Discrete Structures II

Ulf Nilsson
TCSLAB, IDA, LiU

Overview

Topics covered

- Ordered sets
- Lattices and complete partial orders
- Ordinal numbers
- Well-founded and transfinite induction
- Fixed points
- Finite automata for infinite words

Some areas of application

- Semantics of programming languages
- Concurrency theory
- Type systems
- Inheritance
- Taxonomical reasoning
- Proof- and model-theory of logics
- Computability theory
- Formal verification

Preliminaries

Cartesian product

Definition...

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$$

Generalized to finite products...

$$A_1 \times \ldots \times A_n := \{(x_1, \ldots, x_n) \mid x_i \in A_i\}$$

Or simply...

$$A^n$$

(Set of n-tuples.)

Strings

An element $w \in \Sigma^n$ is also called a *string* of length $n \geq 0$. The set of all strings over a (finite) alphabet Σ is denoted Σ^*, and

$$\Sigma^* := \bigcup_{i \geq 0} \Sigma^i$$

A set of strings is called a *language*.

Relations

A relation R on A and B:

$$R \subseteq A \times B$$

Alternative notations

$$(a, b) \in R \text{ or } R(a, b) \text{ or } a \; R \; b$$

Properties of relations

A binary relation $R \subseteq A \times A$ is

- *reflexive* iff $R(x, x)$ for every $x \in A$.
- *irreflexive* iff $R(x, x)$ for no $x \in A$.
- *antisymmetric* iff $x = y$ whenever $R(x, y)$ and $R(y, x)$.
- *symmetric* iff $R(x, y)$ whenever $R(y, x)$.
- *transitive* iff $R(x, z)$ whenever $R(x, y)$ and $R(y, z)$.

More relations

Identity relation on A, denoted ID_A:

$R(x, y)$ iff $x = y$ and $x \in A$

Composition $R_1 \circ R_2$ of $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$:

$$R_1 \circ R_2 := \{(a, c) \in A \times C \mid \exists b \in B \; (R_1(a, b) \wedge R_2(b, c))\}.$$

Note: if $R \subseteq A \times B$ then $\mathsf{ID}_A \circ R = R \circ \mathsf{ID}_B = R$.

More on composition

Iterated Composition of $R \subseteq A \times A$

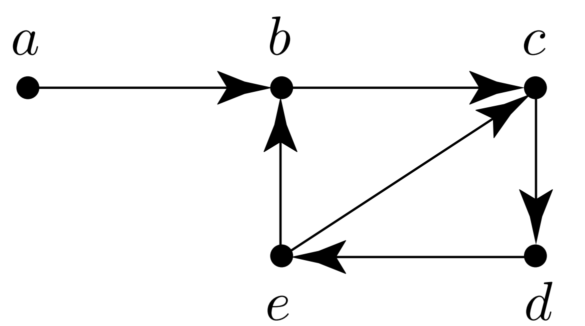
$$\begin{aligned} R^0 &:= \mathsf{ID}_A, \\ R^{n+1} &:= R^n \circ R \quad (n \in \mathbf{N}), \\ R^+ &:= \textstyle\bigcup_{n \in \mathbf{Z}^+} R^n, \\ R^* &:= \textstyle\bigcup_{n \in \mathbf{N}} R^n. \end{aligned}$$

R^+: the *transitive closure* of R,
R^*: the *reflexive and transitive closure* of R.

Example: Transition system

A transition system is a pair $(C, \Rightarrow)$ where

- C is a set of *configurations*;
- $\Rightarrow \subseteq (C \times C)$ is a *transition relation*.



$$\Rightarrow = \{(a,b),(b,c),(c,d),(d,e),(e,b),(e,c)\}$$

$$\Rightarrow^2 = \{(a,c),(b,d),(c,e),(d,b),(d,c),(e,c),(e,d)\}$$

Functions

Space of all *functions* from A to B denoted $A \to B$
$f\colon A \to B$ is a relation on $A \times B$ where each $a \in A$ is related to exactly one element in B.

