Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-06

Formalise!

$P : \mathit{Type}$ — The type of persons
$\_\text{called}\_ : P \to P \to \mathbb{B}$
$\_\text{isBrotherOf}\_ : P \to P \to \mathbb{B}$

---

1. Helen called somebody.
2. Helen called somebody who called her.
3. For everybody, there is somebody they haven't called.
4. Aos called only brothers of Jun.
5. Obama called everybody directly, or indirectly via at most two intermediaries.
6. If Shirley called Alex, then everybody who called Jim also called somebody who called Alex.
7. Jane called more people than Alex.

Plan for Today

- **Textbook Chapter 11: Set Theory**
  - Set comprehension
- **Textbook Chapter 14: Relations**
  - Pairs, Cartesian products

Set Comprehension

Set comprehension example:

$$\{x : \mathbb{Z} \mid 0 \le x < 5 \bullet x \cdot x\} = \{0, 1, 4, 9, 16\}$$

(11.1) **Set comprehension general shape:** $\{x : t \mid R \bullet E\}$

— This set comprehension **binds** variable x!

Evaluated in state s, this denotes the set containing the values of E evaluated in those states resulting from s by changing the binding of x to those values from type t that satisfy R.

Note: The braces "$\{\ldots\}$" are **only** used for set notation!

Abbreviation for special case: $\{x \mid R\} = \{x \mid R \bullet x\}$

(11.2) Provided $\neg occurs(`x', `e_0, \ldots, e_{n-1}')$,

$$\{e_0, \ldots, e_{n-1}\} = \{x \mid x = e_0 \vee \cdots \vee x = e_{n-1} \bullet x\}$$

Formalise!

$P : Type$ — The type of persons
$\_called\_ : P \to P \to \mathbb{B}$

Jane called more people than Alex.

$$\#\{ p : P \mid Jane \text{ called } p \} > \#\{ p : P \mid Alex \text{ called } p \}$$

Formalise!

The equation $f\ x = 0$ has at least five solutions.

Without sets: Use $\neq$ to assert "different":

$$\begin{array}{l} (\exists\, a, b, c, d, e \\ \quad \mid a \neq b \neq c \neq d \neq e \neq c \neq a \neq d \neq b \neq e \neq a \\ \quad \bullet f\ a = f\ b = f\ c = f\ d = f\ e = 0 \qquad) \end{array}$$

With sets — first attempt:

$$\#\{x \mid f\ x = 0\} \ge 5$$

That does not work for, e.g., $(\forall x \bullet f\ x = 0)$, nor for $f = \mathsf{sin}$.

Taking into account possibly infinite sets of solutions:

$$(\exists S : set(\mathbb{R}) \mid \#S \ge 5 \bullet (\forall x \mid x \in S \bullet f\ x = 0))$$

Set Membership

(11.3) **Axiom, Set membership:** Provided $\neg occurs(`x', `F')$,

$$F \in \{x \mid R \bullet E\} \quad \equiv \quad (\exists x \mid R \bullet E = F)$$

$$
\begin{array}{ll}
& F \in \{x \mid R\} \\
= & \langle \text{ Expanding abbreviation } \rangle \\
& F \in \{x \mid R \bullet x\} \\
= & \langle \text{ (11.3) Axiom, Set membership — } \textbf{provided } \neg occurs(`x', `F') \rangle \\
& (\exists x \mid R \bullet x = F) \\
= & \langle \text{ (9.19) Trading for } \exists \rangle \\
& (\exists x \mid x = F \bullet R) \\
= & \langle \text{ (8.14) One-point rule — } \textbf{provided } \neg occurs(`x', `F') \rangle \\
& R[x := F]
\end{array}
$$

(11.3.1) **Simple set compr. membership:** Provided $\neg occurs(`x', `F')$,

$$F \in \{x \mid R\} \quad \equiv \quad R[x := F]$$

Set Membership and Set Enumerations

(11.3) **Axiom, Set membership:** Provided $\neg occurs(`x', `F')$,

$$F \in \{x \mid R \bullet E\} \quad \equiv \quad (\exists x \mid R \bullet E = F)$$

