\{(d'', d') | d''|n, d'|\frac{n}{d''}\right\}$$

Then

$$= \sum_{d''|n} \sum_{d'|\frac{n}{d''}} \mu(d') F(d'') = \sum_{d''|n} F(d'') \sum_{d'|\frac{n}{d''}} \mu(d') = F(n)$$

□

2.2 Computing the number of cyclic sequences

Definition 12 (Linear sequence)
Let A be a set. A linear sequence of length n in the alphabet A is an element of A^n :

$$a = (a_1, \ldots, a_n), a_k \in A \text{ for } k = 1, \ldots, n$$

The number of linear sequences of length n in an alphabet of size r is r^n.
Consider the following equivalence relation on the set of linear sequences

$$(a_1, \ldots, a_n) \sim (a_2, \ldots, a_n, a_1)$$

Two linear sequences are equivalent if one of them can be obtained from another by a cyclic shift.

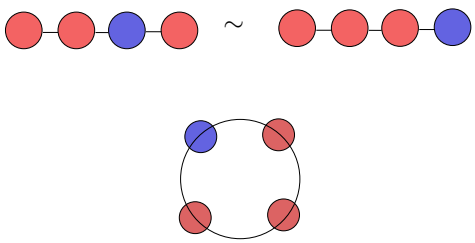

FIGURE 1 – Linear sequence

Exemple

Definition 13 (Cyclic sequence)
A cyclic sequence of length n in an alphabet A is an equivalence class of linear sequences with respect to the relation $\sim$.

Proposition 24
The number of $T(n, r)$ of cyclic sequences of length n on an alphabet of size r is

$$T(n, r) = \frac{1}{n} \sum_{d|n} \phi(\frac{n}{d}) r^d$$

Here, $\phi(\cdot)$ is the Eulers totient function.

Definition 14 (Period of cyclic sequence)
A period of a cyclic sequence $(a_1, \ldots, a_n)$ is a minimal number $k \in \{1, 2, \ldots, n\}$ such that

$$(a_1, a_2, \ldots, a_n) = (a_{1+k}, a_{2+k}, \ldots, a_1, \ldots, a_k)$$

are equal as linear sequences.

Exercise

Show that a k is always a divisor of n.

Let $M(d, r)$ be the number of cyclic sequences of length d and of period r. We notice that

$$r^n = \sum_{d|n} d \cdot M(d, r)$$

Indeed, notice that there exists π a projection from the linear sequences of length n into the cyclic sequences.
The number of preimages of a cyclic sequence under the map π is d, the period of the sequence, therefore, if we denote by $\mathcal{L}(n, r)$ the set of linear sequences, we get

$$r^n = |\mathcal{L}(n, r)| = \sum_{d|n} d \cdot |M(d, r)|$$

Applying the Moebius inversion formula, we obtain

$$n \cdot M(n, r) = \sum_{d|n} \mu(\frac{n}{d}) r^d$$

Each cyclic sequence has a well defined period d and it corresponds to the unique cyclic sequence of length d and period d. Thus

$$T(n, r) = \sum_{d|n} M(d, r)$$

Combining both formulas above, we get

$$\begin{aligned} T(n, r) &= \sum_{d|n} M(d, r) \\ &= \sum_{d|n} \frac{1}{d} \sum_{d'|d} \mu(\frac{d}{d'}) r^{d'} \\ &= \sum_{d'|n} \sum_{d''|\frac{n}{d'}} \frac{1}{d' \cdot d''} \mu(d'') r^{d'} \end{aligned}$$

Now we have to compute the sum

$$\sum_{d''|\frac{n}{d'}} \frac{1}{d''} \mu(d'')$$

As an exercise, show that for $n \in \mathbb{Z}_{\geq 1}, \sum_{d|n} \frac{1}{d}\mu(d) = \frac{\phi(n)}{n}$.
Using this, we finally obtain that

$$T(n,r) = \sum_{d'|n} \frac{\phi(\frac{n}{d'})}{n} r^{d'}$$

2.3 Moebius inversion for posets

Definition 15 (Binary relation)
A binary relation on a set A is a subset $R \subseteq A \times A$.
A relation is antisymmetric provided $(a,b) \in R$ and $(b,a) \in R$ imply $a = b$.
A relation is transitive if $(a,b) \in R$ and $(b,c) \in R$ imply $(a,c) \in R$
A relation is reflexive if $(a,a) \in R$ for all $a \in R$.

Exemple

1. *The relation $\leq$ on $\mathbb{Z}$ is antisymmetric, transitive, and reflexive*
2. *The relation $<$ on $\mathbb{Z}$ is antisymmetric, transitive and not reflexive*
3. *The relation coprime is not antysimmetric, not transitive and not reflexive*

Definition 16 (Partial Order)
A partial order on a set A is an antisymmetricm reflexive and transitive relation $R \subseteq A \times A$.
A partially ordered set (or poset) is a set together with a partial order

Exemple
Let A be a set. The set 2^A of subsets of A is a partially ordered set by inclusion

- *Reflexivity : $X \subseteq X$*
- *Transitivity : if $X \subseteq y$ and $Y \subseteq Z$ then $X \subseteq Z$*
- *Antisymnmetric : if $X \subseteq Y$ and $Y \subseteq X$ then $X = Y$*

Exemple
The set $\mathbb{Z}_{\geq 1}$ is partially ordere by the relation d divides n.

