Eric Du

CS70: DISCRETE MATHEMATICS AND PROBABILITY THEORY

University of California, Berkeley ★ May 6, 2024

CONTENTS

INTRODUCTION

Welcome to my notes for CS 70! When I took this class, one of the things I noticed pretty early on was the common dissatisfaction with the way the course notes are written, as they are very dense and make heavy use of mathematical language that the reader may not be immediately familiar with. So, my goal with this book is to try and strip away all that technical language, and present the material in a way that hopefully makes more sense.

I have to thank my good friend Andrew Binder for his style file: he is largely the reason why I undertook this endeavor to begin with.

0.1 How you should use these notes

Throughout the notes, I will try to be as comprehensive as possible, but at the end of the day, these notes are simply meant to be supplementary reading to official course material. It is also entirely possible that the notation used in this book differs from that used in the course, and if you find that happening make sure you use the official notation.

Also, my goal with this book is not to be as mathematically rigorous as possible, but instead to present the material in a way that practically makes sense – I want you to walk away from each section feeling like you have the ability to utilize the concepts from that section to solve new problems.

One last thing before we dive into the content, let's go over the elements in this book and what they mean:

INTRODUCTION TO SETS

1.1 Introduction

One thing mathematicians love doing is finding similarities between different objects, then grouping these objects based on their common properties. It is precisely this idea of clasification that gives rise to set theory, a field so important that without it many fields of mathematics would (quite literally) collapse.

What use is set theory to computer science? Well, the idea of classifying things based on their similarities is such a natural habit that we do it here as well. For instance, consider the famous P vs NP problem: the entire premise of this problem relies on the notion that we can classify problems based on whether they're efficiently solvable – that's an act of classification, and hence we need set theory here.[1]

The basic definition of a set is as follows:

Definition 1.1 (Set): A *set* is a well-defined collection of objects.

A couple things about this definition here: firstly, there really is no restriction on what the "objects", also more commonly called the "elements" of a set, referred to in this definition can be: it can be numbers, variables, problem statements (as with the P vs. NP example), and even other sets.[2]

Secondly, the notion of what it means to be "well-defined" for our purposes is that there is a clear way to tell whether an element belongs or doesn't belong to a set.[3] As an example, the set of even numbers is well defined, since given a number x, we know it belongs to the set if x is even, and doesn't belong if x is odd. The following box describes how we would talk about set membership mathematically.

Notation (Membership): If an element x is a member of a set S, then we write $x \in S$. If x is not a member of S, then we write $x \notin S$.

1.2 Describing Sets

Now that we know what a set is, what are some ways we can write them down? The easiest and perhaps the most obvious one is to just list out the elements in the set one by one. If we wanted to write down the set of numbers between 1 and 10 inclusive, then we could write:

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

This is certainly a valid way of writing this set, but you can imagine that if you were to write down the set of numbers from 1 to 1000 like this, it would take forever. So, there is indeed a better way to write this: what we do instead is we can define S as belonging to a larger set of items, but with certain conditions. In this way, the set S can be rewritten as:

$$S = \{x \in \mathbb{Z} \mid 1 \leq x \leq 10\} \tag{1.1}$$

In English, we read this as: "x belongs to the set of integers such that x is between 1 and 10". Notice how in this way, we've defined x to first belong to the set of integers (a larger set of numbers), but then we added the restriction that x is between 1 and 10 to construct our set S. Note that we're also not restricted by the number of conditions we can put, as long as all restrictions are satisfied by every element in the set. For instance, if we wanted to describe the set of numbers between 1 and 10 (inclusive) except 5, then we could write:

$$S = \{x \in \mathbb{Z} \mid 1 \leq x \leq 10, x \neq 5\} = \{1, 2, 3, 4, 6, 7, 8, 9, 10\}$$

In English, we read this as "x belongs to the set of integers such that x is between 1 and 10, and x is not equal to 5." Notice that all the elements in the set satisfy both restrictions: they're between 1 and 10, and they're not equal to 5.

