Theorem $\chi(G,x)$ is a polynomial.

Proof: Induction on $|E|+|V|$.

case $|E|=0 \Rightarrow \chi(G,x) = x$ is a polynomial

case $|E|>0$: $\chi(G,x) = \chi(G\setminus e,x) - \chi(G/e,x)$

$\overset{\text{I.H.}}{=}$ polynomial − polynomial

$\square$

② combinatorics

Given a finite set A_n for each $n \in \mathbb{N}$, what is $|A_n|$?, e.g. $A_n = \{\pi \mid \pi \text{ permutation of } \{1,\dots,n\}\}$

An answer might be: •) an „explicit formula": $|A_n| = n!$

•) a recurrence: $|A_n| = n|A_{n-1}|$, $|A_0| = 1$

•) an asymptotic formula $|A_n| \sim n^n e^{-n}\sqrt{2\pi n}$, •) an algorithm

counting principals

Let A, B, C be finite sets

•) $A \cap B = \emptyset \Rightarrow |A \uplus B| = |A| + |B|$

•) $|A \times B| = |A| \cdot |B|$

•) $f: |A| \to |B|$ bijective $\Rightarrow |A| = |B|$

Double counting: Let $A = \{a_1, \dots a_n\}$, $B = \{b_1, \dots b_m\}$, $R \in A \times B$, $|R|$?

Let $R_{i,\cdot} := \{(a_i, b) \in R\}$, $R_{\cdot,j} = \{(a, b_j) \in R \mid a \in A\}$

$$\Rightarrow |R| = \sum_{j=1}^{m} R_{\cdot,j} = \sum_{i=1}^{n} R_{i,\cdot}$$

E.g. $\tau(n)$ = average number of divisors of integers between 1 and n

$\tau(6)$: $\begin{array}{c|cccccc} & 1 & \dots & & & & 6 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 & 0 & 1 & 0 \\ \vdots & & \vdots & & & & \end{array}$ → 1 divides everything, 2 divides even numbers, ...

$\Rightarrow \tau(6) = (1+2+2+3+2+4)\frac{1}{6} = \frac{1}{6}(6+3+2+1+1+1) = \frac{1}{n}\sum_{i=1}^{n}\lfloor \frac{n}{i} \rfloor$

sum over columns — sum over rows

we only want to approximate: $\frac{1}{n}\sum_{i=1}^{n}\lfloor \frac{n}{i} \rfloor = \frac{1}{n}\sum \frac{n}{i} + \underbrace{\mathcal{O}(1)}_{\text{constant error}} = \sum \frac{1}{i} + \mathcal{O}(1) \sim \log(n)$

Pigeonhole - Principle (Schubfachprinzip)

$A_1, \dots A_k$, pairwise disjoint, $|A_1 \cup \dots \cup A_k| > k \cdot r$

$\Rightarrow \exists i: |A_i| > r$

alternatively: $f: |A| \to |B|$, $|A| > |B| \Rightarrow \exists b \in B: |f^{(-1)}(b)| \geq 2$ (not injective).

E.g. $\forall g$ odd $\exists i : g \mid 2^i - 1$, $a_i := 2^i - 1 = 1, 3, 7, 15, 31, 63, 127, \dots$

Proof: Consider $a_1, \dots a_g \bmod g$

If $\exists i \; a_i \equiv 0 \; (g)$, we are done, otherwise $\exists i < j : a_i \equiv a_j (g)$

($a_1 \dots a_g$ are g numbers, but can only have $g-1$ remainders mod g different from 0)

$\Rightarrow a_i - a_j = g \cdot a$ for some a

$= 2^i (1 - 2^{j-i})$, then

g odd $\Rightarrow g \mid 1 - 2^{j-i} = -a_{j-i}$

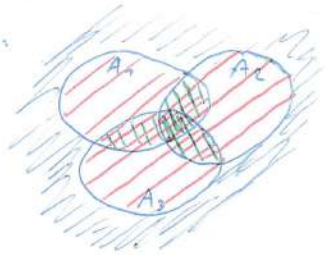
$\square$

Principle of Inclusion / Exclusion (PIE)

Let $E_1 \dots E_n$ be properties, let $A_i = \{x \in A \mid x \text{ has } E_i\}$

$$\Rightarrow |A \setminus \bigcup A_i| = \left(\sum_{\substack{I \neq \emptyset \\ I \subseteq \{1,\dots,n\}}} (-1)^{|I|} \cdot \left| \bigcap_{i \in I} A_i \right| \right) + |A|$$

E.g. $n=3$.



$$|A| - (|A_1| + |A_2| + |A_3|)$$
$$+ |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3|$$
$$- |A_1 \cap A_2 \cap A_3|$$

Sketch of proof: $\left| \bigcup_{i=1}^m A_i \right| \overset{!}{=} - \sum_{\substack{\emptyset \neq I \\ I \subseteq \{1,\dots,m\}}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|$, consider $a \in \bigcup_{i=1}^m A_i$. Let $S := \{i \mid a \in A_i\}$

The element a contributes exactly to summands $I \subseteq S$ on the right side.

$$- \sum_{\substack{\emptyset \neq I \\ I \subseteq S}} (-1)^{|I|} = - \sum_{k=1}^{|S|} \sum_{\substack{|I| = k \\ I \subseteq S}} (-1)^k = - \sum_{k=1}^{|S|} (-1)^k \left(\sum_{\substack{|I| = k \\ I \subseteq S}} 1 \right) = - \sum_{k=1}^{|S|} (-1)^k \binom{|S|}{k} = - \left(\sum_{k=0}^{|S|} (-1)^k \binom{|S|}{k} - 1 \right)$$

$$= -\left((1-1)^{|S|} - 1 \right) = 1$$

$\square$

Balls into boxes (k balls, n boxes), represented by $f : [k] \to [n]$.

