MATH 318 Mathematical Logic

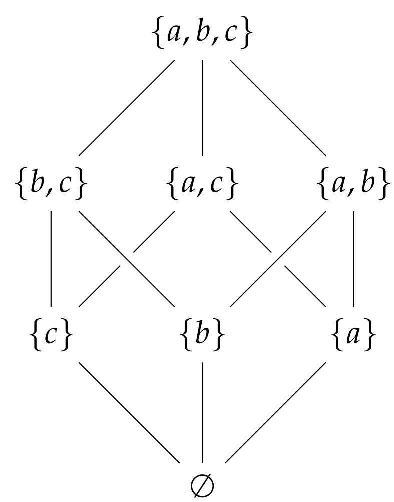
Class notes

Notes by: Yue Ru Sun[1]

Instructor: Dr. Marcin Sabok

McGill University

Last updated: December 15, 2015



[1] If you find any error or typo, please notify the author at yue.r.sun@mail.mcgill.ca

Contents

1 Introduction

These are the class notes of the Mathematical Logic course given by professor Marcin Sabok at McGill University in 2014. There was no required textbook, but a reference:

• "A Mathematical Introduction to Logic" by Herbert B. Enderton

and also a recommended graphic novel:

• "Logicomix: an Epic Search for Truth" by Apostolos Doxiadis and Christos H. Papadimitriou

All errors are responsibility of the author. If you find any error or typo, please notify the author at *yue.r.sun@mail.mcgill.ca*.

2 Basic set theory

In set theory, everything is a set. A set is determined by its elements. Given any set X, we can form the set $\{X\}$.

The empty set : $\emptyset$.
Examples of sets: $\{\emptyset\}$, $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Extensionality property: two sets are equal iff they have the same elements.
The formal axioms of Zermelo-Fraenkl set theory are presented later, in 9.5.

To interpret natural numbers as sets, we adopt the convention

$$\begin{aligned}
0 &:= \emptyset \\
1 &:= \{\emptyset\} \\
2 &:= \{0, 1\} \\
3 &:= \{0, 1, 2\} \\
&\vdots \\
n &:= \{0, 1, ..., n-1\} \\
\mathbb{N} &:= \{0, 1, 2, 3, ...\}
\end{aligned}$$

Definition. A set A is a *subset* of B, denoted $A \subseteq B$, if $\forall a \in A, a \in B$.

Example 2.1. $\{0,1\} \subseteq \{0,1,2,3\}$

$\{2,5\} \subseteq \mathbb{N}$

$3 \not\subseteq \{3,4\}$

$3 \subseteq 4$, and also, $3 \in 4$

Operations on sets

- Intersection
- Union
- Difference
$$A \backslash B := \{a \in A : a \notin B\}$$
- Union of a set
$$\bigcup A := \{x \in B : B \in A\}$$
In words, given a set A, $\bigcup A$ is the set consisting of those sets which are elements of some element of A.

Example 2.2. $\{\emptyset\} \cap \{\{\emptyset\}\} = \emptyset$

$\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

$\bigcup\{A, B\} = A \cup B$

$\bigcup \mathbb{N} = \mathbb{N}$

Proposition 2.3. *For any sets A, B, C,*
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

Proposition 2.4. *For any sets A, B, C,*
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Theorem 2.5. *(De Morgan's Laws)*
For any sets A, B, C,

$$A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$$
$$A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$$

Definition. Given any set A, its *powerset*, denoted by $\mathcal{P}(A)$, is the set of all subsets of A.

Example 2.6. $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Hasse diagram of powerset

$$\begin{tikzcd}[column sep=small]
 & \{1,2\} \arrow[dl, dash] \arrow[dr, dash] & \\
\{1\} \arrow[dr, dash] & & \{2\} \arrow[dl, dash] \\
 & \emptyset &
\end{tikzcd}$$

Definition. Given two sets A and B, define *ordered pair* (A, B) so that

$$(A, B) = (A', B') \iff A = A' \text{ and } B = B'$$

If $A = B$, $(A, B) = \{\{A\}, \{A, B\}\}$.
If $A \neq B$, $(A, B) = \{\{A\}\}$.