[1] Math majors will probably hate me for calling this an application of set theory, but it *somewhat works*, so please just let it slide.
[2] One should be careful about this last point since it's caused a lot of headache for mathematicians over the past 200 years.
[3] If you want a more rigorous definition of what it means to be well-defined, this book really isn't for you.

1.2.1 Notable Sets

There are some sets that are so commonly used throughout the rest of this course that it's in your best interest to just go ahead and memorize them:

- **Natural Numbers:** Denoted by $\mathbb{N} = \{0, 1, 2, \dots\}$
- **Integers:** Denoted by $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- **Rationals:** fractional numbers, denoted by $\mathbb{Q} = \{\frac{x}{y} | y \in \mathbb{Z}, y \neq 0\}$
- **Real Numbers**: any (potentially infinite) decimal number, denoted by $\mathbb{R}$
- **Complex Numbers:** Denoted by $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$
- **Empty set:** The set that contains nothing, denoted by $\varnothing$[4]

1.3 Subsets

When we were describing a set, I implicitly introduced the concept of describing a set S as being *part of* another larger set. Rigorously, what this means is that the elements contained in S can be found within a larger set, in which case S would be considered a subset of that larger set.

> Definition 1.2 (Subset): Given two sets A and B, if every element of A is also a member of B, then A is a *subset* of B, which we write as $A \subseteq B$.

Sometimes, there is also the subtle distinction of whether B contains elements not contained in A. If this is the case, then we sometimes call A a *proper subset* of B:

> Definition 1.3 (Proper Subset): Given two sets A and B, if every element of A is also a member of B and B contains elements not contained in A, then A is a *proper subset* of B, which we write as $A \subset B$.

This distinction is not really explored that much in CS70, so you won't have to worry too much about it. Another thing you won't have to worry about but I'll include here anyways is the notion of a superset:

> Definition 1.4 (Superset): Given two sets A and B, if every element of A is also a member of B, then B is a *superset* of A, denoted as $A \supseteq B$.

And analogous to what a proper subset is to a subset, there is also the notion of a proper superset:

> Definition 1.5 (Proper Superset): Given two sets A and B, if every element of A is also a member of B and B contains elements not contained in A, then B is a *proper superset* of A, denoted as $A \supset B$.

Again, these definitions are really just for completness sake and aren't really things we explore much in CS70. The next section, however, is extremely important.

1.4 Combining Sets

So far, we've covered what a set is, how to describe them, and also how to classify them in terms of one being a subset of another set. What I haven't explained yet is how we can mathematically talk about the relationship between sets, which is done through unions and intersections of sets.

Let's say that you have a set of numbers A, and another set of numbers B. Now, suppose you wanted to describe a set S, which is formed by taking elements in either A or B. Mathematically, we'd write that as

$$S = A \cup B$$

where the $\cup$ symbol denotes a **union**, defined below:

[4] You might be wondering: didn't we just say that a set is defined to have elements in it? Doesn't an empty set contradict that very statement? Short answer: don't worry about it. Long answer: go read a set theory textbook.

Definition 1.6 (Union): Given two sets A and B, the *union* of A and B is the set formed by all elements in A or B, written as $A \cup B$.

To fully illustrate the "or" condition here, it's helpful to look at an example:

Example 1.1

Given a set $A = \{1, 2, 3\}$ and a set $B = \{3, 4, 5\}$, then the *union* is denoted by $S = A \cup B = \{1, 2, 3, 4, 5\}$.

Notice that here, even though the element 3 was contained in both A and B, it only appears once in S. This is the subtlety of the "or" condition: if the same element exists in both A and B, only one copy of it is retained in $A \cup B$.

