Summary last week

- functions as algorithms; finite specifications
- functions defined by imperative programs
- Turing machines; input and output on tape, transitions, halting
- functions defined by functional programs
- functional specifications; input as argument(s), output as value, replacing

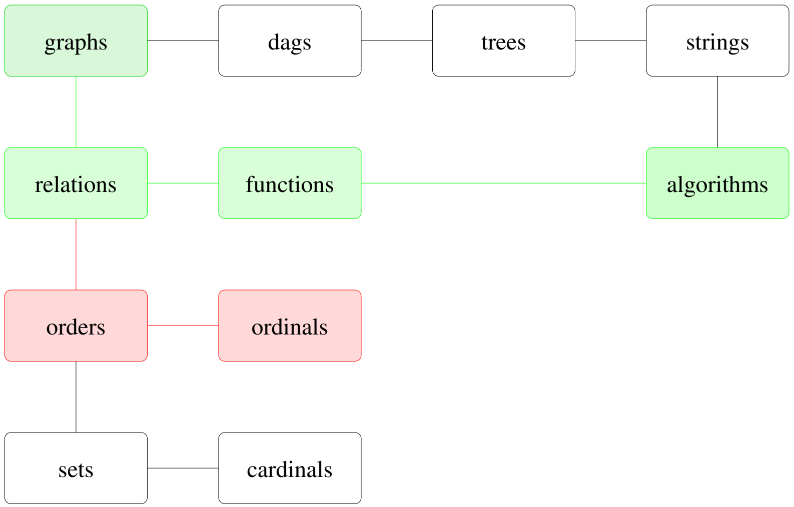
Summary last week

- functions as algorithms; finite specifications
- functions defined by imperative programs
- Turing machines; input and output on tape, transitions, halting
- functions defined by functional programs
- functional specifications; input as argument(s), output as value, replacing
- orders as certain transitive relations; partial, total, strict
- correspondence between partial and strict orders
- strict part (predecessor): $\leq \mapsto <$; reflexive closure: $< \mapsto \leq$
- minimal/maximal elements: no element smaller/greater
- least/greatest elements: smaller/greater than all

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



Orders

Definition

A relation is a

- partial order if it is reflexive, anti-symmetric and transitive;
- total order if moreover every pair of elements is related either way; and
- strict order if it is irreflexive and transitive (so it is anti-symmetric)

Orders

Definition

A relation is a

- partial order if it is reflexive, anti-symmetric and transitive;
- total order if moreover every pair of elements is related either way; and
- strict order if it is irreflexive and transitive (so it is anti-symmetric)

Example

The natural order $\leq$ on $\mathbb{Z}$, defined by $x \leq y$ if $y - x \in \mathbb{N}$ is partial, total order (not strict). $<$ is strict (not total, partial).

Orders

Definition

A relation is a

- partial order if it is reflexive, anti-symmetric and transitive;
- total order if moreover every pair of elements is related either way; and
- strict order if it is irreflexive and transitive (so it is anti-symmetric)

Example

The natural order $\leq$ on $\mathbb{Z}$, defined by $x \leq y$ if $y - x \in \mathbb{N}$ is partial, total order (not strict). $<$ is strict (not total, partial).

Example

$m \in \mathbb{N}$ divides $n \in \mathbb{N}$, if there is some $p \in \mathbb{N}$ such that $n = m \cdot p$. Divisibility is a partial order (not total, strict). Strict divisibility is strict (not total, partial).

Orders

Definition

A relation is a

- partial order if it is reflexive, anti-symmetric and transitive;
- total order if moreover every pair of elements is related either way; and
- strict order if it is irreflexive and transitive (so it is anti-symmetric)

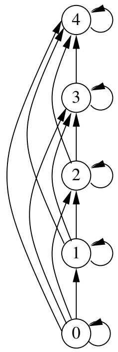
Example

The natural order $\leq$ on $\mathbb{Z}$, defined by $x \leq y$ if $y - x \in \mathbb{N}$ is partial, total order (not strict). $<$ is strict (not total, partial).

