INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

2. Truth tables, equivalences, and proof by contradiction

We use the word "statement" interchangeably with the word "sentence", and we agree that a statement can be true or false or neither, but a statement cannot be simultaneously true and false. In a mathematical system, the true statements and false statements are the propositions of the system, and the label "true" or "false" associated with a given proposition is its truth value.

Notation: We use the symbol $\neg$ to mean "not". We use the symbol $\wedge$ to mean "and". We use the symbol $\vee$ to mean "or". (Note that we do not use $\vee$ to mean "exclusive or"; that is, $P \vee Q$ is true if P is true or if Q is true or if both P and Q are true.) We use the symbol $\implies$ to mean "implies". (So $P \implies Q$ means that if P is true then Q is true.) We use the symbol $\iff$ to mean "if and only if"; so with P, Q propositions, $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. (So $P \iff Q$ means that P is true exactly when Q is true, and P is false exactly when Q is false.) When $P \iff Q$, we say P and Q are equivalent.

When a proposition P is true, we sometimes express this by saying that P holds.

Example: Suppose P and Q represent propositions. $P \implies Q$ is the proposition that P implies Q, or in other words, the proposition that if P is true then Q is true. To state this more emphatically, $P \implies Q$ means that **if** P is true, then Q **must** be true. Note that $P \implies Q$ allows for P and Q to both be true, or for P to be false and Q to be true, or for P and Q to both be false. However, $P \implies Q$ does not allow for P to be true and Q to be false. (Initially, it can seem confusing that $P \implies Q$ is true when P and Q are false. However, having P and Q false does not contradict that Q must be true if P is true.) We can represent this scenario using what is called a "truth table", wherein we consider all possible combinations of the truth values of P and Q, and the consequent truth value of $P \implies Q$:

P	Q	$[P \implies Q]$
T	T	T
T	F	F
F	T	T
F	F	T

(The square brackets on the top line of the truth table are used simply to make it easier to distinguish the three propositions from each other.)

Note: We could prove the truth of the following propositions and theorems without using truth tables, but here we use truth table to establish some fundamental and useful results in a rather painless way.

Example: Suppose P and Q represent propositions. $P \wedge Q$ is true exactly when P and Q are both true. So the corresponding truth table is:

P	Q	$[P \wedge Q]$
T	T	T
T	F	F
F	T	F
F	F	F

Example: Suppose P and Q represent propositions. $P \vee Q$ is true exactly when P or Q is true. We do not use the word "or" to mean "exclusive or", so $P \vee Q$ is true when P and Q are both true. So the corresponding truth table is:

P	Q	$[P \vee Q]$
T	T	T
T	F	T
F	T	T
F	F	F

Example: Suppose P and Q represent propositions. The corresponding truth table for $(\neg P) \vee Q$ is:

P	Q	$[\neg P \vee Q]$
T	T	T
T	F	F
F	T	T
F	F	T

Example: Suppose P and Q represent propositions. The corresponding truth table for $\neg Q \implies \neg P$ is:

P	Q	$[\neg Q \implies \neg P]$
T	T	T
T	F	F
F	T	T
F	F	T

This truth table can be easier to determine by expanding it as follows.

P	Q	$\neg P$	$\neg Q$	$[\neg Q \implies \neg P]$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Theorem 2.1. *Suppose P, Q are propositions.*

(a) $P \implies Q$ *is equivalent to* $\neg Q \implies \neg P$.

(b) $P \implies Q$ *is equivalent to* $\neg P \vee Q$.

Proof. We prove (a) and leave (b) as an exercise.

P	Q	$[P \implies Q]$	$[\neg Q \implies \neg P]$	$[(P \implies Q) \iff (\neg Q \implies \neg P)]$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

So for all truth values of P and Q, $(P \implies Q)$ and $(\neg Q \implies \neg P)$ have the same truth values. Hence $[(P \implies Q) \iff (\neg Q \implies \neg P)]$. □

Definitions. We call the proposition $\neg Q \implies \neg P$ the contrapositive of the proposition $P \implies Q$. As seen above, the proposition $P \implies Q$ is equivalent to its contrapositive. The proposition $Q \implies P$ is called the converse of the proposition $P \implies Q$; as an exercise one shows that $Q \implies P$ is not equivalent to $P \implies Q$.

We also have this easily proved result.

Proposition 2.2. *Suppose P is a proposition. Then $P \iff \neg(\neg P)$.*

Proof.

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

So the truth values of P and $\neg(\neg P)$ always agree, so the propositions P and $\neg(\neg P)$ are equivalent. □

The next proposition shows that $\wedge$ and $\vee$ are "associative", meaning that $P \wedge Q \wedge R$ and $P \vee Q \vee R$ are propositions that do not require parentheses.

Proposition 2.3. *Suppose P, Q, R are propositions.*

(a) $(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R)$.
(b) $(P \vee Q) \vee R \iff P \vee (Q \vee R)$.

Proof. We prove (a), and leave the proof of (b) as an exercise.

P	Q	R	$(P \wedge Q)$	$[(P \wedge Q) \wedge R]$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	F
T	F	F	F	F
F	T	T	F	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

Also:

P	Q	R	$(Q \wedge R)$	$[P \wedge (Q \wedge R)]$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

So for any truth values of P, Q, R, these truth tables show that $[(P \wedge Q) \wedge R] \iff [P \wedge (Q \wedge R)]$.

Note that one could combine the above truth tables into one (large) table, or just combine some of the information from these two truth tables into one truth table as follows:

P	Q	R	$[(P \wedge Q) \wedge R]$	$[P \wedge (Q \wedge R)]$	$[(P \wedge Q) \wedge R] \iff [P \wedge (Q \wedge R)]$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	F	F	T
T	F	F	F	F	T
F	T	T	F	F	T
F	T	F	F	F	T
F	F	T	F	F	T
F	F	F	F	F	T

□

The above proposition shows we can write $P \wedge Q \wedge R$ and $P \vee Q \vee R$, without there being confusion. As a trivial exercise, one can also show the following sometimes useful equivalences.

