Summary last week

- Hasse diagram of a partial order $\leq$ or strict order $<$
- least irreflexive, atransitive subrelation R of $\leq$ such that $\leq = R^*$ or $< = R^+$ (atransitive: $x\ R\ y$ and $y\ R\ z$ then not $x\ R\ z$)
- for total orders, minimal = least and maximal = greatest
- finite partial orders have minimal and maximal elements
- the lexicographic order $<_{\text{lex}}$ on words; partial/total if $\leq$ is.

Summary last week

- Hasse diagram of a partial order $\leq$ or strict order $<$
- least irreflexive, atransitive subrelation R of $\leq$ such that $\leq = R^*$ or $< = R^+$ (atransitive: $x\ R\ y$ and $y\ R\ z$ then not $x\ R\ z$)
- for total orders, minimal = least and maximal = greatest
- finite partial orders have minimal and maximal elements
- the lexicographic order $<_{\text{lex}}$ on words; partial/total if $\leq$ is.
- well-founded relations as not having infinite descending chains
- Three methods to prove that all elements of set have some property:

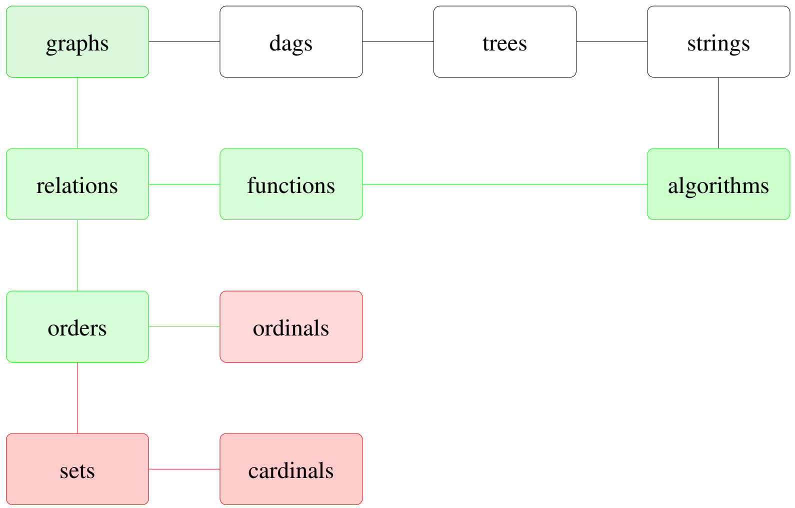
1) by cases; for finite sets, enumerating all elts
2) by universal generalisation; for infinite sets, proving for some arbitrary elt
3) by well-founded induction; for infinite sets, using property (IH) for smaller elts

- well-founded induction principle for well-founded relation R, property P: $\forall n.((\forall m \text{ such that } m\ R\ n.P(m)) \rightarrow P(n)) \rightarrow (\forall n.P(n))$

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



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

Principle of well-founded induction

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

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

Principle of mathematical induction

Assumption: R the well-founded relation $\{(n, n+1) \mid n \in \mathbb{N}\}$. P a property of $n \in \mathbb{N}$.
Induction: for arbitrary $n \in \mathbb{N}$, show that if $P(m)$ for all m such that $m\ R\ n$, then $P(n)$
Conclude: for all $n \in \mathbb{N}$, $P(n)$

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

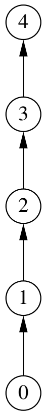
$$\ldots R\ x_2\ R\ x_1\ R\ x_0$$

- 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

Principle of mathematical induction

Assumption: R the well-founded relation $\{(n, n+1) \mid n \in \mathbb{N}\}$. P a property of $n \in \mathbb{N}$.
Induction: for arbitrary $n \in \mathbb{N}$, show that $P(0)$ and if $n > 0$ and $P(n-1)$ then $P(n)$
Conclude: for all $n \in \mathbb{N}$, $P(n)$

Mathematical induction

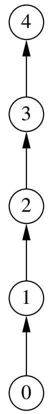


Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

Mathematical induction



Induction basis: P(0)

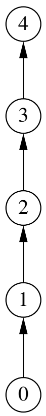
Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

induction step

P(2)?

