Indirect Argument

CS 231

Dianna Xu

1

Proof by Contraposition

- Consider an implication: $p \rightarrow q$
  - Its contrapositive is $\sim q \rightarrow \sim p$
  - If the antecedent ($\sim q$) is false, then the contrapositive is always true
  - Thus, show that if $\sim q$ is true, then $\sim p$ is true
- To perform a proof by contraposition, do a direct proof on the contrapositive

2

Indirect proof example

- If n^2 is an odd integer then n is an odd integer
- Prove the contrapositive: If n is an even integer, then n^2 is an even integer
- Proof:
  - $\exists\, k \in Z,\ n=2k$
  - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
  - $2k^2 \in Z$
  - n^2 is even ■

3

Which to use

- When do you use a direct proof versus an indirect proof?
- If it's not clear from the problem, try direct first, then indirect second
  - If indirect fails, try the other proofs

4

Direct versus Indirect

- Prove that if n is an integer and n^3+5 is odd, then n is even
- Via direct proof
  - $\exists\, k \in Z,\ n^3+5 = 2k+1$ (definition of odd numbers)
  - $n^3 = 2k-4$
  - $n = \sqrt[3]{2k-4}$
  - Umm…
- So direct proof didn't work out. Next up: indirect proof

5

Direct versus Indirect

- Prove that if n is an integer and n^3+5 is odd, then n is even
- Via indirect proof
  - Contrapositive: If n is odd, then n^3+5 is even
  - $\exists\, k \in Z,\ n=2k+1$ (definition of odd numbers)
  - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
  - $(4k^3+6k^2+3k+3) \in Z$
  - n^3+5 is even ■

6

Proof by Contradiction

- Given a statement p, assume it is false
  - Assume $\sim p$
- Prove that $\sim p$ cannot occur
  - $\sim p \rightarrow \mathbf{c}$
  - A contradiction exists
- Given a statement of the form $p \rightarrow q$
  - To assume it's false, you only have to consider the case where p is true and q is false

7

Example

- For any integer a and any prime p, if $p|a$ then $p \nmid (a+1)$
- Proof:
  - Assume $p|a$ and $p|(a+1)$
  - $\exists\, r,s \in \mathcal{Z}$, $a = rp$ and $a+1 = sp$
  - $1 = sp\text{-}a = sp\text{-}rp = (s\text{-}r)p$
  - $s\text{-}r \in \mathcal{Z} \wedge 1 = (s\text{-}r)p \rightarrow p \mid 1$
  - $p|1 \wedge p$ is prime
  - Contradiction ■

8

Contradiction and Contraposition

- $\forall x \in$ D, P(x)→Q(x)
- Contraposition: prove by giving a direct proof for $\forall x \in$ D, ~Q(x)→~P(x)
  - Suppose x is an arbitrary element of D, such that ~Q(x)
  - Prove ~P(x)
- Contradiction:
  - Suppose $\exists\, x \in$ D such that P(x) $\wedge$ ~Q(x)
  - Prove for a contradiction

9

The Infinitude of Primes

- Theorem (by Euclid): There are infinitely many prime numbers.
- Proof
  - Assume there are a finite number of primes p_1, p_2 …, p_n.
  - Consider the number $q = p_1 p_2 \ldots p_n + 1$
  - This number is not divisible by any of the listed primes
    - If we divided p_i into q, it would result in a remainder of 1
  - We must conclude that q is a prime number, and q is not among the primes listed above.
  - Contradiction ■

10

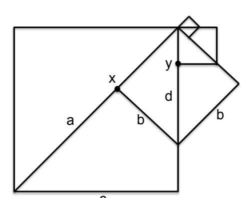
The Irrationality of √2

- Theorem: √2 is irrational
- Proof
  - Assume √2 is rational
  - $\exists\, r \in \mathcal{Q}$, $r^2 = 2$
  - $\exists\, a,b \in \mathcal{Z}$, $(a/b)^2 = 2$ and a, b have no common factors
  - $a^2/b^2 = 2$
  - $a^2 = 2b^2$ (implies a^2 is even and hence a is even)
  - $a^2 = (2k)^2 = 4k^2 = 2b^2$
  - $2k^2 = b^2$ (implies b^2 is even and hence b is even)
  - a and b are both even, and have the common factor 2
  - Contradiction ■

11

√2 and the Infinite Descent

- Eudoxus ladder $\sqrt{2} = \lim_{n\to\infty} \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ldots}}}$



12