# Discrete Mathematics

Daniel Gonzalez Cedre

University of Notre Dame
Spring of 2023

# Chapter 1

# Propositional Logic

## 1.1 Propositions & Connectives

**Definition 1.1** (Proposition).

A *proposition* is a sentence (in our language) that has one (and only one) definite, consistent truth value.

**Definition 1.2** (Negation).

Given a proposition $p$, the *negation* of $p$ is denoted $\neg p$ and is defined by the following truth table:

| $p$ | $\neg p$ |
|---|---|
| $\top$ | $\bot$ |
| $\bot$ | $\top$ |

Some possible readings of $\neg p$:

- Not $p$.
- $p$ does not hold.
- It is not the case that $p$.
- We do not have that $p$.

**Definition 1.3** (Conjunction).

Given two propositions $p$ and $q$, the *conjunction* of $p$ with $q$ is denoted $p \wedge q$ and is defined by the following truth table:

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ |
| $\bot$ | $\top$ | $\bot$ |
| $\bot$ | $\bot$ | $\bot$ |

Some possible readings of $p \wedge q$:

- $p$, and $q$.
- $p$, but $q$.
- $p$; also, $q$.
- $p$; further, $q$.
- In addition to $p$, we also have $q$.

**Definition 1.4** (Disjunction).

Given two propositions $p$ and $q$, the *disjunction* of $p$ with $q$ is denoted $p \vee q$ and is defined by the following truth table:

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\top$ |
| $\bot$ | $\top$ | $\top$ |
| $\bot$ | $\bot$ | $\bot$ |

Some possible readings of $p \vee q$:

- $p$, or $q$.
- Either $p$, or $q$.

**Definition 1.5** (Material Implication)**.**

Given two propositions $p$ and $q$, the *conditional* formed by assuming $p$ and concluding $q$ is denoted $p \to q$ and is defined by the following truth table:

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ |
| $\bot$ | $\top$ | $\top$ |
| $\bot$ | $\bot$ | $\top$ |

Some possible readings of $p \to q$:

- If $p$, then $q$.
- $p$ implies $q$.
- $q$ is conditioned on $p$.
- $q$ only if $p$.
- $p$ is sufficient for $q$.
- $q$ is necessary for $p$.
- $q$ unless not $p$.
- $q$ or not $p$.

**Definition 1.6** (Biconditional)**.**

Given two propositions $p$ and $q$, the *biconditional* formed by $p$ and $q$ is denoted $p \leftrightarrow q$ and is defined by the following truth table:

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ |
| $\bot$ | $\top$ | $\bot$ |
| $\bot$ | $\bot$ | $\top$ |

Some possible readings of $p \leftrightarrow q$:

- $p$ if and only if $q$.
- $p$ is necessary and sufficient for $q$.
- $q$ is necessary and sufficient for $p$.

**Definition 1.7** (Equivalence)**.**

If we have two expressions $\varphi$ and $\psi$ in our formal language, consisting of some number of (possibly shared) propositional variables, connected together by logical connectives, then with the notation $\varphi \Leftrightarrow \psi$ we say that $\varphi$ is equivalent to $\psi$ $:\Leftrightarrow$ every assignment of truth values to the propositional variables of $\varphi$ and $\psi$ results in the same truth value for the two expressions.

**Example 1.1.**

Consider the two expressions $\varphi := p \to q$ and $\psi := \neg p \lor q$. We can see that $\varphi$ has two propositional variables: $p$ and $q$. $\psi$ also has two propositional variables: the same $p$ and the same $q$. If we construct the truth table for these two expressions, we will see that every assignment of truth values to $p$ and $q$ will result in $p \to q$ and $\neg p \lor q$ having the same truth value.

| $p$ | $q$ | $p \to q$ | $\neg p \lor q$ |
|---|---|---|---|
| $\top$ | $\top$ | $\top$ | $\top$ |
| $\top$ | $\bot$ | $\bot$ | $\bot$ |
| $\bot$ | $\top$ | $\top$ | $\top$ |
| $\bot$ | $\bot$ | $\top$ | $\top$ |

**Definition 1.8** (Tautology & Contradiction)**.**

Let $\varphi$ be a propositional expression consisting of the propositional variables $p_1, \dots p_n$.
We say is a *tautology* $:\Leftrightarrow$ every assignment of truth values to $p_1, \dots p_n$ such that $\varphi \Leftrightarrow \top$.
We say $\varphi$ is a *contradiction* $:\Leftrightarrow$ there exists an assignment of truth values to $p_1, \dots p_n$ such that $\varphi \Leftrightarrow \bot$.