Example

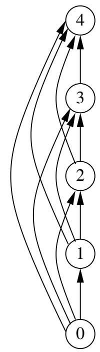
$m \in \mathbb{N}$ divides $n \in \mathbb{N}$, if there is some $p \in \mathbb{N}$ such that $n = m \cdot p$. Divisibility is a partial order (not total, strict). Strict divisibility is strict (not total, partial).

Partial order $\Rightarrow$ strict order $\Rightarrow$ Hasse diagram



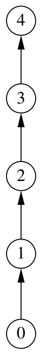
(initial part of) graph of partial order $\leq$ on $\mathbb{N}$
why have reflexive, transitive edges if we can reconstruct them?

Partial order $\Rightarrow$ strict order $\Rightarrow$ Hasse diagram



graph of strict order $<$ on $\mathbb{N}$
$\leq$ reconstructed from strict order as reflexive closure $<^=$ of $<$

Partial order $\Rightarrow$ strict order $\Rightarrow$ Hasse diagram



graph of successor relation $R = \{(n, n+1) \mid n \in \mathbb{N}\}$; Hasse diagram of $\leq$
$\leq$ reconstructed from Hasse diagram as reflexive–transitive closure R^* of R

Lemma

$\leq$ total order

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Proof.

(1) unique:

∎

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Proof.

(1) unique: x, w least

∎

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w$

∎

Lemma

$\leq$ *total order*

- *x least* $\Leftrightarrow$ *x minimal*
- *x greatest* $\Leftrightarrow$ *x maximal*

Theorem

$\leq$ *partial order*

(1) *x least* $\Rightarrow$ *x unique minimal element*

(2) *x greatest* $\Rightarrow$ *x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$

■

Lemma

$\leq$ *total order*

- *x least* $\Leftrightarrow$ *x minimal*
- *x greatest* $\Leftrightarrow$ *x maximal*

Theorem

$\leq$ *partial order*

(1) *x least* $\Rightarrow$ *x unique minimal element*

(2) *x greatest* $\Rightarrow$ *x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$

minimal:

■

Lemma

$\leq$ *total order*

- *x least* $\Leftrightarrow$ *x minimal*
- *x greatest* $\Leftrightarrow$ *x maximal*

Theorem

$\leq$ *partial order*

(1) *x least* $\Rightarrow$ *x unique minimal element*

(2) *x greatest* $\Rightarrow$ *x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$

minimal: x least and $y \leq x$

■

Lemma

$\leq$ *total order*

- *x least* $\Leftrightarrow$ *x minimal*
- *x greatest* $\Leftrightarrow$ *x maximal*

Theorem

$\leq$ *partial order*

(1) *x least* $\Rightarrow$ *x unique minimal element*

(2) *x greatest* $\Rightarrow$ *x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$

minimal: x least and $y \leq x \Rightarrow y \leq x \leq y$

■

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$
minimal: x least and $y \leq x \Rightarrow y \leq x \leq y \Rightarrow y = x$

∎

Lemma

$\leq$ *total order*

- *x least $\Leftrightarrow$ x minimal*
- *x greatest $\Leftrightarrow$ x maximal*

Theorem

$\leq$ *partial order*

(1) *x least $\Rightarrow$ x unique minimal element*

(2) *x greatest $\Rightarrow$ x unique maximal element*

Proof.

(1) unique: x, w least $\Rightarrow w \leq x \leq w \;\Rightarrow w = x$
minimal: x least and $y \leq x \Rightarrow y \leq x \leq y \Rightarrow y = x$
(2) By (1) using that greatest, maximal wrt $\leq$ iff least, minimal wrt its converse $\geq$ ∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element:

∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element: If x is minimal, we are done.

∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element: If x is minimal, we are done.
Otherwise there exists $x_1 \in M$ with $x_1 < x$.

∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element: If x is minimal, we are done.
Otherwise there exists $x_1 \in M$ with $x_1 < x$. If x_1 is not minimal, then there exists $x_2 \in M$ with $x_2 < x_1$, etc.

∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \leq x$ and a maximal z such that $x \leq z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element: If x is minimal, we are done.
Otherwise there exists $x_1 \in M$ with $x_1 < x$. If x_1 is not minimal, then there exists $x_2 \in M$ with $x_2 < x_1$, etc. Because

$$x > x_1 > x_2 > \dots$$

are all distinct elements of M, we reach in finitely many steps a minimal element x_n such that $x_n < x$.

∎

Theorem

(3) *M finite $\Rightarrow$ for every $x \in M$ there exist a minimal w such that $w \le x$ and a maximal z such that $x \le z$*

(4) *If M is finite and has only one minimal element, then that is least.*

(5) *If M is finite and has only one maximal element, then that is greatest*

Proof.

(3) We only show existence of a minimal element: If x is minimal, we are done. Otherwise there exists $x_1 \in M$ with $x_1 < x$. If x_1 is not minimal, then there exists $x_2 \in M$ with $x_2 < x_1$, etc. Because

$$x > x_1 > x_2 > \dots$$

are all distinct elements of M, we reach in finitely many steps a minimal element x_n such that $x_n < x$.

(4) and (5) follow from (3) ■

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Example

- $\mathbb{B} = \{0, 1\}$ is the binary alphabet
- $\{a, b, \dots, z\}$ is the alphabet of letters
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the alphabet of digits

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Example

- $\mathbb{B} = \{0, 1\}$ is the binary alphabet
- $\{a, b, \ldots, z\}$ is the alphabet of letters
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the alphabet of digits

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Example

- $\mathbb{B} = \{0, 1\}$ is the binary alphabet
- $\{a, b, \ldots, z\}$ is the alphabet of letters
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the alphabet of digits

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Example

- $\mathbb{B} = \{0, 1\}$ is the binary alphabet
- $\{a, b, \ldots, z\}$ is the alphabet of letters
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the alphabet of digits

Definition (Word)

$w = (w_0, \ldots, w_{n-1}) \in \Sigma^n$ is a word or string of length $\ell(w) = n$ over Σ

Orders on words

Definition (Alphabet)

Set Σ is an alphabet $a \in \Sigma$ is a symbol

Example

- $\mathbb{B} = \{0, 1\}$ is the binary alphabet
- $\{a, b, \ldots, z\}$ is the alphabet of letters
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is the alphabet of digits

Definition (Word)

$w = (w_0, \ldots, w_{n-1}) \in \Sigma^n$ is a word or string of length $\ell(w) = n$ over Σ

Σ^* is the set of all words over Σ

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ.

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ. For words $v, w \in \Sigma^*$

$$v <_{\text{lex}} w$$

if there exists $k \in \mathbb{N}$ with $k \leq \ell(v)$, $k \leq \ell(w)$ such that

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ. For words $v, w \in \Sigma^*$

$$v <_{\text{lex}} w$$

if there exists $k \in \mathbb{N}$ with $k \leq \ell(v)$, $k \leq \ell(w)$ such that

(1) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ. For words $v, w \in \Sigma^*$

$$v <_{\text{lex}} w$$

if there exists $k \in \mathbb{N}$ with $k \leq \ell(v)$, $k \leq \ell(w)$ such that

(1) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(v) = k$ and $\ell(w) > k)$ or $(\ell(v) > k$, $\ell(w) > k$ and $v_k < w_k)$

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ. For words $v, w \in \Sigma^*$

$$v <_{\text{lex}} w$$

if there exists $k \in \mathbb{N}$ with $k \leq \ell(v)$, $k \leq \ell(w)$ such that

(1) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(v) = k$ and $\ell(w) > k)$ or $(\ell(v) > k$, $\ell(w) > k$ and $v_k < w_k)$

Example

Let $\Sigma = \{a, b\}$ and $a < b$. Then

$$\epsilon <_{\text{lex}} a \qquad \epsilon <_{\text{lex}} b \qquad a <_{\text{lex}} b \qquad aa <_{\text{lex}} ab \qquad aaaa <_{\text{lex}} ab$$