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

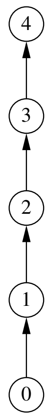
induction step

P(2)?

induction step

P(1)?

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

induction step

P(2)?

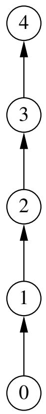
induction step

P(1)?

induction step

P(0)?

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

induction step

P(2)?

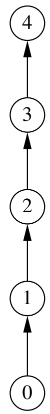
induction step

P(1)?

induction step

P(0) induction basis

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

induction step

P(2)?

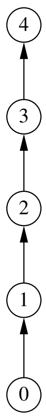
induction step

P(1)

induction step

P(0) induction basis

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)?

induction step

P(2)

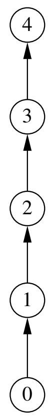
induction step

P(1)

induction step

P(0) induction basis

Mathematical induction



Induction basis: P(0)

Induction step: if n > 0 and P(n−1) then P(n)

P(3)

induction step

P(2)

induction step

P(1)

induction step

P(0) induction basis

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

How

Try to see whether, when proving $P(n)$ for an arbitrary element $n \in N$, it may be helpful to know that $P(m)$ holds already for m smaller than n, for an appropriate notion of smaller. For instance:

- on natural numbers: less-than, successor ('sub-number')
- on positive natural numbers: divisibility

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

How

Try to see whether, when proving $P(n)$ for an arbitrary element $n \in N$, it may be helpful to know that $P(m)$ holds already for m smaller than n, for an appropriate notion of smaller. For instance:

- on natural numbers: less-than, successor ('sub-number')
- on positive natural numbers: divisibility
- on strings: prefix, suffix, subsequence, sub-string

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

How

Try to see whether, when proving $P(n)$ for an arbitrary element $n \in N$, it may be helpful to know that $P(m)$ holds already for m smaller than n, for an appropriate notion of smaller. For instance:

- on natural numbers: less-than, successor ('sub-number')
- on positive natural numbers: divisibility
- on strings: prefix, suffix, subsequence, sub-string
- on (finite) graphs: sub-graph

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

How

Try to see whether, when proving $P(n)$ for an arbitrary element $n \in N$, it may be helpful to know that $P(m)$ holds already for m smaller than n, for an appropriate notion of smaller. For instance:

- on natural numbers: less-than, successor ('sub-number')
- on positive natural numbers: divisibility
- on strings: prefix, suffix, subsequence, sub-string
- on (finite) graphs: sub-graph
- on (finite) sets: sub-set

When and how to apply induction?

When

Prove a property P of elements of an infinite set N.

How

Try to see whether, when proving $P(n)$ for an arbitrary element $n \in N$, it may be helpful to know that $P(m)$ holds already for m smaller than n, for an appropriate notion of smaller. For instance:

- on natural numbers: less-than, successor ('sub-number')
- on positive natural numbers: divisibility
- on strings: prefix, suffix, subsequence, sub-string
- on (finite) graphs: sub-graph
- on (finite) sets: sub-set
- on inductively defined structures: sub-structure

Experimenting to find what may be helpful

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. To show $\forall x \in M.P(x)$ where $P(x) =$ if $\ell(x)$ even, then x has an even number of as.

Experimenting to find what may be helpful

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. To show $\forall x \in M.P(x)$ where $P(x) =$ if $\ell(x)$ even, then x has an even number of as.

Observation

if $x \in M$ then either x empty, or $x = ax'a$ or $x = bx'b$ with $x' \in M$ again

Experimenting to find what may be helpful

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. To show $\forall x \in M.P(x)$ where $P(x) =$ if $\ell(x)$ even, then x has an even number of as.

Observation

if $x \in M$ then either x empty, or $x = ax'a$ or $x = bx'b$ with $x' \in M$ again

Proof.

