CPSC 351 — Mathematics Review
Part Two: Definitions and Proofs

Ideally, everything in the document should be a ***review*** of material that you learned about in a prerequisite course. It will be assumed that you understand and can use all of it in CPSC 351.

This document is based, heavily, on the review included in Sipser's text, *Introduction to the Theory of Computation* [3]. It should also be consistent with material in the textbook in the course in discrete mathematics that you completed as a prerequisite for this one — probably (but not necessarily) either the text of Epp [1] or Rosen [2].

Definitions

While some course material will be written informally, other material — including material that introduces technical terms and provides proofs of significant results — will be written more formally, instead. In these more formal documents, technical terms will be introduced using ***definitions*** resembling the following example.

Definition 1. A ***natural number*** is an integer that is greater than or equal to zero. The set of all natural numbers will be denoted by $\mathbb{N}$.

Definitions generally describe how you can decide whether something is an example of whatever is being defined. They might also introduce notation, concerning what is being defined, that is to be used. In this and other definitions, the technical term being introduced is ***italicized and in bold***.

Axioms

An ***axiom*** is a (generally, unprovable) rule, or "first principle", that is accepted as true because it is self-evident or universally accepted (and especially useful). These include properties of various (commonly used) sets; for example, "the commutative law of integer addition" is the axiom that $a + b = b + a$ for all integers a and b.

Theorems

A ***theorem*** is a significant formal (or "mathematical") statement that has been proved to be true. Less significant results, that are needed to establish more significant results, are often called ***lemmas***. A ***corollary*** of a result is another result that follows directly (or "almost immediately") from the first one. In some documents, these are all called ***claims***.

Significant technical work also sometimes include ***conjectures*** (which are sometimes also called ***postulates***). Unlike theorems, these are *not* statements that have been proved. Instead, they are statements that are *believed* to be true (but might be false, instead) — and they are presented as things that the author would like to prove, and are suggested as useful (if proved).

Proofs

Students in this course will be expected to discover, and write, proofs of various claims.

As Sipser [3] notes, it is important to begin by making sure that you understand the claim that is to be proved — assuming that this has been given in the exercise, assignment or test for which a proof is required. Sometimes the claim has not been given — so that you must start by ***writing it down — in a clear, readable way — yourself.***

You may need to make several attempts to *discover* a proof of the claim: There might be more than one ***proof technique*** that can be applied to establish the desired result, and there might also be more than one way to apply a given proof technique.

Once you *have* discovered a proof then you need to ***write the proof down*** so that it is as clear as you can make it and organized in a way that makes it as easy as possible ***for another person (who does not know the proof already) to read it and understand it***.

While mathematical writing can seem to be quite challenging, many students find that their writing improves with practice. Additional writing advice — which will help you to avoid common mistakes — will be supplied. Note, though, that you might need to re-organize and rewrite a complicated proof at least once before your proof is readable.

Proof Techniques

You should, ideally, have been introduced to several ***proof techniques*** before this course. These are used, along with axioms and previously established theorems, to obtain proofs of additional results (that is, to establish *new* theorems).

- In a ***direct proof*** you begin with what you know and work toward what you want to prove — applying axioms, theorems and definitions as you need to make progress.
- A ***constructive proof*** is a proof that an object exists, which presents a ***process*** — that is, an ***algorithm*** — that can be used to construct this object, along with a proof that this algorithm is correct.
- A ***proof by exhaustion*** (or a "proof by cases") is a proof in which you begin by listing a finite set of cases — arguing that at least one of these cases must always arise. The desired result is then proved for each of the cases that has been listed (often by giving a somewhat different argument, for each case).
- A ***proof by contradiction*** is a proof in which you begin by assuming that what you want to prove is ***false*** and then — ***without assuming anything more*** — establishing a ***contradiction*** (that is, proving that some statement is both true and false, at the same time). Since your result is impossible, your assumption must be incorrect — and this provides a proof of the desired result.
- ***Mathematical induction*** is a proof technique that will be described in the next part of this review.

Long, complicated proofs may include multiple steps, and different proof techniques might be used for different steps of the proof. With that noted, you should generally be able to name the proof technique that you are using, and it is good practice to identify this, for your reader, when your proof begins — because this helps the reader to anticipate, and better understand, whatever will follow.

References

[1] Susanna S. Epp. *Discrete Mathematics with Applications*. Brooks Cole, fifth edition, 2019.

[2] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill Education, eighth edition, 2018.

[3] Michael Sipser. *Introduction to the Theory of Computation*. CENGAGE Learning, third edition, 2013.