Mathematical Background

Outline

Outline

Sets – Basic Notations

$x \in S$	membership
$S \subseteq T$	subset
$S \subset T$	proper subset
$S \subseteq^{\text{fin}} T$	finite subset
$S = T$	equivalence
$\emptyset$	the empty set
$\mathbf{N}$	natural numbers
$\mathbf{Z}$	integers
$\mathbf{B}$	$\{\mathbf{true}, \mathbf{false}\}$

Sets – Basic Notations

$S \cap T$	intersection	$\stackrel{\text{def}}{=} \{x \mid x \in S \text{ and } x \in T\}$
$S \cup T$	union	$\stackrel{\text{def}}{=} \{x \mid x \in S \text{ or } x \in T\}$
$S - T$	difference	$\stackrel{\text{def}}{=} \{x \mid x \in S \text{ and } x \notin T\}$
$\mathcal{P}(S)$	powerset	$\stackrel{\text{def}}{=} \{T \mid T \subseteq S\}$
$[m, n]$	integer range	$\stackrel{\text{def}}{=} \{x \mid m \leq x \leq n\}$

Generalized Unions of Sets

$$\bigcup \mathcal{S} \stackrel{\text{def}}{=} \{x \mid \exists T \in \mathcal{S}.\ x \in T\}$$

$$\bigcup_{i \in I} S(i) \stackrel{\text{def}}{=} \bigcup \{S(i) \mid i \in I\}$$

$$\bigcup_{i=m}^{n} S(i) \stackrel{\text{def}}{=} \bigcup_{i \in [m,n]} S(i)$$

Here $\mathcal{S}$ is a set of sets. $S(i)$ is a set whose definition depends on i. For instance, we may have

$$S(i) = \{x \mid x > i + 3\}$$

Given $i = 1, 2, \ldots, n$, we know the corresponding $S(i)$.

Generalized Unions of Sets

Example (1)

$$A \cup B \; = \bigcup \{A, B\}$$

Proof?

Example (2)

Let $S(i) = [i, i+1]$ and $I = \{j^2 \;\mid\; j \in [1, 3]\}$, then

$$\bigcup_{i \in I} S(i) = \{1, 2, 4, 5, 9, 10\}$$

Generalized Intersections of Sets

$$\bigcap \mathcal{S} \stackrel{\text{def}}{=} \{x \mid \forall T \in \mathcal{S}.\ x \in T\}$$

$$\bigcap_{i \in I} S(i) \stackrel{\text{def}}{=} \bigcap \{S(i) \mid i \in I\}$$

$$\bigcap_{i=m}^{n} S(i) \stackrel{\text{def}}{=} \bigcap_{i \in [m,n]} S(i)$$

Generalized Unions and Intersections of Empty Sets

From

$$\bigcup \mathcal{S} \stackrel{\text{def}}{=} \{x \mid \exists T \in \mathcal{S}.\ x \in T\}$$
$$\bigcap \mathcal{S} \stackrel{\text{def}}{=} \{x \mid \forall T \in \mathcal{S}.\ x \in T\}$$

we know

$$\bigcup \emptyset = \emptyset$$
$$\bigcap \emptyset \quad \text{meaningless}$$

$\bigcap \emptyset$ is meaningless, since it denotes the paradoxical "set of everything" (see Russell's paradox).

Outline

Relations

We need to first define the *Cartesian product* of two sets A and B:
$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$
Here (x, y) is called a *pair*.

Projections over pairs:
$\pi_0(x, y) = x$ and $\pi_1(x, y) = y$.

Then, ρ is a *relation from A to B* if $\rho \subseteq A \times B$.
Or, written as $\rho \in \mathcal{P}(A \times B)$.

Relations

ρ is a *relation from A to B* if $\rho \subseteq A \times B$, or $\rho \in \mathcal{P}(A \times B)$.

ρ is a *relation on S* if $\rho \subseteq S \times S$.

We say ρ *relates x and y* if $(x, y) \in \rho$. Sometimes we write it as $x \, \rho \, y$.

ρ is an *identity relation* if $\forall (x, y) \in \rho.\ x = y$.

