Discrete Mathematics

Jonathan Gribbins

Contents

1 Logic & Proofs

1.1 Propositional Logic & Truth Tables

A **proposition** is a declarative sentence that is **either** true or false, but not both. To represent **propositional variables** to denote propositions—conventionally these are p, q, r, s,... . A proposition has a **truth value** of either T or F, based on whether it is *true* or *false.*

Propositional logic or **propositional calculus** is the area of logic that deals with these propositions. New propositions, called **compound propositions**, are statements built out of already established statements through the use of *logical operators.*

Theorem 1. *Let p be a proposition. The negation of p is $\neg p$, and this is the statement "it is not the case that p." The statement $\neg p$ is read "not p", and the truth value of $\neg p$ is the opposite of p.*

The logical operators that are used to connect two or more propositions and create a new proposition are called **connectives**.

Theorem 2. *Let p and q be propositions. The* ***conjunction*** *of p and q is denoted $p \wedge q$, and is said "p and q." This proposition is true if and only if both p and q are true, and is false otherwise..*

Theorem 3. *Let p and q be propositions. The* ***disjunction*** *of p and q is denoted $p \vee q$, and is said "p or q." This proposition is false if both p and q are false, and is true otherwise.*

The *or* in the disjunction connective is the English *inclusive or*, which means "either or both." On the contrary, the *exclusive or* is the or that mean "either but not both." The exclusive or is given by an altogether different connective.

Theorem 4. *Let p and q be propositions. The* ***exclusive*** *of p and q is denoted $p \oplus q$, and is said "p or q, but not both." This proposition is true only if one of p or q is true. It is false if both are true or if both are false.*

You can also combine propositions with **conditional statements.** These are statements that connect two different propositions and are true based on the truth of the statements.

Theorem 5. *Let p and q be propositions. The* ***conditional statement*** *$p \to q$ is the propositions "if p then q," and is only false when p is true and q is false. In this statement, p is the* ***hypothesis*** *and q is the* ***conclusion.*** *This connective is also called an* ***implication.***

There are various ways to state this implication. Most of them are simple and are easily recognized as $p \to q$, but there are a couple notably confusing ones. For instance, "q only if p" and "q unless ¬p" both mean $p \to q$.

In addition to the conditional statement that $p \to q$, there are three other commonplace conditional statements. These are:

Contrapositive: The contrapositive of $p \to q$ is the proposition $\neg q \to \neg p$. The truth value of the contrapositive is always the same as the truth value of the original implication.

Converse: The converse of $p \to q$ is the proposition $q \to p$. The converse has the same truth values of the inverse.

Inverse: The inverse of $p \to q$ is the proposition $\neg p \to \neg q$. The inverse the same truth values of the converse.

When two different statements have the same truth values, they are called **equivalent**. So the contrapositive and the implication are equivalent, and the inverse and converse are equivalent.

Biconditional statements are statements whose truth is based upon the conditions of two propositions.

Theorem 6. *The **biconditional statement** $p \iff q$ is the proposition "p if and only if q." This statement is only true if $p \to q$ and $q \to p$ have the same truth value, otherwise it is false. Biconditional statements are also called **bi-implications**, and $p \iff q$ is sometimes also written as "p iff q."*

Truth tables are tables that display different values of propositions and how these values effect a certain propositional statement. For instance, a statement like $p \to q$ would have a truth table like

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

The resultant statement of these truth tables are generally much longer than $p \to q$, and in this case, the statement may be broken down into component parts and "built up" from smaller statements.

These different connectives can be combined to create longer logical expressions with different truth values.

Truth values can also be represented with **bits**. Bits are values of 1 or 0, where 1 represents true and 0 represents false. When using bits, connectives are generally represented as AND for $\wedge$, OR for $\vee$, and XOR for $\oplus$. A **bitstring** is a string of bits (like 000101110), and these connectives can be used on bitstrings as **bitwise connectives**. These bitwise connectives take in two strings of equal length and use the operation on corresponding bits. For instance,

$$101110 \oplus \ (XOR)\ 111000 \to 010110.$$

1.2 Introduction to Proofs

A **proof** is an argument that serves to establish the truth of a mathematical or logical statement. A proof utilizes the hypothesis of the proof in conjunction with assumed axioms and other proved statements to complete this argument. In *formal proofs*, every single step used to argue this truth is explicitly stated, but in *informal proofs,* which are generally used in explanations for people, simple steps may be implicit and in-between steps.

There are many different terms used in proofs and when dealing with proofs:

Theorem A theorem is a statement that has been proven to be true. In mathematics, this word is generally saved for really important stuff—"theorems" that are not very important are usually called propositions.

Proof A proof is an argument that establishes a proposition to be true.

Axiom An axiom is a statement that is assumed to be true and is used in proofs. Also called a postulate.

Lemma A lemma is a theorem or proposition that is useful in the proofs of other theorems.

Corollary A corollary is a theorem that can be established directly from a theorem that has been proved.

Conjecture A conjecture is a statement that has been proposed to be true but hasn't been proven yet.

There are two common types of theorems—universal theorems and existence theorems. Universal theorems (with universal qualifier $\forall$) state that for all elements in a domain some proposition holds true. Existence theorems (with existence qualifier $\exists$) state that some element in a domain exists such that a proposition holds true.

