Lecture Notes for MATH 2040 Mathematical Logic I

Semester 1, 2009/10

Michael Rathjen

Chapter 0. Introduction

Maybe not all areas of human endeavour, but certainly the sciences presuppose an underlying acceptance of basic principles of logic. They may not have much in common in the way of subject matter or methodology but what they have in common is a certain standard of rationality. It is assumed that the participants can differentiate between rational argumentation based on accepted principles, and wild speculation or total nonsequiturs.

The importance of logic has been recognized since antiquity. Logical principles - principles connecting the syntactic structure of sentences with their truth and falsity, their meaning, or the validity of arguments in which they figure - can be found in scattered locations in the work of **Plato** (428–348 B.C.). The **Stoic** school of logic was founded some 300 years B.C. by **Zeno of Citium** (not to be confused with Zeno of Elea). After Zeno's death in 264 B.C., the school was led by **Cleanthes**, who was followed by **Chrysippus**. It was largely through the copious writings of Chrysippus that the Stoic school became established, though many of these writings have been lost.

The patterns of reasoning described by Stoic logic are the **patterns of interconnection between propositions** that are completely independent of what those propositions say. Thus, in Stoic logic, propositions are treated the way atoms are treated in present-day chemistry, where the focus is on the way atoms fit together to form molecules, rather than on the internal structure of atoms. The Stoics commenced their analysis by examining a number of ways in which two propositions can be combined to give a third, more complicated proposition. The operations of forming complex propositions from given propositions are called **connectives**. The **"if ... , then ..."** and **"or"** operations are examples of connectives. The Stoics studied the logic of connectives, also known as **propositional logic**. An example of a logically valid argument involving the connectives "or" and "not" is

A or B.

Not B.

A

The idea is that the third assertion, the one below the line, follows logically from the previous two.

The first known systematic study of logic which involved **quantifiers**, components such as "for all" and "some", was carried out by **Aristotle** (384–322 B.C.) whose work

was assembled by his students after his death as a treatise called the **Organon**, the first systematic treatise on logic.

Aristotle tried to analyze logical thinking in terms of simple inference rules called **syllogisms**. These are rules for deducing one assertion from exactly two others. An example of a syllogism is:

$P1$. All men are mortal.

$P2$. Socrates is a man.

C. Socrates is mortal.

Again, the idea is that the third assertion follows logically from the previous two. In the case of this simple example, this deduction certainly seems correct enough, albeit pretty obvious. But as with any scientific explanation, the idea is to uncover **general patterns** that apply in many instances. In the case of the above syllogism, it is obvious that there is a general pattern, namely:

$P1$. All M are P.

$P2$. S is a M.

C. S is P.

The general deduction rule is true whatever M, P and S may be.

Some of the other syllogisms Aristotle formulated are less obvious. For example the following rule is valid, but you have to think a bit to convince yourself that this is so:

$P1$. No M is P.

$P2$. Some S is M.

C. Some S is not P.

Aristotle's proposal was that any logical argument can, in principle, be broken down into a series of applications of a small number of syllogisms involved in logical reasoning. He listed a total of 19, though some on his list were subsequently shown to rely on a tacit assumption to be valid.

As it turned out, the syllogism was found to be too restrictive. There are logically valid arguments that cannot be broken down into a series of syllogisms, now matter how finely those arguments are analyzed. Nevertheless, Aristotle's attempt was one of the first to analyze logical thought, and for that alone his prominent place in history is well deserved. For almost 2000 years Aristotle was revered as the ultimate authority on logical matters.

> *Bachelors and Masters of arts who do not follow Aristotle's philosophy are subject to a fine of five shillings for each point of divergence, as well as for infractions of the rules of the ORGANON.*
>
> *– Statuses of the University of Oxford, fourteenth century.*

However, Aristotle's logic was very weak by modern standards. In particular it is too weak to account for most of the inferences employed in mathematics. In the centuries following Aristotle, various people tried to extend his theory. However, major advances in logic were not achieved until the seventeenth century. The ideas of creating an artificial formal language patterned on mathematical notation in order to clarify logical relationships - called **characteristica universalis** - and of reducing logical inference to a mechanical reasoning process in a purely formal language - called **calculus rationatur** - were due to Gottfried Wilhelm **Leibniz** (1646-1716). But logic as we know it today has only emerged over the past 120 years. The name chiefly associated with this emergence is Gottlob **Frege** (1848 - 1925) who in his **Begriffsschrift 1879** (Concept Script) invented the first programming language. His Begriffsschrift marked a turning point in the history of logic. It broke new ground, including a rigorous treatment of quantifiers and the ideas of functions and variables. Frege wanted to show that mathematics grew out of logic, but in so doing devised techniques that took him far beyond the Aristotelian syllogistic and Stoic propositional logic that had come down to him in the logical tradition.

One reason for using a precise mathematical language and grammar is that the statements of mathematics are supposed to be completely precise, and it is not possible to achieve complete precision unless the language one uses is free of many of the vaguenesses and ambiguities of ordinary speech. Mathematical sentences can also be highly complex: if the parts that made them up were not clear and simple, then the unclarities would rapidly accumulate and render the sentences unintelligible. An ambiguity in the English language is exploited by the following old joke that suggests that traditional grammar, with its structuring principle of parts of speech into subjects, predicates, and objects, needs to be radically rethought.

> *Nothing is better than lifelong happiness.*
> *But a cheese sandwich is better than nothing.*
> *Therefore, a cheese sandwich is better than lifelong happiness.*

Let us try to be precise about how this play on words works. It hinges on the word "nothing", which is used in two different ways. The first sentence means **"There is no single thing that is better than lifelong happiness"**, whereas the second means **"It is better to have a cheese sandwich than nothing at all."** In other words, in the second sentence "nothing" stands for what one might call the null option, the option of having nothing, whereas in the first it does not (to have nothing is not better than to have lifelong happiness).

Words like "all", "some", "any", "every", and "nothing" are examples of **quantifiers**, and in the English language they are highly prone to this kind of ambiguity.

The 20th Century

Over the past century the study of logic has undergone rapid and important advances. Spurred on by logical problems in that most deductive discipline, mathematics, it developed into a discipline in its own right, with its own concepts, methods, techniques, and language.

More recently the study of logic has played a major role in the development of modern day computers and programming languages. Logic continues to play an im-

portant part in computer science. Some of the central questions of mathematical logic are:

- **What is a mathematical proof?**
- **How can axioms and proofs be justified?**
  (The foundations of mathematics)
- **Are there limitations to provability?**
- **To what extent can machines carry out mathematical proofs?**

Only in the last century has there been success in obtaining substantial and satisfactory answers.

(Notes from chapter 1 onwards are based on those by Dr. M. Messmer)

Chapter I. Sets, Functions, Countable sets, Mathematical Induction

Up to a point, one can do and speak mathematics without knowing how to classify the different sorts of words one is using, but many of the sentences of advanced mathematics have a complicated structure that is much easier to understand if one knows a few basic terms from set theory and logic. It is a surprising fact that a small number of set-theoretic concepts and logical terms can be used to provide a precise language that is versatile enough to express all the statements of ordinary mathematics.

1.1. A bit of Naive Set Theory

Goal. Get used to notation, practice some basic proof writing, see the connection with propositional logic.

We introduce *naive set theory* – the point here is that we do not give formal axioms. Part of the idea is to get used to set theory notation, and to writing proofs – both essential later in the module.

Set theory is the creation of the German mathematician Georg **Cantor** (1845–1918). What is a set?

1.1 (Naive) Definition A *set* is a collection of distinct objects , called its *elements* or *members*.
If x is an element of the set A, we write $x \in A$.
We write $x \notin A$, if x is not an element of A.