Relations – Basic Notations

$$\text{the } \textit{identity on } S \quad \mathrm{Id}_S \stackrel{\text{def}}{=} \{(x, x) \mid x \in S\}$$

$$\text{the } \textit{domain} \text{ of } \rho \quad \mathrm{dom}(\rho) \stackrel{\text{def}}{=} \{x \mid \exists y.\,(x, y) \in \rho\}$$

$$\text{the } \textit{range} \text{ of } \rho \quad \mathrm{ran}(\rho) \stackrel{\text{def}}{=} \{y \mid \exists x.\,(x, y) \in \rho\}$$

$$\textit{composition} \text{ of } \rho \text{ and } \rho' \quad \rho' \circ \rho \stackrel{\text{def}}{=} \{(x, z) \mid \exists y.\,(x, y) \in \rho \wedge (y, z) \in \rho'\}$$

$$\textit{inverse} \text{ of } \rho \quad \rho^{-1} \stackrel{\text{def}}{=} \{(y, x) \mid (x, y) \in \rho\}$$

Relations – Properties and Examples

$$(\rho_3 \circ \rho_2) \circ \rho_1 = \rho_3 \circ (\rho_2 \circ \rho_1)$$

$$\rho \circ \mathsf{Id}_S = \rho = \mathsf{Id}_T \circ \rho, \quad \text{if } \rho \subseteq S \times T$$

$$\mathsf{dom}(\mathsf{Id}_S) = S = \mathsf{ran}(\mathsf{Id}_S)$$

$$\mathsf{Id}_T \circ \mathsf{Id}_S = \mathsf{Id}_{T \cap S}$$

$${\mathsf{Id}_S}^{-1} = \mathsf{Id}_S$$

$$\left(\rho^{-1}\right)^{-1} = \rho$$

$$(\rho_2 \circ \rho_1)^{-1} = {\rho_1}^{-1} \circ {\rho_2}^{-1}$$

$$\rho \circ \emptyset = \emptyset = \emptyset \circ \rho$$

$$\mathsf{Id}_\emptyset = \emptyset = \emptyset^{-1}$$

$$\mathsf{dom}(\rho) = \emptyset \iff \rho = \emptyset$$

Relations – Properties and Examples

$$
\begin{aligned}
< &\subseteq \leq \\
< \cup \mathsf{Id}_{\mathbf{N}} &= \leq \\
\leq \cap \geq &= \mathsf{Id}_{\mathbf{N}} \\
< \cap \geq &= \emptyset \\
< \circ \leq &= < \\
\leq \circ \leq &= \leq \\
\geq &= \leq^{-1}
\end{aligned}
$$

Equivalence Relations

ρ is an *equivalence relation* on S if it is reflexive, symmetric and transitive.

Reflexivity: $\mathrm{Id}_S \subseteq \rho$

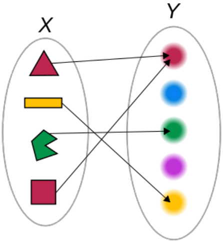
Symmetry: $\rho^{-1} = \rho$

Transitivity: $\rho \circ \rho \subseteq \rho$

Outline

Functions

A function f from A to B is a special relation from A to B.
A relation ρ is a function if, for all x, y and y', $(x, y) \in \rho$ and $(x, y') \in \rho$ imply $y = y'$.



Function application $f(x)$ can also be written as $f\,x$.
Below we only consider *total* functions: $\mathrm{dom}(f) = A$.

Functions

$\emptyset$ and Id_S are functions.

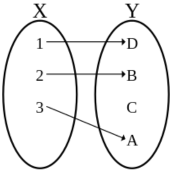
If f and g are functions, then $g \circ f$ is a function.

$$(g \circ f)\, x = g(f\, x)$$

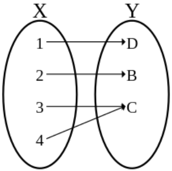
If f is a function, f^{-1} is *not* necessarily a function. (f^{-1} is a function if f is an injection.)