Notation

$$(a, b) \in f \text{ or } (a \mapsto b) \in f \text{ or } f(a) = b$$

Graph of a function f

$$\{0 \mapsto 1, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 6, 4 \mapsto 24 \ldots\}.$$

Closedness

A set $B \subseteq A$ is *closed* under $f\colon A \to A$ iff $f(x) \in B$ for all $x \in B$, that is if $f(B) \subseteq B$.

Extends to n-ary functions $f\colon A^n \to A$.

Example: Regular Languages

Consider subsets of Σ^*, i.e. languages.
The set of regular languages is closed under

- complementation (if L is regular, then so is $\Sigma^* \setminus L$);
- union (if L_1, L_2 are regular, then so is $L_1 \cup L_2$);
- intersection (dito).

Digression

Note: A^n may be seen as the space of all functions from $\{0, \ldots, n-1\}$ to A.

Example: $(5, 4, 2) \in \mathbf{N}^3$ is isomorphic to $\{0 \mapsto 5, 1 \mapsto 4, 2 \mapsto 2\}$.

$\mathbf{N} \to A$ can be thought of as an infinite product "A^∞", but usually written A^ω.

Powersets

Powerset of A: the set of all subsets of a set A

Denoted: 2^A.

Note: 2^A may be viewed as $A \to \{0,1\}$.

Note: The space $A \to B$ is sometimes written B^A.

Example: Boolean interpretation

A boolean interpretation of a set of parameters *Var* is a mapping in $(\mathit{Var} \to \{0,1\})$. For instance, if *Var* $= \{x, y, z\}$

- $\sigma_0 = \{x \mapsto 0, y \mapsto 0, z \mapsto 0\}$
- $\sigma_1 = \{x \mapsto 1, y \mapsto 0, z \mapsto 0\}$
- $\sigma_2 = \{x \mapsto 0, y \mapsto 1, z \mapsto 0\}$
- $\sigma_3 = \{x \mapsto 1, y \mapsto 1, z \mapsto 0\}$
- $\sigma_4 = \{x \mapsto 0, y \mapsto 0, z \mapsto 1\}$
- $\sigma_5 = \{x \mapsto 1, y \mapsto 0, z \mapsto 1\}$
- $\sigma_6 = \{x \mapsto 0, y \mapsto 1, z \mapsto 1\}$
- $\sigma_7 = \{x \mapsto 1, y \mapsto 1, z \mapsto 1\}$

Example (cont)

...or they can be seen as elements of 2^{Var}

- $\sigma_0 = \emptyset$
- $\sigma_1 = \{x\}$
- $\sigma_2 = \{y\}$
- $\sigma_3 = \{x, y\}$
- $\sigma_4 = \{z\}$
- $\sigma_5 = \{x, z\}$
- $\sigma_6 = \{y, z\}$
- $\sigma_7 = \{x, y, z\}$

Basic orderings

Preorder/quasi ordering

Definition A relation $R \subseteq A \times A$ is called a *preorder* (or *quasi ordering*) if it is reflexive and transitive.

Partial order

Definition A preorder $R \subseteq A \times A$ is called a *partial order* if it is also antisymmetric.

Definition If $\leq \subseteq A \times A$ is a partial order then the pair $(A, \leq)$ is called a *partially ordered set*, or *poset*.

Every preorder induces a (unique) poset where $\leq$ is lifted to the equivalence classes of the relation

$$x \equiv y \text{ iff } x \leq y \text{ and } y \leq x$$

Example: Prefix order

Consider an alphabet Σ and its finite words Σ^*. Let $u, v \in \Sigma^*$ and denote by uv the concatenation of u and v. Define the relation $\trianglelefteq \subseteq \Sigma^* \times \Sigma^*$ as follows

$$u \trianglelefteq v \text{ iff there is a } w \in \Sigma^* \text{ such that } uw = v.$$

Example: Information order

Consider the following partial functions from $\mathbf{N}$ to $\mathbf{N}$

- $f_0 = \{0 \mapsto 1\}$
- $f_1 = \{0 \mapsto 1, 1 \mapsto 1\}$
- $f_2 = \{0 \mapsto 1, 1 \mapsto 1, 2 \mapsto 2\}$
- $f_3 = \{0 \mapsto 1, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 6\}$
- $g_2 = \{0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 1\}$

We say that e.g. f_3 is more defined than f_2 since $f_2 \subseteq f_3$, while e.g. f_3 and g_2 are unrelated. The ordering

$$f \leq g \text{ iff } f \subseteq g$$

is called the *information ordering*.

