An Introduction to Mathematical Proofs

Nicholas A. Loehr

April 2022

Contents

1 Logic

1.1 Propositions, Logical Connectives, and Truth Tables

1.1.1 Propositions

Propostional logic **studies how the truth of a complex statement is determined by the truth or falsehoods of its parts.**

A *propositon* is a statement that is either true or false, but not both.

1.1.2 Propositional Forms

An expression which is built up by combining *propositional variables* (capital letters) using logical symbols, is called a *propositional form*

The following tables shows the symbols used in propositional logic and their meaning:

Logical Symbol	English Translation
$\neg P$	P is not true
$P \wedge Q$	P and Q.
$P \vee Q$	P or Q.
$P \oplus Q$	P or Q, but not both
$P \implies Q$	if P, then Q
$P \iff Q$	P if and only if Q

We can also combine this symbols:
$(P \wedge (\neg Q)) \vee ((\neg P) \wedge Q)$

Any expression which is built up by combining *propositional variables* (capital letters) using logical symbols, is called a *propositional form*

1.1.3 Definitions of NOT and AND

In order to properly *define* the exact meaning of logical connective words like NOT, AND, OR, IF, etc. we use so-called *truth tables*. that show how to combine the truth values of propositions to obtain the truth value of a new proposition built from these using a logical connective. The letters T and F stand for *true* and *false* respectively.

Definition of NOT. For any proposition P, the truth value of $\neg P$ ("not P") is determined by the following table

P	$\neg P$
T	F
F	T

Definition of AND. For any propositions, P, Q, the truth value of $P \wedge Q$ ("P and Q") is determined by the following table.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

1.1.4 Definitions of OR and XOR

$\vee$ stands for *inclusive*-OR, and $\oplus$ stands for *exclusive*-OR.

Definition of OR. For any propositions, P, Q, the truth value of PQ ("P or Q") is determined by the following table.

P	Q	$P \wedge Q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition of XOR. For any propositions, P, Q, the truth value of $P \oplus Q$ ("P xor Q") is determined by the following table.

P	Q	$P \wedge Q$
T	T	F
T	F	T
F	T	T
F	F	F

1.1.5 Formal Definition of Propositional Forms

In the main text, we informally defined a propositional form to be any expression built up by combining propositional variables using logical symbols. To give a precise, rigorous definition of propositional forms, we need a *recursive definition*.

Specifically, propositional forms are defined recursively via the following rules:

(a) A single capital italic letter is a propositional form.

(b) If A is a propositional form, then $(\neg A)$ is a propositional form.

(c) If A and B are any propositional forms, then $(A \wedge B)$ is a propositional form.

(d) If A and B are any propositional forms, then $(A \vee B)$ is a propositional form.

(e) If A and B are any propositional forms, then $(A \oplus B)$ is a propositional form.

(f) If A and B are any propositional forms, then $(A \implies B)$ is a propositional form.

(g) If A and B are any propositional forms, then $(A \iff B)$ is a propositional form.

(h) An expression is a propositional form only if it can be formed by applying rules (a) through (g) finetly many times.

1.1.6 Remark: Terminology for Propositional Forms

Let A and B be any propositional forms. In some logic texts, $(\neg A)$ is called the *negation* of A; $(A \wedge B)$ is called the *conjunction* of A and B; $(A \vee B)$ is called the *disjunction* of A and B; $(A \implies B)$ is called an *implication* or *conditional* with *hypothesis* of A and B.

1.2 Logical Equivalences and IF-Statements

1.2.1 Logical Equivalence

Definition: Logically Equivalent Propositional Forms
Two propositional forms A and B are *logically equivalent* when the truth tables for A and B have outputs that agree in every row. We write $\boxed{A \equiv B}$ when A and B are logically equivalent; we write $\boxed{A \not\equiv B}$ when A and B are not logically equivalent.

Theorem on Logical Equivalence. For all propositional forms P, Q, and R, the following lo

(a) *Commutative Laws:* $P \wedge Q \equiv Q \wedge P$, $P \vee Q \equiv Q \vee P$, and $P \oplus Q \equiv Q \oplus P$.

(b) *Associative Laws:* $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$, $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$, and $P \oplus (Q \oplus R) \equiv (P \oplus Q) \oplus R$.

(c) *Distributive Laws:* $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$, $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$, and $P \wedge (Q \oplus R) \equiv (P \wedge Q) \oplus (P \wedge R)$.