Notation: $[n] := \{1, \dots, n\}$

If f is injective, this means balls do not share boxes, if f is surjective, there's no empty box.

	any f	f injective	f surjective
Balls and boxes labelled	n^k	$n(n-1)\cdots(n-k+1)$	not nice
balls unlabelled, boxes labelled	$\binom{n+k-1}{k}$	$\binom{n}{k}$	

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

with this definition $n \in \mathbb{C}$ is possible

because $\underbrace{k!}_{\text{number of possibilities to label } k \text{ balls with } 1,\dots,k}\underbrace{\binom{n}{k}}_{k \text{ plain balls in } n \text{ labelled boxes}} = \underbrace{n(n-1)\cdots(n-k+1)}_{k \text{ balls (labelled) in } n \text{ labelled boxes}}$

Remark: There's no division in combinatorics

Any f, balls unlabelled, boxes labelled:

$$\overset{1}{00|}\ \overset{2}{0|}\ \overset{3}{000|}\ \overset{4}{|}\ \overset{5}{|000} \quad , \begin{matrix} n=5 \\ k=9 \end{matrix}$$

$\rightsquigarrow$ every bit carries information : $00|0|$ $\rightsquigarrow n = 3 = k$

$\#$ bits $= n+k-1$

$\#$ zeros $= k$

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

[f surjective, balls unlabelled, boxes labelled is skipped.]

<u>some binomial identities:</u>

- $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ means n balles and 2 boxes ("x" and "y")

  E.g.: $2xy^3$: 2 possibilities for 1 ball in box x, 3 balls in box y

  $\binom{n}{k} x^k y^{n-k}$: $\binom{n}{k}$ possibilities to place k balls into the x-box, $n-k$ balls into the y-box.

- $\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}$

- $\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}$

- $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, also works for $n \in \mathbb{C}$ (**Lemma**)

proof: easy for $n \in \mathbb{N}$ (exercise)

the left-hand side is a polynomial in n (leading coefficient: $\frac{1}{k!}$), $p(n)$, ($\deg(p(n)) = k$, not needed)

right-hand side is a polynomial in n, $q(n)$, ($\deg(q(n)) = \max(k-1, k) = k$)

$\Rightarrow p(x) = q(x)\ \forall x \in \mathbb{C}$ because $p(n) = q(n)\ \forall n \in \mathbb{N}$

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

Proof: $x, y \in \mathbb{N}$, let $|X| = x$, $|Y| = y$, $X \cap Y = \emptyset$

$\binom{x+y}{n}$: $\#$ subsets of $X \cup Y$ of size n

$\binom{X}{k}\binom{Y}{n-k}$: # subsets of $X \cup Y$ with k elements in X, the rest in Y.

$\square$

Sterling numbers:

Every permutation of $[n]$ is a product of cycles.

Eg: $\underbrace{(10\ 11)}_{\text{(elementary) transposition}}(1\ 3\ 8\ 5\ 2)\underbrace{(6\ 4\ 9)}_{\text{cycle}}\underbrace{(7)}_{\text{fixed point}}$

product: $(1\ 3\ 2)(2\ 3\ 4) = (1\ 3\ 4)(2) \to 2\to 3,\ 3\to 2$

$1\to 1$, $1\to 3$; $3\to 4$, $4\to 4$; $4\to 2$, $2\to 1$

Definition: $s_{n,k}$ is the number of permutations in $\mathfrak{S}_n$ (\mathfrak{S}, permutations of $[n]$) with k cycles, the **stirling number** of the first kind.

E.g.: $s_{n,1} = (n-1)!$, $s_{3,1} = |\{(123),(132)\}|$

$s_{n,n-1} = \binom{n}{2}$

$s_{n,n} = 1$

$s_{0,0} := 0$, $s_{n,0} = s_{0,n} = 0$ for $n > 0$

Theorem $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$

Proof $(1 \dots)(\dots)\cdots(\dots)$

case 1 fixed point: $s_{n-1,k-1}$ possibilities

otherwise: $s_{n-1,k}$ has k cycles, but element one is missing $\Rightarrow n-1$ possibilities to put it without changing the number of cycles.

$\square$

Definition A **set partition** of A is a set of disjoint, non-empty sets with union A.

$S_{n,k}$:= # set partitions of $[n]$ with k parts (or "blocks")

$S_{n,k}$ is called the **Sterling number** of the second kind. ($S_{0,0} := 1$)

$S_{0,0} := 1$, $S_{n,0} = S_{0,n} = 0$, $n > 0$

Theorem $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$

Proof: case $\{n\}$ is a singleton, then $S_{n-1,k-1}$ if removed

otherwise: put n into one of the k blocks : $kS_{n-1,k}$

$\square$

Theorem: $(x)_n := x^{\underline{n}} := x(x-1)\cdots(x-n+1) = \sum_{k=0}^{n} (-1)^{n-k} S_{n,k} x^k$,

$$x^n = \sum_{k=0}^{n} S_{n,k} x^{\underline{k}}$$

Remark $V_n = \{a_0 + \dots + a_n x^n \mid a \in \mathbb{C}\}$ is a vector space, $\{1, x, \dots, x^n\}$ natural basis. $\{1, x, x^{\underline{2}}, \dots, x^{\underline{n}}\}$ is also a basis of V_n. The change of basis matrices are $(S_{n,k})_{n,k}$ and $((-1)^{n-k} s_{n,n})_{n,k}$ (exercises).

Proof of the theorem: Induction on n: $x^{\underline{0}} = 1 = S_{0,0} x^0$ ✓

$$x^{\underline{n}} = x^{\underline{n-1}}(x-n+1) = (x-n+1) \sum_{k=0}^{n-1} (-1)^{n-1-k} S_{n-1,k} x^k = \sum_k (-1)^{n-1-k} S_{n-1,k} x^{k+1} + (n-1) \sum_k (-1)^{n-1-k} S_{n-1,k} x^k$$

$$= \sum_k (-1)^{n-k} S_{n-1,k-1} x^k + (n-1) \sum_k (-1)^{n-1-k} S_{n-1,k} x^k \qquad \square$$

Generating functions

Power series: a sequence $(a_n)_{n \in \mathbb{N}_0}$ ($a_n \in \mathbb{C}$ for example). Consider $\sum_{n \geq 0} a_n z^n$ is the series with **coefficients** a_n. $\sum a_n z^n$ may or may not converge for given complex number $z \in \mathbb{C}$.