Proposition 2.4. *Suppose P, Q, R are propostions. Then*

$$P \wedge Q \wedge R \iff (P \wedge Q) \wedge (P \wedge R), \text{ and } P \vee Q \vee R \iff (P \vee Q) \vee (P \vee R).$$

Proposition 2.5. *Suppose P, Q, R are propositions.*

(a) $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$.
(b) $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$.

Proof. We prove (a) and leave the proof of (b) as an exercise.

P	Q	R	$(Q \vee R)$	$[P \wedge (Q \vee R)]$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

Also:

P	Q	R	$(P \wedge Q)$	$(P \wedge R)$	$[(P \wedge Q) \vee (P \wedge R)]$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

So for any truth values of P, Q, R, these truth tables show that

$$[P \wedge (Q \vee R)] \iff [(P \wedge Q) \vee (P \wedge R)].$$

□

Theorem 2.6. *Suppose P, Q are propositions.*

(a) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.
(b) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$.
(c) $\neg(P \implies Q) \iff (P \wedge \neg Q)$.

Proof. Using a truth table, we prove (a) and leave (b) and (c) as exercises.

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

Thus for any truth values of P, Q, R, the truth values of $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are the same. This proves (1). □

As an exercise, one proves the following.

Proposition 2.7. *Suppose P, Q are propositions. Then $[P \vee Q] \iff [\neg P \implies Q]$.*

Note: With P, Q, R propositions, $P \implies Q \iff R$ and $P \iff Q \implies R$ do not have clear meanings. As exercises, one shows that the statements $P \implies (Q \iff R)$ and $(P \implies Q) \iff R$ are not equivalent, and $P \iff (Q \implies R)$ and $(P \iff Q) \implies R$ are not equivalent. Note that this also means an assertion such as

$$P \implies Q \iff R \implies S$$

has no clear meaning.

Proof by contradiction. A proof by contradiction proceeds as follows. Suppose R is a proposition we want to prove is true, and S is a proposition we know is false. Consider the following truth table:

S	R	$\neg R$	$(\neg R \implies S)$
F	T	F	T
F	F	T	F

If we can prove $\neg R \implies S$ is true, then we must have that R is true.

Example: Suppose $m, n \in \mathbb{Z}_+$ with $m + n < 89$. We claim that $m < 45$ or $n < 45$. For the sake of contradiction, suppose $\neg[(m < 45) \vee (n < 45)]$; that is, suppose $m \geq 45$ and $n \geq 45$. Then $m + n \geq 90$, contradicting the assumption that $m + n < 89$. Hence we must have $(m < 45) \vee (n < 45)$.

In this example, the proposition we know to be false is $R \wedge \neg R$ where R is the proposition that $m + n < 89$.

As an exercise, one uses truth tables to prove the following.

Proposition 2.8. *With P, Q propositions,* $[\neg(P \implies Q) \implies \neg P] \iff [P \implies Q]$.

This gives us another method to argue by contradiction: Suppose we want to prove that $P \implies Q$. For the sake of contradiction, suppose $\neg(P \implies Q)$, or equivalently, suppose $\neg(\neg P \vee Q)$. So we are supposing that $P \wedge \neg Q$. If we can deduce that $(P \wedge \neg Q) \implies \neg P$, then since our assumption $P \wedge \neg Q$ leads to a contradiction [namely $P \wedge \neg P$], $P \wedge \neg Q$ must be false, and hence $P \implies Q$ must be true.

Theorem 2.9. *(Pigeonhole Principle) Let A be a set with n elements and B a set with m elements where $m, n \in \mathbb{Z}_+$ with $m < n$. Then there is no injection from A into B. (So if n pigeons fly into m pigeonholes, then at least one pigeonhole contains more than one pigeon.)*

Proof. (We present two proofs for this result, a proof by contradiction and a proof by contrapositive.)

Proof 1: For the sake of contradiction, suppose $g : A \to B$ is injective. Enumerate the elements of A as $a_1, a_2, \ldots, a_n$ and the elements of B as $b_1, b_2, \ldots, b_m$. Let $C = \{g(a_i) : i \in \mathbb{Z}_+, i \leq n\}$. Thus C is a subset of B, and since g is injective, C is a set with n elements. But this means there is a subset of B containing more elements than are in B, which is impossible. Thus it cannot be possible to have an injective function $g : A \to B$.

Proof 2: The statement of the theorem is equivalent to "Let A be a set with n elements and B a set with m elements where $m, n \in \mathbb{Z}_+$. If $m < n$ then there is no injection from A into B." The contrapositive of this statement is "Let A be a set with n elements and B a set with m elements where $m, n \in \mathbb{Z}_+$. If there is an injection from A into B then $m \geq n$." We will prove this latter statement. Suppose $g : A \to B$ is injective. Enumerate the elements of A as $a_1, a_2, \ldots, a_n$ and the elements of B as $b_1, b_2, \ldots, b_m$. Let $C = \{g(a_i) : \ i \in \mathbb{Z}_+, \ i \leq n \ \}$. Thus C is a subset of B, and since g is injective, C is a set with n elements. Thus B must have at least n elements, meaning $m \geq n$.

□

Sometimes one can prove a result by contrapositive using an argument that is almost identical to proving the result by contradiction (as above). However, there are occassions where this is not the case; we will see an example of this later in the course when we prove by contradiction that the interval $(0, 1) \subseteq \mathbb{R}$ is what we call "uncountable".