Definition. The *Cartesian product* of sets A, B, denoted $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A, b \in B$.

Definition. The set-theoretical definition of the *set of rational numbers* $\mathbb{Q}$ is

$$\{(0, (p,q) \in 2 \times (\mathbb{N} \times \mathbb{N}) : \ \gcd(p,q) = 1, q \neq 0\} \cup \{(1, (p,q) \in 2 \times (\mathbb{N} \times \mathbb{N}) : \ \gcd(p,q) = 1, q \neq 0\}$$

where the binary digit in the first coordinate of the pair is used to indicate the sign of the rational number.

Definition. A *Dedekind cut* of $\mathbb{Q}$ is an order pair (A, B) with $A, B \subseteq \mathbb{Q}$ and

- If $a \in A$, $b \in B$, then $a < b$;
- If $a \in A$, $a' \in \mathbb{Q}$, $a' < a$, then $a' \in A$;
- If $b \in B$, $b' \in \mathbb{Q}$, $b < b'$, then $b' \in B$;

- $\mathbb{Q} = A \cup B$;
- A has no greatest element.

Definition. The *set of real numbers* $\mathbb{R}$ is the set of all Dedekind's cuts of $\mathbb{Q}$.

Definition. n-tuple.

$$(a_1, a_2, a_3, ..., a_n) := (\cdots((a_1, a_2), a_3), ...), a_n)$$

The set $A_1 \times A_2 \times \cdots \times A_n$ consists of all sets of the form $(a_1, a_2, ..., a_n)$ with $a_i \in A_i$, for each $1 \leq i \leq n$.

3 Relations and functions

Definition. A *relation* on sets $X_1, X_2, ..., X_n$ is any subset $R \subseteq X_1 \times X_2 \times \cdots \times X_n$.
A *binary relation* on sets X_1, X_2 is any subset $R \subseteq X_1 \times X_2$.

Definition. A relation R is said to be

- *symmetric* if $(x, y) \in R$, then also $(y, x) \in R$.
- *antisymmetric* if $(x, y) \in R$ and $(y, x) \in R$, then $x = y$;
- *reflexive* if $(x, x) \in R$ for all x.
- *irreflexive* if $(x, x) \notin R$ for all x.
- *transitive* if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

If A is a finite set enumerated as

$$A = \{a_1, a_2, ..., a_n\}$$

and R is a relation on A, then we can form matrix M_R of R

$$M_R = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

where

$$a_{ij} = \begin{cases} 1 & \text{if } (a_i, a_j) \in \mathbb{R} \\ 0 & \text{if } (a_i, a_j) \notin \mathbb{R} \end{cases}$$

Definition. Given the binary relations R and S on a set X, their *composition* is

$$R \circ S = \{(x, y) \in X^2 : \exists z \text{ such that } (x, z) \in R, (z, y) \in S\}$$

Remark 3.1. If R, S are relations on set $A = \{a_1, a_2, ..., a_n\}$, and M_R, M_S are matrices of R and S, then $(a_i, a_j) \in R \circ S$ if and only if the entry $a_{ij} > 0$ in the matrix product $M_R \cdot M_S$.

Definition. Given a binary relation R on X, its *inverse* is

$$R^{-1} = \{(y, x) \in X^2 : (x, y) \in R\}$$

Exercise 3.2. Check that

- $R = R^{-1}$ if and only if R is symmetric.
- $R \cup R^{-1}$ is always symmetric.
- $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Definition. The *transitive closure* of a relation R is

$$\text{tr}(R) = R \cup R^2 \cup R^3 \cup \cdots = \bigcup_{n \in \mathbb{N}^+} R^n$$

where $R^n = \underbrace{R \circ R \circ \cdots \circ R}_{n \text{ times}}$.

