CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

Today

- A missing exercise
- Definitions and facts about numbers
- Direct proof

* Exercise 5

Determine if the following argument is valid:

p ↔ q
q ⊕ r
———
∴ p \/ r

Solution

- It is valid.
- Assume the premises are true.
- Namely, p<->q is true and q xor r is true.
- Since p <->q is true, we know p and q must be the same truth value.
- Since q xor r is true, we know q and r must be different truth values.
- Thus, p and r must be different truth values.
- Thus p and r can be either (true and false), or (false and true)
- Thus q ∨ r, namely, the conclusion, is true.

Definitions and facts about numbers

Symbols

- Integers Z
- Natural numbers N
- Real numbers R

- | x |
- sum Σ
- a | b
- b mod a

Formal definitions

- Even/Odd numbers
- Rational/Irrational numbers
- Prime/Composite numbers

Even/odd numbers

We say an integer n is even if: $\exists k \in \mathbf{Z}$ such that $n = 2k$

How can you define an odd number?

Rational/Irrational numbers

We say a real number r is rational if $\exists m, n \in \mathbf{Z}$ such that $r = n/m$.

(and n and m have no common divisor).

Prime/Composite numbers

We say a natural number n is prime if $n > 1$, and

$$\forall r, s \in \mathbf{N}, n = rs \to (r = 1 \vee s = 1)$$

d | n

We say a non-zero integer d divides an integer n, if

$$\exists k \in \mathbf{Z}, \text{ such that } n = k * d.$$

Direct proof

Methods of mathematical proof

Statements	Method of proof
Proving existential statements	Constructive proof
(Disproving universal statements)	Non-constructive proof
Proving universal statements	Direct proof
(Disproving existential statements)	Proof by mathematical induction
	Well-ordering principle
	Proof by exhaustion
	Proof by cases
	Proof by contradiction

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

- Proof.
    - Suppose n is an even number, and m is an odd number, we need to show n+m is odd
        - since n is an even number, n = 2k for some integer k
        - since m is an odd number, m = 2k’+1 for some integer k’
        - Thus n+m = 2(k+k’)+1 which shows n+m is odd.
- QED.

n is odd $\Rightarrow$ n^2 is odd

Proposition

- The square of an odd integer is odd.

- Proof.
    - Suppose n is an odd number. We want to show that n^2 is an odd number.
        - Since n is odd, n = 2k+1 for some integer k
        - $n^2 = 4k^2+4k+1= 2(2k^2+2k) + 1$
        - Thus n^2 is odd
- QED.

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers

Workout

- Write a formal statement.
  $\forall$ integer k, $\exists$ integers m, n such that
  $(2k+1) = m^2 - n^2$.
- Try out a few examples.

$$1 = 1^2 - 0^2 \qquad -1 = 0^2 - (-1)^2$$
$$3 = 2^2 - 1^2 \qquad -3 = (-1)^2 - (-2)^2$$
$$5 = 3^2 - 2^2 \qquad -5 = (-2)^2 - (-3)^2$$
$$7 = 4^2 - 3^2 \qquad -7 = (-3)^2 - (-4)^2$$

- Find a pattern.
  $(k+1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 =$ odd

- Proof.
  - Suppose x is an odd number, we need to show:
    - There exists two integers m and n such that x = m^2 - n^2
  - Since x is odd, we can write x = 2k+1 for some integer k
  - Let m = k+1, and n = k. Then, we have m^2 - n^2 = 2k+1 = x
- QED.

If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

- Proof.
  - Suppose a, b, c are three integers and a|b, b|c.
  - Since a|b, we have b = ak for some integer k
    - Since b|c, we have c = bk’ for some integer k’
    - Thus, c = a (k*k’)
    - Thus a|c.
- QED.

Summation

Proposition

- $1 + 2 + 3 + \cdots + n = n(n+1)/2.$

That is all for today

- Proof techniques — direct proof. **Commonly used for proving “for all x, P(x) -> Q(x)”.**

Thank you!