ICS141: Discrete Mathematics for Computer Science I

Dept. Information & Computer Sci., University of Hawaii

Jan Stelovsky
based on slides by Dr. Baek and Dr. Still
Originals by Dr. M. P. Frank and Dr. J.L. Gross
Provided by McGraw-Hill
Lecture 7

Chapter 1. The Foundations
1.6 Introduction to Proofs

Chapter 2. Basic Structures
2.1 Sets
Proof Terminology

- A proof is a valid argument that establishes the truth of a mathematical statement.

- **Axiom** (or postulate): a statement that is assumed to be true.

- **Theorem**: A statement that has been proven to be true.

- **Hypothesis, premise**: An assumption (often unproven) defining the structures about which we are reasoning.
More Proof Terminology

- **Lemma**
  - A minor theorem used as a stepping-stone to proving a major theorem.

- **Corollary**
  - A minor theorem proved as an easy consequence of a major theorem.

- **Conjecture**
  - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)
Proof Methods

- For proving a statement $p$ alone
  - *Proof by Contradiction* (indirect proof):
    Assume $\neg p$, and prove $\neg p \rightarrow F$. 

Proof Methods

For proving implications $p \rightarrow q$, we have:

- **Trivial proof**: Prove $q$ by itself.
- **Direct proof**: Assume $p$ is true, and prove $q$.
- **Indirect proof**:
  - **Proof by Contraposition** ($\neg q \rightarrow \neg p$): Assume $\neg q$, and prove $\neg p$.
  - **Proof by Contradiction**: Assume $p \land \neg q$, and show this leads to a contradiction. (i.e. prove $(p \land \neg q) \rightarrow F$)
- **Vacuous proof**: Prove $\neg p$ by itself.
Definition: An integer $n$ is called odd iff $n=2k+1$ for some integer $k$; $n$ is even iff $n=2k$ for some $k$.

Theorem: Every integer is either odd or even, but not both.
- This can be proven from even simpler axioms.

Theorem:
(For all integers $n$) If $n$ is odd, then $n^2$ is odd.

Proof:
If $n$ is odd, then $n = 2k + 1$ for some integer $k$.
Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
Therefore $n^2$ is of the form $2j + 1$ (with $j$ the integer $2k^2 + 2k$), thus $n^2$ is odd. ■
Proof by Contraposition

Theorem: (For all integers \( n \))
If \( 3n + 2 \) is odd, then \( n \) is odd.

Proof:
(Contrapositive: If \( n \) is even, then \( 3n + 2 \) is even)
Suppose that the conclusion is false, i.e., that \( n \) is even.
Then \( n = 2k \) for some integer \( k \).
Then \( 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) \).
Thus \( 3n + 2 \) is even, because it equals \( 2j \) for an integer \( j = 3k + 1 \).
So \( 3n + 2 \) is not odd.
We have shown that \( \neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd}) \),
thus its contrapositive \( (3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd}) \) is also true. ■
Vacuous Proof Example

- Show \( \neg p \) (i.e. \( p \) is false) to prove \( p \rightarrow q \) is true.

- **Theorem:** (For all \( n \)) If \( n \) is both odd and even, then \( n^2 = n + n \).

- **Proof:**
  The statement “\( n \) is both odd and even” is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. ■
Trivial Proof Example

- Show \( q \) (i.e. \( q \) is true) to prove \( p \to q \) is true.

- **Theorem**: (For integers \( n \)) If \( n \) is the sum of two prime numbers, then either \( n \) is odd or \( n \) is even.

- **Proof**:
  
  *Any* integer \( n \) is either odd or even. So the conclusion of the implication is true regardless of the truth of the hypothesis. Thus the implication is true trivially. ■
Proof by Contradiction

  - Assume $\neg p$, and prove both $q$ and $\neg q$ for some proposition $q$. (Can be anything!)
  - Thus $\neg p \rightarrow (q \land \neg q)$
  - $(q \land \neg q)$ is a trivial contradiction, equal to $F$
  - Thus $\neg p \rightarrow F$, which is only true if $\neg p = F$
  - Thus $p$ is true
Rational Number

Definition:
The real number \( r \) is *rational* if there exist integers \( p \) and \( q \) with \( q \neq 0 \) such that \( r = \frac{p}{q} \). A real number that is not rational is called *irrational*. 
Proof by Contradiction

- **Theorem:** $\sqrt{2}$ is irrational.
- **Proof:**

  Assume that $\sqrt{2}$ is rational. This means there are integers $x$ and $y$ ($y \neq 0$) with no common divisors such that $\sqrt{2} = x/y$.

