« Mathematical foundations: (1) Naïve set theory »

Patrick Cousot
Jerome C. Hunsaker Visiting Professor
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics
cousot@mit.edu
www.mit.edu/~cousot

Course 16.399: "Abstract interpretation"

http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/

Set theory

– In naïve set theory everything is a set, including the empty set $\emptyset$; So any collection of objects can be regarded as a single entity (i.e. a set)
– A set is a collection of elements which are sets (but sets in sets in sets ... cannot go for ever);
– In practice one consider a universe of objects (which are not sets and called atoms) out of which are built sets of objects, set of sets of objects, etc.

Georg F. Cantor

Reference

[1] Cantor, G., 1932, "Gesammelte Abhandlungen mathematischen und philosohischen Inhalts", E. Zermelo, Ed. Berlin: Springer-Verlag.

Sets

Membership

- $a \in x$ means that the object a belongs to/is an element of the set x
- $a \notin x$ means that the object a does not belong to/is not an element of the set x:

$$(a \notin x) \stackrel{\text{def}}{=} \neg(a \in x)$$

Logical symbols

If P, Q, ... are logical statements about sets, then we use the following abbreviations:

- $P \wedge Q$ abbreviates "P and Q"
- $\neg P$ abbreviates "not P"
- $\forall x : P$ abbreviates "forall x, P"

Additional notations are as follows:

$P \vee Q \stackrel{\text{def}}{=} \neg((\neg P) \wedge (\neg Q))$	"P or Q"
$P \Longrightarrow Q \stackrel{\text{def}}{=} (\neg P) \vee Q$	"P implies Q"
$P \iff Q \stackrel{\text{def}}{=} (P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$	"P iff[1] Q"
$P \veebar Q \stackrel{\text{def}}{=} (P \vee Q) \wedge \neg(P \wedge Q)$	"P exclusive or Q"
$\exists x : P \stackrel{\text{def}}{=} \neg(\forall x : (\neg P))$	"there exists x such that P"

$$\exists a \in S : P \stackrel{\text{def}}{=} \exists a : a \in S \wedge P$$

$$\exists a_1, a_2, \ldots, a_n \in S : P \stackrel{\text{def}}{=} \exists a_1 \in S : \exists a_2, \ldots, a_n \in S : P$$

$$\forall a \in S : P \stackrel{\text{def}}{=} \forall a : (a \in S) \Longrightarrow P$$

$$\forall a_1, a_2, \ldots, a_n \in S : P \stackrel{\text{def}}{=} \forall a_1 \in S : \forall a_2, \ldots, a_n \in S : P$$

[1] if and only if

Comparison of sets

$x \subseteq y \stackrel{\text{def}}{=} \forall a : (a \in x \Longrightarrow a \in y)$	inclusion
$x \supseteq y \stackrel{\text{def}}{=} y \subseteq x$	superset
$x = y \stackrel{\text{def}}{=} (x \subseteq y) \wedge (y \subseteq x)$	equality
$x \neq y \stackrel{\text{def}}{=} \neg(x = y)$	inequality
$x \subset y \stackrel{\text{def}}{=} (x \subseteq y) \wedge (x \neq y)$	strict inclusion
$x \supset y \stackrel{\text{def}}{=} (x \supseteq y) \wedge (x \neq y)$	strict superset

Operations on sets

$(z = x \cup y) \stackrel{\text{def}}{=} \forall a : (a \in z) \Leftrightarrow (a \in x \vee a \in y)$ union

$(z = x \cap y) \stackrel{\text{def}}{=} \forall a : (a \in z) \Leftrightarrow (a \in x \wedge a \in y)$ intersection

$(z = x \setminus y) \stackrel{\text{def}}{=} \forall a : (a \in z) \Leftrightarrow (a \in x \wedge a \notin y)$ difference

Partial order

$\subseteq$ is a *partial order* in that:

$$\begin{array}{rl} x \subseteq x & \text{reflexivity} \\ (x \subseteq y \wedge y \subseteq x) \Longrightarrow (x = y) & \text{antisymetry} \\ (x \subseteq y) \wedge (y \subseteq z) \Longrightarrow (x \subseteq z) & \text{transitivity} \end{array}$$

$\subset$ is a *strict partial order* in that:

$$\begin{array}{rl} \neg(x \subset x) & \text{irrreflexivity} \\ (x \subset y) \wedge (y \subset z) \Longrightarrow (x \subset z) & \text{transitivity} \end{array}$$

Set theoretic laws

Intuition provided by *Venn diagrams* but better proved formally from the definitions.

$$\begin{array}{rcll} x \cup x & = & x & \\ x \cap x & = & x & \\ x & \subseteq & x \cup y & \text{upper bound} \\ x \cap y & \subseteq & x & \text{lower bound} \\ x \cup y & = & y \cup x & \text{commutativity} \\ x \cap y & = & y \cap x & \\ (x \subseteq z) \wedge (y \subseteq z) & \Longrightarrow & (x \cup y) \subseteq z & \text{lub}^{2} \\ (z \subseteq x) \wedge (z \subseteq y) & \Longrightarrow & z \subseteq (x \cap y) & \text{glb}^{3} \end{array}$$

[2] lub: least upper bound.
[3] glb: greatest lower bound

$$\begin{array}{rcll} x \cup (y \cup z) & = & (x \cup y) \cup z & \text{associativity} \\ x \cap (y \cap z) & = & (x \cap y) \cup z & \\ x \cup (y \cap z) & = & (x \cup y) \cap (x \cup z) & \text{distributivity} \\ x \cap (y \cup z) & = & (x \cap y) \cup (x \cap z) & \\ x \subseteq y & \Longleftrightarrow & (x \cup y) = y & \\ & & (x \cap y) = x & \\ x \setminus y & = & x \setminus (x \cap y) & \\ z \setminus (z \setminus x) & = & x & \\ x \subseteq y & \Longleftrightarrow & (z \setminus y) \subseteq (z \setminus x) & \\ x \cup (z \setminus x) & = & z & \\ z \setminus (x \cup y) & = & (z \setminus x) \cap (z \setminus y) & \\ z \setminus (x \cap y) & = & (z \setminus x) \cup (z \setminus y) & \end{array}$$

Empty set

- $\forall a : (a \notin \emptyset)$ — Definition of the empty set
- The emptyset is unique [4].
- Emptyset laws:

$$\begin{array}{rclcrcl} x \setminus \emptyset &=& x & \qquad & \emptyset &\subseteq& x \\ x \setminus x &=& \emptyset & & x \cup \emptyset &=& x \\ x \cap (y \setminus x) &=& \emptyset & & x \cap \emptyset &=& \emptyset \end{array}$$

[4] $[\forall a.(a \notin x)] \Longrightarrow [(\forall a : (a \notin x) \Longrightarrow (a \notin \emptyset)) \wedge (\forall a : (a \notin \emptyset) \Longrightarrow (a \notin x))] \Longrightarrow [(\forall a : (a \in \emptyset) \Longrightarrow (a \in x)) \wedge (\forall a : (a \in x) \Longrightarrow (at \in \emptyset))] \Longrightarrow [\emptyset \subseteq x \wedge x \subseteq \emptyset] \Longrightarrow [x = \emptyset]$.

Operations on set

Notations for sets

- Definitions in extension:
  - $\emptyset$ — Empty set
  - $\{a\}$ — Singleton
  - $\{a, b\}$ — Doubleton $(a \neq b)$
  - $\{a_1, \ldots, a_n\}$ — Finite set
  - $\{a_1, \ldots, a_n, \ldots\}$ — Infinite set
- Definition in comprehension:
  - $\{a \mid P(a)\}$ Examples:

$$\begin{array}{rcl} x \cup y &=& \{a \mid a \in x \vee a \in y\} \\ x \cap y &=& \{a \mid a \in x \wedge a \in y\} \\ x \setminus y &=& \{a \mid a \in x \wedge a \notin y\} \end{array}$$

Pairs

- $\langle a,\, b\rangle \stackrel{\text{def}}{=} \{\{a\}, \{a, b\}\}$
- $\langle a,\, b\rangle_1 = a$ — first projection [5]
- $\langle a,\, b\rangle_2 = b$ — second projection [6]
- $x_0,\, x_1$ undefined for non-pairs

[5] Other notations are $\langle a,\, b\rangle.1$, $\langle a,\, b\rangle \downarrow 1, \ldots$ Formally $\langle a,\, b\rangle_1 \stackrel{\text{def}}{=} \bigcup\bigcap \langle a,\, b\rangle = \bigcup\bigcap\{\{a\}, \{a, b\}\} = \bigcup\{a\} = a$.

