Introduction to Discrete Mathematics

MAT202 Course Notes

Introduction to Discrete Mathematics

MAT202 Course Notes

TJ Yusun

University of Toronto Mississauga
Mississauga, ON, Canada

June 21, 2020

Edition: Fall/Winter 2020-2021

Website: tjyusun.com/itdm

Preface

The word *discrete* in the title of our course means *separate*; something that is *not smooth*. In the study of discrete mathematics we will typically concern ourselves with discrete objects such as the integers, graphs, finite and countable sets. (In contrast, excluded from this are objects that may vary continuously, such as those ones covered in trigonometry, calculus, and Euclidean geometry.)

Contents

Chapter 1

Review of MAT102

Many of the concepts you learned in your MAT102 course will be useful in MAT202; in this chapter we briefly review some definitions and results, and present some exercises to warm up for the rest of the course! Material in this chapter is based on *MAT102H5 Introduction to Mathematical Proofs* by *Shay Fuchs.*

1.1 Sets and Functions

A **set** is is just a collection of objects (where the order in which the objects are listed does not matter). The following set operations should be familiar to you: intersection $A \cap B$, union $A \cup B$, complement A^c, difference $A \setminus B$, and Cartesian product $A \times B$.

We also recall that proving the set A is a subset of the set B simply necessitates showing that any element of A can also be found in B.

Definition 1.1.1 Set Inclusion and Equality. If A and B are sets in some universe U, then we say A **is a subset of** B, denoted by $A \subseteq B$, if

$$(\forall x \in U)(x \in A \Rightarrow x \in B).$$

We say that A and B are **equal** as sets if $A \subseteq B$ and $B \subseteq A$ both hold. This means that

$$(\forall x \in U)(x \in A \Leftrightarrow x \in B).$$

$\Diamond$

Checkpoint 1.1.2 Define

$$A = \{k \in \mathbb{Z} : k = 6s + 3 \text{ for some } s \in \mathbb{Z}\}$$

and

$$B = \{m \in \mathbb{Z} : m = 3t \text{ for some } t \in \mathbb{Z}\}.$$

Prove that $A \subseteq B$ holds.

Hint. Pick an arbitrary element in A, call it x. Then you know $x = 6s + 3$ for some integer s. Can you express x in the form $3t$ where t is an integer?

We will use the standard notation for these sets of numbers:

$$\mathbb{N} = \{1, 2, 3, \dots, \}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \right\}$$
$$\mathbb{R} = (-\infty, \infty), \text{ the set of real numbers.}$$

Intervals of real numbers are denoted by $(a, b), [a, b]$, and other combinations, with $-\infty$ or ∞ as one of both of the endpoints.

Remark 1.1.3 Interval notation is used to refer to sets of real numbers. It is *incorrect*, for instance, to say that $(-2, 4) = \{-1, 0, 1, 2, 3\}$, or that $\{0, 1, 2, 3, \ldots\} = [0, \infty)$. Watch your notation!

Definition 1.1.4 Function. A **function**

$$f : A \to B$$

is a rule that takes elements from its **domain** A and assigns to each one an element from the **codomain** B. ◊

Definition 1.1.5 Injective, surjective, bijective. A function $f : A \to B$ is

- **injective** if for every $x_1 \neq x_2 \in A$, $f(x_1) \neq f(x_2)$.
- **surjective** if for every $y \in B$, there exists an $x \in A$ so that $f(x) = y$.
- **bijective** if for every $x_1 \neq x_2 \in A$, $f(x_1) \neq f(x_2)$.

◊

Checkpoint 1.1.6 For each function, determine if it is injective, surjective, bijective, or none of these:

(a) $f : \mathbb{R} \to (0, +\infty)$, $f(x) = \sqrt{x^2 + 1}$

(b) $g : \mathbb{N} \to \mathbb{N}$, $g(m) = 3m + 7m^2$

(c) $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $h(a, b) = \dfrac{ab(b-1)}{2}$

Answer. 1. none, 2. injective, 3. surjective.

