

Discrete Mathematics

David Wiedemann

Table des matières

1	Counting	4
1.1	Finite sets	4
1.2	Bijections	4
1.3	Operations with finite sets	4
1.4	Linear recurrences in matrix form	13
2	Moebius inversion formulas	13
2.1	Moebf	13
2.2	Computing the number of cyclic sequences	16
2.3	Moebius inversion for posets	18
3	Graph Theory	22
3.1	Basic Definitions	22
3.2	Important graphs	24
3.3	Wals and paths	26
3.4	Graph isomorphisms	27
3.4.1	Number of isomorphism classes of graphs	27
3.5	Trees	28
3.5.1	Estimating the number of unlabelled trees	29

List of Theorems

1	Definition (First Numbers)	4
1	Theorème	4
2	Definition (Cartesion product)	4
2	Theorème	4
3	Definition (Disjoint union)	4
3	Theorème	4
4	Definition (Exponential object)	4
4	Theorème	5
5	Definition (Binomial coefficient)	5

5	Proposition	5
6	Proposition	5
7	Proposition	5
8	Proposition	5
9	Théorème	6
10	Proposition	6
11	Théorème (Stirling's formula)	7
12	Théorème (Inclusion-Exclusion Formula)	7
14	Théorème (Multinomial theorem)	8
6	Definition (Generating series)	8
7	Definition (Formal power series)	8
15	Proposition	9
16	Théorème (Generalized binomial theorem)	9
8	Definition (Binary Tree)	9
9	Definition (Fibonacci Sequence)	10
17	Théorème	11
10	Definition (Linear Recurrence)	11
18	Lemme	11
19	Théorème	11
11	Definition (Moebius function)	13
21	Lemme	14
22	Théorème (Moebius inversion formula)	14
12	Definition (Linear sequence)	16
13	Definition (Cyclic sequence)	16
24	Proposition	16
14	Definition (Period of cyclic sequence)	17
15	Definition (Binary relation)	18
16	Definition (Partial Order)	18
17	Definition (Locally finite poset)	19
28	Théorème (Moebius inversion for posets)	19
18	Definition (Incidence algebra $A(X)$)	19
19	Definition (Convolution)	20
20	Definition	20
30	Lemme	20
21	Definition (Zeta function)	21
22	Definition (Moebius function)	21
31	Lemme	22
23	Definition (Graph)	22
24	Definition (Complete graph)	24
25	Definition (Cycle graph)	25
26	Definition (Adjacent vertices)	25

27	Definition (Degree of a vertex)	25
33	Lemme (The hand shake lemma)	26
28	Definition (Walk)	26
29	Definition (Path)	26
30	Definition (Closed Walk)	26
31	Definition (Connected graph)	26
32	Definition (Cycle)	26
33	Definition (Tree)	26
34	Definition (Leaf)	26
34	Lemme	26
35	Lemme	27
35	Definition (Graph isomorphisms)	27
38	Théorème (Cayley)	28
39	Théorème	28
40	Théorème	29

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 (Cartesian 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

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

defined by

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

The cardinality of subsets A and $\phi(A)$ always have different parity.

Since $\phi \circ \phi = \text{Id}$ 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 the number of ways in which one can distribute these 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 $x_1 + \dots + x_n = k$

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 $\psi : \mathcal{A} \rightarrow \mathcal{B}$ in the following way

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

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

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

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)

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

meaning the ratio 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

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

To prove Stirling's formula, we take

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

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

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

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

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

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.

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

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

Example

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)

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

Preuve

Note that

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

is the number of sequences of length k from the letters " x_1, x_2, \dots " such that x_j is used i_j times. \square

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 $a(x)$ has derivatives of all orders at 0.

We can add and multiply formal power series.

However, in general, substitution is not well defined

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

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 called the left subtree and the right subtree.

We denote by b_n the number of binary trees with n vertices. We want to find 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 Taylor's theorem

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

We substitute this into the quadratic equation, which yields

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

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 Catalan's number.

Lecture 6: Fibonacci Numbers

Definition 9 (Fibonacci Sequence)

The sequence is defined by

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

Sat 27 Mar

Theorème 17

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

Preuve

Consider

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

Hence

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

Hence

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

Hence F as derivatives of all orders at 0, writing the Taylor expansion yields

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

Lecture 7: Linear Recurrence Relations

Sat 27 Mar

Definition 10 (Linear Recurrence)

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

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \dots + c_{k-1} a_{n+k-1}$$

for all $n \in \mathbb{Z}$

Lemme 18

Let $f = \frac{P}{Q}$ the ratio of two polynomials with $\deg Q > \deg P$.