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

Experimenting to find what may be helpful

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. To show $\forall x \in M.P(x)$ where $P(x) =$ if $\ell(x)$ even, then x has an even number of as.

Observation

if $x \in M$ then either x empty, or $x = ax'a$ or $x = bx'b$ with $x' \in M$ again

Proof.

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

- $x = \epsilon$ is a palindrome, has even length, and an even number of as.

Experimenting to find what may be helpful

Example

Let M be the set of all palindromes over the alphabet $\{a, b\}$. To show $\forall x \in M.P(x)$ where $P(x) =$ if $\ell(x)$ even, then x has an even number of as.

Observation

if $x \in M$ then either x empty, or $x = ax'a$ or $x = bx'b$ with $x' \in M$ again

Proof.

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

- $x = \epsilon$ is a palindrome, has even length, and an even number of as.
- Suppose x non-empty palindrome, and of even length. Induction hypotheses: $P(x')$ holds for palindromes x' shorter than x
  - if first letter of x is a, then $x = ax'a$ for some $x' \in M$ of even length. By the IH $P(x')$ holds, i.e. x' has an even number of as. 2 + even is even.
  - if first letter of x is b, then $x = bx'b$ for some $x' \in M$ of even length. 0+ even is even.

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Observation

The value of `ack` for m and n depends on its value for

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Observation

The value of `ack` for m and n depends on its value for

- $m - 1$ and 1

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Observation

The value of `ack` for m and n depends on its value for

- $m - 1$ and 1
- m and $n - 1$

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Observation

The value of `ack` for m and n depends on its value for

- $m-1$ and 1
- m and $n-1$
- $m-1$ and the value of previous item

Experimenting with the Ackermann function

Ackermann function

Function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$?

```
ack 0 n = n+1
ack m 0 = ack (m-1) 1
ack m n = ack (m-1) (ack m (n-1))
```

`ack 4 4` does not produce an answer? or does it?

Observation

The value of `ack` for m and n depends on its value for

- $m-1$ and 1
- m and $n-1$
- $m-1$ and the value of previous item

well-founded relation such that all of these are smaller?

Lexicographic product

Definition

Let $\leq_1, \leq_2$ be partial orders. Their lexicographic product is defined by

$$(x_1, x_2) \quad \leq_1 \times_{\text{lex}} \leq_2 \quad (y_1, y_2)$$

if $x_1 <_1 y_1$ or ($x_1 = y_1$ and $x_2 \leq_2 y_2$).

Lexicographic product

Definition

Let $\leq_1, \leq_2$ be partial orders. Their lexicographic product is defined by

$$(x_1, x_2) \quad \leq_1 \times_{\text{lex}} \leq_2 \quad (y_1, y_2)$$

if $x_1 <_1 y_1$ or ($x_1 = y_1$ and $x_2 \leq_2 y_2$).

Remarks

First compare the first elements; if that does not decide compare the second elements.
Case $\leq_1 = \leq_2$ corresponds to lexicographic order restricted to strings of length 2.

Lexicographic product

Definition

Let $\leq_1, \leq_2$ be partial orders. Their lexicographic product is defined by

$$(x_1, x_2) \quad \leq_1 \times_{\text{lex}} \leq_2 \quad (y_1, y_2)$$

if $x_1 <_1 y_1$ or ($x_1 = y_1$ and $x_2 \leq_2 y_2$).

Lemma

Lexicographic product preserves well-foundedness: $\leq_1 \times_{lex} \leq_2$ well-founded if $\leq_1, \leq_2$.

Lexicographic product

Definition

Let $\leq_1, \leq_2$ be partial orders. Their lexicographic product is defined by

$$(x_1, x_2) \quad \leq_1 \times_{\text{lex}} \leq_2 \quad (y_1, y_2)$$

if $x_1 <_1 y_1$ or ($x_1 = y_1$ and $x_2 \leq_2 y_2$).

Lemma

Lexicographic product preserves well-foundedness: $\leq_1 \times_{lex} \leq_2$ well-founded if $\leq_1, \leq_2$.

