Theorems and Proofs

Discrete Mathematics

Courtesy of Andrei Bulatov

Previous Lecture

- *Equivalent predicates*
- *Equivalent quantified propositions*
- *Quantifiers and conjunction/disjunction*
- *Order of quantifiers*

A tale of two proofs

- *"Proof" can mean different things:*
  - *A formal, mechanical derivation in an axiomatic system, where each step has an explicit reason*

Step	*Reason*
1. $\neg p$	*premise*
2. $p \vee q$	*premise*
3. q	*Resolution (1,2)*

  - *An informal written argument, often using implicit assumptions about mathematical structures, which can in principle be formalized*

> *"The number x is not less than 0. Then x must be at least 0."*

Axioms

- *Axiomatic systems combine three things:*
  - *A collection of domains, predicates, and propositions*
    e.g. domain: integers
    P(x,y): "x > y"
    Q(x,y): "x = y"
  - *A set of obviously evident truths called the axioms*
    e.g. $\forall x.\forall y.\ (P(x,y) \vee P(y,x) \vee Q(x,y))$
  - *A set of rules for making valid inferences*
    e.g. modus ponens

$$\frac{p \rightarrow q \qquad p}{\therefore\ q}$$

Zermelo-Fraenkel set theory

- *Domain: sets (next week!)*
- *Predicates:*
  "x = y"
  "x Є y"
- *Axioms*

Foundation of mathematics:
every theorem
can be formalized using these axioms & logical inferences*

Ext	$\forall a \forall b\,[\,\forall x(x \in a \leftrightarrow x \in b) \rightarrow a = b\,]$
Pair	$\forall a \forall b\,\exists c\,\forall x[\,x \in c \leftrightarrow (x = a \vee x = b)\,]$
Union	$\forall a\,\exists b\,\forall x[\,x \in b \leftrightarrow \exists y(x \in y \wedge y \in a)\,]$
Pow	$\forall a\,\exists b\,\forall x[\,x \in b \leftrightarrow \forall y(y \in x \rightarrow y \in a)\,]$
Inf	$\exists a[\,\emptyset \in a \wedge \forall x(x \in a \rightarrow x \cup \{x\} \in a)\,]$
Sep_φ	$\forall a\,\exists b\,\forall x[\,x \in b \leftrightarrow (x \in a \wedge \varphi(x, \vec{p}))\,]$
Repl_φ	$\forall a[(\forall x \in a\,\exists!\, y\,\varphi(x, y, \vec{p})) \rightarrow \exists b\,\forall y(y \in b \leftrightarrow \exists x \in a\,\varphi(x, y, \vec{p}))]$
Found	$\forall a[\,a \neq \emptyset \rightarrow \exists x \in a\,\neg\exists y(y \in x \wedge y \in a)\,]$
AC	$\forall a[(\emptyset \notin a \wedge \forall x \neq y \in a\, x \cap y = \emptyset) \rightarrow \exists c\,\forall x \in a\,\exists!\, y(y \in x \wedge y \in c)]$

Modern foundations

- *ZFC Set theory is actually a pretty terrible foundation*
  - *Axiom of choice in particular is contentious*
- *Modern foundations based on (axiomatic) type theory*
  - *Same meaning as "types" in C/Python*
  - *Curry-Howard correspondence: "programs are proofs"*
- *Theorem proving languages like Lean, Rocq use type theories in place of ZFC*
  - *Though ZFC can be defined within them*
- *For theoretical reasons, usually intuitionistic/constructive*
  - *Can't assume law of the excluded middle!*

From formal to informal proofs

- *Axiomatic systems and formal proof are unwieldy for humans to write & understand*
  - *But good for computers / computer programs!*

- *Informal proofs are written in prose and*
  - *Don't explicitly state obvious inferences and axioms*
  - *Do explain assumptions, non-obvious axioms, or non-trivial inferences*

More formal ⟵ ⟶ *Less formal*

premise	1. $\forall x\,(P(x) \rightarrow Q(x))$	*It is assumed that all men are mortal, and so if Socrates is a man, then Socrates is mortal. Since Socrates is in fact a man, by the assumption Socrates must be mortal*	*Socrates is a man, and so Socrates is obviously mortal.*
instantiation	2. $P(Socrates) \rightarrow Q(Socrates)$		
premise	3. $P(Socrates)$		
modus ponens	4. $Q(Socrates)$		

Mathematical taxonomy

- *Result: a proven mathematical fact*
- *Theorem: result of "great" importance*
  e.g. "God exists"
- *Proposition: result of "lesser" importance*
  e.g. "People exist"
- *Lemma: intermediate result used to prove other results*
  e.g. "There exists an ordinal which is greater than all numbers"
- *Corollary: obvious consequence of another result*
  e.g. "Not all ordinals are numbers"
- *Conjecture: a theorem which has not yet been proven*
  e.g. "There are infinite parallel universes"

