Introduction to Proofs

Section 1.7

Section Summary

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

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - 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 known to be true)
  - rules of inference
- Less important theorems are sometimes called ***propositions***.
- 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.
- A ***conjecture*** is a statement that is being proposed to be true (it might be false!). Once a proof of a conjecture is found, it becomes a theorem.

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ "

really means

"For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$."

Methods of Proving Theorems

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

$$p \rightarrow q$$

  - You need to show that q is true if p is true.

Proving Conditional Statements: $p \rightarrow q$

Trivial Proof: If we know q is true, then $p \rightarrow q$ is true as well.
Ex: Prove "If it is raining then 1=1."
Since 1=1, the implication is true. ◀

Vacuous Proof: If we know p is false then $p \rightarrow q$ is true as well.
Ex: Prove "If I am both rich and poor then 2+2 = 5."
Since I can't be both rich and poor, the implication is true. ◀

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

Even and Odd Integers

Definition: The integer n is <u>even</u> if there exists an integer k such that $n = 2k$, and n is <u>odd</u> if there exists an integer k, such that $n = 2k + 1$. 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 some of the example proofs to follow.

Proving Conditional Statements: $p \rightarrow q$

- *Direct Proof*: Assume that *p* is true. Use rules of inference, axioms, and logical equivalences to show that *q* must also be true.

Ex: 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.)

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number ***r*** is rational if there exist integers *p* and *q* where $q \neq 0$ such that $r = p/q$

Ex: Prove that the sum of two rational numbers is rational.

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

Proving Conditional Statements: $p \rightarrow q$

- *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?

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

Solution: Assume by contraposition that n is even. So, $n = 2k$ for some integer k. Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

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). ◀

Proving Conditional Statements: $p \rightarrow q$

Ex: 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. ◀

Proving Conditional Statements: $p \rightarrow q$

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

Assume the statement is false and derive a contradiction. If the statement is $p \rightarrow q$, the negation of this statement is $(p \wedge \neg q)$. Assume p and $\neg q$, then derive a contradiction such as $r \wedge \neg r$. (an indirect form of proof). Since we have shown that $\neg q \wedge p \rightarrow \mathbf{F}$ is true , it follows that the contrapositive $\mathbf{T} \rightarrow (p \rightarrow q)$ also holds.

Ex: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: Assume by contradiction that you pick 22 days from the calendar and 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. This contradicts the assumption that we have picked 22 days. ◀

Proving Conditional Statements: $p \rightarrow q$

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

Solution: Assume by contradiction that n is even and 3n+2 is odd. So, $n = 2k$ for some integer k. Thus

$$3n + 2 = 3(2k) + 2 = 6k+2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even. This contradicts our original assumption that 3n+2 is odd. ◀

Theorems that are Biconditional Statements

- To prove a theorem that is a biconditional statement ($p \leftrightarrow q$), show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Ex: Prove "An integer n is odd iff 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.

What is wrong with this?

- **EX:** If n^2 is positive, then *n* is positive.
- ***"Proof:"*** Suppose that n^2 is positive. Because the conditional statement "If *n* is positive, then n^2 is positive" is true, we can conclude that *n* is positive.

- *Solution:*
  - *P(n): "n* is positive" and *Q(n)* "n^2 is positive." Then our hypothesis is *Q(n)*.
  - The statement "If *n* is positive, then *n*2 is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$.
  - From the hypothesis *Q(n)* and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude *P(n)*, because we are not using a valid rule of inference.
  - A counterexample is supplied by $n = -1$ for which *n*2= 1 is positive, but *n* is negative.

Types of Proofs Summary

How to prove the conditional statement $p \rightarrow q$:

- Trivial Proof (q is already known to be true)
- Vacuous Proof (p is already known to be false)
- Direct Proof
  - Assume p is true.
  - Show q is true.
- Proof by Contraposition (indirect)
  - Assume $\neg q$ is true.
  - Show $\neg p$ is true.
- Proof by Contradiction (indirect)
  - Assume the statement is false: $\neg q$ is true and p is true.
  - Derive a contradiction, such as $r \land \neg r$.

Tips for Writing Proofs

- Rewrite statement in propositional logic. Ex: $p \to q$
  - Determine the hypothesis (p) and consequence (q)
- First try a direct proof.
- If that doesn't work, try an indirect method.
- State proof method and assumptions.

- Example excerpts from proofs
  - "We use a direct proof and assume that (p)"
  - "We prove the contraposition. Assume that (¬q)"
  - "Assume by contradiction that (¬q) and (p)"

Looking Ahead

- First try a direct proof.
- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.
- In the next section, we will see strategies that can be used when straightforward approaches do not work.
  - In Ch. 5, we will see mathematical induction and related techniques.
  - In Ch. 6, we will see combinatorial proofs