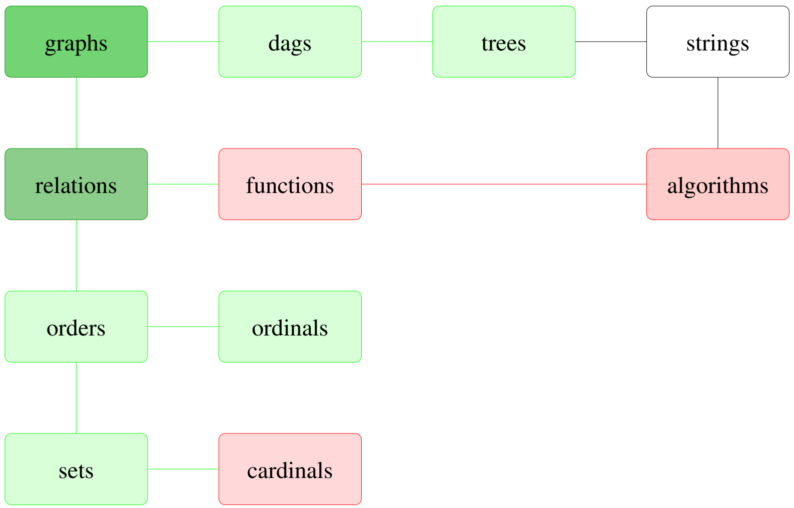
Summary last week

- RSA public-key cryptography based on:
- fundamental theorem of arithmetic (using Bézout)
- Fermat's little theorem
- fast exponentiation using binary representation of exponent
- Chinese remainder theorem (versions: bijective, Bézout, RSA)

Course themes

- directed and undirected graphs
- relations and functions
- orders and induction
- trees and dags
- finite and infinite counting
- elementary number theory
- Turing machines, algorithms, and complexity
- decidable and undecidable problem

Discrete structures



Asymptotic growth

Definition (Big-O)

Let $g\colon \{\ell, \ell+1, \ell+2, \ldots\} \to [0, \infty)$ with $\ell \in \mathbb{N}$.
The set $\mathrm{O}(g)$ comprises all functions

$$f\colon \{k, k+1, k+2, \ldots\} \to [0, \infty) \quad \text{with} \quad k \in \mathbb{N},$$

for which there exists a positive real number c, and a natural number m with $m \geq k$ and $m \geq \ell$, such that for all natural numbers $n \geq m$:

$$f(n) \leq c \cdot g(n)$$

That is, $f \in \mathrm{O}(g)$, if for sufficiently large arguments of f, its value is bounded from above by a constant multiple of the value of g.

Big-Omega and Big-Theta

Definition (Big-Omega and Big-Theta)

- The set $\Omega(g)$ comprises the functions

$$f\colon \{k, k+1, k+2, \ldots\} \to [0, \infty) \quad \text{with} \quad k \in \mathbb{N}\,,$$

for which there exists a positive real number c, and a natural number m with $m \geq k$ and $m \geq \ell$, such that for all natural numbers $n \geq m$:

$$f(n) \geq c \cdot g(n)$$

That is, $f \in \Omega(g)$, if for sufficiently large arguments of f, its value is bounded from below by a constant multiple of the value of g.

- Finally,

$$\Theta(g) := \mathrm{O}(g) \cap \Omega(g)\,.$$

Example

Let $f\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto 3n^2 + 5n + 100$ and $g\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto n^2$. Then $f \in \Theta(g)$.

Example

Let $f\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto 3n^2 + 5n + 100$ and $g\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto n^2$. Then $f \in \Theta(g)$.

Proof.

- We show $f \in \mathrm{O}(g)$.
  We choose $c = 4$ and $m = 13$ in the definition. We have $f(n) \leq 4 \cdot g(n)$ for all $n \geq 13$.
- We show $f \in \Omega(g)$.
  We choose $c = 1$ and $m = 0$ in the definition. By mathematical induction one shows $f(n) \geq g(n)$ for all $n \geq 0$.
- Therefore, $f \in \Theta(g)$.