What if instead of looking at elements in A or B, you wanted to look at the elements that are common between A and B? Then, we'd write it as:

$$S = A \cap B$$

where the $\cap$ symbol denotes a **intersection**, defined below:

Definition 1.7 (Intersection): Given two sets A and B, the *intersection* of A and B is the set formed by the elements common between A and B, written as $A \cap B$.

Like the union, let's illustrate this with an example:

Example 1.2

Given a set $A = \{1, 2, 3\}$ and a set $B = \{3, 4, 5\}$, then the *intersection* is denoted by $S = A \cap B = \{3\}$

Since 3 is the only common element between A and B, this is the only element that the intersection picks out.

Note that the intersection of two sets could potentially contain zero elements: this is what we call a disjoint set:

Definition 1.8 (Disjoint Sets): Two sets A and B are said to be *disjoint* if they contain no elements in common, or equivalently, $A \cap B = \varnothing$.

1.5 Complements

Aside from combining two sets, another thing we would like to do is to learn how to subtract elements from the set. How do we express the act of *taking away* elements from a set? This is where we introduce set complements and set differences.

You might wonder why an operation like this is even useful to begin with. Well, on the surface, with sets you can easily write down, it really isn't that useful. However, when it comes to infinitely sized sets, where describing a rule for them is quite complicated, this idea of subtracting or taking away elements actually comes in very useful.

Consider the set of irrational numbers for example. Because irrational numbers by definition go on infinitely and also don't repeat, you can't ever find a way of writing this set down in the way we described in equation 1.1. However, you *can* define the set of irrationals in terms of a difference between two known sets: the reals and the rationals. By "difference", what we really mean is to take the set of reals $\mathbb{R}$, take away all the rational numbers (members of $\mathbb{Q}$), and the set we're left with is the set of irrational numbers. Mathematically, we write that as:

$$\mathbb{Q}' = \mathbb{R} \setminus \mathbb{Q}$$

Here, the set of irrationals is denoted by $\mathbb{Q}'$. I formalize this notion in the box below:

Definition 1.9 (Set Differences): Given two sets A and B, the set $S = A \setminus B$ consists only of elements in A that are not elements of B.

Remark : There's a couple different ways we write set differences, which I've listed below:

- $A \setminus B = \{x \in A \mid x \notin B\}$

- $A \setminus B = A - A \cap B$
- $x \in A \setminus B \iff x \in A \wedge x \notin B$

The last bullet here might not make sense at the moment; we'll revisit this one later so don't worry. See if you can convince yourself that these are indeed equivalent ways to write $A \setminus B$.

This idea of set differences also allows us to also introduce the idea of *complements*. Let's return to the irrational numbers. Because we've defined the irrationals to be constructed from taking the rationals $\mathbb{Q}$ away from the set of reals $\mathbb{R}$, it should make sense that if we tried to take the union and intersection between the two sets:

$$\mathbb{Q} \cap \mathbb{Q}' = \varnothing \quad \mathbb{Q} \cup \mathbb{Q}' = \mathbb{R}$$

Let's think about why this makes sense: if the intersection was not the empty set, then this would mean there is some element x which is both rational and irrational. However, we know that's impossible, hence the intersection must be the empty set. On the other hand, if we take the union between the two, we can think of this process as adding the irrationals $\mathbb{Q}'$ back into the set of rationals, and since we constructed $\mathbb{Q}'$ by taking $\mathbb{Q}$ away from $\mathbb{R}$, it makes sense that adding them back would give us $\mathbb{R}$ back as well.

Because $\mathbb{Q}$ and $\mathbb{Q}'$ have the property that their combination makes $\mathbb{R}$ and they share no common elements, we say that they are complements of one another.[5]

Notation (Complement): If two sets A and B are complements of each other, we write $\overline{A} = B$ or $A^c = B$. The little c here stands for "complement."

Complements will be useful to us later in the probability section of this book, so for now, keep this in the back of your mind.