Proposition 3.3. *tr(R) is the smallest transitive relation containing R.*

Proof. If $(x, y), (y, x) \in \text{tr}(R)$, then $(x, y) \in R^n$, $(y, x) \in R^m$ for some $n, m \in \mathbb{N}^+$. Then $(x, z) \in R^n \circ R^m = R^{n+m} \subseteq \text{tr}(R)$. This shows $\text{tr}(R)$ is indeed a transitive relation.
To show it is the smallest, it suffices to note that if S is transitive and $R \subseteq S$, then $\text{tr}(R) \subseteq S$; It is so since given that S is transitive, $S \circ S \subseteq S$, so $R^2 \subseteq S$; similarly $S \circ S \circ S \subseteq S$, so $R^3 \subseteq S$, and so on, thus $\text{tr}(R) = \bigcup_{n \in \mathbb{N}^+} R^n \subseteq S$. $\square$

A symmetric relation is also called a *graph*. An arbitrary relation is also called a *directed graph*.

In database theory, a database is a relation if

$$R \subseteq X_1 \times X_2 \times \cdots \times X_n$$

X_i's are called *attributes*. The composition of relations often serve as simple SQL query.

Example 3.4. If R, S are relations, $R \subseteq X \times Y,\ S \subseteq Y \times Z$.

$$\left.\begin{array}{ll} SELECT & R\ x,\ S\ z \\ FROM & R,\ S \\ WHERE & R\ y = S\ y \end{array}\right\} \text{compute } R \circ S.$$

3.1 Equivalence Relations

Definition. A *equivalence relation* is a relation that is reflective, symmetric and transitive.[2]

Exercise 3.5. Check that the followings are equivalence relations.

- The relation $\equiv_k$ on $\mathbb{Z}$, $k \in \mathbb{Z}$, defined by

$$x \equiv_k y \text{ iff } k|(x - y)$$

- The relation E on $\mathbb{R}^2$ defined by

$$(x_1, x_2)E(y_1, y_2) \text{ iff } x_1 = y_1$$

- The relation E_Q on $\mathbb{R}$

$$xE_Q y \text{ iff } x - y \in \mathbb{Q}$$

Exercise 3.6. Show that the followings are <u>not</u> equivalence relations.

- The relation R on $\mathbb{R}$ defined by

$$xRy \text{ iff } x - y \geq 0$$

- The relation R on $\mathbb{Z}$ defined by

$$xRy \text{ iff } x = -y$$

[2] When you want to determine whether a given relation is an equivalence relation, just check these three conditions one by one.

- The relation R on $\mathbb{R}$ defined by

$$xRy \text{ iff } x - y \notin \mathbb{Q}$$

Definition. If E is an equivalence relation on X and $x \in X$, the *equivalence class* of x is

$$[x]_E = \{a \in X : xEa\}$$

We drop the subscript and write simply $[x]$ when the context is clear.

The *quotient of X by E* is

$$X/E = \{[x]_E : x \in X\}$$

Exercise 3.7. Determine the equivalence classes in 3.5.

Proposition 3.8. *If E is an equivalence relation on X and $x, y \in X$, then*

$$xEy \iff [x]_E = [y]_E$$

Proof. Suppose xEy, we take $z \in [x]$, zEx; by transitivity $zEx, xEy \Rightarrow zEy$, so $z \in [y]$. So $[x] \subseteq [y]$. Similarly $[y] \subseteq [x]$. For the "if" direction, suppse $[x] = [y]$. Then $x \in [x] = [y] \Rightarrow x \in [y] \Rightarrow xEy$. □

Definition. A *partition* of a set X is a set $P \subseteq \mathcal{P}(X)$, such that $\bigcup P = X, \emptyset \notin P$ and if $p_1, p_2 \in P$, then either $p_1 = p_2$ or $p_1 \cap p_2 = \emptyset$.

Proposition 3.9. *If E is an equivalence relation on X, then $\{[x]_E : x \in X\}$ is a partition.*

Proof. Clearly $X = \bigcup\{[x]_E : x \in X\}$; We need to show for $x, y \in X$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$. If xEy, then $[x] = [y]$ by 3.8. If $x\not{E}y$, assume $[x] \cap [y] \neq \emptyset$, let $z \in [x] \cap [y]$, but then xEz, zEy, but transitivity, xEy. Contradiction. Thus $[x] \cap [y] = \emptyset$. □

Proposition 3.10. *If P is a partition of a set X, then there exists equivalence relation E on X such that $P = \{[x]_E : x \in X\}$.*

Proof. Define xEy iff $\exists p \in P$ and $x, y \in P$. Check that E is an equivalence relation. To show $P = \{[x]_E : x \in X\}$, we prove a simple lemma first:

Lemma. Fix $p \in P$, if $x \in p$, then $[x]_E = p$.
If yEx, then $\exists p' \in P$ with $x, y \in p'$, but $p \cap p' \notin \emptyset$. Since $x \in p \cap p'$, so $p = p'$, hence $y \in P$. This shows $[x]_E \subseteq p$.

