Indirect Argument

CS 231
Dianna Xu

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

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:
  – \( \exists k \in \mathbb{Z} \), \( n = 2k \)
  – \( n^2 = (2k)^2 = 4k^2 = 2(2k^2) \)
  – \( 2k^2 \in \mathbb{Z} \)
  – \( n^2 \) is even ■

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

Direct versus Indirect

• Prove that if \( n \) is an integer and \( n^3 + 5 \) is
odd, then \( n \) is even
• Via direct proof
  – \( \exists k \in \mathbb{Z} \), \( n^3 + 5 = 2k + 1 \) (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

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
  – \( \exists k \in \mathbb{Z} \), \( n = 2k + 1 \) (definition of odd numbers)
  – \( n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 6 =
  \quad 2(4k^3 + 6k^2 + 3k + 3) \)
  – \( (4k^3 + 6k^2 + 3k + 3) \in \mathbb{Z} \)
  – \( n^3 + 5 \) is even ■
Proof by Contradiction

• Given a statement \( p \), assume it is false
  – Assume \( \sim p \)
• Prove that \( \sim p \) cannot occur
  – \( \sim p \rightarrow c \)
  – 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

Example

• For any integer \( a \) and any prime \( p \), if \( p | a \) then \( p | (a+1) \)
• Proof:
  – Assume \( p | a \) and \( p | (a+1) \)
  – \( \exists r, s \in \mathbb{Z}, a = rp \) and \( a+1 = sp \)
  – \( 1 = sp-a = sp-rp = (s-r)p \)
  – \( s-r \in \mathbb{Z} \land 1 = (s-r)p \rightarrow p | 1 \)
  – \( p | 1 \) and \( p \) is prime
  – Contradiction □

Contradiction and Contraposition

• \( \forall x \in D, P(x) \rightarrow Q(x) \)
• Contraposition: prove by giving a direct proof for \( \forall x \in D, \sim Q(x) \rightarrow \sim P(x) \)
  – Suppose \( x \) is an arbitrary element of \( D \), such that \( \sim Q(x) \)
  – Prove \( \sim P(x) \)
• Contradiction:
  – Suppose \( \exists x \in D \) such that \( P(x) \land \sim Q(x) \)
  – Prove for a contradiction

The Infinitude of Primes

• Theorem (by Euclid): There are infinitely many prime numbers.
• Proof
  – Assume there are a finite number of primes \( p_1, p_2, \ldots, p_n \).
  – Consider the number \( q = p_1p_2 \ldots p_n + 1 \)
  – This number is not divisible by any of the listed primes
  – If we divided \( q \) 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 □

The Irrationality of \( \sqrt{2} \)

• Theorem: \( \sqrt{2} \) is irrational
• Proof
  – Assume \( \sqrt{2} \) is rational
  – \( \exists r \in \mathbb{Q}, r^2 = 2 \)
  – \( \exists a, b \in \mathbb{Z}, (a/b)^2 = 2 \) 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)
  – \( a^2 = (2k)^2 = 4k^2 = 2b^2 \)
  – \( 2b^2 = b^2 \) (implies \( b^2 \) is even, and hence \( b \) is even)
  – \( a \) and \( b \) are both even, and have the common factor 2
  – Contradiction □

\( \sqrt{2} \) and the Infinite Descent

• Eudoxus ladder \( \sqrt{2} = \lim_{n \to \infty} \frac{1}{\frac{1}{2+\frac{1}{2+\frac{1}{2+\ldots}}}} \)