Discrete Mathematics: Lecture 5

- Last time:
  - Chap 1.6: Rules of Inference
- Today:
  - Chap 1.7: Introduction to Proofs
- Next time:
  - Chap 1.8: Proof Methods and Strategy

Review of last time (1)

- Logical equivalences involving quantifiers
  - $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$, $\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$
  - null quantification
  - De Morgan's laws

Review of last time (2)

- An argument form is a sequence of logical sentences
- An argument form is valid if its premises logically implies its conclusion
- A proof that an argument form is valid is a sequence of logical sentences such that
  - The last sentence is the conclusion
  - each sentence is either a premise or is obtained from previous sentences by applying a rule of inference

Chap 1.6: Introduction to proofs

- A proof is a valid argument that establishes the truth of a mathematical argument
- A proof can use the hypotheses of the theorem, axioms assumed to be true, and previously proven theorems.
- Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.
- Chap 1.5: formal proofs: all steps are supplied, rules for each step are given
- Chap 1.6: informal proofs: more than one rule of inference may be used in each step, steps may be skipped, axioms being assumed and the rules of inference used are not explicitly stated

Some terminology (术语)

- Theorem (定理): a statement that can be shown to be true. Reserved for somewhat important statements
- Proposition (命题): a less important theorem
- Proof (证明): a valid argument that establishes the truth of a statement
- Lemma (引理): a less important theorem that is helpful in the proof of other results
- Corollary (推论): a theorem that can be established directly from a theorem that has been proved
- Conjecture (猜想): a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert

Understanding how theorems are stated

- Many theorems assert that a property holds for all elements in a domain, however the universal quantification is stated implicitly
  - *e.g.*, if $x > y$, where x and y are positive real numbers, then $x^2 > y^2$
- When theorems of this type are proved, the law of universal instantiation is often used implicitly
  - The first step usually involves selecting a general element of the domain
  - Subsequent steps show that this element has the property in question
  - Finally, universal generalization implies that the theorem holds for all elements of the domain

Methods of proving theorems

- To prove $\forall x(P(x) \to Q(x))$, we prove $P(c) \to Q(c)$, where c is an arbitrary element of the domain
- We now focus on methods that show that conditional statements are true
    - To prove $p \to q$, it suffices to prove that if p is true, then q is true
- We will discuss these proof methods
    - Direct proofs
    - Proof by contraposition (逆否证明法)
    - Proofs by contradiction (反证法)

Direct proofs

- a direct proof of a conditional statement $p \to q$
  - the first step is the assumption that p is true
  - subsequent steps are constructed using rules of inference
  - the final step shows that q must be true
- Example 1
  - Definition: An integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$
  - Proposition: If n is an odd integer, then n^2 is odd

Proofs by contraposition

- Attempts at direct proofs often reach dead ends
- Indirect proofs
- Note that $p \to q$ is equivalent to its contrapositive $\neg q \to \neg p$
- Thus $p \to q$ can be proved by showing $\neg q \to \neg p$
- Example: Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Vacuous and trivial proofs

- If we can show that p is false, then we have a proof, called a vacuous proof, of $p \to q$
- If we can show that q is true, then we have a proof, called a trivial proof, of $p \to q$
- Vacuous and trivial proofs are often important when special cases of theorems are proved
- Example: Show that $P(0)$ is true, where $P(n)$ is: If $n > 1$, then $n^2 > n$, where the domain consists of all integers

Proofs by contradiction

- Suppose we want to prove p is true.
- Suppose we can find a contradiction q s.t. $\neg p \to q$ is true.
- We can conclude that $\neg p$ is false, and hence p is true.
- How to find a contradiction: $r \wedge \neg r$ for some statement r
- Example: Prove that $\sqrt{2}$ is irrational.

Proof of equivalence of a number of statements

- To prove $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$
- We can prove $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots (p_n \rightarrow p_1)$
- Example: Show that these statements about integer n are equivalent: 1. n is even 2. $n-1$ is odd 3. n^2 is even

Mistakes in proofs

> *Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it.*

What is wrong with this famous supposed "proof" that $1 = 2$.

1. $a = b$
2. $a^2 = ab$
3. $a^2 - b^2 = ab - b^2$
4. $(a - b)(a + b) = b(a - b)$
5. $a + b = b$
6. $2b = b$
7. $2 = 1$