Remark. Two sets A and B are equal, written $A = B$, if they have the same elements; for example $\{x \in \mathbb{R} : x \geq 0\} = \{x \in \mathbb{R} : \text{ there is a } y \in \mathbb{R} \text{ with } y^2 = x\}$.

Why did I call the above definition 'naive'?

It can lead to contradictions:

1.2 Russell's Paradox (1901). Some sets are members of themselves. For example, let
$A =$ the set consisting of all sets describable in ten words.
The sentence on the right has ten words, so $A \in A$.

Consider the collection X of sets which are not elements of themselves, i.e. $X = \{x : x \text{ is a set and } x \notin x\}$. Then consider the question: Is $X \in X$?
If $X \in X$, then $X \notin X$ by definition of X.
If $X \notin X$, then $X \in X$ by definition of X.
So the question can't be answered. That is, we have a contradiction.

This paradox comes in many different guises, for example:

> There is a barber who shaves all and only those people who don't shave themselves. Decide whether he shaves himself or not!

These paradoxes showed that set theory had to be put on a solid, axiomatic foundation. This was carried out by Ernst **Zermelo** in 1908. His axiomatization was

later modified by Abraham Fraenkel into what we now call **ZF** set-theory. Ultimately every mathematical object can be thought of (more precisely 'is') a set, built from the empty set $\emptyset$. For example each natural number is a set as follows:

$0 = \emptyset$
$1 = \{\emptyset\}$
$2 = \{\emptyset, \{\emptyset\}\}$
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$
$\dots$

But not every collection of objects we can think of, can be allowed to be a set,because of Russell's Paradox..

Since this course is not about set theory, we will take the 'naive' approach and work with Definition 1.

1.3 Definition. (a) A is a *subset* of B, written, $A \subseteq B$, if every element in A belongs to B. We also say A is *contained* in B. Note $A \subseteq A$.
(b) A is a *proper* subset of B, written $A \subset B$, or $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$. We also say that A is strictly contained in B.

1.4 Examples.
(a) $\emptyset$ is the empty set. Note: $\emptyset \subseteq A$ for every set A.
(b) Sets of numbers:
$\mathbb{N} = \{0, 1, 2, 3, 4, 5 \dots\}$, the set of natural numbers.
$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$, the set of integers.
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$, the set of rational numbers.
$\mathbb{R}$ = 'the set of all decimal numbers' (= the completion of $\mathbb{Q}$).
$\mathbb{C}$ = 'the complex numbers'
(c) The set of all even integers.
(d) The set of all functions from $\mathbb{Q}$ to $\mathbb{R}$, also written as $\mathbb{R}^{\mathbb{Q}}$.
(e) For $n \in \mathbb{N}$, the set $[n] = \{0, 1, 2, 3, \dots, n-1\}$.
(f) If A is a set, and P is some *condition* or *property* then

$$\{x \in A : x \text{ has property } P\}$$

is a set. For example, $\{x \in \mathbb{R} : x^2 = -1\} = \emptyset$.

How do we show that two sets are the same? For example we can use that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$, i.e. every element in A is in B, and every element in B is in A.

Boolean Operations on Sets.

1.5 Definition. Let A and B be sets.

(1) The *union* $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

(2) The *intersection* $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

(3) The *difference* $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.

(4) A and B are called disjoint, if $A \cap B = \emptyset$.

(5) The *complement* of A in some fixed universe U is $A^c = \bar{A} = -A = U - A = \{x \in U : x \notin A\}$.

Visualize by Venn-Diagrams.

1.6 Lemma. Let A and B be sets. Then

(1) $A \cup B = B \cup A$.

(2) $A \cap B = B \cap A$.

(3) $(A \setminus B) \cap (B \setminus A) = \emptyset$.

(4) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

(5) $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

(6) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

(7) De Morgan's Laws:
(i) $(A \cap B)^c = A^c \cup B^c$.
(ii) $(A \cup B)^c = A^c \cap B^c$

Proof. In class and homework.

1.7 Definition. The *power set* $\mathcal{P}(A)$ of A is the set of all subsets of A.

For example, for $A = \{1, 2\}$, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Question: If A has n elements then $\mathcal{P}(A)$ has how many elements?
We will come back to this question later.

If A is a finite set, we will write $|A| = n$ if A has n elements.

1.8 Definition. Let A and B be sets.
(a) The *cartesian product* of A and B, written $A \times B$ is the set

$$\{(x, y) : x \in A, y \in B\}.$$

The elements (x, y) are called *ordered pairs* or *2-tuples*.

Remark: $(x, y) \neq (y, x)$, unless $x = y$. However: $\{x, y\} = \{y, x\}$.

(b) The set of *k-tuples* over A is $A^k = \{(x_1, \ldots, x_k) : x_i \in A\}$.

Note $A^2 = A \times A$.

For A and B finite sets, $|A \times B| = |A| \cdot |B|$ and $|A^k| = |A|^k$.

1.9 Example. Let $A = \{1, 3, 5\}$.
The set of ordered pairs over A is

$$A \times A = \{(1,1), (1,3), (1,5), (3,1), (3,3), (3,5), (5,1), (5,3), (5,5)\}.$$

The set of 2-element subsets of A is $\{\{1, 3\}, \{1, 5\}, \{3, 5\}\}$.

Functions

1.10 (Vague) Definition. A *function* from a set A to a set B is a rule which assigns to each element $a \in A$ a unique element $b \in B$. Write $f : A \to B$, with $x \mapsto f(x)$.

But what is a 'rule'?

1.11 (Precise) Definition. A *function* f from a set A to a set B is a non-empty subset of $A \times B$ such that for each element $a \in A$ there is one and only one pair $(x, y) \in f$ with $x = a$, i.e. for all $a \in A$ there is $b \in B$ with $(a, b) \in f$, and for all $a \in A$, and $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

(This set f is also referred to as the graph of f. So we identify f with its graph; i.e. writing $f(x) = y$ really means $(x, y) \in f$.)

A is called the *domain* of f, B is called the *codomain* of f.

If $(a, b) \in f$, then we say that b is the *image of* a *under* f or the *value of* f *at* a, and write $b = f(a)$.

The set $f(A) = \{f(a) : a \in A\} = \{b \in B :$ there is $a \in A$ with $(a, b) \in f\}$ is called the *image of* A under f, the *image of* f, or the *range of* f.

Example. Consider $f : \mathbb{Z} \to \mathbb{N}$ with $f(n) = n^2$. Then, formally,

$$f = \{(0, 0), (1, 1), (-1, 1), (2, 4), (-2, 4), (3, 9), (-3, 9), \ldots\}.$$

The domain of f is $\mathbb{Z}$, and the codomain is $\mathbb{N}$. Then the range of f is a proper subset of $\mathbb{N}$, namely $\text{Range}(f) = \{0, 1, 4, 9, \ldots\}$.

For $g : \mathbb{R} \to \mathbb{R}$ with $x \mapsto x^3$, the range of f equals the codomain.

Injections, Surjections, Bijections.

1.12 Definition. A function f from A to B is called *injective* (an *injection*, or *one-to-one*) if for every $b \in B$ there is at most one $a \in A$ with $f(a) = b$.

Equivalently: $f : A \to B$ is injective if for all $x_1, x_2 \in A$, $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$.

Equivalently: $f : A \to B$ is injective if for all $x_1, x_2 \in A$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. (This last is generally the most convenient form to work with.)