- *Reflexivity : n divides n*
- *Transitivity : if $d|n$ and $d'|d$ then $d'|n$*
- *Antisymnmetric : if $n|m$ and $m|n$ then $m = n$.*

We can represent such relations with Hasse diagrams in the following way

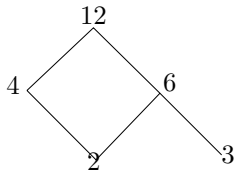

FIGURE 2 – Hasse diagram 12

Definition 17 (Locally finite poset)
A partially ordered set $(X, \geq)$ is locally finite if for all $x, y \in X$ the interval

$$[x, y] \coloneqq \{z \in X | y \leq z \leq x\}$$

is finite.
We say that $0 \in X$ is a zero element if $0 \leq x$ for all $x \in X$

Let $(X, \leq)$ be a partiallly ordered locally finite set with 0.
Suppose that $f : X \to \mathbb{C}$ is a function.
We define a new function $F : X \to \mathbb{C}$ by

$$F(x) \coloneqq \sum_{y \leq x} f(y)$$

How do we recover f from F ?

Theorème 28 (Moebius inversion for posets)
Given a partially ordered set X, there is a two varaiable function $M : X \times X \to \mathbb{R}$ such that

$$F(x) = \sum_{y \leq x} f(y) \iff f(x) = \sum_{y \leq x} F(y) M(x, y)$$

M is called the Moebius function of the poset.

Definition 18 (Incidence algebra $A(X)$)
Given a partially ordered set X, the incidence algebra $A(X)$ is the set of complex valued functions $f : X^2 \to \mathbb{C}$ satisfying $f(x, y) = 0$ unless $x \leq y$.
$A(X)$ is a vector space over $\mathbb{C}$ with respect to pointwise addition and multiplication by scalars.
To make it into an algebra we need one more operation

Definition 19 (Convolution)
Given $f, g \in A(X)$, their convolution $f * g$ is defined by

$$f * g(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y)$$

Definition 20
The delta function δ is the element of $A(X)$

$$\delta(x, y) = \begin{cases} 1 \text{ if } x = y \\ 0 \text{ otherwise} \end{cases}$$

Remarque
Convolution is not always commutative.

Lemme 30
A function $f \in A(X)$ has a left and right inverse with respect to the convolution if and only if $f(x, x) \neq 0$ for all $x \in X$

Preuve
Given $f \in A(X)$ we find $g \in A(X)$ such that

$$f * g(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y) = \delta(x, y)$$

For all $x \in X$

$$f * g(x, x) = f(x, x) g(x, x) = \delta(x, x) = 1$$

Therefore, the condition $f(x, x) \neq 0$ is necessary for the existence of the inverse.
We define $g(x, x) \coloneqq f(x, x)^{-1}$.
To define $g(x, y)$ for $x < y$, we assume by induction, that we have already found all $g(z, y)$ for all z, satisfying $x < z \leq y$.
Then

$$\delta(x, y) = 0 = \sum_{x \leq z \leq y} f(x, z) g(z, y)$$

$$-f(x, x) g(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y)$$

We can now solve for $g(x, y)$.
Finally, if $f * g_1 = \delta$ and $g_2 * f = \delta$, then

$$g_2 = g_2 * \delta = g_2 * f * g_1 = \delta * g_1 = g_1$$

Therefore, the left and the right inverses of f coincide. □

Definition 21 (Zeta function)
The Zeta function $Z(x, y)$ of the poset $(X, \leq)$ is the function

$$Z(x,y) = \begin{cases} 1 \text{ if } x \leq y \\ 0 \text{ otherwise} \end{cases}$$

Definition 22 (Moebius function)
The Moebius function $M(x, y)$ is the inverse of the zeta function Z with respect to convolution.

We can now prove the Moebius inversion for posets

Preuve
Let $f : X \to \mathbb{C}$ be a function and $F : X \to \mathbb{C}$ be defined by

$$F(x) = \sum_{y \leq x} f(y)$$

Then, for a fixed $x \in X$:

$$\begin{aligned} \sum_{y \leq x} F(y)M(y,x) &= \sum_{y \leq x} M(y,x) \sum_{z \leq y} f(z) \\ &= \sum_{z \leq y \leq x} f(z)M(y,x) \\ &= \sum_{z \leq x} f(z) \sum_{z \leq y \leq x} M(y,x) \\ &= \sum_{z \leq x} f(z) \left(\sum_{z \leq y \leq x} Z(z,y)M(y,x) \right) \\ &= \sum_{z \leq y} f(z)(Z * M)(z,x) \\ &= \sum_{z \leq y} f(z)\delta(z,x) \qquad\qquad = f(x) \end{aligned}$$

Now we show that the inverse is also true.
Let $F : X \to \mathbb{C}$ be a function and we define $f : X \to \mathbb{C}$ by

$$f(x) = \sum_{y \leq x} F(y)M(y,x), x \in X$$

Then,

$$\begin{aligned} \sum_{y \leq x} f(y) &= \sum_{y \leq x} \sum_{z \leq y} F(z)M(z,y) \\ &= \sum_{z \leq y \leq x} F(z)M(z,y) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{z \leq y \leq x} F(z) M(z,y) Z(z,y) \\
&= \sum_{z \leq x} F(z) \left(\sum_{z \leq y \leq x} M(z,y) Z(y,x) \right) \\
&= \sum_{z \leq x} F(z) \left(\sum_{z \leq y \leq x} M(z,y) Z(y,x) \right) \\
&= \sum_{z \leq x} F(z) \delta(z,x) = F(x)
\end{aligned}
$$
□