Definition (lexicographic order on words)

Let $\leq$ be total order on Σ. For words $v, w \in \Sigma^*$

$$v <_{\text{lex}} w$$

if there exists $k \in \mathbb{N}$ with $k \leq \ell(v)$, $k \leq \ell(w)$ such that

(1) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(v) = k$ and $\ell(w) > k)$ or $(\ell(v) > k$, $\ell(w) > k$ and $v_k < w_k)$

Example

Let $\Sigma = \{a, b\}$ and $a < b$. Then

$$\epsilon <_{\text{lex}} a \qquad \epsilon <_{\text{lex}} b \qquad a <_{\text{lex}} b \qquad aa <_{\text{lex}} ab \qquad aaaa <_{\text{lex}} ab$$

Theorem

$\leq_{lex}$ is a partial, total order on Σ^*

Proof that $\leq_{\text{lex}}$ is a partial order

Suffices to show that $<_{\text{lex}}$ is a strict order. $<_{\text{lex}}$ is clearly irreflexive.

Proof that $\leq_{\text{lex}}$ is a partial order

Suffices to show that $<_{\text{lex}}$ is a strict order. $<_{\text{lex}}$ is clearly irreflexive. To show transitivity, let $u, v, w \in \Sigma^*$ with

$$u <_{\text{lex}} v \qquad \text{and} \qquad v <_{\text{lex}} w$$

Proof that $\leq_{\text{lex}}$ is a partial order

Suffices to show that $<_{\text{lex}}$ is a strict order. $<_{\text{lex}}$ is clearly irreflexive. To show transitivity, let $u, v, w \in \Sigma^*$ with

$$u <_{\text{lex}} v \qquad \text{and} \qquad v <_{\text{lex}} w$$

Then there is a $k \in \mathbb{N}$ with $k \leq \ell(u)$ and $k \leq \ell(v)$ and

(1) $u_i = v_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(u) = k \text{ and } \ell(v) > k)$ or $(\ell(u) > k \text{ and } \ell(v) > k \text{ and } u_k < v_k)$

Proof that $\leq_{\text{lex}}$ is a partial order

Suffices to show that $<_{\text{lex}}$ is a strict order. $<_{\text{lex}}$ is clearly irreflexive. To show transitivity, let $u, v, w \in \Sigma^*$ with

$$u <_{\text{lex}} v \qquad \text{and} \qquad v <_{\text{lex}} w$$

Then there is a $k \in \mathbb{N}$ with $k \leq \ell(u)$ and $k \leq \ell(v)$ and

(1) $u_i = v_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(u) = k \text{ and } \ell(v) > k)$ or $(\ell(u) > k \text{ and } \ell(v) > k \text{ and } u_k < v_k)$

and moreover an $l \in \mathbb{N}$ with $l \leq \ell(v)$ and $l \leq \ell(w)$ and

(1) $v_i = w_i$ for $i = 0, \ldots, l-1$ and

(2) $(\ell(v) = l \text{ and } \ell(w) > l)$ or $(\ell(v) > l \text{ and } \ell(w) > l \text{ and } v_l < w_l)$

Proof that $\leq_{\text{lex}}$ is a partial order

Suffices to show that $<_{\text{lex}}$ is a strict order. $<_{\text{lex}}$ is clearly irreflexive. To show transitivity, let $u, v, w \in \Sigma^*$ with

$$u <_{\text{lex}} v \qquad \text{and} \qquad v <_{\text{lex}} w$$

Then there is a $k \in \mathbb{N}$ with $k \leq \ell(u)$ and $k \leq \ell(v)$ and

(1) $u_i = v_i$ for $i = 0, \ldots, k-1$ and

(2) $(\ell(u) = k \text{ and } \ell(v) > k)$ or $(\ell(u) > k \text{ and } \ell(v) > k \text{ and } u_k < v_k)$

and moreover an $l \in \mathbb{N}$ with $l \leq \ell(v)$ and $l \leq \ell(w)$ and

