Theory of Sets

CS 2LC3

Ryszard Janicki

Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada

Sets

- A **set** is simply a collection of distinct (different) elements.
- Examples of sets are the set of integers, the set of brown cows, and the set of computer science departments.
- While usually sets contain elements of the same type, a collection "White Elephant, Right Leg of Ryszard Janicki, Number 1, Aria 'La Donna A Mobile' and Black Tesla Car" is a proper set that consists of 5 elements!

Enumeration and Comprehension

- **Enumeration:** the list is delimited by braces and and its elements are separated by commas. Example: $\{5, 2, 3\}$, $\{a, b\}$.
- **Comprehension:** describes a set by stating properties enjoyed (exclusively) by its elements.
  Example $\{x : \mathbb{Z} \mid 0 \leq x < 5 : 2 \cdot x\} = \{0, 2, 4, 6, 8\}$.
- General form of set comprehension:
  $$\{x : t \mid R : E\},$$
  where: R is a predicate, E is an expression, x is a list of dummies, and t is a type.
- Evaluation of $\{x : t \mid R : E\}$ in a state yields the set of values that result from evaluating $E[x := v]$ in the state for each value v in t such that $R[x := v]$ holds in that state.
- , In contexts where the type of the dummy is obvious, the type may be omitted.
- If E has type t_1, then the set comprehension has type $set(t_l)$.

Examples of Comprehension

- In the following examples of set comprehension, the dummies range over the integers.

$\{i \mid 0 < i < 4 : i\}$	The set $\{1, 2, 3\}$
$\{i \mid 0 < i < 50 \wedge even.i : i\}$	Even positive integers less than 50
$\{i \mid 0 < 2 \cdot i < 50 : 2 \cdot i\}$	Even positive integers less than 50
$\{x, y \mid 1 \leq x \leq 2 \leq y \leq 3 : x^y\}$	The set $\{1^2, 1^3, 2^2, 2^3\}$
$\{x \mid 0 \leq x < 3 : x \cdot y\}$	The set $\{0 \cdot y, 1 \cdot y, 2 \cdot y\}$
$\{x \mid 0 \leq x < 0 : x \cdot y\}$	The empty set $\{\,\}$

- We can define a set enumeration $\{e_1, \ldots, e_n\}$ to be an abbreviation of a set comprehension:
$\{e_1, \ldots, e_n\} = \{x \mid x = e_1 \vee \ldots \vee x = e_n : x\}$.

Universe

- A theory of sets concerns sets constructed from some collection of elements.
- There is a theory of sets of integers, a theory of sets of characters, a theory of sets of sets of integers, and so forth.
- This collection of elements is called the *domain of discourse* or the *universe of values*; it is denoted by U.
- The universe can be thought of as the type of every set variable in the theory. For example, if the universe is $set(\mathbb{Z})$, then $v : set(\mathbb{Z})$.
- However again (heterogeneous sets):
  While usually sets contain elements of the same type, a collection "White Elephant, Right Leg of Ryszard Janicki, Number 1, Aria 'La Donna A Mobile' and Black Tesla Car" is a proper set that consists of 5 elements!

Set Membership and Equality

- For an expression e and a set-valued expression S, $e \in S$ is an expression whose value is the value of the statement "e is a member of S", or "e is in S".
- The expression $\neg(e \in S)$ may be abbreviated by $e \notin S$. For example, $2 \in \{1, 2, 4\}$ is *true* and $3 \notin \{1, 2, 4\}$ is *true*.
- For expression F :t and set $\{x \mid R : E : t\}$ (for some type t), we define:

  Axiom, Set membership: Provided $\neg occurs(`x`, `F`)$,
  $F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$.
- Two sets are equal if they contain the same elements.

  Axiom, Extensionality: $S = T \equiv (\forall x \mid: x \in S = x \in T)$.

Traditional Mathematical Notation

- The traditional mathematical notation for set comprehension is $\{x \mid R\}$ (x is a single variable), which we view as an abbreviation of $\{x \mid R : x\}$.
- For example: $\{i \mid 0 < i < 4\}$ is the set of $1, 2, 3$, and $\{i \mid 0 < i < 50 \wedge even.i\}$ is all even positive integers less than 50.
- Traditional notation and our new notation (page 3 of this lecture and 11.1 in the textbook) are equivalent as we have:

  Provided $\neg occurs(`y`, `R`)$ and $\neg occurs(`y`, `E`)$,
  $\{x \mid R : E\} = \{y \mid (\exists x \mid R : y = E)\}$.

