CS1231 Part 1 - Introduction to Proofs

Based on lectures by Terence Sim and Aaron Tan
Notes taken by Andrew Tan
AY18/19 Semester 1

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

1 Proof Techniques

A proof is a concise, polished argument explaining the validity of a statement.

1.1 Proof by Construction

A proof by construction demonstrates the existence of a mathematical object by creating the object.

1.2 Proof by Counterexample

Conversely, a proof by counterexample provides a mathematical object that disproves a given statement.

1.3 Proof by Contraposition

The contraposition of

$$if\ P\ then\ Q$$

is

$$if\ \sim P\ then\ \sim Q$$

Both statements are logically equivalent, and hence you can prove one by proving the other.

1.4 Proof by Contradiction

Given a statement S, only one of the following is true:

$$S\ is\ true$$
$$\sim S\ is\ true$$

Thus to prove a statement S by contradiction, you first assume ∼S is true. Then use facts and theorems to arrive at a contradiction, which then implies that ∼S is false, and hence S is true.

2 Logical Statements

2.1 If-then

Many statements in proofs have the following structure:

$$if\ P\ then\ Q$$

We can use direct proofs to prove statements of this form: We first assume P is true, then work forwards by combining P with other facts and theorems to conclude that Q is true.

2.2 For-all

The for-all statement, $\forall x \ P(x)$, essentially states that P(x) is true for all x in a given set. To prove statements of this form, we prove that P(x) is true for a particular but arbitrary x. Since x is arbitrary (that is, x is no different to the other elements of the set it was taken from), we can conclude that P(x) is true for all x.

A Definitions

Definition 1.3.1 (Divisibility) - if n and d are integers and d $\neq$ 0, then n is divisible by d if, and only if, n equals d times some integer.

$$d|n \iff \exists k \in \mathbb{Z}, n = dk$$

Definition 1.6.1 - An integer n is even if, and only if, n equals twice some integer.
An integer n is odd if, and only if, n equals twice some integer plus 1.

$$n \text{ is even} \iff \exists \text{ an integer } k \text{ such that } n = 2k$$
$$n \text{ is odd} \iff \exists \text{ an integer } k \text{ such that } n = 2k + 1$$

B Theorems

Theorem 4.3.1 (Epp) $\forall a, b \in Z_+$, if a|b then $a \leq b$
Theorem 4.3.3 (Epp) - Transitivity of Divisibility

$$\forall a, b, c \in Z \text{ if a|b and b|c, then a|c}$$

C Notation

C.1 Set Notation

$\mathbb{R}$ - the set of real numbers
$\mathbb{Z}$ - the set of all integers
$\mathbb{Q}$ - the set of all rational numbers

C.2 Logic Notation

$\exists$ - there exists at least one
$\exists !|$ - there exists one and only one
$\forall$ - for all
$\in$ - is a member of
$\notin$ - is not a member of
$\ni$ - such that

D Properties of the Real Numbers

1. Closure: Integers are closed under addition and multiplication.
   $\forall x, y \in \mathbb{Z}, x + y \in \mathbb{Z}$, and $xy \in Z$

   For all real numbers a,b, and c,

2. Commutativity: $a + b = b + a$ and $ab = ba$
3. Distributivity: $a(b + c) = ab + ac$
4. Trichotomy: exactly one of the following is true:
   $a < b$, $a > b$, or $a = b$