Introduction to Computer Science Theory

Alvin Lin

August 2017 - December 2017

Proofs

A proof is a logical argument, inductive or deductive. Some proofs are completely analytical. They are strictly the result of symbolic manipulation (just like a computer program). A major effort in the 20th century mathematics was to make all proofs into symbolic manipulations. This effort failed, but the tools developed are still useful. This led to the theory of computing. In practice, proofs use natural language in a special way though having in mind a gross underlying formal structure can be very helpful.

Sentential Logic

A statement that evaluates to true or false.

- Shakespeare wrote x.
- n is an even prime number.
- Shakespeare wrote x and n is an even prime number.
- $y \in \{x \mid x^2 < 0\}$
- If x is a substring of y and y is a substring of x, then $y = x$.

Logical Forms

- Shakespeare wrote x.

$$P$$

- n is an even prime number.

$$Q$$

- Shakespeare wrote x and n is an even prime number.

$$P \wedge Q$$

Functions that take variables are called **predicates**.

- Shakespeare wrote x.

$$P(x)$$

- n is an even prime number.

$$Q(n)$$

- Shakespeare wrote x and n is an even prime number.

$$P(x) \wedge Q(n)$$

- If x is a substring of y and y is a substring of x, then $y = x$.

$$(S(x, y) \wedge S(y, x)) \rightarrow y = x$$

Free and bound variables

$$y \in \{x \mid x^2 < 9\}$$

Free variables are those that are currently in scope. The truth of the statement depends on what you assign them. y is a free variable in this example. Bound variables are out of scope. They overshadow any value you assign to them. x is a bound variable in this example.

- $y \in \{x \mid x^2 < 9\}$
  y is a free variable in this example.
- $\{x \mid x^2 < 9\}$
  There are no free variables in this example.
- $x^2 < 9$
  x is a free variable in this example.
- $\forall x(DOG(x) \rightarrow \exists y DAY(y) \wedge HAS(x, y))$
  There are no free variables in this example.

Predicate (quantificational) logic

- Everyone at RIT loves CS majors.
  Let P be the predicate "person", let A be the predicate "at", let R be the constant "RIT", let C be the predicate "CS Major", let L be the predicate "loves".
  $$\forall x(P(x) \land A(x, R) \rightarrow \forall y(C(y) \rightarrow L(x, y)))$$

- Someone at RIT loves some CS major.
  Using the same predicates and constants:
  $$\exists x(P(x) \land A(x, R) \land \exists y(C(y) \rightarrow L(x, y)))$$

- There is a CS major that everyone at RIT loves.
  Using the same predicates and constants:
  $$\exists x(C(x) \rightarrow \forall y(P(y) \land A(y, R) \land L(x, y)))$$

- Everybody loves somebody sometime.
  Let L be the predicates "loves", let P be the predicate "person".
  $$\forall x(P(x) \rightarrow \exists y \exists t(L(x, y, t)))$$

Proof meta-strategy

Write the proof in predicate logic, leaving no free variables. Using predicate logic as a roadmap, complete the proof by simplifying the predicate logic using formal definitions.

Example

Theorem: If x is a substring of y and y is a substring of x, then $y = x$.
Predicate logic:

$$\forall x(\forall y((\text{x is a substring of y} \land \text{y is a substring of x}) \rightarrow x = y)))$$

Proof: Choose an arbitrary string x. Choose an arbitrary string y. Assume that x is a substring of $y \land y$ is a substring of x. Substitute the formal definitions for substrings.
$$\forall x(\forall y((\exists w, z(wxz = y) \land \exists w, z(wyz = x)) \rightarrow x = y))$$

Note that what is left matches the for $R \to S$.

$$\exists w, z(wxz = y) \land \forall w, z(wyz = x)$$

By the definition of the substring relation, there exists strings w_1, z_1 such that $w_1 x z_1 = y$ and strings w_2, z_2 such that $w_2 y z_2 = x$.

Example

$$\forall \ sets \ A, B, C(A \cap (B \cup C) \subseteq (A \cap B) \cup C)$$

Substitute for formal definitions:

$$\forall \ sets \ A, B, C(A \cap (\{x \mid x \in B \lor x \in C\}) \subseteq (A \cap B) \cup B)$$

$$\forall \ sets \ A, B, C\Big(\big\{y \mid y \in A \land y \in \{x \mid x \in B \lor x \in C\}\big\} \subseteq (A \cap B) \cup C\Big)$$

$$\forall \ sets \ A, B, C\Big(\big\{y \mid y \in A \land (y \in B \lor y \in C)\big\} \subseteq \big\{x \mid (x \in A \land x \in B) \lor x \in C\big\}\Big)$$

$$\forall \ sets \ A, B, C$$

$$\Big(\forall z\Big(z \in \big\{y \mid y \in A \land (y \in B \lor y \in C)\big\} \to z \in \big\{x \mid (x \in A \land x \in B) \lor x \in C\big\}\Big)\Big)$$

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech