MATH 240 Fall 2024

notes by

MARCEL GOH

A note on these notes. After each class, this document will be updated with the new material that was just covered. The datestamps in the left margin indicate when the notes from each day start. Subsections labelled with a $*$ are optional. This document is heavily based on notes by Jeremy Macdonald, but any errors are likely my own. Please email me if you find any.

I. FOUNDATIONS

Die Mathematik ist in ihrer Entwickelung völlig frei
und nur an die selbstredende Rücksicht gebunden,
dass ihre Begriffe sowohl in sich widerspruchslos sind,
als auch in festen durch Definitionen geordeneten Beziehungen
zu den vorher gebildeten,
bereits vorhandenen und bewährten Begriffen stehen.

— GEORG CANTOR, *Grundlagen einer allgemeinen Mannigfaltigkeitslehre* (1883)

1. Set theory

A *set* is a collection of distinct objects, called its *elements* or its *members*. If x is a member of set A, then we write $x \in A$, and if x is not an element of A, then we write $x \notin A$. Sets can be written by listing out its elements. For example,

$$\left\{ 1, 4, 7, 10, \sqrt{782} \right\}$$

and

$$\left\{ \{1, 2\}, \pi, \{4\} \right\}$$

are both sets (the second example shows that sets can themselves contain other sets). The order of the elements is not important, and duplicate elements are ignored (so $\{1, 2\} = \{2, 1\} = \{1, 1, 2\}$). The notation using $\{$ and $\}$ is useful for defining small, concrete examples, but expressing large sets can become very cumbersome. The first way one can describe larger sets is to use the $\ldots$ symbol and the power of suggestion. For instance, anyone faced with the notation

$$A = \{1, 3, 5, 7, 9, \ldots\}$$

can quickly guess that this set is supposed to contain all the positive odd integers. We can also use $\ldots$ to define finite sets. Most Canadians will be able to tell you that the set

$$\{\text{Alberta}, \text{British Columbia}, \ldots, \text{Yukon}\}$$

of provinces and territories contains 13 elements. But this notation inherently produces some ambiguity. For example, since the sequence of positive palindromic binary numbers starts $1, 3, 5, 7, 9, 15, 17, 21, 27, \ldots$, we are left with some doubt as to whether the set A above should be the set of odd numbers or the set of palindromic binary numbers.

But there is another, less ambiguous way to define large sets. It is called set-builder notation and it refers to any construction of the form

$$\left\{ x \in U : P(x) \right\},$$

where x is a variable, U is a set, and P is a statement about x. The resulting set contains *all x such that $P(x)$ holds*. For example, letting $\mathbf{N}$ denote the set $\{0, 1, 2, 3, \ldots\}$ of counting numbers (more on this later), to define the set of all odd numbers, we can write

$$A = \{x \in \mathbf{N} : \text{there exists } k \in \mathbf{N} \text{ such that } x = 2k + 1\}.$$

Note that the statement $P(x)$ must contain x, but it may also contain other previously defined symbols, as well as new symbols defined within the statement (such as k in the example above).

Special sets of numbers. There are certain infinite sets of numbers that are used so often as to be given special bold notation. Back in elementary school,

you learned to use the counting numbers $0, 1, 2, 3, \ldots$. We already saw this set in the previous paragraph; in the business, this set is known as the *natural numbers*, because if you go on a nature hike you can use them to count the number of bluebells, donkeys, etc. that you see. (Many mathematicians use the symbol $\mathbf{N}$ to denote this set without zero. When in doubt, clarify with the person you're talking to; in this class, $0 \in \mathbf{N}$.)

Sometime towards the start of junior high you were introduced to the concept of natural numbers. The set

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

is called the set of *integers* or *whole numbers*. (The word *integer* just means "whole" in Latin; cf. French *entier*. We use the letter $\mathbf{Z}$ because of the German word *Zahl* meaning "number.")

Even before you learned about negative numbers, you probably learned about fractions. They can be defined in set-builder notation as a collection of ratios of integers, where the denominator is not zero:

$$\mathbf{Q} = \{p/q : p, q \in \mathbf{Z}, q \neq 0\}.$$

(The nitpicky reader will notice that p/q is not stipulated to be a member of any set here. This is because a rigorous definition of $\mathbf{Q}$ involves quotienting out by an equivalence relation, which we don't know how to do yet.) This is the set of *rational numbers*. Remember that sets only contain distinct elements, so $2/3$, $4/6$, $6/9$, etc. are all considered the same rational number.

Lastly, we have the set $\mathbf{R}$ of real numbers. Constructing this set using only notions from set theory and logic is quite the byzantine task and well outside the scope of this course, but you can think of $\mathbf{R}$ as the set of decimal numbers with a finite number of digits to the left of the decimal point, and a possibly infinite number of digits to the right of the decimal point.

A set of numbers near and dear to many mathematicians' hearts is the set of *prime* numbers P, defined by

$$P = \big\{p \in \mathbf{N} : p \geq 2, \text{ and if } p = ab \text{ then } \{a, b\} = \{1, p\}\big\}.$$

(You may have met a different definition of prime numbers in the past. Pause a moment and convince yourself that the statement above defines the set of prime numbers as you know it.)

Set inclusion. When we use set builder notation $B = \big\{x \in A : P(x)\big\}$, every element of B is necessarily a member of the set A as well, since B is defined to be the set of all x in A satisfying $P(x)$. This is one way in which we can obtain a *subset* of another set. More generally, we write $B \subseteq A$ if every element of B is also an element of A, and $B \supseteq A$ if every element of A is an element of B. Sometimes, if $B \supseteq A$, we say that B *contains* A, or B *includes* A. For example, we have the chain

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

for the special sets of numbers defined earlier.

Symbols like $\subseteq$, $\supseteq$, and $=$ (that are used to produce statements) can be negated with a slash; for example, if there is some element of B that is not an element of A, then we write $B \nsubseteq A$.

The concept of set inclusion is important, because the most common way to prove that two sets A and B are equal is to show that A is a subset of B, then show that B is a subset of A. We illustrate this with the following example.

Proposition 1. *The sets*

$$A = \{x \in \mathbf{Z} : \text{there exists } k \in \mathbf{Z} \text{ such that } x = 2k + 1\}$$

and

$$B = \{x \in \mathbf{Z} : \text{there exists } l \in \mathbf{Z} \text{ such that } x = 2l + 5\}$$

are equal. (Both are different ways of expressing the set of all odd integers.)

Proof. Let $x \in A$. Then there exists $k \in \mathbf{Z}$ such that $x = 2k + 1$. Letting $l = k - 2$, we find that l is an integer (since k was). Furthermore,

$$x = 2k + 1 = 2k - 4 + 5 = 2(k - 2) + 5 = 2l + 5.$$

We have found l such that $x = 2l + 5$, so $x \in B$. This shows that $A \subseteq B$.

On the other hand, let $x \in B$, so that there exists $l \in \mathbf{Z}$ such that $x = 2l + 5$. Now we let $k = l + 2$; $k \in \mathbf{Z}$ since $l \in \mathbf{Z}$. We have

$$x = 2l + 5 = 2l + 4 + 1 = 2(l + 2) + 1 = 2k + 1.$$

This shows that $x \in A$, and we have proved that $B \subseteq A$. This combined with the previous paragraph shows that $A = B$. ∎

The above result is not so important, but pay attention to the structure of this proof. It is called a "proof by double inclusion," since we have shown that A includes B and B includes A.

Set operations. Now we describe a number of operations that may be performed on sets to produce other sets. They can all be built up from the following two operations.

- The *union* $A \cup B$ of two sets A and B is the set of all elements that are either in A or in B (or both).
- The *intersection* $A \cap B$ of A and B is the set of all elements that are in both A and B.

As an example, if $A = \{1, 2, 4\}$ and $B = \{1, 3, 5\}$, then $A \cup B = \{1, 2, 3, 4, 5\}$ and $A \cap B = \{1\}$.

To avoid logical difficulties, we always assume that the sets we're working with are a subset of some larger ambient set U, often called the *universe*. Once we know what U is, we may define the *complement* of a set A to be the set $\overline{A}$ of

all the elements in U except those that are in A. So if $U = \{1, 2, 3, 4, 5\}$ in the example above, then $\overline{A} = \{3, 5\}$ and $\overline{B} = \{2, 4\}$. What about $\overline{A \cup B}$? Well since $A \cup B$ is all of U, its complement must be empty, and we can denote it $\{\}$. This is one valid notation for the *empty set.* The other is $\emptyset$.

Now is a good time to define the cardinality $|A|$ of a set A. This is the number of elements in it, so $|A| = |B| = 3$ in our example, and $|A \cup B| = 5$, etc. We have $|\emptyset| = 0$, and it is possible for the cardinality of a set to be infinity; for example, $|\mathbf{N}| = \infty$. We also have $|\mathbf{R}| = \infty$, but this infinity is, in some sense, larger than $|\mathbf{N}|$. (More on that later.)

Next, we define the *difference* $B \setminus A$ (sometimes $B - A$) of two sets. This is the set of all elements in B that are *not* in A. So, using the complement notation we just learned about, we can express $B \setminus A = B \cap \overline{A}$. It is not necessary that A be a subset of B. In the small example above, we have $A \setminus B = \{2, 4\}$ and $B \setminus A = \{3, 5\}$.

Lastly, we define the *symmetric difference* $A \triangle B$ of two sets A and B to be the set of all elements that are either in A or in B *but not both.* Invoking the above example one last time, we have $A \triangle B = \{2, 3, 4, 5\}$. We can express it as using unions, intersections, and complements as

$$A \triangle B = (A \cup B) \cap \overline{A \cap B}. \tag{1}$$

To practise using all the different operations we just learned, convince yourself that the following are three more valid ways to express the symmetric difference:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = \overline{\overline{A \cup B} \cup (A \cap B)}$$

More set identities abound. We state the following proposition without proof; you should try going though this list and convincing yourself that each identity holds, for all sets A, B, and C. (This is a great way of practising proofs by double inclusion.)

Proposition 2. *Let A, B, and C be subsets of a universe U. Then*

   i) $A \cap U = A$ and $A \cup \emptyset = A$;

  ii) $A \cup U = U$ and $A \cap \emptyset = \emptyset$;

 iii) $A \cup A = A$ and $A \cap A = A$;

 iv) $\overline{\overline{A}} = A$;

  v) $A \cup B = B \cup A$ and $A \cap B = B \cap A$;

 vi) $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$;

vii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

viii) $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$; and

 ix) $A \cup \overline{A} = U$ and $A \cap \overline{A} = \emptyset$. ∎

These laws have names, some of which we will use more often than others: (i) is called the identity law, (ii) the domination law, (iii) the idempotent law,

(iv) the law of double negation, (v) the commutative law, (vi) the associative law, (vii) the distributive law, (viii) the absorption law, and (ix) the complement law.

*__Analogy with addition and multiplication.__ Some of these laws bear some resemblance to laws about numbers that you already know. As an exercise, replace $\cup$ with $+$ (addition), $\cap$ with $\cdot$ (multiplication), $\overline{A}$ with $-A$ (negation), U with 1, and $\emptyset$ with 0 in all the formulas above, and now assume that A, B, and C are arbitrary real numbers. Which identities still hold in the number setting, and which ones don't? As a more advanced exercise, try replacing $\cup$ with $\triangle$ in the identities above (some statements will have to be tweaked a bit so that they're actually true, some won't). Now do the same replacement as before, except replace $\triangle$ with $+$. You will find that many more identities carry over.

