Introduction to Proofs

Section 1.7

Proofs of Mathematical Statements

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

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 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 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 $x^2 > y^2$."

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 the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$ where is the p = P(c) and q=Q(c) are propositions.

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]

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.

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:

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

  here $r = 2k^2 + 2k$ is 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. I often use (QED) instead.)

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?

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Contrapositive

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

  Solution: Assume n is not odd, therefore even. So, $n = 2k$ for some integer k. Thus

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2m, \text{ with } m = 2k^2$$

  Therefore n^2 is even, not odd. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well.

◀

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 iif n^2 is odd."

Proving Conditional Statements: $p \rightarrow q$

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

  To prove the conditional statement, assume $\neg q$ and derive a contradiction such as $r \wedge \neg r$ using *p.* Since we have shown that $\neg q \rightarrow (r \wedge \neg r = \mathbf{F})$ is true , it follows that the contrapositive $\mathbf{T} \rightarrow q$ also holds. Therefore $p \rightarrow q$.

Proof by Contradiction

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

Solution: Let

p = "you pick 22 days from the calendar" and

q="at least 4 days must fall on the same day of the week",

now assume

¬q="no more than 3 days fall on the same day of the week".

Now use p to derive a contradiction: p implies 3 weeks and 1 day, which implies that one day will be repeated 4 times. This is a contradiction to our assumption ¬q, therefore q. (QED)