CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

Zoom is needed for today

This week

- Some common mistakes in proof
- Some other proof tech
- SBU exam exercises
- Organizing thoughts into clear writings
- Ungraded homework as a mock exam this Thursday

Midterm 1 Reminder

- Thursday Oct 26 12:30 - 13:50 @B207

- Format: Unlimited notes. In-person. Submit (1) a physical copy to instructor and (2) an e-version on BrightSpace.

- Covered topics: Everything we will have learned by then

Review Exercise 1: Disproof

- Prove if it is true, or disprove if not:
  - For all real number x, if x>0 then $x^2 \geq x$

Review Exercise 2
(a tricky one from last lecture)

- Every odd number can be written as the sum of three odd numbers

Some common mistakes in proof

Mistake 1

Theorem: For all integers k, if $k > 0$ then $k^2 + 2k + 1$ is composite.

“**Proof:** For $k = 2$, $k^2 + 2k + 1 = 2^2 + 2 \cdot 2 + 1 = 9$. But $9 = 3 \cdot 3$, and so 9 is composite. Hence the theorem is true.”

Do not prove a universal statement with a single case

Mistake 2

Theorem: The difference between any odd integer and any even integer is odd.

"**Proof:** Suppose n is any odd integer, and m is any even integer. By definition of odd, $n = 2k + 1$ where k is an integer, and by definition of even, $m = 2k$ where k is an integer. Then

$$n - m = (2k + 1) - 2k = 1.$$

But 1 is odd. Therefore, the difference between any odd integer and any even integer is odd."

Do not use the same "k" coming from two different "there exists k…"

Mistake 3

$\forall$ a and b $\in \mathbb{Z}$, If ab is even, then a is even or b is even

$\exists$ a, b $\in \mathbb{Z}$, ab is even and a, b are odd

$ab = 2K$, $K \in \mathbb{Z}$.

$a = \frac{2K}{b} = 2\left(\frac{K}{b}\right)$ even

$b = 2\frac{K}{a} = 2\left(\frac{K}{a}\right)$ even.

$\neq$

$\therefore$ QED

b is even if b = 2*k for an integer k. Note “k” must be an integer

Mistake 4

- True or false: For any nonnegative integer n, n^2+3n+2 is a composite
- n^2+3n+2= (n+1)(n+2) therefore composite

c is a composite if c = a*b where a!=1 and b!=1. Note the “!=1” parts

Some other mistakes (recitation)

- Confusing assumption, facts, and proof objective
- Missing assumption
- Confusing proof by contradiction and disproof
- Wrong contraposition
- Wrong negation in proof by contradiction

Some other proof tech.

If-and-only-if

- Prove: The integer n is odd if and only if n^2 is odd.
- To prove A if and only if B, first prove A -> B, then prove B ->A

Solution

Proposition The integer n is odd if and only if n^2 is odd.

Proof. First we show that n being odd implies that n^2 is odd. Suppose n is odd. Then, by definition of an odd number, $n = 2a+1$ for some integer a. Thus $n^2 = (2a+1)^2 = 4a^2+4a+1 = 2(2a^2+2a)+1$. This expresses n^2 as twice an integer, plus 1, so n^2 is odd.

Conversely, we need to prove that n^2 being odd implies that n is odd. We use contrapositive proof. Suppose n is not odd. Then n is even, so $n = 2a$ for some integer a (by definition of an even number). Thus $n^2 = (2a)^2 = 2(2a^2)$, so n^2 is even because it's twice an integer. Thus n^2 is not odd. We've now proved that if n is not odd, then n^2 is not odd, and this is a contrapositive proof that if n^2 is odd then n is odd. ■

Equivalent statements

Theorem Suppose A is an $n \times n$ matrix. The following statements are equivalent:

(a) The matrix A is invertible.
(b) The equation $A\mathbf{x} = \mathbf{b}$ has a unique solution for every $\mathbf{b} \in \mathbb{R}^n$.
(c) The equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution.
(d) The reduced row echelon form of A is I_n.
(e) $\det(A) \neq 0$.
(f) The matrix A does not have 0 as an eigenvalue.

(How to actually prove this in details is not a part of our lecture)

$$\begin{array}{ccccc} (a) & \Longrightarrow & (b) & \Longrightarrow & (c) \\ \Uparrow & & & & \Downarrow \\ (f) & \Longleftarrow & (e) & \Longleftarrow & (d) \end{array}$$

$$\begin{array}{ccccc} (a) & \Longrightarrow & (b) & \Longleftrightarrow & (c) \\ \Uparrow & & \Downarrow & & \\ (f) & \Longleftarrow & (e) & \Longleftrightarrow & (d) \end{array}$$

$$\begin{array}{ccccc} (a) & \Longleftrightarrow & (b) & \Longleftrightarrow & (c) \\ & & \Updownarrow & & \\ (f) & \Longleftrightarrow & (e) & \Longleftrightarrow & (d) \end{array}$$

Uniqueness Proof

- Prove: there is a unique function f defined over R such that $f'(x)=2x$ and $f(0)=3$
- To prove there is a unique x such that P(x):
    - first prove there exist an x,
    - then prove “x and y both satisfy P, then $x = y$”

Solution

Proof. *Existence*: $f(x) = x^2 + 3$ works.

Uniqueness: If $f_0(x)$ and $f_1(x)$ both satisfy these conditions, then $f_0'(x) = 2x = f_1'(x)$, so they differ by a constant, i.e., there is a C such that $f_0(x) = f_1(x) + C$. Hence, $3 = f_0(0) = f_1(0) + C = 3 + C$. This gives $C = 0$ and so $f_0(x) = f_1(x)$. ∎