1.13 Examples. Which of the following functions is injective, which is not?

(i) $f : \mathbb{R} \to \mathbb{R}$, with $f(x) = x^3$.
(ii) $g : \mathbb{R} \to \mathbb{R}$ with $g(x) = x^2$
(iii) $h : \mathbb{N} \to \mathbb{Z}$ with $h(x) = x^2$.
(iv) $j : \mathbb{Z} \to \mathbb{Z}$ with $j(x) = x^2$,
(v) $k : \mathbb{N} \to \{0, 1\}$ with $f(n) = \begin{cases} 0 & \text{, if } n \text{ is even} \\ 1 & \text{, if } n \text{ is odd} \end{cases}$
(vi) $l : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, where $f(n, m) = n + m$.
Ans: Only (i), (iii) are injective.

1.14 Definition. A function $f : A \to B$ is called *surjective* (a *surjection*, or *onto*) if for all $b \in B$ there is at least one $a \in A$ with $f(a) = b$.

Equivalently: $f : A \to B$ is surjective if all elements in B are images.

Examples Which of the functions in Examples 1.13 are surjective? Answer: (i), (v), (vi).

1.15 Definition. If $f : A \to B$ and $g : B \to C$ are functions, then the *composition* $h := g \circ f : A \to C$ is defined by: $h(x) = g(f(x))$ for all $x \in A$.

1.16 Exercise. In 1.15, if f, g are injective, so is $g \circ f$. If f, g are both surjective, so is $g \circ f$. Prove these facts!

Combining both conditions:

1.17 Definition. A function $f : A \to B$ is called *bijective* (a *bijection*, or a *one-to-one correspondence*) if f is injective and surjective.

Equivalently: $f : A \to B$ is bijective if for all b in B there is exactly one a in A with $f(a) = b$.

So a bijection $f : A \to B$ establishes a one-to-one correspondence between the elements of A and the elements of B.

Note. If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is also a bijection.

1.18 Examples. Each of the following are bijections. Write down their inverses.

(i) Most trivial example: For any set A, the function $f : A \to A$ with $f(a) = a$ for all a is a bijection.

(ii) $f : \mathbb{Z} \to \mathbb{Z}$ with $f(x) = x + 1$.

(iii) $f : \mathbb{Q} \to \mathbb{Q}$ with $f(x) = 2x$.

(iv) $f : (0, 1] \to [1, \infty)$ with $f(x) = \frac{1}{x}$.

1.3. Cardinality – the sizes of sets

How can we find a mathematically precise way for measuring the 'size' of a set, particularly of an infinite set? Do all infinite sets have the same 'size'?

In this module we will not formally define the size/cardinality $|A|$ of a set A. We will only be able to compare sizes of sets, we give a meaning to the expression $|A| \leq |B|$.

For finite sets, it's pretty obvious that we just have to count the number of elements. More formally:

1.19 Definition.

(1) A set A is *finite* if $A = \emptyset$ or there is a bijection from A to $[n] = \{0, 1, 2, \ldots, n-1\}$ for some $n \geq 1$. Then we say that A has n elements, and we write $|A| = n$ ($|A| = 0$ for $A = \emptyset$).

(2) We say that A is *infinite* if A is not finite.

(3) Two sets A and B are said to have *the same cardinality* (the same size) if there is a bijection from A to B (or equivalently from B to A). In this case, we write $|A| = |B|$ or also $A =_c B$.

(4) With $|A| \leq |B|$ (or $A \leq_c B$) we convey that there is an injection from A to B.

1.20 Lemma. (i) $|A| \leq |B|$ if and only if $A = \emptyset$ or there is an surjection from B to A.

(ii) $|A| \leq |B|$ and $|B| \leq |C|$ imply $|A| \leq |C|$. Likewise $|A| = |B|$ and $|B| = |C|$ imply $|A| = |C|$.

Proof. For (i) see HW2, Q4. (ii) follows from Exercise 1.16.

1.21 Theorem (Schröder-Bernstein). If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$. This is not obvious: you have to stitch together two injections (or two surjections) to create a bijection. This is beyond this module, but a proof can be found in many set theory books.

Note: We have not defined what the cardinality of A *is*!

Let's first look at the size of some finite sets:

Question. How many different functions are there from $A = \{a, b, c\}$ to $B = \{0, 1\}$?

Answer. For each element of A there are 2 possibilities for its image. So there are $2 \cdot 2 \cdot 2 = 8$ different such functions.

1.22 Lemma. (i) In general, if $|A| = m$ and $|B| = n$ $(m, n \geq 1))$, there are $|B|^{|A|} = n^m$ different functions from A to B.

The set of all functions from A to B is often denoted by B^A, and for A and B finite we have $|B^A| = |B|^{|A|}$. See Problem Sheet 2, Q2.

(ii) For $|A| = n$, $|\mathcal{P}(A)| = 2^n$.

Proof. (i) For every element in A there are n possibilities for its image.

(ii) By HW2 Q3, there is a bijection

$$\begin{array}{rccc} G: & \mathcal{P}(A) & \to & \{0,1\}^A \\ & S & \mapsto & f_S \end{array}$$

Therefore, $|\mathcal{P}(A)| = |\{0, 1\}^A| = 2^{|A|} = 2^n$.

Here is a complete proof:

Any subset S of A can be identified with the following function

$$f_S : A \to \{0, 1\} \text{ with } f_S(a) = \begin{cases} 0 & \text{, if } a \notin S \\ 1 & \text{, if } a \in S \end{cases}$$

The function f_S is called the *characteristic function* of S.
In fact, we have a bijection:

$$\begin{array}{rccc} G: & \mathcal{P}(A) & \to & \{0,1\}^A \\ & S & \mapsto & f_S \end{array}$$

Therefore, $|\mathcal{P}(A)| = |\{0,1\}^A| = 2^{|A|} = 2^n$.

1.23 Question. For A and B finite sets, how many bijections are there from A to B?

Answer. If $|A| \neq |B|$, there are none. If $|A| = |B| = n \geq 1$, there are $n!$ bijections from A to B. Why?

How 'big' are infinite sets?

1.24 Definition. A set S is called *countably infinite* (or has *cardinality* $\aleph_0$, read 'aleph zero' or 'aleph nought') if it has the same cardinality as $\mathbb{N}$, i.e. if there is a bijection from $\mathbb{N}$ to S (or from S to $\mathbb{N}$).

A set S is called *countable*, if S is finite or countably infinite.

1.25 Examples.

(i) Let $E \subseteq \mathbb{N}$ be the set of all even natural numbers, $E = \{0, 2, 4, 6, \ldots\}$. Then E is countably infinite since $f : \mathbb{N} \to E$ with $f(n) = 2n$ is a bijection.

(ii) *Claim.* $\mathbb{Z}$, the set of integers, is countably infinite.

Proof. Define $f : \mathbb{N} \to \mathbb{Z}$ as follows:

$$f(n) = \begin{cases} m & \text{, if } n = 2m \\ -m & \text{, if } n = 2m-1 \end{cases}$$

Describe this function? How are the elements of $\mathbb{Z}$ 'listed'? Show that f is a bijection. $f(0) = 0$, $f(1) = -1$, $f(2) = 1$, $f(3) = -2$, $f(4) = 2$, etc.

1.26 Theorem. $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Proof. Idea:

j / i	0	1	2	$\ldots$
0	$(0,0)$	$(0,1)$	$(0,2)$	$\ldots$
1	$(1,0)$	$(1,1)$	$(1,2)$	$\ldots$
2	$(2,0)$	$(2,1)$	$(2,2)$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Note:

1. On every diagonal, the sum of the two coordinates $i + j$ is constant.
2. $1 + 2 + 3 + \cdots + (i + j) = \frac{(i+j)(i+j+1)}{2}$

So define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$f((i,j)) = \frac{(i+j)(i+j+1)}{2} + j$$

Note: Another bijection f from $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$ is given by $f(i,j) = 2^i(2j+1)-1$. Prove that this works!

1.27 Corollary. $\mathbb{N}^k$ has cardinality $\aleph_0$ for all $k \geq 1$.

Proof. Idea:

$k = 1$: $\mathbb{N}$ is countably infinite.