Lemme 31
Let 2^A be the set of subsets of a finite set A.
2^A is partially ordered by inclusion.
The Moebius function of 2^A is given by

$$M(x,y) = (-1)^{|x|-|y|}$$

Where $x \subseteq y \subseteq A$

Preuve
We have to show that $M * Z = \delta$. Let x, y be two subsets of A such that $x \subseteq y$. We compute

$$
\begin{aligned}
M * Z(x,y) &= \sum_{x \subseteq z \subseteq y} M(x,z) Z(z,y) \\
&= \sum_{x \subseteq z \subseteq y} (-1)^{|x|-|z|} \\
&= \sum_{w \subseteq y \setminus x} (-1)^{|w|} \qquad = \begin{cases} 0 \text{ if } |y \setminus x| \geq 1 \\ 1, |y \setminus x| = \emptyset \end{cases} \quad = \delta(x,y)
\end{aligned}
$$
□

Lecture 9: Basics of graph theory

Sat 24 Apr

3 Graph Theory

3.1 Basic Definitions

Definition 23 (Graph)
A graph G is an ordered pair (V, E) where V is a set of elements called vertices and E is a set of 2-element subsets of V.

Exemple
$V = \{1,2,3,4\}$ and $E = \{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$

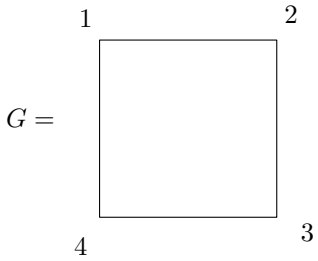

FIGURE 3 – four edged graph

This is called a undirected simple graph.

Non-examples

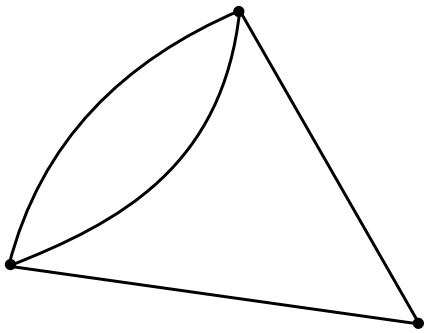

FIGURE 4 – multiple edges

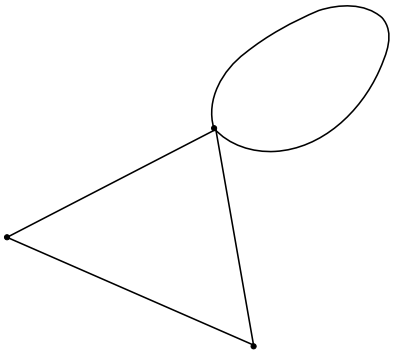

FIGURE 5 – loops

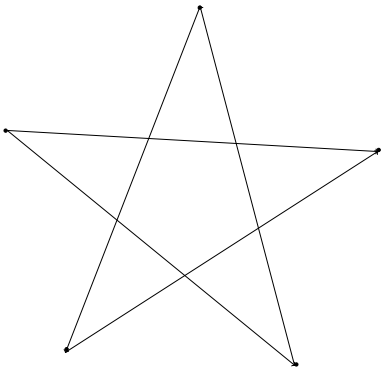

FIGURE 6 – direction of edges

3.2 Important graphs

Definition 24 (Complete graph)
Let V be a finite set.
A complete graph on vertices V (or a clique) is the graphe $G = (V, \binom{V}{2})$

A complete graph with n vertices is denoted K_n

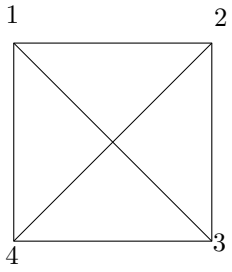

FIGURE 7 – K_4

Definition 25 (Cycle graph)
The cycle C_n is the graph

$$V = \{1, 2, \ldots, n\} \quad E = \{\{1, 2\}, \ldots, \{n-1, n\}, \{n, 1\}\}$$

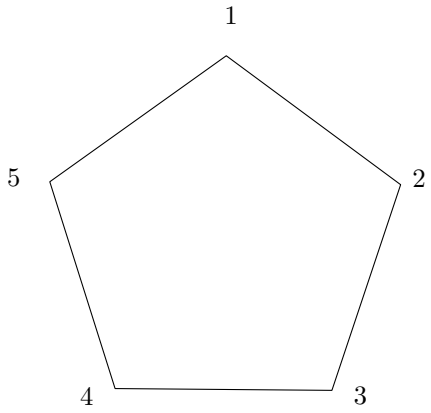

FIGURE 8 – C_5

Let $G = c(V, E)$ be a graph

Definition 26 (Adjacent vertices)
Let $v_1, v_2 \in V$ be vertices of G. If $\{v_1, v_2\} \in E$we say that v_1 and v_2 are connected by and edge or adjacent.

Definition 27 (Degree of a vertex)
A degree of a vertex $v \in V$ is the number of edges adjacent to it.

Lemme 33 (The hand shake lemma)
The sum of degrees of all vertices in a finite graph G is always an even lemma.

Preuve
The sum of degrees of all vertices is equal to twice the number of edges. □

3.3 Wals and paths

Definition 28 (Walk)
A walk on a graph G is a sequence of nodes $v_0, v_1, \ldots, v_k$ such that v_i is adjacent to v_{i+1} for all $i < k$.