(1) $v_i = w_i$ for $i = 0, \ldots, l-1$ and

(2) $(\ell(v) = l \text{ and } \ell(w) > l)$ or $(\ell(v) > l \text{ and } \ell(w) > l \text{ and } v_l < w_l)$

Then we have for $m := \min(k, l)$, $m \leq \ell(u)$ and $m \leq \ell(w)$ and

(a) $u_i = w_i$ for $i = 0, \ldots, m-1$ and

(b) $(\ell(u) = m \text{ and } \ell(w) > m)$ or $(\ell(u) > m \text{ and } \ell(w) > m \text{ and } u_m < w_m)$

from which $u <_{\text{lex}} w$ follows

Proof that $\leq_{\text{lex}}$ is total

To prove that $\leq_{\text{lex}}$ is total, let $v, w \in \Sigma^*$ with $v \neq w$

Proof that $\leq_{\text{lex}}$ is total

To prove that $\leq_{\text{lex}}$ is total, let $v, w \in \Sigma^*$ with $v \neq w$
Then there exists a $k \in \mathbb{N}$ with $k \leq \ell(v)$ and $k \leq \ell(w)$ such that

(a) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

(b) $(\ell(v) = k$ and $\ell(w) > k)$ or $(\ell(v) > k$ and $\ell(w) = k)$ or
$(\ell(v) > k$ and $\ell(w) > k$ and $v_k \neq w_k)$

Proof that $\leq_{\text{lex}}$ is total

To prove that $\leq_{\text{lex}}$ is total, let $v, w \in \Sigma^*$ with $v \neq w$
Then there exists a $k \in \mathbb{N}$ with $k \leq \ell(v)$ and $k \leq \ell(w)$ such that

(a) $v_i = w_i$ for $i = 0, \ldots, k-1$ and

(b) $(\ell(v) = k$ and $\ell(w) > k)$ or $(\ell(v) > k$ and $\ell(w) = k)$ or
$(\ell(v) > k$ and $\ell(w) > k$ and $v_k \neq w_k)$

Since $\leq$ is total on Σ, we have either $v <_{\text{lex}} w$ or $w <_{\text{lex}} v$

Well-founded relations

Definition (well-founded relation)

- Let R be a relation on a set M
- A sequence $(x_0, x_1, x_2, \ldots)$ of elements of M is an infinite descending R-chain, if

$$\ldots \; R \; x_2 \; R \; x_1 \; R \; x_0$$

- R is well-founded, if M has no infinite descending R-chains.
- When we say that partial order $\leq$ is well-founded we mean that its strict part $<$ is

Well-founded relations

Definition (well-founded relation)

- Let R be a relation on a set M
- A sequence $(x_0, x_1, x_2, \ldots)$ of elements of M is an infinite descending R-chain, if

$$\ldots \; R \; x_2 \; R \; x_1 \; R \; x_0$$

- R is well-founded, if M has no infinite descending R-chains.
- When we say that partial order $\leq$ is well-founded we mean that its strict part $<$ is

Example

- The natural order $\leq$ on $\mathbb{N}$ is well-founded
- The natural order $\leq$ on $\mathbb{Z}$ is not well-founded
- The lexicographic order is not well-founded, if alphabet has at least two symbols

Proving that all elements of set have some property

Universal properties

Given: M a set and P a property of elements of the set
Goal: establish that all elements of M have property P

Proving that all elements of set have some property

Universal properties

Given: M a set and P a property of elements of the set
Goal: establish that all elements of M have property P

Example

- M = months of year; $P(m)$ = month m has at least 25 days

Proving that all elements of set have some property

Universal properties

Given: M a set and P a property of elements of the set
Goal: establish that all elements of M have property P

Example

- M = months of year; $P(m)$ = month m has at least 25 days
- M = natural numbers, $P(n)$ = if n is even, then so is n^2