03.IX __De Morgan's laws.__ There are two important laws relating complements with union and intersection. We shall state them as a proposition, this time giving a proof (of one of them).

__Proposition 3__ (*De Morgan's laws*). *Let A and B be sets. Then*

i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$*; and*

ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof. Let $x \in \overline{A \cup B}$. This means that x does not belong to the union of A and B, x cannot be in A, nor can it be in B. Since $x \notin A$, $x \in \overline{A}$, and since $x \notin B$, $x \in \overline{B}$. Therefore, $x \in \overline{A} \cap \overline{B}$. This shows that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Now assume that $x \in \overline{A} \cap \overline{B}$. So $x \in \overline{A}$ and $x \in \overline{B}$, meaning that $x \notin A$ and $x \notin B$. Since x is in neither A nor B, it is also not a member of the union $A \cup B$. We conclude that $x \in \overline{A \cup B}$. We have shown that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$, which fact, combined with the previous paragraph, completes the proof of (i).

The proof of (ii) is similar and left to the reader as an exercise. ∎

Armed with all of these laws, we are able to perform lots of mechanical set manipulations to simplify expressions. For example, consider the expression

$$\big((A \setminus B) \cup A\big) \cap \overline{A \cap \overline{B}}.$$

Since $A \setminus B = A \cap \overline{B}$ and invoking the second De Morgan law on the right of the intersection yields

$$\big((A \cap \overline{B}) \cup A\big) \cap (\overline{A} \cup B).$$

Now, we can use absorption on the left-hand side to obtain

$$A \cap (\overline{A} \cup B),$$

and then distributing gives us

$$(A \cap \overline{A}) \cup (A \cap B) = \emptyset \cup (A \cap B) = A \cap B.$$

We thus see that the nasty expression $\bigl((A \setminus B) \cup A\bigr) \cap \overline{\overline{A} \cap \overline{B}}$ is simply another way of writing $A \cap B$.

The Cartesian product and power set. From the real line $\mathbf{R}$, we can geometrically construct the Cartesian plane $\mathbf{R}^2$ by lining up parallel copies of $\mathbf{R}$, one for each element of the original line and all parallel to the original line. Notationally, $\mathbf{R}^2$ is the set of all ordered pairs (a, b), where $a, b \in \mathbf{R}$. Generalising this, for any sets A and B we can define the *Cartesian product* $A \times B$ to be the set

$$A \times B = \bigl\{(a, b) : a \in A, b \in B\bigr\}.$$

We sometimes write A^2 for $A \times A$, and more generally A^n for the n-fold Cartesian product of A with itself. (This explains the notation $\mathbf{R}^2$ for the Cartesian plane, and $\mathbf{R}^n$ for the n-dimensional vector space over $\mathbf{R}$.) Note that $A \times B$ is not equal to $B \times A$ in general.

Proposition 4. *If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.*

Proof. The set $A \times B$ consists of all ordered pairs (a, b) where $a \in A$ and $b \in B$. There are $|A|$ choices for a, and for a, there are $|B|$ ways to pair it with a b from B. So there are $|A| \cdot |B|$ pairs in total.   ∎

Now we define the *power set*. For a set A, this is the set of all subsets of A, and is commonly denoted by $\mathcal{P}(A)$ or 2^A. (We will use the latter notation in these notes.) In set-builder notation, we have

$$2^A = \{X \subseteq U : X \subseteq A\}.$$

As an example, if $A = \{1, 2, 3\}$, then

$$2^A = \bigl\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\bigr\}.$$

Note that even though, say, $1 \in A$, we do not have $1 \in 2^A$. We do, however, have $\{1\} \in 2^A$.

Another example is $2^{\mathbf{Z}}$, the set of all subsets of integers. If P is the set of primes, then $P \in 2^{\mathbf{Z}}$. Also in $2^{\mathbf{Z}}$ is the set $S = \{n^2 : n \in \mathbf{Z}\}$ of square numbers.

There is a way of encoding subsets with strings of 0s and 1s. Suppose we have a set

$$\{-3, 1, 7, 19, 23\}.$$

Fixing this order of the elements, for any arbitrary subset of this set, we can associate to it a binary string. Consider the subset $\{1, 19, 23\}$. This corresponds to the binary string 01011: since the first element, 3, is not in the subset, we write a 0. Then 1 is in the subset, so we write a 1, and so on. This is a reversible process. Given a binary string of length 5, say, 00101, we can reconstruct the subset that corresponds to it. The first two 0s mean that -3 and 1 do not belong to the set, but 7 does, 19 doesn't, and 23 does. So the subset is $\{7, 23\}$. In this way we see that there is a one-to-one correspondence between the elements of 2^A and binary strings of length $|A|$. We'll use this fact in the proof of the following proposition.

Proposition 5. *If A is finite, then $|2^A| = 2^{|A|}$.*

Proof. We just saw that there is a one-to-one correspondence between elements of 2^A and binary strings of length $|A|$. So it suffices to count the number of binary strings of length $|A|$. Well, each digit can be either 0 or 1, and there are $|A|$ digits, so the number of strings is

$$\underbrace{2 \cdot 2 \cdots \cdots 2}_{|A| \text{ times}} = 2^{|A|}. \quad \blacksquare$$

Counterexamples in proofs. We finish this subsection with a little example problem. *Is it true that $2^A \cup 2^B = 2^{A \cup B}$ for all sets A and B?*

Let's start by trying to prove the statement is true. As usual, we will attempt a double-inclusion proof. Let $2^A \cup 2^B$. This means X is either a subset of A or it is a subset of B. Either way, X is a subset of $A \cup B$, so $X \in 2^{A \cup B}$. So far so good; we have proved that $2^A \cup 2^B \subseteq 2^{A \cup B}$.

Now we try the other direction. Let $X \in 2^{A \cup B}$. So X is a subset of $A \cup B$. From here we want to say that X must be a subset of A or it must be a subset of B, but is that necessarily true? It is possible that X is contained slightly in A and slightly in B. So we have failed to prove that $2^{A \cup B} \subseteq 2^A \cup 2^B$ in general. But just because we have failed to prove that something is true doesn't mean we have proved it is false!

To actually prove that $2^{A \cup B} \subseteq 2^A \cup 2^B$ doesn't hold in general, we need to find a *counterexample*. That is, we need to construct sets A and B such that the statement is false. In this case, we can let $A = \{1, 2\}$, $B = \{3, 4\}$, so that $A \cup B = \{1, 2, 3, 4\}$. Then the set $\{1, 3\}$ is a subset of $A \cup B$ but is not a subset of A and it is not a subset of B. In other words, $\{1, 3\} \in 2^{A \cup B}$ but $\{1, 3\} \notin 2^A \cup 2^B$, proving that $2^{A \cup B} \not\subseteq 2^A \cup 2^B$.

05.IX **Russell's paradox.** Earlier, we said that the sets we are working with need to be a subset of a universe U, which has already been proven to be a set. We gave lots of ways to make sets out of new sets, such as the union and intersection operations, etc. Starting with the assumption that the empty set $\emptyset$ is a set, it is possible to define the set of natural numbers as follows. We can define $0 = \emptyset$, $1 = \{0\}$, and $2 = \{0, 1\}$, and so on. Now we take the set of all of these, and call this $\mathbf{N}$. (We can also define addition and multiplication on these set-theoretic "numbers" so that they behave like addition and multiplication do on $\mathbf{N}$.) From here we can do more funky stuff to define $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$, and prove that these are all sets (you can see this in a higher-level course on set theory, if you're interested). So there isn't much of a problem with all the sets we have played with so far; they are all subsets of things that are already known to be sets.

Ungodly things can happen if we don't stick by these rules. An example, due to Bertrand Russell, is the "set"

$$R = \{\text{sets } X : X \notin X\}.$$

In plain English, R is defined to be the set of all sets that contain themselves. This is not a subset of any known thing, so by our criterion above we would not consider it a set. But supposing it is, let us ask ourselves the following question. Does R contain itself? If it does not, then $R \notin R$, so R would be a set that satisfied the condition of R, so $R \in R$. But on the other hand, if $R \in R$, then R violates the condition defining R, so $R \notin R$. Round and round we go in a circle of contradiction.

Such is the price of meddling with "sets" that aren't subsets of known sets. This also shows that there is no such thing as "the set of all sets."

2. Propositional logic

A *proposition* is a statement that is true or false. For example "8 is even" is a statement we know to be true, and "8 is prime" is a statement we know to be false. The statement "n is prime" is not a proposition because its truth or falsity depends on what n is. The statement "$2^{2^{240}} - 1$ is prime" is a proposition, because it is either true or false (even though you or I might not know which one it is).

A *propositional variable* or a *boolean variable* is a variable which can take either the value 0 or 1, where 0 means "false" and 1 means "true." Usually we use letters p, q, and r to denote propositional variables. The simplest logical operator is negation, defined by the table

p	$\neg p$
0	1
1	0

This is also called the NOT operator, since if p is true, then $\neg p$ is false, and vice versa. Next is *conjunction*, which has the table

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

This is also called the AND operator, because $p \wedge q$ is true if and only if p and q are both true. The OR operator, also called *disjunction*, has the table

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

We see that $p \vee q$ is true if p or q is true (or both). The symbol $\vee$ is meant to recall the Latin word *vel*, meaning "or." (One of the most important early treatises on mathematical logic and set theory was *Arithmetices principia, nova methodo exposita*, published in Latin in 1889 by Giuseppe Peano. It established the now-standard axiomatisation of the natural numbers.)

On the other hand, in English, we often use the word "or" to mean an *exclusive* or; that is, either p and q are true but not both. In mathematics, on the other hand, "or" is usually *inclusive*, so both p and q are allowed to hold at the same time. It is possible to express the exclusive disjunction (often called XOR) by a table, however. We will use the symbol $\oplus$ for this operator, and its table looks like this:

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

So $p \oplus q$ is true if p is true or q is true, but not both.

A *formula* is an expression containing propositional variables, 0, 1, logical operators, and parentheses. The formula must syntactically make sense; for instance, $0(\vee \wedge q\neg$ is not a formula. Just as in ordinary mathematical notation, parentheses are used to clarify which operators should be evaluated first. We will assume that negation applies first, but an expression such as $p \vee q \wedge r$ is ambiguous. (In many programming languages, conjunction has higher priority than disjunction, but in this class, just add parentheses to clarify.)

Above we have illustrated the basic logical operators by writing out their *truth tables*. These are tables that give the value of a formula for all possible values of its variables. We can write truth tables for more complex formulas as well:

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg(p \wedge q) \oplus q$
0	0	0	1	1
0	1	0	1	0
1	0	0	1	1
1	1	1	0	1

Strictly speaking, the third and fourth columns are not necessary, but these intermediary columns help us verify the accuracy of the following ones.

Two formulas f_1 and f_2 are said to be *logically equivalent* if they have the same truth table; that is, they produce the same output if given the same input. In this case we write $f_1 \equiv f_2$. For example, let $f_1 = \neg(p \wedge q) \oplus q$, the formula

whose truth table is illustrated above. Now let $f_2 = p \vee \neg q$. Its truth table is

p	q	$\neg q$	$p \vee \neg q$
0	0	1	1
0	1	0	0
1	0	1	1
1	1	0	1

,

so we conclude that $f_1 \equiv f_2$. As a larger example, suppose we want to find all values of p, q, and r such that

$$f = (p \vee q) \wedge (\neg q \vee \neg r)$$

evaluates to 1. The truth table

p	q	r	$p \vee q$	$\neg q \vee \neg r$	f
0	0	0	0	1	0
0	0	1	0	1	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	0

shows that f evaluates to 1 precisely when

$$(p, q, r) \in \big\{ (0, 1, 0), (1, 0, 0), (1, 0, 1), (1, 1, 0) \big\}.$$

To write out the truth table for a formula with n variables, we need 2^n rows, so this method is unsuitable for formulas with more than three or four variables.