$k = 2$: $\mathbb{N}\times\mathbb{N}$ is countably infinite by the previous theorem.

$k = 3$: For $\mathbb{N}\times\mathbb{N}\times\mathbb{N} = (\mathbb{N}\times\mathbb{N})\times\mathbb{N}$ use the function f from the proof of the previous theorem to define a bijection g from $(\mathbb{N}\times\mathbb{N})\times\mathbb{N}$ to $\mathbb{N}$ as follows:

$$g((i,j,k)) = f(f(i,j),k)$$

$k = 4$: keep going.

This proof requires induction on k. This will be discussed later.

How about

$$\mathbb{N}\cup\mathbb{N}^2\cup\mathbb{N}^3\cup\ldots = \bigcup_{k\geq 1}\mathbb{N}^k \ ?$$

This is the set of all finite tuples (or sequences) over $\mathbb{N}$. It is a countably infinite union of countably infinite sets.

(Note: Usually one includes the empty sequence as an element in this set and looks at $\bigcup_{k\geq 0}\mathbb{N}^k$.)

We will prove that a countable union of countable sets is countable.

We first need two lemmas:

1.28 Lemma. Any subset A of a countable set S is also countable.

Proof. If A is finite, there is nothing to show.

So suppose A is infinite. Then S is infinite and, since S is countable we can write $S = \{b_0, b_1, b_2, b_3, \ldots\}$. Then define the function $f : \mathbb{N}\to A$ inductively as follows.

$f(0)$ = the element b_i with smallest index i with $b_i \in A$, and

$f(n+1)$ = the element b_i with smallest index i with $b_i \in A\setminus\{f(0),\ldots,f(n)\}$.

"Clearly" (why?) f defines a bijection from $\mathbb{N}$ to A.

1.29 Lemma. Let $A \neq \emptyset$. The following are equivalent:

(i) A is countable.

(ii) There is a surjection from $\mathbb{N}$ to A.

(iii) There is a surjection from a countable set B onto A.

Proof. The proofs that (i) implies (ii), and that (ii) implies (iii) are trivial.

To prove that (iii) implies (i), let $f : B \to A$ be a surjection with B countable. So $B = \{b_0, b_1, b_2, \ldots, b_n\}$ if B is finite, or $B = \{b_0, b_1, b_2, b_3, \ldots\}$ if B infinite. Define $g : A \to B$ by letting

$$g(a) = b_i$$

where $f(a) = b_i$ and for all $j < i$, $f(a) \neq b_j$. Clearly g is an injection from A to B, and hence $A =_c g(A)$. Since $g(A)$ is countable by the previous lemma, A is countable.

1.30 Theorem. A countable union of countable sets is countable.

Proof. (Possibly a homework problem.) Let A_i, $i \in \mathbb{N}$, each be countable. We want to show that $A = \bigcup_{i \in \mathbb{N}} A_i$ (which means $A_0 \cup A_1 \cup A_2 \cup \ldots$) is countable. (Note: if this is a finite union many of the A_i are the same.)

By the previous lemma, for each $i \in \mathbb{N}$ there is a surjection $f_i : \mathbb{N} \to A_i$. Then define

$$f : \mathbb{N} \times \mathbb{N} \to A \text{ with } f(i, j) = f_i(j).$$

Clearly f is surjective and $\mathbb{N} \times \mathbb{N}$ is countable, so by the previous lemma, A is countable.

1.31 Theorem. (Cantor) $\mathbb{Q}$ is countable.

Proof. $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$. Define

$$\begin{array}{rccl} f: & \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Q} \\ \text{with} & (a, b) & \mapsto & \begin{cases} 0 & \text{if } b = 0 \\ \frac{a}{b} & \text{if } b \neq 0 \end{cases} \end{array}$$

Clearly f is onto. Since $\mathbb{Z}$ is countable, $\mathbb{Z} \times \mathbb{Z}$ is countable (Why?). So by Lemma 1.29 $\mathbb{Q}$ is countable.

Note: This theorem says that one can *list* the rational numbers. Note however that it is impossible to list them in their natural order, since between any two rational numbers there are infinitely many other rational numbers. The ordering of this list is very different from the usual ordering.

Question. Are there sets which are not countable?

Answer. Yes, lots of them. First we will to show that the set of real numbers $\mathbb{R}$ is not countable.

Decimal Expansions. One way of representing the real numbers is via decimal expansions:

> *Every real number can be written in the form $k.d_1d_2d_3\ldots$ where k is an integer and $d_i \in \{0, 1, 2, \ldots, 9\}$.*

This representation is unique except for those decimal expansions which are constantly 9 from some point onward (i.e end with recurring 9s).

Example:

$0.999\ldots = 0.\bar{9} = 1 = 1.000\ldots$

$-5.12999\ldots = -5.13 = -5.13000\ldots.$

We will use only representations which are not constantly 9 from some point onward. So we can assume that the representation is unique.

1.32 Theorem. $\mathbb{R}$ is not countable. (We say $\mathbb{R}$ is uncountable.)

Note that this means that there is no way to make a '(countably) infinitely long list' of all the real numbers.

Proof. Suppose $\mathbb{R}$ is countable. Then $[0,1) \subset \mathbb{R}$ is countable. Then there is a bijection $f : \mathbb{N} \to [0,1)$. We will show that f is not onto (which is a contradiction): We write each real $f(0), f(1), f(2), \ldots$ in the form

$$f(i) = 0.d_0^i d_1^i d_2^i \ldots.$$

Let

$$\begin{aligned} f(0) &= 0.d_0^0\, d_1^0\, d_2^0\, d_3^0\, \ldots \\ f(1) &= 0.d_0^1\, d_1^1\, d_2^1\, d_3^1\, \ldots \\ f(2) &= 0.d_0^2\, d_1^2\, d_2^2\, d_3^2\, \ldots \\ f(3) &= 0.d_0^3\, d_1^3\, d_2^3\, d_3^3\, \ldots \\ \vdots &\qquad\quad \vdots \end{aligned}$$

using decimal expansions described above without recurring 9s.

Define $r = 0.d_0^*\, d_1^*\, d_2^*\, d_3^*\, \ldots$

$$\text{by } d_i^* = \begin{cases} 4 & \text{if } d_i^i \neq 4 \\ 5 & \text{if } d_i^i = 4 \end{cases} \quad \text{for all } i \geq 0.$$

Example: If

$$\begin{aligned} f(0) &= 0.\underline{1}32978113\ldots \\ f(1) &= 0.0\underline{1}9620013\ldots \\ f(2) &= 0.00\underline{0}000000\ldots \\ f(3) &= 0.223\underline{4}44444\ldots \\ f(4) &= 0.42392\underline{8}776\ldots \\ \vdots &\qquad\quad \vdots \end{aligned}$$

then $r = 0.44454\ldots$.

So $r \neq f(i)$ for all $i \in \mathbb{N}$ since r differs from $f(i)$ in the i'th place. Thus, $r \in [0,1)$, but r is not in the range of f. So f is not surjective, which is a contradiction. So our assumption that $\mathbb{R}$ is countable was wrong.

Remark. This type of proof is called a **diagonal argument**. The proof of the following theorem also uses a diagonal argument (in a more abstract form).

1.33 Theorem (Cantor). For any set X, $|\mathcal{P}(X)| \neq |X|$.

Note: Clearly $|X| \leq |\mathcal{P}(X)|$, since there is an injection $f : X \to \mathcal{P}(X)$ given by $f(x) = \{x\}$ for all $x \in X$. Thus,the theorem means that the power set of a set X is strictly larger than X, i.e. there cannot be a bijection from X to $\mathcal{P}(X)$. So there are arbitrarily large infinite sets, and

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots.$$

Proof of Theorem 1.33. If $X = \emptyset$ the statement is true since $|X| = |\emptyset| = 0$ and $|\mathcal{P}(X)| = 1$ (as $\mathcal{P}(\emptyset) = \{\emptyset\}$ – why?).

