CSC165 Lecture notes

Tianyu Du

January 31, 2018

Info.
Created: January 15, 2018.
Last modified: January 31, 2018

Contents

1 Lecture 2 Jan.15 2018

1.1 Predicate Logic

Allow you to have a domain of objects that you want to talk about, we want to be express reason about this domain.

Predicate Simplest kind of Predicate Logical Formula is called a **predicate**. A predicate is a <u>function</u> with range $\{0, 1\}$.
Examples

1. *Less-than-or-equal-to:* $\leq : \mathbb{Z} \times \mathbb{Z} \to \{0, 1\}$

2. *Equality:* $=: \mathbb{Z} \times \mathbb{Z} \to \{0,1\}$
3. *Prime:* $Prime : \mathbb{N} \to \{0,1\}$
4. Define: $R : \{a,b\} \times \{1,2,3\} \to \{0,1\}$ as $R(a,1) = R(b,1) = R(c,1) = 1, R = 0$ elsewise.

When you specify/define a predicate you have to specify the domain.

Quantifiers Introduce two quantifiers, **exists**: $\exists$ and **for all**: $\forall$, that let us express,

$\exists x \in \mathbb{DOMAIN}$: There is at least one element in domain of predicate that is true.

equivalently, represent as $\vee$,

$$"\exists" \equiv p(x_0) \vee p(x_1) \vee p(x_2) \dots$$

$\forall x \in \mathbb{DOMAIN}$: All element in domain of predicate satisfy the predicate.

equivalently, represented as $\wedge$,

$$"\forall" \equiv p(x_0) \wedge p(x_1) \wedge p(x_2) \dots$$

Negation of quantifier statements

$$\neg(\exists x \in \mathbb{D},\ s.t.\ p(x)) \equiv \forall x \in \mathbb{D}, \neg p(x)$$

$$\neg(\forall x \in \mathbb{D},\ s.t.\ p(x)) \equiv \exists x \in \mathbb{D}, \neg p(x)$$

Nested quantifier more than one variable quantified.
Example

For every natural number x, if x is a power of 2 then $2x$ is a power of 2.

$$\forall x \in \mathbb{N}, (\exists k \in \mathbb{N}\ s.t.\ x = 2^k) \implies (\exists k' \in \mathbb{N}\ s.t.\ 2^{k'} = 2x)$$

2 Lecture 3 Jan.17 2018

Another example There are infinitely many natural number that are even.

$$\text{Even(...)}: \exists y \in \mathbb{N},\ x = 2y$$

$$\forall x \in \mathbb{N},\ \exists y\ s.t.\ y > x \wedge Even(y)$$

$$Q(x): \text{ some predicate}$$
$$Q(x): \mathbb{N} \to \{0,1\}$$
$$\forall x \in \mathbb{N}[Q(x) \implies \exists y \in \mathbb{N}[y > x \wedge Q(y)]]$$

Does this express *there are infinitely many numbers that satisfy* Q?
Not, consider a Q that is false for all x, the statement is vacuous truth, but it does not express what we want.
Fix it.

$$\exists z \in \mathbb{N}[Q(z)] \wedge \forall x \in \mathbb{N} \exists y \in \mathbb{N}[y > x \wedge Q(y)]$$

<u>To ensure that there are some elements satisfy Q</u>

Tips

1. Make sure you write down a predicate logic formula with **correct syntax**.
2. Use different variable names for different quantities.
3. When you quantify ($\exists x$ *or* $\forall y$) you must specify the **set**. e.g. We want to quantify over all $x \in \mathbb{N}$ such that $x \geq 5$.
   (a) Method 1: Predefine your set.
   $$\text{Let } S = \{x \mid x \in \mathbb{N},\ x \geq 5\} \quad \forall x \in S, x \geq 3$$
   (b) Method 2: By implication.
   $$\forall x \in \mathbb{N}, \quad x \geq 5 \implies x \geq 3$$

Note We will spend a lot of time defining new predicates using predicate logic and then reasoning about them.

Example: Divisibility Let $n, d \in \mathbb{Z}$, we say that d **divides** n or n is **divisible** by d iff

$$\exists k \in \mathbb{Z}\ s.t.\ n = d * k$$

$$Divides(d, n) : \exists k \in \mathbb{Z}\ [n = d * k]$$

this formula is a predicate logic, some of variables (k) are quantified and others (n, d) are not quantified, called **free variable**. This formula since it has free variables, it represents a predicate.
A formula with no free variable is called a **sentence**, sentences are true or false.