Example

Let $f\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto 3n^2 + 5n + 100$ and $g\colon \mathbb{N} \to \mathbb{N}$ with $n \mapsto n^2$. Then $f \in \Theta(g)$.

Proof.

- We show $f \in \mathrm{O}(g)$.
  We choose $c = 4$ and $m = 13$ in the definition. We have $f(n) \leq 4 \cdot g(n)$ for all $n \geq 13$.
- We show $f \in \Omega(g)$.
  We choose $c = 1$ and $m = 0$ in the definition. By mathematical induction one shows $f(n) \geq g(n)$ for all $n \geq 0$.
- Therefore, $f \in \Theta(g)$.

∎

Infima, suprema, and limits

Definition

Let $\leq$ be a partial order on M and $S \subseteq M$.

- We say $y \in M$ is an infimum of S, if for all $x \in S$ $y \leq x$ and for all $z \in M$ having that property, $z \leq y$ (greatest lower bound).
- We say $y \in M$ is a supremum of S, if for all $x \in S$ $y \leq x$ and for all $z \in M$ having that property, $y \leq z$ (least upper bound).

Infima, suprema, and limits

Definition

Let $\leq$ be a partial order on M and $S \subseteq M$.

- We say $y \in M$ is an infimum of S, if for all $x \in S$ $y \leq x$ and for all $z \in M$ having that property, $z \leq y$ (greatest lower bound).
- We say $y \in M$ is a supremum of S, if for all $x \in S$ $y \leq x$ and for all $z \in M$ having that property, $y \leq z$ (least upper bound).

Remark

Infima and suprema need not exist

Definition

Let $f\colon \mathbb{N} \to [0,\infty)$ be a function. Then

$$\lim_{n\to\infty} f(n) = L$$

if for all positive reals ε, there exists $m \in \mathbb{N}$, such that $|f(n) - L| < \varepsilon$ for all $n \geqslant m$. L is the limit of f.

Definition

Let $f\colon \mathbb{N} \to [0,\infty)$ be a function. Then

$$\lim_{n\to\infty} f(n) = L$$

if for all positive reals ε, there exists $m \in \mathbb{N}$, such that $|f(n) - L| < \varepsilon$ for all $n \geqslant m$. L is the limit of f.

Example

Let $f\colon \mathbb{N} \to [0,\infty)$ with $n \mapsto n^2$ and $g\colon \mathbb{N} \to [0,\infty)$ with $n \mapsto \frac{1}{n}$. Then $\lim_{n\to\infty} f(n) = \infty$ and $\lim_{n\to\infty} g(n) = 0$. The function $h\colon \mathbb{N} \to [0,\infty)$ with

$$h(n) = \begin{cases} 1 & \text{if } n \text{ even} \\ 0 & \text{if } n \text{ odd} \end{cases}$$

has no limit.

Definition (Limes inferior and superior)

- Let $f\colon \mathbb{N} \to [0,\infty)$. Then

$$\liminf_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\inf\{f(m) \mid m \geqslant n\}\right)$$

and

$$\limsup_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\sup\{f(m) \mid m \geqslant n\}\right).$$

where $\inf$ ($\sup$) denotes the infimum (supremum).

Definition (Limes inferior and superior)

- Let $f\colon \mathbb{N} \to [0,\infty)$. Then

$$\liminf_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\inf\{f(m) \mid m \geqslant n\}\right)$$

and

$$\limsup_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\sup\{f(m) \mid m \geqslant n\}\right).$$

where $\inf$ ($\sup$) denotes the infimum (supremum).
- For every sequence $f(n)_{n\geqslant \ell}$ of real numbers, the limes inferior and superior exist in the extended real numbers $\mathbb{R} \cup [-\infty, +\infty]$.