Simplifying logical formulas. Just as we have rules for simplifying set expressions, there are ways to turn complicated logical formulas into simpler ones that are logically equivalent. What might surprise you is that the rules turn out to be exactly the same! To see the basis for this correspondence, consider the definition of a union of sets A and B. In set-builder notation, this is

$$A \cup B = \{x \in U : x \in A \text{ or } x \in B\}.$$

The "or" in the definition suggests that $\cup$ is intimately related to the $\vee$ operation in propositional logic. Repeating this process, we have the "dictionary"

Set theory	Propositional logic
sets A, B	variables p, q
unions $A \cup B$	disjunctions $p \vee q$
intersections $A \cap B$	conjunctions $p \wedge q$
complements $\overline{A}$	negations $\neg p$
symmetric differences $A \triangle B$	exclusive disjunctions $p \oplus q$
the empty set $\emptyset$	0
the universe U	1

Exploiting this connection, we have the following analogue of Proposition 2.

Proposition 2. *Let p, q, and r be propositional variables. Then*

   i) $p \wedge 1 \equiv p$ *and* $p \vee 0 \equiv p$;

  ii) $p \vee 1 \equiv 1$ *and* $p \wedge 0 \equiv 0$;

 iii) $p \vee p \equiv p$ *and* $p \wedge p \equiv p$;

 iv) $\neg\neg p \equiv p$;

  v) $p \vee q \equiv q \vee p$ *and* $p \wedge q \equiv q \wedge p$;

 vi) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ *and* $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r)$;

vii) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ *and* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$;

viii) $p \vee (p \wedge q) \equiv p$ *and* $p \wedge (p \vee q) \equiv p$; *and*

 ix) $p \vee \bar{p} \equiv 1$ *and* $p \wedge \bar{p} \equiv 0$. ▮

Since they are essentially the same as their set equivalents, the names of these laws are the same as in the realm of sets. We also have the propositional equivalent of De Morgan's law, which states that

 x) $\neg(p \vee q) \equiv \neg p \wedge \neg q$ *and* $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

Using these rules, we can now show that $\neg(p \wedge q) \oplus q \equiv p \vee \neg q$, which we already saw earlier from their truth tables. First we observe that

$$p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q), \tag{2}$$

which is analogous to the identity (1) for symmetric differences. So

$$
\begin{aligned}
\neg(p \wedge q) \oplus q &\equiv \big(\neg(p \wedge q) \vee q\big) \wedge \neg\big(\neg(p \wedge q) \wedge q\big) \\
&\equiv (\neg p \vee \neg q \vee q) \wedge \big((p \wedge q) \vee \neg q\big) \\
&\equiv (\neg p \vee 1) \wedge \big((p \vee \neg q) \wedge (q \vee \neg q)\big) \\
&\equiv 1 \wedge \big((p \vee \neg q) \wedge 1\big) \\
&\equiv p \vee \neg q,
\end{aligned}
$$

where in the first line we use (2), in the second line we use De Morgan's law twice, in the third line we use the complement and distributive laws, the fourth line we use the domination and complement laws, and in the last line we use the identity law (twice). (It is not super important to remember the names of all these laws, as long as you remember their statements, but you may actually find it is easier to remember the names along with the statements, just as it might be easier to remember faces of people you've met if you also know their names.)

10.IX   **Conditional and biconditional.** We now examine the *conditional* logical relation IF p THEN q. It is denoted by $p \Rightarrow q$ and its truth table is given by

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

.

Within the conditional statement, p is called the *antecedent*; this is the assumption. The statement that is asserted, conditional that the antecendent holds, is called the *consequent* q. You can quickly check that the relation $p \Rightarrow q$ is equivalent to $\neg p \vee q$. This fact is useful when performing mechanical simplifications. In English, the statement "if p then q" asserts a causal relation between p and q. Take a moment and reconcile this idea with the truth table above. It is normal to get a little tripped up if it's your first time seeing this table. In the first row, q doesn't even happen, so it might feel weird to say that p has "caused" q to happen in this case, and in the second row, p is not true and q is true, so it might seem odd that we have set $p \Rightarrow q$ to true, because there seems to be no relation between p and q. But it should make sense if you think of p as a precondition to a promise q, and then considering whether the promise is broken. As an example, suppose your friend says, If it snows tomorrow I'll work in Trottier with you. If it doesn't snow and she doesn't pull up, she hasn't technically broken her promise. If it doesn't snow and she shows up, then she still hasn't broken her promise. The only way she can break her promise is if it snows and she doesn't come to Trottier; this situation corresponds to the only 0-row in the truth table.

The conditional is a very important logical operator to understand, because most theorem statements assume some hypothesis and claim some conclusion. You will be asked to prove statements of this form, so it is important to understand the logical nature of the statements to begin with.

The last relation is called the *biconditional*, and it asserts that variables p and q are logically equivalent. That is, p happens if and only if q happens. It's truth table

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

is pretty self-explanatory; in it, $p \Leftrightarrow q$ is true whenever p and q have the same truth value. The name "biconditional" is suggested by (part of) the following proposition.

Proposition 6. *Let p and q be propositional variables. Then*

$$\begin{aligned}
p \Leftrightarrow q &\equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \\
&\equiv \big((\neg p) \vee q\big) \wedge \big((\neg q) \vee p\big) \\
&\equiv (p \wedge q) \vee \big((\neg p) \wedge (\neg q)\big).
\end{aligned}$$

Proof. We leave the first equivalence to the reader (writing out the truth table is one way of proving it). The second equivalence follows from our earlier observation that $p \Rightarrow q \equiv \neg p \vee q$, and the third equivalence follows from the distributive, complement, and identity laws. ▮

A formula f is called a

i) *tautology* if $f \equiv 1$, i.e., f always evaluates to true;

ii) *contradiction* if $f \equiv 0$, i.e., f always evaluates to false;

iii) *contingency* if f can evaluate to both 1 and 0, depending on the values of its variables;

iv) *satisfiable* if f evaluates to 1 for at least one input; and

v) *falsifiable* if f evaluates to 0 for at least one input.

An example of a tautology is $p \vee \neg p$ and an example of a contradiction is $p \wedge \neg p$. This follows from the complement laws. To say that something is satisfiable is precisely to say that it is not a contradiction, and to say that something is falsifiable is equivalent to saying that it is not a tautology. Contingencies are those formulas that are both satisfiable and falsifiable (in other words, formulas that are neither tautologies nor contradictions).

Suppose we are asked which of the above definitions the formula

$$f \equiv \big(p \wedge (p \Rightarrow q)\big) \Rightarrow q$$

satisfies. This formula only has two variables, so it is easy enough to use a truth table for this purpose, but we will take the opportunity to practise simplifying the expression symbolically. First of all, let's change all conditionals of the form $r \Rightarrow s$, to disjunctions of the form $\neg r \vee s$. This gives us

$$f \equiv \neg\big(p \wedge (\neg p \vee q)\big) \vee q.$$

Now we use the distributive law to distribute the conjunction over the innermost disjunction, obtaining

$$f \equiv \neg\big((p \wedge \neg p) \vee (p \wedge q)\big) \vee q;$$

by the complement and identity laws in that order, this simplifies to

$$f \equiv \neg(p \wedge q) \vee q.$$

Now De Morgan's law and associativity give

$$f \equiv (\neg p \vee \neg q) \vee q \equiv \neg p \vee (\neg q \vee q),$$

and thus

$$f \equiv \neg p \vee 1 \equiv 1,$$

by the complement and domination laws in that order. We conclude that f is a tautology, which also means that it is satisfiable.

The fact that $\big(p \wedge (p \Rightarrow q)\big) \Rightarrow q$ is a tautology symbolically justifies the argument that of p is true and $p \Rightarrow q$ is true, then we should be able to conclude q. This form of argument is called *modus ponens*, and it dates back to ancient

times. You probably use *modus ponens* all the time in everyday life without knowing it, and we will certainly use it in this class a lot.

Encoding problems in propositional logic. Many algorithmic and logical problems can be encoded in propositional logic (and then later solved by a computer program). For example, suppose we want to play 4×4 Sudoku. In this game, we have a 4×4 grid and we want to fill it with the numbers 1 through 4 such that

  i) every row contains 1 through 4;

 ii) every column contains 1 through 4; and

iii) the four subsquares each contain 1 through 4.

    In a given instance of the game, some cells are already filled in. The puzzle is: *Is there a solution and if so, what is it?*

Fig. 1. An example 4×4 Sudoku game.

    To represent a Sudoku game in propositional logic, we can define boolean variables $p_{i,j,k}$, where i, j, and k range over $\{1, 2, 3, 4\}$. (So there are 4^3 variables in total.) We shall set

$$p_{i,j,k} = \begin{cases} 1, & \text{if the number } k \text{ is in row } i \text{ and column } j; \\ 0, & \text{otherwise.} \end{cases}$$

We'll number the rows increasing from the top and the columns increasing from left to right. For example, in Fig. 1 there is a 2 in row 1 and column 3, so $p_{1,3,2} = 1$.

    Now we set to work encoding the conditions of a Sudoku grid in propositional logic:

  i) To stipulate that every row contain 1 through 4, we first define auxiliary variables

$$r_{i,k} = p_{i,1,k} \vee p_{i,2,k} \vee p_{i,3,k} \vee p_{i,3,k},$$

for $i, k \in \{1, 2, 3, 4\}$. With these helper variables, we now see that

$$r_{1,1} \wedge r_{1,2} \wedge r_{1,3} \wedge r_{1,4}$$

encodes the requirement that row 1 contains one of each number. We do the same for rows 2, 3, and 4 as well, and then combine with AND.

ii) We do a similar thing as in part (i) for each of the four columns.

iii) Ditto for subsquares.

iv) We need to set the initial values of the grid. For the grid in Fig. 1, we have the formula

$$p_{1,3,2} \wedge p_{3,1,1} \wedge p_{3,2,3}.$$

v) Lastly, we need to make sure that there is not more than one number per cell. To do this, for each cell $(i,j) \in \{1,2,3,4\}^2$ we write

$$p_{i,j,1} \Rightarrow (\neg p_{i,j,2} \wedge \neg p_{i,j,3} \wedge \neg p_{i,j,4}),$$

and so on (four conditionals in total). Of course we'll need to AND all these together.

Now we combine the formulas from each of these five steps into one long formula f such that f is satisfiable if and only if the grid has a solution, and the values for $p_{i,j,k}$ give a solution.

Defining all of these variables was a rather arduous and cumbersome process, and not entirely worth it for a 4×4 game of Sudoku (which can just be solved by eyeballing the grid). But one could imagine writing a general computer program to encode larger and larger grids. In fact, there are lots of problems that can be *reduced* to the problem of determining if a boolean formula is satisfiable. This means that if we have a program capable of taking a formula f as input and spitting out whether or not it is satisfiable (in a reasonable amount of time), then there are lots of real-world problems that this program could be applied to.