So suppose $X \neq \emptyset$, and let $f : X \to \mathcal{P}(X)$ be a function. We will show that f cannot be surjective.

Define

$$S = \{x \in X : x \notin f(x)\}.$$

S is different from all $f(y)$ since they differ on the element y. (More precisely, for each y,

$$y \in f(y) \Leftrightarrow y \notin S,$$

so $y \neq f(S)$.)

So S is not in the range of f,so f is not surjective. This completes the proof.

1.34 Exercise. Why is the following not a proof of this theorem? The function $f : X \to \mathcal{P}(X)$ with $f(x) = \{x\}$ for each $x \in X$ is not a surjection. So $|X| \neq |\mathcal{P}(X)|$.

1.35 Question. Where does $|\mathbb{R}|$ fit into the hierarchy

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots?$$

1.36 Remarks. (1) For any set X, $|\mathcal{P}(X)| = |[2]^X|$. (Recall: as $[2] := \{0, 1\}$, $[2]^X$ is the set of all functions from X to $\{0, 1\}$, also denoted by 2^X.)

Proof. For every subset S of X define the function

$$f_S : X \to \{0, 1\} \text{ with } f_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{if } x \notin S \end{cases}$$

(f_S is the characteristic function of S which we defined earlier.)

Then the function $F : \mathcal{P}(X) \to 2^X$ with $F(S) = f_S$ is a bijection. Therefore $|\mathcal{P}(X)| = |2^X|$.

(2) One can show that $|\mathbb{R}| = |2^{\mathbb{N}}|$ by using the fact that every real number has a binary representation (using 0 and 1). So $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Mathematical Induction

I will assume some familiarity with mathematical induction.

1.37 Principle of Mathematical Induction.

Let $P(n)$ be a statement about the natural number n.

If

(1) *Induction base:* $P(0)$ is true, **and**

(2) *Induction step:* for all $k \geq 0$, $P(k)$ implies $P(k+1)$,

then

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

1.38 Examples.

(i) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Prove it using induction!

(ii) $|P([n])| = 2^n$.

We proved this before without induction. Here is the hint for a proof using induction:

$$\mathcal{P}([n+1]) = \mathcal{P}([n]) \cup \{S \cup \{n\} \,:\, S \in \mathcal{P}([n])\}.$$

(iii) The sum of the first n odd numbers is n^2. That is,

$$1 + 3 + 5 + \ldots + (2n-1) = n^2.$$

1.39 Lemma We can start mathematical induction at any natural number:

Let $P(n)$ be a statement about the natural number n. Let n_0 be a fixed natural number. **If**

(1) *Induction base:* $P(n_0)$ is true, **and**

(2) *Induction step:* for all $k \geq n_0$, $P(k)$ implies $P(k+1)$,

then

$P(n)$ is true for all $n \geq n_0$.

1.40 Example. $2^n > n^3$ for all $n \geq 10$. Indeed, $2^{10} \geq 10^3$ (as $1028 > 1000$); and suppose $2^n \geq n^3$, with $n \geq 10$. Then $2^{n+1} = 2 \times 2^n \geq 2n^3 \geq n^3 + 3n^2 + 2n + 1 = (n+1)^3$. The last inequality holds because $n^3 \geq 7n^2 \geq 3n^2 + 3n + 1$ for $n \geq 10$.

1.41 Exercise. Show that all people have the same gender.

Proof. Let n be the number of people in the world. If $n = 1$, the statement is true. Now let $S = \{a_1, \ldots, a_{n+1}\}$ be the set of people. Since $|S \setminus \{a_1\}| = n$, by induction hypothesis all people in $S \setminus \{a_1\}$ have the same gender, the same gender as a_2. Also, since $|S \setminus \{a_{n+1}\}| = n$, by induction hypothesis all people in $S \setminus \{a_{n+1}\}$ have the same gender, again the same gender as a_2. So all people in S have the same gender as a_2.

What is wrong with this proof?

The argument does not work when $n = 1$.

Moral of the story: Make sure that the induction step holds for all relevant k.

There are certain situations (frequently in logic, but sometimes also in algebra) where we need

1.42 The Principle of Strong Induction:

Let $P(n)$ be a statement about the natural number n.

If

(1) *Induction base:* $P(0)$ is true, **and**

(2) *Induction step:* for all $k \geq 0$, *if* $P(i)$ is true for all $0 \leq i \leq k$, *then* $P(k+1)$ is true,

then

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

Note. Though I have formulated all these induction principles so that the inductive step involves an assumption on k, in practice we often don't introduce a symbol k, but just work directly with n.

1.43 Example. Every natural number is a product of prime numbers. (Here, $p \in \mathbb{N}$ is *prime* if $p \neq 0, 1$, and for any expression $p = ab$ where $a, b \in \mathbb{N}$, we have $a = 1$ or $b = 1$).

Proof. Let $P(k)$ be the statement that the natural number k is a product of primes. For $n = 0$ and $n = 1$ the statement is clearly true. Suppose $n \geq 2$ and $P(k)$ holds for all $k < n$. If n is prime, then $P(n)$ holds. Otherwise, there are $a, b \in \mathbb{N}$ with $a, b < n$ and $ab = n$. Since $P(a)$ and $P(b)$ hold, a and b are each a product of primes, and hence (multiplying all these primes together), so is n.

Chapter 2. Propositional Logic

How can we formalize the following arguments?

If demand rises, then companies expand.

If companies expand, then they hire workers.

If demand rises, then companies hire workers

and

This computer program has a bug, or the input is erroneous.

The input is not erroneous.

This computer program has a bug.

If the premises are true, then we cannot avoid the conclusions. The type of the argument in the first example is

If A, then B.

If B, then C.

If A, then C.

It doesn't matter what the propositions A, B, and C stand for.

The form of the argument in the second example is

A or B.

Not A.

B.

In Propositional Logic, rather than analyzing the meaning of 'atomic' sentences $A, B, C, \ldots$, we explore how more complicated statements are built from $A, B, C, \ldots$, and how their truth depends on that of $A, B, C, \ldots$.

Definition 2.1. (Syntax of propositional logic, PROP)

Alphabet and Symbols. The alphabet of the language consists of $A_1, A_2, A_3, \ldots$, called the *atomic formulas*. We use parentheses '(' and ')', and symbols $\neg, \wedge, \vee, \rightarrow$, which are called *logical connectives*.

Formulas are defined inductively as follows:

1. All atomic formulas $A_1, A_2, A_3, \ldots$ (or sometimes A, B, C) are formulas.
2. If F is a formula, then $(\neg F)$ is a formula, called the *negation* of F.
3. If F and G are formulas, then

   (i) $(F \vee G)$ is a formula, read as 'F or G', the *disjunction* of F and G.

(ii) $(F \wedge G)$ is a formula, read as 'F and G', the *conjunction* of F and G.

(iii) $(F \to G)$ is a formula, read as 'F implies G', or 'If F then G', called *implication*.

The parentheses are needed to make it unambiguous how a formula was formed. When it is unambiguous, we sometimes leave out some of the parenthesis. There adopt certain conventions about omitting parentheses, for example $\neg F \vee G$ means $(\neg F) \vee G$, not $\neg(F \vee G)$.

$(F \leftrightarrow G)$ is an abbreviation for $((F \to G) \wedge (G \to F))$.

The set of all formulas is denoted by FOM.

