Discrete Mathematics

CS204: Spring, 2008

Jong C. Park
Computer Science Division, KAIST

Today's Topics

Nested Quantifiers

Proofs

Mathematical Systems

Types of Proof

Direct Proof

Proof by Contradiction

Proof by Contrapositive

Proof by Case Analysis

Existence Proof

Logic and Proofs

Nested Quantifiers

- Examples
  - Write the following statement symbolically.
    - The sum of any two positive real numbers is positive.
    - $\forall x \forall y((x > 0) \wedge (y > 0) \rightarrow (x + y > 0))$
  - Restate $\forall m \exists n(m < n)$ in words.

    The domain of discourse is the set of integers.
    - For every integer *m*, there exists an integer *n* such that $m < n$.
    - If you take any integer *m*, there is an integer *n* greater than *m.*
    - There is no greatest integer.
  - Write the following assertion symbolically.
    - Everybody loves somebody.
    - $\forall x \exists y\ L(x,y)$

Nested Quantifiers

- What are the values of the following statements?
  - $\forall x \forall y((x > 0) \land (y > 0) \rightarrow (x + y > 0))$
    - domain of discourse is the set of real numbers
  - $\forall x \forall y((x > 0) \land (y < 0) \rightarrow (x + y \neq 0))$
    - domain of discourse is the set of real numbers
  - $\forall x \exists y(x + y = 0)$
    - domain of discourse is the set of real numbers
  - $\forall x \exists y(x > y)$
    - domain of discourse is the set of positive integers
  - $\exists x \forall y(x \leq y)$
    - domain of discourse is the set of positive integers
  - $\exists x \forall y(x \geq y)$
    - domain of discourse is the set of positive integers

Proofs

- A *mathematical system* consists of
  - Axioms
    - assumed to be true
  - Definitions
    - used to create new concepts in terms of existing ones
  - Undefined terms
    - implicitly defined by the axioms
- Theorem and proof
  - A theorem is a proposition that has been proved to be true.
    - cf. lemma, corollary
  - A proof is an argument that establishes the truth of a theorem.

Mathematical Systems

- Euclidean geometry
  - Axioms
    - Given two distinct points, there is exactly one line that contains them.
    - Given a line and a point not on the line, there is exactly one line parallel to the line through the point.
  - Definitions
    - Two triangles are congruent if their vertices can be paired so that the corresponding sides and corresponding angles are equal.
    - Two angles are supplementary if the sum of their measures is 180°.

Mathematical Systems

- Real numbers
  - Axioms
    - For all real numbers x and y, $xy = yx$.
    - There is a subset P of real numbers satisfying

      (a) If x and y are in P, then $x + y$ and xy are in P.

      (b) If x is a real number, then exactly one of the following statements is true:

      x is in P, $\quad x = 0$, $\quad -x$ is in P.
  - Definitions
    - The elements in P (of the preceding axiom) are called positive real numbers.
    - The absolute value $|x|$ of a real number x is defined to be x if x is positive or 0 and $-x$ otherwise.

Types of Proof

- Direct proof
- Proof by contradiction (indirect proof)
- Proof by contrapositive
- Proof by case analysis
- Existence proof
- ...

Direct Proof

- Suppose that we have statements of the form

  For all $x_1, x_2, \ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$, then $q(x_1, x_2, \ldots, x_n)$.

- This universally quantified statement is true provided that the conditional proposition

  if $p(x_1, x_2, \ldots, x_n)$, then $q(x_1, x_2, \ldots, x_n)$

  is true for all $x_1, x_2, \ldots, x_n$ in the domain of discourse.

- If $p(x_1, x_2, \ldots, x_n)$ is false, the statement is vacuously true.
- A direct proof assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then, using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, and previously derived theorems, shows directly that $q(x_1, x_2, \ldots, x_n)$ is true.

Direct Proof

- Definition
  - An integer n is even if there is an integer k such that $n = 2k$. An integer n is odd if there is an integer k such that $n = 2k + 1$.
- Give a direct proof of the following statement.

  For all integers m and n, if m is odd and n is even, then $m + n$ is odd.