[6] Formally, if $\bigcup \langle a,\, b\rangle = \bigcap \langle a,\, b\rangle$ then $a = b$ whence $\langle a,\, b\rangle_2 \stackrel{\text{def}}{=} \bigcup\bigcup \langle a,\, b\rangle = \bigcup\bigcup\{\{b\}\} = \bigcup\{b\} = b$. Otherwise $\bigcup \langle a,\, b\rangle \neq \bigcap \langle a,\, b\rangle$ that is $a \neq b$, in which case $\langle a,\, b\rangle_2 \stackrel{\text{def}}{=} \bigcup(\bigcup \langle a,\, b\rangle \setminus \bigcap \langle a,\, b\rangle) = \bigcup(\bigcup\{\{a\}, \{a, b\}\} \setminus \bigcap\{\{a\}, \{a, b\}\}) = \bigcup(\bigcup\{a, b\} \setminus \{a\}) = \bigcup\{b\} = b$.

Tuples

- $\langle a_1, \ldots, a_{n+1} \rangle \stackrel{\text{def}}{=} \langle \langle a_1, \ldots, a_n \rangle, a_{n+1} \rangle$ tuple
- $\langle a_1, \ldots, a_n \rangle_i \stackrel{\text{def}}{=} a_i$ $i = 1, \ldots, n$ projection
- Law:
  $\langle a_1, \ldots, a_n \rangle = \langle a'_1, \ldots, a'_n \rangle \Leftrightarrow a_1 = a'_1 \wedge \ldots \wedge a_n = a'_n$

Powerset

- $\wp(x) \stackrel{\text{def}}{=} \{y \mid y \subseteq x\}$ powerset
- $\bigcup y \stackrel{\text{def}}{=} \{a \mid \exists x \in y : a \in x\}$ Union
- $\bigcap y \stackrel{\text{def}}{=} \{a \mid \forall x \in y : a \in x\}$ Intersection
- Laws:

$$x \cup y = \bigcup\{x, y\} \qquad \bigcap\{x\} = x$$
$$x \cap y = \bigcap\{x, y\} \qquad \bigcup\emptyset = \emptyset$$
$$\bigcup\{x\} = x \qquad \bigcap\emptyset = \{a \mid \mathit{true}\} \quad \text{Universe}$$

Cartesian product

- $x \times y \stackrel{\text{def}}{=} \{\langle a, b \rangle \mid a \in x \wedge b \in y\}$
- $x_1 \times \ldots \times x_{n+1} \stackrel{\text{def}}{=} (x_1 \times \ldots \times x_n) \times x_{n+1}$ so
  $x_1 \times \ldots \times x_n = \{\langle a_1, \ldots, a_n \rangle \mid a_1 \in x_1 \wedge \ldots \wedge a_n \in x_n\}$
- $x^n \stackrel{\text{def}}{=} \underbrace{x \times \ldots \times x}_{n \text{ times}}$
- $x^0 \stackrel{\text{def}}{=} \emptyset$

Families (indexed set of sets)

- $x = \{y_i \mid i \in I\}$ I indexing set for the elements of x
- $\bigcup_{i \in I} y_i \stackrel{\text{def}}{=} \bigcup x$
  $= \{a \mid \exists i \in I : a \in y_i\}$
- $\bigcap_{i \in I} y_i \stackrel{\text{def}}{=} \bigcap x$
  $= \{a \mid \forall i \in I : a \in y_i\}$
- Laws:

$$\forall i \in I : (x_i \subseteq y) \Longrightarrow (\bigcup_{i \in I} x_i \subseteq y)$$
$$\forall i \in I : (y \subseteq x_i) \Longrightarrow (y \subseteq \bigcap_{i \in I} x_i)$$

$$\bigcup_{i\in I}(x_i \cup y_i) = (\bigcup_{i\in I} x_i) \cup (\bigcup_{i\in I} y_i)$$

$$\bigcap_{i\in I}(x_i \cap y_i) = (\bigcap_{i\in I} x_i) \cap (\bigcap_{i\in I} y_i)$$

$$\bigcup_{i\in I}(x_i \cap y) = (\bigcup_{i\in I}(x_i)) \cap y$$

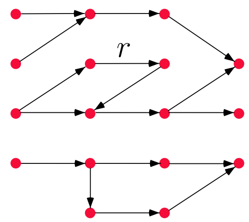
$$\bigcap_{i\in I}(x_i \cup y) = (\bigcap_{i\in I}(x_i)) \cup y$$

$$z \setminus \bigcup_{i\in I} x_i = \bigcap_{i\in I}(z \setminus x_i)$$

$$z \setminus \bigcap_{i\in I} x_i = \bigcup_{i\in I}(z \setminus x_i)$$

Relations

- $r \subseteq x$ unary relation on x
- $r \subseteq x \times y$ binary relation
- $r \subseteq x_1 \times \ldots \times x_n$ n-ary relation
- Graphical representation of a relation r on a finite set x:



●	elements of the set x
a ●⟶● b	$\langle a, b\rangle \in r$

Relations

Notations for relations

- If $r \subseteq x_1 \times \ldots \times x_n$ then we use the notation:

$$r(a_1, \ldots, a_n) \stackrel{\text{def}}{=} \langle a_1, \ldots, a_n\rangle \in r$$

- In the specific case of binary relation, we also use:

$$a \; r \; b \stackrel{\text{def}}{=} \langle a, b\rangle \in r \quad \text{example: } 5 \leq 7$$

$$a \stackrel{r}{\longrightarrow} b \stackrel{\text{def}}{=} \langle a, b\rangle \in r$$

Properties of binary relations

Let $r \subseteq x \times x$ be a binary relation on the set x

- $\forall a \in x : (a \; r \; a)$ reflexive
- $\forall a, b \in x : (a \; r \; b) \iff (b \; r \; a)$ symmetric
- $\forall a, b \in x : (a \; r \; b \wedge a \neq b) \Longrightarrow \neg(b \; r \; a)$ antisymmetric
- $\forall a, b \in x : (a \neq b) \Longrightarrow (a \; r \; b \vee b \; r \; a)$ connected
- $\forall a, b, c \in x : (a \; r \; b) \wedge (b \; r \; c) \Longrightarrow (a \; r \; c)$ transitive

Reflexive transitive closure

Operations on relations

- $\emptyset$ empty relation
- $\mathbf{1}_x \stackrel{\text{def}}{=} \{\langle a, a\rangle \mid a \in x\}$ identity
- $r^{-1} \stackrel{\text{def}}{=} \{\langle b, a\rangle \mid \langle a, b\rangle \in r\}$ inverse
- $r_1 \circ r_2 \stackrel{\text{def}}{=} \{\langle a, c\rangle \mid \exists b : \langle a, b\rangle \in r_1 \wedge \langle b, c\rangle \in r_2\}$ composition
- set operations $r_1 \cup r_2$, $r_1 \cap r_2$, $r_1 \setminus r_2$

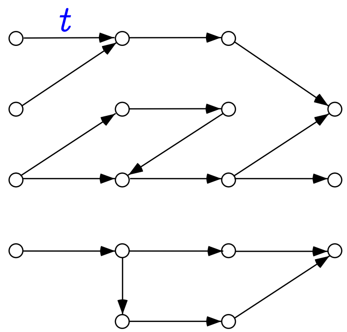
Reflexive transitive closure of a relation

Let r be a relation on x:

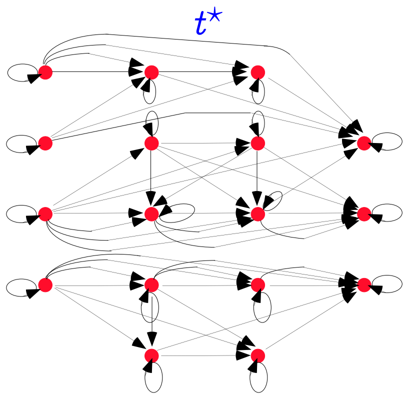
- $r^0 \stackrel{\text{def}}{=} \mathbf{1}_x$ powers
- $r^{n+1} \stackrel{\text{def}}{=} r^n \circ r \; (= r \circ r^n)$
- $r^\star \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} r^n$ reflexive transitive closure
- $r^+ \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}\setminus\{0\}} r^n$ strict transitive closure

  so $r^\star = r^+ \cup \mathbf{1}_x$

Example of relation



The reflexive transitive closure of the example relation



Equational definition of the reflexive transitive closure

– $t^\star = \mathbf{1}_x \cup t \circ t^\star$

PROOF.