Definition 1.1.7 Composition. Given two functions $f : A \to B$ and $g : B \to C$, the **composition** $g \circ f : A \to C$ is defined as the function

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

for all $x \in A$. ◊

Theorem 1.1.8 *The composition of two (injections, surjections, bijections) is a(n) (injection, surjection, bijection).*

Checkpoint 1.1.9 Prove Theorem 1.1.8.

Later in the course we will learn techniques for counting objects and proving that two sets have the same number of elements; the notion of cardinality will be a useful tool to remember.

Definition 1.1.10 Two sets A and B are said to have the **same cardinality**, written as

$$|A| = |B|,$$

if there exists a bijection between them.

We also say A has cardinality **less than or equal to** the cardinality of B, written as

$$|A| \leq |B|,$$

if there exists an injective function from A to B. ◊

Checkpoint 1.1.11 Prove that the set of odd integers

$$O = \{\ldots, -3, -1, 1, 3, \ldots\}$$

has the same cardinality as $\mathbb{N}$.

Hint. Construct a bijection from O to $\mathbb{N}$.

Definition 1.1.12 Power Set. Let A be a set. The **power set** of A, denoted by $P(A)$, is the set

$$P(A) = \{X : X \subseteq A\},$$

that is, it contains all subsets of A. ◊

Checkpoint 1.1.13 Prove that if A is finite, then

$$|P(A)| = 2^{|A|}.$$

1.2 Logic and Proof Techniques

Mathematical statements can typically be phrased as an implication $P \Rightarrow Q$, read as *if P, then Q*, where P or Q may be complex statements themselves that involve conjunctions (and), disjunctions (or), negations, quantifiers, even implications. There are various ways in which an implication can be proven true, and there is no hard and fast rule that dictates which proof method to use given a particular problem. In MAT102 you were introduced to the following proof techniques:

- Direct proof: Assume P is true, then prove Q is true.
- Contrapositive: Assume $\neg Q$ is true, then prove $\neg P$ is true.
- Contradiction: Assume the conclusion is false, then use this to arrive at a statement that contradicts one of the assumptions.

Activity 1.2.1 Prove each statement, noting which proof technique you used. Explain all your steps clearly, as if you are writing for the current batch of MAT102 students.

(a) The sum of two odd numbers is even.

(b) The square of an even number is divisible by 4.

(c) The equation $x^3 + x + 1 = 0$ has no rational solutions.

(d) For integer n, if $n^3 + 5$ is odd, then n is even.

(e) There is no smallest positive rational number.

(f) Every multiple of 4 can be written as $1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

(g) The sum of a rational number and an irrational number is irrational.

(h) A three-digit natural number is divisible by 9 if and only if the sum of its digits is divisible by 9.

(i) If A and B are defined as in Checkpoint 1.1.2, then $B \not\subseteq A$.

Many of these statements are *quantified* universally, which means it involves some variable (say n), and you need to prove the claim holds for all relevant

values of the variable (say $n \in \mathbb{N}$). For 1, 2, and 4, for example, the relevant quantities are integers; the statements need to be proven for all integers.

We can use mathematical induction to prove that a statement is true for all natural numbers.

Theorem 1.2.1 Principle of Mathematical Induction. *Let $P(n)$ be a predicate defined for $n \in \mathbb{N}$. If the following conditions hold:*

(a) $P(1)$ is true;

(b) For all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$ is true.

then $P(n)$ is true for all $n \in \mathbb{N}$.

One can also replace the second condition with the following:

b. For all $k \in \mathbb{N}$, $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \Rightarrow P(k+1)$ is true.*

*This is called **strong induction**, where one assumes the induction step holds for all natural numbers from 1 to k in order to prove the claim for $k+1$.*

Depending on what is being proved, one may need to make slight modifications to the standard technique: e.g. changing/adding to the base case, or "skipping" from k to $k+2$ in the case when one only has to prove the claim for every other natural number starting from the base case.

Checkpoint 1.2.2 Prove the following statements using induction:

(a) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all $n \in \mathbb{N}$.

(b) $2^n \geq n^2$ for all $n \in \mathbb{N}, n \geq 4$.

(c) $4^{2n} - 1$ is divisible by 5 for every $n \in \mathbb{N}$.