Example

Computing `ack m n` always yields a (unique) value, because recursive calls have arguments that are strictly smaller w.r.t. $\leq \times_{\text{lex}} \leq$. That is, we may speak of the Ackermann function.

Inductively defined structures

Inductive definitions

A set S of structures is inductively defined by clauses of shape

$$\text{if } n_1, \ldots, n_k \in N \text{, then } s(n_1, \ldots, n_k) \in N$$

with s structures depending on $n_1, \ldots, n_k$. if it is the least set satisfying the clauses.

Inductively defined structures

Inductive definitions

A set S of structures is inductively defined by clauses of shape

$$\text{if } n_1, \ldots, n_k \in N \text{, then } s(n_1, \ldots, n_k) \in N$$

with s structures depending on $n_1, \ldots, n_k$. if it is the least set satisfying the clauses.
The sub-structure relation relates each $n_i \in S$ to $s(n_1, \ldots, n_k)$.

Inductively defined structures

Inductive definitions

A set S of structures is inductively defined by clauses of shape

$$\text{if } n_1, \ldots, n_k \in N, \text{ then } s(n_1, \ldots, n_k) \in N$$

with s structures depending on $n_1, \ldots, n_k$. if it is the least set satisfying the clauses. The sub-structure relation relates each $n_i \in S$ to $s(n_1, \ldots, n_k)$.

Lemma

If $s(n_1, \ldots, n_k) \in S$, then $n_1, \ldots, n_k \in S$, assuming the former uniquely depends on the latter, and then the sub-structure relation is well-founded.

Inductively defined structures

Inductive definitions

A set S of structures is inductively defined by clauses of shape

$$\text{if } n_1, \ldots, n_k \in N, \text{ then } s(n_1, \ldots, n_k) \in N$$

with s structures depending on $n_1, \ldots, n_k$. if it is the least set satisfying the clauses. The sub-structure relation relates each $n_i \in S$ to $s(n_1, \ldots, n_k)$.

Lemma

If $s(n_1, \ldots, n_k) \in S$, then $n_1, \ldots, n_k \in S$, assuming the former uniquely depends on the latter, and then the sub-structure relation is well-founded.

Proof.

By S being least, every element in S has a unique and finite derivation tree with nodes in S, and only constructed from clauses (with leaves constructed by the base-clauses ($k = 0$)). R relates children to parents in the tree. ∎

Inductively defined structures

Example

The natural numbers $\mathbb{N}$ can be inductively defined by:

- $0 \in N$
- if $n \in N$, then $n + 1 \in N$.

Sub-structure relation: successor.

Inductively defined structures

Example

The natural numbers $\mathbb{N}$ can be inductively defined by:

- $0 \in N$
- if $n \in N$, then $n + 1 \in N$.

Sub-structure relation: successor.

Example

The palindromes P over $\{0, 1\}$ can be inductively defined by:

- $\epsilon, 0, 1 \in N$
- if $n \in N$, then $0n0 \in N$, $1N1 \in N$.

Sub-structure relation: 'middle'-sub-palindromes

Definition (inductive with explicit base cases)

A set M can be defined inductively by:

- Induction basis: We introduce one or more elements of M.
- Induction step: We specify how, on the basis of already constructed elements of M, new elements of M can be constructed

The set M then comprises exactly those elements that can be obtained by the repeated application of the induction step on elements constructed by the induction basis (finitely many only; corresponding to least)

Definition (inductive with explicit base cases)

A set M can be defined inductively by:

- Induction basis: We introduce one or more elements of M.
- Induction step: We specify how, on the basis of already constructed elements of M, new elements of M can be constructed

The set M then comprises exactly those elements that can be obtained by the repeated application of the induction step on elements constructed by the induction basis (finitely many only; corresponding to least)

Example

The formulas of propositional logic may be inductively defined by:

1. An atomic formula p is a formula
2. A truth symbol (True, False) is a formula
3. If A and B are formulas, then so are $\neg A$, $(A \wedge B)$, $(A \vee B)$ and $(A \rightarrow B)$