$$
\begin{aligned}
& t^\star \\
= \; & \bigcup_{n \in \mathbb{N}} t^n && \text{(def. } t^\star\text{)} \\
= \; & t^0 \cup \bigcup_{n \in \mathbb{N}\setminus\{0\}} t^n && \text{(isolating } t^0\text{)}
\end{aligned}
$$

$$
\begin{aligned}
= \; & \mathbf{1}_x \cup \bigcup_{k \in \mathbb{N}} t^{k+1} && \text{(def. } t^0 \text{ and } k+1=n\text{)} \\
= \; & \mathbf{1}_x \cup \bigcup_{k \in \mathbb{N}} t \circ t^k && \text{(def. power)} \\
= \; & \mathbf{1}_x \cup t \circ (\bigcup_{k \in \mathbb{N}} t^k) && \text{(def. } \circ\text{)} \\
= \; & \mathbf{1}_x \cup t \circ t^\star && \text{(def. } t^\star\text{)}
\end{aligned}
$$

□

- If $r = \mathbf{1}_x \cup t \circ r$ then $t^\star \subseteq r$

PROOF. - $t^0 = \mathbf{1}_x \subseteq \mathbf{1}_x \cup t \circ r = r$ so $t^0 \subseteq r$
- if $t^n \subseteq r$ then $t^{n+1} = t \circ t^n \neq\subseteq t \circ r \subseteq \mathbf{1}_x \cup t \circ r = r$ so $t^{n+1} \subseteq r$
- By recurrence, $\forall n \in \mathbb{N} : (t^n \subseteq r)$
- $t^\star = \bigcup_{n\in\mathbb{N}} t^n \subseteq r$

□

Equivalences and partitions

- If follows that $r^\star$ is the $\subseteq$-least solution of the equation:

$$X = \mathbf{1}_x \cup t \circ X$$ [7]

- This least solution is unique.

PROOF. - let r_1 and r_2 be two solutions to $X = \mathbf{1}_x \cup t \circ X$
- $r_1 \subseteq r_2$ since r_1 is the least solution
- $r_2 \subseteq r_1$ since r_2 is the least solution
- $r_1 = r_2$ by antisymmetry.

□

[7] So called $\subseteq$-least fixpoint of $F(X) = \mathbf{1}_x \cup t \circ X$, written $\mathsf{lfp}^{\subseteq} F$.

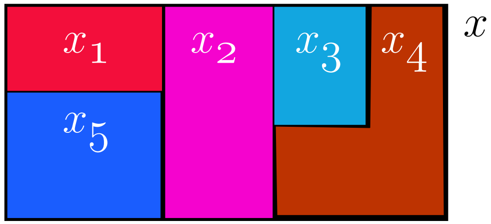
Equivalence relation

- A binary relation r on a set x is an equivalence relation iff it is reflexive, symmetric and transitive
- Examples: $=$ equality, $\equiv[n]$ equivalence modulo $n > 0$
- $[a]_r \stackrel{\text{def}}{=} \{b \in x \mid a \; r \; b\}$ — equivalence class
- Examples: $[a]_= = \{a\}$, $[a]_{\equiv[n]} = \{a + k \times n \mid k \in \mathbb{N}\}$
- $x/_r \stackrel{\text{def}}{=} \{[a]_r \mid a \in x\}$ — quotient of x by r
- Examples: $x/_= = \{\{a\} \mid a \in x\}$ [8], $x/_{\equiv[n]} = \{[0]_{\equiv[n]}, \ldots, [n-1]_{\equiv[n]}\}$ [9]

[8] which is isomorphic to x through $a \mapsto \{a\}$.
[9] which is isomorphic to $\{0, \ldots, n-1\}$ through $a \mapsto [a]_{\equiv[n]}$.

Partition

– P is a partition of x iff P is a family of disjoint sets covering x:
  - $\forall y \in P : (y \neq \emptyset)$
  - $\forall y, z \in P : (y \neq z) \Longrightarrow (y \cap z = \emptyset)$
  - $x = \bigcup P$



Posets

Correspondence between partitions and equivalences

– If P is a partition of x then

$$\{\langle a, b\rangle \mid \exists y \in P : a \in y \wedge b \in y\}$$

is an equivalence relation

– Inversely, if r is an equivalence relation on x, then

$$\{[a]_r \mid a \in x\}$$

is a partition of x.

Partial order relation

– A relation r on a set x is a partial order if and only if it is reflexive, antisymmetric and transitive.

Examples of partial order relations

- $\leq$ on $\mathbb{N}$
- $\leq$ on $\mathbb{Z}$
- $\subseteq$ on $\wp(x)$
- $\langle a,\ b\rangle \leq_2 \langle c,\ d\rangle \stackrel{\text{def}}{=} (a \leq c) \wedge (b \leq d)$ component-wise/cartesian ordering
- $\langle a,\ b\rangle \leq_\ell \langle c,\ d\rangle \stackrel{\text{def}}{=} (a \leq c \wedge a \neq c) \vee (a = c \wedge b \leq d)$ lexicographic ordering
- $a_1 \ldots a_n \leq_a b_1 \ldots b_m \stackrel{\text{def}}{=} \exists k : (0 \leq k \leq n) \wedge (k \leq m) \wedge (a_1 = b_1 \wedge \ldots a_{k-1} = b_{k-1}) \wedge (a_k \leq b_k)$ alphabetic ordering

Notations for partial order relations

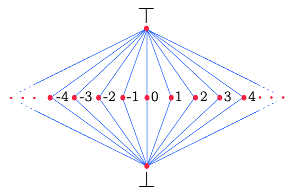
- Partial order relations are often denoted in infix form by symbols such as $\leq$, $\sqsubseteq$, $\subseteq$, $\preceq$, ..., meaning:
$$\leq\ = \{\langle a,\ b\rangle \mid a \leq b\}$$
- The inverse is written $\geq$, $\sqsupseteq$, $\supseteq$, $\succeq$, ..., meaning:
$$\geq\ =\ \leq^{-1}\ = \{\langle b,\ a\rangle \mid a \leq b\}$$
- The negation is written $\not\leq$, $\not\sqsubseteq$, $\not\subseteq$, $\not\preceq$, ..., meaning:
$$\not\leq\ = \{\langle a,\ b\rangle \mid \neg(a \leq b)\}$$
- The strict ordering is denoted $<$, $\sqsubset$, $\subset$, $\prec$, ..., meaning:
$$<\ = \{\langle a,\ b\rangle \mid a \leq b \wedge a \neq b\}$$

Posets

- A partially ordered set (poset for short) is a pair $\langle x,\ \leq\rangle$ where:
  - x is a set
  - $\leq$ ia a partial order relation on x
- if $\langle x,\ \leq\rangle$ is a poset and $y \subseteq x$ then $\langle y,\ \leq\rangle$ is also a poset.

Hasse diagram

- The Hasse diagram of a poset $\langle x,\ \leq\rangle$ is a graph with
  - vertices x
  - arcs $\langle a,\ b\rangle$ whenever $a \leq b$ and $\neg(\exists c \in x : a < c < b)$
  - the arc $\langle a,\ b\rangle$ is oriented bottom up, that is drawn with vertex a below vertex b whenever $a \leq b$
- Example: $\forall i \in \mathbb{Z} : \bot \sqsubseteq \bot \sqsubseteq i \sqsubseteq i \sqsubseteq \top \sqsubseteq \top$ is represented as:



Encoding $\mathbb{N}$ with sets

In set theory, natural numbers are encoded as follows:

- $\emptyset$ — 0
- $\{\emptyset\}$ — $1 = \{0\}$
- $\{\emptyset, \{\emptyset\}\}$ — $2 = \{0, 1\}$
- $\ldots$
- $Sn = n \cup \{n\}$ — $n + 1 = \{0, 1, \ldots, n\}$
- $\ldots$
- $w = \{0, 1, \ldots, n, \ldots\} = \mathbb{N}$ — first infinite ordinal

The ordering is:

- $n < m \stackrel{\text{def}}{=} n \in m$ so that $0 < 1 < 2 < 3 < \ldots < n < \ldots < \omega$
- $n \leq m \stackrel{\text{def}}{=} (n < m) \vee (n = m)$

Functions

Domain and range of a relation

Let r be a $n+1$-ary relation on a set x.

- $\text{dom}(r) \stackrel{\text{def}}{=} \{a \mid \exists b : \langle a,\ b\rangle \in r\}$ — domain
- $\text{rng}(r) \stackrel{\text{def}}{=} \{b \mid \exists b : \langle a,\ b\rangle \in r\}$ — range/codomain

Functions

- An n-ary function on a set x is an $(n+1)$-ary relation r on x such that for every $a \in \text{dom}(r)$ there is at most one $b \in \text{rng}(r)$ such that $\langle a,\ b\rangle \in r$:
$$(\langle a,\ b\rangle \in r \wedge \langle a,\ c\rangle \in r) \Longrightarrow (b = c)$$
- Fonctional notation:
One writes $r(a_1, \ldots, a_n) = b$ for $\langle a_1,\ \ldots,\ a_n,\ b\rangle \in r$

Partial and total functions

- $x \mapsto y$ is the set of (total) functions f such that $\mathrm{dom}(f) = x$ and $\mathrm{rng}(f) \subseteq y$
- $x \not\mapsto y$ is the set of (partial) functions f such that $\mathrm{dom}(f) \subseteq x$ and $\mathrm{rng}(f) \subseteq y$. So $f(z)$ is undefined whenever $z \in x \setminus \mathrm{dom}(f)$.

