CS1382 Discrete Computational Structures

Lecture 11: Introduction to Proofs

Spring 2019

Richard Matovu

TEXAS TECH UNIVERSITY

Proofs of Mathematical Statements

A ***Proof*** is a valid argument that establishes the truth of a statement.

In Math or CS, informal proofs are generally used.

- More than one rule of inference are often used in a step.
- Easier for to understand and to explain to people.
- But it is also easier to introduce errors.

Proofs have many practical applications:

- Verification that computer programs are correct
- Establishing that operating systems are secure
- Enabling programs to make inferences in artificial intelligence
- Showing that system specifications are consistent

Definitions

- A ***theorem*** is a statement that can be shown to be true using:
    - definitions
    - other theorems
    - axioms (statements which are given as true)
    - rules of inference
- A ***corollary*** is a result which follows directly from a theorem

Proving Theorems

- Many theorems have the form: $\forall x (P(x) \to Q(x))$

- To prove them, we show that when *c* is an arbitrary element of the domain,

$$P(c) \to Q(c)$$

- By universal generalization the truth of the original formula follows.

- So, we must prove something of the form: $p \longrightarrow q$

Even and Odd Integers

- The integer ***n*** is **even** if there exists an integer *k* such that $\boldsymbol{n = 2k}$
- ***n*** is **odd** if there exists an integer *k*, such that $\boldsymbol{n = 2k + 1}$.
- Note that every integer is either even or odd and no integer is both even and odd.

We will need this basic fact about the integers in many example proofs to follow.

Proving Conditional Statements: $p \rightarrow q$

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction

Direct Proof

- **Assume that *p* is true**

  Use rules of inference, axioms, and logical equivalences to show that q must also be true.

- **Example**: Give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

- **Solution**: Assume that n is odd. Then $n = 2k + 1$ for an integer k.

  Squaring both sides of the equation, we get:

  $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

  where $r = 2k^2 + 2k$, an integer.

  We have proved that if n is an odd integer, then n^2 is an odd integer. ◀

*(◀ marks the end of the proof. Sometimes **QED** is used instead.)*

Direct Proof

Definition:

The real number *r* is *rational* if there exist integers *p* and *q* where *q* ≠ 0 such that *r* = *p* /*q*

- **Example**: Prove that the sum of two rational numbers is rational.

$$r = p/q, \quad s = t/u, \quad u \neq 0, \; q \neq 0$$

- **Solution***:* Assume *r* and *s* are two rational numbers. Then there must be integers *p, q* and also *t, u* such that

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu} = \frac{v}{w}$$

where *v* = *pu* + *qt*

w = qu ≠ 0

Thus the sum is rational. ◀

Proof by Contraposition

- **Assume $\neg q$ and show $\neg p$ is true also.**

  This is sometimes called an ***indirect proof*** method.

- If we give a direct proof of $\neg q \rightarrow \neg p$, then we have a proof of $p \rightarrow$ q.

  Why does this work?

  - **Example**: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

  - **Solution***:* Assume n is even. So, $n = 2k$ for some integer k.

    Thus $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$

    Therefore $3n + 2$ is even.

    Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well.

    If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even). ◀

Proof by Contraposition

- **Example**: Prove that for an integer n, if n^2 is odd, then n is odd.

- **Solution**: Use proof by contraposition.

  - Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$.

    Hence,

    $n^2 = 4k^2 = 2\,(2k^2)$ and n^2 is even (i.e., not odd).

    We have shown that if n is an even integer, then n^2 is even.

    Therefore by contraposition, for an integer n, if n^2 is odd, then n is odd. ◀

Proof by Contradiction *(AKA reduction ad absurdum)*

- To prove p, **assume $\neg p$ and derive a contradiction** such as $p \land \neg p$. (an indirect form of proof).
  - Assume $\neg p$
  - Find some contradiction $p \land \neg p$.
  - Claim $\neg \neg p = p$.

Proof by Contradiction

- **Example**: Show that $\sqrt{2}$ is irrational.