**Definition 1.9** (Satisfiability)**.**

A propositional expression $\varphi$ consisting the propositional variables $p_1, \dots p_n$ is *satisfiable* $:\Leftrightarrow$ there exists an assignment of truth values to $p_1, \dots p_n$ that results in $\varphi$ being equivalent to $\top$.

## 1.2 Boolean Algebras

**Definition 1.10** (Boolean Algebra).

A *Boolean algebra* is a collection of *terms* $B$ with two distinguished (and distinct) terms called $\top$ and $\bot$, along with a unary operation called $\neg$ and two binary operations called $\wedge$ and $\vee$, such that the following statements are true for any terms $p, q, r$ in $B$:

| Axioms of a Boolean Algebra | |
|---|---|
| Identity | $p \wedge \top \Leftrightarrow p$<br>$p \vee \bot \Leftrightarrow p$ |
| Complement (*a.k.a.* Negation) | $p \wedge \neg p \Leftrightarrow \bot$<br>$p \vee \neg p \Leftrightarrow \top$ |
| Commutativity | $p \wedge q \Leftrightarrow q \wedge p$<br>$p \vee q \Leftrightarrow q \vee p$ |
| Associativity | $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$<br>$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ |
| Distributive Laws | $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$<br>$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ |

This kind of structure is also referred to as a *complemented, distributive lattice*. Since we are establishing the algebra of *propositions*, our terms consist only of $\top$ and $\bot$.

However, since none of these axioms tell us how to use the (very useful) symbols $\rightarrow$ and $\leftrightarrow$, we need two additional axioms that will turn our Boolean algebra into an example of a *Heyting algebra*:

| Heyting Axioms | |
|---|---|
| Conditional Disintegration | $p \rightarrow q \Leftrightarrow \neg p \vee q$ |
| Biconditional Disintegration | $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$ |

By referring to the truth tables, it should be easy to see that these axioms are *truth preserving* transformations, meaning that taking an expression like $p \wedge (q \rightarrow r)$ and applying an axiom like Identity to it does not change the truth value of the resulting expression $(p \wedge \top) \wedge (q \rightarrow r)$. For this reason, these are sometimes referred to as *equivalence laws* and many treatments of this subject *prove* these laws by referring to the truth tables.

For our purposes, we don't need to refer to the truth tables at all. The truth tables were a nice, intuitive, and compact way of defining the logical connectives, but we could just as easily have defined them by assuming that all of the axioms are true, without ever writing down a truth table. This provides a more *algebraic* approach to the study of logic, which is more in-line with the way logic is used to actually prove theorems in mathematics.

As such, while the while the truth tables provided a nice way of defining the logical connectives, we will be taking the algebraic approach by *assuming the axioms* of a Boolean algebra are true about our propositional logic and using them to prove theorems about our logical system.

**Theorem 1.1** (Uniqueness of Complements).

*Let $p$ be a term in a Boolean algebra $(B, \neg, \wedge, \vee)$. Suppose there were two terms $x$ and $y$ in the Boolean algebra such that*

$$\begin{aligned} p \wedge x &\Leftrightarrow \bot, & p \wedge y &\Leftrightarrow \bot, \\ p \vee x &\Leftrightarrow \top, & p \vee y &\Leftrightarrow \top, \end{aligned}$$

*meaning that $x$ and $y$ act like negations for $p$. Then, we have $x \Leftrightarrow y$.*

*Proof.*

Let $(B, \neg, \wedge, \vee)$ be a Boolean algebra and consider an arbitrary term $p$ in the algebra. Suppose we have $x$ and $y$ satisfying the conditions given in the statement of the theorem above. Then, we can observe

$$\begin{aligned} x &\Leftrightarrow \top \wedge x && \text{by Identity} \\ &\Leftrightarrow (p \vee y) \wedge x && \text{by the assumption } p \vee y \Leftrightarrow \top \\ &\Leftrightarrow (p \wedge x) \vee (y \wedge x) && \text{by Distributivity} \\ &\Leftrightarrow \bot \vee (y \wedge x) && \text{by the assumption } p \wedge x \Leftrightarrow \bot \\ &\Leftrightarrow y \wedge x && \text{by Identity.} \end{aligned}$$

Similarly, we can see that

$$\begin{aligned} y &\Leftrightarrow \top \wedge y && \text{by Identity} \\ &\Leftrightarrow (p \vee x) \wedge y && \text{by the assumption } p \vee x \Leftrightarrow \top \\ &\Leftrightarrow (p \wedge y) \vee (x \wedge y) && \text{by Distributivity} \\ &\Leftrightarrow \bot \vee (x \wedge y) && \text{by the assumption } p \wedge y \Leftrightarrow \bot \\ &\Leftrightarrow x \wedge y && \text{by Identity.} \end{aligned}$$

So, from Commutativity, we can conclude that $x \Leftrightarrow (y \wedge x) \Leftrightarrow (x \wedge y) \Leftrightarrow y$.

