Notes on Logic

1 Propositional Calculus

A *proposition* or *statement* is an assertion which can be determined to be either true or false (T or F). For example, "zero is less than any positive number" is a statement. We are interested in combining and simplifying statements, as well as developing ways to check whether a given statement is true or false using a set of rules called *propositional calculus*. This hasn't got anything to do with ordinary calculus, although later on we'll deal with statements which have variables, when we introduce *quantifiers*. In order to work with and simplify statements, we often assign letters to represent them, which allows us a convenient way to manipulate logical expressions. For example, p could be the statement "zero is less than any positive number" and q could be the statement "zero is larger than any negative number". In the next section we will see how to write the statement "p and q" using logical symbols.

2 Logical Operators and Truth Tables

At this point we can introduce notation for *logical operators*: the word *and* is represented by $\wedge$, and called the *conjunction operator*. The word *or* is represented by $\vee$, and called the *disjunction operator*. For any statement p, we write $\neg p$ (or sometimes in textbooks one sees $\overline{p}$) for the statement "p is false", which is the *complement of* p. So now we can write expressions like $p \wedge q$ and $(p \vee q) \wedge (\neg r)$. The use of brackets here will be explained in more detail later. Such abstract expressions can often be simplified: for example, it is clearly redundant to say $p \wedge p$, since this is the same as p itself. Let's look more closely at some of the rules whereby symbolic logical statements can be simplified, using *truth tables*. A truth table gives all possible values (T or F) of a statement which combines a number of simpler statements. For example, suppose that p and q are statements. Then the truth tables for $\neg p$, $p \wedge q$, $p \vee q$, are respectively

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

We can already evaluate a statement such as $\neg(\neg p \vee \neg q)$. The brackets tell us first to evaluate $\neg p \vee \neg q$, and then to take the complement of the result. The truth table looks like this:

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(\neg p \vee \neg q)$
F	F	T	T	T	F
F	T	T	F	T	F
T	F	F	T	T	F
T	T	F	F	F	T

But we already know this truth table – it is $p \wedge q$. This is our first example of a simplification of a logical symbolic expression, and we refer to it as *de Morgan's Law.* It allows us, from now on, to reduce $\neg(\neg p \vee \neg q)$ to $p \wedge q$ inside any complicated statement. Two statements are *equivalent* if they have the same truth table. The symbol for equivalence is $\leftrightarrow$ (sometimes people use $\equiv$), and we just saw

$$\neg(\neg p \vee \neg q) \leftrightarrow p \wedge q$$

Another way of saying $p \leftrightarrow q$ is p *if and only if* q. It is also true that $\neg(\neg p \wedge \neg q) \leftrightarrow p \vee q$, and we refer to this also as de Morgan's Law. As one would guess, there are many other such equivalences; we list the most important onces here with their names:

	Rules of Logic	
•	$\neg(\neg p) \leftrightarrow p$	double negation
•	$p \wedge p \leftrightarrow p$	absorption rule
•	$p \vee p \leftrightarrow p$	absorption rule
•	$p \vee (p \wedge q) \leftrightarrow p$	absorption rule
•	$p \wedge (p \vee q) \leftrightarrow p$	absorption rule
•	$p \wedge q \leftrightarrow q \wedge p$	commutative rule for conjunction
•	$p \wedge q \leftrightarrow q \wedge p$	commutative rule for disjunction
•	$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge p$	associative rule for conjunction
•	$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$	associative rule for disjunction
•	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	distributive rule for conjunction
•	$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	distributive rule for disjunction
•	$\neg(\neg p \vee \neg q) \leftrightarrow p \wedge q$	de Morgan's Law
•	$\neg(\neg p \wedge \neg q) \leftrightarrow p \vee q$	de Morgan's Law

All of these equivalences can be checked with truth tables; this is left as an exercise. These rules allow us to simplify logical statements (simplify means replace with a simpler equivalent statement). For example, suppose we want to simplify $p \vee \neg(\neg p \wedge \neg q)$. The brackets tell us which part to evaluate first, and we work from inside to outside. Therefore

$$\begin{aligned} p \vee \neg(\neg p \wedge \neg q) &\leftrightarrow p \vee (p \vee q) && \textsf{de Morgan} \\ &\leftrightarrow (p \vee p) \vee q && \textsf{associative rule} \\ &\leftrightarrow p \vee q && \textsf{absorption rule} \end{aligned}$$

A final and very useful operator is called the *exclusive or* or *xor* operator, denoted $\oplus$. The truth table for this operator is:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

