Discrete Mathematics
Introduction to Proofs

Definition: A *theorem* is a statement that can be shown to be true.

We demonstrate that a theorem is true with a *proof* (valid argument) using:

- Definitions
- Other theorems
- Rules of logic
- Axioms

- A *lemma* is a 'helping theorem' or a result that is needed to prove a theorem.
- A *corollary* is a result that 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.

Example:

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

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

Methods of Proving Theorems

1. **Direct Proofs**

In direct proof, we show that conditional $p \to q$ is true. We assume that p is true and show that q must be true.

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.

Example: -21 is odd since $-21 = 2(-11) + 1$; 0 is even since $0 = 2(0)$

Example: Give a *direct* proof of the theorem "If n is an odd integer, then n^2 is odd."

p q

Proof: Assume n is an odd integer.

Then $n = 2k+1$ for some integer k. (by def.)

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

$= 2(2k^2+2k)+1$

$= 2m+1$ which is odd.

QED

QED is an abbreviation of the words from the Latin phrase "***Quod Erat Demonstrandum***" that literally means, "**what was to be shown**". Traditionally, the abbreviation is placed at the end of a mathematical proof to indicate that the proof or argument is complete.

Example: Use a *direct* proof to show that "The product of two odd numbers is odd."

Proof: Let m and n be odd integers.

Then $m = 2k+1$ and $n = 2r+1$.

$$m \cdot n = (2k+1)(2r+1)$$

$$= 4kr + 2k + 2r + 1$$

$$= 2(2kr + k + r) + 1$$

$$= 2\ell + 1 \text{ which is odd.}$$

QED

Example: Give a *direct* proof of the theorem "If n is a perfect square, then $n + 2$ is NOT a perfect square."

$0 = 0^2$ $1 = 1^2$ $4 = (1+1)^2$ $9 = (2+1)^2 \ldots$

Proof: Assume n is a perfect square.

Then $n = m^2$ for some integer m.

If $n = 0$, then $n+2 = 0+2 = 2$ is
$(m = 0)$ NOT a perfect square.

If $n \geq 1$, then the smallest perfect
$(m \geq 1)$ square greater than
n is $(m+1)^2$.

$$(m+1)^2 = m^2 + 2m + 1 \geq m^2 + 2(1) + 1$$
$$= m^2 + 3 = n + 3.$$

$$n \longrightarrow \geq n+3$$

Hence $n+2$ is NOT a perfect square.

QED.

2. Proof by Contraposition

We know that $p \to q \equiv \neg q \to \neg p$.

This means that the conditional statement $p \to q$ can be proven by showing that its contrapositive, $\neg q \to \neg p$, is true. We assume that $\neg q$ is true and show that $\neg p$ is true.

Example: Prove that "If m and n are integers and $m \times n$ is even, then m is even or n is even."

Try Direct Proof: Assume $m \times n$ is even.
Then $m \times n = 2k$ for some integer k.

Contraposition: Assume m is odd and n is odd.
Then $m = 2k+1$ and $n = 2r+1$.

Hence $m \times n = (2k+1)(2r+1)$
$= 4kr + 2k + 2r + 1$
$= 2(2kr + k + r) + 1$
$= 2\ell + 1$ for some int. ℓ
which is odd.

QED.

3. Proofs by Contradiction

Suppose we want to prove that a statement $p \to q$ is true. We assume $p \wedge \neg q$, then show that leads to a contradiction.

Why does it work to prove $p \to q$ is true? $p \wedge \neg q \equiv F \Rightarrow \neg q \equiv F \Rightarrow q \equiv T$ (p: T, q)

Example: Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using

a. a proof by *contraposition*
b. a proof by *contradiction*

Contraposition:

Assume $\neg q$. Show $\neg p$.

Assume n is odd. By the definition $n = 2k+1$ for some integer k.

$n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+1+5$

$= 2(4k^3+6k^2+3k+3 = 2\ell$ (for some integer ℓ) which is even.

QED.

Contradiction:

Assume $p \wedge \neg q$. $p \wedge \neg q \equiv F$

Suppose n^3+5 is odd and n is odd.

If n is odd, then n^2 is odd.

Hence n^3 is odd.

$5 = \underbrace{n^3+5}_{\text{odd}} - \underbrace{n^3}_{\text{odd}} = \text{even}$

Contradiction!

QED.

Other types of proofs

- *Trivial Proof*: If we know q is true, then $p \to q$ is true as well.

  Example: "If it is raining then 1=1."

- *Vacuous Proof*: If we know p is false then $p \to q$ is true as well.

  Example: "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 later.

- *Proofs of Equivalence*: To prove a theorem that is biconditional statement, that is $p \leftrightarrow q$, we show that $p \to q$ and $q \to p$ are BOTH true.

  Example: Prove that the following is true for all positive integers n: n is even if and only if $3n^2 + 8$ is even.

→ If n is even, then $3n^2+8$ is even

Direct proof:

Let n be even, then $n = 2k$ for some integer k.

Therefore $3n^2+8 = 3(2k)^2+8 = 12k^2+8$

$= 2(6k^2+4) = 2r$ (r is an int.)

which is even

← If $3n^2+8$ is even, then n is even.

Proof by contraposition:

Let n be odd, then $n = 2k+1$ for some integer k.

Hence $3n^2+8 = 3(2k+1)^2+8$

$= 12k^2+12k+11 = 2(6k^2+6k+5)+1$, which is odd.

- *Counterexamples*: When we believe a statement of the form $\forall x P(x)$ to be false, we look for a counterexample.

  Example: Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Counterexample: $3 = 2+1$
$= 3+0$

What is wrong with this proof?

"Proof" that $1 = 2$.

Step	**Reason**
1. $a = b$	1. Given
2. $a^2 = ab$	2. Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	3. Subtract b^2 from both sides of (2)
4. $(a-b)(a+b) = b(a-b)$	4. Algebra on (3)
5. $a + b = b$	5. Divide both sides by $a - b$ $= 0$
6. $2b = b$	6. Replace a by b in (5) since $a = b$
7. $2 = 1$	7. Divide both sides of (6) by b

QED