Propositions and Proofs

Chang-Gun Lee (cglee@snu.ac.kr)

Assistant Professor

The School of Computer Science and Engineering

Seoul National University

Propositions

- A proposition is a declarative sentence that is either true or false
- Examples
  - It rained yesterday
  - The pressure inside of the reactor chamber exceeds the safety threshold
  - What time is it? (Not a proposition)
  - Please submit your report as soon as possible (Not a proposition)
  - 15 is divisible by 3 (True)
  - Champaign is the state capital of Illinois (False)

Mathematical Propositions

- Based on clear (precise and unambiguous) definitions of mathematical concepts
- Definition 2.1: (Even) An integer is called “even” provided it is divisible by two
  - Clear?
  - It involves more concepts: “integer” , “divisible”, “two”
  - Set of integers: positive whole numbers, negative whole numbers, and zero, i.e., Z = {..., -3, -2, -1, 0, 1, 2, 3, ...}
  - We know how to add, subtract, and multiply
  - Let’s start from there
- Definition 2.2: (Divisible) Let a and b be integers. We say that a is “divisible” by b provided there is an integer c such that $bc=a$. We also say b “divides” a, or b is a “factor” of a, or b is a “divisor” of a. The notation for this is $b|a$.

More definitions

- Definition 2.4 (Odd): An integer *a* is called *odd* provided there is an integer *x* such that $a = 2x+1$
  - Why not saying "an integer is odd provided it is not even"?
- Definition 2.5 (Prime): An integer *p* is called *prime* provided that $p>1$ and the only positive divisors of *p* are 1 and *p*
  - *Is 11 prime?*
  - *What about 1?*
- Definition 2.6 (Composite): A positive integer *a* is called composite provided there is an integer *b* such that $1 < b < a$ and $b|a$
  - *A prime number is NOT composite*
  - *Is every non-prime number composite?*

Theorem

- An IMPORTANT mathematical “TRUE” proposition is called a THEOREM
  - There should be a PROOF that the proposition is true
- Mathematicians make statements that we believe are true about mathematics
  - Statements we know to be true because we can prove them - *theorems*
  - Statements whose truth we cannot ascertain - *conjectures*
  - Statements that are false - *mistakes*
- Mathematical truth is most strict compared to any other discipline
  - *Meteorological Fact: In July, the weather in Seoul is hot and humid*
  - *Physical Fact: When an object is dropped near surface of the earth, it accelerate at a rate of 9.8 meter/sec*^{2}
  - In mathematics, the word TRUE is meant to be considered absolute, unconditional, and without exception

Typical form of theorem (If-Then)

- If A, then B (A => B, A implies B, B <= A, B is implied by A)
- If x and y are even integers, then $x+y$ is also even.
  - *The sum of two even integers is even*
- Theorem 3.1 (Pythagorean): If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2+b^2=c^2$
- Mathematical meaning of If-Then
  - *If you don't finish your lima beans, the you won't get dessert (Two promises)*
    - *If A happens, then B will happen as well*
    - *If A does not happen, then B will not happen*
  - *If x and y are two even integers, then x+y is also even (One promise)*
    - *If A happens, then B will happen as well*
    - *If A does not happen, we don't care B*

A	B	A => B
T	T	T
T	F	F
F	T	T
F	F	T

Typical form of theorem (If and Only If)

- A if and only if B (A iff B, A is equivalent to B, A <=> B)
  - If A then B, and if B then A
- An integer *x* is even if and only if *x+1* is odd.
  - *The sum of two even integers is even*
- Mathematical meaning of If-And-Only-If
  - *If you don't finish your lima beans, the you won't get dessert (Two promises)*
    - *In mathematical sense, it actually means "your will get dessert if and only if you finish your lima beans"*

A	**B**	**A <=> B**
T	T	T
T	F	F
F	T	F
F	F	T

Other Mathematical Logics

- AND
  - “A and B” is true if and only if both A, B are true
  - Every integer whose ones digit is 0 is divisible by 2 AND 5

A	B	A and B
T	T	T
T	F	F
F	T	F
F	F	F

- NOT
  - “not A” is true if and only if A is false
  - Not all primes are odd

A	not A
T	F
F	T

Other Mathematical Logics

- OR
  - "A and B" is true if and only if
    - A is true but not B
    - B is true but not A
    - Both A and B are ture
  - cf. "Tonight, when we go out for dinner, would you like to have pizza or Chinese food? → choose only one not both: This differs from the mathematical definition of OR.

