Discrete Mathematics

Proof

Shin Hong

Proof

- A **theorem** is an important proposition that can be shown true
  - a theorem (or fact) is a proposition that is true
  - a lemma is a less important proposition that is true (usullay a part of a theorem)
  - a corollary is a theorem directly established from a main theorem

- A **proof** is a valid argument that establishes the truth of a theorem
  - a proof includes axioms (postulates) which are statement known, assumed, or believed to be true
  - a proof include a conclusion from valid assertions by a valid inference rule
  - a proof can include proven theorems
  - a proof can include premises

- A **conjecture** is a statement proposed to be true (yet) without a proof

Proving Methods

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Exhaustive proof
- Existence proof

Direct Proofs

- A direct proof of $p \rightarrow q$ is constructed as follows:
  - first step is the assumption that p is true
  - subsequent steps are constructed by rules of inferences
  - final step shows that q is true under the assumption

- Example: prove that n^2 is odd if n is an odd integer

1.	x is odd iff there is a positive integer y s.t. x=2y -1	theorem
2.	n is odd	premise
3.	there is a positive integer m s.t. n = 2m - 1	MP 1L,2
4.	$n^2 = (2m-1)^2 = 4m^2 - 4m + 1$	arithem.
5.	$n^2 = 2(2m^2 - 2m) + 1$	arithem.
6.	n^2 is odd	MP 1R,5

Proof by Contraposition

- Use the fact that $p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$

- Example: prove that an integer n is odd if $3n$+2 is odd
  = if n is not an odd integer, then $3n$+2 is not odd (CP)

1.	an integer is not odd iff the integer is even	theorem
2.	*n* is not an odd integer	premise
3.	*n* is even	MP 2,1
4.	if *x* is even, there is an integer y s.t. *x* = 2*y*	theorem
5.	there is an integer m s.t. n = 2m	MP 3, 4
6.	3n+2 = 3(2m) + 2 = 2(3m + 1)	arithm.
7.	if there is an integer y s.t. x = 2y, x is even	theorem
8.	3n+2 is even	MP 6,7

Proof by Contradiction

- Proving p by contradiction
  1. show that $\neg p \rightarrow q$ is true for a statement q
  2. show that q is not true (i.e., unsatisfiable or contradiction)
  3. conclude that p is true (i.e., Modus Tollens 1, 2)

- Example: prove that $\sqrt{2}$ is irrational.
  1. assume that $\sqrt{2}$ is rational
  2. there are two integers a and b such that $\sqrt{2} = \frac{a}{b}$, and a and b have no common factor
  3. $2b^2 = a^2$
  4. a^2 is even, and there is an integer c such that $2c = a$
  5. $2b^2 = (2c)^2 = 4c^2$
  6. b^2 is even as $b^2 = 2c^2$
  7. a and b have a common factor as 2
  8. it is a contradiction that statements 2 and 7 hold at the same time

Exhaustive Proof

- An exhaustive proof of a conditional statement $p \rightarrow q$
  first divides the condition into multiple cases (i.e., $p = p_1 \vee p_2 \dots \vee p_n$) and then proves that the conclusion holds for every case (i.e., $\bigwedge_{i=1}^{n} p_i \rightarrow q$)

- Proof by cases
  - A proof must cover all possible cases that arise in a theorem exhaustively.

- Ex. Prove that if n is an integer, then $n^2 \geq n$ holds.
  - Case 1. $n = 0$: it is shown that $n^2 \geq n$ as $0^2 \geq 0$.
  - Case 2. $n > 0$: $n^2 \geq n$ as $n^2 \geq n \times 1$ and $n \geq 1$
  - Case 3. $n < 0$: $n^2 \geq n$ as $n^2 \geq 0 > n$

Existence Proof

- An existence proof is to assert $\exists x P(x)$
- Strategies
  - Constructive proof: give a concrete case x that $P(x)$ holds
  - Nonconstructive proof: e.g., prove that $\neg\exists x P(x)$ is false
- Ex1 (constructive proof). show there is a positive integer that can be written as the sum of cubics of two positive integers in two different ways.
  - Proof. $1729 = 10^3 + 9^3 = 12^3 + 1^3$
- Ex2 (nonconstructive proof). show that there are two irrational numbers x and y such that x^y is a rational number.
  - $\sqrt{2}$ is an irrational number.
  - Case 1. $\sqrt{2}^{\sqrt{2}}$ is rational : the claimed statement holds for $x = \sqrt{2}$ and $y = \sqrt{2}$
  - Case 2. $\sqrt{2}^{\sqrt{2}}$ is irrational : the claimed statement holds for $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

    because $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$ is a rational number

Creative Proof Idea

- Is there any way to cover a 8x8 grid with the upper left and lower right squares removes using two-dominos?