Proving theorems (or results)

- *Key: should be evidently formalizable!*
- *What this means in practice: should use known, valid rules of inference*

Theorem:

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

Logical form:

$\forall x.\ (2x - 6 = 0) \rightarrow (x = 3)$

Proof:

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

Q.E.D

Universal generalization

Formalization

- *Statement:* ``*If* $2x - 6 = 0$ *then* $x = 3$.''
- *Predicates:* $P(x)$ - ``$2x - 6 = 0$'', $Q(x)$ - ``$2x = 6$'', $R(x)$ - ``$x = 3$''
- *Need to prove:* $\forall x\,(P(x) \rightarrow R(x))$
- *Axioms:* $\forall x\,(P(x) \rightarrow Q(x))$, $\forall x\,(Q(x) \rightarrow R(x))$

Step	*Reason*
1. $P(c)$	*assumption*
1. $\forall x\,(P(x) \rightarrow Q(x))$, $\forall x\,(Q(x) \rightarrow R(x))$	*premises*
2. $P(c) \rightarrow Q(c)$, $Q(c) \rightarrow R(c)$,	*univ. instantiation*
3. $R(c)$	*Modus Ponens*
4. $\forall x\,(P(x) \rightarrow R(x))$	*univ. generalization*

Direct Proofs

- *Direct proofs are used when we need to proof propositions like*

$$\forall x\,(P(x) \rightarrow Q(x))$$

- *Goal: prove that* $P(a) \rightarrow Q(a)$ *is a tautology for an arbitrary a.*
- *Proof structure:*

1. *Assume that* $P(a)$ *is true*
2. *Using axioms, previous theorems etc. prove that* $Q(a)$ *is true*
3. *Conclude that* $P(a) \rightarrow Q(a)$ *is true*
4. *Use the rule of universal generalization to infer*

$$\forall x\,(P(x) \rightarrow Q(x))$$

Example

$Even(n) \leftrightarrow \exists k.\ n = 2k$

$Odd(n) \leftrightarrow \exists k.\ n = 2k+1$

- *Definitions:*

  n is even if and only if there exists k such that $n = 2k$

  n is odd if and only if exists k such that $n = 2k+1$

- *Theorem:*

  If n is odd, then n^2 is odd

- *Proof:*

  - *Let n be an arbitrary odd integer.*
  - *Then there exists k such that $n = 2k+1$.* (Exist. instantiation)
  - *Now, $n^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2(2k^2 + k) + 1$.* (Implicit axioms)
  - *Hence there exists k' such that $n^2 = 2k' + 1$.* (Exist. generalization)
  - *Therefore n^2 is odd*

Q.E.D.

Proof by contrapositive

- *Sometimes a direct proof of $\forall x\,(P(x) \rightarrow Q(x))$ doesn't work out*
- *In these cases, it can be easier to instead prove the equivalent contrapositive, $\forall x\,(\neg Q(x) \rightarrow \neg P(x))$*
- *Theorem:*
  If 3n + 2 is odd, then n is odd
- *Proof:*
  - *Let n be an arbitrary integer and assume n is not odd.*
  - *Then there exists k such that n = 2k.*
  - *Now, 3n+2 = 3(2k) + 2 = 6k + 2 = 2(6k + 1).*
  - *Hence there exists k' such that 3n+2 = 2k'.*
  - *Therefore 3n+2 is not odd*

Q.E.D.

Proof by Contraposition (cont)

- *Used when need to prove* $\forall x\,(P(x) \rightarrow Q(x))$
- *Goal: prove that* $\neg Q(a) \rightarrow \neg P(a)$ *for an arbitrary a*
- *Proof structure:*

1. *Assume that* $\neg Q(a)$ *is true*
2. *Using axioms, previous theorems etc. prove that* $\neg P(a)$ *is true*
3. *Conclude that* $\neg Q(a) \rightarrow \neg P(a)$ *is true*
4. *Conclude that* $P(a) \rightarrow Q(a)$ *is true by logical equivalence*
5. *Use the rule of universal generalization to infer*

$$\forall x\,(P(x) \rightarrow Q(x))$$

Example

- *Theorem:*
  If n=ab, then a ≤ √(n) ∨ b ≤ √(n)

- *Proof:*

  - *Let a and b be arbitrary*
  - *Suppose a > √(n) and b > √(n)*
  - *Then ab > √(n)√(n) ≥ n*
  - *Thus n is not equal to ab*

Q.E.D.

Practice

Exercises from the Book:

7th edition: 13, 15, 23, 27 (page 79 – 80)

8th edition: 13, 15, 23, 27 (page 83 – 84)