Suppose that $Q(x) = (x - \mu_1)^{l_1} \dots (x - \mu_t)^{l_t}$ for some μ_1, \dots , 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

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \dots + c_{k-1} a_{n+k-1}$$

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

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

where λ_i as multiplicity k_i .

Then there exist polynomials P_1, \dots, 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

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

Rewriting this expression yields

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

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

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

Therefore $a(x) = x \frac{P(x)}{Q(x)}$.

Suppose $Q(x) = (x - \mu_1)^{l_1} \dots$

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

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

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

$$-n(n-1) \dots (n-m+1) \quad \square$$

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: Moebius inversion formula

Sat 17 Apr

2 Moebius inversion formulas

2.1 Moebf

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

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

Example

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)

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

is defined as follows.

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

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

then

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

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

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

Set $n^* := \prod p_i$, the square free part of n .

If $d|n$ and $d \nmid n^*$, 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

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

Theorème 22 (Moebius inversion formula)

Let $f, F : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{C}$ be such that

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

Then

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

Moreover, (2) implies (1)

Preuve

Let d and n be positive integers such that $d|n$.

Then $F\left(\frac{n}{d}\right) = \sum_{d'| \frac{n}{d}} f(d')$, therefore

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

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 $F : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{C}$ be any function.

Set $f(n) := \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$, then for $n \in \mathbb{Z}_{\geq 1}$

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

we make the change of variables

$$\{(d, d') | d|n, d'|d\} \rightarrow \{(d'', d') | d''|n, d' | \frac{n}{d''}\}$$

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 :

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

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

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

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

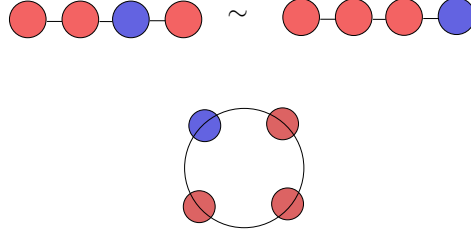


FIGURE 1 – Linear sequence

Example

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

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

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

Definition 14 (Period of cyclic sequence)

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

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

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

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

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

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

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 $a \in R$.

Example

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 antisymmetric, not transitive and not reflexive

Definition 16 (Partial Order)

A partial order on a set A is an antisymmetric reflexive and transitive relation $R \subseteq A \times A$.

A partially ordered set (or poset) is a set together with a partial order

Example

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 $X \subseteq Z$
- Antisymmetric : if $X \subseteq Y$ and $Y \subseteq X$ then $X = Y$

Example

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

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

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

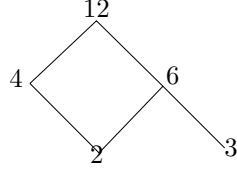


FIGURE 2 – Hasse diagram 12

Definition 17 (Locally finite poset)

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

$$[x, y] := \{z \in X \mid y \leq z \leq x\}$$

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 partially ordered locally finite set with 0.

Suppose that $f : X \rightarrow \mathbb{C}$ is a function.

We define a new function $F : X \rightarrow \mathbb{C}$ by

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

How do we recover f from F ?

Theorème 28 (Möbius inversion for posets)

Given a partially ordered set X , there is a two variable function $M : X \times X \rightarrow \mathbb{R}$ 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 Möbius 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 $f : X^2 \rightarrow \mathbb{C}$ 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 $g(x, x) := f(x, x)^{-1}$.

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

$$\begin{aligned} \delta(x, y) = 0 &= \sum_{x \leq z \leq y} f(x, z)g(z, y) \\ -f(x, x)g(x, y) &= \sum_{x \leq z \leq y} f(x, z)g(z, y) \end{aligned}$$

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

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

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

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

Now we show that the inverse is also true.

Let $F : X \rightarrow \mathbb{C}$ be a function and we define $f : X \rightarrow \mathbb{C}$ by

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

Then,

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

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

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

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

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 $E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}\}$

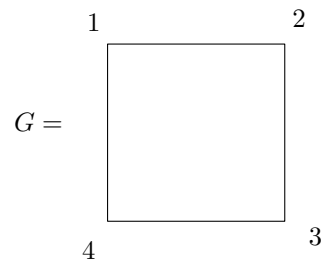


FIGURE 3 – four edged graph

This is called a undirected simple graph.

