Theorems and Proofs

Discrete Mathematics
Andrei Bulatov

Previous Lecture

- Quantifiers and compound statements
- Definitions, rules, and theorems
- Universe and interpretations
- Equivalent predicates
- Equivalent quantified statements
- Quantifiers and conjunction/disjunction

More Equivalences

- $\forall x\,(P(x) \land Q(x)) \;\Leftrightarrow\; (\forall x\, P(x)) \land (\forall x\, Q(x))$

  Prove!

- $\forall x\,(P(x) \lor Q(x))$ is not equivalent to $(\forall x\, P(x)) \lor (\forall x\, Q(x))$

  Find a counter-example!

Much More Equivalences

- If $\Phi \Leftrightarrow \Psi$ is a pair of logically equivalent compound statements, and $\Phi(x)$, $\Psi(x)$ denote the open compound statements obtained from Φ and Ψ by replacing every propositional variable occurring in these statements $(p,q,r, \ldots)$ with open statements $(P(x),Q(x),R(x),\ldots)$. Then

$$\forall x\, \Phi(x) \Leftrightarrow \forall x\, \Psi(x) \quad \text{and} \quad \exists x\, \Phi(x) \Leftrightarrow \exists x\, \Psi(x)$$

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r) \qquad \text{distributive law}$$

P(x)
Q(x)
R(x)

$$\forall x\, (P(x) \wedge (Q(x) \vee R(x))) \Leftrightarrow \forall x\, ((P(x) \wedge Q(x)) \vee (P(x) \wedge R(x)))$$

Much More Equivalences (cntd)

- $\exists x\, \neg(P(x) \wedge Q(x)) \Leftrightarrow \exists x\, (\neg P(x) \vee \neg Q(x))$

  $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

  DeMorgan's law

- $\exists x\, (P(x) \vee (Q(x) \vee R(x)) \Leftrightarrow \exists x\, ((P(x) \vee Q(x)) \vee R(x))$

  $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

  associativity

- $\forall x\, (P(x) \vee (P(x) \wedge Q(x)) \Leftrightarrow \forall x\, P(x)$

  $p \vee (p \wedge q) \Leftrightarrow p$

  absorption law

- $\forall x\, (P(x) \vee \neg P(x)) \Leftrightarrow T$

Quantifiers and Negation

- As we saw $\forall x\, P(x)$ is false if and only if there is a such that $P(a)$ is false.

  This means that $\neg(\forall x\, P(x)) \Leftrightarrow \exists x\, \neg P(x)$

- Similarly, $\neg(\exists x\, P(x)) \Leftrightarrow \forall x\, \neg P(x)$

  ``Not all lions are fierce'' $\Leftrightarrow$ ``There is a peaceful lion''

  ``Not all people like coffee'' $\Leftrightarrow$ ``Some people don't like coffee''

  ``There is no number such that $a^2 = -1$'' $\Leftrightarrow$ ``For all numbers $a^2 \neq -1$''

Multiple Quantifiers and Equivalences

- Logic equivalences for statements with multiple quantifiers are similar to those with one quantifier.
  - $\forall x\ \forall y\ (P(x) \wedge (Q(y) \vee R(x,y))) \Leftrightarrow \forall x\ \forall y\ ((P(x) \wedge Q(y)) \vee (P(x) \wedge R(x,y)))$
  - $\exists x\ \forall y\ \neg(P(x,y) \wedge Q(y,x)) \Leftrightarrow \exists x\ \forall y\ (\neg P(x,y) \vee \neg Q(y,x))$
  - $\exists x\ \exists y\ \exists z\ (P(x) \vee (Q(y) \vee R(z)) \Leftrightarrow \exists x\ \exists y\ \exists z\ ((P(x) \vee Q(y)) \vee R(z))$
  - $\neg(\exists x\ \forall y\ P(x,y)) \Leftrightarrow \forall x\ \exists y\ \neg P(x,y)$
  - $\neg(\forall x\ \exists y\ \forall z\ P(x,y,z)) \Leftrightarrow \exists x\ \forall y\ \exists x\ \neg P(x,y,z)$

Permutation of Quantifiers

- As is easily seen

$$\forall x\, \forall y\, P(x,y) \iff \forall y\, \forall x\, P(x,y)$$

$$\exists x\, \exists y\, P(x,y) \iff \exists y\, \exists x\, P(x,y)$$

Indeed, $\forall x\, \forall y\, P(x,y)$ means that whatever values a,b from the universe are $P(a,b)$ is true. Statement $\forall y\, \forall x\, P(x,y)$ means exactly the same.