Checkpoint 1.2.3 The **Fibonacci sequence** $\{F_n\}$ is defined recursively as

$$\begin{cases} F_n = F_{n-1} + F_{n-2}, n \geq 3 \\ F_1 = F_2 = 1 \end{cases}.$$

Prove that

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

using strong induction.

Checkpoint 1.2.4 Let T_n be the number of ways one can tile a $2 \times n$ grid with 1×2 rectangles. For example, $T_2 = 2$ since there are two tilings of a 2×2 grid using only 1×2 rectangles.

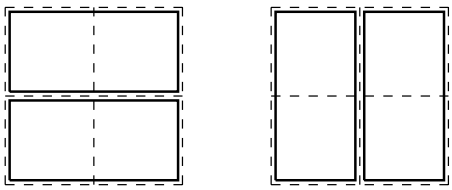

Figure 1.2.5 The two tilings of a two-by-two grid.

Find a recurrence relation for T_n and prove that $T_n = F_{n+1}$ as defined in Checkpoint 1.2.3.

1.3 Integers and Divisibility

For completeness we restate here the definition of divisibility and the Division Algorithm.

Definition 1.3.1 Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. We say that a **is divisible by** b, or b **divides** a, denoted by

$$b \mid a,$$

if there exists $m \in \mathbb{Z}$ such that $a = mb$.

If b is not divisible by a, then we write $b \nmid a$.

We say that the natural number p is a **prime number** if the only natural numbers that divide p are 1 and p. ♢

Theorem 1.3.2 *Let $a, b \in \mathbb{N}$. Then there exist unique q and r that satisfy all of the following:*

$$a = qb + r, q \geq 0, 0 \leq r < b.$$

Checkpoint 1.3.3 Find q and r that satisfy the Division Algorithm for the following pairs of numbers a and b:

(a) $a = 140, b = 22$

(b) $a = 22, b = 140$

(c) $a = 735, b = 21$

Definition 1.3.4 GCD. Given integers a and b not both zero, their **greatest common divisor**, denoted by

$$\gcd(a, b),$$

is the largest integer that divides both numbers.

We say that a and b are **relatively prime** if $\gcd(a, b) = 1$. ♢

There are a number of ways to determine the GCD of two numbers a and b:

- Listing all factors of a and b, then finding the largest one they have in common;
- Writing out the prime factorizations of a and b, then collecting all common prime factors;
- The Euclidean Algorithm (repeated division).

Checkpoint 1.3.5 Apply the three techniques above to compute $\gcd(220, 360)$.

Answer. The GCD is 20.

Solution. The Euclidean Algorithm performs the following steps:

$$\begin{aligned} 360 &= 1 \cdot 220 + 140 \\ 220 &= 1 \cdot 140 + 80 \\ 140 &= 1 \cdot 80 + 60 \\ 80 &= 1 \cdot 60 + 20 \\ 60 &= 3 \cdot 20 + 0 \end{aligned}$$

The GCD is the divisor in the last line (where the remainder becomes zero).

Theorem 1.3.6 Bezout's Identity. *Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $m, n \in \mathbb{Z}$ such that $am + bn = \gcd(a, b)$.*

Checkpoint 1.3.7 Find a pair of integers x and y such that

$$13x + 11y = 2.$$

Then explain why the equation $13x + 11y = 2$ has infinitely many solutions. Can you characterize all such solutions?

Checkpoint 1.3.8 Prove that the equation

$$14x - 35y = 9$$

has no integer solutions.

Checkpoint 1.3.9 Let $a, b, d, \in \mathbb{N}$. Prove that $ax+by = d$ has integer solutions x and y if and only if $\gcd(a, b) \mid d$.

Lemma 1.3.10 Euclid's Lemma. *If p is prime, and a and b are integers such that $p \mid ab$, then either $p \mid a$ or $p \mid b$ (or both).*

Checkpoint 1.3.11 Prove Lemma 1.3.10 using Theorem 1.3.6.

Checkpoint 1.3.12 Let $m, a, b \in \mathbb{N}$. Using Theorem 1.3.6, prove that if $m \mid ab$ and $\gcd(a, m) = 1$, then $m \mid b$.