1.6 Cartesian Products

Now we've come to the second last thing about sets: the Cartesian product. Even though it may not seem like it, this is actually something you're familiar with already: you know how in algebra you write $\mathbb{R}^2$ to denote the real plane? That is a Cartesian product in disguise! I'll give the definition below:

Definition 1.10 (Cartesian Product): Given two sets A and B, the *Cartesian Product*, denoted $A \times B$, is the set of all pairs (x, y) such that $x \in A$ and $y \in B$. Equivalently:

$$A \times B = \{(a, b) \mid x \in A \wedge y \in B\}$$

Looking back now at $\mathbb{R}^2$, hopefully you can see why we say that this defines the 2D-plane of numbers. We write $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, and based on the definition above we know that it means all pairs (x, y) such that both x and y are real numbers. That's exactly the definition of the real plane!

Example 1.3

Given the set $A = \{1, 2\}$ and $B = \{2, 3\}$, the set $A \times B$ is written as:

$$A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$$

Notice the difference between this and a union: the point $(2, 2)$ exists here because we're pulling the first 2 from set A and the second 2 from set B. If we were to union the two sets, we'd get $\{1, 2, 3\}$, and not the pairs.

[5] Implicitly, we've defined the universe $\mathbb{U}$ to be $\mathbb{R}$ here. For the purposes of this book, we won't worry too much about what a universe is; it'll be very clear whether two sets are complements of each other.

1.7 Power Sets

Now we come to the last thing about sets: the power set. This is not a very important concept since it appears only once elsewhere in this book, so let's go over the definition, and we'll discuss it further when the time comes.

Definition 1.11 (Power Set): Given a set S, the power set, denoted by $\mathcal{P}(S)$, is the set of all subsets of S. Note that the empty set is also in $\mathcal{P}(S)$, as it's a valid subset of S.

Example 1.4

Given a set $A = \{1, 2, 3\}$, the power set is written as:

$$\mathcal{P}(A) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

You can check that each one of these are indeed subsets of A.

That's all for sets! If you don't understand everything that we've talked about here just yet, that's okay! Sets are a fairly abstract concept, intentionally so because they're meant to be a very general kind of mathematical object. Hopefully, when we start applying these concepts, things will make more sense.

PROPOSITIONAL LOGIC

Now that we've covered sets and how to construct them, let's take a look at one of the many ways we use them in propositional logic. In my opinion, propositional logic is one of the most important topics of CS70, because of how universal this language is throughout all areas of math and theoretical computer science. If you take any kind of theoretical upper division course (like CS170, EE126, EE127, etc.), you'll definitely encounter this language in those classes as well.

2.1 Propositions

At the heart of propositional logic, the basic building block that we're concerned with is what we call a **proposition**. A proposition is basically a sentence that is either true or false; the way you could think about is that it's a statement you can "propose" as a potential truth.

Example 2.1

The following are some examples of valid propositions:

- π is an irrational number.
- There are no real solutions x to the equation $x^2 + x + 1 = 0$.
- $1 + 1 = 5$.
- n is less than 10.

Remark : Notice that a proposition doesn't need to be true at all! The statement $1 + 1 = 5$ is a perfectly valid proposition, depsite it being blatantly false.

More rigorously, we label a proposition as a statement $P(n)$, which has some truth value based on the input to n.[1] In the first three statements above, even though they don't explicitly contain n as an input, they *implicitly* do – in the sense that they don't care about what the value of n is.

Because $P(n)$'s truth value is dependent on the input n, it should also make sense that $P(n)$ could be true for some values of n, and false for some others. Take the last proposition mentioned in the example:

$$P(n) = n \text{ is less than } 10$$

We know that when $n < 10$, then $P(n)$ is true, but when $n \geq 10$, then $P(n)$ is false. This is perfectly allowable in propositional logic. However, notice that there isn't a value of n for which $P(n)$ is true and false at the same time. This is known as the **law of the excluded middle**:

Theorem 2.1: Law of the Excluded Middle

Given a proposition $P(n)$, for every value of n, $P(n)$ is either true or false, but not both.

