CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

September 20, 2022

Outline

- Review exercises with Direct proof.
- Proof by contradiction
- Very much appreciated questions during previous classes

Review: Direct Proof

Review exercise 1

Prove 2^999+1 is composite

Review exercise 1

Prove $2^{999}+1$ is composite

- Proof.

  - $2^{999}+1$
    $= (2^{333})^3 + 1^3$
    $= (2^{333}+1) * (2^{666}-2^{333}+1)$

- QED.

Review exercise 2

Prove: For any natural number n, $n^2 + 3n + 2$ is composite

Review exercise 2

Prove: For any natural number n, n^2 + 3n + 2 is composite

- Proof.
  - Suppose n is an arbitrary integer.
  - n^2 + 3n + 2 can be written as (n+1)*(n+2)
  - Thus, n^2 + 3n + 2 is a composite number
- QED.

Review exercise 3

For any integer x, y, if x is even, then xy is even.

Review exercise 3

For any integer x, y, if x is even, then xy is even.

Proof. Suppose $x, y \in \mathbb{Z}$ and x is even.
Then $x = 2a$ for some integer a, by definition of an even number.
Thus $xy = (2a)(y) = 2(ay)$.
Therefore $xy = 2b$ where b is the integer ay, so xy is even. ■

Review exercise 4

Prove: there exist two irrational number r1, r2, such that r1*r2 is a rational number.

Review exercise 4

Prove: there exist two irrational number r1, r2, such that r1*r2 is a rational number.

- Proof.
    - Let r1 and r2 be square root of 2.
    - r1 and r2 are irrational, and r1*r2 is rational.
- QED.

Review exercise 5

Prove: Suppose a is an integer. If $7|4a$, then $7|a$.

Review exercise 5

Prove: Suppose a is an integer. If $7|4a$, then $7|a$.

Proof. Suppose $7 \mid 4a$.
By definition of divisibility, this means $4a = 7c$ for some integer c.
Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.
But then c can't be odd, because that would make $7c$ odd, not even.
Thus c is even, so $c = 2d$ for some integer d.
Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.
Dividing both sides by 2 gives $2a = 7d$.
Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.
Then d is even, so $d = 2e$ for some integer e.
Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.
Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.
Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. ■

Summary for Direct proof

- “If A, then B” ==> Suppose A, … Therefore B.
- “for all real number x, P(x)” ==> Suppose x is real, … Therefore P(x).
- To prove there exist x, P(x) ==> We have P(x) for x = …

Proof by Contradiction

Prove: There is no greatest integer

Prove: There is no greatest integer

- Proof.
  - We use proof by contradiction.
  - Assume there exists a greatest integer n.
  - Namely, any integer m, m <=n
  - But n+1 > n which contradicts with our hypothesis above
  - Thus, there does not exist a greatest integer
- QED.

$\sqrt{2}$ is irrational

$\sqrt{2}$ is irrational

- Proof.
  - We use proof by contradiction.
  - Assume sqrt(2) is a rational number.
  - Namely, 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 the assumption that m and n has no common factors.
  - Thus, our hypothesis above is tase, We conclude sqrt(2) must be irrational.
- QED.

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

Proposition

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

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

Proposition

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

Proof

- Negation. Suppose there is an integer n such that n^2 is even but n is odd.
- $n = 2k + 1$ (definition of odd number)
  $\implies n^2 = (2k+1)^2$ (squaring both sides)
  $\implies n^2 = 4k^2 + 4k + 1$ (expand)
  $\implies n^2 = 2(2k^2 + 2k) + 1$ (taking 2 out from two terms)
  $\implies n^2 = 2m + 1$ (set $m = 2k^2 + 2k$)
  (m is an integer as multiplication is closed on integers)
  $\implies n^2 = \text{odd}$ (definition of odd number)
- Contradiction! Hence, the proposition is true.

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

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

Proposition

- For any integer n and any prime p, if $p|n$, then $p \nmid (n+1)$.

Proof

- Negation. Suppose there exists integer n and prime p such that $p|n$ and $p|(n+1)$.
  $p|n$ implies $pr = n$ for some integer r
  $p|(n+1)$ implies $ps = n+1$ for some integer s
  Eliminate n to get:
  $1 = (n+1) - n = ps - pr = p(s-r)$
  Hence, $p|1$, from the definition of divisibility.
  As $p|1$, we have $p \leq 1$.
  As p is prime, $p > 1$.
  Contradiction! Hence, the proposition is true.

Break if time allows

A special kind of proof by contradiction - proof by contraposition

Exercises

To finish by 1h50pm

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

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

- Proof.
    - We want to prove,
        - for all integer n, n^2 even $\rightarrow$ n even
    - Equivalently, we only need to prove the contraposition:
        - for all integer n, n is odd $\rightarrow$ n^2 is odd
        - Suppose n is an arbitrary integer and n is odd.
        - Then $n = 2k + 1$ for some integer k.
        - Thus, $n^2 = 4k^2 + 4k + 1 = 2(2k^2+2k)+1$ which is odd
- QED.

Exercise 1: Prove the following

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

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

Exercise 1: Prove the following

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

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

- We only need to prove x>=0 -> x^2+5x>=0
  - Suppose x>=0
  - …
  - Thus x^2+5x>=0
- We only need to prove x<=-1 -> x^3-x <=0
  - Suppose x<=-1
  - …
  - Thus x^3-x<=0

Exercise 2

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

Exercise 2

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.

That is all for today

- Direct proof
- proof by contradiction
- Proof by contraposition
- Practice, practice, and practice

Thank you!