Sets, Functions, Domains

Wolfgang Schreiner
Research Institute for Symbolic Computation (RISC-Linz)
Johannes Kepler University, A-4040 Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at
http://www.risc.uni-linz.ac.at/people/schreine

Sets

Collections of elements.

- Enumeration of elements

  $\{1, \{1, 4, 7\}, 4\}, \{\text{red, yellow}\}, \{\}$

- Defining property

  $\{x|P(x)\}$

  $\{x|\ x \text{ is an even integer}\}$

Examples

- Natural numbers **N**

  $\{0, 1, 2, \ldots\}$

- Truth values (Booleans) **B**

  $\{\text{true, false}\}$

- Rational numbers **Q**

  $\{x|x = p/q \text{ for some } p, q \in \mathbf{N}, q \neq 0\}$

Set Predicates

Based on concept of membership

- Membership $x \in S$

  Only basic predicate
  (sets are black boxes otherwise)

- Equivalence $R = S$

  $x \in R \Leftrightarrow x \in S$ (for all x)
  (extensionality principle)

- Subset $R \subseteq S$

  $x \in R \Rightarrow x \in S$ (for all x)
  ($\{\} \subseteq S$, $S \subseteq S$)

Set Constructions

Composition of sets

- Union $R \cup S$

  $\{x | x \in R \text{ or } x \in S\}$

  $\cup_i S_i = S_{j_1} \cup S_{j_2} \cup \ldots \cup S_{j_n}$

- Intersection $R \cap S$

  $\{x | x \in R \text{ and } x \in S\}$

  $\cap_i S_i = S_{j_1} \cap S_{j_2} \cap \ldots \cap S_{j_n}$

- Powerset $\mathbf{P}(R)$

  $\{x | x \subseteq R\}$

  $(\{\} \in \mathbf{P}(R), R \in \mathbf{P}(R))$

Product

Concept of ordered pair

- Constructor (x, y)
- Selectors

  fst(x,y) = x
  snd(x,y) = y
- Product $R \times S$

  $\{(x, y) | x \in\ R$ and $x \in\ S\}$

Sum

Concept of disjoint union

- Sum $R + S$

  $\{(\mathsf{zero}, x) | x \in\ R\} \cup \{(\mathsf{one}, y) | y \in\ S\}$
  "tags" to preserve origin of element

- Constructors

  $\mathsf{inR}(x) = (\mathsf{zero}, x)$ (for $x \in\ R$)
  $\mathsf{inS}(x) = (\mathsf{one}, y)$ (for $y \in\ S$)

- Selector

  cases m of
  $\quad\mathsf{isR}(x) \Rightarrow \boxed{\ldots \mathsf{x} \ldots}$
  $\quad\mathsf{isS}(y) \Rightarrow \boxed{\ldots \mathsf{y} \ldots}$
  end

  $m = (\mathsf{zero}, x) \Rightarrow \boxed{\ldots \mathsf{x} \ldots}$
  $m = (\mathsf{zero}, y) \Rightarrow \boxed{\ldots \mathsf{y} \ldots}$

Functions

Black box that accepts object as input and produces another object as output

Definition in terms of sets

- $f : R \Rightarrow S$

  f is function from R to S
  R domain of f, S codomain of f
  $R \Rightarrow S$ arity (functionality) of f

- Application $f(a)$

  $a \in R$, $f(a) \in S$

- Equality $f = g$

  $f, g : R \Rightarrow S\ f(x) = g(x)$ (for all x)
  (extensionality principle)

- Composition $f \circ g$

  $f : R \Rightarrow S, g : S \Rightarrow T$
  $f \circ g : R \Rightarrow T$
  $(f \circ g)(x) = g(f(x))$

Classification of Mappings

- Injective (one-one, 1-1)

  $f(x) = f(y) \Rightarrow\ x = y$ (for all $x, y \in\ R$)

- Surjective (onto)

  for every $y \in\ S$ there is some $x \in\ R$ such that $f(x) \in\ y$

- Identity function

  $f : R \Rightarrow\ R$
  $f(x) = x$ (for all $x \in\ R$)

- Inverse function

  $f : R \Rightarrow\ S$ injective and surjective
  $g : S \Rightarrow\ R, g(y) = x \Leftrightarrow\ f(x) = y$
  $g = f^{-1}$

Isomorphism

Relationship between sets defined by functions

R and S are isomorphic if there is a pair of functions

$$
\begin{aligned}
&f : R \Rightarrow S \\
&g : S \Rightarrow R \\
&f \circ g \text{ is identity on } R \\
&g \circ f \text{ is identity on } S
\end{aligned}
$$

f and g are then called $isomorphisms$.