- **Solution:**

  Suppose $\sqrt{2}$ is rational. Then there exists integers *a* and *b* with $\sqrt{2} = a/b$, where $b \neq 0$ and *a* and *b* have no common factors. Then $2 = \frac{a^2}{b^2}$ $\quad 2b^2 = a^2$

  Therefore a^2 must be even. If a^2 is even then *a* must be even (an exercise).
  Since *a* is even, $a = 2c$ for some integer *c*. Thus, $2b^2 = 4c^2$ $\quad b^2 = 2c^2$

  Therefore b^2 is even. Again then *b* must be even as well.
  But then 2 must divide both *a* and *b*.

  This contradicts our assumption that *a* and *b* have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational .

◀

Proof by Contradiction

- **Example**: Prove that there is no largest prime number.
- **Solution**: Assume that there is a largest prime number. Call it p_n.
  - Hence, we can list all the primes 2,3,.., p_n.
  - Form $r = p_1 \times p_2 \times \ldots \times p_n + 1$
  - None of the prime numbers on the list divides r.
  - Therefore, by a theorem in Chapter 4, either r is prime or there is a smaller prime that divides r.
  - This contradicts the assumption that there is a largest prime. Therefore, there is no largest prime. ◀

Theorems that are Biconditional Statements

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

  - **Example**: Prove the theorem: "If n is an integer, then n is odd if and only if n^2 is odd."

  - **Solution:**

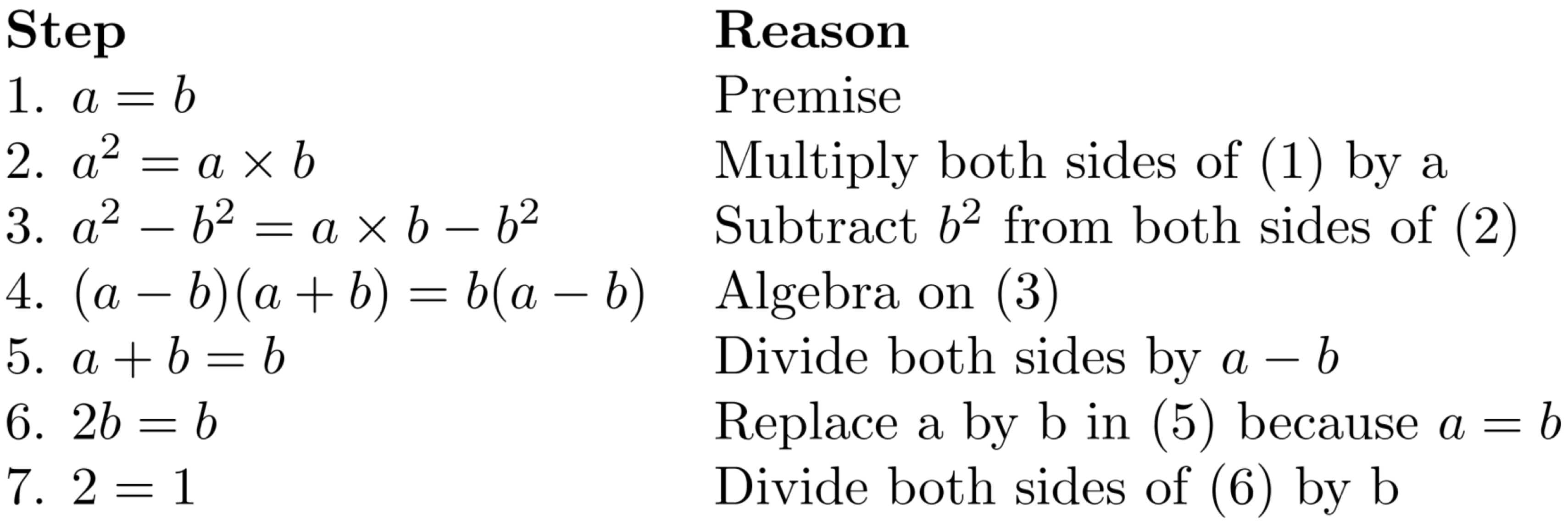
    We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for "if an only if," as in

"If *n* is an integer, then *n* is odd iff n^2 is odd."

What is wrong with this?

“Proof” that *1* = *2*



Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Step 5. a - b = 0 by the premise and division by 0 is undefined.