Strict order

Definition A relation $R \subseteq A \times A$ which is transitive and irreflexive is called a (*strict*) *partial order*.

Total orders/chains and anti-chains

Definition A poset $(A, \leq)$ is called a *total order* (or *chain*, or *linear order*) if either $a \leq b$ or $b \leq a$ for all $a, b \in A$.

Definition A poset $(A, \leq)$ is called an *anti-chain* if $x \leq y$ implies $x = y$, for all $x, y \in A$.

Used also in the context of strict orders.

Induced order

Let $\mathcal{A} := (A, \leq)$ be a poset and $B \subseteq A$. Then $\mathcal{B} := (B, \preceq)$ is called the *poset induced by* $\mathcal{A}$ if

$$x \preceq y \text{ iff } x \leq y \text{ for all } x, y \in B.$$

Componentwise and pointwise order

Theorem Let $(A, \leq)$ be a poset, and consider a relation $\preceq$ on $A \times A$ defined as follows

$$(x_1, y_1) \preceq (x_2, y_2) \text{ iff } x_1 \leq x_2 \wedge y_1 \leq y_2.$$

Then $(A \times A, \preceq)$ is a poset.

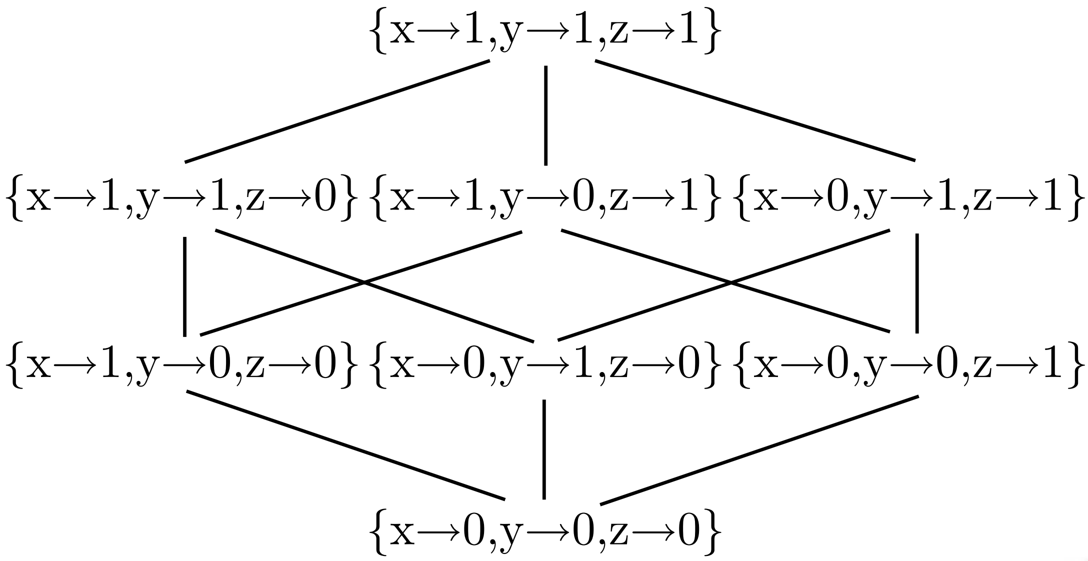
Theorem Let $(A, \leq)$ be a poset, and consider a relation $\preceq$ on $B \to A$ defined as follows

$$\sigma_1 \preceq \sigma_2 \text{ iff } \sigma_1(x) \leq \sigma_2(x) \text{ for all } x \in B.$$

Then $(B \to A, \preceq)$ is a poset.

