Theorems and Proofs II

Discrete Mathematics

Courtesy of Andrei Bulatov

Previous Lecture

- *Axiomatic systems*
- *Informal proof*
- *Proof methods*
  - *Direct proof*
  - *Proof by contrapositive*

Proof = logical inference

- *Any theorem can be expressed in symbolic logic*
- *The formula being proved gives a (direct, mechanical) proof structure*

Formula	Direct inference
$\forall x\, P(x)$	*Show P(a) for an arbitrary a*
$\exists x\, P(x)$	*Show P(a) for some specific a*
$P \rightarrow Q$	*Assume P and show Q*
$P \leftrightarrow Q$	*Show $P \rightarrow Q$ and $Q \rightarrow P$*
$P \wedge Q$	*Show P and Q*
$P \vee Q$	*Show P or show Q*

- *Can always rewrite to a logically equivalent formula and prove that*
  e.g. Proof by contrapositive
- *What about other logical inferences?*

Proof by Contradiction

- *Based on the rule of contradiction*

$$\frac{\neg p \rightarrow F}{\therefore\ p}$$

- *Can be used to prove propositions of any form*

- *Proof structure:*
  1. *Assume* $\neg p$.
  2. *Infer a contradiction, i.e.* F
  3. *Conclude* p.

Usually by showing r and $\neg r$

Example

- **Definition**: *a barber is called strict if he shaves those and only those who do not shave themselves.*
- **Theorem**. *There is no strict barber.*
- **Proof**.
- *Assume the contrary: a strict barber (c such that S(c)) exists*
- *Does he shave himself – say Q(c)?*
- *If no ($\neg Q(c)$), then by definition he must shave himself (Q(c))*
- *If yes (Q(c)), then by definition he must not ($\neg Q(c)$)*
- *Either way we have $Q(c) \wedge \neg Q(c)$, a contradiction*
- *We conclude that a strict barber does not exist*

Example (cntd)

Another Example

- *Definition: a real number is said to be rational if it can be represented as a fraction* $\frac{a}{b}$ *where* a, b *are integers*
- *Prove that* $\sqrt{2}$ *is irrational*
- *Proof*

  Suppose that $\sqrt{2}$ *is rational*

  Then there are integers a, b *such that* $\sqrt{2} = \frac{a}{b}$.

  We may assume that a, b *have no common divisor.*

  Squaring we obtain $a^2 = 2b^2$.

  Since a^2 *is even,* a *is also even, hence* $a = 2c$ *for some* c.

  Therefore $2b^2 = 4c^2$, *and so* $b^2 = 2c^2$.

  Hence b *is even.*

  We get that a *and* b *have a common factor – 2. A contradiction.*

Proof by cases

- *Based on the inference rule*

$$\frac{p \rightarrow r \qquad q \rightarrow r}{\therefore\ (p \vee q) \rightarrow r}$$

- *Used to prove implications where the premise can be decomposed into a small number of cases*
- *Proof structure (proving $p \rightarrow q$):*
  1. *Assume p*
  2. *Decompose p into cases $p_1 \vee p_2$ --- that is, infer $p \rightarrow p_1 \vee p_2$*
  3. *Show that $p_1 \rightarrow q$* *(Case 1)*
  4. *Show that $p_2 \rightarrow q$* *(Case 2)*
  5. *Conclude $p \rightarrow q$.*

Example

- *Theorem:*

  If n is an integer, then $n^2 \geq n$

- *Proof:*

  Suppose n is an integer

  Then either (1) n = 0, (2) n > 0, or (3) n < 1

  Case 1: n = 0

  Then $n^2 = 0 = n$, so $n^2 \geq n$

  Case 2: n > 0

  Then $n \geq 1$, so multiplying both sides by n, $n^2 \geq n$

  Case 3: n < 0

  Then $n^2 \geq 0 > n$, so $n^2 \geq n$

  In all cases, $n^2 \geq n$ *Q.E.D.*

Proof play-by-play

- *In the last example, the theorem had the form*

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

  so why was this valid?

- *We implicitly used that fact that*

  $$\forall x\,(\mathit{Integer}(x) \rightarrow (x = 0) \vee (x > 0) \vee (x < 0))$$

- *Then we showed for arbitrary n by case inference that*

  $$(n = 0) \vee (n > 0) \vee (n < 0) \rightarrow n^2 \geq n$$

- *Then we used syllogism to infer the conclusion:*

  $$\mathit{Integer}(n) \rightarrow (n = 0) \vee (n > 0) \vee (n < 0)$$
  $$(n = 0) \vee (n > 0) \vee (n < 0) \rightarrow n^2 \geq n$$
  $$\therefore\ \mathit{Integer}(n) \rightarrow n^2 \geq n$$

Exhaustive proof

- *Special case of proof by cases*
- *Replace an arbitrary a with disjunction of every possible value*

Theorem:

if $0 < n \leq 4$, then $3^n \leq (n + 1)^3$

Proof:

There are 4 cases to consider: n = 1, 2, 3, or 4

Case 1: n = 1

Then $3^1 = 3 \leq (1 + 1)^3 = 8$

Case 2: n = 2

Then $3^2 = 9 \leq (2 + 1)^3 = 27$

Case 3: n = 3

"By calculation"

"remaining cases follow similarly"

Don't do this
(proof by intimidation)

Q.E.D.

Excluding cases

- *Common error is incorrectly thinking you considered all cases*
  e.g. Case 1: x > 0, Case 2: x < 0

- *If two cases are clearly identical, can just show one*

Theorem:
if xy and x + y are even, then x and y are both even

Proof:
Suppose x and y are not both even
Without loss of generality, assume x is odd
Case 1: y is even
Then x+y = 2k+1 + 2k' = 2(k+k') + 1 is odd
Case 2: y is odd
Then xy = (2k+1)(2k'+1) = 2(2kk' + k + k') + 1 is odd

"other case follows identically"

Constructive vs non-constructive proofs

- *Want to prove the existential statement $\exists x\, P(x)$.*
- *Direct method involves finding a witness c such that P(c) is true.*

  e.g. Prove that there exists a red car…

  My car is red!

- *Non-constructive proofs do not find an explicit c. How?*
- *One method: proof by contradiction*

$$\frac{\neg\, \exists x\, P(x) \rightarrow F}{\therefore\ \exists x\, P(x)} \qquad \frac{\forall x \neg\, P(x) \rightarrow F}{\therefore\ \exists x\, P(x)}$$

Example

- *Theorem:*

  There exist irrational numbers x, y such that x^y is rational

- *Proof:*

  Suppose instead that for all irrational x, y, x^y is irrational

  Consider the number $\sqrt{2}^{\sqrt{2}}$. Either it is rational or irrational

  Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational

  Then since $x=y=\sqrt{2}$ is irrational we have a contradiction

  Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational

  Then $x=\sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ are both irrational

  But $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$ is rational

  Hence we have a contradiction.

Q.E.D.

Summary

- *Proofs are logical arguments*
- *A valid proof must use valid logical inferences*
- *Knowing which statements are logically equivalent and valid rules of inferences gives access to a wide array of valid proofs*
- *If it doubt, write it out! (in symbolic, explicit form)*

Practice

Exercises from the Book:

7th edition: 3, 9, 15, 17 (page 91)

8th edition: 3, 9, 17, 19 (page 95)