Sets versus Predicates

- Connection between sets and predicates: a predicate is a representation for the set of argument-values for which it is *true*:

  $$x \in \{x \mid R\} \equiv R.$$

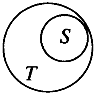
- Equivalently: $y \in \{x \mid R\} \equiv R[x := y]$.
- **Principle of comprehension**. To each predicate R there corresponds a set comprehension $\{x : t \mid R\}$, which contains the objects in t that satisfy R; R is called a *characteristic predicate* of the set.
- The following are equivalent: $S = \{3, 5\}$
  $S = \{x \mid x = 3 \vee x = 5\}$
  $x \in S \equiv x = 3 \vee x = 5$ (for all x).
- **Theorem.** $\{x \mid Q\} = \{x \mid R\}$ is valid iff $Q = R$ is valid.
- The above theorem gives us another method of proving equality of sets: show that their characteristic predicates are equivalent.

Expression	Example (with types)	Type of result
Empty set, universe, variable	$\emptyset$ or $\mathbf{U}$ or S	$set(t)$
Set enumeration	$\{e_1{:}t, \ldots, e_n{:}t\}$	$set(t)$
Set comprehension	$\{x \mid R{:}\mathbb{B} : E{:}t\}$	$set(t)$
	$\{x{:}t \mid R{:}\mathbb{B}\}$	$set(t)$
Set membership	$x{:}t \in S{:}set(t)$	$\mathbb{B}$
Set equality	$S{:}set(t) = T{:}set(t)$	$\mathbb{B}$
Set size	$\# S{:}set(t)$	$\mathbb{N}$
$\subset$, $\supset$, $\subseteq$, $\supseteq$	$S{:}set(t) \subseteq T{:}set(t)$	$\mathbb{B}$
Complement	$\sim S{:}set(t)$	$set(t)$
$\cup$, $\cap$, $-$	$S{:}set(t) \cup T{:}set(t)$	$set(t)$
Power set	$(\mathcal{P}\ S){:}set(t)$	$set(set(t))$

Cardinality of Finite Sets

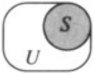
- The cardinality or size of a finite set S , denoted by $\#S$ (or, more often, $|S|$) , is the number of elements in S .
- **Axiom, Size:** $\#S = (\sum x \mid x \in S : 1)$.

Subset and Superset

- 

Set S is a *subset* of set T if every element of S is an element of T. This is depicted in the *Venn diagram*.
- S is a *proper subset* of T if it is a subset of T and $S \neq T$ holds.
- Predicates $S \subseteq T$ and $S \subset T$ denote subset and proper subset:

  Axiom, Subset: $S \subseteq T = (\forall x \mid x \in S : x \in T)$
  Axiom, Proper subset: $S \subseteq T \equiv S \subseteq T \vee S \neq T$
- Set T is a *superset* of (*proper superset* of) S if S is a subset of (proper subset of) T.

- 

The *complement* of S, written $\sim S$ (or $\overline{S}$), is the set of elements that are not in S (but are in the universe).

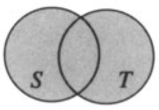
  Axiom, Complement: $v \in \sim S \equiv v \in U \wedge v \notin S$

- For example, for $U = \{0, 1, 2, 3, 4, 5\}$, we have

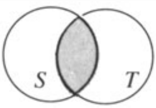
  $\sim \{3, 5\} = \{0, 1, 2, 4\}$
  $\sim U = \emptyset$, $\sim \emptyset = U$,

  where $\emptyset$ denotes *the empty set*.

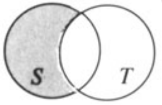
Union, Intersection and Difference



$S \cup T$



$S \cap T$



$S - T$

- The three operations union ($\cup$), intersection ($\cap$), and difference ($\setminus$ or $-$) are used to construct a set from two other sets.
- **Axiom, Union:** $v \in S \cup T \equiv v \in S \vee v \in T$
- **Axiom, Intersection:** $v \in S \cap T \equiv v \in S \wedge v \in T$
- **Axiom, Difference:** $v \in S \setminus T \equiv v \in S \wedge v \notin T$
- Right hand side of '$\equiv$' is a *Boolean expression*!
- Example: $\{3,5,6\} \cup \{3,2,1\} = \{1,2,3,5,6\}$
  $\{3,5,6\} \cap \{3,2,1\} = \{3\}$,
  $\{3,5,6\} \setminus \{3,2,1\} = \{5,6\}$.
- Sets S and T are *disjoint* if they have no elements in common, i.e. if $S \cap T = \emptyset$.

Power Set

- The *power set* of a set S , denoted by $\mathcal{P}S$ (or 2^S), is the set of subsets of S:

  Axiom, Power set: $v \in \mathcal{P}S \equiv v \subseteq S$.
- For example, $\mathcal{P}\{3,5\} = \{\emptyset, \{3\}, \{5\}, \{3,5\}\}$.

Set Operations and Boolean Expression

- **Definition.** Let E_s be a set expression constructed from set variables, $\emptyset$, U (a universe for all set variables in question), $\sim$, $\cup$, and $\cap$. Then E_p is the expression constructed from E_s by replacing $\emptyset$ with *false*, U with *true*, $\cup$ with $\vee$, $\cap$ with $\wedge$ and $\sim$ with $\neg$.
- **Metatheorem.** For any set expressions E_s and F_s :
  (a) $E_s = F_s$ is valid iff $E_p \equiv F_p$ is valid,
  (b) $E_s \subseteq F_s$ is valid iff $E_p \Rightarrow F_p$ is valid,
  (c) $E_s = U$ is valid iff E_p is valid.

Properties of Set Operators

Basic properties of $\cup$

(11.26) **Symmetry of $\cup$:** $S \cup T = T \cup S$

(11.27) **Associativity of $\cup$:** $(S \cup T) \cup U = S \cup (T \cup U)$

(11.28) **Idempotency of $\cup$:** $S \cup S = S$

(11.29) **Zero of $\cup$:** $S \cup \mathbf{U} = \mathbf{U}$

(11.30) **Identity of $\cup$:** $S \cup \emptyset = S$

(11.31) **Weakening:** $S \subseteq S \cup T$

(11.32) **Excluded middle:** $S \cup \sim S = \mathbf{U}$

Basic properties of $\cap$

(11.33) **Symmetry of $\cap$:** $S \cap T = T \cap S$

(11.34) **Associativity of $\cap$:** $(S \cap T) \cap U = S \cap (T \cap U)$

(11.35) **Idempotency of $\cap$:** $S \cap S = S$

(11.36) **Zero of $\cap$:** $S \cap \emptyset = \emptyset$

(11.37) **Identity of $\cap$:** $S \cap \mathbf{U} = S$

(11.38) **Strengthening:** $S \cap T \subseteq S$

(11.39) **Contradiction:** $S \cap \sim S = \emptyset$

Basic properties of combinations of $\cup$ and $\cap$

(11.40) **Distributivity of $\cup$ over $\cap$:**

$$S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$$

(11.41) **Distributivity $\cap$ over $\cup$:**

$$S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$$

Basic properties of combinations of $\cup$ and $\cap$ (cont.)

(11.42) **De Morgan:** (a) $\sim(S \cup T) = \sim S \cap \sim T$

(b) $\sim(S \cap T) = \sim S \cup \sim T$

Additional properties of $\cup$ and $\cap$

(11.43) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cup U) \subseteq (T \cup V)$

(11.44) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cap U) \subseteq (T \cap V)$

(11.45) $S \subseteq T \equiv S \cup T = T$

(11.46) $S \subseteq T \equiv S \cap T = S$

(11.47) $S \cup T = \mathbf{U} \equiv (\forall x \mid x \in \mathbf{U} : x \notin S \Rightarrow x \in T)$

(11.48) $S \cap T = \emptyset \equiv (\forall x \mid : x \in S \Rightarrow x \notin T)$

Properties of set difference

(11.49) $S - T = S \cap \sim T$

(11.50) $S - T \subseteq S$

(11.51) $S - \emptyset = S$

(11.52) $S \cap (T - S) = \emptyset$

(11.53) $S \cup (T - S) = S \cup T$

(11.54) $S - (T \cup U) = (S - T) \cap (S - U)$

(11.55) $S - (T \cap U) = (S - T) \cup (S - U)$

Implication versus subset

(11.56) $(\forall x \mid : P \Rightarrow Q) \equiv \{x \mid P\} \subseteq \{x \mid Q\}$.