This problem is called the *boolean satisfiability problem*, often abbreviated SAT. One way of solving it for any given f is to just compute its truth table. We already know the downside of this approach: if f has n variables, then its truth table will have 2^n rows. Given a few minutes, you are certainly capable of writing down a formula f that has 300 variables, call them $p_1, \ldots, p_{300}$. The truth table of f will have 2^{300} rows, which is more than the number of atoms in the observable universe. You can learn a lot more about SAT in a higher-level class on computational complexity (e.g., COMP 360/362).

3. Predicate logic

12.IX Propositional logic allows us to work with simple declarations, but this isn't powerful enough to express some deeper mathematical concepts. For this purpose, we now introduce the notion of a *predicate*. This is a statement involving some number of variables, each of which may take values coming from a universe U, such that the statement evaluates to either true or false *once all variables are assigned values*. The statement $P(n)$ given by "n is prime" is an example of this, where n can take any value in the universe $\mathbf{Z}$. An example with two variables is the predicate $L(x,y)$ defined by "x is less than y." (A more commonly-used notation for this predicate is "$x < y$.")

Predicates contain variables, but at the moment we don't have any way of introducing new variables into a statement. This is done using two different *quantifiers*. The first is the *universal quantifier*, denoted $\forall$ and meaning "for all." The statement $\forall n : P(n)$ is true if and only if $P(n)$ is true for every possible value that n can take. The second quantifier is the *existential quantifier*, written "$\exists$" and with the meaning "there exists." The statement $\exists n : P(n)$ is true if and only if there is (at least) one value that n can take such that $P(n)$ is true. The colon doesn't really have any mathematical meaning in these formulas; they just visually set the quantifiers apart from the predicates that follow.

For instance, taking $P(n)$ to be the statement "n is prime," where the universe U is $\mathbf{N}$, the statement $\exists n P(n)$ is true and the statement $\forall n : P(n)$ is false. What about the statement $\forall x\, \exists y : y < x$? Well, if the universe U is taken to be $\mathbf{N}$, then the statement is false, because setting x equal to 0, there is no element y of $\mathbf{N}$ such that $y < 0$. But if $U = \mathbf{Z}$, then the statement is true, since for every integer x, we can put $y = x - 1$, so that $y < x$.

Now we practise translating converting mathematical statements written in English into formulas in predicate logic. Suppose we want to write, Every integer is even or odd. The universe here is is the set $\mathbf{Z}$ of integers. The word "every" has the same meaning as "for all," so right off the bat, we can reexpress the statement as, For all $n \in \mathbf{Z}$, n is even or n is odd. In symbols, this is

$$\forall n\, (n \text{ even} \vee n \text{ odd}).$$

Lastly, we need to figure out how to express the property of being even or being odd. An integer n is even if an only if it is a multiple of two; that is, if there is some integer k such that $2k = n$. Likewise, an integer is odd if and only if it is one more than a multiple of two. The corresponding formula is $\exists k : 2k + 1 = n$. So our statement can be expressed

$$\forall n\, \big((\exists k : n = 2k) \vee (\exists k : n = 2k + 1)\big).$$

The variable k appears twice in this formula, but its first instance is independent of its second instance, because of the parentheses. (Readers who write computer programs will be familiar with the concept of a variable "going out of scope.") So there is nothing wrong with this formula, but to be extra clear that the first k is different from the second k, why don't we replace it with a different letter? Thus we arrive at

$$\forall n\, \big((\exists k : n = 2k) \vee (\exists l : n = 2l + 1)\big),$$

a formula in predicate logic that means, Every integer is even or odd.

Restrictions using quantifiers. It is not true that every real number has a multiplicative inverse, since one cannot divide by zero. However, the statement "every nonzero real number has a multiplicative inverse" is true. How should

we write this as a formula in predicate logic? One way is to use the conditional: over the universe $U = \mathbf{R}$, we could write

$$\forall x : (x \neq 0 \Rightarrow \exists y : xy = 1).$$

Another is to use subscripts: in the same universe, we write

$$\forall x_{x \neq 0} \, \exists y : xy = 1.$$

Using subscripts is slightly informal, since we didn't formally define above what a subscript is supposed to mean, but it is something that you might encounter. The last way is to simply restrict the universe itself: in the universe $U = \mathbf{R} \setminus \{0\}$, the statement

$$\forall x \, \exists y : xy = 1$$

is true.

Multiple quantifiers. Withing a formula, quantifiers cannot be interchanged willy-nilly. The order of $\forall$ and $\exists$ matters! They are read from left to right. Consider the following examples, over the universe $U = \mathbf{R}$. The statement

$$\forall x \, \exists y : x + y = 0$$

is true, since for each given x we can take y to be $-x$. On the other hand,

$$\exists y \, \forall x : x + y = 0$$

is false, since it would mean that there is some integer that adds up to zero with *any* integer. Of course, sometimes switching the order of quantifiers, doesn't change the truth value of a statement. Both

$$\exists y \, \forall x : xy = 0$$

and

$$\forall x \, \exists y : xy = 0$$

are true, since in the first case, we can take $y = 0$, and in the second case, we can set y to 0 no matter what x is given.

So we know that the order of $\forall$ and $\exists$ matters in general, but repeated instances of the *same* quantifier *can* be interchanged. For instance,

$$\forall x \, \forall y : x^2 + y^4 \geq 0$$

is the same as

$$\forall y \, \forall x : x^2 + y^4 \geq 0,$$

and we can even write $\forall x, y : x^2 + y^4 \geq 0$, to introduce both variables simultaneously.

Negating quantifiers. The universal quantifier is sort of like a big chain of conjunctions that goes over the whole of the universe. For example, in the universe $\mathbf{N}$, the statement $\forall n : P(n)$ is equivalent to

$$P(1) \wedge P(2) \wedge P(3) \wedge \cdots,$$

if this were a valid propositional formula (it isn't because we don't allow propositional formulas to be infinite). Likewise, the existential quantifier $\exists n : P(n)$ is equivalent to

$$P(1) \vee P(2) \vee P(3) \vee \cdots.$$

We know, by De Morgan's laws, that negating a big series of conjunctions requires us to flip all the ANDs to ORs. So, once again abusing notation somewhat, we expect

$$\neg\big(P(1) \wedge P(2) \wedge P(3) \wedge \cdots\big) \equiv \neg P(1) \vee \neg P(2) \vee \neg P(3) \vee \cdots.$$

Thus we conclude that

$$\neg\big(\forall n : P(n)\big) \equiv \exists n : \neg P(n).$$

You can play the same game with the other De Morgan's law to show that

$$\neg\big(\exists n : P(n)\big) \equiv \forall n : \neg P(n).$$

Going back to our example of $P(n)$ denoting "n is prime," the statement $\neg\big(\forall n : P(n)\big)$ is true, since not all integers n are prime, and we have just shown that this is equivalent to the statement $\exists n : \neg P(n)$; that is, there exists n such that n is not prime.

We end this section with a longer example. Let's express the statement, "There is a nonzero real number such that every real number is not its inverse or is negative." In the universe $\mathbf{R}$, the formula corresponding to this statement is

$$\exists x : (x \neq 0 \wedge (\forall y : xy \neq 1 \vee y < 0)).$$

(Work it out yourself!) Is this statement true or false? It turns out that it is true. You might be able to stare at the formula long enough to convince yourself of this fact, but another way to see that it's true is to note that its negation is false. Let's do this now (it's a good excuse to practise negating a formula). We have

$$\neg\Big(\exists x : (x \neq 0 \wedge (\forall y : xy \neq 1 \vee y < 0))\Big)$$
$$\equiv \forall x : \neg(x \neq 0 \wedge (\forall y : xy \neq 1 \vee y < 0))$$
$$\equiv \forall x : \big(x = 0 \vee \neg(\forall y : xy \neq 1 \vee y < 0)\big)$$
$$\equiv \forall x : \big(x = 0 \vee \exists y : \neg(xy \neq 1 \vee y < 0)\big)$$
$$\equiv \forall x : \big(x = 0 \vee \exists y : (xy = 1 \wedge y \geq 0)\big).$$

This negated statement is false, since if $x = -2$, then $x = 0$ doesn't hold, so the left-hand side of the OR isn't true, and there is no y such that $-2y = 1$ and $y \geq 0$ are both true, since the only y satisfying $-2y = 1$ is $-1/2$.

Negating a formula in predicate logic is entirely mechanical. The $\neg$ symbol moves from left to right like a bulldozer that flips quantifiers and negates predicates it finds along the way, until eventually its job is done and it disappears. More broadly, we write mathematical statements in formal logic to make things more precise and mechanical. This can be useful to humans, since English is often ambiguous whereas the notation we just established is not. It can be useful to machines as well, since, as we just saw, manipulating a formula is something that can very easily be automated.

4. Proofs

We're getting to the fun part of the course now. Further back in these notes, we already proved a few statements about sets. This was just a taste of what's to come, as the main focus of this course is to teach you how to prove mathematical statements. These will all be statements that can ultimately be stated in predicate logic, so using the tools from the previous section, you can boil them down to their logical skeleton. In this section, we will formally define what it means to prove a statement in predicate logic.

To prove a statement, we always process the quantifiers from left to right. Whenever we encounter something of the form $\exists x : P(x)$, we are allowed to choose the value for x (from the given universe), and we just need to show that $P(x)$ holds for that value of x. Here's an example.

Proposition 7. *There exists an integer $m > 0$ and an integer $n < 0$ such that $m^2 + n^2 = 25$.*

We've written the statement in words, and we will continue to do so for all the propositions in these notes because we are humans and not cyborgs, but notice that the underlying predicate logical formula here is

$$\exists m \, \exists n : m > 0 \wedge n < 0 \wedge m^2 + n^2 = 25,$$

with $U = \mathbf{Z}$. For the remainder of this section, we'll continue to write out the formulaic equivalents of propositions, to practise converting between the two worlds.

Proof. After a moment's contemplation, we notice that $9 + 16 = 25$. So we need a positive integer that squares to to 9 and a negative number that squares to 16. Hence we may pick $m = 3$ and $n = -4$, and $m^2 + n^2 = 25$. ▮

On the other hand, to prove a statement of the form $\forall x : P(x)$, we are not allowed to choose the value of x. Instead, we imagine it is given to us, and we still have to prove $P(x)$, no matter what the x might be. Here's what we mean.

Proposition 8. *For all $x \in \mathbf{Q}$, there exists $y \in \mathbf{Z}$ such that $xy \in \mathbf{Z}$.*

The formula this time is

$$\forall x \, \exists y : y \in \mathbf{Z} \wedge xy \in \mathbf{Z},$$

over $U = \mathbf{Q}$.

Proof. Let $x \in \mathbf{Q}$. Then x can be expressed as the ratio of two integers; write $x = m/n$ with $m, n \in \mathbf{Z}$. Then, setting $y = n \in \mathbf{Z}$, we have $xy = (m/n) \cdot n = m \in \mathbf{Z}$. ∎

Notice how we introduced the variable x in the above proof. Because we're trying to prove a "for all" statement, we use the word "let," to indicate that x is given to us by some higher power. In fact, we should sort of view this higher power as possibly being malicious. A very useful way to think about writing a proof is to imagine a game in which you are trying to prove a statement in predicate logic, and a supernatural adversary is attempting to thwart you. Let's say this predicate has four variables, so the statement is

$$\exists x \, \forall y \, \forall z \, \exists w : P(x, y, z, w).$$

The variables in the statement are introduced from left to right. Each time you see a $\exists$ symbol, it's your turn. In the example above, you get to set the variable x to any element of the given universe (keeping in mind that your eventual goal is to prove $P(x, y, z, w)$). Each time there is a $\forall$ symbol, it's the adversary's turn, and you should be prepared for whatever he throws at you. So in our example, the adversary may set y and z to anything in the universe, and he knows you picked x. Lastly, you get to pick w. If $P(x, y, z, w)$ is true, you win, and if not, the adversary wins. Writing a proof is equivalent to describing a winning strategy for the player against the adversary.