Example: Pointwise order

Consider the function space $(Var \rightarrow \{0,1\})$ of boolean interpretations of *Var*, given the poset $(\{0,1\}, \leq)$:



Lexicographical order

Theorem Let $\Sigma = \{a_1, \ldots, a_n\}$ be a finite alphabet totally ordered $a_1 < \ldots < a_n$. Let Σ^* be the set of all (possibly empty) strings from Σ and define $x_1 \ldots x_i \sqsubset y_1 \ldots y_j$ iff

- $i < j$ and $x_1 \ldots x_i = y_1 \ldots y_i$, or
- there is some $k < i$ such that $x_{k+1} < y_{k+1}$ and $x_1 \ldots x_k = y_1 \ldots y_k$.

Then $(\Sigma^*, \sqsubset)$ is a (strict) total order.

Well-founded relations and well-orders

Extremal elements

Definition Consider a relation $R \subseteq A \times A$. An element $a \in A$ is called R-*minimal* (or simply minimal) if there is no $b \in A$ such that $b \; R \; a$.
Similary, $a \in A$ is called *maximal* if there is no $b \in A$ such that $a \; R \; b$.

Definition An element $a \in A$ is called *least* if $a \; R \; b$ for all $b \in A$; it is called *greatest* if $b \; R \; a$ for all $b \in A$.

Well-founded and well-ordered sets

Definition A relation $R \subseteq A \times A$ is said to be *well-founded* if every non-empty subset of A has an R-minimal element.

Definition A strict total order $(A, <)$ which is well-founded is called a well-order.

More on well-founded sets

Theorem Any subset $(B, <)$ of a well-order $(A, <)$ is a well-order.

Definition Let $(A, \leq)$ be a poset. A well-order $x_0 < x_1 < \dots$ where $\{x_0, x_1, \dots\} \subseteq A$ is called an *ascending chain in* A. Descending chain is defined dually.

Theorem A relation $< \subseteq A \times A$ is well-founded iff $(A, <)$ contains no infinite descending chain $\dots < x_2 < x_1 < x_0$.

Order ideals

Definition Let $(A, \leq)$ be a poset. A set $B \subseteq A$ is called a *down-set* (or an *order ideal*) iff

$$y \in B \text{ whenever } x \in B \text{ and } y \leq x.$$

A set $B \subseteq A$ induces a down-set, denoted $B{\downarrow}$,

$$B{\downarrow} := \{x \in A \mid \exists y \in B, x \leq y\}.$$

By $\mathcal{O}(A)$ we denote the set of all down-sets in A,

$$\{B{\downarrow} \mid B \subseteq A\}.$$

A notion of *up-set*, also called *order filter*, is defined dually.

Lattices

Upper and lower bounds

Definition Let $(A, \leq)$ be a poset and $B \subseteq A$. Then $x \in A$ is called an *upper bound* of B iff $y \leq x$ for all $y \in B$ (often written $B \leq x$ by abuse of notation). The notion of *lower bound* is defined dually.

Definition Let $(A, \leq)$ be a poset and $B \subseteq A$. Then $x \in A$ is called a *least upper bound* of B iff $B \leq x$ and $x \leq y$ whenever $B \leq y$. The notion of *greatest lower bound* is defined dually.

Lattice

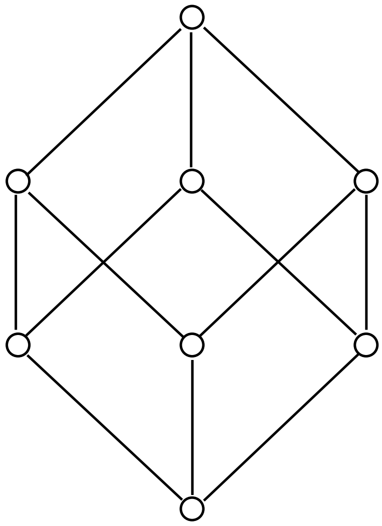
Definition A *lattice* is a poset $(A, \leq)$ where every pair of elements $x, y \in A$ has a least upper bound denoted $x \vee y$ and greatest lower bound denoted $x \wedge y$.