Theorem (Structural induction with explicit base cases)

1. *We want to show $A(x)$ holds for all structures $x \in M$, where M is defined by induction.*

Theorem (Structural induction with explicit base cases)

1. *We want to show $A(x)$ holds for all structures $x \in M$, where M is defined by induction.*
2. *We proceed as follows:*
   - *Induction basis: We show that $A(x)$ holds for the base structure(s) x*
   - *Induction step: We choose a structure y that is recursively constructed from the structures $y_1, y_2, \ldots, y_k$. The IH for the latter states that $A(y_1)$, $A(y_2)$, …, $A(y_k)$ hold. Using those, we show $A(y)$*

Theorem (Structural induction with explicit base cases)

1. *We want to show $A(x)$ holds for all structures $x \in M$, where M is defined by induction.*
2. *We proceed as follows:*
   - *Induction basis: We show that $A(x)$ holds for the base structure(s) x*
   - *Induction step: We choose a structure y that is recursively constructed from the structures $y_1, y_2, \ldots, y_k$. The IH for the latter states that $A(y_1)$, $A(y_2)$, $\ldots$, $A(y_k)$ hold. Using those, we show $A(y)$*

Proof.

By ordering $x \in M$ by, say, the minimal number of construction steps needed to show that $x \in M$ (size of the construction tree).

Theorem (Structural induction with explicit base cases)

1. *We want to show $A(x)$ holds for all structures $x \in M$, where M is defined by induction.*
2. *We proceed as follows:*
   - *Induction basis: We show that $A(x)$ holds for the base structure(s) x*
   - *Induction step: We choose a structure y that is recursively constructed from the structures $y_1, y_2, \ldots, y_k$. The IH for the latter states that $A(y_1)$, $A(y_2)$, $\ldots$, $A(y_k)$ hold. Using those, we show $A(y)$*

Proof.

By ordering $x \in M$ by, say, the minimal number of construction steps needed to show that $x \in M$ (size of the construction tree). ∎

Proof by minimal counterexample

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 by minimal counterexample

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 by minimal counterexample

Assumption: P a property on set N. R a well-founded relation on N

Minimal counterexample: show if n minimal such that not $P(n)$, then contradiction

Conclude: for all $n \in N$, $P(n)$

Proof by minimal counterexample

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 by minimal counterexample

Assumption: P a property on set N. R a well-founded relation on N
Minimal counterexample: show if n minimal such that not $P(n)$, then contradiction
Conclude: for all $n \in N$, $P(n)$

Example

Assumption: $P(n) = n$ can be written as a product of primes if $n > 2$. $<$ on $\mathbb{N}$.

Proof by minimal counterexample

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 by minimal counterexample

Assumption: P a property on set N. R a well-founded relation on N
Minimal counterexample: show if n minimal such that not $P(n)$, then contradiction
Conclude: for all $n \in N$, $P(n)$

Example

Assumption: $P(n) = n$ can be written as a product of primes if $n > 2$. $<$ on $\mathbb{N}$.
Minimal counterexample: let n be minimal and not a product of primes.

Proof by minimal counterexample

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 by minimal counterexample

Assumption: P a property on set N. R a well-founded relation on N
Minimal counterexample: show if n minimal such that not $P(n)$, then contradiction
Conclude: for all $n \in N$, $P(n)$

Example

Assumption: $P(n) = n$ can be written as a product of primes if $n > 2$. $<$ on $\mathbb{N}$.
Minimal counterexample: let n be minimal and not a product of primes.
Then $n = m \cdot k$ with $m, k < n$. By minimality m and k are products of primes, but then so is n. Contradiction.

Questions and methodology for structures

- When are two structures the same?
- When is one structure a sub-structure of another?
- How can we represent structures?
- What operations can we do on the structures?

Questions and methodology for structures

- What operations can we do on the structures?

For relations, functions, partial orders, well-founded relations.