Definition (Limes inferior and superior)

- Let $f\colon \mathbb{N} \to [0,\infty)$. Then

$$\liminf_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\inf\{f(m) \mid m \geqslant n\}\right)$$

and

$$\limsup_{n\to\infty} f(n) := \lim_{n\to\infty} \left(\sup\{f(m) \mid m \geqslant n\}\right).$$

where $\inf$ ($\sup$) denotes the infimum (supremum).
- For every sequence $f(n)_{n\geqslant \ell}$ of real numbers, the limes inferior and superior exist in the extended real numbers $\mathbb{R} \cup [-\infty, +\infty]$.

Theorem

Let $f\colon \mathbb{N} \to [0,\infty)$. If $\lim_{n\to\infty} f(n)$ is defined, then $\lim_{n\to\infty} f(n) = \limsup_{n\to\infty} f(n) = \liminf_{n\to\infty} f(n)$. ■

Theorem

Let $f\colon \{k, k+1, \ldots\} \to [0,\infty)$ and $g\colon \{\ell, \ell+1, \ldots\} \to (0,\infty)$. Then

$$f \in \mathrm{O}(g) \;\Leftrightarrow\; \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$$

and

$$f \in \Omega(g) \;\Leftrightarrow\; \liminf_{n\to\infty} \frac{f(n)}{g(n)} > 0\,.$$

Theorem

Let $f\colon \{k, k+1, \ldots\} \to [0,\infty)$ and $g\colon \{\ell, \ell+1, \ldots\} \to (0,\infty)$. Then

$$f \in \mathrm{O}(g) \;\Leftrightarrow\; \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$$

and

$$f \in \Omega(g) \;\Leftrightarrow\; \liminf_{n\to\infty} \frac{f(n)}{g(n)} > 0\,.$$

Proof.

We show the first equivalence, the second one being analogous. If $f(n) \leqslant c \cdot g(n)$ for sufficiently large n, then $\limsup_{n\to\infty} \frac{f(n)}{g(n)} \leqslant c$.

Conversely, if $s := \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$ then $\frac{f(n)}{g(n)} \leqslant s+1$ for n sufficiently large.

Theorem

Let $f\colon \{k, k+1, \ldots\} \to [0,\infty)$ and $g\colon \{\ell, \ell+1, \ldots\} \to (0,\infty)$. Then

$$f \in \mathrm{O}(g) \;\Leftrightarrow\; \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$$

and

$$f \in \Omega(g) \;\Leftrightarrow\; \liminf_{n\to\infty} \frac{f(n)}{g(n)} > 0\,.$$

Proof.

We show the first equivalence, the second one being analogous. If $f(n) \leqslant c \cdot g(n)$ for sufficiently large n, then $\limsup_{n\to\infty} \frac{f(n)}{g(n)} \leqslant c$.

Conversely, if $s := \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$ then $\frac{f(n)}{g(n)} \leqslant s+1$ for n sufficiently large. ■

Definition (small-o)

Let $f\colon \{k, k+1, \ldots\} \to [0,\infty)$ and $g\colon \{\ell, \ell+1, \ldots\} \to (0,\infty)$. Then $f \in \mathrm{o}(g)$, if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0\,,$$

That is, f is asymptotically negligible w.r.t. g

Definition (small-o)

Let $f\colon \{k, k+1, \ldots\} \to [0,\infty)$ and $g\colon \{\ell, \ell+1, \ldots\} \to (0,\infty)$. Then $f \in \mathrm{o}(g)$, if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0\,,$$

That is, f is asymptotically negligible w.r.t. g

Example

We have $n \in \mathrm{o}(n^2)$, as

$$\lim_{n\to\infty} \frac{n}{n^2} = \lim_{n\to\infty} \frac{1}{n} = 0\,,$$

but $n \notin \mathrm{o}(2n)$, as

$$\lim_{n\to\infty} \frac{n}{2n} = \lim_{n\to\infty} \frac{1}{2} = \frac{1}{2}\,.$$