Note 2. To every formula is associated a tree, its **parsing tree**, which displays how the formula is generated:

For example the formula $(((\neg A_2) \to (A_4 \wedge A_5)) \vee A_1)$ has the following tree:

$$((\neg A_2) \to (A_4 \wedge A_5)) \vee A_1$$

$$(\neg A_2) \to (A_4 \wedge A_5)$$

$$\neg A_2 \qquad\qquad A_4 \wedge A_5$$

$$A_2 \qquad\qquad A_4 \qquad\qquad A_5 \qquad\qquad A_1$$

Important: The letters $A_1, A_2, A_3, \ldots$ and $A, B, C, \ldots$ always denote atomic formulas, whereas $F_1, F_2, F_3, \ldots$ and $F, G, H, \ldots$ denote arbitrary formulas.

2.2. Semantics for Propositional Logic.

In formal logic, we keep a clear distinction between:

- **syntax**: formal languages, formulas, proofs, strings of symbols, etc.

on the one hand and

- **semantics**: truth values, models, interpretation, meaning, content, etc.

on the other hand.

At this point, formulas are simply strings of symbols with no meaning assigned to them. The following definition associates them with the notion of truth:

Definition 2.3. (Semantics of Propositional Logic) A *truth assignment* is a function

$$\mu : FOM \to \{0, 1\}$$

satisfying the following conditions for all formulas $F, G \in \mathcal{F}$:

(1) $\mu((\neg F)) = 1 - \mu(F)$.

(2) $\mu((F \vee G)) = max\{\mu(F), \mu(G)\}$.

(3) $\mu((F \wedge G)) = \mu(F) \cdot \mu(G)$.

(4) $\mu((F \to G)) = max\{1 - \mu(F), \mu(G)\}$.

Here, 0 and 1 are called the truth values, where $\mu(F) = 0$ is interpreted as meaning 'F is false' and $\mu(F) = 1$ as 'F is true'.

Notice:

(1)′ $\mu((\neg F)) = 1$ iff $\mu(F) = 0$.

(2)′ $\mu((F \vee G)) = 1$ iff $\mu(F) = 1$ or $\mu(G) = 1$. ('or' always mean 'one or the other or both'.)

(3)′ $\mu((F \wedge G)) = 1$ iff $\mu(F) = 1$ and $\mu(G) = 1$.

(4)′ $\mu((F \to G)) = 1$ iff $\mu(F) = 0$ or $\mu(G) = 1$,
also $(\mu(F \to G)) = 0$ iff $\mu(F) = 1$ and $\mu(G) = 0$.

Example. Let A, B, C be atomic formulas with $\mu(A) = 1$, $\mu(B) = 1$, and $\mu(C) = 0$. What is $\mu(F)$, where $F = \neg((A \wedge B) \vee C)$? (Use the tree associated to this formula. You should find $\mu(F) = 0$.)

Remark 2.4. The truth table for implication "$\to$" coincides with the meaning of implication in the following scenario, where we make make a promise to a small child.

If the sun shines on Sunday, we go to the zoo.

Letting A stand for "*the sun shines on Sunday*" and B for "*we go to the zoo*", there is only one situation when the child could justifiably complain, namely when the sun shines on Sunday but we don't go to the zoo. This is when A is true but B is false. In all other cases, $A \to B$ is true, which is in keeping with not breaking our promise.

Lemma 2.5. If μ' is a function from $\{A_1, A_2, \ldots\}$ to $\{0, 1\}$, then μ' extends uniquely to a truth assignment μ. (So every truth assignment is uniquely determined by its values on $A_1, A_2, A_3, \ldots$.)

This is pretty obvious. But we will write down a precise proof, using induction on the length of the formulas. This is a standard method of proof in logic.

So let's first define the length of a formula.

Definition 2.6. The *length $l(F)$ of a formula F* is the number of symbols in F, counting atomic formulas, logical connectives and parenthesis.

Proof of Lemma 2.5. We have to show:

(a) *Existence.* If μ' is an arbitrary function from $\{A_1, A_2, \ldots\}$ to $\{0, 1\}$, then μ' extends to a truth assignment μ.

Prove this by induction on the length of a formula. The details are omitted.

(b) (*Uniqueness.* If μ_1 and μ_2 are two truth assignments with $\mu_1(A_i) = \mu_2(A_i)$ for all $i \geq 1$, then $\mu_1 = \mu_2$.

We prove part (b) by induction on the length of formulas. We show that for all $F \in \mathcal{F}$, $\mu_1(F) = \mu_2(F)$:

Induction base. $l(F) = 1$ means $F = A_i$. So $\mu_1(A_i) = \mu_2(A_i)$ as given.

Induction hypothesis. Let $n \geq 1$. Assume that for all formulas F with $l(F) \leq n$, $\mu_1(F) = \mu_2(F)$.

Induction step. Let $l(F) = n + 1$. Then F is built from simpler formulas (of smaller length) in one of four ways.

(i): $F = (\neg G)$. Since $l(G) \leq n$, $\mu_1(G) = \mu_2(G)$. So $\mu_1(F) = 1 - \mu_1(G) = 1 - \mu_2(G) = \mu_2(F)$.

(ii): $F = (G \vee H)$. Since $l(G) \leq n$ and $l(H) \leq n$, $\mu_1(G) = \mu_2(G)$, and $\mu_1(H) = \mu_2(H)$. So

$$\mu_1(F) = max\{\mu_1(G), \mu_1(H)\} = max\{\mu_2(G), \mu_2(H)\} = \mu_2(F).$$

(iii): $F = (G \wedge H)$. Fill in yourself.

(iv): $F = (G \rightarrow H)$. Fill in yourself.

Q: Did we use induction or strong induction?

2.7. Truth Tables. This is a way of describing how the truth value of a formula depends on those of its atomic subformulas. First, we give truth tables for the connectives.

$\mu(A)$	$\mu(B)$	$\mu(\neg A)$	$\mu(A \vee B)$	$\mu(A \wedge B)$	$\mu(A \rightarrow B)$	$\mu(A \leftrightarrow B)$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

Note that each line in this truth table represents a different truth assignment.

You could introduce other connectives, like 'A iff $\neg B$'. Is there any point?

We can write down truth tables for any formula, such as the following one for $(A \wedge B \rightarrow \neg C)$.

A	B	C	$A \wedge B$	$\neg C$	$(A \wedge B) \rightarrow \neg C$
1	1	1	1	0	0
1	1	0	1	1	1
1	0	1	0	0	1
1	0	0	0	1	1
0	1	1	0	0	1
0	1	0	0	1	1
0	0	1	0	0	1
0	0	0	0	1	1

Write down the truth tables of the following formulas:

(1) $(\neg A) \vee B$

(2) $(\neg A) \rightarrow B$

(3) $(\neg B) \rightarrow (\neg A)$

(4) $\neg(\neg A)$

What do you notice? $(A \to B) \equiv (1) \equiv (3)$, $A \vee B \equiv (2)$, $A \equiv (4)$.

This motivates the following definition:

Definition 2.8. Two formulas F and G are *(semantically) equivalent*, if for every truth assignment μ, $\mu(F) = \mu(G)$. We denote this by $F \equiv G$.

Note. The symbol $\leftrightarrow$ is read as (syntactically) equivalent, whereas $\equiv$ is semantic.

Question. Can formulas containing different atomic formulas be semantically equivalent?

Adequate Sets of Connectives. I raised earlier the question whether $\neg, \wedge, \vee, \to$ are 'enough'.

Definition 2.9. A set of connectives $\mathcal{C}$ is called *adequate* (or *functionally complete*), if every connective can be expressed with connectives from $\mathcal{C}$; more precisely, $\mathcal{C}$ is adequate if for every formula F in $\mathcal{F}$ there is a formula G just using connectives from $\mathcal{C}$ such that $F \equiv G$.