Preservation

Definition

A property P is preserved by some operation, If P holds for the arguments, then it holds for the result.

Preservation

Definition

A property P is preserved by some operation, If P holds for the arguments, then it holds for the result.

Example

Positiveness is preserved by addition and multiplication. Negativeness is preserved by addition but not by multiplication.

Preservation

Definition

A property P is preserved by some operation, If P holds for the arguments, then it holds for the result.

Lemma

The componentwise extension preserves well-foundedness, i.e. if $\leq$ is a well-founded partial order, then so is $\leq_{comp}$.

Proof.

For a proof by contradiction, suppose $x_1 >_{\text{comp}} x_2 >_{\text{comp}} x_3 >_{\text{comp}} \dots$ were an infinite descending $\leq_{\text{comp}}$-chain, where $x_i = (x_{i1}, \dots, x_{ik})$, for some minimal k. Then for their first elements $x_{11} \geq x_{21} \geq x_{31} \geq \dots$. Either this contains an infinite descending $\leq$-chain, or there exists an N such that for all $n \geq N$, $x_{N1} = x_{n1}$ and then $(x_{N2}, \dots, x_{Nk}) >_{\text{comp}} (x_{N+1\,2}, \dots, x_{N+1\,k}) >_{\text{comp}} (x_{N+2\,2}, \dots, x_{N+2\,k}) >_{\text{comp}} \dots$ would be an infinite descending chain for a smaller k. Contradiction. ∎

Operations on relations

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;
- converse $a\ R^{-1}\ b$ if $b\ R\ a$;
  many names, notations: opposite, dual, inverse ...

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;
- converse $a\ R^{-1}\ b$ if $b\ R\ a$;
  many names, notations: opposite, dual, inverse ...
- intersection $a\ (R \cap S)\ b$ if $a\ R\ b$ and $a\ S\ b$;

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;
- converse $a\ R^{-1}\ b$ if $b\ R\ a$;
  many names, notations: opposite, dual, inverse ...
- intersection $a\ (R \cap S)\ b$ if $a\ R\ b$ and $a\ S\ b$;
- union $a\ (R \cup S)\ b$ if $a\ R\ b$ or $a\ S\ b$;

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;
- converse $a\ R^{-1}\ b$ if $b\ R\ a$;
  many names, notations: opposite, dual, inverse ...
- intersection $a\ (R \cap S)\ b$ if $a\ R\ b$ and $a\ S\ b$;
- union $a\ (R \cup S)\ b$ if $a\ R\ b$ or $a\ S\ b$;
- composition $a\ (R\ ;\ S)\ b$ if $\exists c \in A$, $a\ R\ c$ and $c\ S\ b$;

Operations on relations

Operations on relations

Let R, S be relations on A.

- identity $a\ I\ b$ if $a = b$;
- converse $a\ R^{-1}\ b$ if $b\ R\ a$;
  many names, notations: opposite, dual, inverse ...
- intersection $a\ (R \cap S)\ b$ if $a\ R\ b$ and $a\ S\ b$;
- union $a\ (R \cup S)\ b$ if $a\ R\ b$ or $a\ S\ b$;
- composition $a\ (R\ ;\ S)\ b$ if $\exists c \in A$, $a\ R\ c$ and $c\ S\ b$;
- product $(a, a')\ R \times S\ (b, b')$ if $a\ R\ b$ and $a'\ S\ b'$;
  relation on $A \times A$

Operations on functions?

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function?

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function?

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? × (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function? $\times$ (✓ iff $f = g$);

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function? $\times$ (✓ iff $f = g$);
- composition $f \,;\, g$ a function?

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function? $\times$ (✓ iff $f = g$);
- composition $f \,;\, g$ a function? ✓
  Mathematical notation $g \circ f$; g after f. Haskell notation `f . g`

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function? $\times$ (✓ iff $f = g$);
- composition $f \,;\, g$ a function? ✓
  Mathematical notation $g \circ f$; g after f. Haskell notation `f . g`
- product $f \times g$ a function?

