The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

With Question/Answer Animations

Summary

- Valid Arguments and Rules of Inference
- Proof Methods
- Proof Strategies

Introduction to Proofs

Section 1.7

Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
    - Proof of the Contrapositive
    - Proof by Contradiction

Proofs of Mathematical Statements

proof : valid argument that establishes truth of statement.

In math & CS, informal proofs (short) are generally used.

- More than one rule of inference are often used in a step.
- Steps may be skipped.
- Rules of inference used, are not explicitly stated.
- Easier to understand
- Easier to explain
- But it is easy to **introduce errors!**

Proofs of Mathematical Statements

Proofs have several 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

Terminology

- 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 *lemma* is a ‘helping theorem’ or a result which is needed to prove a theorem.
- A *corollary* is a result which follows directly from a theorem.
- Less important theorems are *propositions*.
- A *conjecture* is a statement that is proposed.
  - Once a proof of a conjecture is found, it becomes a theorem.
  - On the other hand, it can turn out to be false!

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, which could be
  - a set of numbers: Z, R, Q, R\Q
  - some discrete structure that we study in the course
- Often $\forall$(needed for a precise statement) is omitted
  - For example

“If x, y $\in$ R and $x > y$, then $x^2 > y^2$ ”

really means

“Let U = R, $\forall\ x\ \forall\ y$, if $x > y$, then $x^2 > y^2$.”

Proving Theorems

- Many theorems have the logical structure:

  $$\forall x(P(x) \rightarrow Q(x))$$

- To prove them, we show that where *c* is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof*: If we know q is true, then

  $p \rightarrow q$ is true as well.

  "If it is raining then 1=1."

- *Vacuous Proof*: If we know p is false then

  $p \rightarrow q$ is true as well.

  "If I am both rich and poor then $2 + 2 = 5$."

[Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5)]

Even and Odd Integers

Definition: The integer n is

- even if $\exists k \in$ Z such that $n = 2k$
- odd if $\exists k \in$ Z such that $n = 2k + 1$.

Note that every integer is either even or odd and no integer is both even and odd.

We need these basic facts about integers in the example proofs to follow.

We will learn more about integers in Chapter 4.

Proving Conditional Statements: $p \rightarrow q$

Direct Proof: Assume p is true and use rules of inference, axioms, & logical equivalences to show that q also is true.

Example: "If n is an odd integer, then n^2 is odd."

Solution: Assume n is odd. Then $n = 2k + 1$ (for $k \in$ Z). 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 $r = 2k^2 + 2k \in$ Z and so n^2 is indeed odd] (this last line is often omitted)

◀

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

Proving Conditional Statements: *p* → *q*

Definition: The real number *r* is *rational* (Q) if $\exists p, q \in$ Z, $q \neq 0$ such that $r = p/q$

Example: Prove "sum of two rational numbers is rational".

Solution: Assume *r* and *s* are two rational numbers. Then $\exists p, q, t, u \in$ Z such that

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

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

where $v = pu + qt$
$w =$ qu $\neq 0$

Thus the sum is rational. ◀

(As before, change of variables to v and w may be omitted. However, you can NOT omit noting that qu ≠ 0.)

Proving Conditional Statements: $p \to q$

Proof by Contraposition: Assume $\neg q$ and show $\neg p$ is true also. This is an *indirect proof* method.

(In reality, we are giving a direct proof of $\neg q \to \neg p$.)

Example: Prove that if $n \in$ Z and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So $n = 2k$ for $k \in$ Z. And

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$ [$= 2j$ for $j = 3k + 1$]

$\therefore$ $3n + 2$ is even.

[Since we showed $\neg q \to \neg p$, $p \to q$ must hold as well.]

◀

(statements within [ ] can be omitted as before)

Proving Conditional Statements: $p \rightarrow q$

Example: Prove that if $n \in Z$, n^2 is odd, then n is odd. Use proof by contraposition.

Solution: Assume n is even (i.e., not odd). Then $\exists k \in Z$ 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.]

Proving Conditional Statements: $p \rightarrow q$

Proof by Contradiction: (AKA *reductio ad absurdum*).

To prove p, assume $\neg p$ and derive a contradiction such as $p \wedge \neg p$ (this is another indirect form of proof).

Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true , it follows that the contrapositive $\mathbf{T} \rightarrow p$ also holds.

Example: Prove that if you pick 22 days from the calendar at least 4 must fall on the same day of the week (this is an example of the pigeon principle).

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week. Because there are 7 days of the week, we could only have picked 21 days at most. This contradicts the assumption that we have picked 22 days. ◀

Proof by Contradiction

Example: Use proof by contradiction to show that √2 is irrational.

Solution: Suppose √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

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

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,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b.

However, we assumed that a and b have no common factors $\Rightarrow\Leftarrow$

$\therefore \sqrt{2}$ 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 *r* is prime, but r is larger than all the known primes $\Rightarrow\Leftarrow$

$\therefore$ 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

both $p \rightarrow q$ and $q \rightarrow p$ are true.

Example: Prove the theorem: "If $n \in$ Z, then n is odd if and only if n^2 is odd."

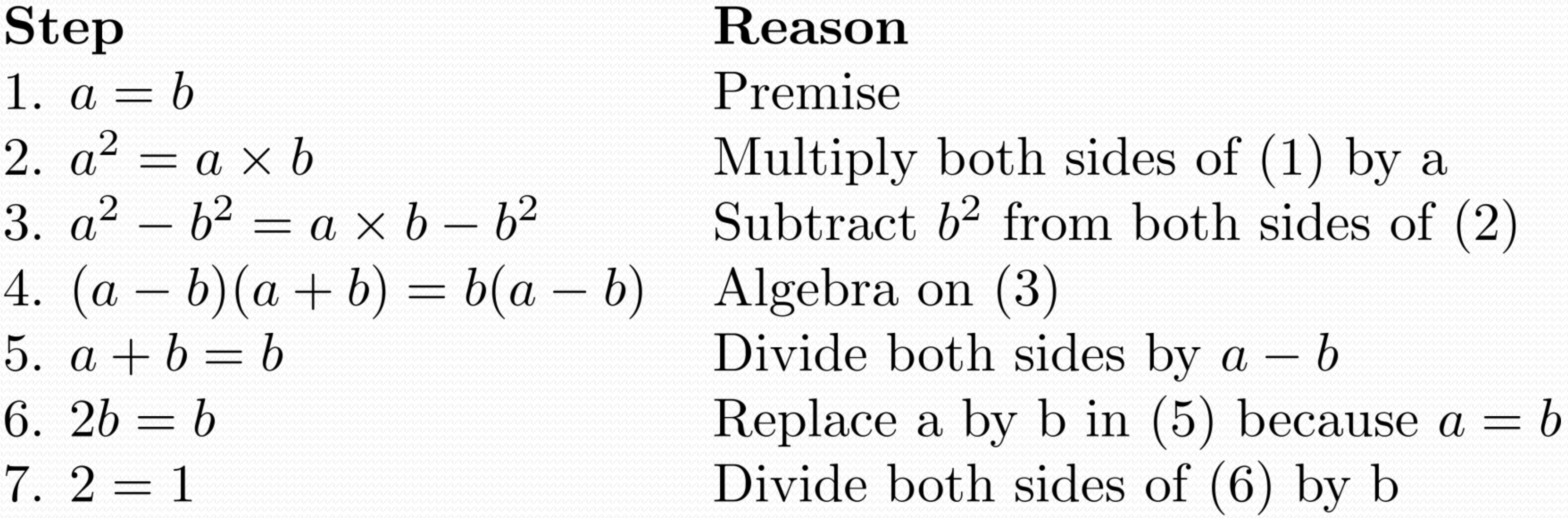
Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. $\therefore p \leftrightarrow q$.

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

"If $n \in$ Z, 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.

Summary and Looking Ahead

- If direct methods of proof do not work:
  - Try a proof by contraposition.
  - Or a proof by contradiction.
- In section 1.8 (not part of syllabus but which you are encouraged to read anyway) are strategies for when straightforward approaches do not work.
- In Chapter 5, we will see mathematical induction and related techniques.
- In Chapter 6, you will find combinatorial proofs/ techniques: important for probability and CS. (In 2540 Discrete Structures II will see some of it.)