A **formal power series**, written $\sum a_n z^n$ is the same information as the sequence $(a_n)_{n \in \mathbb{N}_0}$.

$$\sum_{n=0}^{\infty} a_n z^n \overset{\text{power series}}{:=} \lim_{N \to \infty} \sum_{n=0}^{N} a_n z^n$$, i.e. as a limit of a sequence of complex numbers.

Theorem: $\lim_{N \to \infty} \sum_{n=0}^{N} a_n z^n$ exists if $|z| < \frac{1}{\overline{\lim}_{n \to \infty} \sqrt[n]{|a_n|}} =: R$, $\overline{\lim}$ being the limit superior.

If $|z| = \frac{1}{\overline{\lim} \sqrt[n]{|a_n|}}$ an ad hoc analysis is necessary, if $|z| > \frac{1}{\overline{\lim} \sqrt[n]{|a_n|}}$ it diverges.

Remark. $\{z \mid \sum a_n z^n \text{ converges}\}$ is the **domain** of convergence, essentially a circle centered at the origin.

E.g.: $\sum_{n \geq 0} z^n = \frac{1}{1-z}$ geometric series, $R = 1$.

$\sum_{n \geq 0} \frac{z^n}{n!} = e^z$ exponential series, $R = \infty$ (converges everywhere)

$\sum_{n \geq 0} \binom{\alpha}{n} z^n = (1+z)^\alpha$, $\alpha \in \mathbb{C}$

Theorem (Identity theorem for power series)

$f(z) = \sum_{n \geq 0} a_n z^n$ converges for $|z| < R$ and $R > 0$.

Then $a_n = \frac{f^{(n)}(0)}{n!}$

Corollary: $f(z) = \sum a_n z^n = \sum b_n z^n$ $|z| < R$ $\Rightarrow$ $a_n = b_n \ \forall n$

Operations on formal power series

$A(z) := \sum_{n \geq 0} a_n z^n$, $B(z) := \sum_{n \geq 0} b_n z^n$ (however, z is not a complex number now!)

Write $(a_n) \leftrightarrow A(z)$, $(b_n) \leftrightarrow B(z)$, $(0,1,0,0,\dots) \leftrightarrow z$, $(1,0,0,\dots) \leftrightarrow 1$, ...

- $(\alpha a_n + \beta b_n)_{n \in \mathbb{N}_0} \leftrightarrow: \alpha A(z) + \beta B(z)$
- $\left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n \in \mathbb{N}_0} \leftrightarrow: A(z)B(z)$ (Convolution)
- $(a_n \gamma^n)_{n \in \mathbb{N}_0} \leftrightarrow: A(\gamma z)$
- $(a_{n-1})_{n \in \mathbb{N}_{\geq 1}} \leftrightarrow: zA(z) = a_0 z + a_1 z^2 + \dots$
- $(n a_n)_{n \in \mathbb{N}_0} \leftrightarrow: zA'(z)$

Remark: formal power series are not functions, generating functions are not functions.

E.g.: $\frac{1}{1+z} = \sum_{n \geq 0} (-1)^n z^n$ is an equality of FPS.

$$\frac{z}{(1-z)^2} = z \cdot \left(\frac{1}{1-z}\right)' = \sum_{n \geq 0} n z^n$$

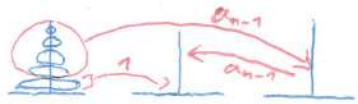
$$\frac{1}{(1-z)^k} = \sum_{n \geq 0} \binom{n+k-1}{k-1} z^n$$

Remark: if $A(z) = B(z)$ as FPS and $A(z)$ and $B(z)$ converge as FPS for $|z| < R$, then $A(z) = B(z)$ as power series.

$\sum_{n \geq 0} n! z^n$ is a FPS which converges only at 0 as a power series.

Why are FPS useful?

E.g.: (Towers of Hanoi:)



Goal: Move disks to another peg, but a disk can only be put at a larger disk.

There is a recurrence for a_n = # moves required to move n disks: $a_n := 1 + 2a_{n-1}$, $a_0 = 0$

We want an explicit expression for a_n:

$$a_n = 2a_{n-1} + 1 \quad | \ z^n$$

$$a_n z^n = 2a_{n-1} z^n + z^n \quad | \ \sum_{n \geq 1}$$

$$\underbrace{\sum_{n\geq 1} a_n z^n}_{=: A(z) - a_0} = 2 \underbrace{\sum_{n\geq 1} a_{n-1} z^n}_{a_0 z + a_1 z^2 + \dots} + \underbrace{\sum_{n\geq 1} z^n}_{\frac{1}{1-z} - 1}$$

$$\Rightarrow \quad A(z) - a_0 = 2z A(z) + \frac{1}{1-z} - 1 \quad \text{as FPS!}$$

$$(1-2z) A(z) = \frac{1}{1-z} - 1 + a_0 \overset{a_0 = 0}{=} \frac{z}{1-z}$$

$$A(z) = \underbrace{\frac{z}{(1-z)(1-2z)}}_{} \quad \text{as FPS! (no function involved)}$$

$$= \frac{-1}{1-z} + \frac{1}{1-2z} = -\sum_{n\geq 0} z^n + \sum_{n\geq 0} 2^n z^n = \sum_{n\geq 0} \underbrace{(2^n - 1)}_{a_n} z^n$$

E.g.: $F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n,\ n \geq 0$ (Fibonacci)

$$F(z) := \sum_{n\geq 0} F_n z^n$$

$$\sum_{n\geq 0} F_{n+2} z^{n+2} = \sum_{n\geq 0} F_{n+1} z^{n+2} + \sum_{n\geq 0} F_n z^{n+2}$$

$$F(z) - F_0 - F_1 z = z\left(F(z) - F_0\right) + z^2 F(z)$$

$$(1 - z - z^2) F(z) = z F_0 + F_0 + F_1 z$$

$$F(z) = \frac{z}{1 - z - z^2} = \frac{\frac{1}{\sqrt{5}} \cdot \frac{1-\sqrt{5}}{2}}{z - \frac{-1+\sqrt{5}}{2}} + \frac{-\frac{1}{\sqrt{5}} \frac{1+\sqrt{5}}{2}}{z - \frac{-1-\sqrt{5}}{2}}$$