This principle should make intuitive sense: the whole point of coming up with propositions is so that we can talk about whether it's true or false for values of n, so if $P(n)$ could be true *and* false for some values of n, then how could we ever talk about the truth value of $P(n)$ rigorously?

2.2 Combining Propositions

Now that we know how to make propositions, let's talk about how we can combine propositions together to create new, more complex ones. In this vein, there are only three ways that we really combine propositions:

- **Conjunction:** combining two propositions with an "and", written like $R(n) = P(n) \wedge Q(n)$. Here, $R(n)$ is only true when $P(n)$ is true *and* $Q(n)$ is true.

[1] In this sense, you can almost think of $P(n)$ as a function based on the input n.

- **Disjunction:** combining two propositions with an "or", written like $R(n) = P(n) \vee Q(n)$. Here, $R(n)$ is true when either $P(n)$ is true *or* $Q(n)$ is true, or both.
- **Negation:** flipping the truth value of $P(n)$, written like $R(n) = \neg P(n)$. Here, $R(n)$ is true when $P(n)$ is false.

With these three methods, we can make any proposition we want!

2.2.1 Propositional Sentences

And now we come to the most important concept in propositional logic: the act of generating logical sentences from propositional statements. In a sense, constructing propositions $P(n)$ alone without combining them into a sentence is rather pointless, since we can't really do much with them. However, when we combine them into sentences, that's where we get our system of logic from. What do we mean by combining propositional sentences together? Let's consider the statement:

$$\text{If } n \text{ is an integer, then } n^2 \text{ is an integer.}$$

What do you notice here? This is basically the combination of two propositions! Specifically, if we let $P(n)$ be the statement "n is an integer" and $Q(n)$ be the statement "n^2 is an integer", then this statement basically simplifies to "If $P(n)$ holds, then $Q(n)$ holds". Mathematically, what we've just constructed is what's known as an **implication**, defined below:

Definition 2.1 (Implication): An *implication* between two propositional statements $P(n)$ and $Q(n)$ is equivalent to the statement "If $P(n)$, then $Q(n)$". We write that as $P(n) \implies Q(n)$.

Before we move on, let's fully understand what an implication is doing: remember that $P(n) \implies Q(n)$ is the same as saying "If $P(n)$ is true, then $Q(n)$ is true". So, another way you can understand that as is that *under the condition* that $P(n)$ is true, then $Q(n)$ is also true. Using the example we had above, we can say that *under the condition* that n is an integer, then n^2 is also an integer.

Remark : In terms of mathematical theorems that follow the form $P(n) \implies Q(n)$, this is what we mean as well. We first assume that $P(n)$ is true, then the theorem tells us that $Q(n)$ is true as well.

Along with $P \implies Q$, there's also two other sentences with P and Q that are commonly introduced here:

Definition 2.2 (Contrapositive, Converse): Given an implication $P \implies Q$, the *contrapositive* and *converse* are written as follows:

- **Contrapositive:** $\neg Q \implies \neg P$
- **Converse:** $Q \implies P$

Warning : Note that contrapositive and converse are not the same thing! For an implication $P \implies Q$, the contrapositive is $\neg Q \implies \neg P$, while the converse is $Q \implies P$. As we'll see in the next section, the contrapositive is logically equivalent to the original implication, whereas the converse is not.

There's one last detail about implications you need to know: if both $P(n) \implies Q(n)$ and $Q(n) \implies P(n)$ is also true, then this is what we call an **if and only if** statement. In English, we'd say "$P(n)$ if and only if $Q(n)$".

Notation (If and only if): Given two propositional statements $P(n)$ and $Q(n)$, if $P(n)$ is true if and only if $Q(n)$ is true, then we write $P(n) \iff Q(n)$.

