Intro to Discrete Structures
Lecture 8

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

wocjan@eecs.ucf.edu

Proof Strategy

- We have seen two important methods for proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$.

  These two methods are

  - the direct proof and
  - the indirect proof

  methods.

- It takes some practice (solving homework problems) to learn to recognize quickly the correct approach.
- Try first the direct approach. If it does not work then try the indirect approach.

Direct or Indirect Proof?

Definition: The real number r is **rational** if there exist integers p and q with $q \neq 0$ such that $r = p/q$.

Example 7: Prove that the sum of two rational numbers is rational.

$$r = \frac{p}{q} \qquad \tilde{r} = \frac{\tilde{p}}{\tilde{q}}$$

$$r + \tilde{r} = \frac{p}{q} + \frac{\tilde{p}}{\tilde{q}} = \frac{p\tilde{q} + \tilde{p}q}{q\tilde{q}}$$

direct proof

Direct or Indirect Proof?

p

Example 8: Prove that if n is an integer and n^2 is odd, then

q n is odd.

$$p \to q \equiv \underbrace{\neg q \to \neg p}_{\text{means}}$$

If n is even, then n^2 is even.

$$n = 2k \qquad n^2 = (2k) = 4k^2 = 2 \cdot 2k^2$$

Proof by Contradiction I

- Suppose we want to prove that p is true.
- Furthermore, suppose that we can find a contradiction q such that

$$\neg p \rightarrow q$$

  is true.
- Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

Proof by Contradiction II

- The statement

$$(r \wedge \neg r)$$

  is a contradiction whenever r is a proposition.

- Therefore, we can prove that p is true if we can show that

$$\neg p \longrightarrow (r \wedge \neg r)$$

  is true for some proposition r.

Proof by Contradiction III

Example 9: Show that at least four of any 22 days must fall on the same day of the week.

Proof by Contradiction IV

- p : At least four of 22 days chosen fall on the same day of the week.
- Suppose $\neg p$ is true.
- This means that at most three days of the 22 days fall on the same day.
- This implies that at most 21 days could have been chosen.
- This contradicts the hypothesis that we have 22 days under consideration.
- r : 22 days are chosen.

$$\neg p \rightarrow (r \wedge \neg r)$$

$\sqrt{2}$ is irrational

$p: \sqrt{2}$ irrational $\quad \neg p: \sqrt{2}$ rational

$\sqrt{2} = \frac{a}{b}$ with a, b are integers having no common factors $[\gcd(a,b) = 1]$

$2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow a^2$ even

$\Rightarrow$ a even $\Rightarrow a = 2c$

$\Rightarrow 2b^2 = (2c)^2 = 4c^2$

$\Rightarrow b^2 = 2c^2 \Rightarrow$ b is even

$\sqrt{2}$ is irrational

Reading Assignment

- Examples 11 – 14
- Subsection “Mistakes in Proofs”

Exhaustive Proof

Prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq \cancel{4}\ 2$.

$(1+1)^2 = 2^2 = 4 \geq 3^1 = 3$ ✓

$(2+1)^2 = 3^2 = 9 \geq 3^2 = 9$

$4^2 = 16 \qquad 3^3 = 27$

$n = 3 \qquad (n+1)^3$

Proof by Cases

Based on the logical equivalence

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$$

$\equiv \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q$

$\equiv \neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q$

$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q)$

$\equiv$

Proof by Cases

Example 3: Prove that if n is an integer, then $n^2 \geq n$.

n negative $-1, -2, -3, \ldots$

$n = 0$

n positive $+1, +2, +3, \ldots$

Proof by Cases

Example 4: Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers.