Notations for functions

The function f such that:

- $\mathrm{dom}(f) = x$, $\mathrm{rng}(f) \subseteq y$ i.e. $f \in x \mapsto y$
- $\forall a \in x : \langle a,\ e(a)\rangle \in f$ [10]

is denoted as:

- $f(a) = e$ or $f(a : x) = e$ — functional notation
- $f = \lambda a \cdot e$ or $f = \lambda a : x \cdot e$ — Church's lambda notation
- $f : a \in x \mapsto e$
- $\{a \to b, c \to d, e \to f\}$ denotes the function $g = \{\langle a,\ b\rangle, \langle c,\ d\rangle, \langle e,\ f\rangle\}$ such that $g(a) = b$, $g(c) = d$, $g(e) = f$, $\mathrm{dom}(g) = \{a, c, e\}$ and $\mathrm{rng}(g) = \{b, d, f\}$.

[10] $e(a)$ is an expression depending upon variable $a \in x$ which result is in y.

Operations on functions

- $f = \lambda a \cdot k \stackrel{\mathrm{def}}{=} \{\langle a,\ k\rangle \mid a \in \mathrm{dom}(f)\}$ [11] — constant function
- $1_x \stackrel{\mathrm{def}}{=} \{\langle a,\ a\rangle \mid a \in x\}$ — identity function
- $f \circ g \stackrel{\mathrm{def}}{=} \lambda a \cdot f(g(a))$ — function composition
- $f \upharpoonright u \stackrel{\mathrm{def}}{=} f \cap (u \times \mathrm{rng}(f))$ — function restriction
- $f^{-1} \stackrel{\mathrm{def}}{=} \{\langle f(a),\ a\rangle \mid a \in \mathrm{dom}(f)\}$ — function inverse [12]

[11] where $k \in \mathrm{rng}(f)$.

[12] a relation but in general not a function.

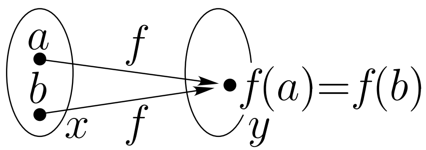
Properties of functions

Injective/one-to-one function

– A function $f \in x \mapsto y$ is injective/one-to-one if different elements have different images:

$$\begin{aligned} & \forall a, b \in x : a \neq b \Longrightarrow f(a) \neq f(b) \\ \Longleftrightarrow\ & \forall a, b \in x : f(a) = f(b) \Longrightarrow a = b \end{aligned}$$

– The following situation is excluded:



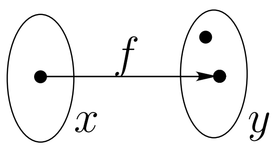
– Notation: $f \in x \rightarrowtail y$, $f \in x \not\rightarrowtail y$

Surjective/onto function

– A function $f \in x \mapsto y$ is surjective/onto function if all elements of its range are images of some element of their domain:

$$\forall b \in y : \exists a \in x : f(a) = b$$

– The following situation is excluded:



– Notation: $f \in x \twoheadrightarrow y$, $f \in x \not\twoheadrightarrow y$

Bijective function

– A function is bijective iff it is both injective and surjective

– Notation: $f \in x \rightarrowtail\!\!\!\!\twoheadrightarrow y$

– A bijective function is a bijection, also called an isomorphism

– Two sets x and y are isomorphic iff there exists an isomorphism $i \in x \rightarrowtail\!\!\!\!\twoheadrightarrow y$

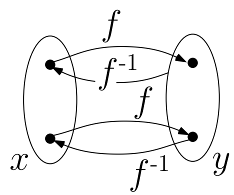
Inverse of bijective functions

– If $f \in x \rightarrowtail\!\!\!\!\twoheadrightarrow y$ is bijective then its inverse is the function f^{-1} defined by:

$$f^{-1} = \{\langle b,\ a\rangle \mid \langle a,\ b\rangle \in f\}$$

thus:

- $f^{-1} \in y \rightarrowtail\!\!\!\!\twoheadrightarrow x$
- $f^{-1} \circ f = \mathbf{1}_x$
- $f \circ {}^{-1} = \mathbf{1}_y$



Cartesian product (revisited)

- Given a family $\{x_i \mid i \in I\}$ of sets, the cartesian product of the family $\{x_i \mid i \in I\}$ is defined as:

$$\prod_{i \in I} x_i \stackrel{\text{def}}{=} \{f \mid f \in I \mapsto \bigcup_{i \in I} x_i \wedge \forall i \in I : f(i) \in x_i\}$$

- If $\forall i \in I : x_i = x$ then we write:

$$x^I \text{ or } I \mapsto x \text{ instead of } \prod_{i \in I} x_i$$

- For example $x^n = \underbrace{x \times \ldots \times x}_{n \text{ times}}$

Characteristic functions of subsets

- The powerset $\wp(x)$ of a set x is isomorphic to $x \mapsto \mathbb{B}$ where the set of booleans is $\mathbb{B} = \{\text{true}, \text{false}\}$ or $\{\text{ff}, \text{tt}\}$ or $\{0, 1\}$ or $\{\text{NO}, \text{YES}\}$.
- The isomorphism is called the characteristic function: $c \in \wp(x) \rightarrowtail\!\!\!\rightarrow (x \mapsto \mathbb{B})$

  $c(y) \stackrel{\text{def}}{=} \lambda a \in x \cdot a \in y$ where $y \subseteq x$

  $c^{-1}(y) = \lambda f \in x \mapsto \mathbb{B} \cdot \{a \in x \mid f(a) = \text{tt}\}$
- Useful to implement subsets of a finite set by bit vectors

Sequences

Finite sequences

Given a set x:

- $x^{\vec{0}} \stackrel{\text{def}}{=} \{\vec{\epsilon}\}$ where $\vec{\epsilon} \in \emptyset \mapsto x$ is the empty sequence of length 0
- $x^{\vec{n}} \stackrel{\text{def}}{=} \{0, \ldots, n-1\} \mapsto x$, finite sequences σ of length $|\sigma| = n$. The i-th element of $\sigma \in x^{\vec{n}}$ is $\sigma(i)$ abbreviated σ_i so $\sigma = \sigma_0\sigma_1 \ldots \sigma_{n-1}$
- $x^{\vec{\star}} \stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N}} x^{\vec{n}}$ finite sequences
- $x^{\vec{+}} \stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N} \setminus \{0\}} x^{\vec{n}}$ finite nonempty sequences

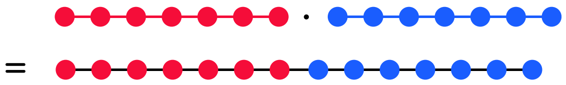
Infinite sequences

- $x^{\vec{\omega}} \stackrel{\text{def}}{=} \mathbb{N} \mapsto x$ infinite sequences σ of length $|\sigma| = \omega$ where $\forall i \in \mathbb{N} : i < \omega$
- $x^{\vec{\propto}} \stackrel{\text{def}}{=} x^{\vec{\star}} \cup x^{\vec{\omega}}$ infinitary sequences
- $x^{\vec{\infty}} \stackrel{\text{def}}{=} x^{\vec{+}} \cup x^{\vec{\omega}}$ nonempty infinitary sequences
- The i-th element of $\sigma \in x^{\vec{\infty}}$ is $\sigma(i)$ abbreviated σ_i so $\sigma = \sigma_0\sigma_1 \ldots \sigma_n, \ldots$

Operations on sequences

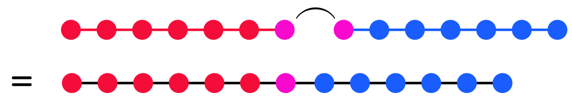
Concatenation $\cdot$:

- $\vec{\epsilon} \cdot \sigma \stackrel{\text{def}}{=} \sigma \cdot \vec{\epsilon} \stackrel{\text{def}}{=} \sigma$
- $\sigma \cdot \sigma' \stackrel{\text{def}}{=} \sigma$ whenever $\sigma \in x^{\vec{\omega}}$
- $\sigma_0 \ldots \sigma_{n-1} \cdot \sigma' = \sigma_0 \ldots \sigma_{n-1}\sigma'$
- $\sigma \cdot \sigma'$ is often denoted $\sigma\sigma'$
- $x \cdot y \stackrel{\text{def}}{=} \{\sigma\sigma' \mid \sigma \in x \wedge \sigma' \in y\}$