For $\exists x\, \exists y\, P(x,y) \iff \exists y\, \exists x\, P(x,y)$ the argument is similar.

Permutation of Quantifiers (cntd)

- However, statements

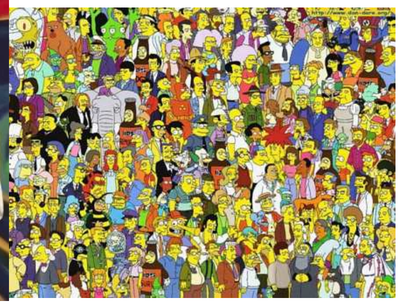
$$\forall x\ \exists y\ P(x,y) \quad \text{and} \quad \exists y\ \forall x\ P(x,y)$$

are not equivalent

Let $P(x,y)$ mean ``y is the mother of x''

Then $\forall x\ \exists y\ P(x,y)$ means ``Everyone has a mother''

While $\exists y\ \forall x\ P(x,y)$ can be translated as
``There is a person who is the mother of everyone''



What is a Theorem?

- The word `theorem' is understood in two ways
- First, a theorem is a mathematical statement of certain importance

  ``Every statement is equivalent to a certain CNF''

  ``A quadratic equation $ax^2 + bx + c = 0$ has at most 2 solutions''

- Second, a theorem is any statement inferred within an axiomatic theory

  ``Prove that the computer chip design is correct''

Axioms

- In both cases, to infer a theorem we need to start with something.
- Such starting point is a collection of axioms
- Two understandings of axioms:

  - self evident truth

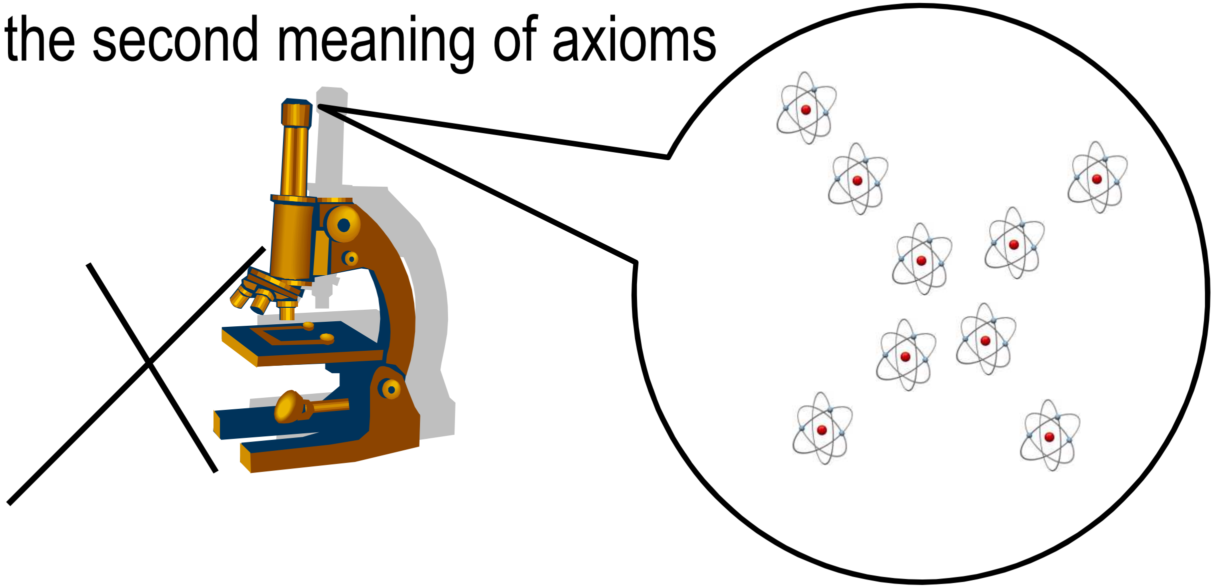
    ``Two non-parallel lines intersect''

    ``There is something outside me''

