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

- 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 to understand and to explain to people.
  - But, it is also easier to introduce errors.

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.

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, $P(c) \to Q(c)$
- So, we must prove something of the form: $p \to q$
- By universal generalization the truth of the original formula follows.

Proving Conditional Statements: $p \rightarrow q$

- ***Direct Proof*:** Assume that p is true. Bring axioms, definitions, rules of inference, 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.)

Proving Conditional Statements: $p \to q$

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

  $p \to q$ is true as well.

"If it is raining then 1=1."

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

  $p \to q$ is true as well.

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

Proving Conditional Statements: $p \to q$

- ***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 $\neg q \to \neg p$ 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). ◀

Proving Conditional Statements: $p \rightarrow q$

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.

◀

Proving (Conditional) Statements: ($q \rightarrow$) ***p***

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

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

Proof by Contradiction

Example: 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 .

◀

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.

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.

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.
  - In the next section, we will see strategies that can be used when straightforward approaches do not work.
  - In Chapter 5, we will see mathematical **induction** and related techniques.
  - In Chapter 6, we will see **combinatorial proofs**