Lemma 2.10. $\{\neg, \wedge\}$ is adequate.

Proof. This is by induction on the length of a formula. The base case is obvious – if $l(F) = 1$ then F is atomic so has no connectives. We assume that for all $F \in \mathcal{F}$ with $l(F) \leq n$ there is G just using $\neg, \wedge$ such that $F \equiv G$. Suppose $l(F) = n + 1$.

Case (i). F is $\neg F'$. Now $l(F') \leq n$, so by induction there is G' just using $\neg, \wedge$ with $F' \equiv G'$. Then $F \equiv \neg G'$, and $\neg G'$ just uses $\wedge, \neg$.

Case (ii). F is $F_1 \wedge F_2$: Exercise.

Case (iii). F is $F_1 \vee F_2$. By induction there are G_1, G_2 just using $\wedge, \neg$ with $F_1 \equiv G_1$ and $F_2 \equiv G_2$. Then F is $F_1 \vee F_2 \equiv \neg(\neg F_1 \wedge \neg F_2) \equiv \neg(\neg G_1 \wedge \neg G_2)$.

Case (iv). F is $F_1 \to F_2$. Find G_1, G_2 as in case (iii). Now F is $F_1 \to F_2 \equiv \neg(F_1 \wedge \neg F_2) \equiv \neg(G_1 \wedge \neg G_2)$.

Corollary 2.11. $\{\neg, \vee\}$ is adequate.

Proof. Just note $(F \wedge G) \equiv \neg(\neg F \vee \neg G)$.

Question. Is there a *single* connective which is adequate?

Definition 2.12. (a) The connective $\downarrow$ ('joint denial', 'not or', 'nor') is defined as follows:

$$\mu(F \downarrow G) = 1 - max\{\mu(F), \mu(G)\}.$$

So its truth table looks like this:

F	G	$F \downarrow G$
1	1	0
1	0	0
0	1	0
0	0	1

(b) The connective | ('alternative denial', 'not and') is defined as follows:

$$\mu(F|G) = 1 - \mu(F) \cdot \mu(G).$$

So its truth table looks like this:

F	G	$F \downarrow G$
1	1	0
1	0	1
0	1	1
0	0	1

Proposition 2.13. (a) $\{\downarrow\}$ is adequate.
(b) $\{|\}$ is adequate.

Proof. Homework. Note that it suffices to show that $\neg$ and $\wedge$ (or $\neg$ and $\vee$) can be expressed using just $\downarrow$ (same for $|$).

Remark. One can show that $\downarrow$ and $|$ are the only connectives which by themselves are adequate.

Definition 2.14.

(1) A formula F is called *satisfiable* if there is a truth assignment μ with $\mu(F) = 1$.

(2) If a formula F is not satisfiable, i.e. $\mu(F) = 0$ for all truth assignments μ, then F is called *unsatisfiable*, or *contradictory*.

(3) A formula F is called *valid* or *a tautology* if for every truth assignment μ, we have $\mu(F) = 1$.

Examples. A is satisfiable.
$A \wedge \neg A$ is contradictory.
$A \vee \neg A$ is valid.
This can be seen by the truth table below.

A	$\neg A$	$A \wedge \neg A$	$A \vee \neg A$
1	0	0	1
0	1	0	1

Note.

- If F is valid then F is satisfiable. (Prove it!)
- F is a tautology iff $\neg F$ is unsatisfiable. (Prove it!)

- It does not make sense to talk about a formula being true, but rather it having truth value 1 under a truth assignment.

Exercise 2.15. Decide whether the following formulas are satisfiable, contradictory, tautologies:

(i) $F_1 = \neg A \to (A \to B)$ *(tautology)*

(ii) $F_2 = (A \to B) \to (B \to A)$ *(satisfiable, but not valid)*

(iii) $F_3 = (\neg(A \to B)) \wedge (\neg A \vee B)$ *(contradictory)*

We check these three through the following truth table.

A	B	$\neg A$	$A \to B$	F_1	$B \to A$	F_2	$\neg(A \to B)$	$\neg A \vee B$	F_3
1	1	0	1	1	1	1	0	1	0
1	0	0	0	1	1	1	1	0	0
0	1	1	1	1	0	0	0	1	0
0	0	1	1	1	1	1	0	1	0

The truth table checks the truth value of F_1, F_2, F_3 under all truth assignments. Since the F_1 column is all-1, F_1 is a tautology. Since the F_2 column has a 1, F_2 is satisfiable. Since the F_3 column is all-0, F_3 is contradictory.

(iv) True or false: If $F \to G$ is satisfiable, and F is satisfiable, then G is satisfiable.

This is false: put $F = A_1$, $G = A_2 \wedge \neg A_2$. Then $F \to G$ is satisfiable (let $\mu(A_1) = 0$), and F is satisfiable (let $\mu(A_1) = 1$), but G is not satisfiable.

(v) True or false: If $F \to G$ is valid, and F is valid, then G is valid.

This is true. Let μ be any truth assignment. Then $\mu(F \to G) = 1$ and $\mu(F) = 1$ (as these are valid), so $\mu(G) = 1$.

Question 2.16. (1) How many formulas are there just using the three atomic formulas A, B, C?

Ans.: there are countably infinitely many (consider A, $A \wedge A$, $A \wedge (A \wedge A)$, etc.

(2) How many (semantically) non-equivalent such formulas are there?

This really breaks up into two questions.

(i) How many truth tables are there?

For formulas with n atomic formulas, there are 2^n possible assignments of truth values to the atomic formulas, and a truth table assigns 0 or 1 to each of these 2^n choices. So a truth table is really a function $\{0,1\}^n \to \{0,1\}$, so there are 2^{2^n} truth tables with n atomic subformulas. For example, for $n = 4$, there are 65,536 truth tables!

(ii) Is every such *truth table* (i.e. every function $\{0,1\}^n \to \{0,1\}$ expressible by a propositional formula from $\mathcal{F}$? For $n = 2$, this is easily checked – there are $2^{2^2} = 16$ functions. In general, the answer is yes.

I describe now how to obtain a formula, given a truth table. Consider the truth

table below.

A_1	A_2	A_3	ϕ
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

The formula ϕ is true if and only if A_1 and A_2 are true and A_3 is false (line 2), or A_1 is false and A_2, A_3 true (l.5) or all the A_i are false (l.8). So the formula ϕ is equivalent to

$$(A_1 \wedge A_2 \wedge \neg A_3) \vee (\neg A_1 \wedge A_2 \wedge A_3) \vee (\neg A_1 \wedge \neg A_2 \wedge \neg A_3).$$

Normal Forms

Definition 2.17 (a) A *literal* is an atomic formula (positive literal) or the negation of an atomic formula (negative literal).

(b) A formula F is in *conjunctive normal form* (CNF) if it is a conjunction of disjunctions of literals, i.e.

$$F = (L_{11} \vee L_{12} \vee \ldots \vee L_{1m_1}) \wedge (L_{21} \vee L_{22} \vee \ldots \vee L_{2m_2}) \wedge \ldots \wedge (L_{n1} \vee L_{n2} \vee \ldots \vee L_{nm_n}),$$

for short:

$$F = \bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_i} L_{i,j} \right),$$

where $L_{i,j} \in \{A_1, A_2, \ldots\} \cup \{\neg A_1, \neg A_2, \ldots\}$.

(c) A formula F is in *disjunctive normal form* (DNF) if it is a disjunction of conjunctions of literals, i.e.

$$F = \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_i} L_{i,j} \right),$$

where $L_{i,j} \in \{A_1, A_2, \ldots\} \cup \{\neg A_1, \neg A_2, \ldots\}$.