(d) *Idempotent Laws:* $P \wedge P \equiv P$ and $P \vee P \equiv P$

(e) *Absorption Laws:* $P \wedge (P \vee Q) \equiv P$ and $P \vee (P \wedge Q) \equiv P$.

(f) *Negation Laws:* $\neg(\neg P) \equiv P$, $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$, and $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$.

1.2.2 Converse and Contrapositive

Definition: Converse and Contrapositive
For any propositional forms P and Q: the $\boxed{\text{converse of } P \implies Q}$ is $\boxed{Q \implies P}$; the $\boxed{\text{contrapositive of } P \implies Q}$ is $\boxed{(\neg Q) \implies (\neg P)}$.

Theorem on IF. Let P and Q be distinct propositional variables.

(a) *Non-equivalence of Converse:* $P \Rightarrow Q \not\equiv Q \Rightarrow P$

(b) *Equivalence of Contrapositive:* $P \Rightarrow Q \equiv (\neg Q) \Rightarrow (\neg P)$

(c) *Elimination of IF:* $P \Rightarrow Q \equiv (\neg P) \vee Q$

(d) *Denial of IF:* $\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$

1.2.3 Five Remarks on Logical Equivalence

(1). The Theorem on Logical Equivalence shows that many of the laws of logic have an algebraic character analogous to algebraic laws for arithmetical operations on real numbers. To make this analogy more explicit, we introduce the convention of representing true (T) by 1 and false (F) by 0. The symbols 0 and 1 are called *bits*. In this notation, the defining truth tables for the six logical operators (including *IFF*, discussed in the next section) look like this:

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \Rightarrow Q$	$P \iff Q$
0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0
1	0	0	0	1	1	0	0
1	1	0	1	1	0	1	1

If we think of P and Q as bits (the actual integers 0 and 1, rather than propositions), we see that $\neg P = 1 - P$; $P \wedge Q = P \cdot Q = min(P, Q)$, the product or minimum of P and Q; $P \vee Q = max(P, Q)$, maximum of P and Q; and $P \oplus Q$ is the mod-2 sum of P and Q. We can also think of $\oplus$, $\Rightarrow$, and $\iff$ as *relations* comparing their two inputs. In this interpretation, $P \oplus Q$ is true precisely when $P \neq Q$, so $\oplus$A models non-equality of bits; $P \iff Q$ is true precisely when $P = Q$, so $\iff$ models equality of bits; and $P \Rightarrow Q$ is true precisely when $P \leq Q$, so $\Rightarrow$ models ordering of bits. Now the various identities in the Theorem on Logical Equivalences translate into identities for these algebraic operations on bits. For instance, supposing we already know that $x(yz) = (xy)z$ for all integers x, y, z we can deduce the associativity law $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ for propositional forms.

(2). Logical equivalence of propositional forms (denoted $\equiv$) is similar to, but not the same as, equality of forms (denoted $=$). Thinking of propositional forms A and B as strings of symbols, $A = B$ means that A has exactly the same symbols as B, in the same order. For example, $P \vee Q$ is not *equal* to $Q \vee P$ since the first symbols do not match. Yet, as we know, $P \vee Q \equiv Q \vee P$ since the two truth tables agree. For most purposes of logic, two logically equivalent forms are interchangeable with each other (since their truth values must agree), even though such forms are often not equal as strings.

(3). Although logical equivalence of propositional forms (denoted $\equiv$) is not the same concept as logical equality (denoted $=$), these two concepts share many common properties. For example, given any objects x, y, z whatsoever, the following facts are true about equality:

$$x = x, \text{ if } x = y \text{ then } y = x; \text{ if } x = y \text{ and } y = z \text{ then } x = z.$$

These facts are called *reflexivity*, *symmetry*, and *transitivity* of equality. Three analogous facts also hold for logical equivalence: given any propositional forms A, B, C,

$$A \equiv A; \text{ if } A \equiv B \text{ then } B \equiv A; \text{ if } A \equiv B \text{ and } B \equiv C \text{ then } A \equiv C.$$

These facts follow from the corresponding facts for equality, applied to the rows of the truth tables. For instance, if the output in every row of A's truth table equals the corresponding output of B's truth table, then the output in every row of B's truth table equals the corresponding output of A's truth table, which is why the second fact is true. The text implicitly uses the reflexivity, symmetry and transitivity of logical equivalence in many place. For instance, the derivation has the form $A \equiv B \equiv C \equiv D$, which is really an abbreviation for "$A \equiv B$ and $B \equiv C$ and $C \equiv D$." Using transitivity once, we see that $A \equiv C$. Using transitivity again, we see that $A \equiv D$, which is the required conclusion. Similarly, symmetry of $\equiv$ is needed whenever we want to use known logical equivalence in reverse, e.g., to replace $(P \wedge Q) \vee (P \wedge R)$ by $P \wedge (Q \vee R)$ by invoking the Distributive Law.

