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)

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

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 $\binom{n}{k+1}$ $\square$

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 $x_1 + \ldots + x_n = k$

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

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

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.

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

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

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

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

where

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

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

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

Consider

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

And we use

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

Now we use

$$b(x) \cdot b(x) = \sum_{k=0}^{\infty} \left(\sum_{m=0}^{\infty} b_m b_{k-m} \right) x^k$$

$$= \frac{1}{x}\left(\sum_{k=1}^{\infty} b_k x^k\right) = \frac{1}{x}(b(x) - b_0)$$

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

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

Hence

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

Hence F as derivatives of all 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

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

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

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

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

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

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

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

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

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