Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-05

Anything Wrong?

$$
\begin{array}{ll}
& v \in (S - (T \cap U)) \\
\equiv & \langle \text{Set difference (11.22)} \rangle \\
& v \in S \land v \notin (T \cap U) \\
\equiv & \langle \text{Intersection (11.21)} \rangle \\
& v \in S \land (v \notin T \land v \notin U) \\
\equiv & \langle \text{Distributivity of } \land \text{ over } \land \rangle \\
& (v \in S \land v \notin T) \ \land (v \in S \land v \notin U) \\
\equiv & \langle \text{Intersection (11.21)} \rangle \\
& (v \in S \land v \notin T) \ \cap (v \in S \land v \notin U) \\
\equiv & \langle \text{Set difference (11.22)} \rangle \\
& (v \in (S - T)) \ \cap (v \in (S - U)) \\
\equiv & \langle \text{Intersection (11.21)} \rangle \\
& v \in ((S - T) \ \cap (S - U))
\end{array}
$$

Plan for Today

- **Textbook Chapter 11: Set Theory**
  — set comprehension

The Axioms of Set Theory — Overview

(11.2e) **Membership in Set Enumerations:**

$$v \in \{e_1, \ldots, e_n\} \quad \equiv \quad v = e_1 \vee \cdots \vee v = e_n$$

(11.2f) **Empty Set:** $v \in \{\} \equiv \mathit{false}$

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

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

(11.13T) **Axiom, Subset:** Provided $\neg occurs(`x', `S,T')$,

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

(11.14) **Axiom, Proper subset:** $S \subset T \quad \equiv \quad S \subseteq T \wedge S \neq T$

(11.20) **Axiom, Union:** $v \in S \cup T \quad \equiv \quad v \in S \vee v \in T$

(11.21) **Axiom, Intersection:** $v \in S \cap T \quad \equiv \quad v \in S \wedge v \in T$

(11.22) **Axiom, Set difference:** $v \in S - T \quad \equiv \quad v \in S \wedge v \notin T$

(11.23) **Axiom, Power set:** $v \in \mathbb{P}\, S \quad \equiv \quad v \subseteq S$

Set Equality and Inclusion

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

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

(11.13T) **Axiom, Subset:** Provided $\neg occurs(`x', `S,T')$,

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

(11.11b) **Metatheorem Extensionality:**
Let S and T be set expressions and v be a variable.
Then $S = T$ is a theorem iff $v \in S \equiv v \in T$ is a theorem.

(11.13m) **Metatheorem Subset:**
Let S and T be set expressions and v be a variable.
Then $S \subseteq T$ is a theorem iff $v \in S \Rightarrow v \in T$ is a theorem.

Extensionality (11.11b) and Subset (11.13m) will mostly be used **by LADM** as the following inference rules:

$$\frac{v \in S \quad \equiv \quad v \in T}{S \quad = \quad T} \qquad\qquad \frac{v \in S \quad \Rightarrow \quad v \in T}{S \quad \subseteq \quad T}$$

Using Set Extensionality — LADM-Style

Extensionality (11.11b) inference rule: $\dfrac{v \in S \equiv v \in T}{S = T}$

Ex. 8.2(a) Prove: $\{E, E\} = \{E\}$ for each expression E.

By extensionality (11.11b):

Proving $v \in \{E, E\} \quad \equiv \quad v \in \{E\}$**:**

$$\begin{aligned}
& v \in \{E, E\} \\
\equiv\ & \langle \text{ Membership in set enumerations (11.2e) } \rangle \\
& v = E \vee v = E \\
\equiv\ & \langle \text{ Idempotency of } \vee \text{ (3.26) } \rangle \\
& v = E \\
\equiv\ & \langle \text{ Membership in set enumerations (11.2e) } \rangle \\
& v \in \{E\}
\end{aligned}$$

Using Set Extensionality — More CalcCheck-Style

Axiom (11.4) "Set extensionality": $S = T \quad \equiv \quad (\forall x \bullet x \in S \equiv x \in T)$
— provided $\neg occurs(\text{'}x\text{'}, \text{'}S, T\text{'})$

Example (8.2a): $\{E, E\} = \{E\}$
Proof:
Using "Set extensionality":
Subproof for `$\forall v \bullet v \in \{E, E\} \quad \equiv \quad v \in \{E\}$`:
For any `$v$`:

$$
\begin{array}{ll}
& v \in \{E, E\} \\
\equiv & \langle \text{ Membership in set enumerations (11.2e) } \rangle \\
& v = E \vee v = E \\
\equiv & \langle \text{ Idempotency of } \vee \text{ (3.26) } \rangle \\
& v = E \\
\equiv & \langle \text{ Membership in set enumerations (11.2e) } \rangle \\
& v \in \{E\}
\end{array}
$$

Cardinality of Finite Sets

(11.12) **Axiom, Size:** Provided $\neg occurs(\text{'}x\text{'}, \text{'}S\text{'})$,

$$\# S = (\Sigma x \mid x \in S \bullet 1)$$

This uses: $\#\_ : set(t) \to \mathbb{N}$

Note:
- $(\Sigma x \mid x \in S \bullet 1)$ is defined only if S is finite.
- $\# \mathbb{N}$ **is undefined!**

Calculate!