Operations on functions?

Operation on functions?

Let f, g be functions on A.

- identity I a function? ✓
  Haskell notation `id`
- converse f^{-1} a function? $\times$ (✓ iff f a bijection: $f \,;\, f^{-1} = I$ and $f^{-1} \,;\, f = I$);
- intersection $f \cap g$ a function? $\times$ (✓ iff $f = g$);
- union $f \cup g$ a function? $\times$ (✓ iff $f = g$);
- composition $f \,;\, g$ a function? ✓
  Mathematical notation $g \circ f$; g after f. Haskell notation `f . g`
- product $f \times g$ a function? ✓

Operations on partial orders?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- product $\leq \times \sqsubseteq$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- product $\leq \times \sqsubseteq$ a partial order? ✓
  if $\leq = \sqsubseteq$, then special case of componentwise extension $\leq_{\text{comp}}$

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- product $\leq \times \sqsubseteq$ a partial order? ✓
  if $\leq = \sqsubseteq$, then special case of componentwise extension $\leq_{\text{comp}}$
- lexicographic order $\leq_{\text{lex}}$ a partial order?

Operations on partial orders?

Operations on partial orders?

Let $\leq, \sqsubseteq$ be partial orders on A.

- identity I a partial order? ✓
- converse $\geq = \leq^{-1}$ a partial order? ✓
- intersection $\leq \cap \sqsubseteq$ a partial order? ✓
- union $\leq \cup \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- composition $\leq ; \sqsubseteq$ a partial order? $\times$ (anti-symmetry, transitivity may fail)
- product $\leq \times \sqsubseteq$ a partial order? ✓
  if $\leq = \sqsubseteq$, then special case of componentwise extension $\leq_{\text{comp}}$
- lexicographic order $\leq_{\text{lex}}$ a partial order? ✓ (done before)

Operations on well-founded relations?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? $\checkmark$

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? $\checkmark$
- union $R \cup S$ well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? $\checkmark$
- union $R \cup S$ well-founded? $\times$

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? ✓
- union $R \cup S$ well-founded? $\times$
- composition $R ; S$ well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? ✓
- union $R \cup S$ well-founded? $\times$
- composition $R ; S$ well-founded? $\times$

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? ✓
- union $R \cup S$ well-founded? $\times$
- composition $R ; S$ well-founded? $\times$
- product $R \times S$ well-founded?

Operations on well-founded relations?

Operations on well-founded relations?

Let R, S be well-founded relations on A.

- identity I well-founded? $\times$ (strict part is)
- converse R^{-1} well-founded? $\times$
- intersection $R \cap S$ well-founded? ✓
- union $R \cup S$ well-founded? $\times$
- composition $R ; S$ well-founded? $\times$
- product $R \times S$ well-founded? ✓

Well-(founded)orders

Definition

A relation R is

- a well-founded order if it is well-founded and transitive
- a well-order if moreover for all a, b, $a\ R\ b$ or $a = b$ or $b\ R\ a$ holds

This extends to partial orders $\leq$ via their strict part $<$.

Well-(founded)orders

Definition

A relation R is

- a well-founded order if it is well-founded and transitive
- a well-order if moreover for all a, b, $a\ R\ b$ or $a = b$ or $b\ R\ a$ holds

This extends to partial orders $\leq$ via their strict part $<$.

Theorem

A relation is a well-founded order iff it is a well-founded strict order.

Proof.

It suffices to show that a well-founded transitive relation R is irreflexive. This holds, since if $a\ R\ a$ were to hold, then $\ldots R\ a\ R\ a\ R\ a$ would be an infinite descending chain, contradicting well-foundedness. ∎

Examples of well-(founded)orders

Example

Less-than is a well-order on the natural numbers, but greater-than is not (not well-founded), and neither is $\{(n, n+1) \mid n \in \mathbb{N}\}$ (not transitive).