Non-examples

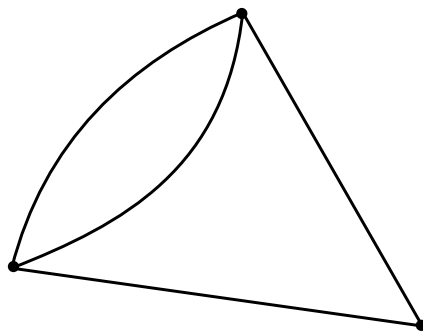


FIGURE 4 – multiple edges

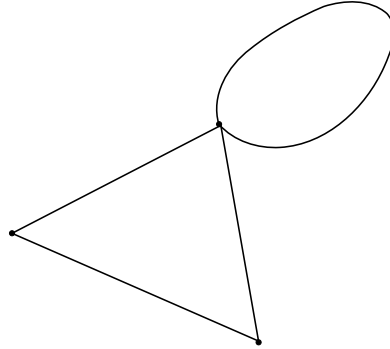


FIGURE 5 – loops

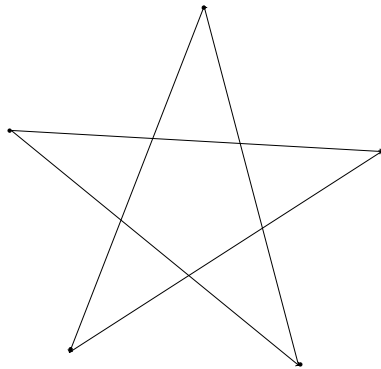


FIGURE 6 – direction of edges

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

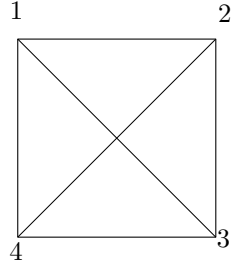


FIGURE 7 – K_4

Definition 25 (Cycle graph)

The cycle C_n is the graph

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

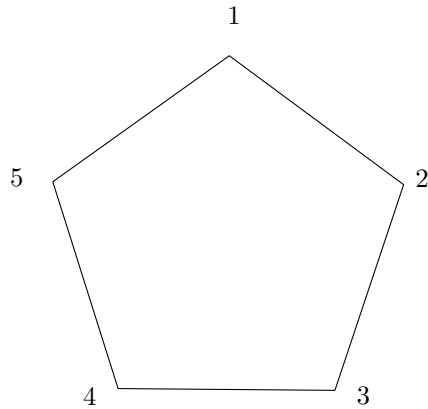


FIGURE 8 – C_5

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 an 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, \dots, 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 $v_1, \dots, v_r \in V$ such that $v_{i \bmod r}$ is adjacent to $v_{i+1 \bmod r}$.

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, \dots, 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 trees 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 $T' := (V \setminus \{v\}, E \setminus \{e\})$.

The new graph T' contains no cycles and is connected, hence T' is a tree.

By induction hypothesis

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

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 $f : V \rightarrow V'$ 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 $\{1, 2, \dots, n\}$. 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 write 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 $1, 2, \dots, n$
- Step 2 : Make the list $= (1, 2, \dots, n)$
- Step 3 : If there are only two numbers left on the list, connect them with an 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 an 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. 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 $[n]$

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

The maps are inverse to each other, namely

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

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, \dots, 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 $\{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_{n-2}\}$ is the set of all leaves of T .

Now we apply algorithm 2 to the sequence (a_1, \dots, a_{n-2}) .

The smallest element of the list $[n]$ which is not in the sequence (a_1, \dots, 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, \dots, a_{n-2}) will give us the tree T_1 with vertices labeled by the set $\{1, \dots, n\} \setminus \{n_0\}$.

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

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

Preuve

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

We know that

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

This max number of trees is $n!$.

Now we show that $T_n \leq 4^n$.

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

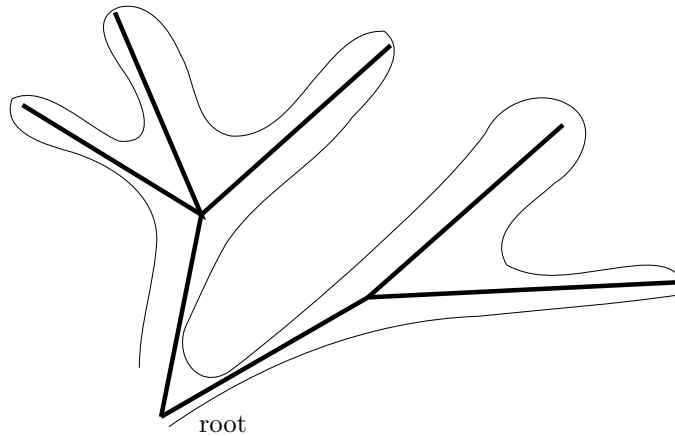


FIGURE 9 – embedded tree

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 $\{+, -\}^{2n-2}$

□