Q.E.D.

**Theorem 1.2** (Double Negation)**.**

*For any Boolean algebra* $(B, \neg, \wedge, \vee)$ *and any term* $p$ *in the algebra, we have* $\neg\neg p \Leftrightarrow p$.

*Proof.*

Let $(B, \neg, \wedge, \vee)$ be a Boolean algebra and consider an arbitrary term $p$ in the algebra. We want to show that $\neg\neg p \Leftrightarrow p$.

By the Complement axiom, we know $p \wedge \neg p \Leftrightarrow \bot$ and $p \vee \neg p \Leftrightarrow \top$, meaning that $p$ is the complement of $\neg p$. Similarly, we can see that $\neg p \wedge \neg(\neg p) \Leftrightarrow \bot$ and $\neg p \vee \neg(\neg p) \Leftrightarrow \top$, showing us that $\neg\neg p$ is the complement of $\neg p$.

Since complements are unique, as seen in Theorem 1.1, and both $p$ and $\neg\neg p$ are complements of $\neg p$, we must have that $p \Leftrightarrow \neg\neg p$.

Q.E.D.

**Theorem 1.3** (Idempotency)**.**

*For every Boolean algebra* $(B, \neg, \wedge, \vee)$ *and every term* $p$ *in the algebra, we have*

$$\begin{aligned} p \wedge p \Leftrightarrow p \\ p \vee p \Leftrightarrow p. \end{aligned}$$

*Proof.*

Let $p$ be a term in an arbitrary Boolean algebra $(B, \neg, \wedge, \vee)$. Observe

$$\begin{aligned} p \wedge p &\Leftrightarrow (p \wedge p) \vee \bot && \text{by Identity} & p \vee p &\Leftrightarrow (p \vee p) \wedge \top && \text{by Identity} \\ &\Leftrightarrow (p \wedge p) \vee (p \wedge \neg p) && \text{by Complement} & &\Leftrightarrow (p \vee p) \wedge (p \vee \neg p) && \text{by Complement} \\ &\Leftrightarrow p \wedge (p \vee \neg p) && \text{by Distributivity} & &\Leftrightarrow p \vee (p \wedge \neg p) && \text{by Distributivity} \\ &\Leftrightarrow p \wedge \top && \text{by Complement} & &\Leftrightarrow p \vee \bot && \text{by Complement} \\ &\Leftrightarrow p && \text{by Identity,} & &\Leftrightarrow p && \text{by Identity.} \end{aligned}$$

Therefore, $p \wedge p \Leftrightarrow p$ and $p \vee p \Leftrightarrow p$, as desired.

Q.E.D.

**Theorem 1.4** (Domination)**.**

*For every Boolean algebra $(B, \neg, \wedge, \vee)$ and every term $p$ in the algebra, we have*

$$p \wedge \bot \Leftrightarrow \bot$$
$$p \vee \top \Leftrightarrow \top.$$

*Proof.*

Let $p$ be a term in an arbitrary Boolean algebra $(B, \neg, \wedge, \vee)$. Observe

$$\begin{aligned} p \wedge \bot &\Leftrightarrow p \wedge (p \wedge \neg p) && \text{by Complement} \\ &\Leftrightarrow (p \wedge p) \wedge \neg p && \text{by Associativity} \\ &\Leftrightarrow p \wedge \neg p && \text{by Idempotency} \\ &\Leftrightarrow \bot && \text{by Complement,} \end{aligned} \qquad \begin{aligned} p \vee \top &\Leftrightarrow p \vee (p \vee \neg p) && \text{by Complement} \\ &\Leftrightarrow (p \vee p) \vee \neg p && \text{by Associativity} \\ &\Leftrightarrow p \vee \neg p && \text{by Idempotency} \\ &\Leftrightarrow \top && \text{by Complement.} \end{aligned}$$

Therefore, $p \wedge \bot \Leftrightarrow \bot$ and $p \vee \top \Leftrightarrow \top$.

Q.E.D.