A	**B**	**A or B**
T	T	T
T	F	T
F	T	T
F	F	F

Names of Theorem

- Theorem: An important fact (true proposition) that deserves to have such a profound name
  - Pythagorean Theorem
  - 6+3 = 9 (?)
- Lemma: A true proposition whose main purpose to help prove another, more important theorem
- Corollary: A result with a short proof using another, previously proved theorem

Proof

- The effort of proof is the most important tool
  - to train your mental ability
  - to discover important findings
  - to pursuing research in any fields
- General steps of research
  - study a number of examples and collect sample data
  - take a common features from those examples and samples
  - make a guess, formulate a statement we believe to be true (conjecture)
  - try to prove the statement (proof)
  - now the conjecture becomes a theorem

Proof Template 1
(Direct proof of an if-then theorem)

- Write the first sentence(s) of the proof by restating the hypothesis of the result. Invent suitable notation (e.g., assign letters to stand for variables)
- Write the last sentence(s) of the proof by restating the conclusion of the result
- Unravel the definitions, working forward from the beginning of the proof and backward from the end of the proof
- Figure out what you know and what you need. Try to forge a link between the two halves of your argument

Proof Template 1
(Direct proof of an if-then theorem)

- Proposition 4.3: Let a, b, and c be integers. If $a|b$ and $b|c$, then $a|c$.
- Proof

> Suppose a, b, and c are integers with $a|b$ and $b|c$.
> ......
> Therefore $a|c$.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b=ax$. Likewise there is an integer y such that $c=by$.
> ......
> Therefore there is an integer z such that $c=az$. Therefore $a|c$.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b=ax$. Likewise there is an integer y such that $c=by$.
> Let $z=xy$. Then $az=a(xy)=(ax)y=by=c$.
> Therefore there is an integer z such that $c=az$. Therefore $a|c$.

Proof Template 1
(Direct proof of an if-then theorem)

- Proposition 4.6: Let a, b, c and d be integers. If $a|b$, $b|c$, and $c|d$, then $a|d$.
- Proof (Use Proposition 4.3 as a lemma)

Suppose a, b, c, and d are integers with $a|b$, $b|c$, and $c|d$.
......
Therefore $a|d$.

Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$ and $b|c$, by Proposition 4.3, we have $a|c$. Now since $a|c$ and $c|d$, again by Proposition 4.3, we have $a|d$. (Therefore $a|d$.)

Proof Template 1
(Direct proof of an if-then theorem)

- Research on prime and composite
- Study examples
  - $3^3 + 1 = 27 + 1 = 28$
  - $4^3 + 1 = 64 + 1 = 65$
  - $5^3 + 1 = 125 + 1 = 126$, and
  - $6^3 + 1 = 216 + 1 = 217$
- Any guess?
  - If x is a positive integer, then $x^3 + 1$ is composite. (wrong!)
  - If an integer $x > 1$, then $x^3 + 1$ is composite. (Likely → Conjecture)
- Try to prove it to convert it to a theorem

> Let x be an integer and suppose $x > 1$.
> ......
> Therefore x^3+1 is composite.