Exkurs Partialbruchzerlegung:

$$\frac{z}{(z-2)(z-5)^2} = \frac{A}{z-2} + \frac{B}{z-5} + \frac{C}{(z-5)^2} \quad \Big| \ (z-2)$$

$$\frac{z}{(z-5)^2} = A + (z-2) \cdot (\text{something which exist for } z = 2)$$

$$z = 2: \quad \frac{z}{(z-5)^2} = A + 0 \cdot \text{something} \quad \Rightarrow A = \frac{2}{9} \quad \text{(multiplicity doesn't always work)}$$

$$\frac{z}{z-2} = (z-5)\left((z-5)\frac{A}{z-2} + B\right) + C$$

$$z = 5: \quad \frac{5}{3} = C \quad \rightsquigarrow \ \Big| (z-5) \text{ doesn't work but we can plug in } C$$

$$\text{plug in } C: \quad \underbrace{\frac{z}{(z-2)(z-5)^2} - \frac{5}{3}\frac{1}{(z-5)^5}}_{} = \frac{A}{z-2} + \frac{B}{z-5} \quad \Big| (z-5) \text{ now works:}$$

$$= \frac{z - \frac{5}{3}(z-2)}{(z-2)(z-5)(z-5)} = -\frac{2}{3}\frac{1}{(z-2)(z-5)}$$

$$z = 5: \quad [\dots]$$

~~Theorem: [illegible] homogeneous [illegible] of order k~~

(start topic again)

In general $a_{n+k} + q_1 a_{n+k-1} + \dots + q_k a_n = 0$ for $n \geq 0$, $a_0, \dots a_{k-1}$ are given as initial conditions. We are interested in $A(z) = \sum_{n \geq 0} a_n z^n \quad \Big| \cdot z^{n+k}, \sum_{n \geq 0}$

$$\Rightarrow \sum_{n \geq 0} a_{n+k} z^{n-k} + q_1 \sum_{n \geq 0} a_{n+k-1} z^{n+k} + \dots + q_k \sum_{n \geq 0} a_n z^{n+k} = 0$$

$$A(z) - a_0 - a_1 z - \dots - a_{k-1} z^{k-1} + q_1 z \left(A(z) - \sum_{i=0}^{k-2} a_i z^i \right) + \dots + q_k z^k \left(A(z) \right) = 0$$

$$A(z) \underbrace{\left(1 + q_1 z + \dots + q_k z^k \right)}_{1 - z - z^2 \text{ for Fibonacci}} = \underbrace{p(z)}_{F_0 + z(F_1 - F_0)}$$

, p a polynomial at most $k-1$ (essentially the initial condition)

$=: q(z)$ contains as information the recurrence, has degree k

$$\Rightarrow A(z) = \frac{p(z)}{q(z)}$$

We have proven that $A(z)$ is a rational function!

partial fraction decomposition: $q(z) = \prod_{i=1}^{r} (z - z_i)^{\lambda_i}$, $\sum_{i=1}^{r} \lambda_i = k$

Fibonacci: $q(z) = \left(z - \frac{1+\sqrt{5}}{2}\right)\left(z - \frac{1-\sqrt{5}}{2}\right)$

Ansatz: $\frac{p(z)}{q(z)} = \sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{A_{i,j}}{(z - z_i)^j}$

(*) goal: expand into generating function

example: $\frac{1}{3z-2} \; \frac{-\frac{1}{2}}{-\frac{1}{2}} = \frac{a}{1 - qz} = a \cdot \sum (qz)^n$

$$\overset{(*)}{=} \sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{A_{ij}}{(1 - \frac{z}{z_j})^j}$$

$$= \sum_{n \geq 0} \overbrace{\left(A_{11} + \binom{n+1}{1} A_{12} + \dots + \binom{n+\lambda_1 - 1}{\lambda_1 - 1} A_{1\lambda_1} \right)}^{p_1(n) \text{ polynomial of degree } \lambda_1 - 1} \left(\frac{z}{z_1}\right)^n + \dots +$$

$$+ \sum \left(A_{i1} + \binom{n+1}{1} A_{i2} + \dots \right) \left(\frac{z}{z_i}\right)^n + \dots$$

$$= \sum_{n \geq 0} \underbrace{\left(p_1(n) \left(\frac{1}{z_1}\right)^n + \dots + p_r(n) \left(\frac{1}{z_r}\right)^n \right)}_{= a_n} z^n$$

Definition: $\chi(z) = z^k + q_1 z^{k-1} + \dots + q_k$ is called the characteristic polynomial of the recurrence relation.

Remark: $\left(\chi(z) = q(z) \big|_{z^k u \to z^{n-k}} \right)$ $\rightsquigarrow$ each root is flipped to its multiplicative inverse

$$\chi(z) = \prod_{i=1}^{r} \left(z - \frac{1}{z_i}\right)^{\lambda_i}$$

E.g.: Fibonacci $F_n = \frac{1}{\sqrt{5}}\Big(\underbrace{\frac{1+\sqrt{5}}{2}}_{\approx 1{,}5}\Big)^n - \frac{1}{\sqrt{5}}\Big(\underbrace{\frac{1-\sqrt{5}}{2}}_{\approx -0{,}5}\Big)^n \in \mathbb{N}$

[for large n: $\Rightarrow F_n \approx \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n$]

unlabelled enumeration

Definition: A binary tree is a rooted tree where each node has no sucessors or exactly two successors. $\mathcal{B}$ is the set of all binary trees.

$$\mathcal{B} = \{\bullet\} \,\dot\cup\, \{ \underset{B_1 \quad B_2}{\overset{\bullet}{\wedge}} \mid B_1, B_2 \in \mathcal{B}\}$$