Conversely if $y \in p$, then xEy by definition of P, so $y \in [x]$. Thus also $[x]_E \supseteq p$. $\square$

Take $p \in P$, let $x \in p$ then $p \in [x]_E$ by lemma. Let $x \in X$, find $p \in P$ such that $x \in p$ and get $[x]_E = p$ by lemma again. $\square$

Form equivalence relation from any relation:

If R is a relation on X,

$$E = \text{tr}(Id \cup R \cup R^{-1})$$

is an equivalence relation.

If the relation T is symmetric, then $T \circ T$ is symmetric, since $(T \circ T)^{-1} = T^{-1} \circ T^{-1} = T \circ T$. Then $\text{tr}(T) = \bigcup_{n \in \mathbb{N}^+} T^n$ is symmetric too.

3.2 Functions and their inverses

Definition. A *function* is a binary relation $f \subseteq A \times B$ such that for any $x \in A$, $\exists! y \in B$ such that $(x, y) \in f$. Alternatively, we can also define a *function* as a triple (f, A, B) such that $f \subseteq A \times B$ is a function in the previous sense, we write $f : A \to B$, $\text{dom}(f) = A$, $\text{range}(f) = \{y \in B : \exists x \in A, f(x) = y\}$.

Definition. For $B' \subseteq B$, the *inverse image* of B' is

$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

Definition. The set of functions from A to B

$$B^A = \{f \subseteq A \times B : (f : A \to B) \text{ is a function}\}$$

If $A = n$, B^n is the set of all n-sequences of elements of B.

Definition. The *restriction* of f to $A' \subseteq A$ is

$$f \restriction A' = \{(a, b) \in A' \times B : f(a) = b\}$$

Definition. If $f : A \to A$ is a bijection and A is finite, then f is also called a *permutation*. We write $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ where $b_i = f(a_i)$.[3]

[3] The cycle notation can also be used.

Definition. If $f : A \to B,\ g : B \to C$, then their *composition* is[4]

$$gf = \{(a,c) \in A \times C : \exists b \in B, (a,b) \in f, (b,c) \in g\}$$

Definition. Given a function $f : A \to B$ and function $g : B \to A$.
g is called a *left inverse* of f if $gf = id_A$; g is called a *right inverse* of f if $fg = id_B$.

Proposition 3.11. *f is injective iff it has a left inverse.*

Proof. $\Rightarrow$ Write $B = \text{range}(f)$ and for $b \in B'$, let $a = g(b)$ be the unique element such that $f(a) = b$. Next, let $a \in A$ be arbitrary and define $g(b) = a_0$ if $b \notin B'$. Now g is well-defined on B and $gf = id_A$.
$\Leftarrow$ Suppose $gf = id_A$. If $f(a_1) = f(a_2)$ then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$, so f is injective. $\square$

Proposition 3.12. *f is surjective iff it has a right inverse.*

Proof. $\Rightarrow$ Suppose $f : X \to Y$ is surjective, for any $y \in Y, \exists x \in X$ such that $f(x) = y$, for each $y \in Y$, choose one $x \in X$ with this property and call it $g(y)$. g defined this way satisfies the requirement, $g : Y \to X,\ fg = id_Y$.
$\Leftarrow$ Suppose $fg = id_Y$. For $y \in Y$, note that $f(g(y)) = y$, so $\exists x (= g(y))$ such that $f(x) = y$ and f is surjective. $\square$

Definition. Given $f : A \to B$, we say that $g : B \to A$ is *the inverse* of f if $gf = id_A$ and $fg = id_B$.