It is evident that $p \oplus q$ is the same as $(p \vee q) \wedge \neg(p \wedge q)$ – as a phrase this is written "p or q, but not both". We could add a number of rules for $\oplus$ to our list above, but we will leave these as exercises. Events p and q for which $p \oplus q = p \vee q$ are called *mutually exclusive* (so statements p and q are mutually exclusive if $p \wedge q$ is always false – for example "it is raining and I have an umbrella" and "it is raining and I have no umbrella" are mutually exclusive statements). For mutually exclusive statements p and q, $p \vee q$ is often written $p \overset{\circ}{\vee} q$ to stress that $p \wedge q$ is false.

3 Conditional Statements

If we are given two very complicated statements, it might be difficult to check directly whether they are equivalent. So it is often easier to break down the equivalence into a number of *implications*. We write $p \rightarrow q$ for "statement p implies statement q". The truth table for this is given by:

p	q	$p \rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

Depending on how one reads the English, the second line of the truth table may seem curious: why is "p is false implies q is true" a true statement? One should interpret it this way: p implies q can be false only if the guarantee that whenever p is true then q is true is violated, and this happens only on the third line of the truth table. For example, the claim "if it rains, then I carry an umbrella" is not violated by carrying an umbrella when there is no rain. In English, we often state $p \to q$ as "*q is a necessary condition for p*" and "*p is a sufficient condition for q*". In many statements of theorems, this terminology is used. Also $p \leftrightarrow q$ is written "*p is a necessary and sufficient condition for q*" or "*p if and only if q*".

The *converse* of $p \to q$ is $q \to p$. As we have defined it,

$$(p \to q) \land (q \to p) \leftrightarrow (p \leftrightarrow q).$$

So to check whether two statements are equivalent, we have to check that each implies the other. We also say "*q if p*" instead of $p \to q$ and "*q only if p*" for $q \to p$. This clarifies our use of "if and only if" for equivalence of two statements. As an exercise, check the above equivalence, using truth tables. Another rule we can use is that $p \to q$ is equivalent to $\neg p \lor q$:

$$(p \to q) \leftrightarrow (\neg p \lor q).$$

This is useful for simplifying logical statements. As an exercise, the above equivalence can be verified by truth tables. The *contrapositive* of $p \to q$ is written $\neg q \to \neg p$, and is very often extremely useful in proofs, as we shall see in the next section, since

$$(p \to q) \leftrightarrow (\neg q \to \neg p) \quad \textsf{contrapositive}$$

As an exercise, verify this statement.

4 Contradictions and Tautologies

A statement which is always true is called a *tautology* (the truth table should display T in every row of the last column) and a statement which is always false is called a *contradiction* (the truth table should display F in every row of the last column). We write 0 to denote that a generic contradiction and 1 to denote a generic tautology. For example, if p is any statement, then $\neg p \lor p$ is a tautology whereas $\neg p \land p$ is a contradiction (a statement can't be false and true at the same time). The rules for interaction between a statement p and tautologies and contradictions are as follows:

$$1 \lor p \leftrightarrow 1$$
$$0 \lor p \leftrightarrow p$$
$$1 \land p \leftrightarrow p$$
$$0 \land p \leftrightarrow 0$$

So to check equivalence of two statements, we are really showing that their equivalence is a tautology. All of the rules given previously are tautologies. Let's do an example. To see whether $p \land (p \lor q)$ is a tautology, we could write out the truth table as follows:

p	q	$p \land (p \lor q)$
F	F	F
F	T	F
T	F	T
T	T	T

So in fact we get the truth table of p (this actually proves one of the absorption rules). Since p could be false, we conclude that $p \land (p \lor q)$ is not a tautology, since it is equivalent to p. Consider, on the other hand, $p \lor (p \land q) \lor (p \to q)$. The truth table is

p	q	$p \lor (p \land q) \lor (p \to q)$
F	F	T
F	T	T
T	F	T
T	T	T

so this is a tautology. Checking tautologies via truth tables is tedious; for example the truth table of a statement which is a logical combination of ten other statements requires a truth table with $2^{10} = 1024$ rows – by no means painless! But we don't have to do it with truth tables, since we have the rules of logic to guide us (as an exercise, check this):

$$\begin{aligned} p \lor (p \land q) \lor (p \to q) &\leftrightarrow p \lor (p \land q) \lor (\neg p \lor q) \\ &\leftrightarrow p \lor (\neg p \lor q) \\ &\leftrightarrow (p \lor \neg p) \lor q \\ &\leftrightarrow 1 \lor q \\ &\leftrightarrow 1. \end{aligned}$$

The above argument represents something called a *proof*, which we discuss in the next section.