$B(z) = \sum_{n\geq 0} b_n z^n$ where b_n is the number of binary trees with n internal nodes

$$\Rightarrow B(z) = 1 + \underbrace{z}_{\text{node added}} \underbrace{B(z)^2}_{B_1 \cdot B_2}$$

can't apear because $\frac{1}{z}$ is not a generating function

$$\Rightarrow B(z) = \frac{1 \overset{(+)}{-} \sqrt{1-4z}}{2} = 1 + z + 2z^2 + 5z^3 + 14z^4 + \dots$$ (Catalan numbers, exercise)

dictionary for unlabelled structures: $(\mathcal{A} \,\dot\cup\, \mathcal{B})(z) = \mathcal{A}(z) + \mathcal{B}(z)$

$(\mathcal{A} \times \mathcal{B})(z) = \mathcal{A}(z) \cdot \mathcal{B}(z) = \sum_{n\geq 0} \sum_{k=0}^{n} a_k b_{n-k} z^n$

size of (a,b) is the size of a + size of b

$$\underbrace{1}_{\text{empty sequence}} + \underbrace{\underbrace{(z}_{\text{size 1}} + \underbrace{z^2)}_{\text{size 2}}}_{\text{one object}} + \underbrace{\underbrace{(z+z^2)^2}_{\text{sequences of length 2 but not necessary size}}}_{\text{pairs of objects}} + \dots = \frac{1}{1-(z+z^2)}$$

E.g. sequences of 1's and 2's (compositions with parts in $\{1,2\}$)

$\emptyset$, 1, $1+1$, 2, $1+1+1$, $2+1$, $1+2$, $1+1+1+1$, $2+1+1$, $1+2+1$, $1+1+2$, $2+2$

(size 0), (size 1), (size 2), (size 3), (size 4)

[$A(z) = \sum_{n\geq 0} (\#\text{ elements of size } n)\, z^n$] Notation: $[z^n]A(z) = a_n$ — extract coefficient of a generating function

$$(\text{sequences of objects in } \mathcal{A})(z) = 1 + A(z) + A^2(z) + \dots = \frac{1}{1-A(z)}$$

Example: red, blue and yellow balls, 2 or 3 red, at least one blue, at most one yellow, n balls, what's the generating function?

$$\underbrace{2 \text{ or } 3 \text{ red}}_{(r^2+r^3)}, \underbrace{\text{at least one blue}}_{(b+b^2+b^3+\dots)=\left(\frac{b}{1-b}\right)}, \underbrace{\text{at most one yellow}}_{(1+y)}$$

In total: $A(z) = \left((rz)^2 + (rz)^3\right) \frac{b \cdot z}{1-bz} (1+yz)$

for n balls: $[z^n]A(z)$ = generating function in r, b, y

$$A(z)\Big|_{r=b=y=1} = (z^2+z^3)\left(\frac{z}{1-z}\right)(1+z) = \frac{z^3+2z^4+5z^5}{1-z} \quad \text{so } [z^n]A(z) = 4 \text{ for } n \geq 5$$

Example: combinations without repetitions: balls $a_1, a_2, \dots, a_N$

generating function for selecting balls (selecting a ball or not)

$(1+a_0)(1+a_2)\cdots(1+a_N)$, set $a_i := z$ (not caring which ball)

$$(1+z)^N = \sum_{n\geq 0} \binom{N}{n} z^n$$

with repetitions: $\left(\sum_{n\geq 0} a_1^n\right)\left(\sum_{n\geq 0} a_2^n\right)\cdots\left(\sum_{n\geq 0} a_N^n\right)$, $a_i := z$ $\left(\frac{1}{1-z}\right)^N = \sum_{n\geq 0}\binom{n+N-1}{n} z^n$

Labelled enumeration

exponent generating function: $\sum_{n\geq 0} a_n \frac{z^n}{n!} = \hat{A}(z)$

unlabelled enumeration: $\sum_{n\geq 0} a_n z^n = A(z)$, a_n = # objects of size n

Example: permutations: $A(z) = \sum_{n\geq 0} n!\, z^n$, cyclic permutations: $\hat{A}(z) = \sum_{n\geq 0} n! \frac{z^n}{n!} = \frac{1}{1-z}$

dictionary:

$$\widehat{(A \cup B)}(z) = \hat{A}(z) + \hat{B}(z)$$

$$\widehat{(A \times B)}(z) = \hat{A}(z) \cdot \hat{B}(z)$$

$$\widehat{(\text{sets of objects})}(z) = e^{\hat{A}(z)}$$

$$\widehat{(\text{cycles of objects in } A)}(z) = \log \frac{1}{1-\hat{A}(z)}$$

Remark: $\widehat{A\cdot B}(z) = \hat{A}(\hat{B}(z))$

Definition: Let A and B be sets closed under relabelling. Let $A[1,2,\dots,n]$ be be the set of objects with labels $1,2,\dots,n$.

Then $A\times B[1,\dots,n]$ is the set of pairs (a,b) with $a\in A$, $b\in B$ such that the total set of labels is $1,\dots,n$.

Formally, $A\times B[1,\dots n] = \dot{\bigcup}_{\substack{U\subseteq\{1,\dots,n\}\\ V=\{1,\dots,n\}\setminus U}} A[U]\times B[V]$

$$[z^n]\,\widehat{A\times B}(z) = \sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}$$

$$\widehat{A\times B}(z) = \sum_{n\geq 0}\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}\frac{z^n}{n!} = \sum_{n\geq 0}\sum_{k=0}^{n}\frac{\cancel{n!}}{k!(n-k)!}\frac{1}{\cancel{n!}}a_k b_{n-k}\, z^k z^{n-k}$$

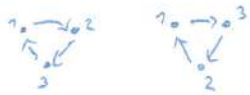
$$= \sum_{n\geq 0}\sum_{k=0}^{n}\frac{a_k z^k}{k!}\frac{b_{n-k}z^{n-k}}{(n-k)!} = \sum_{k\geq 0}\sum_{l\geq 0}\frac{a_k z^k}{k!}\frac{b_l z^l}{l!} = \hat{A}(z)\hat{B}(z)$$

Definition Let A be a set closed under relabelling. Then $\mathrm{set}(A)$ is the set of objects $\{a_1,\dots,a_i\}$, $a_i\in A$, such that the total set of labels is $\{1,\dots n\}$.