Junction $\frown$:

- $\vec{\epsilon} \frown \sigma$ and $\sigma \frown \vec{\epsilon}$ are undefined
- $\sigma \frown \sigma' \stackrel{\text{def}}{=} \sigma$ whenever $\sigma \in x^{\vec{\omega}}$
- $\sigma_0 \ldots \sigma_{n-1} \frown \sigma' = \sigma_0 \ldots \sigma_{n-2}\sigma'$ is defined only if $\sigma_{n-1} = \sigma'_0$
- $x \frown y \stackrel{\text{def}}{=} \{\sigma \frown \sigma' \mid \sigma \in x \wedge \sigma' \in y \wedge \sigma \frown \sigma'$ is well-defined$\}$



Set transformers

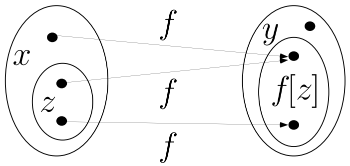
Image (postimage) of a set by a function/relation

- Let $r \subseteq x \times y$ and $z \subseteq x$.
  - The image (or postimage) of z by r is:

$$r[z] \stackrel{\text{def}}{=} \{b \mid \exists a \in z : \langle a,\, b\rangle \in r\}$$

  (which is also written $\text{post}[r]z$ or even $r(z)$)
- For $f \in x \mapsto y$ and $z \subseteq x$, we have:

$$f[z] = f(z) = \text{post}[f]z \stackrel{\text{def}}{=} \{f(a) \mid a \in z\}$$



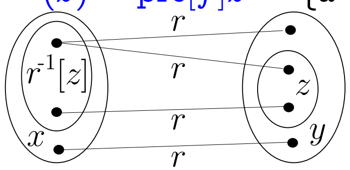
Preimage of a set by a function/relation

- Let $r \subseteq x \times y$ and $z \subseteq y$. The inverse image (or preimage) of z by r is:

$$\begin{aligned} r^{-1}[z] &\stackrel{\text{def}}{=} \{a \mid \exists b \in z : \langle a,\, b\rangle \in r\} \\ &= \{a \mid \exists b \in z : \langle b,\, a\rangle \in r^{-1}\} = \text{post}[r^{-1}]z \end{aligned}$$

  (which is also written $\text{pre}[r]z$ or even $r^{-1}(z)$)
- For $f \in x \mapsto y$ and $z \subseteq u$, we have:

$$f^{-1}[z] = f^{-1}(z) = \text{pre}[f]z \stackrel{\text{def}}{=} \{a \mid f(a) \in z\}$$

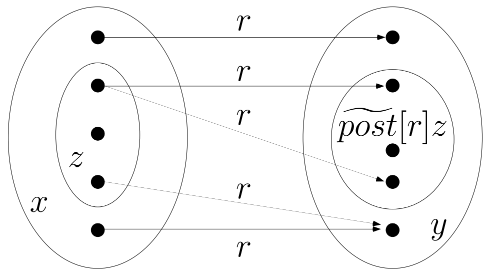


Dual image of a set by a function/relation

- Let $r \subseteq x \times y$ and $z \subseteq x$.

$$\begin{aligned} \widetilde{\text{post}}[r]z &= \neg\text{post}[r](\neg z) && \text{(informally)} \\ &= y \setminus \text{post}[r](x \setminus z) && \text{(formally)} \\ &= \neg\{b \mid \exists a \in (\neg z) : \langle a,\, b\rangle \in r\} \\ &= \neg\{b \mid \exists a : a \notin z \wedge \langle a,\, b\rangle \in r\} \\ &= \{b \mid \forall a : a \in z \vee \langle a,\, b\rangle \notin r\} \\ &= \{b \mid \forall a : (\langle a,\, b\rangle \in r) \Longrightarrow (a \in z)\} \end{aligned}$$

It is impossible to reach $\widetilde{\text{post}}(r)z$ from x by following r without starting from z

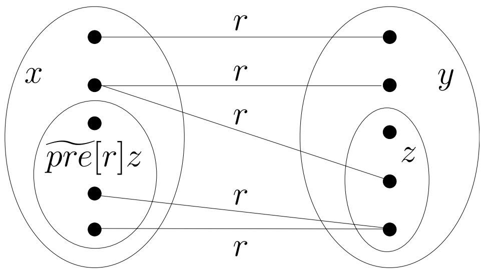


Dual preimage of a set by a function/relation

– Let $r \subseteq x \times y$ and $z \subseteq y$.

$$\begin{aligned}
\widetilde{\text{pre}}[r]z &= \neg\text{pre}[r](\neg z) && \text{≀informally≀} \\
&= x \setminus \text{pre}[r](y \setminus z) && \text{≀formally≀} \\
&= \neg\{a \mid \exists b \in (\neg z) : \langle a,\, b\rangle \in r\} \\
&= \neg\{a \mid \exists b : b \notin z \wedge \langle a,\, b\rangle \in r\} \\
&= \{a \mid \forall b : b \in z \vee \langle a,\, b\rangle \notin r\} \\
&= \{a \mid \forall b : (\langle a,\, b\rangle \in r) \Longrightarrow (b \in z)\}
\end{aligned}$$

Starting from $\widetilde{\text{pre}}(r)z$ from x and following r, it is impossible to arrive outside z (or one must reach z)



Properties of [dual [inverse]] images

– $\text{post}[r](\bigcup_{i \in I} x_i) = \bigcup_{i \in I} \text{post}[r](x_i)$

$\text{pre}[r](\bigcup_{i \in I} x_i) = \bigcup_{i \in I} \text{pre}[r](x_i)$

$\widetilde{\text{pre}}[r](\bigcap_{i \in I} x_i) = \bigcap_{i \in I} \widetilde{\text{pre}}[r](x_i)$

$\widetilde{\text{post}}[r](\bigcap_{i \in I} x_i) = \bigcap_{i \in I} \widetilde{\text{post}}[r](x_i)$

– $\text{post}[r](x) \subseteq y \iff x \subseteq \widetilde{\text{pre}}[r](y)$

$\text{pre}[r](x) \subseteq y \iff x \subseteq \widetilde{\text{post}}[r](y)$

– $\text{pre}[r](x) = \text{post}[r^{-1}](x)$

$\text{post}[r](x) = \text{pre}[r^{-1}](x)$

$\widetilde{\text{pre}}[r](x) = \widetilde{\text{post}}[r^{-1}](x)$

$\widetilde{\text{post}}[r](x) = \widetilde{\text{pre}}[r^{-1}](x)$

– Notice that if $f \in x \rightarrowtail\!\!\!\!\twoheadrightarrow y$ is bijective with inverse f^{-1} then the two possible interpretations of $f^{-1}[z]$ as $f^{-1}[z] = \text{pre}[f](z)$ and $f^{-1}[z] = \text{post}[f^{-1}]z$ do coincide since $\text{pre}[f](z) = \text{post}[f^{-1}]z$.

Induction

Well-founded relation, woset

- Let $\langle x, \leq\rangle$ be a poset, and let $y \subseteq x$. An element a of y is a minimal element of y iff $\neg(\exists b \in y : b < a)$ [13]
- A poset $\langle x, \leq\rangle$ is well-founded iff every nonempty subset of x has a minimal element
- A woset $\langle x, \leq\rangle$ is a poset $\langle x, \leq\rangle$ such that the partial ordering relation $\leq$ is well-founded
- Example: $\langle \mathbb{N}, \leq\rangle$, counter-example: $\langle \mathbb{Z}, \leq\rangle$ [14]

13 where as usual $a < b \stackrel{\text{def}}{=} a \leq b \wedge a \neq b$.

14 $\mathbb{Z} \subseteq \mathbb{Z}$ has no minimal element since $\forall a \in \mathbb{Z} : \exists b \in \mathbb{Z} : b < a$.

Characteristic property of wosets

- $\langle x, \leq\rangle$ is a woset iff there is no infinite strictly decreasing sequence $a \in \mathbb{N} \mapsto x$ (that is such that $a_0 > a_1 > a_2 > \ldots$).

PROOF.

1) If $\langle x, \leq\rangle$ is not well-founded, their exists $y \subseteq x$ which is nonempty and has no minimal element. So let $a_0 \in y$. Since a_0 is not minimal, we can find $a_1 \in y$ such that $a_1 < a_0$. If we have built $a_0 > \ldots > a_n$ in y then a_n is not minimal, so we can find $a_{n+1} \in y$ such that $a_{n+1} < a_n$. So proceeding inductively, we can build an infinite strictly decreasing sequence $a_0 > \ldots > a_n > \ldots$ in y.