A universal theorem is usually in the form $\forall x(P(x) \rightarrow Q(x))$. These theorems are usually proved by assuming some element c in the domain in question, and showing that $P(c) \rightarrow Q(c)$ holds true for this arbitrary case.

1.2.1 Direct Proofs

Direct proofs are proofs that begin by assuming that p is true, and then attempting to show that q holds true because of that. These proofs are generally self-evident if they end up working out.

1.2.2 Proof by Contrapositive

Indirect proofs are proofs that do not begin with the assumption that p is true. An important type of indirect proof is the **proof by contrapositive**. This type of proofs begins by assuming that $\neg q$ is true, and trying to find that $\neg p$ is always true as a result—this works because the contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$, and these two statements are *logically equivalent.*

It is important to note that proving a proposition $p \rightarrow q$ true is trivial if we can prove p is false because when p is false, $p \rightarrow q$ is always true. his type of proof is called **vacuous.** If a proposition $p \rightarrow q$ is proven by showing that q is true, this proof is called **trivial**.

1.2.3 Proof by Contradiction

If we want to prove that a statement p is true and we find a contradiction q that is proven false that is implied by $\neg p \rightarrow q$, then $\neg p$ must be false—therefore p must be true. This type of proof is called **proof by contradiction,** and is started by assuming that q and $\neg p$ are true, and using this assumption to lead to a contradiction.

1.2.4 Proofs of Equivalence

A **proof of equivalence** is a proof of a biconditional statement. This type of proof is based on the logical fact that

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

That is—p if and only if q if and only if p implies q and q implies p. If the statement $p \iff q \iff r$ is true, the truth or falsity of one statement (p, q, or r) guarantees identical truth or falsity of the other statements (this works form more than three propositions too!).

1.2.5 Counterexamples

To disprove a universal proposition like $\forall x(P(x))$, it takes only one example c for which $P(c)$ is not true. Additionally, for existence proofs like $\exists x(P(x))$, it takes only one example c for which $P(c)$ holds true to prove the statement.

1.2.6 Mistakes in Proofs

It is very easy to make mistakes in proofs. However, if in a proof there is some mistake in the axiomatic or logical foundation, the proof becomes incorrect, and the results are no longer correct.

1.2.7 Exhaustive Proofs/Proof by Cases

If a proposition has the form $(p_1 \lor p_2 \lor p_3 \lor \ldots) \to q$, then the proof may be broken up into separate proofs for each separate part of the proposition. You would have to prove $p_n \to q$ for each n, and this type of proof is called an **exhaustive proof** or **proof by cases.** Common cases for integers are things like proving for zero, proving for odds, evens, positives, negatives, etc.

1.3 Existence Proofs

Proofs that assert that $\exists x P(x)$ (there is some x such that P(x) holds true) are called **existence proofs**. A **constructive** existence proof is one where some a is found such that $P(a)$ is true. A **nonconstructive** existence proof is one where this a is not found, but it is proved that one must exist. Nonconstructive proofs generally follow the same pathways to proving that universality proofs follow.

1.3.1 Uniqueness Proofs

Sometimes proofs assert that there exists an element that holds a certain property, and also that this is the one **unique** element that holds this property. These proofs are called **uniqueness proofs**, and they assert that a) *an element a exists such that $P(a)$ is true* and b) *no other element x exists such that $P(x)$ holds true.* Symbolically, a uniqueness proof for $P(x)$ is the proposition that

$$\exists a \left(P(a)\right) \land \left(\forall b \neq a \to \neg P(b)\right).$$

2 Vocabulary

Proposition A declarative statement that is either true or false, but not both.

Propositional variables Letters used to represent a proposition

Truth value The truth (T) or falsehood (F) of a proposition

Propositional calculus/logic Area of logic that deals with propositions

Compound propositions Propositions built out of other propositions with logical operators

Connectives Logical operators that connect two or more propositions and create a new proposition

Conjunction Connective that combines two propositions and is true if and only if both propositions are true

Disjunction Connective that combines two propositions and is false if both propositions are false, and true otherwise

Exclusive Connective that combines two propositions and is true only if one of the two propositions is true, but not both

Conditional statements Statements that connect two different propositions and whose truth value is based on the truth of the statements

Implication A conditional statement stating "if p then q" that is only false if p is true and q is false

Contrapositive A conditional statement rearranging $p \to q$ and stating "if not p then not q" that is only false if q is false and p is true

Converse A conditional statement rearranging $p \to q$ and stating "if q then p" that is only false if q is true and p is false

Inverse A conditional statement rearranging $p \to q$ and stating "if not p then not q" that is only false if q is true and p is false

Logically equivalent Two statements are logically equivalent if all of their truth values are the same

Biconditional statement A conditional statement stating "p if and only if q" that is only true if $p \to q$ and $q \to p$ have the same truth value

Bit A value of 1 or 0, where 1 denotes truth and 0 denotes falsehood

Bitstring A string of bits

Bitwise connectives Connectives operating upon corresponding bits in two bitstrings

Proof An argument establishing the truth of a mathematical or logical statement