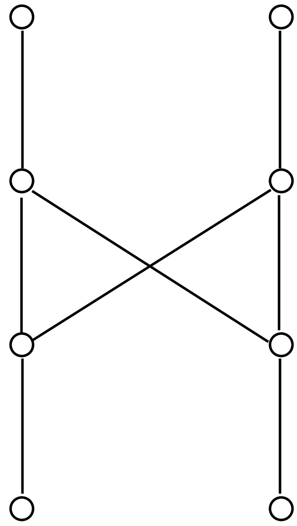
Synonyms:

Least upper bound/lub/join/supremum

Greatest lower bound/glb/meet/infimum

Lattice





Lattice terminology

Definition Let $(A, \leq)$ be a lattice. An element $a \in A$ is said to *cover* an element $b \in A$ iff $a > b$ and there is no $c \in A$ such that $a > c > b$.

Definition The *length* of a poset $(A, \leq)$ (and hence lattice) is $|C| - 1$ where C is the longest chain in A.

Complete lattice

Definition A *complete lattice* is a poset $(A, \leq)$ where every subset $B \subseteq A$ (finite or infinite) has a least upper bound $\bigvee B$ and a greatest lower bound $\bigwedge B$.

$\bigvee A$ is called the *top* element and is usually denoted $\top$.

$\bigwedge A$ is called the *bottom* element and is denoted $\bot$.

Theorem Any finite lattice is a complete lattice.

Complemented lattice

Definition Let $(A, \leq)$ be a lattice with $\bot$ and $\top$. We say that $a \in A$ is the *complement* of $b \in A$ iff $a \vee b = \top$ and $a \wedge b = \bot$.

Definition We say that a lattice is *complemented* if every element has a complement.

Distributive and Boolean lattice

Definition A lattice $(A, \leq)$ is said to be *distributive* iff $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in A$.

Definition A lattice $(A, \leq)$ is said to be *Boolean* iff it is complemented and distributive.

More on lattices

Definition Let A be a set and $B \subseteq 2^A$. If $(B, \subseteq)$ is a (complete) lattice, then we refer to it as a (complete) *lattice of sets*.

Theorem We have the following results:

1. Any lattice of sets is distributive.
2. $(2^A, \subseteq)$ is distributive, and Boolean.
3. If $(A, \leq)$ is Boolean then the complement of all $x \in A$ is unique.

Lattices as algebras

The algebraic structure $(A, \otimes, \oplus)$ is a lattice if the operations satisfy

(L_1) Idempotency: $a \otimes a = a \oplus a = a$

(L_2) Commutativity: $a \otimes b = b \otimes a$ and $a \oplus b = b \oplus a$

(L_3) Associativity: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ and $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

(L_4) Absorption: $a \otimes (a \oplus b) = a$ and $a \oplus (a \otimes b) = a$

The algebra induces partial order: $x \leq y$ iff $x \otimes y = x$ (iff $x \oplus y = y$).

Complete partial orders (cpo's)

Complete partial order

Definition A partial order $(A, \leq)$ is said to be *complete* if it has a bottom element $\perp$ and if each ascending chain

$$a_0 < a_1 < a_2 < ...$$

has a least upper bound $\bigvee\{a_0, a_1, a_2, ...\}$.

Ordinal numbers

Cardinal numbers

Two sets A and B are isomorphic iff there exists a bijective map $f\colon A \to B$ (and hence a bijection $f^{-1}\colon B \to A$). Notation $A \sim B$.

$\sim$ is an equivalence relation.

A cardinal number is an equivalence class of all isomorphic sets.

(Order-) isomorphism

Definition A function f from $(A, <)$ to $(B, \prec)$ is called *monotonic* (*isotone*, *order-preserving*) iff $x < y$ implies $f(x) \prec f(y)$ for all $x, y \in A$.

Definition A monotonic map f from $(A, <)$ into $(B, \prec)$ is called

- a *monomorphism* if f is injective;
- an *epimorphism* if f is onto (surjective);
- an *isomorphism* if f is bijective (injective and onto).

Notation: $A \simeq B$ when A and B are isomorphic (the order is implicitly understood).

Ordinal numbers

Definition An ordinal (number) is an equivalence class of all (order-)isomorphic well-orders.

Notation: The finite ordinals $\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, ...$

Definition Ordinals containing well-orders with a maximal element are called *successor ordinals*. Otherwise they are called *limit ordinals*.