Remark 3.13. The inverse of a function is unique. If f and g both have inverses, then so does their composition $fg,\ (fg)^{-1} = g^{-1}f^{-1}$.

Proposition 3.14. *If $f : A \to B$ is a function, the followings are equivalent:*

- *f has an inverse;*
- *f is a bijection;*
- *f^{-1} (as a relation) is a function.*

Proof. Exercise. $\square$

Proposition 3.15. *For function $f : X \to Y$ and $A, B \subseteq Y$,*

[4] It is also sometimes confusingly written as $f \circ g$ to parallel the notation used in composition of relations $R \circ S$.

- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
- $f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B)$.

For $A, B \subseteq X$,

- $f(A \cup B) = f(A) \cup f(B)$.[5]

[5] It does <u>not</u> always hold that $f(A \cap B) = f(A) \cap f(B)$ or $f(A \backslash B) = f(A) \backslash f(B)$. For instance, take $f : x \mapsto x^2$, $A = \mathbb{R}^-$, $B = \mathbb{R}^+$, then $f(A \cap B) = f(0) = 0$, but $f(A) \cap f(B) = \mathbb{R}^+ \cap \mathbb{R}^+ = \mathbb{R}^+$.

4 Cardinality

Definition. Two sets X and Y are said to be *equinumerous*, denoted $X \sim Y$, if there exists a bijection $f : X \to Y$.

Proposition 4.1. *1. For each natural number n, there does not exist an injective function*[6]

$$f : n+1 \to n$$

2. *If n and m are natural numbers and $n \sim m$, then $n = m$.*

3. *$\mathbb{N} \not\sim n$ for any natural number n.*

Proof. (1) Suppose exists such a function. Let n_0 be thee smallest such natural number. Note that $n_0 \neq 0$ because there exists no bijection from $\{\emptyset\}$ to $\emptyset$.

Let $f_0 : n_0 + 1 \to n_0$ be bijective.
Case 1: $n_0 - 1 \notin \text{range}(f_0)$. Then $f_0 \restriction n_0 : n_0 \to n_0 - 1$ is still bijective, thus contradicts the minimality of n_0.
Case 2: $n_0 - 1 \in \text{range}(f_0)$. Let i be the unique number in $n_0 + 1$ such that $f_0(i) = n_0 - 1$. Construct $g_0 : n_0 \to n_0 - 1$ as follows:

$$g_0(x) = \begin{cases} f_0(x) & \text{if } x < i \\ f_0(x+1) & \text{if } x > i \end{cases}$$

then $g_0 : n_0 \to n_0 - 1$ is a bijection, again contradicts the choice of n_0.

(2) Suppose $n \sim m$ and $n \neq m$. Say $n < m$, then $n + 1 \leq m$. Let $f : m \to n$ be a bijection, so $f \restriction n+1 : n+1 \to n$ is injective, contradicting (1).
(3) Suppose $\mathbb{N} \sim n$ for some natural number n. Let $f : \mathbb{N} \to n$ be a bijection, then $f \restriction n+1 : n+1 \to n$ is injective. his Contradicts (1) again. □

Proposition 4.2. *If X is a set, then $\sim \subseteq \mathcal{P}(X) \times \mathcal{P}(X)$ (i.e. for $a, b \in \mathcal{P}(X)$, $a \sim b$ iff there exists a bijection from a to b) is an equivalence relation.*

Lemma 4.3. *If $a < b$, $c < d$ are real numbers, then*

$$[a, b] \sim [c, d]$$

[6] Recall that from our definition, n is also a set.

Lemma 4.4. *For every set X, we have*

$$\mathcal{P}(X) \sim 2^X$$

where 2^X denotes the set of all functions from X to $\{0,1\}$.

Proof. Define $f : \mathcal{P}(X) \to 2^X$, equivalently, $f : \mathcal{P}(X) \to (X \to 2)$ as

$$f(S)(x) = \begin{cases} 0 & \text{if } x \notin S \\ 1 & \text{if } x \in S \end{cases}$$

f is clearly injective. The inverse of f is $g : 2^X \to \mathcal{P}(X)$,

$$g(t) = \{x \in X : t(x) = 1\}$$

Check that $f \circ g = id_{2^X}$, $g \circ f = id_{g(x)}$. □

Theorem 4.5. *(Cantor)*
For every set X, there is no surjection from X to $\mathcal{P}(X)$.