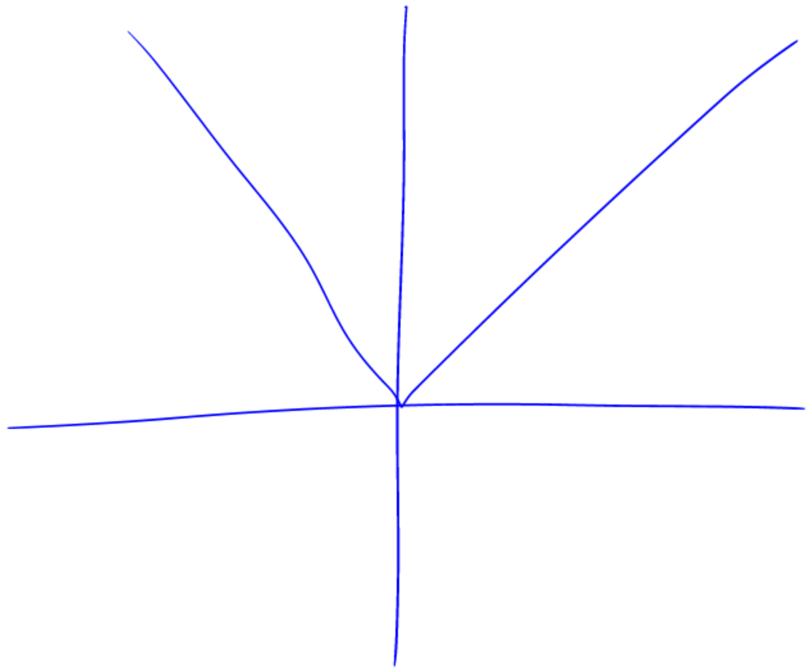
(i) $x < 0 \wedge y < 0$

(ii) $x > 0 \wedge y < 0$

(iii) $x < 0 \wedge y > 0$

(iv) $x > 0 \wedge y > 0$

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{otherwise} \end{cases}$$



Proof by Cases

Example 5: Formulate a conjecture about the decimal digits that occur as the final digit of the square of an integer and prove your result.

$11^2 = 121$

$19^2 = 361$

$12^2 = 144$

$18^2 = 324$

$(10 \cdot x + y) = 100x^2 + 10 \cdot 2xy + y^2$

$21^2 = 441$

$39^2 = 1521$

$0 - 0$

$1, 9 \to 1$

$3, 7 \to 9$

$2, 8 \to 4$

$4, 6 \to 6$

$5 - 5$

Existence Proofs

- Many theorems are assertions that objects of a particular type exist.
- A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate.
- A proof of a proposition of the form $\exists x P(x)$ is called **existence proof**.

Constructive vs. Nonconstructive

- Constructive Existence Proof:
  - Sometimes an existence proof can be given by finding a concrete element a such that $P(a)$ is T.
- Nonconstructive Existence Proof:
  - We do not find an element a such that $P(a)$ is T, but rather prove that $\exists x P(x)$ is true in some other way.
  - One common method of give a nonconstructive proof is to use proof by contradiction and show the negation of the existential quantifier implies a contradiction.

A Constructive Existence Proof

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

A Constructive Existence Proof

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
- Solution: After considerable computation (such as computer search) we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \,.$$

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

Nonconstructive Existence Proof

- Show that there exist irrational numbers x and y such that x^y is rational.

$$a^3 = a \cdot a \cdot a \qquad a^{-3} = \frac{1}{a^3}$$

$$a^{\frac{1}{3}} = \sqrt[3]{a} \qquad a^{-\frac{1}{3}} = \frac{1}{\sqrt[3]{a}}$$