(11.3.1) **Simple set compr. membership:** Provided $\neg occurs(`x', `F')$,

$$F \in \{x \mid R\} \quad \equiv \quad R[x := F]$$

(11.2) Provided $\neg occurs(`x', `e_0, \ldots, e_{n-1}')$,

$$\{e_0, \ldots, e_{n-1}\} = \{ x \mid x = e_0 \lor \cdots \lor x = e_{n-1} \bullet x \}$$

The empty set: $\{ x \mid false \bullet x \} = \{\} = \{\}$

Singleton sets: $\{ x \mid x = E \bullet x \} = \{E\}$ — provided $\neg occurs(`x', `E')$

One-point set comprehension: $\{x \mid x = E \bullet F\} = \{ F[x := E] \}$ — provided $\neg occurs(`x', `E')$

Set Comprehension versus Predicates

(11.5) $S = \{x \mid x \in S\}$ provided $\neg occurs(`x', `S')$

(11.7) $x \in \{x \mid R\} \quad \equiv \quad R$

(11.8) **Principle of comprehension:** To each predicate R there corresponds a set comprehension $\{x : T \mid R\}$ which contains the objects in T that satisfy R.

R is called a **characteristic predicate** of the set.

$f_R : T \to \mathbb{B}$ with $f\ x = R$ is also called the **characteristic function** of the set.

Two alternatives for defining sets:

$$
\begin{array}{lllllll}
S & = & \{x \mid R\} & \qquad & x \in S & \equiv & R \\
T & = & \{x \mid x = 3 \lor x = 5\} & \qquad & x \in T & \equiv & x = 3 \lor x = 5
\end{array}
$$

Calculate!

The size of a finite set S, that is, the number of its elements, is written $\# S$

- $\# \mathbb{B}$
- $\# \{ S : set(\mathbb{B}) \mid true \in S \bullet S \}$
- $\# \{ T : set(set(\mathbb{B})) \mid \{\} \notin T \bullet T \}$
- $\# \{ S : set(\mathbb{N}) \mid (\forall x : \mathbb{N} \mid x \in S \bullet x < n) \wedge \# S = k \bullet S \}$

- $\mathbb{B} = \{ false, true \}$
- $S \in set(\mathbb{B}) \quad \equiv \quad S \subseteq \mathbb{B}$
- $set(\mathbb{B}) = \{ \{\}, \{false\}, \{true\}, \{false, true\} \}$
- $T \in set(set(\mathbb{B})) \quad \equiv \quad T \subseteq set(\mathbb{B})$

Set Equality via Equivalence

(11.4) **Axiom, Extensionality:** Provided $\neg occurs(`x', `S, T')$,

$$S = T \quad \equiv \quad (\forall x \bullet x \in S \equiv x \in T)$$

(11.9) $\{x \mid Q\} = \{x \mid R\} \quad \equiv \quad (\forall x \bullet Q \equiv R)$

(11.10) **Metatheorem set comprehension equality:**

$\{x \mid Q\} = \{x \mid R\}$ is valid iff $Q \equiv R$ is valid.

(11.11) **Methods for proving set equality $S = T$:**

(a) Use Leibniz directly

(b) Use axiom Extensionality (11.4) and prove

$$v \in S \quad \equiv \quad v \in T$$

(c) Prove $Q \equiv R$ and conclude $\{x \mid Q\} = \{x \mid R\}$

Pairs and Cartesian Products

(14.1) — intentionally skipped

If b and c are expressions,
then $\langle b, c \rangle$ is their **2-tuple** or **ordered pair**

— "ordered" means that there is a **first** constituent (b) and a **second** constituent (c).