Definition 29 (Path)
A path is a walk such that all its vertices are distinct.

Definition 30 (Closed Walk)
A closed walk is a walk such that the first vertex coincides with the last one.

Definition 31 (Connected graph)
A graph $G = (V, E)$ is connected if for every two vertices $u, v \in V$ there exists a path in G between them.

Definition 32 (Cycle)
A cycle in a graph $G = (V, E)$ is a sequence of distinct vertices $v_1, \ldots, v_r \in V$ such that $v_{i \mod r}$ is adjacent to $v_{i+1 \mod r}$.

Definition 33 (Tree)
A tree is a connected graph without cycles.

Definition 34 (Leaf)
A vertex of degree 1 in a tree is called a leaf.

Lemme 34
Every finite tree with $n \geq 2$ vertices has at least two leaves

Preuve
Consider a path of maximum length, say $v_1, v_2, \ldots, v_n$.
A tree is connected, therefore such a path exists and has lenght at least 2.
The initial point v_1 and the final point v_n mus be leaves otherwise the path can be extended. □

Lemme 35
Every tree with n vertices has exactly $n-1$ edges.

Preuve
We prove the lemma by induction on n.
For $n=1$, it is clear that the graph contains 0 edges.
Suppose the lemma is true for all threes with $\leq n$ vertices.
Let $T=(V,E)$ be a tree with $n+1$ vertices.
By the previous lemma T has a leave, say $v \in V$.
Let e be the unique edge adjacent to v.
We define a new graph $T' \coloneqq (V \setminus \{v\}, E \setminus \{e\})$.
The new graph T' contains no cycles and is connected, hence T is a tree.
By induction hypothesis

$$|E \setminus \{e\}| = |V \setminus \{v\}| - 1 = n-1 \qquad \square$$

Which concludes the proof.

Lecture 10: graph isomorphism

Sun 02 May

3.4 Graph isomorphisms

Two graphs $G=(V,E)$ and $G'=(V',E')$ are considered identical if they have the same set of vertices and edges

Definition 35 (Graph isomorphisms)
Two graphs $G=(V,E)$ and $G'=(V',E')$ are called isomorphic if there is a bijection $f: V \to V'$ such that for all $x,y \in V$:

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

Such an f is called an isomorphism of the graphs G and G', we write $G \simeq G'$

Remarque
In general, deciding whether two graphs are isomorphic is a difficult computational problem.
Finding efficient algorithms is an active research area.

3.4.1 Number of isomorphism classes of graphs

What is the number of isomorphism classes of graphs with vertices $\{1,2,\ldots,n\}$.
The number of different graphs is $2^{\binom{n}{2}}$.
Each isomorphism class contains at most $n!$ elements, therefore

$$\frac{2^{\binom{n}{2}}}{n!} \leq |\text{ isomorphism classes } \leq 2^{\binom{n}{2}}$$

Remarque
An isomorphism class is also called an unlabeled graph.

3.5 Trees

Theorème 38 (Cayley)
The number of trees on n labelled vertices is n^{n-2}.

Preuve
We will prove this theorem by using Pruefer codes.
We will define a one-to-one correspondence between the set of all trees on n labelled vertices and the set of sequences of length $n-2$ consisting of numbers in $\{1,\dots,n\}$.
The result will then follow by comparing the cardinality of both sets.
Consider the following algorithm.

- *Input : a tree of vertices $\{1,\dots,n\}$*
- *Step 1 : Find the leaf with smallest label and writie down the number of its neighbours*
- *Step 2 : Delete this leaf and the only edge adjacent to it*
- *Repeat until we are left with only two vertices.*
- *Output : string of labels we have written down.*

The reverse construction is done through the following algorithm.
Input : a sequence $(a_1,\dots,a_{n-2}) \in [n]^{n-2}$

- *Step 1 : Draw n nodes $12\dots n$*
- *Step 2 : Make the list $= (1,2\dots,n)$*
- *Step 3 : If there are only two numbers left on the list, connect them with and edge and stop. Otherwise, continue to step 4*
- *Find the smallest number in the list which is not in the sequence. Take the first number in the sequence.*
  Add and edge connecting the nodes whose labels correspond to those numbers.
- *Delete the smallest number which is not in the sequence from the list and the first number in the sequence. This gives a smaller list and shorter sequence. The return to step 3.*

Theorème 39
These algorithms provide a map, name them ψ_1, from the set of trees of vertices $\{1,2\dots,n\}$ to the set $[n]^{n-2}$