  Squaring both sides, $2 = x^2/y^2$, so $2y^2 = x^2$. So $x^2$ is even; thus $x$ is even (see earlier).

  Let $x = 2k$. So $2y^2 = (2k)^2 = 4k^2$. Dividing both sides by $2$, $y^2 = 2k^2$. Thus $y^2$ is even, so $y$ is even.

  But then $x$ and $y$ have a common divisor, namely $2$, so we have a contradiction.

  Therefore, $\sqrt{2}$ is irrational. $\blacksquare$
Proof by Contradiction

- Proving implication $p \rightarrow q$ by contradiction
  - Assume $\neg q$, and use the premise $p$ to arrive at a contradiction, i.e. $(\neg q \land p) \rightarrow F$
  
  \[
  (p \rightarrow q \equiv (\neg q \land p) \rightarrow F)
  \]

- How does this relate to the proof by contraposition?

- Proof by Contraposition $(\neg q \rightarrow \neg p)$:
  Assume $\neg q$, and prove $\neg p$. 
Proof by Contradiction

Example: Implication

Theorem: (For all integers $n$)
If $3n + 2$ is odd, then $n$ is odd.

Proof:
Assume that the conclusion is false, i.e., that $n$ is even, and that $3n + 2$ is odd.

Then $n = 2k$ for some integer $k$ and $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$.

This contradicts the assumption “$3n + 2$ is odd”.

This completes the proof by contradiction, proving that if $3n + 2$ is odd, then $n$ is odd. ■
Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof. Example:

- Prove that an integer $n$ is even, if $n^2$ is even.

- Attempted proof:
  Assume $n^2$ is even. Then $n^2 = 2k$ for some integer $k$.
  Dividing both sides by $n$ gives $n = (2k)/n = 2(k/n)$.
  So there is an integer $j$ (namely $k/n$) such that $n = 2j$.
  Therefore $n$ is even.

- Circular reasoning is used in this proof.

**Begs the question:** How do you show that $j = k/n = n/2$ is an integer, without first assuming that $n$ is even?
Chapter 2

Basic Structures:
Sets, Functions, Sequences, and Sums
2.1 Sets

- A **set** is a new type of structure, representing an *unordered* collection (group) of zero or more *distinct* (different) objects. The objects are called *elements* or *members* of the set.

  - Notation: \( x \in S \)

- Set theory deals with operations between, relations among, and statements about sets.

- Sets are ubiquitous in computer software systems.

  - (E.g. data types **Set**, **HashSet** in **java.util**)
Basic Notations for Sets

- For sets, we’ll use variables $S$, $T$, $U$, ...
- We can denote a set $S$ in writing by listing all of its elements in curly braces:
  - \{a, b, c\} is the set whose elements are $a$, $b$, and $c$
- **Set builder notation**:
  - For any statement $P(x)$ over any domain,
    - $\{x \mid P(x)\}$ is *the set of all $x$ such that $P(x)$ is true*
  - Example: \{1, 2, 3, 4\}
    - = \{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5 \}
    - = \{x \in \mathbb{Z} \mid x > 0 \text{ and } x < 5 \}
Basic Properties of Sets

- Sets are inherently *unordered*:
  - No matter what objects $a$, $b$, and $c$ denote,
    $$\{a, b, c\} = \{a, c, b\} = \{b, a, c\} = \{b, c, a\} = \{c, a, b\} = \{c, b, a\}.$$

- All elements are *distinct* (unequal); multiple listings make no difference!
  - If $a = b$, then $\{a, b, c\} = \{a, c\} = \{b, c\} = \{a, a, b, a, b, c, c, c, c\}$.
  - This set contains (at most) 2 elements!
Definition of Set Equality

- Two sets are declared to be equal if and only if they contain exactly the same elements.

- In particular, it does not matter how the set is defined or denoted.

Example:
The set \{1, 2, 3, 4\}  
\hspace{1cm} = \{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5\}  
\hspace{1cm} = \{x \mid x \text{ is a positive integer where } x^2 < 20\}
Infinite Sets

- Conceptually, sets may be *infinite* (i.e., not *finite*, without end, unending).

- Symbols for some special infinite sets:
  \( N = \{0, 1, 2, \ldots\} \) the set of *Natural* numbers.
  \( Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) the set of *Integers*.
  \( Z^+ = \{1, 2, 3, \ldots\} \) the set of positive integers.
  \( Q = \{p/q \mid p, q \in Z, \text{ and } q \neq 0\} \) the set of *Rational* numbers.
  \( R = \text{the set of “Real” numbers.} \)

- “Blackboard Bold” or double-struck font is also often used for these special number sets.