COT3100: Introduction to Proofs (Sec 1.6)

1 – Some Terminology

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

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

Theorems can also be referred to as **results** or **facts**.

Relatively less important results are sometimes called **propositions**.

A **lemma** is an intermediate result that is helpful in the proof of other results.

A **corollary** is a theorem that can be established directly from a (proven) theorem.

A **conjecture** is a statement that is being proposed to be true.

2 – Direct Proofs

In order to prove $p \longrightarrow q$, start with p and reach the conclusion q using the rules of inference.

EXAMPLE. Prove that if n is an odd integer, then n^2 is odd.

n is odd	$\longrightarrow$	$n = 2k + 1$	(by definition of an odd integer)
	$\longrightarrow$	$n^2 = (2k + 1)^2$	(square both sides)
	$\longrightarrow$	$n^2 = 4k^2 + 4k + 1$	(simple algebra)
	$\longrightarrow$	$n^2 = 2(2k^2 + 2k) + 1$	(factor the first two terms by 2)
	$\longrightarrow$	n^2 is odd	(by definition of an odd integer)

3 – Vacuous Proofs

Proving $\neg p$ is sufficient to prove $p \rightarrow q$

EXAMPLE. Prove that $P(0)$ is true, where $P(n)$ is "if $n > 1$, then $n^2 > n$" and the domain consists of all integers.

$P(0)$ is "if $0 > 1$, then $0^2 > 0$."

This is true because $0 > 1$ is false.

4 – Trivial Proofs

Proving q is sufficient to prove $p \longrightarrow q$

EXAMPLE. Prove that $P(0)$ is true, where $P(n)$ is "if $a \geq b > 0$, then $a^n \geq b^n$" and the domain consists of all integers.

$P(0)$ is "if $a \geq b > 0$, then $a^0 \geq b^0$."

This is true because the conclusion $a^0 = 1 \geq b^0 = 1$ of the implication is true.

The hypothesis $a \geq b > 0$ is not needed in the proof.

5 – Proof by Contraposition

Instead of proving $p \longrightarrow q$, prove that $\neg q \longrightarrow \neg p$, which is equivalent.

EXAMPLE. Prove that if $3n + 2$ is odd, then n is odd.

CONTRAPOSITIVE: "If n is not odd, then $3n + 2$ is not odd."

n is not odd	$\longrightarrow$	n is even	(n is either odd or even but not both)
	$\longrightarrow$	$n = 2k$	(n is divisible by 2)
	$\longrightarrow$	$3n + 2 = 3(2k) + 2$	(substitute 2k for n)
	$\longrightarrow$	$3n + 2 = 2(3k + 1)$	(simple algebra)
	$\longrightarrow$	$3n + 2$ is even	(divisible by 2)
	$\longrightarrow$	$3n + 2$ is not odd	

6 – Proof by Contradiction (Reductio ad absurdum)

We want to prove that q is TRUE.

Suppose the conclusion is FALSE, that is $\neg q$ is TRUE.

Derive a contradiction usually of the form $p \wedge \neg p$ which establishes $\neg q \longrightarrow$ FALSE.
The contrapositive of this assertion is TRUE $\longrightarrow q$ from which q follows.

RECALL. A positive integer is called a **prime** number if it is divisible by only 1 and itself.
THEOREM. There is no largest prime number.

PROOF BY CONTRADICTION. Suppose that there is a largest prime number, a.
Hence, the set of all primes lie between 1 and a.

Take the product of all these primes to get $b = 1.2.3.5.7.\ldots.a$.
But $b + 1$ is a prime number larger than a. (why?)

This contradicts the assumption that there is a largest prime number.

7 – Proof by Cases

Break the premise of $p \longrightarrow q$ into an equivalent disjunction of the form $p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$.

Then use the equivalance

$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q \equiv (p_1 \longrightarrow q) \wedge (p_2 \longrightarrow q) \wedge \ldots \wedge (p_n \longrightarrow q)$

Each of the implication $p_i \longrightarrow q$ is **a case**.

To complete a proof by cases:

1. You must convince the reader that the cases are inclusive, i.e., they exhaust all possibilities.
2. You must establish all the implications.

8 – Disproving via Counterexamples

To prove a theorem is false, we can construct counterexamples.

EXAMPLE. Show that ”every positive integer is the sum of square of two integers” is false.

3 is a counterexample.

The only perfect squares not exceeding 3 are 0 and 1.

3 cannot be written as a sum of two terms each of which is 0 or 1.