E.g.: sets of cycles with labels $\{1,2,3,4\}$.

cycles of $\{1\}$, ... 

cycles of $\{1,2\}$, ... 

cycles of $\{1,2,3\}$, ... 

E.g.: $A[1,2,3] = \{1,2,3\}$ is not closed under relabelling. It produces all objects with labels $\{1,2,3\}$

E.g: $A[1,2] := \{12, 21\}$, $B[1,2] := \{12, 21\}$

$$A \times B[1,2,3,4] = \{(13,42), (12,34), (14,23), (31,42), (21,34), (41,23), (13,24), (12,43), (14,32), (31,24), (21,43), (41,32)\}$$

cardinality: 24

$A[\heartsuit, \lightning] = \{\heartsuit\lightning, \lightning\heartsuit\}$, $A[\heartsuit] = \{\ \}$

$\widehat{\text{sets}}(z) = e^z$, $e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots$

$\widehat{\text{cycles}}(z) = \log \frac{1}{1-z}$

$\widehat{\text{sets}(\text{cycles})}(z) = e^{\log \frac{1}{1-z}} = \frac{1}{1-z} = \widehat{\text{permutations}}(z)$

$\mathbb{B}$:= sets of non-empty sets

$\hat{\mathbb{B}}(z) = e^{(e^z - 1)}$ is the <u>(exponential) generating function</u> for set partitions.

Partially ordered sets

Definition. A partial order is a set P together with a relation $\leq$, such that

- $a < b \Rightarrow b \not< a$ (antisymmetry)
- $a \not< a$
- $a < b,\ b < c \Rightarrow a < c$ (transitivity)

(poset, partially ordered set)

Notation: $a \leq b$ means $a < b$ or $a = b$.

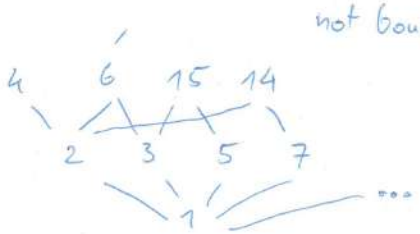
The <u>Hasse-diagram</u> is the digraph with vertices P and (a,b) is an arc if $a < b$ and $\nexists c: a < c < b$.

Remark: equivalently define $(P, \leq)$ with $\leq$ reflexive, transitive.

E.g.:

$(\mathbb{N}_{\geq 1}, |)$

not bound,



$(\mathbb{N}_{\geq 1}, \leq)$

not bound, is a linear order

Definition A minimal element is an $a \in P$ such that $\forall\, b \in P : a \leq b$,
a maximal element is an $a \in P$, such that $\forall\, b \in P : b \leq a$.

Definition: An interval is a subset $[x,y] := \{ z \mid x \leq z \leq y \}$ of P

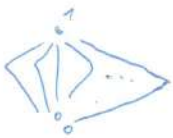
P is bounded if $\exists\, M \leq P : \forall x \in P\ \exists y \in M : x \leq y$,

$\exists\, M \leq P : \forall x \in P\ \exists y \in M : y \leq x$

$(P, \leq)$ is locally finite if all intervals have finite cardinality.

$$|[x,y]| < \infty \quad \forall x,y \in P.$$

E.g.:



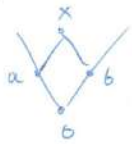
is not locally finite

$P = \{ x \in \mathbb{Q} \mid 0 \leq x \leq 1 \}$, $a \leq b$ if $a = 0$ or $b = 1$

Definition Let $(P, \leq)$ be locally finite, bounded (or at least bounded below)

$f : P \to \mathbb{R}$, $\quad S_f(x) := \sum_{z \leq x} f(z)$

E.g.:



$S_f(x) = f(0) + f(a) + f(b) + f(x)$

Goal: find f for given $S_f(x)$.

Definition: Let $(P, \leq)$ be a poset, locally finite with a minimal element "0".

$\mu : P \times P \to \mathbb{R}$ is called Möbiusfunction of P if and only if

$$\forall x,y : \sum_{z \in [x,y]} \mu(z,y) = \delta_{xy} = \begin{cases} 0 & x \neq y \\ 1 & x = y \end{cases}$$

Remark This relation determines μ uniquely.

If $x \not\leq y$, then $\mu(x,y) := 0$

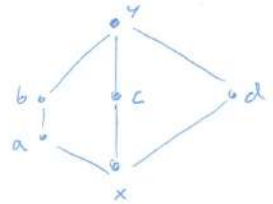
Examples: •) $[x,x] = \{x\} \Rightarrow \mu(x,x) = 1$

•) $[x,y] = \{x,y\} \Rightarrow \mu(x,y) + \mu(y,y) = 0$, $\mu(y,y) = 1 \Rightarrow \mu(x,y) = -1$

•) $(\mathbb{N}, \leq)$: $\mu(n,n) = 1$, $\mu(n,n+1) = -1$, $\mu(n,m) = 0 \quad \forall m \geq n+2$ or $m < n$

because $\mu(n,n+2) = -\underbrace{\mu(n,n+1)}_{-1} - \underbrace{\mu(n,n)}_{1}$

·)



$$\mu(x,y) = -\Big(\mu(a,y) + \underbrace{\mu(b,y)}_{-1} + \underbrace{\mu(c,y)}_{-1} + \underbrace{\mu(d,y)}_{-1} + \underbrace{\mu(y,y)}_{1}\Big)$$

$$\mu(a,y) = -\big(\underbrace{\mu(b,y)}_{-1} + \underbrace{\mu(y,y)}_{1}\big) = 0$$

$$\Rightarrow \mu(x,y) = 2$$

Definition: Let $(P_1, \leq_1) \times (P_2, \leq_2) := (P_1 \times P_2, \leq_3)$ (product poset) has

$(x_1, x_2) \leq_3 (y_1, y_2) \;:\Leftrightarrow\; (x_1 \leq_1 y_1)$ and $(x_2 \leq_2 y_2)$

Theorem If P_1 and P_2 both have a unique minimal element, then $P_1 \times P_2$ has a unique minimal element and $\mu_{P_1 \times P_2}(\vec{x}, \vec{y}) = \mu_{P_1}(x_1, y_1)\,\mu_{P_2}(x_2, y_2)$

Proof is left as exercise (plug in definition).