$$a^{\frac{m}{n}} = \sqrt[n]{a^m}$$

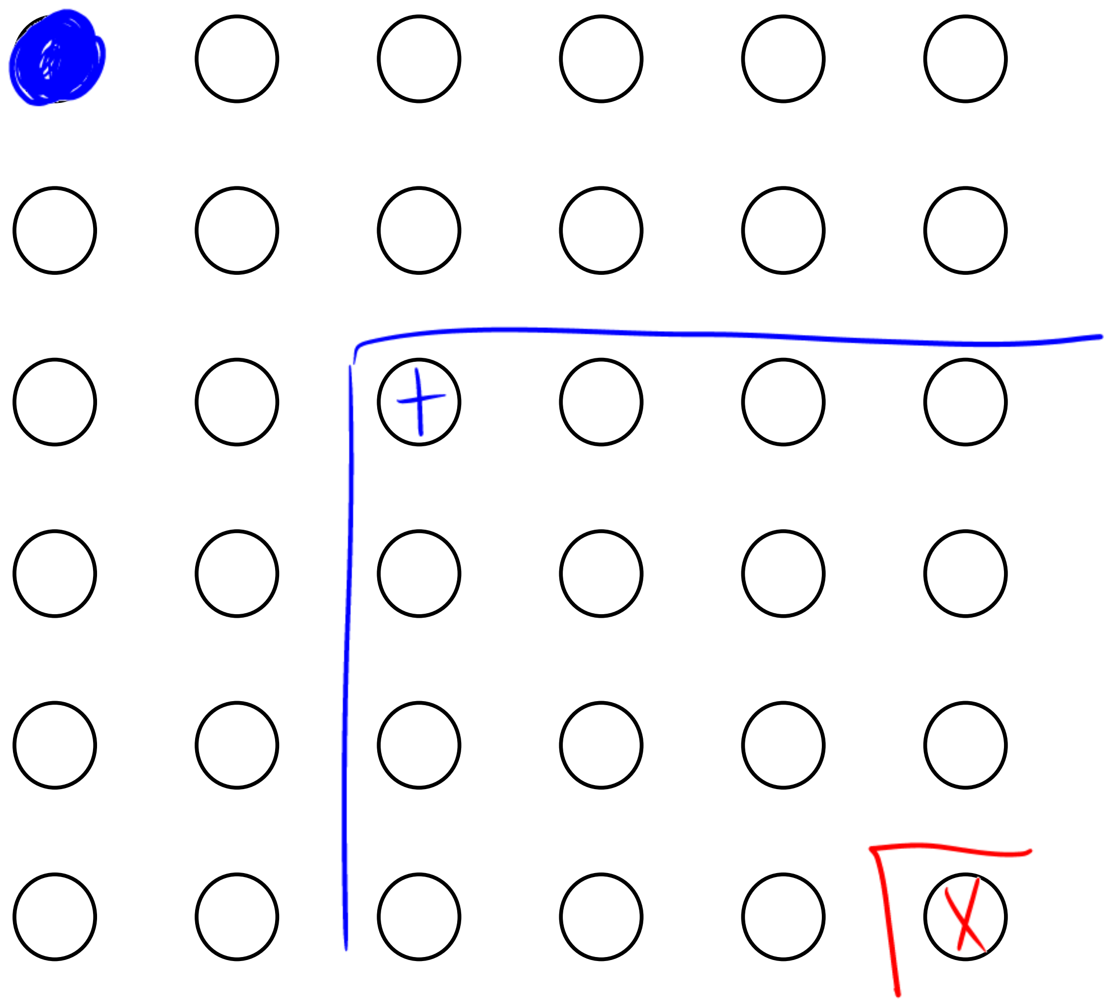
$$a^{\sqrt{2}}$$

Nonconstructive Existence Proof

- Show that there exist irrational numbers x and y such that x^y is rational.
- Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.
  - If $\sqrt{2}^{\sqrt{2}}$ is rational, we have two irrational numbers x and y with x^y rational, namely, $x = \sqrt{2}$ and $y = \sqrt{2}$.
  - On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2\,.$$

Chomp



Uniqueness Proof

- Some theorems assert the existence of a unique element with a particular property.
- The two parts of **uniqueness proof** are:
  - Existence: We show that there is an element x with the desired property.
  - Uniqueness: We show that if $y \neq x$, then y does not have the desired property.
- This is the same as showing that

$$\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$$

is true.

Uniqueness Proof

Example 13: Show that if a and b are real numbers and $a \neq 0$, then there exists a unique real number r such that $ar + b = 0$.

Reading Assignment + Lab

- Read pages 93 – end of Chapter 1 on your own.
- The teaching assistants will go over material relevant to proofs during the lab sections.
- Proof strategies etc. are relevant for homework 2 (to be posted soon).