17.IX **Proving conditional statements.** Many mathematical statements introduce some hypotheses, then assert some conclusion. Thus they are some kind of statement of the form $p \Rightarrow q$. To prove this kind of statement, we assume that p holds, then prove that q is true. This is because the only way a statement for $p \Rightarrow q$ to be false is if p is true and q is false, so we're showing this cannot happen. Take a look at the following example.

Proposition 9. *If n is an odd integer, then n^2 is also odd.*

The underlying formula is $\forall n \big((\exists k : n = 2k + 1) \Rightarrow (\exists l : n^2 = 2l + 1) \big)$, in the universe $U = \mathbf{Z}$.

Proof. Let n be an arbitrary odd integer, so that there exists k such that $n = 2k + 1$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

so setting $l = 2k^2 + 2k$, which is an integer, we have $n^2 = 2l + 1$. Hence n^2 is odd. ▌

To disprove a statement, we simply prove that its negation is true. For example, suppose we want to disprove the statement $\exists x \, \forall y : x + y = 0$ (this was a statement we encountered in the previous section). Its negation is

$$\forall x \, \exists y : x + y \neq 0,$$

and to prove it we let x be given, set $y = -x + 1$, and observe that $x + y = x + (-x + 1) = 1$, which is not equal to 0.

Now we define two words that sound similar but are very different, logically speaking. The *converse* of a conditional statement $p \Rightarrow q$ is the statement $q \Rightarrow p$. The statement $p \Rightarrow q$ and its converse both hold if and only if the biconditional statement $p \Leftrightarrow q$ holds. On the other hand, the *contrapositive* to $p \Rightarrow q$ is the statement $\neg q \Rightarrow \neg p$. What's the deal with this silly-looking conditional? Well, it turns out to actually be equivalent to $p \Rightarrow q$. Check it out:

$$\begin{aligned} p \Rightarrow q &\equiv \neg p \lor q \\ &\equiv q \lor \neg p \\ &\equiv \neg(\neg q) \lor \neg p \\ &\equiv \neg q \Rightarrow \neg p \end{aligned}$$

So to prove a statement of the form $p \Rightarrow q$, it is sufficient to prove $\neg q \Rightarrow \neg p$. Sometimes, this can make the proof a lot easier. Here's an example. (It is the converse of Proposition 9.)

Proposition 10. *If n is an integer such that n^2 is odd, then n is odd.*

Proof attempt. Assume n^2 is odd, so that $n^2 = 2k + 1$ for some integer k. Then $n = \sqrt{2k + 1}$.

Where do we go from here? It's not even clear that $\sqrt{2k + 1}$ is an integer, let alone an odd one. The contrapositive comes to the rescue.

Proof of Proposition 10. We proceed by contraposition. Suppose that n is not odd; that is, n is even. So there exists an integer k such that $n = 2k$. Then $n^2 = (2k)^2 = 4k^2$. Setting $l = 2k^2$, we have $n^2 = 2l$, so n^2 is even. Hence n^2 is not odd. ▌

Proofs by contradiction. We now discuss a powerful method of proof, which dates back to at least the ancient Greeks and referred to for much of Western history by its Latin name, *reductio ad absurdum*. It proceeds to prove a statement p by assuming its negation $\neg p$ holds, then deriving a contradiction, i.e., a statement whose truth value is 0. By doing this, one will have proved that $\neg p \Rightarrow 0$, which in turn shows that p is true, since

$$\neg p \Rightarrow 0 \equiv \neg(\neg p) \lor 0 \equiv p \lor 0 \equiv p.$$

Here is an example of a proof by contradiction.

Proposition 11. *There is no least positive rational number.*

In $U = \mathbf{Q}$, one way to formulate this is

$$\neg\big(\exists x : x > 0 \wedge (\forall y : y > 0 \Rightarrow x \leq y)\big).$$

Proof. Suppose, towards a contradiction, that there exists some rational $x > 0$ such that for all $y \in \mathbf{Q}$ with $y > 0$, $x \leq y$. Then, we can apply this property with $y = x/2$ to see that $x \leq x/2$. Since x is positive, we can divide this inequality by x on both sides to obtain $1 \leq 1/2$. But this is absurd, since $1/2 < 1$. This contradiction completes the proof. ∎

Here is another classical example of a proof by contradiction. It was known to the Pythagoreans.

Proposition 12. *The number $\sqrt{2}$ is irrational.*

Proof. Suppose, towards a contradiction, that $\sqrt{2}$ is rational. Then there are integers p and q such that $\sqrt{2} = p/q$, and furthermore, we can assume that p and q do not have any common factors, since if they did, we could divide them out and the ratio would remain the same. Squaring both sides of the equation, we have $2 = p^2/q^2$, or in other words, $2q^2 = p^2$. This implies that p^2 is even, so by (the contrapositive of) Proposition 10, p is even as well. That means we can write $p = 2r$ for some integer r, and substitute this new information into the above equation to obtain $2q^2 = (2r)^2 = 4r^2$. Dividing out by 2 yields $q^2 = 4r^2$, so q^2 is even, and so is q.

We have deduced that p and q are both even. On the other hand, we assumed they had no common factors. This is a contradiction. ∎

Earlier we described the composition of a proof as playing a game with a supernatural adversary. To prove something by contradiction, then is is akin to starting the game by letting adversary believe he has already won, and then working from that assumption to derive an impossibility. Quite the devious strategem.

> Reductio ad absurdum, *which Euclid loved so much,*
> *is one of a mathematicians finest weapons.*
> *It is a far finer gambit than any chess gambit:*
> *a chess player may offer the sacrifice of a pawn*
> *or even a piece,*
> *but a mathematician offers the* game.
>
> — G. H. HARDY, *A Mathematician's Apology* (1940)

Case analysis. For all $n \geq 2$ and all propositions $p_1, \ldots, p_n, q$, we have the equivalence

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q).$$

(As an exercise, prove this when $n = 2$. Later on, when we learn about mathematical induction, you'll be able to prove it in general.)

Why is this useful? Well, if we have two or more propositions $p_1, p_2, \ldots, p_n$ such that at least one of them must hold, that is,

$$p_1 \vee p_2 \vee \cdots \vee p_n \equiv 1,$$

then if we are able to show that

$$p_1 \Rightarrow q, \quad p_2 \Rightarrow q, \quad \ldots, \quad \text{and} \quad p_n \Rightarrow q$$

all hold, then we will have shown

$$1 \Rightarrow q \equiv \neg 1 \vee q \equiv 0 \vee q \equiv q.$$

Let's see an example of this in action.

Proposition 13. *For all integers $n \geq 0$, $1 + (-1)^n(2n - 1)$ is a multiple of 4.*

Proof. Let an integer $n \geq 0$ be given. We know that n is even or n is odd.

If n is even, then $n = 2k$ for some integer k, and

$$1 + (-1)^{2k}\big(2(2k) - 1\big) = 1 + 1^k(4k - 1) = 4k,$$

which is a multiple of 4.

If n is odd, then $n = 2k + 1$ for some integer k, and

$$1 + (-1)^{2k+1}\big(2(2k + 1) - 1\big) = 1 - (4k + 2 - 1) = 1 - (4k + 1) = -4k,$$

which is also a multiple of 4. ∎

19.IX   Sometimes, the cases into which one might split the proof are not so obvious.

Proposition 14. *There exist irrational numbers a and b such that a^b is rational.*

Proof. Consider the number $(\sqrt{2})^{\sqrt{2}}$. It is either rational or irrational.

If it is rational, then we can set $a = b = \sqrt{2}$, which we already know to be irrational, by Proposition 12.

If it is irrational, then we can set $a = (\sqrt{2})^{\sqrt{2}}$ and $b = \sqrt{2}$. We compute

$$a^b = \big((\sqrt{2})^{\sqrt{2}}\big)^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2,$$

which is rational. ∎

Note that in this proof, we did not need to know whether $(\sqrt{2})^{\sqrt{2}}$ is rational or not; we just know that it must either be rational or irrational. (In fact, it is known that $(\sqrt{2})^{\sqrt{2}}$ is irrational, but the usual proof of this requires some notions from complex analysis as well as Galois theory, subjects that are typically not encountered until at least the second or third year of a mathematics degree.)

Mathematical induction. Sometimes we want to prove an infinite number of statements, indexed by the natural numbers. If the complexity of the statements sort of "grows" in n (a vague notion to be made precise soon), the following theorem holds.

Theorem 15 (*Principle of mathematical induction*). *Let $P(n)$ be a family of predicates indexed by $n \in \mathbf{N}$. Let $m \in \mathbf{N}$. If*

  i) *$P(m)$ holds; and*

  ii) *for all $n \geq m$,*

$$\big(P(m) \wedge P(m+1) \wedge \cdots \wedge P(n)\big) \Rightarrow P(n+1)$$

  then $P(n)$ holds for all $n \geq m$.

In the following proof, we use the *well-ordering principle*, which is the fact that every nonempty subset of the natural numbers has a least element. You can see the proof of the well-ordering principle in a higher-level set theory course.

Proof. Assume that (i) and (ii) both hold. Our goal is to prove that $P(n)$ is true for all $n \geq m$, so we shall suppose, towards a contradiction, that there is some $n \geq m$ such that $\neg P(n)$ holds. (As an exercise, convince yourself, via symbolic manipulations, that

$$\neg \forall n : n \geq m \Rightarrow P(n) \equiv \exists n : n \geq m \wedge \neg P(n).)$$

In other words, the set of $n \geq m$ such that $\neg P(n)$ holds is nonempty, so it has a least element, call it k. So $k \geq m$, and we cannot have $k = m$ due to (i), so $k > m$. Furthermore, by the minimality of k, the statements $P(m)$, $P(m+1)$, all the way up to $P(k-1)$ are true. By (ii) though, this implies that $P(k)$ holds: a contradiction. ▌

When proving something by induction, we need to prove two things: one of the form (i) and another of the form (ii). The former is called the *base case* and the latter the *induction step* or *inductive step*. The assumption to the left of the $\Rightarrow$ symbol in (ii) is called the *induction hypothesis* or *inductive hypothesis*. Technically, the theorem above is called the principle of *strong* induction; the principle of *weak* induction has

  ii)′ for all $n \geq m$, $P(n) \Rightarrow P(n+1)$,

instead of the stronger (ii). It turns out that both types of induction are actually equivalent, so we'll use both interchangeably. More often than not, the hypothesis (ii)′ is perfectly sufficient, and in these cases we'll simply use weak induction so as not to clutter our proofs with lots of unused hypotheses.

Here is an example. Suppose we want to find (and prove) a formula for the sum of the first n odd numbers. The first thing to do is to try some small cases. When $n = 1$, the sum is just 1. When $n = 2$, the sum is $1 + 3 = 4$, when $n = 3$, we have $1 + 3 + 5 = 9$, and for $n = 4$, we compute $1 + 3 + 5 + 7 = 16$. So the pattern goes $1, 4, 9, 16, \ldots$, which leads us to conjecture that the sum of the first n odd numbers might equal n^2. In fact, this is true, and we shall prove it by induction.