Examples of well-(founded)orders

Example

Less-than is a well-order on the natural numbers, but greater-than is not (not well-founded), and neither is $\{(n, n+1) \mid n \in \mathbb{N}\}$ (not transitive).

Example

Divisibility is a well-founded order on the natural numbers: it's a partial order with its strict part well-founded. It is not a well-order.

Examples of well-(founded)orders

Example

Less-than is a well-order on the natural numbers, but greater-than is not (not well-founded), and neither is $\{(n, n+1) \mid n \in \mathbb{N}\}$ (not transitive).

Example

Divisibility is a well-founded order on the natural numbers: it's a partial order with its strict part well-founded. It is not a well-order.

Example

The prefix order is a well-founded order on the strings over Σ, but not a well-order in case Σ as more than 1 symbol (neither of ab, ba is a prefix of the other).

Ordinals

Motivation/intuition

Capture ordinals as in counting; e.g. the 1st, the 2nd, the 100th.

Ordinals

Motivation/intuition

Capture ordinals as in counting; e.g. the 1st, the 2nd, the 100th.

Definition

Well-orders $<$ on A and $\sqsubset$ on B are isomorphic if there is a bijection f from A to B with

1. if $a < a'$ then $f(a) \sqsubset f(a')$;
2. if $b \sqsubset b'$ then $f^{-1}(b) < f^{-1}(b')$;

Ordinals represent isomorphic well-orders.

Ordinals

Motivation/intuition

Capture ordinals as in counting; e.g. the 1st, the 2nd, the 100th.

Definition

Well-orders $<$ on A and $\sqsubset$ on B are isomorphic if there is a bijection f from A to B with

1. if $a < a'$ then $f(a) \sqsubset f(a')$;
2. if $b \sqsubset b'$ then $f^{-1}(b) < f^{-1}(b')$;

Ordinals represent isomorphic well-orders.

Example

$<$ on natural numbers isomorphic to $<_{\text{lex}}$ on words over $\{a\}$.

Ordinals

Motivation/intuition

Capture ordinals as in counting; e.g. the 1st, the 2nd, the 100th.

Definition

Well-orders $<$ on A and $\sqsubset$ on B are isomorphic if there is a bijection f from A to B with

1. if $a < a'$ then $f(a) \sqsubset f(a')$;
2. if $b \sqsubset b'$ then $f^{-1}(b) < f^{-1}(b')$;

Ordinals represent isomorphic well-orders.

Example

$<$ on natural numbers isomorphic to $<_{\text{lex}}$ on words over $\{a\}$.

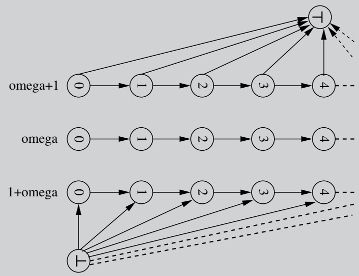
Example

Each finite well-order isomorphic to $<$ on $\{m \mid m < n\}$ for some $n \in N$.

Infinite ordinals

Example

Extending the ordinal ω of the natural numbers either with an element $\bot$ smaller than all natural numbers to $1 + \omega$, or with an element $\top$ greater than all natural numbers to $\omega + 1$, can be depicted (omitting many transitive arrows) as:



we see that ω and $1 + \omega$ are isomorphic, but non-isomorphic to $\omega + 1$.

Cardinals

Motivation/intuition

Capture cardinals as in counting: e.g. 1, 2, 100.
(only number no order)

Cardinals

Motivation/intuition

Capture cardinals as in counting: e.g. 1, 2, 100.
(only number no order)

Definition

If there exists a bijection $f : M \to N$, then the sets M and N are equinumerous or equipollent. Cardinals represent equinumerous sets.

Example

Each finite set equinumerous to set $\{m \mid m < n\}$ for some $n \in \mathbb{N}$.

Example

Adjoining $*$ to the natural numbers is equinumerous to the natural numbers; ω, $1 + \omega$, and $\omega + 1$ are equinumerous as sets of nodes (forgetting about the edges/order).