By contraposition [15], if $\langle x, \leq\rangle$ has no infinite strictly decreasing sequence $a_0 > \ldots > a_n > \ldots$ then $\langle x, \leq\rangle$ is a woset

2) Reciprocally, if x has an infinite strictly decreasing sequence $a_0 > a_1 > a_2 > \ldots > a_n > \ldots$ then $y = \{a_0, a_1, a_2, \ldots, a_n, \ldots\}$ has no minimal element.

By contraposition, if x $\langle x, \leq\rangle$ is a woset then $\langle x, \leq\rangle$ has no infinite strictly decreasing sequence $a_0 > \ldots > a_n > \ldots$. □

15 $\neg P \Longrightarrow \neg Q$ iff $P \Longrightarrow Q$

Proof by induction on a woset

If $\langle x, \leq \rangle$ is a woset, and $P \subseteq x$. One wants to prove $x \subseteq P$ (that is property P holds for all elements of x).

If one can prove property P for any element a of x by assuming that P holds for strictly smaller elements (which requires a direct proof for minimal elements) then P holds for all elements of x.

Formally:

$$\frac{\forall a \in x : (\forall b : (b < a) \Longrightarrow (b \in P)) \Longrightarrow a \in P}{\forall a \in x : a \in P}$$ [16]

[16] The rule $\frac{P_1, \ldots, P_n}{c}$ with premiss $P_1, \ldots, P_n$ and conclusion c is a common notation for $(\bigwedge_{i=1}^{n} P_i) \Longrightarrow c$.

PROOF. By reductio ad absurdum, assume the premiss holds but not the conclusion. So $\exists a_0 \in x : a_0 \notin P$. By the premiss, $a_0 \notin P$ implies $\neg(\forall b : (b < a_0) \Longrightarrow (b \in P))$ $= \exists a_1 < a_0 : a_1 \notin P$. Assume we have built $a_n < \ldots < a_1 < a_0$ with all a_i in x but not in P. Again by the premiss, $a_n \notin P$ implies $\exists a_{n+1} < a_n : a_{n+1} \notin P$. So we can built a strictly decreasing infinite chain $a_0 > \ldots > a_n > \ldots$ of elements of x, in contradiction with $\langle x, \leq \rangle$ is a woset.

□

Proof by recurrence

For $\langle \mathbb{N}, \leq \rangle$, the structural induction principle becomes (writing $P(n)$ for $n \in P$ that is "n has property P"):

$$\frac{\forall n \in \mathbb{N} : (\forall k : (k < n) \Longrightarrow P(k)) \Longrightarrow P(n)}{\forall n \in \mathbb{N} : P(n)} \quad (1)$$

We can distinguish the case of 0 [17]:

$$\frac{P(0),\ \forall n \in \mathbb{N} \setminus \{0\} : (\forall k < n : P(k)) \Longrightarrow P(n)}{\forall n \in \mathbb{N} : P(n)} \quad (2)$$

[17] and abbreviate $\forall k : (k < n) \Longrightarrow Q$ by $\forall k < n : Q$.

This is equivalent to the more classical:

$$\frac{P(0),\ \forall n \in \mathbb{N} : P(n) \Longrightarrow P(n+1)}{\forall n \in \mathbb{N} : P(n)} \quad (3)$$

PROOF. A proof done with (3) can also be done with (2) since $\forall n \in \mathbb{N} \setminus \{0\} : (\forall k < n : P(k)) \Longrightarrow P(n)$ implies $\forall n \in \mathbb{N} : P(n) \Longrightarrow P(n+1))$. Reciprocally, if a proof has been done by (2), then by redefining $P'(n) = (\forall k < n : P(k))$ we can prove by (3) that $\forall n \in \mathbb{N} : P'(n)$ which implies the conclusion of (2), namely $\forall n \in \mathbb{N} : P(n)$.

□

Example of recursive/structural definitions

$h(n, k) = n * k$ can be recursively defined on $\mathbb{N}$ as:

$$\begin{aligned} h(0, k) &= 0 \\ h(n, k) &= k + h(n-1, k) \qquad \text{when } n > 0 \end{aligned}$$

This can be written as

$$h(n, k) = f(n, k, h \upharpoonright \{\langle n', k\rangle \mid n' < n\})$$

where

$$\begin{aligned} f(0, k, g) &= 0 \\ f(n, k, g) &= k + g(n-1, k) \qquad \text{when } n > 0 \end{aligned}$$

Recursive/Structural Definitions

Let $\langle x, \leq\rangle$ be a woset, y be a set, and $f \in (x \times y \times ((x \times y) \mapsto y)) \mapsto y$. Define

$$g(a, b) \stackrel{\text{def}}{=} f(a, b, g \upharpoonright \{\langle a', b\rangle \mid a' < a\})$$

then $g \in (x \times y) \mapsto y$ is well-defined and unique.

Proof.

(1) Define $\leq^2 \stackrel{\text{def}}{=} \{\langle\langle a', b\rangle, \langle a, b\rangle\rangle \mid a' \leq a\}$. Then $\langle x \times y, \leq^2\rangle$ is a woset since otherwise the existence of $\langle a_0, b_0\rangle >^2 \langle a_1, b_1\rangle >^2 \ldots$ would imply $b_0 = b_1 = \ldots$ so $\langle a_0, b\rangle \geq^2 \langle a_1, b\rangle$ and $\langle a_0, b\rangle \neq \langle a_1, b\rangle, \ldots$ implies $a_0 > a_1 > \ldots$ in contradiction with the hyposthesis that $\langle x, \leq\rangle$ is a woset.

(2) Assuming that $g(a', b')$ is well-defined for all $\langle a', b'\rangle <^2 \langle a, b\rangle$ that is, by definition of $\leq^2$, iff $b = b'$ and $a' < a$ then $g \upharpoonright \{\langle a', b\rangle \mid a' < a\}$ is well defined. It follows that $g(a, b) = f(a, b, g \upharpoonright \{\langle a', b\rangle \mid a' < a\})$ is well-defined by hypothesis that f is a total function. By structural induction, we have proved $g \in (x \times y) \mapsto y$ is well-defined for all $\langle a, b\rangle \in x \times y$.

(3) If g' also satisfies the definition and $g'(a', b') = g(a, b)$ for all $\langle a', b'\rangle <^2 \langle a, b\rangle$ by induction hypothesis, then obviously $g \upharpoonright \{\langle a', b\rangle \mid a' < a\} = g' \upharpoonright \{\langle a', b\rangle \mid a' < a\}$ so $g(a, b) = g'(a, b)$ proving $g' = g$ by structural induction.

□

Cardinals

Intuition on ordinals and cardinals

– The ordinals 1^{st}, 2^{nd}, 1^{rd}, ... and cardinals 1, 2, 3, ... elements do coincide for natural numbers
– This is not otherwise the case.
– For example if we consider the sets $\{0, 1, 2, \ldots\}$ and $\{0, 1, 2, \ldots, +\infty\}$ ordered by $0 < 1 < 2 < \ldots < +\infty$, they are equipotent (by $b(+\infty) = 0$ and $b(n) = n + 1$ otherwise) hence have same cardinality [18] but the ∞^{th} element does not exists in $\{0, 1, 2, \ldots\}$ so the two sets are different as ordinals [19].

[18] hence are equivalent when used as quantities for mesuring the "size"/number of elements of sets.
[19] hence are different when used as positions for ranking elements of a set.

Equipotence

– Two sets x and y are *equipotent* of and only if there exists a bijection $b \in x \rightarrowtail\!\!\!\twoheadrightarrow y$ [20]
– Examples:
  - The set of even integers is equipotent to the set $\mathbb{Z}$ of integers (by $b(n) = 2n$)
  - The set of odd integers is equipotent to the set $\mathbb{Z}$ of integers (by $b(n) = 2n + 1$)
  - The set of integers $\mathbb{Z}$ is equipotent to the set $\mathbb{N}$ of natural numbers, by

$$\begin{array}{lcll} b(n) & \stackrel{\text{def}}{=} & 2n - 1 & \text{if } n > 0 \\ b(n) & \stackrel{\text{def}}{=} & -2n & \text{if } n < 0 \\ b(0) & \stackrel{\text{def}}{=} & 0 & \end{array}$$

[20] The intuition is that "x and y have the same number of elements".

Properties of Equipotence

– *Equipotence* is an equivalence relation denoted $\equiv_c$
– A set x is *denumerable* (also said *countable*) iff $x \equiv_c \mathbb{N}$ (otherwise *uncountable*)
– A set x is *finite* iff $\exists n \in \mathbb{N} : x \equiv_c \{i \mid i < n\}$ (otherwise *infinite*)
– Example: $\mathbb{Z}$ is denumerable and infinite

Cardinality

- The cardinality $|x|$ (also written $\mathrm{Card}(x)$) of a set x is

$$|x| \stackrel{\text{def}}{=} [x]_{\equiv_c}$$

  i.e., intuitively, a representative of the class of all sets with "the same number of elements"
- $|\mathbb{N}| \stackrel{\text{def}}{=} \aleph_0$ [21]

[21] $\aleph$ is the hebrew aleph letter.