5 Proofs

The $\rightarrow$ symbol is *transitive*: this means that

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r).$$

As an exercise, check this using truth tables. Note that sometimes we write $p \rightarrow q \rightarrow r$ as shorthand for the left hand side. We call r the *conclusion* and p the *premise* of the statement $p \rightarrow q \rightarrow r$. A *proof* of conclusion r starting with premise p is a series of implications $p \rightarrow p_1 \rightarrow p_2 \cdots \rightarrow p_k \rightarrow r$ where each p_i is a statement. Many very complicated mathematical proofs have long chains of simple implications (i.e. they are broken down into many steps). In this section, we prove some elementary mathematical statements using the logic developed so far. The first example is a direct proof of the equivalence of two statements. To verify the equivalence $p \leftrightarrow q$, we break it down into checking $p \rightarrow q$ and $q \rightarrow p$.

Proposition 5.1 *Let $P(x)$ be a polynomial with real coefficients. Then $P(0) = 0$ if and only if $P(x) = xQ(x)$ for some polynomial $Q(x)$.*

Proof. (Direct Proof) We want to prove that "$P(0) = 0$" if and only if "$P(x) = xQ(x)$ for some polynomial $Q(x)$". We could start by showing that the first statement implies the second. We can suppose $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where a_i are real numbers. Then here is the proof:

$$\begin{aligned}
P(0) = 0 \quad &\rightarrow \quad a_n 0^n + a_{n-1}0^{n-1} + \ldots + a_1 0 + a_0 = 0 \\
&\rightarrow \quad a_0 = 0 \\
&\rightarrow \quad P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \\
&\rightarrow \quad P(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) \\
&\rightarrow \quad P(x) = xQ(x)
\end{aligned}$$

where $Q(x)$ is the polynomial $a_n x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1$. This proves that the first statement implies the second. Now we have to show the converse: the second statement implies the first. This is easy: $P(x) = xQ(x) \rightarrow P(0) = 0 \cdot Q(0) \rightarrow P(0) = 0$, as required. This completes the proof. ∎

In this example, $P(0) = 0$ is the premise and $P(x) = xQ(x)$ is the conclusion. Note the use of a box to show that the proof is finished. In many cases in mathematics, it is extremely helpful to use the contrapositive instead of direct proof (this really can't be stressed enough). That is, instead of proving $p \to q$, we prove that $\neg q \to \neg p$. It is often the case that proving $p \to q$ directly is much harder than showing $\neg q \to \neg p$. This will be referred to henceforth as a *proof by contradiction*. One of the most basic examples leads to an extremely useful combinatorial technique known as the *pigeonhole principle*. We will use this principle many times in the material to follow.

Proposition 5.2 (The Pigeonhole Principle) *If more than n numbers are selected from $\{1, 2, \ldots, n\}$, then there are two of the numbers which are the same.*

Proof. (Proof by contradiction) Suppose that the statement "there are two numbers which are the same" is false; this is the same as saying all the numbers are different. But there are only n available numbers, namely $1, 2, \ldots, n$, so we have a selection of at most n numbers. In other words, "at most n numbers have been selected from $\{1, 2, \ldots, n\}$", so the first statement of the proposition is false. This completes the proof. ∎

Although this may be an obvious statement, it is the beginning of a very powerful technique in discrete mathematics called *averaging*, and sometimes gives very surprising results, as we shall see later.

Recall that a prime number is a positive integer larger than 1 which is divisible only by 1 and itself. For instance, $2, 3, 5, 7, 11, 13, 17, 19$ are the first eight prime numbers. Here is a proof by contradiction that there are infinitely many prime numbers using the double negation rule. We assume there are finitely many prime numbers and derive a statement which is obviously false. We refer to this, too, as a proof by contradiction. The proof goes back to Euclid, and is despite the fact that there is no known simple formula for prime numbers (for example formulas like $2^n + 1$ or $n^2 + n + 1$ are not always prime for $n \geq 1$).