$$\psi_1(\text{ tree }) = \text{ Pruefer code of a tree}$$

Algorithm 2 provides a map, name it ψ_2, from the set of sequences $[n]^{n-2}$

to the set of trees of vertices $[n]$

$$\psi_2(\ \textit{sequence}\ ) = \ \textit{tree}$$

The maps are inverse to each other, namely

$$\psi_1 \circ \psi_2 = \psi_2 \circ \psi_1 = \mathrm{Id}$$

Preuve
We prove the theorem by induction on n.
For $n = 2$, *the unique tree is* $1 - 2$ *and its Pruefer code is* $\emptyset$.
Let T *be a tree of vertices* $[n]$.
We apply algorithm 1 to T.
Let T_1 *be the tree obtained from* T *after applying step 2 once.*
Observe that $a_2, \ldots, a_{n-2}$ *is the Pruefer code of the tree* T_1. *Note that the vertices of* T_1 *are labelled by* $[n] \setminus \{n_0\}$, *where* n_0 *is the smallest leaf in* T.
Also, the set $\{1, 2 \ldots, n\} \setminus \{a_1, a_2, \ldots, a_{n-2}\}$ *is the set of all leaves of* T.
Now we apply algorithm 2 to the sequence $(a_1, \ldots, a_{n-2})$.
The smallest element of the list $[n]$ *which is not in the sequence* $(a_1, \ldots, a_{n-2})$ *is the smallest leaf* n_0 *of* T.
The first iteration adds an edge between nodes n_0 *and* a_1.
By the assumption, algorithm 2 applied to the sequence $(a_2, \ldots, a_{n_{n-2}})$ *will give us the tree* T_1 *with vertices labeled by the set* $\{1, \ldots, n\} \setminus \{n_0\}$.
This finishes the proof

3.5.1 Estimating the number of unlabelled trees

There is no explicit formula for the number of unlabelled trees with n vertices.

Theorème 40
Let T_n *be the number of unlabelled trees with* n *vertices. Then*

$$\underbrace{2^n}_{for\ n>30} \leq \frac{n^{n-2}}{n!} \leq T_n \leq 4^{n-1}$$

Preuve
First, we prove that $T_n \geq \frac{n^{n-2}}{n!}$.
We know that

$$T_n \geq \frac{|\ \textit{labelled trees}\ |}{\textit{max number of trees in one equivalence class}}$$

This max number of trees is $n!$.
Now we show that $T_n \leq 4^{n-1}$.

Take an unlabelled tree T with n vertices.
Choose one vertex of T and call it a root.
Embed T into a plane

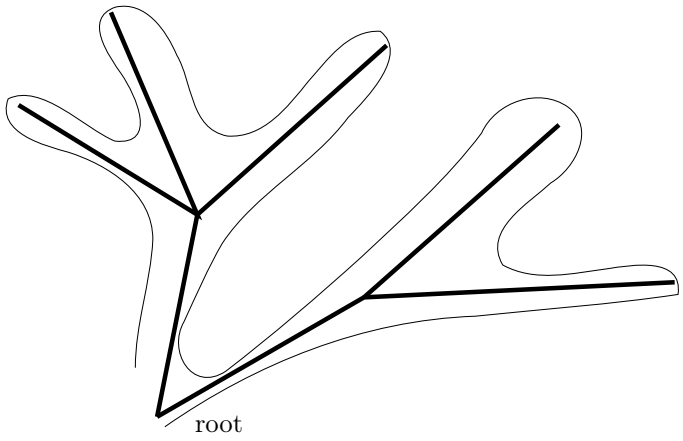

FIGURE 9 – embedded tree

We start from the root and go counterclockwise around the tree and write
- *+ if the distance to the root increases*
- *− if the distance to the root decreases*

At the end of the path, we obtain a sequence $\{+,-\}^{2n-2}$.
An unlabelled tree can be uniquely reconstructed from the sequence.

- *Each tree correspond to at least one and possibly more sequences*
- *Each sequence corresponds to one unlabelled tree*
- *Some sequences do not correspond to any tree* □

Lecture 11: Subgraphs vs induced subgraphs

Sun 09 May

3.6 Subgraphs vs induced subgraphs

Definition 36 (Subgraph)
A subgraph of a graph $G = (V, E)$ is a graph $G' = (V', E')$ such that $V' \subset V$ and $E' \subset E$.

Definition 37 (Induced subgraph)
The graph $G' = (V', E')$ is an induced subgraph of $G = (V, E)$ if $V' \subset V$ and $E' = E \cap \binom{V'}{2}$.

Definition 38 (Spanning tree)
Let $G = (V, E)$ be a graph.

An arbitrary tree of the form (V, E') where $E' \subseteq E$ is called a spanning tree of the graph G.

Lemme 41
Every connected graph contains a spanning tree.

Preuve
Let $G = (V, E)$ be a connected graph.
We construct a spanning tree of G by the following algorithm.

1. *Start with an empty sungraph $T = \emptyset$*
2. *Pick an edge $e \in E$ such that $e \notin E(T)$*
3. *Consider the new subgraph T' obtained from T by adding e, i.e.*

$$V(T') = V(T) \cup \{v_1, v_2\}, E(T') = E(T) \cap \{e\}$$

4. *If T' does not contain cycles set $T \coloneqq T'$*
5. *If there is no edge $e \in E$ such that 2 and 3 hold, then stop.*

Note that
— *T contains all vertices of G*
— *T is connected*
— *T contains no cycles*
Hence, T is a spanning tree. □

3.7 Minimal spanning trees

Definition 39 (Weighted graph)
A weighted graph is a graph in which each edge is assigned a numerical weight. We define the weight of a graph as the sum of weights of all its edges.

Problem

Find a minimum weight spanning tree T for a given weighted connected graph G.

3.7.1 Greedy algorithm (or Kruskal's algorithm)

— Input : Connected weighted graph
— Step 1 : Start with an empty graph
— Step 2 : Take all the edges that have not been selected and that would not creat a cycle with the already selected edges. Add the one with the smallest weight
— Step 3 : Repeat until the graph is connected and contains all vertices.

Let us show that the algorithm yields the desired result.