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

- $\# \{1, 2\}$
- $\# \{1, 1\}$
- $\# \{1\}$
- $\# \{\}$
- $\# \{\{\}\}$
- $\# \{\{\{\}\}\}$
- $\# \{\{\}, \{\{\}\}\}$
- $\# \{\{\}, \{\}\}$
- $\# (\{1, 2, 3\} \cap \{3, 4\})$
- $\# (\{1, 2, 3\} \cup \{3, 4\})$
- $\# (\{1, 2, 3\} \times \{3, 4\})$
- $\# (\{1, 2, 3\} \cap \{3, 2\})$
- $\# (\{1, 2, 3\} \cup \{3, 2\})$
- $\# (\{1, 2, 3\} \times \{3, 2\})$
- $\# (\mathbb{P} \{1, 2, 3\})$
- $\# (\mathbb{P}\, \mathbb{P} \{1, 2, 3\})$

Power Set

(11.23) **Axiom, Power set:** $v \in \mathbb{P}\, S \quad \equiv \quad v \subseteq S$

$\mathbb{P}\,\mathbb{B} = \{\{\}, \{\mathit{false}\}, \{\mathit{true}\}, \{\mathit{false}, \mathit{true}\}\}$

- Each type t is a set of type $\mathit{set}(t)$
- For a type t, the **type of subsets of** t is $\mathit{set}(t)$
- For a type t considered as a set, its powerset is $\mathbb{P}\, t$
- According to the textbook, **type annotations** $v : t$, in particular in variable declarations in quantifications and in set comprehensions, **may only use types** t.
- We occasionally follow the specification notation Z in writing "$\mathbb{P}\, t$" also for "$\mathit{set}(t)$"

- $\#(\mathbb{P}\,\{1,2,3\})$
- $\#(\mathbb{P}\,\mathbb{P}\,\{1,2,3\})$

The Universe, and Set Complement

Frequently, a "domain of discourse" is assumed, that is, a set of "all objects under consideration".

This is often called a "**universe**".

Special notation: **U**

(11.17) **Axiom, Complement:** $v \in {\sim} S \quad \equiv \quad v \in \mathbf{U} \land v \notin S$

Complement can be expressed via difference:

$$\sim S \;=\; \mathbf{U} - S$$

Complement ~ **always implicitly depends on the universe U!**

Consider a context where $\mathbb{N} \subseteq \mathbb{Z}$:

- Let S be a subset of $\mathbb{N}$.
- Consider the complement $\sim S$
- Is $\quad -5 \in {\sim} S \quad$ true or false?

Metatheorem (11.25): Sets $\Longleftrightarrow$ Propositions

Let

- $P, Q, R, \ldots$ be set variables
- $p, q, r, \ldots$ be propositional variables
- E, F be expressions built from these set variables and $\cup$, $\cap$, $\sim$, **U**, $\{\}$.

Define the Boolean expressions E_p and F_p by replacing

$P, Q, R, \ldots$	with	$p, q, r, \ldots$	$\sim$	with	$\neg$
$\cup$	with	$\lor$	$\mathbf{U}$	with	true
$\cap$	with	$\land$	$\{\}$	with	false

Then:

- $E = F$ is valid iff $E_p \equiv F_p$ is valid.
- $E \subseteq F$ is valid iff $E_p \Rightarrow F_p$ is valid.
- $E = \mathbf{U}$ is valid iff E_p is valid.

Metatheorem (11.25): Sets $\Longleftrightarrow$ Propositions — Examples

Let E, F be expressions built from set variables P, Q, R, ...
and $\cup$, $\cap$, $\sim$, $\mathbf{U}$, $\{\}$.

Define the Boolean expressions E_p and F_p by replacing

$P, Q, R, \ldots$	with	$p, q, r, \ldots$	$\sim$	with	$\neg$
$\cup$	with	$\vee$	$\mathbf{U}$	with	*true*
$\cap$	with	$\wedge$	$\{\}$	with	*false*

Then:

- $E = F$ is valid iff $E_p \equiv F_p$ is valid.
- $E \subseteq F$ is valid iff $E_p \Rightarrow F_p$ is valid.
- $E = \mathbf{U}$ is valid iff E_p is valid.

Free theorems!

$$
\begin{array}{lcl}
P \cap (P \cup Q) & = & P \\
P \cap (Q \cup R) & = & (P \cap Q) \cup (P \cap R) \\
P \cup (Q \cap R) & \subseteq & P \cup Q \\
\vdots & &
\end{array}
$$

Set Comprehension

Set comprehension example:

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

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

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