An if and only if (also referred to as iff) statement is powerful because it gives us the ability to say for certain that if *either* $P(n)$ or $Q(n)$ is true, then the other is true automatically. Later when we visit proofs, you'll hopefully appreciate why this is such a powerful condition.

2.3 Logical Equivalence

Now that we can build an infinite number of propositional sentences, how can we tell whether two of these sentences are saying the same thing? As you'll discover, there *are* some propositional forms that initialy look very different, but are in

fact are logically equivalent (i.e. mean the same thing). These are particularly useful becuase it can sometimes drastically simplify how we go about proving statements.

How do we determine logical equivalence? Let's look at the theorem below:

Theorem 2.2: Logical Equivalence

If two propositional sentences P and Q have the same truth table, then they are *logically equivalent*.

Now what is a truth table? It's basically a table that summarizes the truth values that the sentence formed by P and Q can take on. Suppose we have the statements P and Q, and we look at the sentence $P \implies Q$:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

This shows us that given the truth values of P and Q, what the truth value of $P \implies Q$ is. How did I come up with this table? Let's go through each combination of P and Q and see if $P \implies Q$ makes sense:

- $P = \text{T}, Q = \text{T}$. In this case, it is indeed true that a true statement implies a true statement, so this one makes sense.
- $P = \text{T}, Q = \text{F}$. True statements should only imply other true statements, since we want our mathematics to be logically consistent (i.e. truth implies truth). Therefore, a true statement cannot imply a false one, hence the truth value being false.
- $P = \text{F}, Q = \text{T/F}$. The last two cases here both fall under the same category: both of these fall under the category where our initial statement P was false. Imagine this: if you started off a proof with a false premise, then you can ostensibly prove anything you wanted, even false statements. Therefore, both the implications here are assigned true values.

Now that we've looked at $P \implies Q$, let's also take a look at the truth table for $\neg P \vee Q$:

P	Q	$\neg P \vee Q$
T	T	T
T	F	F
F	T	T
F	F	F

Notice that $P \implies Q$ and $\neg P \vee Q$ take on the same truth values given the same truth values to P and Q! Because they have the same truth table, then we say that $P \implies Q$ and $\neg P \vee Q$ are *logically equivalent*.

Notation (Logical Equivalence): If two propositional sentences A and B are logically equivalent, then we write that as $A \equiv B$.

In our case, we'd write $P \implies Q \equiv \neg P \vee Q$. Another sentence which is logically equivalent to $P \implies Q$ is the contrapositive:

$$\neg Q \implies \neg P$$

This fact is particularly useful since in proofs it's sometimes easier to prove $\neg Q \implies \neg P$ than $P \implies Q$, and because they're logically equivalent statements, proving one proves the other as well!

Exercise 2.1

Verify that $P \implies Q$ and $\neg Q \implies \neg P$ have the same truth tables.

2.4 Quantifiers

We've covered how to make propositional sentences $P(n)$, now it's time to focus on the part with n: how do we specify to the reader what values can n take on? This is the role of quantifiers in propositional phrases.

There are only two quantifiers in propositional logic:

- **Universal:** Denoted by $\forall$, it refers to all the elements of a particular set we define.
- **Existential:** Denoted by $\exists$, it refers to the existence of an object within a set of our choice.

Now we are finally ready to fully create our first propositional logic statement: we're going to transform the sentence:

$$\text{If } n \text{ is an integer, then } n^2 \text{ is an integer}$$

completely into propositional language. To do this, the first thing we'll want to do is to tell the reader what set of numbers n lives in: in this case, it's the integers. Next, the statement makes no reference to the existence of a particular n, so we'll want to use the universal quantifier $\forall$ here. Finally, as before, let $P(n)$ be the statement that n is an integer, and $Q(n)$ be the statement that $Q(n)$ is an integer. Then, we can write:

$$(\forall x \in \mathbb{Z})(P(n) \implies Q(n))$$

And that's the complete transformation of our sentence into mathematical terms! The parentheses here aren't absolutely necessary; you'll see some textbooks that don't use them at all, but I use them here becuase I think they're useful to highlight the different parts of our phrase.