Examples

- $R = \{1, 4, 7\}$ is isomorphic to $S = \{2, 4, 6\}$
- $A \times B$ is isomorphic to $B \times A$
- $\mathbf{N}$ is isomorphic to $\mathbf{Z}$

Functions as Sets

Every function $f : R \Rightarrow S$ can be represented by its $graph$:

$$\begin{aligned} graph(f) &= \{(x, f(x)) | x \in R\} \\ &\subseteq R \times S \end{aligned}$$

Successor function on $\mathbf{Z}$

$\{\ldots, (-2, -1), (-1, 0), (0, 1), (1, 2), \ldots\}$

- Function application

  $f(a) = b \Leftrightarrow (a, b) \in \mathsf{graph}(f)$
  $f(a) := \mathsf{apply}(\mathsf{graph}(f), a)$

- Function composition

  $\mathsf{graph}(f \circ g) =$
  $\{(x, z) |\ x \in R$ and, for some $y \in S$,
  $(x, y) \in \mathsf{graph}(f)$ and
  $(y, z) \in \mathsf{graph}(g)\}$

Examples

- $add : (\mathsf{N} \times \mathsf{N}) \Rightarrow \mathsf{N}$

  $\{((0,0),0),((1,0),1),((0,1),1),$
  $((1,1),2),((2,0),2),((2,1),3),$
  $((2,2),4),\ldots\}$

- $duplicate : R \Rightarrow R \times R, = \{1,4,7\}$

  $\{(1,(1,1)),(4,(4,4)),(7,(7,7))\}$

- $which : (\mathsf{B} + \mathsf{N}) \Rightarrow \{\mathsf{isbool}, \mathsf{isnum}\}$

  $\{((\mathsf{zero}, \mathsf{true}), \mathsf{isbool}),$
  $((\mathsf{zero}, \mathsf{false}), \mathsf{isbool}),$
  $((\mathsf{one}, 0), \mathsf{isnum}), ((\mathsf{one}, 1), \mathsf{isnum}),$
  $((\mathsf{one}, 2), \mathsf{isnum}), \ldots\}$

- $singleton : \mathsf{N} \Rightarrow \mathsf{P}(\mathsf{N})$

  $\{(0,\{0\}),(1,\{1\}),\ldots,(n,\{n\}),\ldots\}$

- nothing : $\mathrm{B} \cap \mathrm{N} \Rightarrow \mathrm{B}$

  $\{\}$

Examples

- $split\text{-}add : \mathbf{N} \Rightarrow (\mathbf{N} \Rightarrow \mathbf{N})$

$$\begin{aligned}\{\ &(0, \underline{\{(0,0),(1,1),(2,2),\ldots\}}),\\ &(1, \underline{\{(0,1),(1,2),(2,3),\ldots\}}),\\ &(2, \underline{\{(0,2),(1,3),(2,4),\ldots\}}),\\ &\ldots,\\ &(n, \underline{\{(0,n),(1,n+1),(2,n+2),\ldots\}}),\\ &\ldots\}\end{aligned}$$

- $make\text{-}succ : (\mathbf{N} \Rightarrow \mathbf{N}) \Rightarrow (\mathbf{N} \Rightarrow \mathbf{N})$

$$\begin{aligned}\{\ &\ldots,\\ &(\underline{\{(0,1),(1,1),(2,1),(3,6),\ldots\}},\\ &\underline{\{(0,2),(1,2),(2,2),(3,7),\ldots\}}),\ldots\}\end{aligned}$$