Proposition 5.3 *There are infinitely many prime numbers.*

Proof. (Proof by contradiction) Consider the statement: "there are infinitely many prime numbers". If we call this statement p, then it is enough to show that the statement $\neg p$ is false to show that p is true, by the double negative rule. Now $\neg p$ is the statement "there are finitely many prime numbers". Let's prove that this is false. Suppose the finitely many prime numbers in the statement are $p_1, p_2, \ldots, p_r$. Take a number $n = p_1 p_2 \cdots p_r + 1$ (this is the key step of the proof). Then n is not prime, so n must be divisible by a prime number m where $1 < m < n$. But the primes are $p_1, p_2, \ldots, p_r$, so m must be one of the primes $p_1, p_2, \ldots, p_r$. But that is impossible since m then divides $p_1p_2\cdots p_r$, but m does not divide $p_1p_2\dots p_r+1$. So $\neg p$ is false, and this completes the proof. ∎

Later on we will study primes in much more detail; in particular with applications to cryptography, where their use is fundamental.

6 Cases and Counterexamples

In many proofs, we have to break things down even further into *cases*. If premise $p \vee q$ is given, and we want to prove r, then it is enough to show

$$(p \to r) \wedge (q \to r).$$

As an exercise, check this using the rules given above. This breaks the proof into two cases: we have to check that $p \to r$, and then we have to check that $q \to r$. For example, suppose we want to show that if x is not divisible by three, then x^2+2 is divisible by three. For short, we write this as $3|x^2+2$. If x is not divisible by three (we write this as $3 \nmid x$), then we know that $x = 3m+1$ or $x = 3m+2$ for some integer m. These are the statements p and q, and we want to derive r:

$$(x = 3m+1) \;\vee\; (x = 3m+2) \to 3|x^2+2.$$

Let's first prove $x = 3m+1 \to 3|x^2+2$:

$$\begin{aligned} x = 3m+1 \quad &\to \quad x^2+2 = (3m+1)^2+2 \\ &\leftrightarrow \quad x^2+2 = 9m^2+6m+3 \\ &\leftrightarrow \quad x^2+2 = 3(3m^2+2m+1) \\ &\leftrightarrow \quad 3|x^2+2. \end{aligned}$$

That proves $p \to r$, and similarly one shows $q \to r$. We deduce $(p \vee q) \to r$, which is what we wanted.

The statement $p \wedge q$ is false if p is false or q is false, by definition of conjunction. We say that p is a *counterexample* to $p \wedge q$ if p is false. More generally, to show that a chain of conjunctions is false, all we have to do is produce a proof that one of the statements in the chain is false (this statement is then a counterexample). For instance, the statement "n^2+n+1 is prime for all positive integers $n < 10$" is false, since $4^2+4+1 = 21$ is not prime, and it is a chain of conjunctions of nine statements.

7 Predicate Calculus and Quantifiers

The phrase "$n^2 + n + 1$ is prime" is not really a statement if we don't say what n is, since the primality of $n^2 + n + 1$ depends on the value of n. Remember that statements are true or false, so this can't be a statement. To turn it into a proper statement, we introduce *quantifiers*. How can we write "$n^2 + n + 1$ is prime for all positive integers n" as a statement using logical symbols? The problem is the phrase "for all". If we tried to write it using $\wedge, \vee, \neg$, we get into trouble since we'd have to write an infinite chain of conjunctions and that is not defined so far. So we introduce a new symbol, called a *quantifier*, and which represents "for all". The symbol is $\forall$, and the statement is written

$$\forall n \geq 1(n^2 + n + 1 \text{ is prime}).$$

The brackets tell us to which statement $\forall n \geq 1$ applies to. We refer to n in this statement as the *variable* of the statement; this is the main difference between propositional and predicate calculus: now sentences p accept a variable n, so we write statements as $\forall n(p(n))$. More generally, there is no reason not to have statements which depend on many variables, such as $\forall l, m, n(p(l, m, n))$.

How do we represent disjunctions? Consider the statement "there exists a positive integer n such that $n^2 + n + 1$ is prime". This is the same as the disjunction $p_1 \vee p_2 \vee p_3 \vee \cdots$ where p_i is the statement $i^2 + i + 1$ is prime for $i = 1, 2, \ldots$. The phrase "there exists" is replaced with the symbol $\exists$:

$$\exists n \geq 1(n^2 + n + 1 \text{ is prime}).$$

Using the rule $p \vee q = \neg(\neg p \wedge \neg q)$, we see that the symbols $\forall$ and $\exists$ are related in the following important way:

$$\forall n(p(n)) \leftrightarrow \neg(\exists n(\neg p(n))) \quad \textsf{negation}$$