Proposition 16. *For all integers $n \geq 1$,*

$$\sum_{i=1}^{n}(2i - 1) = n^2.$$

Proof. By induction on n. First we prove the base case, $n = 1$. We have

$$\sum_{i=1}^{1}(2i - 1) = 2 - 1 = 1 = 1^2.$$

Now for the inductive step. Let $n \geq 1$ and assume that

$$\sum_{i=1}^{n}(2i - 1) = n^2.$$

Then

$$\begin{aligned}
\sum_{i=1}^{n+1}(2i - 1) &= \sum_{i=1}^{n}(2i - 1) + \big(2(n + 1) - 1\big) \\
&= n^2 + 2n + 2 - 1 \\
&= n^2 + 2n + 1 \\
&= (n + 1)^2,
\end{aligned}$$

where it is in the second line that we used the inductive hypothesis. ▌

The first thing to notice about doing a proof by induction is that the proof method itself doesn't tell you what it is you should prove. You have to guess at the correct statement first. Also, proofs by induction are often "unenlightening," in that they often don't reveal the fundamental reasons why something might be true. (The previous proposition can be illustrated by a rather simple picture, which is not a proof, but is somewhat more elucidating that the induction proof.)

A longer example now. Suppose we have a pile of n stones, with $n \geq 1$. We have a job, which can be described by a pseudo-algorithm.

Algorithm S (*Divide stones*). The input to this algorithm is an integer $n \geq 1$, representing a number of stones. We have a list `PILES` of integers representing a collection of piles of stones, as well as an integer variable `BALANCE`. Initialise `PILES` $\Leftarrow 1$ (one pile with n stones), and set `BALANCE` $\leftarrow 0$. This algorithm splits the stones into n piles of 1 stone each, accumulating profits into `BALANCE` along the way.

S1. [Done?] If every element of `PILES` is 1, terminate the algorithm and output `BALANCE`.

S2. [Choose a pile.] Select some element $m > 2$ from `PILES` and remove it from the list. (The variable m is the number of stones in this pile.)

S3. [Split.] Let k and l be two numbers with $k + l = m$. We append $\texttt{PILES} \Leftarrow k$ and $\texttt{PILES} \Leftarrow l$, and increment $\texttt{BALANCE} \leftarrow \texttt{BALANCE} + k \cdot l$. (We have split pile n into two piles of size k and l, and the payout for doing so is $k \cdot l$ dollars.)

S4. [Loop.] Go to step S1.   ▌

This is not, strictly speaking, an algorithm, since we didn't specify how the algorithm should choose the integers k and l that add up to m in step S3. However, running through a few instances with, say, $n = 6$, on paper, using whatever choices of split you like in every iteration of step S3, you'll find that the algorithm always terminates with $\texttt{BALANCE} = 15$. Trying a few different starting values of n might lead you to conjecture the following proposition, which we will prove by (strong) induction.

Proposition 17. *For a given input n, Algorithm S always outputs* $\texttt{BALANCE} = n(n-1)/2$, *regardless of the choice of split at any given iteration of step S3.*

Proof. By induction on n. For the base case $n = 1$, note that we immediately output $\texttt{BALANCE} = 0$ in the very first step of the algorithm, and $0 = 1(1-1)/2$.

Now for the inductive step, let $n \geq 1$ and suppose that for $1 \leq k \leq n$, the payout for running algorithm S on input l is $l(l-1)/2$. Suppose we have a pile of $n + 1$ stones. We shall divide it into piles of size k and size $n + 1 - k$. The total payout will be the pay for this division, namely $k(n + 1 - k)$, plus the pay for further subdividing the two piles. Thus by the induction hypothesis applied twice, the total payout will be

$$
\begin{aligned}
k(n + 1 - k) &+ \frac{k(k-1)}{2} + \frac{(n+1-k)(n-k)}{2} \\
&= \frac{2nk + 2k - 2k^2 + k^2 - k + n^2 + n - 2nk - k + k^2}{2} \\
&= \frac{n^2 + n}{2} \\
&= \frac{(n+1)\big((n+1) - 1\big)}{2},
\end{aligned}
$$

which is the expected formula for $n + 1$.   ▌

5. Functions

A *function* f from a set A to a set B is a subset $f \subseteq A \times B$ such that for every $a \in A$, there is exactly one $b \in B$ such that $(a, b) \in f$. (If there is no $b \in B$, or more than one, we say that f is not well-defined. If $(a, b) \in f$, we write $f(a) = b$. The set A is called the *domain* and the set B is the *codomain*. The notation $f : A \to B$ is a way of concisely writing "f is a function with domain A and codomain B."

Here are some examples and non-examples.

i) The function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is

$$f = \{(a, b) \in \mathbf{R}^2 : b = a^2\},$$

when written in set-builder notation.

ii) On the other hand, the set

$$g = \{(a, b) \in \mathbf{R}^2 : a = b^2\}$$

is not a function, since $(1, 1)$ and $(1, -1)$ are both in g. Furthermore, there is no element of g with -1 as its first coordinate.

iii) If $X = \{1, 2, 5\}$ and $Y = \{0, 1, 2, 3, 4, 5\}$, then

$$\{(1, 0), (2, 4), (5, 5)\}$$

is a function from X to Y.

iv) The set
$$h = \{(x, y) \in \mathbf{R}^2 : y = 1/x\}$$

is not a function, since there is no y such that $(0, y) \in h$. However if we amend the domain and consider

$$h = \{(x, y) \in (\mathbf{R} \setminus \{0\}) \times \mathbf{R} : y = 1/x\},$$

then in fact, $h : \mathbf{R} \setminus \{0\} \to \mathbf{R}$ is a function.

24.IX **Injective and surjective functions.** The *range* or *image* of a function $f : A \to B$ is

$$f(A) = \{b \in B : \text{there exists } a \in A \text{ such that } b = f(a)\}.$$

These are all the values f actually outputs. For instance, if we let $f : \mathbf{Z} \to \mathbf{N}$ be given by $f(n) = n^2$, then

$$\begin{aligned}
f(\mathbf{Z}) &= \{\ldots, f(-2), f(-1), f(0), f(1), f(2), \ldots\} \\
&= \{\ldots, 9, 4, 1, 01, 4, 9, \ldots\} \\
&= \{0, 1, 4, 9, 16, 25, \ldots\}.
\end{aligned}$$

A function $f : A \to B$ is called *surjective* or *onto* if $f(A) = B$, that is, for every $b \in B$ there exists some $a \in A$ such that $f(a) = b$. An example of a surjective function is $f : \mathbf{Q} \to \mathbf{Q}$ sending $x \mapsto x/2$. This is because for any $q \in \mathbf{Q}$, we can set $r = 2q$, and

$$f(r) = \frac{r}{2} = \frac{2q}{2} = q.$$

A function $f : A \to B$ is called *injective* or *one-to-one* if for all $a_1, a_2 \in A$ with $a_1 \neq a_2$, we also have $f(a_1) \neq f(a_2)$. Equivalently, f is injective if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$ for all $a_1, a_2 \in A$. For instance, the function $f : \mathbf{Z} \to \mathbf{N}$ that sends $n \mapsto n^2$ is not injective since $f(-1) = f(1)$, but $-1 \neq 1$. On the other hand, if we modify the domain, considering $f : \mathbf{N} \to \mathbf{N}$ sending $n \mapsto n^2$, then now f is injective, since if $f(m) = f(n)$, then $m^2 = n^2$, and there is only one positive integer that squares to any given integer, so $m = n$.

Hence we see that any function can be transformed into an injective one, in principle, by shrinking its domain (though this new function might no longer have the properties you liked in the original one), and any function $f : A \to B$ can be made surjective by changing its codomain to its range, i.e., letting $B = f(A)$.

The pigeonhole principle. We now take a brief pause to introduce one of the most fundamental laws in discrete mathematics, called the pigeonhole principle. We begin with the following intuitive theorem.

Theorem 18. *Let $a_1, a_2, \ldots, a_n$ be a finite sequence (repeats allowed) of real numbers. Let*

$$a = \frac{1}{n} \sum_{i=1}^{n} a_i$$

be the average value of the sequence and let m be the maximum value the sequence attains. Then $m \geq a$.

Proof. We have

$$a = \frac{1}{n} \sum_{i=1}^{n} a_i \leq \frac{1}{n} \sum_{i=1}^{n} m = \frac{mn}{n} = m. \quad \blacksquare$$

This theorem can be summed up in one sentence: *The maximum is at least the average.* Don't underestimate this theorem even though its proof was a one-liner! It is often used to prove highly nontrivial results. (As an exercise, prove the similar statement: *The minimum is at most the average.*) From here we are now equipped to prove (a general version of) the pigeonhole principle.

Theorem 19. *Let A and B be finite sets with $|A| = m$ and $|B| = n$. For every function $f : A \to B$, then there is some $b \in B$ such that there are at least $\lceil m/n \rceil$ elements $a \in A$ with $f(a) = b$.*

Proof. Enumerate $B = \{b_1, b_2, \ldots, b_n\}$. For $1 \leq i \leq n$, let r_i be the number of $a \in A$ such that $f(a) = b_i$. This is a sequence that adds up to m, since every a in A maps to exactly one element of B. So the sequence has average m/n, and by the previous theorem, there must be some j such that $r_j \geq m/n$. But the r_i are all actually integers (since cardinalities of finite sets are integers), meaning that $r_j \geq \lceil m/n \rceil$. Letting $b = b_j$ completes the proof. $\quad \blacksquare$

The reason this is called the pigeonhole principle is because of the following special case.

Corollary 20 (*Pigeonhole principle*). *Let $n \geq 2$. If n pigeons nest in $n - 1$ holes, there is at least one hole that contains at least two pigeons.*

Proof. Let A be the set of pigeons and B the set of pigeonholes. Let f be any function sending the set of pigeons to the set of holes. By the previous theorem, there is some hole with at least $\lceil n/(n-1) \rceil = 2$ pigeons in it. (This is because $1 < n/(n-1) < 2$ for all integers $n \geq 2$.) $\blacksquare$

Bijections. A function f is called *bijective* (or a *bijection*, or a *one-to-one correspondence*) if it is injective and surjective. Bijections are important because of the following proposition.

Proposition 21. *Let A and B be finite sets. Then*

   i) there exists a bijection $f : A \to B$ if and only if $|A| = |B|$; and

  ii) if $|A| = |B|$ and $f : A \to B$ then f is injective if and only if f is surjective.

Proof. Suppose $|A| = |B| = n$. Then choose an ordering $a_1, \ldots, a_n$ of A and an ordering $b_1, \ldots, b_n$ of B. Let $f(a_i) = b_i$ for all $1 \leq i \leq n$. By construction, this is a bijection, proving one direction of (i).

On the other hand, suppose $|A| \neq |B|$ (so we prove this direction by contraposition). If $A < B$, then f cannot be surjective, since the image of f has size at most $|A| < |B|$ (at least one element of B must be missed). If $A > B$, then $|A|/|B| > 1$, so by Theorem 19, there is some element $b \in B$ such that the number of $a \in A$ mapping to b is at least $\lceil |A|/|B| \rceil \geq 2$. This means that f is not injective. We have proved part (i).

To prove part (ii), let $|A| = |B|$ and let $f : A \to B$. First we assume that f is injective. We enumerate $A = \{a_1, a_2, \ldots, a_n\}$. Then

$$f(A) = \big\{ f(a_1), f(a_2), \ldots, f(a_n) \big\} \subseteq B.$$

All of the $f(a_i)$ are distinct, since if $f(a_i) = f(a_j)$, then $a_i = a_j$. So $\big| f(A) \big| = |A| = n$, and $f(A)$ is a size n subset of B, which also has size n. Hence $f(A) = B$; that is, f is surjective.

