CSE215
Foundations of Computer Science

State University of New York, Korea

Instructor: Zhoulai Fu

- Today:
  - Proof by contradiction
  - Proof by contraposition
- Reminder: Zoom
- Midterm to be scheduled after the Proof part finishes

Contradiction

Proof by contradiction

You are asked to prove P and you feel ~P is ridicules

Prove: There is no greatest integer

- Proof.
    - We use proof by contradiction.
    - Assume there exists a greatest integer.
    - Let n denote the greatest integer. We have
        - (A): for any integer m, m <=n.
    - But n + 1 > n which contradicts with (a)
    - Therefore, there does not exist a greatest integer
- QED.

$\sqrt{2}$ is irrational

- Proof.
  - We use proof by contradiction.
  - Assume sqrt(2) is a rational number, namely:
    - (A) there exists two integers m, n such that sqrt(2)=m/n, and m and n have no common factors.
  - Thus m^2 = 2 n^2. Thus, m^2 is even. Thus m must be even (otherwise m^2 becomes odd).
  - Thus m = 2k for some integer k. Thus, n ^2= 2 k^2. Thus n^2 is even and therefore n must be even.
  - But the fact that m and n are both even contradicts with (A)
  - Therefore sqrt(2) must be irrational.
- QED.

Prove: For any prime number p and natural number n,

If $p|n$, then $p \nmid (n+1)$.

- Proof.
    - We use proof by contradiction
    - Assume:
        - (A) there exists a prime p and a natural number n, such that $p \mid n$ and $p \mid (n+1)$
    - Since $p \mid n$, $n = pk$ for some integer k
    - Since $p \mid (n+1)$, $n+1=pk'$ for some integer k'
    - Thus $1 = p (k' - k)$. Thus $p = 1$ which contradicts with the fact p is a prime.
    - Therefore (A) is false
- QED

Summary so far

- To prove P is true, we can prove ~P -> False
- So, we assume ~P and try to derive a contradiction

Proof by contraposition

You are asked to prove P -> Q and you feel ~Q -> ~P is easier to prove

n^2 is even $\implies$ n is even

Proposition

- For all integers n, if n^2 is even, then n is even.

Idea:
proof by contraposition

- Proposition, for all integer n, n^2 even -> n even
- Equivalently, for all integer n, n is odd -> n^2 is odd

Solution1 — proof by contraposition

- Proof.
  - We use proof by contraposition
  - We want to prove: for any integer n, n is odd -> n^2 is odd.
  - Let n be an arbitrary integer.
  - Suppose n is odd
  - ….
  - Therefore n^2 is odd
- QED

Solution2 — proof by contradiction

- Proof.
  - We use proof by contradiction
  - Assume:
    - (A) there exists integer n, such that n^2 is even and n is odd
  - Since n is odd, n=2k+1 for some k
  - Then n^2 = 2 (2k^2+2k)+1 is odd, which contradicts with (A)
  - Therefore (A) is false
- QED

Break

Exercises

Exercise 1

If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

- Proof.
  - Suppose a and b are two integers.
  - Suppose, for the sake of contradiction, that $a^2 - 4b -3 = 0$
  - Thus $a^2 = 4b + 3 = 2 (2b + 1) + 1$. Thus a is an odd number. We can write a as $2c+1$ for some integer c
  - Thus $(2c+1)^2 = 4b + 3$
  - Namely, $4c^2+4c+1 = 4b + 3$. We have $2(c^2 + c)=2b+1$
  - Left-hand-side is even, whereas right-hand-side is odd. Contradiction.
- QED.

Exercise 2: Prove the following

Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.

- Proof.
  - Proof by contraposition
  - We only need to prove $x>=0$ -> $x^2+5x>=0$
    - Suppose $x>=0$
    - …
    - Thus $x^2+5x>=0$
- QED.

Exercise 3: Prove the following

Suppose $x \in \mathbb{R}$. If $x^3 - x > 0$ then $x > -1$.

- Proof.
  - Proof by contraposition.
  - We will prove $x<=-1 \ -> \ x^3-x <=0$
    - Suppose $x<=-1$
    - …
    - Thus $x^3-x<=0$
- QED.

Exercise 4

Prove . If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Proof. Suppose this proposition is *false*.
This conditional statement being false means there exist numbers a and b for which $a, b \in \mathbb{Z}$ is true, but $a^2 - 4b \neq 2$ is false.
In other words, there exist integers $a, b \in \mathbb{Z}$ for which $\boxed{a^2 - 4b = 2.}$
From this equation we get $a^2 = 4b + 2 = 2(2b+1)$, so a^2 is even.
Because a^2 is even, it follows that a is even, so $a = 2c$ for some integer c.
Now plug $a = 2c$ back into the boxed equation to get $(2c)^2 - 4b = 2$, so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.
Therefore $1 = 2(c^2 - b)$, and because $c^2 - b \in \mathbb{Z}$, it follows that 1 is even.
We know 1 is **not** even, so something went wrong.
But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true. ■

That is all for today

- proof by contradiction
- Proof by contraposition

Thank you!