Convention: we often identify a well-order, e.g. $1 < 2 < 3$, with its ordinal number, e.g. $\mathbf{3}$, and write that $\mathbf{3} = 1 < 2 < 3$.

Finite von Neumann ordinals

NOTATION	CANONICAL REPRESENTATION
$\mathbf{0}$	$\emptyset$
$\mathbf{1}$	$\{\emptyset\} = \mathbf{0} \cup \{\mathbf{0}\} = \{\mathbf{0}\}$
$\mathbf{2}$	$\{\emptyset, \{\emptyset\}\} = \mathbf{1} \cup \{\mathbf{1}\} = \{\mathbf{0}, \mathbf{1}\}$
$\mathbf{3}$	$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \mathbf{2} \cup \{\mathbf{2}\} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$
$\mathbf{4}$	$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} =$ $\mathbf{3} \cup \{\mathbf{3}\} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$
etc.	

More generally $\alpha + 1 = \alpha \cup \{\alpha\}$.

Infinite (countable) ordinals

Least infinite ordinal: $\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, ...$
Denoted: ω

Then follows: $\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, ..., \omega$
Denoted: $\omega + \mathbf{1}$

...and: $\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, ..., \omega, \omega + \mathbf{1}$
Denoted: $\omega + \mathbf{2}$

...up to: $\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, ..., \omega, \omega + \mathbf{1}, \omega + \mathbf{2}, ...$
Denoted: $\omega + \omega$ (or $\omega \cdot \mathbf{2}$)

von Neumann ordinals

More generally

- $\emptyset$ is a von Neumann ordinal,
- if α is a von Neumann ordinal then so is $\alpha \cup \{\alpha\}$,
- if $\{\alpha_i\}_{i \in I}$ is a set of von Neumann ordinals, then so is

$$\bigcup_{i \in I} \alpha_i$$

Addition of ordinals

Consider two ordinals α and β. Let $A \in \alpha$ and $B \in \beta$ be disjoint well-orders.

Then $\alpha + \beta$ is the equivalence class of all well-orders isomorphic to $A \cup B$ ordered as before and where in addition $x < y$ for all $x \in A$ and $y \in B$.

Addition of finite ordinals reduces to ordinary addition of natural numbers, but ...

Ordinal addition isn't commutative

Consider

$$\omega = \{1, 2, 3, 4, ...\} \text{ and } \mathbf{1} = \{0\}.$$

Then $\omega + \mathbf{1}$ is $1, 2, 3, 4, ..., 0$ which is isomorphic to $0, 1, 2, ..., \omega$.

But $\mathbf{1} + \omega$ is $0, 1, 2, 3, 4, ...$ which is the limit ordinal ω.

Hence, $\mathbf{1} + \omega \neq \omega + \mathbf{1}$.

Multiplication of ordinals

Consider two ordinals α and β. Let $A \in \alpha$ and $B \in \beta$.

Then $\alpha \cdot \beta$ is the equivalence class of all well-orders isomorphic to $\{(a, b) \mid a \in A$ and $b \in B\}$ where

$(a_1, b_1) \prec (a_2, b_2)$ iff either $b_1 < b_2$, or $b_1 = b_2$ and $a_1 < a_2$.

Multiplication of finite ordinals reduces to ordinary multiplication of natural numbers, but...

Multiplication isn't commutative

$\mathbf{2} \cdot \omega$ is

$$(0,0),(1,0),(0,1),(1,1),(0,2),(1,2),...$$

which is isomorphic to ω.

$\omega \cdot \mathbf{2}$ is

$$(0,0),(1,0),(2,0),(3,0),...,(0,1),(1,1),(2,1),(3,1),...$$

which is isomorhic to $\omega + \omega$.

Hence, $\omega \cdot \mathbf{2} = \omega + \omega \neq \mathbf{2} \cdot \omega = \omega$.