(4). The logical equivalences in this section's theorems apply to *all* propositional forms P, Q, R which means that we can replace each letter P, Q, R (wherever it appears in an identity) by a longer propositional form. For instance, replacing P by $A \Rightarrow B$ and Q by $B \oplus C$ in the second negation law, we see that $\neg((A \Rightarrow B) \wedge (B \oplus C)) \equiv (\neg(A \Rightarrow B)) \vee (\neg(B \oplus C))$. In contrast, consider the non-logical equivalence asserted in part (a) of the Theorem on IF. In that theorem, P and Q are distinct propositional variables (as opposed to general some choices of the form P and the form Q, the logical equivalence will hold; for instance, suppose P and Q are both R. It can be checked that when P and Q are logically equivalent forms, $(P \Rightarrow Q) \equiv (Q \Rightarrow P)$, because in this case we must always be in row 1 or row 4 of the truth table shown in the proof (In fact, using terminology from the next section, $P \Rightarrow Q$ and $Q \Rightarrow P$ are both tautologies in this situation.) For example, $((A \vee B) \Rightarrow (B \vee A))$ is logically equivalent to $((B \vee A) \Rightarrow (A \vee B))$. On the other hand, when P and Q are not logically equivalent, there must exist some assignment of truth values to the propositional variables appearing in P and Q that cause P and Q themselves to have opposite truth values. In this row of the truth table, $P \Rightarrow Q$ and $Q \Rightarrow P$ disagree, so that these forms are not logically equivalent. For instance, $((A \vee B) \Rightarrow (A \oplus B))$ and $((A \oplus B) \Rightarrow (A \vee B))$ are not logically equivalent, as we see by considering the row of the truth table where A and B are both true.

(5). In algebra, if we know two variable represent the same number, we can replace one variable by the other in longer expressions. We can express this fact symbolically by *substitution rules* such as the following: for all numbers x, y, z if $y = z$ then $x + y = x + z$ and $xy = xz$. There are analogous substitution rules for logically equivalent propositional forms. For instance, given any propositional forms A, B and C if $B \equiv C$, then $(A \vee B) \equiv (A \vee C)$, $(AB) \equiv (A \wedge C)$, $(A \Rightarrow B) \equiv (A \Rightarrow C)$, $(B \Rightarrow A) \equiv (C \Rightarrow A)$, and so on. We freely use these substitution rules without justification in the main text, but it is possible to provide each rule by comparing truth tables. As an example, assume $B \equiv C$, and consider a fixed row in the truth table for $A \Rightarrow B$ and $A \Rightarrow C$. Suppose that, for the values of the input propositional variables appearing in this row, A is true B is false. On one hand, $A \Rightarrow B$ must be false in this row. On the other hand, since B and C were assumed to be logically equivalent, C is false in this row, so $A \Rightarrow C$ is also false in this row. Thus, $A \Rightarrow B$ and $A \Rightarrow C$ have the same truth value (namely, false) in this row. Considering the other possible cases, we see that $A \Rightarrow B$ and $A \Rightarrow C$ have the same truth value in every row of the truth table, so they are logically equivalent. We can summarize the cases in a *meta-truth table* that looks like this:

A	B	C	$A \Rightarrow B$	$A \Rightarrow C$
T	T	T	T	T
T	F	F	F	F
F	T	T	T	T
F	F	F	T	T

We call this a meta-truth table because the underlying propositional variables appearing in A, B and C are not explicitly listed. (For example, these forms might involve five propositional variables P, Q, R, S and T, so that the actual truth table would have 32 rows.) However, to prove the logical equivalence of $A \Rightarrow B$ and $A \Rightarrow C$, we only need to know the truth values of the propositional forms, A, B and C. Row 2 of the table is an abbreviation for the discussion preceding the table, and the other rows cover the remaining cases. The key point is that the table has four rows, not eight, because we have assumed that B and C are logically equivalent forms, hence always have the same truth value. You can construct similar meta-truth tables to prove the other substitution principles.