Properties of subset

(11.57) **Antisymmetry** : $S \subseteq T \wedge T \subseteq S \;\equiv\; S = T$

(11.58) **Reflexivity** : $S \subseteq S$

(11.59) **Transitivity** : $S \subseteq T \wedge T \subseteq U \;\Rightarrow\; S \subseteq U$

(11.60) $\emptyset \subseteq S$

(11.61) $S \subset T \;\equiv\; S \subseteq T \;\wedge\; \neg(T \subseteq S)$

(11.62) $S \subset T \;\equiv\; S \subseteq T \;\wedge\; (\exists x \mid x \in T : x \notin S)$

(11.63) $S \subseteq T \;\equiv\; S \subset T \;\vee\; S = T$

(11.64) $S \not\subset S$

(11.65) $S \subset T \Rightarrow S \subseteq T$

(11.66) $S \subset T \Rightarrow T \not\subseteq S$

(11.67) $S \subseteq T \Rightarrow T \not\subset S$

(11.68) $S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S)$

(11.69) $(\exists x \mid x \in S : x \notin T) \Rightarrow S \neq T$

(11.70) **Transitivity** : (a) $S \subseteq T \wedge T \subset U \;\Rightarrow\; S \subset U$

(b) $S \subset T \wedge T \subseteq U \;\Rightarrow\; S \subset U$

(c) $S \subset T \wedge T \subset U \;\Rightarrow\; S \subset U$

Theorems Concerning Power Set $\mathcal{P}$

- $\mathcal{P}\emptyset = \{\emptyset\}$
- $S \in \mathcal{P}S$
- $|\mathcal{P}S| = 2^{|S|}$, for finite set S

Union and Intersection of Families of Sets

- Union and intersection are symmetric, associative, and idempotent and have identities. Therefore, each is a binary operator $*$ (quantifier) for which the notation $(*x \mid R : E)$ (or $*(x \mid R : E)$ is defined, as discussed in Lecture Notes 6 and Section 8 of the textbook.
- Union: $(\cup x \mid R : E)$
- Intersection: $(\cap x \mid R : E)$
- For example, $(\cup i \mid 0 \leq i < n : \{5^i, 6^i, 7^i\})$ denotes the set of values $5^i, 6^i, 7^i$ for i satisfying $0 \leq i < n$.
- A set S of sets is called a *partition* of another set T if every element of T is in exactly one of the elements of S.
- **Partition:** $(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge$
  $(\cup u \mid u \in S : u) = T$.

The Axiom of Choice

- Given a bag of candy, you can reach in and pick out a piece.
- What about *infinite* bag? Is this also so obvious?
- Consider and interval $[0, 1]$. Is it obvious that you can really get any number from this interval? Even not rational like, say, $1/\pi$?
- **Axiom of Choice:** For any type t, there exists a function $f : set(t) \rightarrow t$ such that for any nonempty set S, $f(S) \in S$.
- A function f chooses an element from S; it is our formalization of the hand that picks out a piece from a bag of candy.

Paradoxes

- **Liar Paradox:** Epimenides about 600 BC. : " I am lying". What is the logical value of this statement?
- *Wise citizen of* X: They are two neighbour tribes X and Y that hate each other. The king of Y issued an order that every citizen of X, if caught on Y territory must say something and if he/she is telling the truth he/she will be shot, and he/she is lying he/she will be hang. A wise citizen of X has been caught and he/she says: "I will be hang". What would happen?
- *Sicilian Barber:* There is a small village in remote Sicilian mountains where mafia rules and one of the rules that everyone must obey is that all males must always be shaved. There is only one barber, who comes from a old family of barbers which has its own sacred rule 'they never shave those who shave themselves'. This barber has good mafia connections, so nobody else can shave customers in this village. Does such a barber exist?

Some Formalisation of Paradoxes

- When discussing Propositional Logic we have proved that: $\neg P \not\equiv P$ for all predicates P.
- We may then prove that
  $$(\neg Q \not\equiv Q) \equiv (\neg Q \equiv Q)$$
  is *false*
- **Russell/Zermelo Paradox:** Suppose our theory of sets is untyped. Consider the set S of all sets that do not contain themselves as elements, which we define by
  $$x \in S \equiv x \notin x \text{ (for all sets } x \text{).}$$
- Direct substitution of set S for x above yields
  $$S \in S \equiv S \notin S$$
  which is *false*.
- *Conclusion 1*: The set $S = \{x \mid x \notin x\}$ does not exist.
- *Conclusion 2*: The set of all sets does not exist.
- Liar Paradox is used in proving almost all results about non existence of abstract entity/ solution, as for instance halting problem for Turing Machines (and computer programs), most undecidability problems, Gödel theorems (implicitly) etc.