Functions – Injection, Surjection and Bijection

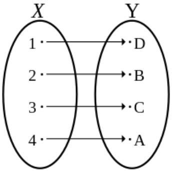
Injective and non-surjective:



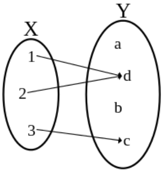
Surjective and non-injective:



Bijective:



Non-injective and non-surjective:



Functions – Denoted by Typed Lambda Expressions

$\lambda x \in S.\, E$ denotes the function f with domain S such that $f(x) = E$ for all $x \in S$.

Example

$\lambda x \in \mathbf{N}.\, x + 3$ denotes the function $\{(x, x + 3) \mid x \in \mathbf{N}\}$.

Functions – Variation

Variation of a function at a single argument:

$$f\{x \rightsquigarrow n\} \stackrel{\text{def}}{=} \lambda z. \begin{cases} f\,z & \text{if } z \neq x \\ n & \text{if } z = x \end{cases}$$

Note that x does not have to be in $\text{dom}(f)$.

$$\begin{aligned} \text{dom}(f\{x \rightsquigarrow n\}) &= \text{dom}(f) \cup \{x\} \\ \text{ran}(f\{x \rightsquigarrow n\}) &= \text{ran}(f - \{(x, n') \mid (x, n') \in f\}) \cup \{n\} \end{aligned}$$

Example

$(\lambda x \in [0..2].\, x + 1)\{2 \rightsquigarrow 7\} = \{(0,1), (1,2), (2,7)\}$
$(\lambda x \in [0..1].\, x + 1)\{2 \rightsquigarrow 7\} = \{(0,1), (1,2), (2,7)\}$

Function Types

We use $A \to B$ to represent the set of all functions from A to B.

$\to$ is right associative. That is,

$$A \to B \to C \; = A \to (B \to C)\,.$$

If $f \in A \to B \to C$, $a \in A$ and $b \in B$, then $f\,a\,b = (f(a))b \in C$.

Functions with multiple arguments

$$f \in A_1 \times A_2 \times \cdots \times A_n \to A$$

$$f = \lambda x \in A_1 \times A_2 \times \cdots \times A_n.\, E$$

$$f\,(a_1, a_2, \ldots, a_n)$$

Currying it gives us a function

$$g \in A_1 \to A_2 \to \cdots \to A_n \to A$$

$$g = \lambda x_1 \in A_1.\, \lambda x_2 \in A_2.\, \ldots \lambda x_n \in A_n.\, E$$

$$g\; a_1\; a_2\; \ldots\; a_n$$

Outline

Cartesian Products

Recall $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$.
Projections over pairs: $\pi_0(x, y) = x$ and $\pi_1(x, y) = y$.

Generalize to n sets:
$S_0 \times S_1 \times \cdots \times S_{n-1} = \{(x_0, \ldots, x_{n-1}) \mid \forall i \in [0, n-1].\ x_i \in S_i\}$
We say $(x_0, \ldots, x_{n-1})$ is an *n-tuple*.

Then we have $\pi_i(x_0, \ldots, x_{n-1}) = x_i$.

Tuples as Functions

We can view a pair (x, y) as a function

$$\lambda i \in \mathbf{2}.\ \begin{cases} x & \text{if } i = 0 \\ y & \text{if } i = 1 \end{cases}$$

where $\mathbf{2} = \{0, 1\}$.

$$A \times B \quad \stackrel{\text{def}}{=} \quad \{f \mid \text{dom}(f) = \mathbf{2},\ \text{and } f\,0 \in A \text{ and } f\,1 \in B\}$$

(We re-define $A \times B$ in this way, in order to generalize $\times$ later. Functions and relations are still defined based on the old definitions of $\times$.)