- $apply : (((\mathbf{N} \Rightarrow \mathbf{N})) \times \mathbf{N}) \Rightarrow \mathbf{N}$

$$\begin{aligned}\{\ &\ldots,\\ &((\underline{\{(0,1),(1,1),(2,1),(3,6),\ldots\}},0),1),\\ &((\underline{\{(0,1),(1,1),(2,1),(3,6),\ldots\}},1),1),\\ &((\underline{\{(0,1),(1,1),(2,1),(3,6),\ldots\}},2),1),\\ &((\underline{\{(0,1),(1,1),(2,1),(3,6),\ldots\}},3),6),\\ &\ldots\}\end{aligned}$$

Functions as Equations

More convenient form of specification

- $add : (\mathbf{N} \times \mathbf{N}) \Rightarrow \mathbf{N}$

  $\mathsf{add}(m, n) = m + n$

- $duplicate : R \Rightarrow R \times R, = \{1, 4, 7\}$

  $\mathsf{duplicate}(r) = (r, r)$

- $which : (\mathbf{B} + \mathbf{N}) \Rightarrow \{\mathsf{isbool}, \mathsf{isnum}\}$

  $$\begin{aligned}\mathsf{which}(m) = \ & \mathsf{cases}\ m\ \mathsf{of} \\ & \quad \mathsf{isB}(b) \Rightarrow \mathsf{isbool} \\ & \quad \mathsf{isN}(n) \Rightarrow \mathsf{isnum} \\ & \mathsf{end}\end{aligned}$$

- $singleton : \mathbf{N} \Rightarrow \mathbf{P}(\mathbf{N})$

  $\mathsf{singleton}(n) = \{n\}$

- $\mathsf{nothing} : \mathbf{B} \cap \mathbf{N} \Rightarrow \mathbf{B}$

  no equational definition (domain empty)!

Equations are just function representations!

Evaluation of Equations

- Definition $f : A \Rightarrow B, f(x) = \alpha$
- Application $f(a_0)$
  1. Substitution $[a_0/x]\alpha$
  2. Simplification to underlying value

Lambda Notation $f = \lambda x.\alpha$

split-add$(x) = \lambda y.x + y$
slit-add $= \lambda x.\lambda y.x + y$

Updating Functions $[a_0 \mapsto b_0]f$

$([a_0 \mapsto b_0]f)(a_0) = b_0$
$([a_0 \mapsto b_0]f)(a) = f(a)$, for all $a \neq a_0$

Semantic Domains

Those sets that are used as value spaces in denotational semantics.

- Primitive domains

  N, **Z**, **B**, ...

- Compound domains
  - Product domains $A \times B$
  - Sum domains $A + B$
  - Function domains $A \Rightarrow B$
  - Lifted domains $A_\perp = A \cup \{\perp\}$
    - $\perp$ = "bottom"
    - Non-termination, no value at all
    - Strict functions $f : A_\perp \Longrightarrow B_\perp, f = \underline{\lambda} x.\alpha$

      $f(\perp) = \perp$

      $f(a) = [a/x]\alpha,$ for $a \in A$

Semantic Algebras

Format for presenting semantic domains

Rational Numbers

Domain Rat $= (\mathbf{Z} \times \mathbf{Z})_\perp$

Operations

makerat : $\mathbf{Z} \Rightarrow (\mathbf{Z} \Rightarrow Rat)$
makerat $= \lambda p.\lambda q.(q = 0) \Rightarrow \perp [] (p, q)$
addrat : Rat $\Rightarrow$ (Rat $\Rightarrow$ Rat)
addrat $= \underline{\lambda}(p_1, q_1).\underline{\lambda}(p_2, q_2).((p_1 * q_2) + (p_2 * q_1), q1 * q2)$
multrat : Rat $\Rightarrow$ (Rat $\Rightarrow$ Rat)
multrat $= \underline{\lambda}(p_1, q_1).\underline{\lambda}(p_2, q_2).(p_1 * p_2, q_1 * q_2)$

Choice function $e_1 \Rightarrow e_2 [] e_3$
$\Rightarrow e_2$, if $e_1 =$ true
$\Rightarrow e_3$, if $e_1 =$ false