Preuve
Let T be the graph obtained as the output of Kruskal's algorithm to a weighted connected graph G, we observe
- *T contains all vertices of G*
- *T is connected*
- *T contains no cycles*

So T contains no cycles. □

Now we show that T has minimal weight.
Let F be another spanning tree of G, we want to show that $wt(F) \geq wt(T)$.
We number the edges of T according to the order we have added them while running Kruskal's algorithm.
Let e be the edge with the smallest number such that $e \in E(T)$ and $e \notin E(F)$.
Add e to F, the ne new graph will contain a cycle C.
C is not fully contained in T, so C has and edge f that is not an edge of T.
If we add the edge e to F and delete f, we get a third tree H.
Suppose $wt(f) < wt(e)$.
If whe chose e and not f in the algorithm, it means that f would forme a cycle with the already selected edges of T.
All previously selected edges of T are edges of F, f is an edge of F implies F contains a cycle, which is impossible since F is a tree.
Hence, $wt(F) > wt(H)$

Lecture 12: Graphs and matrices

Sun 16 May

3.8 Graphs and matrices

Let G be a graph. Suppose $|V(G)| = n, |E(G)| = m$.

Definition 40 (Adjacency matrix)
The adjacency matrix of G is the $n \times n$ matrix $A(G)$ given by

$$A_{ij} = \begin{cases} 1 \text{ if } \{v_i, v_j\} \in E \\ 0 \text{ otherwise} \end{cases}$$

Definition 41 (Degree matrix)
The degree matrix of G is the diagonal $n \times n$ matrix $D(G)$ given by

$$D_{ij} = \begin{cases} \deg v_i \text{ if } i = j \\ 0 \text{ otherwise} \end{cases}$$

Definition 42 (Laplace matrix)
The Laplace matrix of G is defined as

$$L(G) \coloneqq D(G) - A(G)$$

Lemme 42
Let G be agraph and $A = A(G)$ be its adjacency matrix. The entries of the matrix $B \coloneqq A^n$ have the following combinatorial interpretaion : B_{ij} is the number of walks of length n starting at v_i and ends at v_j

Preuve

$$B_{ij} = \sum_{k_1=1}^{|V(G)|} \sum_{k_2}^{|V(G)|} \dots \sum_{k_{n-1}=1}^{|V(G)|} A_{i,k} A_{k_1,k_2} \dots A_{k_{n-1},j}$$

And we have that

$$A_{i,k} A_{k_1,k_2} \dots A_{k_{n-1},j} = \begin{cases} 1 \text{ if } \{i, k_1, \dots k_{n-1}, j\} \text{ is a walk} \\ 0 \text{ otherwise} \end{cases}$$

□

Let G be a graph. Suppose $|V(G)| = n, |E(G)| = m$

Definition 43 (orientation)
We say that a graph G has and orientation $\mathcal{O}$ if for every edge $\{v_1, v_2\}$of G, we say that v_1 is the intial vertex and v_2 is the finite vertex.

Definition 44 (Incidence matrix)
The incidence amtrix $M(G, \mathcal{O})$ is the $n \times m$ matrix given by

$$M_{ij} = \begin{cases} 1 \text{ if the edge } e_j \text{ has initial vertex } v_i \\ -1 \text{ if the edge } e_j \text{ has final vertex } v_i \\ 0 \text{ otherwise} \end{cases}$$

Lemme 43
We have that

$$M(G, \mathcal{O}) M(G, \mathcal{O})^T = L(G)$$

Preuve
$M(G, \mathcal{O}) M(G, \mathcal{O})^T$ is an $n \times n$ matrix.
The (i, j)-th entry of $M(G, \mathcal{O}) M(G, \mathcal{O})^T$ is

$$\sum_{k=1}^{m} M_{i,k} \cdot M_{j,k} = \sum_{\substack{k: \\ e_k \text{ is adjoint to } v_i \text{ and } v_j}} M_{i,k} M_{k,k}$$

If $i \neq j$, then

$$\sum_{k=1}^{m} M_{i,k}M_{j,k} = \begin{cases} 0 \text{ if } \{v_1, v_j\} \notin E \\ -1 \text{ if } \{v_i, v_j\} \in E \end{cases}$$

If $i = j$, then $\sum_{k=1}^{m} M_{i,k} \cdot M_{i,k} = \deg v_i$ □

3.9 Kirchhof theorem

Theorème 44 (Kirchhoff)
Let G be a connecte graph on n vertices. Then the rank of the Laplace matrix $L(G)$ is $n-1$.
Let $0, \lambda_1, \ldots, \lambda_{n-1}$ bet the eigenvalues of $L(G)$, then the number of spanning trees of G is

$$\frac{1}{n}\lambda_1\lambda_2 \ldots \lambda_{n-1}$$

Theorème 45 (Binet-Cauchy)
Let A be a rectangular matrix of size $m \times n$.
Suppose $m \leq n$ and S is an m-element subset of $[n]$.
The we denote by $A[S]$ the matrix $(A_{i,j})_{i=1,\ldots,m,j\in S}$ consisting of columns of A indexed by elements of S. For $A, B \in \mathbb{C}^{m\times n}$, we have

$$\det(AB^T) = \sum_S (\det A[S])(\det B[S])$$

where S runs over all m-element subsets of $[n]$.

Lemme 46
Let S be a set of $n-1$ edges of G.
If S does not form the set of edges of a spanning tree, then $\det M_0(S)$ =0.
If S is the set of edges of a spanning tree of G, then $\det M_0(S) = \pm 1$.