  - Proof sketch.
    - We assume that m and n are arbitrary integers and that

      m is odd and n is even

      is true.
    - We then prove that

      $m + n$ is odd

      is true.

Direct Proof

- If a and b are real numbers, we define min{a,b} to be the minimum of a and b or the common value if they are equal.
  - More precisely, $\min\{a,b\} = a$ if $a < b$, a if $a = b$, b if $b < a$.
- Give a direct proof of the following statement.
  - For all real numbers d, d_1, d_2, x, if $d = \min\{d_1, d_2\}$ and $x \leq d$, then $x \leq d_1$ and $x \leq d_2$.
- Proof.
  - Exercise.

Proof by Contradiction

- A *proof by contradiction* establishes a conditional statement by assuming that the hypothesis is true and that the conclusion is false, and then, using the hypothesis and the negated conclusion as well as other axioms, definitions, and previously derived theorems, derives a contradiction.

Proof by Contradiction

- Give a proof by contradiction of the following statement.

  For all real numbers x and y, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

- Proof sketch.
  - We begin by letting x and y be arbitrary real numbers.
  - We then suppose that the conclusion is false, that is, that $\neg(x \geq 1 \vee y \geq 1)$ is true.

Proof by Contrapositive

- In order to prove $p \to q$, a proof by contrapositive proves $\neg q \to \neg p$.
- Example.
  - Use proof by contrapositive to show that

    For all integers m, if m^2 is odd, then m is odd.
  - Proof.
    - We begin by letting m be an arbitrary integer.
    - The contrapositive of the statement is

      if m is not odd, then m^2 is not odd

      or equivalently, if m is even, then m^2 is even.
    - So suppose that m is even. Then $m = 2k$ for some integer k.
    - Now $m^2 = (2k)^2 = 2(2k^2)$. Since m^2 is of the form $2 \times$ an integer (namely $2k^2$), m^2 is even.

Proof by Case Analysis

- Proof by cases is used when the original hypothesis naturally divides itself into various cases.
  - Example
    - The hypothesis "x is a real number" can be divided into cases:

      (a) x is a nonnegative real number and

      (b) x is a negative real number.
    - Suppose that the task is to prove $p \to q$ and that p is equivalent to $p_1 \lor p_2 \lor \ldots \lor p_n$ ($p_1, p_2, \ldots, p_n$ are the cases).
    - Instead of proving

      $$(p_1 \lor p_2 \lor \ldots \lor p_n) \to q,$$

      we prove

      $$(p_1 \to q) \land (p_2 \to q) \land \ldots \land (p_n \to q).$$
    - Cf. Show that the two statements are logically equivalent.

Proof by Case Analysis

- Examples
  - Prove that for every real number x, $x \leq |x|$.
  - Prove that for all integers n, n is odd if and only if n -1 is even.
    - Proof.
      - Use the equivalence $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$, that is, to prove "*p* if and only if *q*," prove "if *p* then *q*" and "if *q* then *p*."
  - Prove that for all real numbers x and all positive real numbers d, $|x| < d$ if and only if $-d < x < d$.

Existence Proof

- In order to prove $\exists x\, P(x)$, we simply need to find one member x in the domain of discourse that makes $P(x)$ true.
  - A proof of this kind is called an existence proof.
- Example
  - Let a and b real numbers with $a < b$.
  - Prove that there exists a real number x satisfying $a < x < b$.
    - Proof.
      - It suffices to find one real number x satisfying $a < x < b$.
      - The real number $x = (a + b)/2$ surely satisfies $a < x < b$.

Existence Proof

- To disprove $\forall x\, P(x)$, we simply need to find one member x in the domain of discourse that makes $P(x)$ false.
  - Such a value for x is called a counterexample.
- Example
  - Prove that the statement $\forall n(2^n + 1$ is prime) is false.
    - Proof.
      - A counterexample is $n = 3$, since $2^3 + 1 = 9$, which is not prime.

Summary

- Nested Quantifiers
- Proofs
- Mathematical Systems
- Types of Proof
- Direct Proof

Proof by Contradiction

Proof by Contrapositive

Proof by Case Analysis

Existence Proof