The box below shows a more complex sentence translation, and I encourage you to study it because it involves a technique that is very common in propositional logic.

Example 2.2

Let's try converting the following phrase into propositional logic:

$$\text{There exists only two distinct real solutions to the equation } x^2 - 1 = 0.$$

Where do we even start with this one? First, let's handle the fact that there are two real solutions, and worry about the "only" keyword later. To write the fact that there are two distinct solutions, what we can do is say instead is that there are two numbers x, y such that $x^2 - 1 = 0$ and $y^2 - 1 = 0$, and $x \neq y$. Written in propositional logic, this is what the phrase looks like so far:

$$(\exists x, y \in \mathbb{R})(x^2 - 1 = 0 \wedge y^2 - 1 = 0 \wedge x \neq y)$$

Now, how do we say that there are "only" two solutions? The trick is to first *suppose* that there is a third solution z, then say that if z also solves this equation, then z is either x or y.[a] Therefore, the full equation is:

$$(\forall z \in \mathbb{R})(\exists x, y \in \mathbb{R})(x^2 - 1 = 0 \wedge y^2 - 1 = 0 \wedge x \neq y) \wedge (z^2 - 1 = 0 \implies z = x \vee z = y)$$

[a] Try convincing yourself as to why this is valid.

And that's all for quantifiers! The final sentence we've made in this example box is a little complex, but spend some time with it, and see if you can identify the purpose of each piece in the sentence and how we joined them together.

2.5 De Morgan's Laws

De Morgan's laws refer to how the negation operator $\neg$ interacts with the other objects we've explored in this chapter. In terms of the conjunction $\wedge$ and disjunction $\vee$ symbols, De Morgan's laws says that:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q \quad \neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

You can check using truth tables that these are in fact logically equivalent. The reason these laws are so powerful is because they allow us to potentially discover that two statements are in fact logically equivalent, without having to go through the pain of making a truth table.

What about existential quantifiers? How does negation affect those symbols? Well, let's say you have a statement $\forall x P(x)$, in other words that $P(x)$ is true for all values of x. What would the negation of this statement be? One way to say the opposite of this statement is to say that there *exists* a value of x such that $P(x)$ is true, or equivalently that $\neg P(x)$ is true. And with that, we've discovered how negation works with quanitifers:

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x)$$

PROOFS

In this chapter, we'll talk about the proof techniques you'll have to be familiar with in this class. Before we get to that though, I want to emphasize that this chapter alone might be the single most important chapter in this entire book, especially if you intend to pursue any theory-heavy course in the future.

To really explain why proofs are so important, we have to look at the structure upon which mathematical logic is built. At the very base, we have a set of axioms, which are a set of statements that are taken to be true without proof. These axioms serve as the foundation of all mathematical logic; without them, we wouldn't have anything to build off of.

The way we build off these axioms is through proofs – a process in which we take true statements (either axioms or previously proven statements), and massage them to arrive at a novel conclusion. At its core, what we are really doing is asking "given the set of true statements we have, what else can we *provably show* is also true?" This is the fundamental question that pushes the boundaries of mathematics.

3.1 Methods of Proof

Now, how do we actually go about proving things? Well, we will generally be asked to prove a statement of the form $P(n) \implies Q(n)$, so we need to show that *if* $P(n)$ is true, then $Q(n)$ is also true. There are many different ways we can do that, which we will go over now.

Also, I should mention that while I will try to motivate the thought process behind choosing any particular proof method for a problem, ultimately the process does take a lot of practice and there's no amount of explaining I can do to remedy that.

