AAA616: Program Analysis

Lecture 1 — Basic Math Notations

Hakjoo Oh
2022 Fall

Reference

- Chapter 1 of "The formal semantics of programming languages".

Logical Notation

For statements A and B,

- $A \;\&\; B$: A and B, the conjunction of A and B
- $A \implies B$: A implies B, if A then B
- $A \iff B$: A iff B, the logical equivalence of A and B
- $\neg A$: not A

Logical Notation

Logical quantifiers $\exists$ and $\forall$:

- $\exists x.\ P(x)$: for some x, $P(x)$
- $\forall x.\ P(x)$: for all x, $P(x)$
- Abbreviations:
  - $\exists x, y, \ldots, z.\ P(x, y, \ldots, z) \equiv \exists x \exists y \ldots \exists z.\ P(x, y, \ldots, z)$
  - $\forall x, y, \ldots, z.\ P(x, y, \ldots, z) \equiv \forall x \forall y \ldots \forall z.\ P(x, y, \ldots, z)$
  - $\forall x \in X.\ P(x) \equiv \forall x.\ x \in X \implies P(x)$
  - $\exists x \in X.\ P(x) \equiv \exists x.\ x \in X \ \&\ P(x)$
  - $\exists ! x.\ P(x) \equiv (\exists x.\ P(x)) \ \&\ (\forall y, z.\ P(y) \ \&\ P(z) \implies y = z)$

Sets

- A set is a collection of objects (also called elements or members)
- $a \in X$: a is an element of the set X
- A set X is a subset of a set Y, $X \subseteq Y$, iff every element of X is an element of Y:

$$X \subseteq Y \iff \forall z \in X.\ z \in Y.$$

- Sets X and Y are equal, $X = Y$, iff $X \subseteq Y$ and $Y \subseteq X$.
- $\emptyset$: empty set
- ω: the set of natural numbers $0, 1, 2, \ldots$

Constructions on Sets

- Comprehension: If X is a set and $P(x)$ is a property, the set

$$\{x \in X \mid P(x)\}$$

denotes the subset of X consisting of all elements x of X which satisfy $P(x)$.

- Powerset: the set of all subsets of a set:

$$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}.$$

- Indexed sets: Suppose I is a set and that for any $i \in I$ there is a unique object x_i. Then

$$\{x_i \mid i \in I\}$$

is a set. The elements x_i is *indexed* by the elements $i \in I$.

Constructions on Sets

- Union and intersection:

$$\begin{array}{rcl} X \cup Y & = & \{a \mid a \in X \text{ or } a \in Y\} \\ X \cap Y & = & \{a \mid a \in X \ \& \ a \in Y\} \end{array}$$

- Big union and intersection: When X is a set of sets,

$$\begin{array}{rcl} \bigcup X & = & \{a \mid \exists x \in X.\ a \in x\} \\ \bigcap X & = & \{a \mid \forall x \in X.\ a \in x\} \end{array}$$

When $X = \{x_i \mid i \in I\}$ for some index set I,

$$\bigcup_{i \in I} x_i = \bigcup X$$

$$\bigcap_{i \in I} x_i = \bigcap X$$

Constructions on Sets

- Disjoint union:

$$X \uplus Y = (\{0\} \times X) \cup (\{1\} \times Y).$$

- Product: For sets X and Y, their product is the set

$$X \times Y = \{(a, b) \mid a \in X \;\&\; b \in Y\}.$$

  In general,

$$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid \forall i \in [1, n].\ x_i \in X_i\}.$$

- Set difference:

$$X \setminus Y = \{x \mid x \in X \;\&\; x \notin Y\}.$$

Relations and Functions

- A binary relation R between X and Y is an element of $\mathcal{P}(X \times Y)$, $R \in \mathcal{P}(X \times Y)$, or $R \subseteq X \times Y$.
- When R is a binary relation $R \subseteq X \subseteq Y$, we write xRy for $(x, y) \in R$.
- A partial function f from X to Y is a relation $f \subseteq X \times Y$ such that

$$\forall x, y, y'. \ (x, y) \in f \ \& \ (x, y') \in f \implies y = y'.$$

- We use the notation $f(x) = y$ when there is y such that $(x, y) \in f$ and say $f(x)$ is *defined*, and otherwise $f(x)$ is *undefined*.
- A total function from X to Y is a partial function such that $f(x)$ is defined for all $x \in X$.
- $(X \rightharpoonup Y)$: the set of all partial functions from X to Y
- $(X \rightarrow Y)$: the set of all total functions from X to Y
- $\lambda x. \ e$: the lambda notation for functions

Relations and Functions

- Composition: When $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ are binary relations, their composition is a relation of type $X \times Z$ defined as,

  $$S \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y.\ (x, y) \in R \ \&\ (y, z) \in S\}$$

- $Id_X = \{(x, x) \mid x \in X\}$

Relations and Functions

- An equivalence relation on X is a relation $R \subseteq X \times X$ which is
  - reflexive: $\forall x \in X.\ xRx$,
  - symmetric: $\forall x, y \in X.\ xRy \implies yRx$, and
  - transitive: $\forall x, y, z \in X.\ xRy \ \&\ yRz \implies xRz$.
- Example: $=$ on numbers, the relation "has the same age" on people
- We sometime write $x \equiv y \pmod{R}$ for $(x, y) \in R$.
- The equivalence class of x under R, denoted $\{x\}_R$ or $[x]_R$:

$$[x]_R = \{y \in X \mid xRy\}.$$

- Quotient set: the set of all equivalence classes of X by R:

$$X/R = \{[x]_R \mid x \in X\}.$$

- For any equivalence relation R, X/R is a partition of X.

Relations and Functions

- Let R be a relation on a set X. Define $R^0 = Id_X$, and $R^1 = R$, and
$$R^{n+1} = R \circ R^n.$$
- The transitive closure of R:
$$R^+ = \bigcup_{n \in \omega} R^{n+1}$$
- The reflexive transitive closure of R:
$$R^* = \bigcup_{n \in \omega} R^n = Id_X \cup R^+.$$

Sequences

- Given a set S, S^+ denotes the set of all finite nonempty sequences of elements of S
- When σ is a finite sequence, σ_k denotes the $(k+1)$th element of the sequence, σ_0 the first element, and $\sigma_{\dashv}$.
- Given a sequence $\sigma \in S^+$ and an element $s \in S$, $\sigma \cdot s$ denotes a sequence obtained by appending s to σ.