Properties of ordinal arithmetic

For all ordinals α, β, γ:

- $\alpha + \mathbf{0} = \mathbf{0} + \alpha = \alpha$
- $\omega + \mathbf{1} \neq \mathbf{1} + \omega$
- $\alpha \cdot \mathbf{1} = \mathbf{1} \cdot \alpha = \alpha$
- $\omega + \omega = \omega \cdot \mathbf{2} \neq \mathbf{2} \cdot \omega = \omega$
- If $\beta \neq \mathbf{0}$ then $\alpha < \alpha + \beta$
- If $\alpha < \beta$ then $\alpha + \gamma \leq \beta + \gamma$
- If $\alpha < \beta$ then $\gamma + \alpha < \gamma + \beta$
- $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
- $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

Ascending ordinal powers

Consider a function $f\colon A \to A$ on a complete lattice $(A, \leq)$. The (ascending) ordinal powers of f are

$$\begin{aligned} f^0(x) &:= x \\ f^{\alpha+1}(x) &:= f(f^\alpha(x)) \text{ for successor ordinals } \alpha + 1 \\ f^\alpha(x) &:= \bigvee_{\beta<\alpha} f^\beta(x) \text{ for limit ordinals } \alpha \end{aligned}$$

When x equals $\perp$ we write f^α instead of $f^\alpha(\perp)$.

Descending ordinal powers

$$
\begin{array}{lcl}
f^0(x) & := & x \\
f^{\alpha+1}(x) & := & f(f^\alpha(x)) \text{ for successor ordinals } \alpha+1 \\
f^\alpha(x) & := & \bigwedge_{\beta<\alpha} f^\beta(x) \text{ for limit ordinals } \alpha
\end{array}
$$

Principles of induction

Standard inductions

Standard induction derivation rule:

$$\frac{P(0) \qquad \forall n \in \mathbf{N}\ (P(n) \Rightarrow P(n+1))}{\forall n \in \mathbf{N}\ P(n)} \,.$$

Applies to any well-ordered set isomorphic to ω.

Strong mathematical induction

$$\frac{P(0) \qquad \forall n \in \mathbf{N}\ (P(0) \wedge \ldots \wedge P(n) \Rightarrow P(n+1))}{\forall n \in \mathbf{N}\ P(n)}$$

or more economically

$$\frac{\forall n \in \mathbf{N}\ (P(0) \wedge \ldots \wedge P(n-1) \Rightarrow P(n))}{\forall n \in \mathbf{N}\ P(n)} \,.$$

Well-founded induction

Inductive definition

An inductive definition of A consists of three statements

- one or more *base cases*, B, saying that $B \subseteq A$,
- one or more *inductive cases*, saying schematically that if $x \in A$ and $R(x, y)$, then $y \in A$,
- an *extremal* condition stating that A is the least set closed under the previous two.

Let $\mathcal{R}(X) := \{y \mid \exists x \in X, R(x, y)\}$. Then A is the least set X such that

$B \subseteq X$ and $\mathcal{R}(X) \subseteq X$, that is, $B \cup \mathcal{R}(X) \subseteq X$

(A, R) is typically well-founded (or can be made well-founded) with minimal elements B.

Well-founded induction principle

Let $(A, \prec)$ be a well-founded set and P a property of A.

1. If P holds of all minimal elements of A, and
2. whenever P holds of all x such that $x \prec y$ then P holds of y,

then P holds of all $x \in A$.

Well-founded induction principle II

As a derivation rule:

$$\frac{\forall y \in A\ (\forall x \in A\ (x < y \Rightarrow P(x)) \Rightarrow P(y))}{\forall x \in A\ P(x)}\ .$$

Transfinite induction

Transfinite induction principle

Let P be a property of ordinals, then P is true of every ordinal if

- P is true of 0,
- P is true of $\alpha + 1$ whenever P is true of α,
- P is true of β whenever β is a limit ordinal and P is true of every $\alpha < \beta$.

Transfinite induction II

Theorem Let $(A, \leq)$ be a complete lattice and assume that $f\colon A \to A$ is monotonic. We prove that $f^\alpha \leq f^{\alpha+1}$ for all ordinals α.

Lemma Let $(A, \leq)$ be a complete lattice and assume that $f\colon A \to A$ is monotonic. If $B \subseteq A$ then $f(\bigvee B) \geq \bigvee \{f(x) \mid x \in B\}$.