Lecture 4: Introduction to Proofs

Section 1.7

Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof by Contraposition
  - Proof by Contradiction

Proofs of Mathematical Statements

- A ***proof*** is a valid argument that <u>establishes the truth</u> of a statement.

- 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 ***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 sometimes called ***propositions*** .
- A ***conjecture*** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Forms of Theorems

- Many theorems assert that a property holds <u>for all elements in a domain</u>, 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 $x^2 > y^2$."

Proving Theorems

- Many theorems have the form:

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

- To prove them, we show that: where 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: $p \to q$

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 there exists an integer k such that $n = 2k$, and n is odd 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. We will learn more about the integers in Chapter 4.

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.

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. ◀

Proving Conditional Statements: $p \to q$

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

Example : 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

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

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

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

Thus the sum is rational. ◀

Proof by Contraposition

- ***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 $\neg q \to \neg p$ then we have a proof of $p \to$ 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 $\neg q \to \neg p$, $p \to q$ 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

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

To prove p (the theorem), assume $\neg p$ and derive a contradiction (such as $p \wedge \neg p$).

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.

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. This contradicts the assumption that we have picked 22 days.

Proof by Contradiction

- **Example-1** : Use a proof by contradiction to give a proof 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 (see Chapter 4). 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. 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-2** : Give a proof by contradiction of the statement: "If $3n + 2$ is odd, then n is odd."

  Solution: Let p be "$3n + 2$ is odd" and q be "n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true. That is, assume that $3n + 2$ is odd and that n is not odd. Because n is not odd, we know that it is even.
  -> Because n is even, there is an integer k such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
  -> Because $3n + 2$ is $2t$, where $t = 3k + 1$, $3n + 2$ is even. Note that the statement "$3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd.
  -> Because both p and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd.

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 $p \to q$ and $q \to p$ 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 $p \to q$ and $q \to p$. Therefore we can conclude $p \leftrightarrow q$.

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

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

Biconditional Statements are useful for proving equivalence

- **Example** : Show that these statements about the integer x are equivalent: (i) $3x + 2$ is even, (ii) $x + 5$ is odd, (iii) x^2 is even. *[Ch 1.7, Exercise 33]*

Solution: Let, p = "$3x + 2$ is even", q = "$x + 5$ is odd", and r = "x^2 is even".

Assume, $3x + 2$ is even. Therefore, $3x$ is even. [even – even = even]

Since, 3 is odd, x must be even.

Then, $x + 5$ must be odd. [even + odd = odd] (proved $p \rightarrow q$)

Also, x can be written as $2k$, where k is an integer.

Then $x^2 = (2k)^2 = 4k^2$. Thus, x^2 is even. (proved $p \rightarrow r$)

Now, we must prove the converse, $r \rightarrow p$ and $q \rightarrow p$. Complete it yourself.

Then we will have, $p \leftrightarrow q$ and $p \leftrightarrow r$. Therefore, $p \equiv q$ and $p \equiv r$.

In other words, $p \equiv q \equiv r$.

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.

Assumptions are important.

What should be the assumption when we try to prove these statements?

- "if x is an irrational number and $x > 0$, then $\sqrt{x}$ is also irrational."
  - for direct proof: Assume x cannot be written as p/q, where $q \neq 0$. (Difficult to prove the statement, as we cannot explicitly represent irrationality in algebra)
  - for contraposition: Assume $\sqrt{x}$ is rational, therefore $\sqrt{x} = p/q$, where $q \neq 0$. (easier to proof for x from $\sqrt{x}$)

Assumptions are important.

What should be the assumption when we try to prove these statements?

- "If x, y, and z are integers and all three are even, then x +y +z is even,"
    - <u>for direct proof:</u> Assume x, y and z are evens, therefore, $x = 2a$, $y = 2b$ and $z = 2c$. (Easier to find x+y+z)
    - <u>for contraposition:</u> Assume $x+y+z = 2k + 1$. (Relatively Lengthy, have to separately consider x, y and z and their cases)

- "if m and n are integers and mn is even, then m is even or n is even."
    - <u>for direct proof:</u> Assume mn is even, therefore $mn = 2k$. (Relatively Difficult, have to consider all cases of m and n)
    - <u>for contraposition:</u> Assume m is odd and n is odd, therefore $m = 2a+1$, $n = 2b+1$. (Easier to find mn)

Looking Ahead

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.
  - Or try to ***disprove*** by counterexamples.
  - In Chapter 5, we will see mathematical induction and related techniques.