Lastly, suppose f is not injective (again we are using contraposition). So there are a_i and a_j such that $a_i \neq a_j$ but $f(a_i) = f(a_j)$. So

$$\big| f(A) \big| = \big| \big\{ f(a_1), f(a_2), \ldots, f(a_n) \big\} \big| < n = |B|,$$

so $f(A) \neq B$ and f is not surjective. $\blacksquare$

Item (i) of the previous proposition should be entirely intuitive, especially if we use the alternative nomenclature "one-to-one correspondence" instead of "bijection." (In fact, we already implicitly used (i) in these notes, in the proof of Proposition 5.) Item (ii) is perhaps not as immediate, but should become clear if you work it out with a picture.

Bijections. A function $f : A \to B$ is called *invertible* if there exists $g : B \to A$ such that

    i) for all $b \in B$, $f\bigl(g(b)\bigr) = b$; and

    ii) for all $a \in A$, $g\bigl(f(a)\bigr) = a$.

If g exists, it can be shown that g must be unique, so we write $g = f^{-1}$ and speak of *the* inverse of f.

Proposition 22. *Let $f : A \to B$ be a function. Then f is invertible if and only if f is bijective.*

Proof. First we assume that f is invertible. So there exists an inverse g of f. For each $b \in B$, setting $a = g(b)$ we have

$$f(a) = f\bigl(g(b)\bigr) = b.$$

This proves that f is surjective. To show that f is injective, suppose that $f(a_1) = f(a_2)$. By applying g on both sides, we have $g\bigl(f(a_1)\bigr) = g\bigl(f(a_2)\bigr)$, whence $a_1 = a_2$, by definition of g.

    Now assume that f is bijective. We need to define $g : B \to A$. Well, gven any $b \in B$, there is some a such that $f(a) = b$, from surjectivity of f, and this a is unique, since f is injective. So set $g(b) = a$ (and repeat this process for every $b \in B$). We have $f\bigl(g(b)\bigr) = f(a) = b$, and for every $a \in A$, by definition of g the element $g\bigl(f(a)\bigr)$ is the unique element in A that gets brought to $f(a)$ by f, has to be a itself. ∎

    Sometimes to prove that two sets have the same cardinality, it is easier to prove that there exists a bijection (as we already saw in the example of Proposition 5), and sometimes to prove that a function is a bijection, it is easier to show that it has an inverse, rather than messing around with the definitions of injective and surjective. Here's an example.

Proposition 23. *Let X be a finite nonempty set. Let E be the set of all subsets of X with even cardinality, and let F be the set of all subsets of X with odd cardinality. Then $|E| = |F|$.*

Proof. We shall construct a function $f : E \to F$. Fix one specific $x \in X$; we can do this because $X \neq \emptyset$. Now, for all $A \in E$, let

$$f(A) = \begin{cases} A \setminus \{x\}, & \text{if } x \in A; \\ A \cup \{x\}, & \text{if } x \notin A. \end{cases}$$

Note that since $|A|$ is even for all $A \in E$, the cardinality of $f(A)$ is odd (in the first case it is $|A| - 1$ and in the second case it is $|A| + 1$. This shows that f is indeed a function with codomain F. Now to prove $|E| = |F|$ we will show that f is bijective, which we do by showing that f is an inverse (as an exercise, you might instead try to prove bijectivity from the definitions of injective and surjective).

    We define $g : F \to E$ by

$$g(A) = \begin{cases} A \setminus \{x\}, & \text{if } x \in A; \\ A \cup \{x\}, & \text{if } x \notin A. \end{cases}$$

As before, $\big|g(A)\big|$ is even, since A is assumed to be a member of F now. Now for any $A \in E$,

$$
\begin{aligned}
g\big(f(A)\big) &= \begin{cases} g\big(A \setminus \{x\}\big), & \text{if } x \in A; \\ g\big(A \cup \{x\}\big), & \text{if } x \notin A \end{cases} \\
&= \begin{cases} \big(A \setminus \{x\}\big) \cup \{x\}, & \text{if } x \in A; \\ \big(A \cup \{x\}\big) \setminus \{x\}, & \text{if } x \notin A \end{cases} \\
&= \begin{cases} A, & \text{if } x \in A; \\ A, & \text{if } x \notin A \end{cases} \\
&= A.
\end{aligned}
$$

The proof that $f\big(g(A)\big) = A$ is similar. Thus g is the inverse of f. ∎

6. Cardinality

26.IX Earlier, we defined the cardinality of a set to be the number of elements it contains. What, then, is the cardinality of $\mathbf{N}$? How about $\mathbf{R}$? You might say ∞, but this is not a number (at least, it's not an element of $\mathbf{N}$, the way all cardinalities of finite sets are). So perhaps we should amend our question to the following: *When do infinite sets have the same size?* Our experience with functions leads us to the answer: *When there exists a bijection between them.* We shall say that A and B are *equipotent* (or *equinumerous*, or *have the same cardinality*) if there exists a bijection between A and B. In this case we write $|A| = |B|$.

As an example, the sets $\mathbf{N}$ and $\mathbf{N} \setminus \{0\}$ are equipotent, since f given by $n \mapsto n + 1$ is a bijection $\mathbf{N} \to \mathbf{N} \setminus \{0\}$. (Check that $f^{-1}(m) = m - 1$ is its inverse.)

It is even possible to remove an infinite number of elements from $\mathbf{N}$ and end up with something still equipotent with $\mathbf{N}$. To see this, let E be the set of nonnegative even integers, and consider the function $f : \mathbf{N} \to E$ sending $n \mapsto 2n$. This is injective because if $2m = 2n$, then dividing out by 2 on both sides yields $m = n$. It is surjective because if $n \in E$, then $n = 2k$ for some $k \in \mathbf{N}$, by definition, and $f(k) = 2k = n$.

So we can find subsets of $\mathbf{N}$ equipotent with it. It turns out we can also find supersets of $\mathbf{N}$ with the same property.

Theorem 24. *We have $|\mathbf{N}| = |\mathbf{Z}|$.*

Proof. We define $f : \mathbf{N} \to \mathbf{Z}$ by

$$
f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even;} \\ -\frac{n+1}{2}, & \text{if } n \text{ is odd.} \end{cases}
$$

We shall show that f is a bijection.

Note first that if n is even, then $f(n) \geq 0$, and if n is odd, then $f(n) < 0$. So if $f(m) = f(n)$ for some $m, n \in \mathbf{N}$, then $f(m)$ and $f(n)$ must either both be

negative, or both be nonnegative. Either way, m and n are either both even or they are both odd. If m and n are both even, then from $f(m) = f(n)$ we derive

$$\frac{m}{2} = \frac{n}{2},$$

whence multiplying by 2 on both sides we see that $m = n$. If m and n are both odd, then

$$-\frac{m+1}{2} = -\frac{n+1}{2},$$

so, multiplying by -2 and subtracting 1 from both sides we have $m = n$ in this case as well.

Now we show that f is surjective. Let $k \in \mathbf{Z}$. If $k \geq 0$, then consider $n = 2k$. We have

$$f(n) = f(2k) = \frac{2k}{2} = k.$$

If $k < 0$, then consider $n = -2k - 1$. (Check that this is an element of $\mathbf{N}$.) Then

$$f(n) = f(-2k - 1) = -\frac{-2k - 1 + 1}{2} = -\frac{-2k}{2} = k.$$

This shows that f is surjective, so f is in fact bijective and we conclude that $|\mathbf{N}| = |\mathbf{Z}|$. ∎

We say that a set A is *countably infinite* if there exists a bijection $f : \mathbf{N} \to A$, that is, if $|\mathbf{N}| = |A|$. A set is said to be *countable* if it is either finite or countably infinite. Otherwise it is called *uncountable*. The previous theorem shows that $\mathbf{Z}$ is countably infinite.

Sometimes it is difficult to come up with a bijection directly. Instead, we would like to find an injection from A to B (which, in some sense, shows that $|A| \leq |B|$), and then an injection from B to A. This is made possible by the following useful theorem, named for Ernst Schröder and Felix Bernstein, who independently proved it in 1898. The proof is a bit difficult, so it's technically outside the scope of the course. For fun, you might try to do it as an exercise.

Theorem 25. (*Schröder–Bernstein theorem*). *If there exists an injective function $f : A \to B$ and another injective function $g : B \to A$, then there is a bijection $h : A \to B$.*

Proof. We present the proof as a (difficult) exercise. Here is the roadmap. Call $b \in B$ *unattached* if there is no $a \in A$ such that $f(a) = b$. Let $h : B \to B$ be given by $h(b) = f\big(g(b)\big)$. Given $b, b' \in B$, we shall say that b is a *peer* of b' if either $b = b'$ or there exists some $n \in \mathbf{N}$ such that

$$b = \underbrace{h(h(\cdots(h(b'))\cdots))}_{n \text{ times.}}$$

Say that $b \in B$ is a *PAE* if it is the peer of an unattached element. (So unattached elements are automatically PAEs, by setting $n = 0$.)

a) Show that if $a \in A$ is such that $f(a)$ is a PAE, then there is a unique element $b^* \in B$ such that $g(b^*) = a$, and that this element is a PAE.

By part (a), if $f(a)$ is a PAE, it makes sense to speak of $g^{-1}(a)$. It is the element $b^* \in B$ such that $g(b^*) = a$. From here we define

$$r(a) = \begin{cases} g^{-1}(a), & \text{if } f(a) \text{ is a PAE;} \\ f(a), & \text{otherwise.} \end{cases}$$

b) Show that if $b \in B$ is a PAE then so is $f\big(g(b)\big)$.
c) Show that r is surjective. [*Hint*: Do a proof by cases. Every $b \in B$ is either a PAE or it is not a PAE.]
d) We already proved in part (a) that if $f(a)$ is a PAE, then so is $r(a)$. Prove the converse of this statement.
e) Show that r is injective, and therefore bijective. [*Hint*: Assume $r(a_1) = r(a_2)$, and do a proof by cases again. Part (d) will be useful here.] ▮

Once again, this proof is outside the scope of the course. Don't lose sleep over it if you can't do it. Feel free to ask questions at office hours if you get stuck.

Using the Schröder–Bernstein theorem, we now show that the Cartesian product of two countable sets is also countable. In the proof, we shall employ the fact that if a set A is countable, then there exists an enumeration

$$A = \{a_0, a_1, a_2, \ldots\}.$$

(If f is the bijection given by the definition, we can set $a_0 = f(0)$, $a_1 = f(1)$, and so on.)

In the following proof, we'll also use the Fundamental Theorem of Arithmetic, which we state now, and prove later in the course (in the number theory section). It says that any integer can be factored as a product of primes, a theorem you should have learned in grade school.

Theorem 26 (*Fundamental Theorem of Arithmetic*). *Every positive integer $n \geq 2$ can be factored into a product*

$$p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n},$$

where $n \geq 0$ is an integer and, for $1 \leq i \leq n$, p_i is a prime and v_i is a positive integer. This factorisation is unique up to the order of the primes. ▮

Theorem 27. *If A and B are countably infinite sets, then $A \times B$ is also countably infinite.*

Proof. Enumerate $A = \{a_0, a_1, \ldots\}$ and $B = \{b_0, b_1, \ldots\}$. Now given $(a_i, b_j) \in A \times B$ for some $i, j \in \mathbf{N}$, we can let

$$f(a_i, b_j) = 2^i 3^j.$$

We show that this defines an injective function. Suppose that $f(a_i, b_j) = f(a_{i'}, b_{j'})$. Then $2^i 3^j = 2^{i'} 3^{j'}$, and by the uniqueness of prime factorisations in the Fundamental Theorem of Arithmetic, we see that $i = i'$ and $j = j'$.