This is very useful in proofs, since proving $\forall n(p(n))$ might be hard if we consider all values of n, whereas checking that there can't be a value of n such that $p(n)$ does not hold could be easier. For example, consider proving that $n^2 + 1$ is never divisible by three. This is precisely the statement that $\forall n(3 \nmid n^2 + 1)$. We can't very well go through all integers n to check that the statement in brackets is true. Rather, suppose that there is a value of n such that $3 \mid n^2 + 1$. Let's derive from this a contradiction. We can write $n = 3m + r$ where $r \in \{0, 1, 2\}$ and m is an integer. Then $n^2 + 1 = (3m + r)^2 + 1 = 9m^2 + 6mr + r^2 + 1$. But if $r \in \{0, 1, 2\}$, then $r^2 + 1 \in \{1, 2, 5\}$, and so $3 \nmid r^2 + 1$ and $3 \nmid n^2 + 1$. That proves $\forall n(3 \nmid n^2 + 1)$.

Many mathematical statements can now be written very succinctly using quantifiers (although sometimes it is hard to read). Let's consider examples. Suppose we are given statements $p(x)$: "x is a power of two" and $q(y)$: "y is a power of three" and the statement $r(z)$: "z is prime". How do we say there is at least one value of x and at least one value of y such that $x - y$ is a prime?

$$\exists x, y(p(x) \wedge q(y) \wedge r(x-y)).$$

This is quite a simple example, since we did not mix occurrances of $\exists$ and $\forall$. A good exercise at this point is to try to write the statement "71 is prime" using quantifiers.

7.1 Definition of Limits

We now consider the example of the definition of a limit using quantifiers. In all of this section, variables ϵ, δ, X and so on are assumed to be real numbers. The definition of $\lim_{x \to a} f(x) = L$ in words is "the closer x gets to a, the closer $f(x)$ gets to L". This is more complicated to write with quantifiers, since we have to introduce new variables ϵ and δ to take care of the word "closer", which appears twice in the definition. The logical definition of $\lim_{x \to a} f(x) = L$ is:

$$\forall \epsilon > 0(\exists \delta > 0(|x-a| < \delta \to |f(x) - L| < \epsilon)).$$

Here is another example of limits, where we have to introduce a new variable. We wish to write $\lim_{x \to \infty} f(x) = L$ using quantifiers. Informally, this can be written "the larger the value of x, the closer $f(x)$ is to L". The problem is that "the larger the value of x..." has to be written with quantifiers: the key is to introduce a new variable X. Then the statement is

$$\forall \epsilon > 0(\exists X(\forall x > X(|f(x) - L| < \epsilon))).$$

8 Quick Summary

- Logical symbols $\neg, \vee, \wedge, \oplus, \mathring{\vee}, \to, \leftrightarrow, \forall, \exists$.
- Truth tables.
- Laws for manipulating logical expressions.
- Conditional statements and equivalence, contrapositive.
- Contradiction and tautology.
- Proof by contradiction and direct proof.
- Pigeonhole principle.
- Quantifiers and negating quantifiers.

9 Exercises

Question 1. Consider "this sentence is false". Is this a proposition? [1]

Question 2. Determine which of the following statements are tautologies. If the statement is a tautology, give a proof by referring to the appropriate rules at each step of your proof. If not, then justify your answer by giving a counterexample or using truth tables. [10]

(a) $(p \to q) \land (q \to r) \leftrightarrow (p \to r)$

(b) $p \lor (p \land q) \leftrightarrow p$

(c) $(p \land (p \oplus r)) \leftrightarrow (r \to p)$

(d) $(r \to p) \lor (p \land r) \lor (p \to r)$

(e) $(p \oplus q \oplus r) \leftrightarrow ((p \lor q \lor r) \land \neg((p \land r) \lor (q \land r) \lor (p \land q)))$

Question 3. Prove that if we choose any $n+1$ integers from $\{1, 2, \ldots, 2n\}$, then one of the integers chosen divides another. You may find it useful to note that every positive integer x can be written in the form $x = 2^k \cdot m$ for some positive integer m and some integer $k \geq 0$, and then to use the pigeonhole principle applied to the number of possible different values of m. [4]

Question 4. Write the statement "there are infinitely many primes" in terms of the statements $p(n)$, $q(m,n)$ and $r(m,n)$, where $p(n)$ is the statement "$n > 1$ is an integer", $q(m,n)$ is the statement "$m > n$ is an integer" and $r(m,n)$ is the statement "$m < n$ is an integer". [3]

Question 5. Use quantifiers to write the statement "$\lim_{x\to\infty} \sin x$ does not exist". [3]