(14.2) **Axiom, Pair equality:**

$$\langle b, c \rangle = \langle b', c' \rangle \quad \equiv \quad b = b' \wedge c = c'$$

(14.3) **Axiom, Cross product:**

$$S \times T \;=\; \{ b, c \mid b \in S \wedge c \in T \bullet \langle b, c \rangle \} \;=\; \{ b : S; c : T \bullet \langle b, c \rangle \}$$

(14.4) **Membership:** $\quad b \in S \wedge c \in T \quad \equiv \quad \langle b, c \rangle \in S \times T$

For types: $\quad b : t_1 \; ; \; c : t_2$ iff $\langle b, c \rangle : t_1 \times t_2$

Some Cross Product Theorems

(14.5) $\langle x,y\rangle \in S\times T \quad\equiv\quad \langle y,x\rangle \in T\times S$

(14.6) $S=\{\} \quad\Rightarrow\quad S\times T = T\times S = \{\}$

(14.7) $S\times T = T\times S \quad\equiv\quad S=\{\}\vee T=\{\}\vee S=T$

(14.8) **Distributivity of $\times$ over $\cup$:**

$$\begin{array}{rcl} S\times(T\cup U) &=& (S\times T)\cup(S\times U) \\ (S\cup T)\times U &=& (S\times U)\cup(T\times U) \end{array}$$

(14.9) **Distributivity of $\times$ over $\cap$:**

$$\begin{array}{rcl} S\times(T\cap U) &=& (S\times T)\cap(S\times U) \\ (S\cap T)\times U &=& (S\times U)\cap(T\times U) \end{array}$$

(14.10) **Distributivity of $\times$ over $-$:**

$$\begin{array}{rcl} S\times(T-U) &=& (S\times T)-(S\times U) \\ (S-T)\times U &=& (S\times U)-(T\times U) \end{array}$$

(14.12) **Monotonicity:** $S\subseteq S' \wedge T\subseteq T' \quad\Rightarrow\quad S\times T\subseteq S'\times T'$

Pairs and Pair Projections

(14.2) **Axiom, Pair equality:** $\langle b,c\rangle = \langle b',c'\rangle \quad\equiv\quad b=b'\wedge c=c'$

(14.4p) **Axiom, Pair projections:**

$$\begin{array}{lcl@{\qquad}l} \mathsf{fst} &:& t_1\times t_2\to t_1 & \mathsf{fst}\ \langle b,c\rangle = b \\ \mathsf{snd} &:& t_1\times t_2\to t_2 & \mathsf{snd}\ \langle b,c\rangle = c \end{array}$$

(14.2p) **Pair equality:** For $p,q : t_1\times t_2$,

$$p=q \quad\equiv\quad \mathsf{fst}\ p = \mathsf{fst}\ q \ \wedge\ \mathsf{snd}\ p = \mathsf{snd}\ q$$

Proving (14.2e) **Pair extensionality:** $p=\langle \mathsf{fst}\ p, \mathsf{snd}\ p\rangle$**:**

$$\begin{array}{cl} & p=\langle \mathsf{fst}\ p,\mathsf{snd}\ p\rangle \\ = & \langle\ \text{(14.2p) Pair equality}\ \rangle \\ & \mathsf{fst}\ p = \mathsf{fst}\ \langle \mathsf{fst}\ p,\mathsf{snd}\ p\rangle \quad\wedge\quad \mathsf{snd}\ p = \mathsf{snd}\ \langle \mathsf{fst}\ p,\mathsf{snd}\ p\rangle \\ = & \langle\ \text{(14.4p) Pair projections}\ \rangle \\ & \mathsf{fst}\ p = \mathsf{fst}\ p \quad\wedge\quad \mathsf{snd}\ p = \mathsf{snd}\ p \\ = & \langle\ \text{(1.2) Reflexivity of equality, (3.38) Idempotency of } \wedge\ \rangle \\ & \mathit{true} \end{array}$$

Some Spice...

Converting between "different ways to take two arguments":

$$\begin{array}{lcl} \mathsf{curry} &:& (A\to B\to C)\to(A\times B\to C) \\ \mathsf{curry}\ f\ \langle x,y\rangle &:=& f\ x\ y \\ \mathsf{uncurry} &:& (A\times B\to C)\to(A\to B\to C) \\ \mathsf{uncurry}\ g\ x\ y &:=& g\langle x,y\rangle \end{array}$$

These functions correspond to the "Shunting" law:

(3.65) **Shunting:** $p\wedge q \Rightarrow r \quad\equiv\quad p\Rightarrow(q\Rightarrow r)$

The "currying" concept is named for Haskell Brooks Curry (1900–1982), but goes back to Moses Ilyich Schönfinkel (1889–1942) and Gottlob Frege (1848–1925).