Let's express *For every integer x, if x divides 10 then it also divide 100.*

$$\forall x \in \mathbb{Z}\ [Divides(x, 10) \implies Divides(x, 100)]$$

equivalently,

$$\forall x \in \mathbb{Z}\ [\exists k \in \mathbb{Z}[10 = k * x] \implies \exists k' \in \mathbb{Z}[100 = k' * x]]$$

Note Proposition is a special type of predicate but it's **not** a sentence.

3 Lecture 4 Jan.22 2018

3.1 Introduction to proofs

Proof A **proof** is a logical argument that convinces another person that a statement is true. Can also have a **disproof** showing that a statement if false.

1. Write down what we want to prove using language of first order logic.
2. Introducing variable(s).
3. Write body of proof.

Example Prove that every natural number n satisfies the inequality $n^2+3n+7 \geq 4$,

Statement in first order logic:

$$\forall n \in \mathbb{N}, n^2 + 3n + 7 \geq 4$$

proof:

Introducing variable(s):

Let $n \in \mathbb{N}$

Body of proof:

$$\text{Since } n \in \mathbb{N},\ n \geq 0$$

$$\text{Therefore } n^2 \geq 0$$

$$\text{Similarly, } sincen \in \mathbb{N}, n \geq 0, 3n \geq 0$$

$$\therefore n^2 + 3n + 7 \geq 0 + 0 + 4$$

■

Example Prove that for every natural number n greater than 20, n satisfies $1.5n - 4 \geq 3$.

$$\forall n \in \mathbb{N}, [\ n > 20 \implies 1.5n - 4 > 3\ ]$$

proof.

$$\text{Let } n \in \mathbb{N},\ \text{assume that } n > 20$$

$$\text{Since } n > 20,\ 1.5n > 1.5(20) = 30$$

$$\text{So } 1.5n > 30$$

$$\therefore 1.5n - 4 > 26$$

$$\therefore 1.5n - 4 > 3$$

■

(More complex)Example Define a natural number to be a **Prime** numbers:

$$Divides(x,n) : \exists xk = n$$

$$Prime(n) : (n > 1) \wedge (\forall x \in \mathbb{N}, ((x \neq 1 \wedge x \neq n) \implies \neg Divides(x,n)))$$

Equivalently, take <u>contrapositive</u>

$$Prime(n) : (n > 1) \wedge (\forall x \in \mathbb{N}, Divides(x,n) \implies (x = 1 \vee x = n))$$

Example For every integer x, $x|x+1$ then $x|5$

$$\forall x \in \mathbb{Z}, [\ Divides(x, x+5) \implies Divides(x,5)\ ]$$

$$\forall x \in \mathbb{Z}, [\ (\exists k \in \mathbb{Z}\ s.t.\ xk = x+5) \implies (\exists k' \in \mathbb{Z}\ s.t.\ xk' = x)\ ]$$

proof.

$$\begin{gathered} \text{Let } x \in \mathbb{Z} \\ \text{Assume } k \in \mathbb{Z} \text{ is such that } xk = x+5 \\ \text{Let } k' = k-1 \\ \text{Then, } k'x = (k-1)x \\ = kx - x \\ \text{By assumption,} \\ = 5 \\ \text{Therefore, } \exists k' \in \mathbb{Z},\ s.t.\ k'x = 5 \end{gathered}$$

■

4 Lecture 5 Jan.24 2018

Generalization

$$\forall x \in \mathbb{Z}, \forall d \in \mathbb{Z} \forall a \in \mathbb{Z}\ [x|ax + d \implies x|d]$$

In more complicated proofs, a proof body is a sequence of true statements, where each statement follows logically from:

1. Definitions.
2. Assumptions. (mentioned in proof header)
3. Previous statements.
4. External facts/claims.

5 Lecture7 Jan.31.2018

5.1 Greatest common divisor

$IsCD : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \{0, 1\}$

$$IsCD(x, y, d) := d|x \wedge d|y$$

$IsGCD : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \{0, 1\}$

$$IsGCD(x, y, d) := IsCD(x, y, d) \wedge \forall d' \in \mathbb{Z},\ IsCD(x, y, d') \implies d' \leq d$$