Proof Template 2
(Direct proof of an if-and-only-if theorem)

- (=>) Prove "If A, then B"
- (<=) Prove "If B, then A"

Proof Template 2
(Direct proof of an if-and-only-if theorem)

- Proposition 4.5: Let x be an integer. Then x is even if and only if $x+1$ is odd.
- Proof

Let x be an integer
(=>) Suppose x is even. ... Therefore $x+1$ is odd.
(<=) Suppose $x+1$ is odd. ... Therefore x is even.

Let x be an integer
(=>) Suppose x is even. This means that there is an integer a such that $x = 2a$ (By definition of even). ... Therefore $x+1$ is odd.
(<=) Suppose $x+1$ is odd. So there is an integer b such that $x+1 = 2b+1$ (By definition of odd) ... Therefore x is even.

Let x be an integer
(=>) Suppose x is even. This means that there is an integer a such that $x = 2a$ (By definition of even). Adding 1 to both sides gives $x+1 = 2a+1$. Therefore $x+1$ is odd.
(<=) Suppose $x+1$ is odd. So there is an integer b such that $x+1 = 2b+1$ (By definition of odd). Subtracting 1 from both sides gives $x=2b$. Therefore x is even.

Proof Template 3 (Disprove If-Then Statement)

- It is enough to show an example (called counterexample) that makes "A is true but B is not"
- Statement 5.1 (false): Let a and b be integers. If $a|b$ and $b|a$, then $a=b$.
- Disprove

It seems plausible. It seems that if $a|b$, then $a <= b$, and if $b|a$ then $b<=a$, and so $a=b$.

But try strange examples such as 0 and negative numbers.
What about $a = 5$ and $b = -5$? ← counterexample

Boolean Algebra

- Algebra is useful for reasoning about “numbers”
  - operations: +, - , *, /
  - $x^2 - y^2 = (x-y)(x+y)$
  - It holds for any values of *x* and *y*
- Boolean algebra is useful for reasoning about “propositions” whose values are TRUE or FALSE
  - operations: and (^), or (v), not (~), if-then (→), if-and-only-if (<->)
  - boolean expression: A and (B or C) = (A and B) or (A and C)

Truth tables

x	*y*	*x ^ y*
T	T	T
T	F	F
F	T	F
F	F	F

x	*y*	*x v y*
T	T	T
T	F	T
F	T	T
F	F	F

x	~x
T	F
F	T

Equivalence of Boolean Expressions

- Equivalence of Expressions:
  - x^2-y^2 = $(x$-$y)(x+y)$: Impossible to try all the values to prove this equivalence
- Equivalence of Boolean Expressions
  - ~ (x ^ y) = (~x) v (~y): Possible to try out all values of x and y

Proof Template 4
(Truth table proof of logical equivalence)

- To show that two Boolean expressions are logically equivalent:
  - Construct a truth table showing the values of the two expressions for all possible values of the variables
- Check to see that the two Boolean expressions always have the same value

Proof Template 4
(Truth table proof of logical equivalence)

- Proposition 6.3: The expression $x \rightarrow y$ and $(\sim x) \vee y$ are logically equivalent
- Proof:

x	**y**	$x \rightarrow y$	$(\sim x) \vee y$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Known Theorems on Boolean Algebra

- Theorem 6.2:
  - $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$. (Commutative properties)
  - $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$. (Associative properties)
  - $x \wedge \text{TRUE} = x$ and $x \vee \text{FALSE} = x$. (Identity elements)
  - $\sim(\sim x) = x$.
  - $x \wedge x = x$ and $x \vee x = x$.
  - $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. (Distributive properties)
  - $x \wedge (\sim x) = \text{FALSE}$ and $x \vee (\sim x) = \text{TRUE}$.
  - $\sim(x \wedge y) = (\sim x) \vee (\sim y)$ and $\sim(x \vee y) = (\sim x) \wedge (\sim y)$. (DeMorgan's Laws)
- Proof: Easy.... Truth table proof

Homework

- 2.2, 2.4
- 3.1, 3.6
- 4.1, 4.8, 4.13
- 5.1, 5.6, 5.9
- 6.4, 6.19