Proving that all elements of set have some property

Universal properties

Given: M a set and P a property of elements of the set
Goal: establish that all elements of M have property P

Example

- M = months of year; $P(m)$ = month m has at least 25 days
- M = natural numbers, $P(n)$ = if n is even, then so is n^2
- M = natural numbers, $P(n) = (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$

Proving that all elements of set have some property

Universal properties

Given: M a set and P a property of elements of the set
Goal: establish that all elements of M have property P

Example

- M = months of year; $P(m)$ = month m has at least 25 days
- M = natural numbers, $P(n)$ = if n is even, then so is n^2
- M = natural numbers, $P(n) = (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$
- M = pairs of positive natural numbers, $P(n, m)$ = Euclid's algorithm yields $\gcd(m, n)$

Proof by cases

Program

```
data Month = Jan | Feb | Mar | Apr | May | Jun
           | Jul | Aug | Sep | Oct | Nov | Dec
days :: Month -> Int
days Jan = 31
...
days Dec = 31
```

Lemma

for every `Month m`, `days m` ≥ 25

Proof by cases

Program

```
data Month = Jan | Feb | Mar | Apr | May | Jun
           | Jul | Aug | Sep | Oct | Nov | Dec
days :: Month -> Int
days Jan = 31
...
days Dec = 31
```

Lemma

for every `Month m`, `days m` ≥ 25

Proof by cases.

`days Jan = 31` ≥ 25 ✓, ..., `days Dec = 31` ≥ 25 ✓
we conclude since we checked all cases ∎

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof.

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof.

1. take an arbitrary natural number n

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof.

1. take an arbitrary natural number n
2. suppose n is even: $n = 2m$ for some natural number m

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof.

1. take an arbitrary natural number n
2. suppose n is even: $n = 2m$ for some natural number m
3. then $n^2 = (2m)^2 = 2(2m^2)$ ✓

Proof by universal generalisation

Lemma

for every natural number n that is even, n^2 is even.

Proof.

1. take an arbitrary natural number n
2. suppose n is even: $n = 2m$ for some natural number m
3. then $n^2 = (2m)^2 = 2(2m^2)$ ✓

we conclude since n was taken to be arbitrary ■

Proof by mathematical induction

Lemma

for every natural number $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof by mathematical induction

Lemma

for every natural number $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Principle of well-founded induction

Assumption: R a well-founded relation on set N
Induction: for arbitrary $n \in N$, show that if $P(m)$ for all $m\ R\ n$, then $P(n)$
Conclude: for all $n \in N$, $P(n)$

the $P(m)$ for $m\ R\ n$ are the induction hypotheses

Proof.

■

Proof by mathematical induction

Lemma

for every natural number $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Principle of well-founded induction

Assumption: R a well-founded relation on set N
Induction: for arbitrary $n \in N$, show that if $P(m)$ for all $m\ R\ n$, then $P(n)$
Conclude: for all $n \in N$, $P(n)$

Proof.

- Take the well-founded relation $\{(n, n+1) \mid n \in \mathbb{N}\}$.

■

Proof by mathematical induction

Lemma

for every natural number $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Principle of well-founded induction

Assumption: R a well-founded relation on set N
Induction: for arbitrary $n \in N$, show that if $P(m)$ for all $m \; R \; n$, then $P(n)$
Conclude: for all $n \in N$, $P(n)$

Proof.

- Take the well-founded relation $\{(n, n+1) \mid n \in \mathbb{N}\}$.
- if $n = 0$, then no induction hypotheses; directly show $P(0)$

$$\sum_{i=1}^{0} i = 0 = \frac{0(0+1)}{2}$$

∎

Proof by mathematical induction

Lemma

for every natural number $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Principle of well-founded induction

Assumption: R a well-founded relation on set N
Induction: for arbitrary $n \in N$, show that if $P(m)$ for all $m \; R \; n$, then $P(n)$
Conclude: for all $n \in N$, $P(n)$

Proof.

- Take the well-founded relation $\{(n, n+1) \mid n \in \mathbb{N}\}$.