Tuples as Functions

Similarly, we can view an n-tuple $(x_0, \ldots, x_{n-1})$ as a function

$$\lambda i \in \mathbf{n}. \begin{cases} x_0 & \text{if } i = 0 \\ \ldots & \ldots \\ x_{n-1} & \text{if } i = n-1 \end{cases}$$

where $\mathbf{n} = \{0, 1, \ldots, n-1\}$.

$$S_0 \times \cdots \times S_{n-1} \quad \stackrel{\text{def}}{=} \quad \{f \mid \text{dom}(f) = \mathbf{n},\ \text{and } \forall i \in \mathbf{n}.\ f\ i \in S_i\}$$

Generalized Products

From

$$S_0 \times \cdots \times S_{n-1} \stackrel{\text{def}}{=} \{f \mid \text{dom}(f) = \mathbf{n},\ \text{and}\ \forall i \in \mathbf{n}.\ f\ i \in S_i\}$$

we can generalize $S_0 \times \cdots \times S_{n-1}$ to an infinite number of sets.

$$\prod_{i \in I} S(i) \stackrel{\text{def}}{=} \{f \mid \text{dom}(f) = I,\ \text{and}\ \forall i \in I.\ f\ i \in S(i)\}$$

$$\prod_{i=m}^{n} S(i) \stackrel{\text{def}}{=} \prod_{i \in [m,n]} S(i)$$

Generalized Products

Let θ is a function from a set of indices to a set of sets, i.e., θ is an indexed family of sets. We can define $\Pi\,\theta$ as follows.

$$\Pi\,\theta \stackrel{\mathsf{def}}{=} \{f \mid \mathrm{dom}(f) = \mathrm{dom}(\theta),\ \text{and } \forall i \in \mathrm{dom}(\theta).\ f\ i \in \theta\ i\}$$

Example

Let $\theta = \lambda i \in I.\, S(i)$. Then

$$\Pi\,\theta = \prod_{i \in I} S(i)$$

Generalized Products – Examples

$$\Pi\,\theta \stackrel{\text{def}}{=} \{f \mid \text{dom}(f) = \text{dom}(\theta),\ \text{and}\ \forall i \in \text{dom}(\theta).\ f\ i \in \theta\ i\}$$

Example (1)

Let $\theta = \lambda i \in \mathbf{2}.\mathbf{B}$. Then

$$\begin{aligned}\Pi\,\theta = \{\ &\{(0, \textbf{true}), (1, \textbf{true})\},\\ &\{(0, \textbf{true}), (1, \textbf{false})\},\\ &\{(0, \textbf{false}), (1, \textbf{true})\},\\ &\{(0, \textbf{false}), (1, \textbf{false})\}\ \}\end{aligned}$$

That is, $\Pi\,\theta = \mathbf{B} \times \mathbf{B}$.

(Here $\mathbf{B} \times \mathbf{B}$ uses the new definition of $\times$. If we use its old definition, we will see an elegant correspondence between $\Pi\,\theta$ and $\mathbf{B} \times \mathbf{B}$.)

Generalized Products – Examples

$$\Pi\,\theta \;\stackrel{\text{def}}{=}\; \{f \mid \mathrm{dom}(f) = \mathrm{dom}(\theta),\ \text{and } \forall i \in \mathrm{dom}(\theta).\ f\ i \in \theta\ i\}$$

Example (2)

$\Pi\,\emptyset \;=\; \{\emptyset\}$.

Example (3)

If $\exists i \in \mathrm{dom}(\theta).\ \theta\ i = \emptyset$, then $\Pi\,\theta \;=\; \emptyset$.

Exponentiation

Recall $\prod_{x \in T} S(x) = \Pi\lambda x \in T.\, S(x)$.

We write S^T for $\prod_{x \in T} S$ if S is independent of x.

$$\begin{aligned} S^T &= \prod_{x \in T} S = \Pi\lambda x \in T.\, S \\ &= \{f \mid \mathrm{dom}(f) = T,\ \text{and } \forall x \in T.\ f\,x \in S\} = (T \to S) \end{aligned}$$

Recall that $T \to S$ is the set of all functions from T to S.

Exponentiation – Example

We sometimes use $\mathbf{2}^S$ for powerset $\mathcal{P}(S)$. Why?

Exponentiation – Example

We sometimes use $\mathbf{2}^S$ for powerset $\mathcal{P}(S)$. Why?

$$\mathbf{2}^S \;=\; (S \to \mathbf{2})$$

For any subset T of S, we can define

$$f \;=\; \lambda x \in S. \begin{cases} 1 & \text{if } x \in T \\ 0 & \text{if } x \in S - T \end{cases}$$

Then $f \in (S \to \mathbf{2})$.