The set of all real numbers is uncountable

PROOF. (Cantor) Assume that $\mathbb{R}$ is countable, i.e., is the range of some infinite sequence $r(n)$, $n \in \mathbb{N}$. We show that some $r \in \mathbb{R}$ is missing in that enumeration.

Let $a_0^{(n)}.a_1^{(n)}a_2^{(n)}a_3^{(n)}\ldots$ be the decimal expansion of $r(n)$. Let $b_n = 1$ if $a_n^{(n)} = 0$ and otherwise $b_n = 0$. Let r be the real number whose decimal expansion is $0.b_1b_2b_3\ldots$. We have $b_n \neq a_n^{(n)}$, hence $\forall n \in \mathbb{N} : r \neq r(n)$, for all $n = 1, 2, 3, \ldots$, a contradiction.
□

The set of all sets of naturals is uncountable

$|\wp(\mathbb{N})| > |\mathbb{N}|$

PROOF. The function $f \in \mathbb{N} \mapsto \wp(\mathbb{N})$ defined by $f(n) = \{n\}$ is injective, so $|\mathbb{N}| \leq |\wp(\mathbb{N})|$.
Let $s \in \mathbb{N} \mapsto \mathbb{N}$ be a sequence $s_n, n \in \mathbb{N}$ of naturals.We show that some $S \in \wp(\mathbb{N})$ is missing in that enumeration. Define the set $S = \{n \in \mathbb{N} \mid n \notin s_n\}$. If $n \in s_n$ then $n \notin S$ and if $n \notin s_n$ then $n \in S$. So $\forall n : S \neq s_n$. This shows that there is no surjective mapping of $\mathbb{N}$ onto $\wp(\mathbb{N})$, whence $|\wp(\mathbb{N})| > |\mathbb{N}|$.
□

Operations on cardinals

- Cardinal addition $\mathfrak{m} + \mathfrak{n} = |A \cup B|$ where $\mathfrak{m} = |A|$, $\mathfrak{n} = |B|$ and $A \cap B = \emptyset$ [22]
- Cardinal multiplication $\mathfrak{m} \times \mathfrak{n} = |A \times B|$ where $\mathfrak{m} = |A|$ and $\mathfrak{n} = |B|$
- Cardinal exponentiation $\mathfrak{m}^{\mathfrak{n}} = |B \mapsto A|$ where $\mathfrak{m} = |A|$ and $\mathfrak{n} = |B|$
- For example, $2^{\mathfrak{n}} = |\wp(A)|$ where $2 = |\mathbb{B}|$ and $\mathfrak{m} = |A|$ [23]

[22] All these definitions are independant of the choice of A and B.
[23] Using the characteristic function of subsets of A into the booleans $\mathbb{B} = \{\mathtt{tt}, \mathtt{ff}\}$. This explains the notation 2^A for $\wp(A)$.

Ordering on cardinals

- We write $\mathfrak{m} \leq \mathfrak{n}$ where $\mathfrak{m} = |A|$ and $\mathfrak{n} = |B|$ iff there exists an injective function of A into B [24]
- A cardinal $\mathfrak{m}$ is finite iff $\mathfrak{m} < \aleph_0$, otherwise it is infinite

[24] Again this definition is independant of the choice of A and B.

Order-preserving maps

- Given two posets $\langle x,\ \leq\rangle$ and $\langle y,\ \preceq\rangle$, a map $f \in x \mapsto y$ which is *order-preserving* (also called *monotone*, *isotone*, ...) if and only if:

$$\forall a, b \in x : (a \leq b) \Longrightarrow (f(a) \preceq f(b))$$

- Example: $\lambda x \in \mathbb{Z} \cdot x + 1$
- Counter-example: $\lambda x \in \mathbb{Z} \cdot |x|$ [25]

[25] Here $|x|$ is the absolute value of x.

Ordinals

Order-isomorphism

- Two posets $\langle x,\ \leq\rangle$ $\langle y,\ \preceq\rangle$ are *order-isomorphic* iff there exists an order-preserving bijection $b \in x \rightarrowtail\!\!\!\!\twoheadrightarrow y$
- Notation: $\langle x,\ \leq\rangle \equiv_o \langle y,\ \preceq\rangle$
- $\equiv_o$ is an equivalence relation on wosets [26].

[26] Not true on posets sincee symmetry is lacking.

Ordinals

- The equivalence classes $[\langle x,\ \leq\rangle]_{\equiv_O}$ for wosets $\langle x,\ \leq\rangle$ are called the ordinals. $[\langle x,\ \leq\rangle]_{\equiv_O}$ is called the rank (also called order-type) of the woset $\langle x,\ \leq\rangle$
- We let $\mathbb{O}$ be the class [27] of all ordinals
- On $\mathbb{O}$ which is the quotient of wosets by $\equiv_O$, $\equiv_O$ and $=$ do coincide (so we use $=$)
- the rank of $\{0, 1, \ldots, n-1\}$ with ordering $0 < 1 < 2 < \ldots$ is written n so $0 \stackrel{\text{def}}{=} [\langle\emptyset,\ \emptyset\rangle]_{\equiv_O}$
- the rank of $\mathbb{N}$ is writen ω so $\omega \stackrel{\text{def}}{=} [\langle\mathbb{N},\ \leq\rangle]_{\equiv_O}$

[27] It is a class but not a set because sets are not large enough to contain all ordinals.

Ordering on ordinals

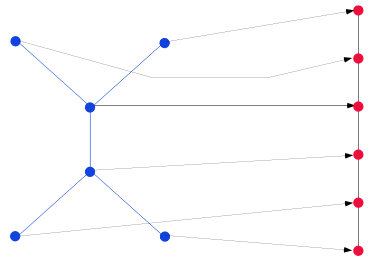
- We have $\delta \leq \eta$ whenever $\delta = [\langle x,\ \leq\rangle]_{\equiv_O}$, $\eta = [\langle y,\ \preceq\rangle]_{\equiv_O}$ and there exists an order-preserving injection $i \in x \rightarrowtail y$ [28]
- Example: $0 < 1 < 2 < \ldots < \omega$
- An ordinal δ is finite if $\delta < \omega$ and otherwise infinite

[28] This definition does not depend upon the particular choice of $\langle x,\ \leq\rangle$ and $\langle y,\ \preceq\rangle$

Wosets and ordinals

- The rank of $\langle\{\beta \mid \beta < \alpha\},\ \leq\rangle$ is α so $\alpha \equiv_O \{\beta \mid \beta < \alpha\}$ that is $\alpha = \{\beta \mid \beta < \alpha\}$
- it follows that every woset is order-isomorphic to the woset of all ordinals less than some given ordinal α:
$$[\langle x,\ \leq\rangle]_{\equiv_O} \equiv_O \alpha \equiv_O \{\beta \mid \beta < \alpha\}$$
- It follows that for any woset $\langle x,\ \preceq\rangle$ there is an ordinal α and an indexing $x_\gamma, \gamma \in \{\beta \mid \beta < \alpha\}$ such that $\langle x,\ \leq\rangle$ is order-isomorphic to $\langle\{x_\beta \mid \beta < \alpha\},\ \leq'\rangle$ and $x_\gamma \leq' x_\delta$ iff $\gamma < \delta$
- Otherwise stated, every woset is order isomorphic to an ordinal

- A well-founded set is ismorphic to an ordinal through an order-preserving bijection, for example:



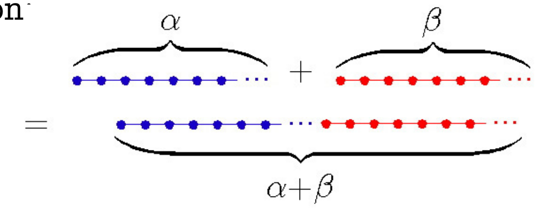
- This is the reason why ordinals are used in Manna-Pnueli proof rule for while-loops instead of arbitrary wosets in Floyd's method.