Preuve
First, suppose that S is not the set of edges of a spanning tree. Then some subset R of S forms the edges of a cycle C in G.
Suppose that the cycle C has edges $f_1, \ldots, f_s$ in this order.
Let $w_1, \ldots, w_s$ be the corresponding column vectors of $M_0(S)$.
Define

$$k_i := \begin{cases} +1 \text{ if orientation of } f_i \text{ coincides with orientation of } C \\ -1 \text{ if not} \end{cases}$$

We have

$$\sum_{i=1}^{s} k_i w_i = 0$$

□

Therefore, $rg(M_0(S)) < n-1 \Rightarrow \det M_0(S) = 0$. *Now suppose that* S *is the set of edges of a spanning tree* T.
Recall : v_n *is the last vertex of* G *which corresponds to the row removed from* M *to obtain* M_0.
Let e *be an edge of* T *which is connected to* v_n. *The column of* $M_0(S)$ *indexed by* e *contains exactly one non-zero entry (which is* ± 1*).*
Remove from $M_0(S)$ *the row containing this non-zero entry (the row corresponding to* v_i*) and the column corresponding to* e.
We obtain a $(n-2) \times (n-2)$ *matrix* M_0'.
We have $\det M_0(S) = \pm \det(M_0')$.
Let T' *be the tree obtaine from* T *by contracting the edge* e *to a single vertex* u.
Then M_0' *is the matrix obtaine from the incidence matrix of* T' *by removing the row indexed by* u.
By induction on the number n *of vertices we have* $\det M_0' = \pm 1$ *(the case* $n = 2$ *is trivial).*

Preuve
Let $M = M(G)$ *be an incidence matrix of* G.
Let $M_0(G)$ *be be the matrix obtaine from* $M(G)$ *by removing the last row.*
Let $S \subset E$ *be a subset of edges such that*

$$|s| = |V(G)| - 1$$

The $M_0(S) \coloneqq$ *submatrix of* $M_0(G)$ *formed by columns of* M_0 *indexed by edges of* S.
Let $L_0(G)$ *be the matrix obtained from* $L(G)$ *by removing the last row and the last column.*
By definition of the laplace matrixe, we have

$$L_{in} = -\sum_{j=1}^{n-1} L_{ij}, i = 1, \ldots, n$$

Finally, by Binet-Cauchy theorem

$$\begin{aligned} \det L_0 &= \sum_{S \subset E, |S| = n-1} (\det M_0[S])(\det M_0^T[S]) \\ &= \sum_{S \subset E, |S| = n-1} (\det M_0[S])^2 \\ &= \sum_S (\pm 1)^2 + \sum_S 0^2 \end{aligned}$$ □

Where S *is the set of edges of a spanning tree.*

Lecture 13: Binet-Cauchy Theorem

Sun 23 May

3.10 Binet-Cauchy Theorem

Let A be a rectangular matrix of size $m \times n$. Suppose $m \leq n$ and S is an $m-$ element subset of $\{1, 2, \ldots, n\}$. Then we denote by $A[S]$ the matrix $A_{i,j,i\in[m],j\in S}$

Theorème 47 (Binet-Cauchy)
Let $A, B \in M_{m\times n}(\mathbb{C})$. If $m \leq n$, then $\det(AB^t) = \sum_S (\det A[S])(\det B[S])$, where S runs over all $m-$element subsets of $\{1, 2, \ldots, n\}$.

Lecture 14: Finite probability spaces

Sat 29 May

4 Finite probability spaces and probabilistic methods

Definition 45 (Finite probability space)
A finite probabilite space is a pair (Ω, P) , where Ω is a finite set and $P : 2^\Omega \to [0, 1]$ such that

1. *$P(\emptyset) = 0$*
2. *$P(\Omega) = 1$*
3. *$P(A \cup B) = P(A) + P(B)$ for any two disjoint sets $A, B \subset \Omega$*

The set Ω can be thought as the set of all possible outcomes of some random experiment. The elements of Ω are called elementary events. Subsets of Ω are called events.
Let $w \in \Omega, A, B \subset \Omega$

— $w \in A \leftrightarrow$ event A occured
— $w \in A \cap B \leftrightarrow$ both events occured
— $A \cap B = \emptyset \leftrightarrow$ events A and B are incompatible
— $P(A) \leftrightarrow$ the probability of event A

4.1 A random graph

We define

$$\Omega = \mathcal{G}_n \coloneqq \text{ set of all possible labelled graphs on vertex set } V = \{1, \ldots, n\}$$

for $A \subset \mathcal{G}_n$.
We define the probability function to be

$$P(A) \coloneqq \frac{|A|}{|\Omega|} = |A| 2^{-\binom{n}{2}}$$

Proposition 48
A random graph is almost never a tree, i.e.

$$\lim_{n\to+\infty} P(\text{“ } A \text{ graph in } \mathcal{G}_n \text{ is a tree } \text{”}) = 0$$

Preuve

$$P(T_n) = \frac{|T_n|}{|\mathcal{G}_n|}$$

By caley's theorem $|T_n| = n^{n-2}$ *, hence*

$$\lim_{n\to+\infty} \frac{n^{n-2}}{2^{\frac{n(n-1)}{2}}} = \lim_{n\to+\infty} e^{-\ln(2)\frac{n(n-1)}{2}+(n-2)\ln(n)} = 0$$

□

Definition 46 (independent events)
Two events A, B *in a probability space* (Ω, P) *are called independent if*

$$P(A \cap B) = P(A) \cdot P(B)$$

One can easily generate this definition

Definition 47
Events $A_1, \ldots, A_n \subset \Omega$ *are independent if for each set of indices* $I \subset [n]$

$$P(\bigcap_{i\in I} A_i) = \prod_{i\in I} P(A_i)$$

Definition 48
Let (Ω, P) *be a finite probability space. A random variable on* Ω *is any map* $f : \Omega \to \mathbb{R}$.