Note that $\wedge$ and $\vee$ are associative, i.e. $(F \wedge G) \wedge H) \equiv F \wedge (G \wedge H)$ and $(F \vee G) \vee H \equiv F \vee (G \vee H)$, so the expressions above are not ambiguous.

Theorem 2.18. For every formula F there is a formula C in conjunctive normal form and a formula D in disjunctive normal form with $C \equiv F \equiv D$.

Proof. We will use two different methods to prove this:

(1) The truth table method, discussed above, yields a formula in DNF. It can be adapted to get a formula in CNF. For example, consider the formula

$$(A_1 \wedge A_2 \wedge \neg A_3) \vee (\neg A_1) \wedge A_2 \wedge A_3) \vee (\neg A_1) \wedge \neg A_2 \wedge \neg A_3)$$

arising from the last truth table considered above. By considering the same truth table, the formula $\neg\phi$ is equivalent to the following one in DNF (obtained by considering the rows where ϕ has a 0:

$$(A_1 \wedge A_2 \wedge A_3) \vee (A_1 \wedge \neg A_2 \wedge A_3) \vee (A_1 \wedge \neg A_2 \wedge \neg A_3) \vee (\neg A_1 \wedge A_2 \wedge \neg A_3) \vee (\neg A_1 \wedge \neg A_2 \wedge A_3).$$

Thus, applying De Morgan's Laws to the last formula, ϕ is equivalent to the following one:

$$(\neg A_1 \vee \neg A_2 \vee \neg A_3) \wedge (\neg A_1 \vee A_2 \vee \neg A_3) \wedge (\neg A_1 \vee A_2 \vee A_3) \wedge (A_1 \vee \neg A_2 \vee A_3) \wedge (A_1 \vee A_2 \vee \neg A_3).$$

(2) Now we will discuss a method for finding C and D without going through the truth table of the formula. We prove that C and D exist, but our proof also gives an *algorithm* for finding C and D.

We need the following facts:

- Let F be a formula, G a subformula of F (i.e. a formula occurring in the tree of F). If $G_1 \equiv G$ and F_1 is the formula obtained from F by replacing G by G_1, then $F \equiv F_1$.
- $\neg(\neg F) \equiv F$
- *De Morgan's Laws:*
  $\neg(F \wedge G) \equiv \neg F \vee \neg G$ (see homework).
  $\neg(F \vee G) \equiv \neg F \wedge \neg G$

  In general:
  $\neg \left(\bigwedge_{i=1}^{n} F_i\right) \equiv \bigvee_{i=1}^{n} (\neg F_i)$
  $\neg \left(\bigvee_{i=1}^{n} F_i\right) \equiv \bigwedge_{i=1}^{n} (\neg F_i)$
  (Prove these by induction on n using the equivalences above.)
- *Distributive Laws:*
  $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
  $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$

  These generalize to:
  $F \wedge (\bigvee G_i) \equiv \bigvee (F \wedge G_i)$
  $F \vee (\bigwedge G_i) \equiv \bigwedge (F \vee G_i)$
- *Associative Laws:* (which we are using all along when using $\bigwedge$ and $\bigvee$)
  $F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H$
  $F \vee (G \vee H) \equiv (F \vee G) \vee H$

We know that $\{\neg, \vee\}$ is an adequate set of connectives. So we can assume that F only contains these connectives by replacing occurrences of the form $G \to H$ by $\neg G \vee H$, and occurrences of $G \wedge H$ by $\neg(\neg G \vee \neg H)$. For example, if F is $(A \leftrightarrow B)$, we get

$$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A) \equiv (\neg A \vee B) \wedge (\neg B \vee A) \equiv \neg(\neg(\neg A \vee B) \vee \neg(\neg B \vee A)).$$

The proof of Theorem 2.18 is now by induction on the length $l(F)$ of the formula F:

Induction base. If F is an atomic formula, F is already in CNF and DNF.

Induction step. (1) Let $F = \neg G$. By induction hypothesis, as $l(G) < l(F)$, there are G_c, G_d so that $G \equiv G_c$ with $G_c = \bigwedge_i \bigvee_j L_{ij}$ in CNF, and $G \equiv G_d$ with $G_d = \bigvee_i \bigwedge_j K_{ij}$ in DNF. Then

$$F = \neg G \equiv \neg G_c = \neg \left(\bigwedge_i \bigvee_j L_{ij} \right) \equiv \bigvee_i \neg \left(\bigvee_j L_{ij} \right) \equiv \bigvee_i \left(\bigwedge_j \neg L_{ij} \right) \equiv \bigvee_i \bigwedge_j (\bar{L_{ij}})$$

where $\bar{L_{ij}} = \begin{cases} \neg A_k & \text{if } L_{ij} = A_k, \text{ a positive literal} \\ A_k & \text{if } L_{ij} = \neg A_k, \text{ a negative literal} \end{cases}$.

So $\bigvee_i \bigwedge_j (\bar{L_{ij}})$ is in DNF.

Using $F \equiv \neg G_d$ yields a formula in CNF equivalent to F. (Fill the details in yourself!)

(2) For $F = G \vee H$. Again, as $l(G), l(H) < l(F)$, there are G_c, G_d, H_c, H_d so that $G \equiv G_c$ with $G_c = \bigwedge_i \bigvee_j L^1_{ij}$ in CNF, and $G \equiv G_d$ with $G_d = \bigvee_i \bigwedge_j K^1_{ij}$ in DNF, and $H \equiv H_c$ with $H_c = \bigwedge_n \bigvee_m L^2_{nm}$ in CNF, and $H \equiv H_d$ with $H_d = \bigvee_n \bigwedge_m K^2_{nm}$ in DNF , we have

$$F \equiv G_c \vee H_c = \bigwedge_i \bigvee_j L^1_{ij} \vee \bigwedge_n \bigvee_m L^2_{nm} \equiv \bigwedge_{i,n} \left(\bigvee_j L^1_{ij} \vee \bigvee_m L^2_{nm} \right) \text{ (distributive law)}$$

which is in CNF.

Also

$$F \equiv G_d \vee H_d = \bigvee_i \bigwedge_j K^1_{ij} \vee \bigvee_n \bigwedge_m K^2_{nm}$$

which is in DNF.

Example. Put $(\neg A \to B) \wedge ((A \wedge \neg C) \leftrightarrow B)$ in CNF.
Here,

$$\begin{aligned} & (\neg A \to B) \wedge ((A \wedge \neg C) \leftrightarrow B) \\ \equiv\ & (\neg\neg A \vee B) \wedge [((A \wedge \neg C) \to B) \wedge (B \to (A \wedge \neg C))] \\ \equiv\ & (A \vee B) \wedge [(\neg(A \wedge \neg C) \vee B) \wedge (\neg B \vee (A \wedge \neg C))] \\ \equiv\ & (A \vee B) \wedge [((\neg A \vee C) \vee B) \wedge ((\neg B \vee A) \wedge (\neg B \vee \neg C))] \end{aligned}$$

$$\equiv (A \vee B) \wedge (\neg A \vee C \vee B) \wedge (\neg B \vee A) \wedge (\neg B \vee \neg C),$$

which is in CNF.

As another example, the formula $\psi = (\neg A_1 \vee A_2) \wedge (\neg A_3 \vee A_4 \vee A_5) \wedge A_6$ which is already in CNF, is equivalent to the following formula in DNF, found using distributivity.

$$(\neg A_1 \wedge \neg A_3 \wedge A_6) \vee (\neg A_1 \wedge A_4 \wedge A_6) \vee (\neg A_1 \wedge A_5 \wedge A_6) \vee$$
$$\vee (A_2 \wedge \neg A_3 \wedge A_6) \vee (A_2 \wedge A_4 \wedge A_6) \vee (A_2 \wedge A_5 \wedge A_6).$$