On the other hand, for any $f \in (S \to \mathbf{2})$, we can construct a subset of S.

Outline

Sums (or Disjoint Unions)

Example

Let $A = \{1, 2, 3\}$ and $B = \{2, 3\}$.
To define the disjoint union of A and B, we need to index the elements according to which set they originated in:

$$\begin{aligned} A' &= \{(0,1),(0,2),(0,3)\} \\ B' &= \{(1,2),(1,3)\} \end{aligned}$$

$$A + B = A' \cup B'$$

Sums (or Disjoint Unions)

$$A + B \overset{\text{def}}{=} \{(i, x) \mid i = 0 \text{ and } x \in A, \text{ or } i = 1 \text{ and } x \in B\}$$

Injection operations:

$$\iota^0_{A+B} \in A \to A + B$$
$$\iota^1_{A+B} \in B \to A + B$$

The sum can be generalized to n sets:

$$S_0 + S_1 + \cdots + S_{n-1} \overset{\text{def}}{=} \{(i, x) \mid i \in \mathbf{n} \text{ and } x \in S_i\}$$

Generalized Sums (or Disjoint Unions)

It can also be generalized to an infinite number of sets.

$$\sum_{i \in I} S(i) \stackrel{\text{def}}{=} \{(i, x) \mid i \in I \text{ and } x \in S(i)\}$$

$$\sum_{i=m}^{n} S(i) \stackrel{\text{def}}{=} \sum_{i \in [m,n]} S(i)$$

The sum of θ is

$$\Sigma\, \theta \stackrel{\text{def}}{=} \{(i, x) \mid i \in \text{dom}(\theta) \text{ and } x \in \theta\, i\}$$

So

$$\sum_{i \in I} S(i) = \Sigma \lambda i \in I . S(i)$$

Generalized Sums (or Disjoint Unions) – Examples

$$\Sigma\,\theta \;\overset{\text{def}}{=}\; \{(i, x) \mid i \in \mathrm{dom}(\theta) \text{ and } x \in \theta\, i\}$$

Example (1)

$$\sum_{i \in \mathbf{n}} S(i) \;=\; \Sigma \lambda i \in \mathbf{n}. S(i) \;=\; \{(i, x) \mid i \in \mathbf{n} \text{ and } x \in S(i)\}$$

Example (2)

Let $\theta = \lambda i \in \mathbf{2}.\mathbf{B}$. Then

$$\Sigma\,\theta = \{\ (0, \mathbf{true}), (0, \mathbf{false}), (1, \mathbf{true}), (1, \mathbf{false})\ \}$$

That is, $\Sigma\,\theta = \mathbf{2} \times \mathbf{B}$.

Generalized Sums (or Disjoint Unions) – Examples

$$\Sigma\,\theta \;\stackrel{\text{def}}{=}\; \{(i,x) \mid i \in \mathrm{dom}(\theta) \text{ and } x \in \theta\, i\}$$

Example (3)

$\Sigma\,\emptyset \;=\; \emptyset.$

Example (4)

If $\forall i \in \mathrm{dom}(\theta).\ \theta\, i = \emptyset$, then $\Sigma\,\theta \;=\; \emptyset$.

Example (5)

Let $\theta \;=\; \lambda i \in \mathbf{2}. \begin{cases} \mathbf{B} & \text{if } i = 0 \\ \emptyset & \text{if } i = 1 \end{cases}$,

then $\Sigma\,\theta \;=\; \{(0, \mathbf{true}), (0, \mathbf{false})\}$.

More on Generalized Sums (or Disjoint Unions)

$$\Sigma\,\theta \stackrel{\text{def}}{=} \{(i,x) \mid i \in \mathrm{dom}(\theta) \text{ and } x \in \theta\, i\}$$

$$\sum_{x \in T} S(x) \stackrel{\text{def}}{=} \Sigma\lambda x \in T.S(x)$$

We can prove $\sum_{x \in T} S = T \times S$ if S is independent of x.

$$\begin{aligned}\sum_{x \in T} S &= \Sigma\lambda x \in T.\,S \\ &= \{(x,y) \mid x \in T \text{ and } y \in S\} = (T \times S)\end{aligned}$$