- if $n > 0$, then one induction hypothesis $P(n-1)$: $\sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}$

$$\sum_{i=1}^{n} i = (\sum_{i=1}^{n-1} i) + n =_{IH} \frac{(n-1)n}{2} + n = \frac{n(n+1)}{2}$$

∎

Proof by mathematical induction

mathematical induction

1. Suppose we want to show $P(n)$ for all natural numbers n
2. To that end, we may proceed as follows:
   - Induction basis: We show that P holds for the base value 0;
   - Induction step: We show that for all $n > 0$, $P(n-1)$ entails $P(n)$.
3. Then $P(n)$ holds for all n

Mathematical induction = well-founded induction wrt. $R = \{(n, n+1) \mid n \in \mathbb{N}\}$.

Proof by mathematical induction

mathematical induction

1. Suppose we want to show $P(n)$ for all natural numbers n
2. To that end, we may proceed as follows:
   - Induction basis: We show that P holds for the base value 0;
   - Induction step: We show that for all $n > 0$, $P(n-1)$ entails $P(n)$.
3. Then $P(n)$ holds for all n

Mathematical induction = well-founded induction wrt. $R = \{(n, n+1) \mid n \in \mathbb{N}\}$.

mathematical induction formally

$$(P(0) \wedge \forall n > 0.(P(n-1) \rightarrow P(n))) \rightarrow (\forall n.P(n))$$

Proof by mathematical induction

mathematical induction

1. Suppose we want to show $P(n)$ for all natural numbers n
2. To that end, we may proceed as follows:
   - Induction basis: We show that P holds for the base value 0;
   - Induction step: We show that for all $n > 0$, $P(n-1)$ entails $P(n)$.
3. Then $P(n)$ holds for all n

Mathematical induction = well-founded induction wrt. $R = \{(n, n+1) \mid n \in \mathbb{N}\}$.

well-founded induction formally

$$\forall n.((\forall m \text{ such that } m\ R\ n.P(m)) \to P(n)) \to (\forall n.P(n))$$

Foundations of well-founded induction

Theorem

Let $\leq$ be a partial order on the set M. Then $\leq$ is well-founded iff every non-empty subset of M has a minimal element.

Proof.

Let $\leq$ be a well-founded order on M and N a non-empty subset of N. Then there exists some element x_0 in N. If x_0 is minimal in N, then we are done.

Proof.

Let $\leq$ be a well-founded order on M and N a non-empty subset of N. Then there exists some element x_0 in N. If x_0 is minimal in N, then we are done.
Otherwise, there exists some element $x_1 \in N$ with $x_1 < x_0$. If x_1 is minimal, then we are done again. Otherwise, there is some $x_2 \in N$ with $x_2 < x_1$, etc.. Since

$$x_0 > x_1 > x_2 > \dots$$

we reach a minimal element x_n after finitely many steps.

$$x_0 > x_1 > x_2 > \dots$$

Proof.

Let $\leq$ be a well-founded order on M and N a non-empty subset of N. Then there exists some element x_0 in N. If x_0 is minimal in N, then we are done.
Otherwise, there exists some element $x_1 \in N$ with $x_1 < x_0$. If x_1 is minimal, then we are done again. Otherwise, there is some $x_2 \in N$ with $x_2 < x_1$, etc.. Since

$$x_0 > x_1 > x_2 > \dots$$

we reach a minimal element x_n after finitely many steps.

$$x_0 > x_1 > x_2 > \dots$$

To prove the other direction, we suppose that $\leq$ were not well-founded. Then there would be an infinitely descending chain

$$x_0 > x_1 > x_2 > \dots,$$

and the non-empty subset $N = \{x_0, x_1, x_2, \dots\}$ has no minimal element.

Proof.