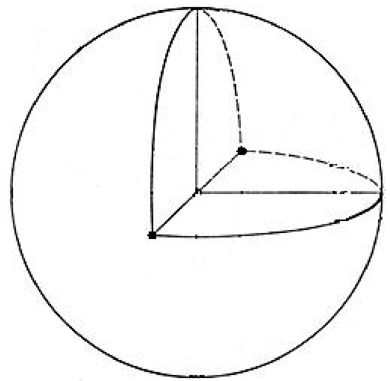
  - statements we assume as true, facts from experiment or observation, something we suggest and want to see implications

Axioms (cntd)

- Self evident truths are usually not quite truths, so we are left with the second meaning of axioms



- For any two points there is only one line that goes through them



Proving Theorems

- To prove theorems we use rules of inference.
  Usually implicitly
- In axiomatic theories it is done explicitly:
  - Specify axioms
  - Specify rules of inference
- Elementary geometry is an axiomatic theory.
- Axioms are Euclid's postulates

Proving Theorems

- We know rules of inference to reason about propositional statements. What about predicates and quantified statements?
- The simplest method is the method of exhaustion:

  To prove that $\forall x\ P(x)$, just verify that $P(a)$ is true for all values a from the universe.

  To prove that $\exists x\ P(x)$, by checking all the values in the universe find a value a such that $P(a)$ is true

``Every car in lot C is red''

``There is a blue car in lot C''

Rule of Universal Specification

- Reconsider the argument

  Every man is mortal.
  Socrates is a man.

  $\therefore$ Socrates is mortal

- In symbolic form it looks like

$$\begin{array}{l} \forall x\,(P(x) \rightarrow Q(x)) \\ P(\text{Socrates}) \\ \hline \therefore\ Q(\text{Socrates}) \end{array}$$

where
$P(x)$ stands for x is a man, and
$Q(x)$ stands for x is mortal

Rule of Universal Specification (cntd)

- If an open statement becomes true for all values of the universe, then it is true for each specific individual value from that universe

$$\frac{\forall x\ P(x)}{\therefore\ P(c)}$$

- Example

Premises: $\forall x\ (P(x) \to Q(x))$, $P(Socrates)$

Step	Reason
1. $\forall x\ (P(x) \to Q(x))$,	premise
2. $P(Socrates) \to Q(Socrates)$,	rule of universal specification
3. $P(Socrates)$	premise
4. $Q(Socrates)$	modus ponens

Rule of Universal Generalization

- Let us prove a theorem:

  If $2x - 6 = 0$ then $x = 3$.

- Proof

  Take any number c such that $2c - 6 = 0$. Then $2c = 6$, and, finally $c = 3$. As c is an arbitrary number this proves the theorem.

  Q.E.D

- Look at the first and the last steps.
  - In the first step instead of the variable we start to consider its generic value, that is a value that does not have any specific property that may not have any other value in the universe
  - In the last step having proved the statement for the generic value we conclude that the universal statement is also true

Rule of Universal Generalization (cntd)

- If an open statement $P(x)$ is proved to be true when x is assigned by any arbitrary chosen (generic) value from the universe, then the statement $\forall x\, P(x)$ is also true.
- Example: ``If $2x - 6 = 0$ then $x = 3$.''
- Notation: $P(x)$ - ``$2x - 6 = 0$'', $Q(x)$ - ``$2x = 6$'', $R(x)$ - ``$x = 3$''
- Premises: $\forall x\, (P(x) \to Q(x))$, $\forall x\, (Q(x) \to R(x))$
- Conclusion: $\forall x\, (P(x) \to R(x))$,

Step	Reason
1. $\forall x\, (P(x) \to Q(x))$, $\forall x\, (Q(x) \to R(x))$	premises
2. $P(c) \to Q(c)$, $Q(c) \to R(c)$,	rule of univ. specification
3. $P(c) \to R(c)$	rule of syllogism
4. $\forall x\, (P(x) \to Q(x))$	rule of univ. generalization

Existential Rules

- Rule of Existential Specification.

  If $\exists x\, P(x)$ is true in a given universe, then there is value a in this universe with $P(a)$ true.

- Rule of Existential Generalization.

  If $P(a)$ is true for some value a in a given universe, then $\exists x\, P(x)$ is true in this universe.

Homework

Exercises from the Book:

No. 5, 9, 11, 13, 15, 17 (page 116-117)