1.4 Reading and Writing Proofs

Proofs are a form of communication. They are used to argue (that a claim holds true); and sometimes explain (*why* a claim is true).

Activity 1.4.1 When writing proofs, one needs to be *clear*, *complete*, and *correct*. Comment on the three proofs below of the statement

Let $m \in \mathbb{Z}$. Then m is even if and only if $m^3$is even.

Which one(s) is/are

- convincing?
- easiest to read?
- missing steps?
- correct?

Proof 1 ($\Rightarrow$) $m = 2k \Rightarrow m^3 = 8k^3 = 2(4k^3)$, so m^3 is even.
($\Leftarrow$) By contradiction. Assume m^3 is even but m is odd. Then $m = 2k+1 \Rightarrow m^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1$, which is odd.
Contradiction, so m must be even. So m even $\Leftrightarrow m^3$ even.
Proof 2

$$m \text{ even } \Leftrightarrow m = 2k \Leftrightarrow m^3 = 8k^3 \Leftrightarrow m^3 = 2(4k^3) \Leftrightarrow m^3 \text{ even},$$

hence proven.
Proof 3 We want to prove that

$$m \text{ is even if and only if } m^3 \text{ is even.}$$

($\Rightarrow$) First, we show m even $\Rightarrow m^3$ even. If m is even, then we can write $m = 2k$ for some $k \in \mathbb{Z}$. Then,

$$\begin{aligned} m^3 &= (2k)^3 \\ &= 8k^3 \\ &= 2(4k^3). \end{aligned}$$

Since $k \in \mathbb{Z}$, then $4k^3 \in \mathbb{Z}$ as well, and so m^3 is even.

($\Leftarrow$) Next, we prove that m^3 even $\Rightarrow$ m even. To do this we prove the contrapositive: If m is odd, then m^3 is odd.

If m is odd, then there is a $k \in \mathbb{Z}$ such that $m = 2k + 1$. Then

$$\begin{aligned} m^3 &= (2k+1)^3 \\ &= 8k^3 + 12k^2 + 6k + 1 \\ &= 2(4k^3 + 6k^2 + 3k) + 1. \end{aligned}$$

Since $k \in \mathbb{Z}$, then $4k^3 + 6k^2 + 3k \in \mathbb{Z}$ as well. Therefore m^3 is odd. This completes the proof.

The use of English words makes proofs more approachable and understandable. Here are some commonly-used phrases in mathematical proofs. Note the use of the plural *we* instead of the singular *I*.

Declare intentions

- We will prove...
- We want to show that...
- In order to prove... we...
- At this point we need to find...
- We consider the following cases...

Clarify implications

- Since... then...
- Because..., we have...
- Therefore/thus/hence...
- This means that...
- The previous statement implies...

Explain steps

- By assumption, we know that...
- By simplication/manipulation,rearranging,...
- Because of property/theorem/definition, we have...

Activity 1.4.2 Write a complete and convincing proof of the following claim that uses the mathematical statements given below (in some order). Note that this is a proof by contradiction.

Claim: Let A, B be subsets of some universal set U. Prove that if $(A \cup B)^c = A^c \cup B^c$, then $A \subseteq B$.

$x \in A$	$x \in A^c \cup B^c$
$x \notin B$	$x \in A \cup B$
$x \in B^c$	$x \notin (A \cup B)^c$

Chapter 2

Counting Techniques

Objectives

- State the Sum Rule and the Product Rule, and use them to solve counting problems.
- Derive the formulas for permutations and combinations (of n objects taken k at a time), multi-permutations, and permutations and combinations with repetition allowed.
- Given a word problem, recognize which of the above techniques is applicable, and use it to solve the problem.
- Prove simple combinatorial identities.

2.1 The Basic Counting Principles

This is a longer sentence that is followed by another sentence. Two sentences, and a second paragraph to follow.

Let's end with some mathematics.

If the two sides of a right triangle have lengths a and b and the hypotenuse has length c, then the equation

$$a^2 + b^2 = c^2$$

will always hold.