Now we produce an injection $g : \mathbf{N} \to A \times B$ by simply setting

$$g(n) = (a_n, b_0).$$

It is clear this is injective, since if $g(m) = g(n)$, then $(a_m, b_0) = (a_n, b_0)$, and that implies that $m = n$. $\blacksquare$

Corollary 28. *We have $|\mathbf{Z} \times \mathbf{Z}| = |\mathbf{N}|$.*

Proof. We proved earlier that $\mathbf{Z}$ is countably infinite, so we may apply the previous theorem with $A = B = \mathbf{Z}$. $\blacksquare$

This corollary concerning $\mathbf{Z} \times \mathbf{Z}$ allows us to prove that $\mathbf{Q}$ is countable as well.

Theorem 29. *The set $\mathbf{Q}$ of rational numbers is countable.*

Proof. We define $f : \mathbf{Q} \to \mathbf{Z} \times \mathbf{Z}$ as follows. For an element $q \in \mathbf{Q}$, we let $q = a/b$ the fraction q written in lowest terms (where $a \in \mathbf{Z}$ and $b \in \mathbf{N} \setminus \{0\}$). Then we set $f(q) = (a, b)$. This is an injective function because if $f(q) = f(q')$, then writing $q = a/b$ and $q' = a'/b'$ in lowest terms, we have $(a, b) = (a', b')$, so $q = a/b = a'/b' = q'$.

To define an injection $g : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Q}$, we recycle the injection we had from the proof of Theorem 27. We already know that $\mathbf{Z}$ is countable, so fix an enumeration $\mathbf{Z} = \{a_0, a_1, a_2, \ldots\}$. Then let $g(a_i, a_j) = 2^i 3^j$. The range of g is a subset of $\mathbf{N}$, so *a fortiori* it is a subset of $\mathbf{Q}$, and we already showed before that it is an injection.

We have shown that $|\mathbf{Q}| = |\mathbf{Z} \times \mathbf{Z}|$, which in turn shows that $|\mathbf{Q}| = |\mathbf{N}|$, after applying Corollary 28. $\blacksquare$

So far, we have just given lots of examples of countably infinite sets. Finally, we give an example of a set that is not countably infinite.

Theorem 30. *The set A of all infinite binary strings is uncountable.*

Proof. Certainly A is not finite, so we need to show that $|\mathbf{N}| \neq A$.

Let $f : \mathbf{N} \to A$. We shall show that f is not surjective. For all $m, n \in \mathbf{N}$, let $a_{m,n}$ be the nth bit of $f(m)$. Consider the infinite binary string

$$s = (1 - a_{0,0}, 1 - a_{1,1}, 1 - a_{2,2}, 1 - a_{3,3}, \ldots).$$

This string s cannot equal $f(m)$ for any $m \in \mathbf{N}$, since given an arbitrary m, the mth bit of $f(m)$ is $a_{m,m}$, whereas the mth bit of s is $1 - a_{m,m}$. Hence there is some $s \in A$ such that $f(m) \neq s$ for all $m \in \mathbf{N}$. So f is not surjective.

Since there can be no surjection $f : \mathbf{N} \to A$, *a fortiori* we cannot have a bijection $\mathbf{N} \to A$. We conclude that $|A| \neq |\mathbf{N}|$. $\blacksquare$

The proof above was published by Georg Cantor in 1891, and hence is known as *Cantor's diagonal argument.* The technique has since been used to prove many other things.

The set of all infinite binary strings is in bijection with the set of all real numbers in the interval $[0, 1)$. If we're being extra pedantic, we need to forbid an infinite trailing string of all 1s, since, e.g., $0.0111\ldots = 0.1000\ldots$ after carrying the 1s (akin to the fact that, e.g., $0.0999\ldots = 0.1$). After dealing with this detail, one will have shown that $\bigl|[0,1]\bigr| \neq |\mathbf{N}|$.

7. Relations

01.X A *relation* on a set X is a subset $R \subseteq X \times X$. If $(a, b) \in R$ we write aRb and say "a is related to b." Here are some examples.

i) The set $L = \bigl\{(a,b) \in \mathbf{R} \times \mathbf{R} : a < b\bigr\}$ is a relation. For instance, we can write $(2, \pi) \in L$, or $2L\pi$, or $2 < \pi$ (which is the more common notation for this relation).

ii) The set $E = \bigl\{(a,b) \in \mathbf{R} \times \mathbf{R} : a = b\bigr\}$ is a relation (it is the "equals" relation).

iii) On $\mathbf{Z}$, the set
$$R = \bigl\{(-1, 4), (8, -3), (0, 0), (0, 1)\bigr\}$$
is a relation.

iv) For any set A, a function $f : A \to A$ is by definition a subset of $A \times A$, and hence is an example of a relation.

v) Let H be the set of all humans, define $M \subseteq H \times H$ by setting (h_1, h_2) if and only if h_1 is married to h_2. For instance,

$$(\text{Michelle Obama}, \text{Barack Obama}) \in M.$$

On the other hand, it is unfortunately the case that

$$(\text{Marcel Goh}, \text{Taylor Swift}) \notin M.$$

Properties of relations. Let $R \subseteq A \times A$ be a relation. R is called

i) *reflexive* if for all $a \in A$, aRa;

ii) *symmetric* if for all $a, b \in A$ with aRb, we also have bRa; and

iii) *transitive* if for all $a, b, c \in A$ with aRb and bRc, we also have aRc.

Going back to the examples we had above, the relation L is transitive but neither reflexive nor symmetric, the relation E satisfies all three properties, the relation R satisfies none of them, and the relation M is symmetric but neither reflexive nor transitive. (Convince yourself of all of these facts.)

As a more involved example, let X be any set with $|X| \geq 2$. On 2^X, define a relation R by

$$(A, B) \in R \Leftrightarrow A \cap B \neq \emptyset$$

for all $A, B \subseteq X$. Which of the three properties above does R satisfy?

Is it reflexive? Well, is it true that for all $A \subseteq X$, $A \cap A \neq \emptyset$? The answer is no, since we have $\emptyset \cap \emptyset = \emptyset$, so we have $(\emptyset, \emptyset) \notin R$.

Is R symmetric? Well, if $A \cap B \neq \emptyset$, then since $\cap$ is commutative, we have $B \cap A \neq \emptyset$ as well, so $(A, B) \in R$ implies that $(B, A) \in R$. In other words, yes, R is symmetric.

Is R transitive? If $A \cap B \neq \emptyset$ and $B \cap C \neq \emptyset$, does that necessarily mean that $A \cap C \neq \emptyset$? The answer is no. Here's the proof. Since $|X| \geq 2$ we can find $x, y \in X$ with $x \neq y$. Let $A = \{x\}$, $B = \{x, y\}$, and $C = \{y\}$. Then $A \cap B = \{x\} \neq \emptyset$, $B \cap C = \{y\} \neq \emptyset$, but alas $A \cap C = \emptyset$.

Equivalence relations and classes. If R is reflexive, symmetric, and transitive, then we say that R is an *equivalence relation*. Here are two examples (as an exercise, prove that both of these are equivalence relations).

  i) Let F be the set of all formulas in propositional logic with the variables p, q, and r, and operations $\neg$, $\wedge$, and $\vee$. The relation $\equiv$ defined by $f_1 \equiv f_2$ if and only if f_1 and f_2 have the same truth table is an equivalence relation.

 ii) On the set $\mathbf{R}^2$, define the relation $R \subseteq \mathbf{R}^2 \times \mathbf{R}^2$ by letting $(x, y)R(w, z)$ if and only if $\sqrt{x^2 + y^2} = \sqrt{w^2 + z^2}$. This is also an equivalence relation

If R is an equivalence relation, often we shall write $x \sim y$ to mean xRy. Sometimes we might even just say that $\sim$ *is* the equivalence relation.

Let $R \subseteq A \times A$ be an equivalence relation. Define the *equivalence class* of $a \in A$ to be the set

$$[a] = \{b \in A : a \sim b\}.$$

This is the set of all $b \in A$ that are related to a.

Take for instance the example F above of all formulas under the relation $\equiv$. The equivalence class of the formula $p \vee \neg p$ is the set of all formulas whose truth table contains only 1s, that is, the set of all tautologies. And for the example R above, the equivalence class of the point $(1, 3)$ is the set

$$[(1,3)] = \{(x, y) \in \mathbf{R}^2 : \sqrt{10} = \sqrt{x^2 + y^2}\};$$

that is, the circle of radius $\sqrt{10}$ centred about the origin.

We have the following proposition concerning equivalence relations.

Proposition 31. *Let R be an equivalence relation on A. Then*

  i) *for all $x \in A$, $x \in [x]$;*

 ii) *for all $x, y \in A$, $x \sim y$ if and only if $[x] = [y]$; and*

iii) *for all $x, y \in A$, $x \not\sim y$ if and only if $[x] \cap [y] = \emptyset$.*

Proof. Let $x \in A$. Since R is reflexive, $x \sim x$, so we have $x \in [x]$. This proves part (i).

For part (ii), first we prove the "only if" direction. Let $x, y \in A$ be such that $x \sim y$. To prove that $[x] \subseteq [y]$, we let $z \in [x]$; so $x \sim z$. By symmetry, we have $z \sim x$, and this combined with $x \sim y$ allow us to deduce that $z \sim y$, by transitivity. Then by symmetry again, we have $y \sim z$, so $z \in [y]$. *Mutatis mutandis*, i.e., by swapping the roles of x and y, we also have $[y] \subseteq [x]$. Hence $[x] = [y]$.

Now for the "if" direction of (ii). Let $x, y \in A$ be such that $[x] = [y]$. By (i), we have $x \in [x]$, but then this means that $x \in [y]$. By definition of $[y]$, this means that $y \sim x$, so $x \sim y$ by symmetry.

On to part (iii). We prove both implications by contraposition (that is, we negate both sides of the statement). Let $x, y \in A$ be such that $[x] \cap [y] \neq \emptyset$. This means there is some $z \in A$ such that $z \in [x]$ and $z \in [y]$; so $x \sim z$ and $y \sim z$. By symmetry, $z \sim y$, so by transitivity, we have $x \sim y$.

On the other hand, suppose that $x, y \in A$ satisfy $x \sim y$. By (ii), we have $[x] = [y]$, so $[x] \cap [y] = [x] \neq \emptyset$, where we know that $[x] \neq \emptyset$ because it contains at least x (again, using (i)). ∎

Let A be a set. A *partition* of A is a set P of subsets of A (i.e., $P \subseteq 2^A$), such that

  i) for all $x \in A$ there exists $S \in P$ such that $x \in S$;

 ii) for all $S_1, S_2 \in P$ with $S_1 \neq S_2$, the intersection $S_1 \cap S_2$ is empty; and

iii) $\emptyset \notin P$.

Here are some examples.

  i) Let E be the set of all even integers and F the set of all odd integers. Then $\{E, F\}$ is a partition of $\mathbf{Z}$.

 ii) The set $\big\{(-\infty, 0), \{0\}, (0, \infty)\big\}$ is a partition of $\mathbf{R}$.