Let $\leq$ be a well-founded order on M and N a non-empty subset of N. Then there exists some element x_0 in N. If x_0 is minimal in N, then we are done.
Otherwise, there exists some element $x_1 \in N$ with $x_1 < x_0$. If x_1 is minimal, then we are done again. Otherwise, there is some $x_2 \in N$ with $x_2 < x_1$, etc.. Since

$$x_0 > x_1 > x_2 > \dots$$

we reach a minimal element x_n after finitely many steps.

$$x_0 > x_1 > x_2 > \dots$$

To prove the other direction, we suppose that $\leq$ were not well-founded. Then there would be an infinitely descending chain

$$x_0 > x_1 > x_2 > \dots,$$

and the non-empty subset $N = \{x_0, x_1, x_2, \dots\}$ has no minimal element. ■

Proof by well-founded induction

Lemma

for all pairs of positive natural numbers, Euclid's algorithm yields $\gcd(m, n)$

Euclid's greatest common divisor algorithm

```
euclid m n = if m == n then m else if m > n
  then euclid (m-n) n else euclid m (n - m)
```


Proof by well-founded induction

Lemma

for all pairs of positive natural numbers, Euclid's algorithm yields $\gcd(m, n)$

Euclid's greatest common divisor algorithm

```
euclid m n = if m == n then m else if m > n
  then euclid (m-n) n else euclid m (n - m)
```

Principle of well-founded induction

Assumption: R a well-founded relation on set N
Induction: for arbitrary $n \in N$, show that if $P(m)$ for all $m\ R\ n$, then $P(n)$
Conclude: for all $n \in N$, $P(n)$

Proof by well-founded induction

Lemma

for all pairs of positive natural numbers, Euclid's algorithm yields $\mathrm{gcd}(m,n)$

Euclid's greatest common divisor algorithm

```
euclid m n = if m == n then m else if m > n
  then euclid (m-n) n else euclid m (n - m)
```

Proof.

- Take the well-founded relation $\{((m,n),(m',n')) \mid m+n < m'+n'\}$.

Proof by well-founded induction

Lemma

for all pairs of positive natural numbers, Euclid's algorithm yields $\mathrm{gcd}(m,n)$

Euclid's greatest common divisor algorithm

```
euclid m n = if m == n then m else if m > n
  then euclid (m-n) n else euclid m (n - m)
```

Proof.

- Take the well-founded relation $\{((m,n),(m',n')) \mid m+n < m'+n'\}$.
- if $m=n$, then no induction hypotheses needed; `euclid m m` $= m = \mathrm{gcd}(m,m)$

Proof by well-founded induction

Lemma

for all pairs of positive natural numbers, Euclid's algorithm yields $\mathrm{gcd}(m,n)$

Euclid's greatest common divisor algorithm

```
euclid m n = if m == n then m else if m > n
  then euclid (m-n) n else euclid m (n - m)
```

Proof.

- Take the well-founded relation $\{((m,n),(m',n')) \mid m+n < m'+n'\}$.
- if $m=n$, then no induction hypotheses needed; `euclid m m` $= m = \mathrm{gcd}(m,m)$
- if $m>n$, then induction hypotheses: `euclid m' n'` $= \mathrm{gcd}(m',n')$ if $m'+n' < m+n$

  `euclid m n` $=$ `euclid (m-n) n` $=_{IH} \mathrm{gcd}(m-n,m) = \mathrm{gcd}(m,n)$

Example

Let M be the set of all palindromes over the alphabet $\{a,b\}$. We show

?*If* $x \in M$ *and* $\ell(x)$ *even, then* x *has an even number of* a*s.****?***

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. We show
?If $x \in M$ and $\ell(x)$ even, then x has an even number of as.?

Proof.

By well-founded induction. Take $R = \{(w, w') \mid \ell(w) < \ell(w')\}$; order by length

- if x the empty string, then property holds; 0 is even
- if x non-empty induction hypotheses: property holds for words shorter than x
  - if first letter of x is a, then $x = ax'a$ for some palindrome $x' \in M$. then conclude since 2 + even is even
  - if first letter of x is b, then $x = bx'b$ for some palindrome $x' \in M$. then conclude since 0 + even is even

■