Example: $A = \{a_1, \dots a_n\}$, consider $(2^A, \subseteq) \simeq (\{0,1\}, \leq)^n$ componentwise not lexicographic

binary strings of length n

e.g. $x = \{a_2, a_5\}$, $y = \{a_1, a_2, a_3, a_5\}$, $n = 5$
≈ 01001 ≈ 11101

then $\mu(x,y) = \mu(0,1)\mu(1,1)\mu(0,1)\mu(0,0)\mu(1,1)$
$= (-1) \cdot 1 \cdot (-1) \cdot 1 \cdot 1 = 1$

In general: (for this example) $\mu(x,y) \in \{-1, 1\}$ (if x, y are comparable, $x \leq y$)

$$\Rightarrow \mu(x,y) = (-1)^{\#\text{different positions}} = (-1)^{|x|-|y|} = (-1)^{|y|-|x|} = (-1)^{|y \setminus x|}$$

Theorem (Möbius Inversion): Let $(P, \leq)$ be locally finite with "0" (unique minimal element).

$f: P \to \mathbb{R}$, $S_f(x) = \sum_{z \in [0,x]} f(z) \quad \Rightarrow \quad f(x) = \sum_{z \in [0,x]} S_f(z)\,\mu(z,x)$

Proof: $$\sum_{0 \leq z \leq x} S_f(z)\,\mu(z,x) = \sum_{0 \leq z \leq x} \sum_{0 \leq y \leq z} f(y)\,\mu(z,x) \overset{\text{double counting}}{=} \sum_{0 \leq y \leq x} \sum_{y \leq z \leq x} f(y)\,\mu(z,x)$$

$$= \sum_{y \in [0,x]} f(y) \sum_{z \in [y,x]} \mu(z,x) = \sum_{y \in [0,x]} f(y) \cdot \delta_{yx} = f(x)$$

$\square$

Example: $(\mathbb{N}, \leq)$, $\mu(m,n) = \begin{cases} 1 & m = n \\ -1 & m+1 = n \\ 0 & \text{otherwise} \end{cases}$

$f: \mathbb{N}_0 \to \mathbb{R}$, $S_f(n) = \sum_{k=0}^{n} f(k) \Rightarrow f(n) = \sum_{k=0}^{n} S_f(k)\mu(k,n) = \begin{cases} S_f(n) - S_f(n-1), \\ S_f(n) & \text{if } n = 0 \end{cases}$

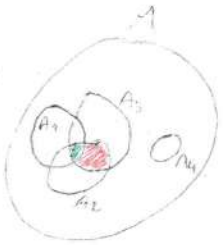
Example (PIE): $A_1, \dots A_m \subseteq M$, consider $(2^{\{1,\dots m\}}, \supseteq)$ poset of indices

$I \subseteq \{1,\dots,m\}$, $f(I) := \left| \bigcap_{i \in I} A_i \cap \bigcap_{j \in \{1,\dots m\} \setminus I} \overset{\text{complement}}{\bar{A}_j} \right| = |\text{elements precisely in all } A_i, i \in I|$

$S_f(I) = \sum_{J \supseteq I} f(J) = \left| \bigcap_{i \in I} A_i \right|$

$= |\text{elements in } A_i \text{ for } i \in I|$

e.g.:



$f(2,3) = |A_2 \cap A_3 \cap \bar{A}_1 \cap \bar{A}_4|$

$S_f(2,3) = \underline{f(2,3)} + \underline{f(1,2,3)} + f(2,3,4) + \underbrace{f(1,2,3,4)}_{\text{empty}}$

Möbius inversion: $f(I) = \sum_{J \supseteq I} S_f(J)\mu(J,I) = \sum_{J \supseteq I} (-1)^{|I|+|J|} \left| \bigcap_{j \in J} A_j \right|$

In particular: $f(\emptyset) = \left| \bigcap_{j \in \{1,\dots m\}} \bar{A}_j \right| = \sum_{J \subseteq \{1,\dots m\}} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right|$

Example: "classical" number theoretic Möbius function.

$(\mathbb{N}_+, |)$, $m = p_1^{e_1} \cdots p_r^{e_r}$, $p_i \in \mathbb{P}$, $e_i \in \mathbb{N}_0$

$n = p_1^{f_1} \cdots p_r^{f_r}$, $m | n \Leftrightarrow e_i | f_i \ \forall i$

$\cong (\mathbb{N}_0, \leq) \times (\mathbb{N}_0, \leq) \times \dots$

finite entries $\neq 0$ in the infinite product

$\mu(n) := \mu_{(\mathbb{N}_+,|)}(1,n) = \mu_{(\mathbb{N},|)}(0,e_1)\mu_{(\mathbb{N},|)}(0,e_2) \cdots \mu_{(\mathbb{N},|)}(0,e_r)\underbrace{\mu_{(\mathbb{N},|)}(0,0)}_{=1} \cdots$

$\mu(0,k) = \begin{cases} 1 & k = 0 \\ -1 & k = 1 \\ 0 & k > 1 \end{cases} \Rightarrow \mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = p_1 \cdots p_r, \ p_i \neq p_j \text{ for } i \neq j \\ 0 & \text{otherwise} \end{cases}$

conclusion:

$f: \mathbb{N}_+ \to \mathbb{R}$, $S_f(n) = \sum_{d | n} f(d)$

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

Remark $\mu_{(\mathbb{N},|)}(m,n) = \mu\left(\frac{m}{n}\right)$ e.g.: $[m,n] \cong [1, \frac{n}{m}]$

$[2,24]$

Lattices (Verband in DE)

Definition. $(P, \leq)$ poset, $x, a, b \in P$, $a \leq x \leq b$ ($\Rightarrow$ a lower bound/b upper bound for x). Let $x \vee y$ ("join") be the smallest common upper bound of x and y and $x \wedge y$ ("meet") the largest common lower bound of x and y, if it exists.

