ICT600 COMPUTATIONAL MATHEMATICS

Mathematical Proofs

Composed by Nirattaya Khamsemanan, Ph.D

Disclaimer: this partial note is my attempt to help you learn the material in this course. Things in here might not be in the real exam and vice versa. Don't use this as your main study. There might be some typos and/or mistakes.

Be advised: these partial notes have been created for the sole purpose of aiding your studies in this class, and are *for personal use only*. They may not be duplicated, copied, modified or translated without my written consent.

.-**-..-**-..-**-..-**-..-**-.∼ ♡ Have Fun!♡ ∽.-**-..-**-..-**-..-**-..-**-.

'Theorems and proofs are the heart and soul of mathematics and definitions are its spirit.' – Michael Sipser

Being a mathematician for over a decade, I can't agree enough with what Professor Sipser said in his book. So let's dive into all these wonderful definitions, theorems and most importantly, proofs.

Statement is a sentence expressed in (mathematical) words that is either true or false.[1]

Definition is a statement of the precise meaning of a world or phrase, a mathematical symbol or concept.

Theorem is a mathematical statement that can be proved by a chain of logical reasoning on the basis of certain assumptions that are given or implied in the theorem.

Proof is a valid logical argument that a statement is true.

Lemma is an auxiliary theorem proved beforehand to be used in the proof of another theorem.

Corollary is a theorem that is a natural consequence, that is, it follows logically from something else. It is a 'by-product of another theorem'.

[1] Putting aside things like the incompleteness theorem for now...

1 Direct Proof

A direct proof is based on the assumption that the hypothesis is true and proceeds by a series of logically connected steps to the conclusion. Theorems that are put in the form $P \to Q$ are good candidate for this type of proof. We assume P and proceed to prove that Q is true.

Recall that:

Definition 1. Suppose $a, b \in \mathbb{Z}$. We say that a divides b,(or b is divisible by a) written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a divisor or a factor of b, and that b is a multiple of a.

Definition 2. A natural number p is prime if it has exactly two positive divisors, 1 and p.

Theorem 1. *The sum of two prime numbers larger than 2 is not a prime number.*

Proof

Recall that:

Definition 3. Let $f(x)$ and $g(x)$ be real-valued functions defined for all real numbers. The composition function $f \circ g$ is defined by

$$(f \circ g)(x) = f(g(x)).$$

The domain of $f \circ g$ consists of those input x (in the domain of g) for which $g(x)$ is in the domain of f.

Theorem 2. *Let f and g be two real-valued functions defined for all real numbers. If f and g are injective, the $f \circ g$ is also injective.*

Proof

2 Contrapositive Proof

A contrapositive proof is a good alternative to direct proof. We are using the fact that the statement $P \to Q$ is equivalent to the statement $\neg Q \to \neg P$. We assume $\neg Q$ and proceed to prove that $\neg P$ is true. Although it is possible to use direct proof exclusively, there are some occasions where contrapositive proof is much easier.

Theorem 3. *Suppose $k \in \mathbb{Z}$. If $3k + 1$ is even, then k is odd.*

Proof

Theorem 4. *Suppose $x, y \in \mathbb{R}$. If $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$.*

Proof

3 Proof by Construction

A proof by construction is a direct demonstration that a claimed object exists (a construction). Here are some examples.

Theorem 5. *Suppose n is the product of three distinct primes, $n = pqr$, where $p \neq q \neq r \neq p$. Then n has at least 6 distinct factors.*

Proof

Definition 4. A graph is called k-regular if every vertex in the graph has degree k.

Theorem 6. *For each even number n greater than 2, there exists a 3-regular graph with n vertices.*

Proof

4 Proof by Contradiction

This is another strategy of proving a theorem $P \to Q$. We begin by assuming that P is true and Q is false i.e. we assume $P \wedge \neg Q$ The proof proceeds until we derive contradiction F.

Recall that

Definition 5. A real number x is rational if there exist integers a and b with $b \neq 0$ such that $x = a/b$. If x is not rational it is called irrational.

Theorem 7. *If x is a rational number and y is an irrational number, then $x + y$ is an irrational number.*

Proof

Theorem 8. *Let n be a non prime counting number. Then n is divisible by a prime number p such that $p \leq n$*

Proof

5 Proof by Induction

Mathematical induction is a common and basic method for proving a statement that holds for all natural numbers 1, 2, 3, ...,n, ..., or just about any situation where one case depends on previous cases. We start off with some conjecture that is true for the basic case, typically when the case of 1. Then we assume that the conjecture also holds for all numbers less than or equal to n. If we can show that the statement is true for the case of $n + 1$ as well, then, by induction, we can be sure that the conjecture is true for all natural numbers.

Principle of Mathematical Induction

1. The *basis (base case)*: Show that the conjecture is true for the lowest value that n is given. Note that n does not necessary have to be 1.

2. The *inductive step*: Prove that if the conjecture holds for some k, then the statement also holds for $k + 1$.

Then the conjecture/statment is true for all positive integers. The assumption in the inductive step that the statement holds for some n is called the *induction hypothesis (or inductive hypothesis)*.

Theorem 9. *The sum of the first n natural numbers is given by the following formula*

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

Proof

Theorem 10. *For all integer $n \geq 1$, $3^{2n} - 1$ is divisible by 4.*

Proof

Example 1. *Tower of Hanoi: You have three pegs and a collection of disks of different sizes. Initially all of the disks are stacked on top on each other according to size on the first peg – the largest disk being on the bottom, and the smallest on the top. A move in this game consists of moving a disk from one peg to another, subject to the condition that a larger disk may never rest on a smaller one. The objective of the game is to find a number of permissable moves that will transfer all of the disks from the first peg to the third peg, making sure that the disks are assembled on the third peg according to size. The second peg is used as an intermediate peg.*

Show that it takes $2^n - 1$ *moves to move* n *disks from the first peg to the third peg.*

6 Proving Non-Conditional Statements

Sometimes theorems cannot be put into conditional form $P \rightarrow Q$. Such theorems are biconditional statements. They are usually in the form of if-and-only-if theorems or equivalence theorems. To attack this type of theorems, we separate our proof into two parts. First we proof $P \rightarrow Q$ and then we proof $Q \rightarrow P$. If succeeded, we will obtain P if and only if Q. For the equivalence theorems type, we must show that each statement is equivalent to any other statement in the theorem.

Theorem 11. *The integer n is odd if and only if n^2 is odd.*

Proof

Theorem 12. *If A, B, and C are any three sets, then*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap B)$$

Proof

Theorem 13. *Let a and b be two distinct real numbers. Then the following statements are equivalent*

(*i*) b *is larger than* a

(*ii*) *Their average,* $\dfrac{a+b}{2}$, *is larger than* a

(*iii*) *Their average,* $\dfrac{a+b}{2}$, *is smaller than* b

Proof

References

[1] Michael Sipser, *Introduction to the Theory of Computation, 2nd Edition, Thomson Course Technology*, Thomson Course Technology 2006. ISBN 0-534-95097-3.

[2] Richard Cole, *Theory of Computing. What is Feasible, Infeasible, and Impossible Computationally*, Lecture notes.

[3] Antonella Cupillari, *The Nuts and Bolts of Proofs*, PWS Publishing Company 1993. ISBN 0-534-10320-0.