Definition 49
Let (Ω, P) *be a finite probability space, and let* f *be a random variable on it. The expectation of* f *is a real number* $\mathbb{E}(f)$ *defined by the formula*

$$\mathbb{E}(f) \coloneqq \sum_{w\in\Omega} P(\{w\}) \cdot f(w)$$

Is there an easy way to compute $\mathbb{E}(f)$?

Definition 50 (Indicator)
Let $A \subset \Omega$ *be an event in a probability space* (Ω, P) *. The indicator of the event* A *is the random variable* $I_A : \Omega \to \{0, 1\}$ *defined as*

$$I_A(w) \coloneqq \begin{cases} 1 \text{ fo } w \in A \\ 0 \text{ for } w \notin A \end{cases}$$

Lemme 49
For any event A , we have $\mathbb{E}(I_A) = P(A)$

Preuve

$$\mathbb{E}(I_A) = \sum_{w\in\Omega} I_A(w)P(\{w\}) = \sum_{w\in A} P(\{w\}) = P(A)$$

□

Theorème 50 (linearity of expectation)
Let f, g be arbitrary random variables on a finite probability space (Ω, P) and let $\alpha \in \mathbb{R}$. Then

$$\mathbb{E}(\alpha f) = \alpha\mathbb{E}(f) \text{ and } \mathbb{E}(f + g) = \mathbb{E}(f) + \mathbb{E}(g)$$

4.2 Probabilistic method

Theorème 51
Let (Ω, P) be a finite probability space and let $f : \Omega \to \mathbb{R}$ be a random variable.
If $\mathbb{E}(f) = m$, then there exists a t least one elementary event w_1 such that $f(w_1) \geq m$.
Analogously, there exists at least one elementary event w_2 such that $f(w_2) \leq m$

We consider two applications of this theorem.

Theorème 52
Let G be a graph with an even number $2n$ of vertices and with $m > 0$ edges. Then the set $V = V(G)$ can be divided into two disjoint $n-$element subsets A and B in such a way that more than $\frac{m}{2}$ edges go between A and B .

Preuve
Consider the probability space (Ω, P) where $\Omega = \binom{V}{n}$ with the probability measyre

$$P(S) \coloneqq \frac{|S|}{|\Omega|} \text{ for } S \subset \Omega$$

Let $A \in \Omega$ be a random n -element subset of $V(G)$.
Define $B \coloneqq V(G) \setminus A$ its complement.
Consider the following random variable :

$$X(A) \coloneqq | \text{ edges between } A \text{ and } B | = |\{\{a, b\} | a \in A, b \in B, \{a, b\} \in E(G)\}.$$

Let's compute $\mathbb{E}(X)$.
For $e = \{u, v\} \in E(G)$ we define the event

$$C_e \coloneqq \{A \in \Omega || A \cap e| = 1\}$$

We have

$$X = \sum_{e \in E(G)} I_{C_e}$$

and therefore

$$\mathbb{E}(X) = \sum_{e \in E(G)} \mathbb{E}(I_{C_e}) = \sum_{e \in E(G)} P(C_e)$$

We compute $P(C_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} > \frac{1}{2}$.
Thus

$$\mathbb{E}(X) = \sum_{e \in E(G)} P(C_e) > \frac{m}{2}$$

□

By theorem, $X(A) > \frac{m}{2}$ *for some* $A \in \Omega$.

Definition 51
Let G *be a graph. A set* $S \subset V(G)$ *is an independent set if no two vertices of* S *are connected by an edge.*
We define $\alpha(G)$ *to be the size of the largest independent set of vertices in the graph* G.

Theorème 53 (Turan's theorem)
For every graph G *we have*

$$\alpha(G) \geq \frac{|V(G)|^2}{2|E(G)| + |V(G)|}$$

Lemme 54
For any graph G *we have*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{\deg v + 1}$$

Preuve
Suppose that the vertices of G *are numberd* $1, \ldots, n$.
Pick a random permutation π *of the vertices.*
Define the set $M(\pi) \subset V(G)$ *by*

$$M(\pi) \coloneqq \{v \in V |\ \textit{all neighbours } u \textit{ of } v \textit{ satisfy } \pi(u) > \pi(v)\ \}$$

$M(\pi)$ *is an independent set of* G .
Therefore $|M(\pi)| \leq \alpha(G)$ *for any permutation* π *, hence*

$$\mathbb{E}(|M(\pi)|) \leq \alpha(G)$$

Now we calculate the expected size of M .
Let $v \in V$, $A_V :=$ the event " $v \in M(\pi)$ " Then

$$P(A_v) = \frac{1}{\deg v + 1} \qquad \square$$

The lemma follows.

Preuve (of Turan's theorem)
Let $|V(G)| = n$ and $d_1, \ldots, d_n$ be the degrees of the vertices of G .
Then

$$\sum_{i=1}^{n} d_i = 2|E(G)|$$

$$\sum_{i=1}^{n} \frac{1}{d_i + 1} \geq \frac{n^2}{d_1 + \ldots + d_n + n} = \frac{n^2}{2|E| + n} \qquad \square$$

Which proves Turan's theorem.