Notation: $\bigvee_{x \in V} x := x_1 \vee x_2 \vee \dots \vee x_n$

basic properties: $x \vee y = y \vee x$, $x \vee x = x$, $(x \vee y) \vee z = x \vee (y \vee z)$, $a \vee (a \wedge b) = a = a \wedge (a \vee b)$

Definition: L is a **lattice** if $\forall x, y \in L : \exists\, x \vee y$ and $x \wedge y$.

J is a **join-semilattice** if $\forall x, y \in L : \exists\, x \vee y$, analouge **meet-semilattice**

L is a **complete lattice** if $\forall X \subseteq L : \exists \bigvee_{x \in X} x$ and $\bigwedge_{x \in X} x$

Example: $(2^M, \subseteq)$ is a lattice: $A, B \subseteq M \Rightarrow A \vee B := A \cup B$, $A \wedge B := A \cap B$

Lemma: L lattice, $x, y, s, t \in L$

$x \leq s,\ y \leq s \Rightarrow x \vee y \leq s$

$x \geq t,\ y \geq t \Rightarrow x \wedge \geq t$

$x \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x \wedge y = x$

1 is the neutral el. for $\wedge$, 0 is neutral for $\vee$

Lemma L a finite meet-semi-lattice with a 1-element (larger than all other elements). Then L is a lattice.

Proof: $x, y \in L$, $B = \{u \in L \mid x \leq u,\ y \leq u\}$, $1 \in B \Rightarrow B \neq \emptyset$

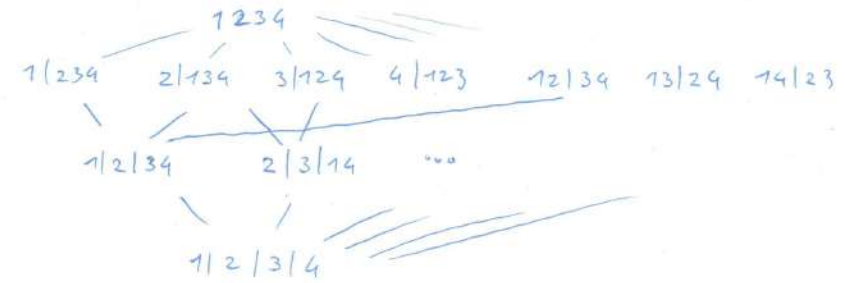
$|B| \neq < \infty \Rightarrow B = \{u_1, \dots u_m\}$, $u := \bigwedge_{i=1}^{m} u_i \in B$

$\Rightarrow u =: x \vee y$ (minimal element in B) (not shown: unique) $\square$

Example: $\Pi_n = \{\pi$ a set partition of $\{1, \dots n\}\}$

$(\Pi_n, \text{refinement})$ is a lattice. 1 is the set partition with 1 block: $\{\{1, \dots, n\}\}$, 0 is the set of all singletons $\{\{1\}, \dots \{n\}\}$.

$\alpha, \beta \in \Pi_n$: $\alpha \wedge \beta$: set partition, where i, j are in the same block if and only if they are in the same block in α and β



Theorem L lattice with $0, 1$, $b \neq 1$, $b \in L$

$$\Rightarrow \quad \mu(0,1) = - \sum_{\substack{x : x \wedge b = 0 \\ x \neq 0}} \mu(x,1)$$

Proof:

$$\overset{\text{since } 0 \wedge b = 0}{(*) \Leftrightarrow} \quad 0 = \sum_{x : x \wedge b = 0} \mu(x,1)$$

$$N(y) := \sum_{x : x \wedge b = y} \mu(x,1) \quad \text{for } y \leq b$$

given x and $b \Rightarrow y = x \wedge b \leq b$ only one y

sum over an interval of the Möbius function

$$S(b) = \sum_{y : y \leq b} N(y) = \sum_{y \leq b} \sum_{x \wedge b = y} \mu(x,1) \overset{!}{=} \sum_{x \in L} \mu(x,1) = \sum_{x \in [0,1]} \mu(x,1) = 0$$

$$\overset{\text{Möbius inversion}}{\Rightarrow} \quad N(b) = \sum_{y \leq b} \underbrace{S(y)}_{=0} \mu(y,b) = 0 \quad \Rightarrow \quad N(0) = 0$$

$\square$

Corollary: $\mu_{\Pi_n}(0,1) = (-1)^{n-1}(n-1)!$

Proof: exercise (induction, choose $b = \{\{1 \dots n-1\}, \{n\}\}$ (split of largest element))

3 Number theory

Definition $a, b \in \mathbb{Z}$, then $a | b :\Leftrightarrow \exists c \in \mathbb{Z} : a \cdot c = b$ (a divides b)

(more generally for any ring, e.g. $\mathbb{Z}[x]$, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, ...)

Definition: $a, b \in \mathbb{Z}$, $d = \gcd(a,b) \Leftrightarrow$ •) $d | a$, $d | b$ (greatest common divisor)
•) $t | a$, $t | b \Rightarrow t | d$

$b > 0 \Rightarrow \exists\, q, r \in \mathbb{Z}$: •) $a = bq + r$ (division with remainder)
•) $0 \leq r < b$

Euclidian algorithm (theorem)

$a = bq_0 + r_0$ $\Rightarrow$ $b > r_0 > r_1 > \dots > r_k > 0$

$b = r_0 q_1 + r_1$ $\Rightarrow$ $r_k = \gcd(a,b)$

$r_0 = r_1 q_2 + r_2$

$\vdots$

$r_{k-2} = r_{k-1} q_k + r_k$, $r_{k-1} = r_k q_{k+1}$ (no remainder anymore)