Operations on ordinals

– The *addition* of $\alpha = [\langle x, \leq\rangle]_{\equiv_o}$ and $\beta = [\langle y, \preceq\rangle]_{\equiv_o}$ where $x \cap y = \emptyset$ is $\alpha + \beta = [\langle x \cup y, \sqsubseteq\rangle]_{\equiv_o}$ with

$$\begin{array}{lll} a \sqsubseteq b & \text{iff} & (a, b \in x \wedge a \leq b) \\ & & \vee\ (a \in x \wedge b \in y) \\ & & \vee\ (a, b \in y \wedge a \preceq y) \end{array}$$

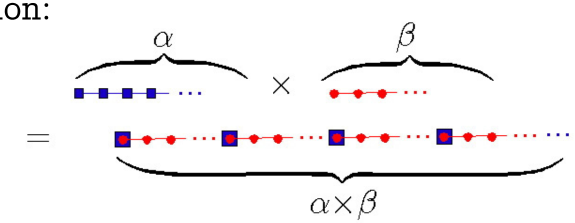
– Intuition



– Addition is not commutative: $\omega = 1 + \omega \neq \omega + 1$

– The *multiplication* of $\alpha = [\langle x, \leq\rangle]_{\equiv_o}$ and $\beta = [\langle y, \preceq\rangle]_{\equiv_o}$ where $x \cap y = \emptyset$ is $\alpha \times \beta = [\langle x \times y, \leq_\ell\rangle]_{\equiv_o}$ [29].

– Intuition:



[29] Recall that $\leq_\ell$ is the lexicographic ordering: $\langle a, b\rangle \leq_\ell \langle a', b'\rangle$ iff $(a < a') \vee ((a = a') \wedge (b < b'))$.

Successor and limit ordinal

– A successor ordinal is $\alpha \in \mathbb{O}$ such that

$$\begin{array}{l} \exists \beta : \alpha = \beta + 1 \\ \Longleftrightarrow \exists \beta : \alpha = \beta \cup \{\beta\} \end{array}$$

Otherwise it's a limit ordinal [30].

– 0 is the first limit ordinal. ω is the first infinite limit ordinal.

– Intuition: ● = successor ordinal, ■ = limit ordinal

[30] A limit ordinal λ is such that $\forall \alpha < \lambda : \exists \beta : \alpha < \beta < \lambda$ and so for a successor ordinal η, $\exists \alpha < \eta : \forall \beta : \neg(\alpha < \beta < \eta)$.

Induction principal for ordinals

– As a special case of structural induction, we get:

$$\frac{\begin{array}{l} P(0), \\ \forall \beta : P(\beta) \Longrightarrow P(\beta + 1), \\ (\forall \beta < \lambda : P(\beta)) \Longrightarrow P(\lambda) \text{ for all limit ordinals } \lambda \end{array}}{\forall \alpha : P(\alpha)}$$

Properties of limit ordinals

– The successor $\alpha + 1$ (also written $\mathcal{S}\alpha$) of α satisfies

$$\begin{aligned} & \alpha + 1 \\ = \; & \{\beta \mid \beta < \alpha + 1\} \\ = \; & \{\beta \mid \beta < \alpha\} \cup \{\alpha\} \\ = \; & \alpha \cup \{\alpha\} \end{aligned}$$

Properties of limit ordinals

– A limit ordinal λ is such that if $\gamma < \lambda$ then $\exists \beta : \gamma < \beta < \lambda$

– This is not true of $\eta < \eta + 1$ whence of successor ordinals

Properties of limit ordinals (Cont'd)

Assume that λ is a limit ordinal, then:

$$\begin{aligned} & \lambda \\ = \; & \{\gamma \mid \gamma < \lambda\} \\ = \; & \{\gamma \mid \gamma < \beta < \lambda\} && \wr \lambda \text{ is a limit ordinal} \wr \\ = \; & \bigcup \{\{\gamma \mid \gamma < \beta\} \mid \beta < \lambda\} \\ = \; & \bigcup \{\beta \mid \beta < \lambda\} && \wr \text{since } \beta = \{\gamma \mid \gamma < \beta\} \wr \\ = \; & \bigcup_{\beta < \lambda} \beta \end{aligned}$$

Ordinals are well-ordered by $\in$

– If $\alpha < \beta$ then $\beta = \{\gamma \mid \gamma < \beta\}$ so $\alpha \in \beta$

– Reciprocally, if $\alpha \in \beta$ then $\beta = \{\gamma \mid \gamma < \beta\}$ implies $\alpha \in \{\gamma \mid \gamma < \beta\}$ so $\alpha < \beta$

– we conclude that $\alpha < \beta \iff \alpha \in \beta$

Ordinals are well-ordered by "$\subseteq$"

$$
\begin{array}{ll}
 & \alpha < \beta \\
\Longleftrightarrow & \forall \gamma : (\gamma < \alpha) \Longrightarrow (\gamma < \beta) \\
\Longleftrightarrow & \forall \gamma : (\gamma \in \alpha) \Longrightarrow (\gamma \in \beta) \\
\Longleftrightarrow & \alpha \subseteq \beta
\end{array}
$$

So ordinals are $\in$-transitive in that $\forall \alpha \in \beta : (\alpha \subseteq \beta)$.
Every member of an ordinal is $\in$-transitive.

Transfinite inductive definitions on ordinals

- $g(0) = a$
- $g(\beta + 1) = f(\beta, g(\beta))$
- $g(\lambda) = h(\lambda, g \upharpoonright \lambda)$ when λ is a limit ordinal

is well defined and unique.

Proof by transfinite induction on ordinals

$$
\frac{\begin{array}{l} P(0), \\ \forall \beta : P(\beta) \Longrightarrow P(\beta + 1), \\ \forall \lambda \text{ limit ordinal} : (\forall \beta < \lambda : P(\beta)) \Longrightarrow P(\lambda) \end{array}}{\forall \alpha : P(\alpha)}
$$

More generaly, transfinite inductive definitions on α have the form:

- $f \in (\alpha \times y \times ((\alpha \times y) \mapsto y) \mapsto y)$
- $d(\beta, b) \stackrel{\text{def}}{=} f(\beta, b, g \upharpoonright \{\langle \gamma,\ b \rangle \mid \gamma < \beta\})$

and $g \in (\alpha \times y) \mapsto y$ is well-defined and unique.

Totally ordered set

– A total order (or “totally ordered set”, or “linearly ordered set”) is a partial order $\langle x, \leq \rangle$ such that any two elements are comparable:

$$\forall a, b \in x : (a \leq b) \vee (b \leq a)$$

Well ordered set

– A well ordered set is a well-founded total order.

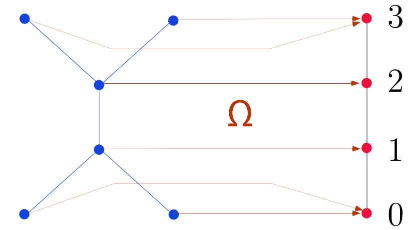
– totally ordered set is well ordered.

– The set of integers $\mathbb{Z}$, which has no least element, is an example of a set that is not well ordered.

Ordinal number (rank) of a well ordered set

– Let $\langle x, \leq \rangle$ be a well ordered set. We define the rank $\rho \in x \mapsto \mathbb{O}$ as follows:

  - $\rho(a) = 0$ iff a the minimal element of x
  - $\rho(a) = \bigcup_{b<a} \rho(b)$
  - $\rho(x) = \bigcup_{a \in x} \rho(a)$



Burali-Forti Paradox

Assume $\mathbb{O}$ is a set. We have seen that:

1. Every well ordered set has a unique rank;
2. Every segment of ordinals (i.e., any set of ordinals arranged in natural order which contains all the predecessors of each of its elements) has a rank which is greater than any ordinal in the segment, and
3. The set $\mathbb{O}$ of all ordinals in natural order is well ordered.

Then by statements (3) and (1), $\mathbb{O}$ has a rank, which is an ordinal β. Since β is in $\mathbb{O}$, it follows that $\beta < \beta$ by (2), which is a contradiction.

So the class $\mathbb{O}$ of ordinals is not a set [31].

[31] It's an ordinal $\mathbb{O} \in \mathbb{O}$.

Axiomatizations

Two main Axiomatizations of naïve set theory:

- Zermalo/Fraenkel
- Bernays/Gödel

that lead to a rigourous treatment of the notion of set/class avoiding seeming paradoxes.

Paul I. Bernays

Adolf A. Fraenkel

Ernst Zermelo

Bibliography on set theory

- Keith Devlin
  "The Joy of Sets, Fundamental of Contemporary Set Theory". 2^{nd} edition. Undergraduate texts in mathematics. Springer-Verlag, 1993.
- Yannis N. Moschovakis
  "Notes on Set Theory". Undergraduate texts in mathematics. Springer-Verlag, 1993.
- J. Donald Monk
  "Introduction to set theory". McGraw-Hill Book Compagny. International series in pure and applied mathematics. 1969.
- Karel Hrbacek and Thomas Jech
  "Introduction to Set Theory", Third Edition, Marcel Dekker, Inc., New York 1999.

THE END

My MIT web site is http://www.mit.edu/~cousot/

The course web site is http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/.

THE END, THANK YOU

My MIT web site is http://www.mit.edu/~cousot/

The course web site is http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/.