3.1.1 Direct Proof

Perhaps the most obvious method of proof is called a *direct proof*. Basically, this method is to start wtih the assumption that $P(n)$ is true, and work our way towards the statement $Q(n)$. Let's look at the example below:

Example 3.1

Let's prove the statement that if $a \mid b$,[a] then $a \mid kb$ for any integer k.

To prove this using the direct proof method, all we have to do is start with the statement $a \mid b$, and show that for any integer k, that $a \mid kb$ as well. Starting with $a \mid b$, another way we can write that is that b is represented as some integer multiple of a, so $b = na$ for some integer n. With this in mind, the integer kb is now written as $kb = kna$, and since k is also an integer, this implies that kb is also an integer multiple of a. Therefore, $a \mid kb$! And that concludes the proof.

[a] The $\mid$ symbol here stands for "divides", basically meaning that $\frac{b}{a}$ is an integer.

The hallmark of a direct proof is that we start with the assumption given to us in the "if" statement: in the example above, this corresponds to $a \mid b$. Then, we take this assumption in hand, and use the information provided by the assumption to show that the "then" statement, that $a \mid kb$ in our example, is also true.

Usually, one of the things to look out for when trying to directly prove something is to see whether the "if" clause gives you information that looks like it can be applied to prove the statement. Looking back at the example, we see that since both the "if" and "then" statements involved looking at divisibility, then it isn't a stretch to imagine that we could take the information of $a \mid b$ and directly massage it into the conclusion that $a \mid kb$ as well.

3.1.2 Contrapositive

Along with a direct proof, the method by contrapositive also involves proving a direct implication. The principle of the contrapositive is as follows: suppose you're asked to prove the statement $P \implies Q$. You could go about this directly, but remember in section 2.3 we introduced the idea of a contrapositive, $\neg Q \implies \neg P$, and because they have the same truth tables (see exercise 2.1), then proving $\neg Q \implies \neg P$ is the same as proving $P \implies Q$! The reason this is convenient is that sometimes proving $\neg Q \implies \neg P$ is far easier than $P \implies Q$.

We'll illustrate this with an example:

Example 3.2

Prove that if a is an irrational number, then for all integers k, ka is also an irrational number for all nonzero integers k.

Proving this via a direct proof would be relatively difficult – even though we know that a is irrational, there is no tangible information that allows us to use this information and prove that ka is irrational. On the other hand, consider the contrapositive statement: if ka is a rational number, then a must be a rational number for all integers k. This is a far easier statement to prove.

Recall that if ka is a rational number, then $ka = \frac{p}{q}$ where p and q are integers. We can then express $a = \frac{ka}{k} = \frac{p}{kq}$, and since k is an integer, kq is also an integer, and hence the fraction $\frac{p}{kq}$ is rational, as desired.

This problem illustrates perfectly why the contrapositive may be a useful tactic for some proofs. Take some time to think about how difficult the forward direction would be: we know that a is irrational, but how do we even begin representing what an irrational number is? Even if we could figure out how to do this, how do we go about showing that multiplication by any integer k is still irrational?

On the other hand, consider the simplicity of the contrapositive stastement. We know very concretely how to represent ka if it were rational, and from there division by k is also well defined so we can conclude that $\frac{p}{kq}$ is also rational, which completes the proof.

3.1.3 Contradiction

While direct and contrapositive proofs do have their place, probably by far the most popular proof technique is a proof by contradiction. The essence of this proof is exactly what the name suggests: instead of proving that something is true, you show that it can't be untrue instead. The basic structure of a proof by contradiction is as follows: suppose you wanted to prove that $A \implies B$. Then, to prove by contradiction, we first assume that $A \implies \neg B$. Then, we prove that this is impossible by showing that $A \implies B$ and $A \implies \neg B$ must both be true at the same time – by the law of the excluded middle (theorem 2.1), both of these cannot be true at the same time. Therefore, $A \implies \neg B$ must be false, and hence we've proven our original statement.

3.1.4 Induction