**Theorem 1.5** (Absorption)**.**

*For every Boolean algebra $(B, \neg, \wedge, \vee)$ and any two terms $p$ and $q$ in the algebra, we have*

$$p \wedge (p \vee q) \Leftrightarrow p$$
$$p \vee (p \wedge q) \Leftrightarrow q.$$

*Proof.*

Let $p$ and $q$ be terms in an arbitrary Boolean algebra $(B, \neg, \wedge, \vee)$. Observe

$$\begin{aligned} p \wedge (p \vee q) &\Leftrightarrow (p \vee \bot) \wedge (p \vee q) && \text{by Identity} \\ &\Leftrightarrow p \vee (\bot \wedge q) && \text{by Distributivity} \\ &\Leftrightarrow p \vee \bot && \text{by Domination} \\ &\Leftrightarrow p && \text{by Identity,} \end{aligned} \qquad \begin{aligned} p \vee (p \wedge q) &\Leftrightarrow (p \wedge \top) \vee (p \wedge q) && \text{by Identity} \\ &\Leftrightarrow p \wedge (\top \vee q) && \text{by Distributivity} \\ &\Leftrightarrow p \wedge \top && \text{by Domination} \\ &\Leftrightarrow p && \text{by Identity.} \end{aligned}$$

Therefore, $p \wedge (p \vee q) \Leftrightarrow p$ and $p \vee (p \wedge q) \Leftrightarrow q$.

Q.E.D.

**Theorem 1.6** (De Morgan's Laws)**.**

*For every Boolean algebra $(B, \neg, \wedge, \vee)$ and any two terms $p$ and $q$ in the algebra, we have*

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$
$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q.$$

*Proof.*

Let $p$ and $q$ be terms in an arbitrary Boolean algebra $(B, \neg, \wedge, \vee)$. For the first statement, we need to show that $p \wedge q$ is a complement for $\neg p \vee \neg q$, meaning $(p \wedge q) \wedge (\neg p \vee \neg q) \Leftrightarrow \bot$ and $(p \wedge q) \vee (\neg p \vee \neg q) \Leftrightarrow \top$.

Observe that

$$\begin{aligned} (p \wedge q) \wedge (\neg p \vee \neg q) &\Leftrightarrow (q \wedge p) \wedge (\neg p \vee \neg q) && \text{by Commutativity} \\ &\Leftrightarrow q \wedge (p \wedge (\neg p \vee \neg q)) && \text{by Associativity} \\ &\Leftrightarrow q \wedge ((p \wedge \neg p) \vee (p \wedge \neg q)) && \text{by Distributivity} \\ &\Leftrightarrow q \wedge (\bot \vee (p \wedge \neg q)) && \text{by Complement} \end{aligned}$$

$$
\begin{aligned}
&\Leftrightarrow q \wedge (p \wedge \neg q) && \text{by Identity} \\
&\Leftrightarrow q \wedge (\neg q \wedge p) && \text{by Commutativity} \\
&\Leftrightarrow (q \wedge \neg q) \wedge p && \text{by Associativity} \\
&\Leftrightarrow \bot \wedge p && \text{by Complement} \\
&\Leftrightarrow \bot && \text{by Domination.}
\end{aligned}
$$

Further, we have

$$
\begin{aligned}
(p \wedge q) \vee (\neg p \vee \neg q) &\Leftrightarrow (p \wedge q) \wedge (\neg q \vee \neg p) && \text{by Commutativity} \\
&\Leftrightarrow ((p \wedge q) \vee \neg q) \vee \neg p && \text{by Associativity} \\
&\Leftrightarrow ((p \vee \neg q) \wedge (q \vee \neg q)) \vee \neg p && \text{by Distributivity} \\
&\Leftrightarrow ((p \vee \neg q) \wedge \top) \vee \neg p && \text{by Complement} \\
&\Leftrightarrow (p \vee \neg q) \vee \neg p && \text{by Identity} \\
&\Leftrightarrow (\neg q \vee p) \vee \neg p && \text{by Commutativity} \\
&\Leftrightarrow \neg q \vee (p \vee \neg p) && \text{by Associativity} \\
&\Leftrightarrow \neg q \vee \top && \text{by Complement} \\
&\Leftrightarrow \top && \text{by Domination.}
\end{aligned}
$$

So, we can see that $p \wedge q$ is a complement for $\neg p \vee \neg q$. Since complements are unique by Theorem 1.1, we can conclude that $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$.

Showing $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ is left as an exercise to the reader.

Q.E.D.