Proof. Suppose for the sake contradiction that $f : X \to \mathcal{P}(X)$ is a surjection. Consider

$$Y := \{x \in X : x \notin f(x)\}$$

We claim that $Y \notin \text{range}(f)$. If $Y \in \text{range}(f)$ then $Y = f(x_0)$ for some $x_0 \in X$.
If $x_0 \notin Y$ then $x_0 \in f(x_0) = Y$. But also, if $x_0 \in Y$ then $x_0 \notin f(x_0) = Y$. Contradiction, so such f does not exist. □

Corollary 4.6. *For any set X and $X_0 \subseteq X$, $\mathcal{P}(X) \nsim X_0$.*

Proof. If $g : x_0 \to \mathcal{P}(X)$ is a bijection, then let $f : X \to X_0$ be an injection, then $fg : X \to \mathcal{P}(X)$ is surjective, this contradicts Theorem 4.5. □

Corollary 4.7. *There does not exist a set of all sets.*

Proof. If X is the set containing all sets, $\mathcal{P}(X) \subseteq X$, contradicting Theorem 4.5 again. □

By Lemma 4.4, $2^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N})$, we call $2^{\mathbb{N}}$ the *Cantor set*, i.e. the set of all infinite sequence of $\{0,1\}$.

This is equivalent to the *Cantor ternary set* obtained by removing middle intervals. Each number in [0,1] can be represented uniquely as

$$\sum_{n=1}^{\infty} \frac{i_n}{3^n} : i_n \in \{0,2\}$$

. Check that there is a bijection $x^{\mathbb{N}} \to C := \{\sum_{n=}^{\infty} \frac{i_n}{3^n} : i_n \in \{0,2\}\}$ defined by

$$f(x) = \sum_{n=0}^{\infty} \frac{2x_n}{3^{n+1}} \text{ where } x \in x^{\mathbb{N}}$$

.

Definition. A *topological space* is a pair (X, T) where $T \subseteq \mathcal{P}(X)$ such that

- $\emptyset, X \in T$;
- If $T_1, T_2 \in T$ then $T_1 \cap T_2 \in T$;
- If $T_0 \subseteq T$, then $\bigcup T_0 \in T$.

Remark. The Cantor set $2^{\mathbb{N}}$ is a topological space $U \in T \iff U \subseteq 2^{\mathbb{N}}$, either $U = \emptyset$ or for every $x \in U$, there exists $n \in \mathbb{N}$ such that $\{y \in 2^{\mathbb{N}} : y \restriction n = x \restriction n\} \subseteq U$.

On the ternary Cantor set, there is a topology $U \subseteq C$, it is open if for every $x \in U$ there exists $a < b, x \in (a, b), (a, b) \subseteq U$.

Definition. A set X has cardinality *continuum* if X is equinumerous with $2^{\mathbb{N}}$.

Theorem 4.8. *(Cantor-Bernstein-Schröder Theorem, abbr. CBS)*
If X and Y are sets such that there exist injective functions $f : X \to Y$ and $g : Y \to X$, then $X \sim Y$.

Proof. TO DO □

Corollary 4.9. *If X and Y are sets such that there exist surjective functions $f : X \to Y$ and $g : Y \to X$, then $X \sim Y$.*

Proof. Since f and g are surjections, they have right inverses f', g'. Now f', g' have left inverses so they are injective. Apply CBS theorem. □

Example 4.10. Show that

$$[0, 1] \sim 2^{\mathbb{N}}$$

The function $f : 2^{\mathbb{N}} \to C \subseteq [0, 1]$ defined by

$$f(x_0, x_1, x_2, ...) = \sum_{i=1}^{\infty} \frac{2x_{i-1}}{3^i}$$

is injective. Also we can find an injective function $g : [0,1] \to 2^{\mathbb{N}}$. For any $x \in [0,1]$, choose a binary representation $x = \sum_{i=1}^{\infty} \frac{x_i}{2^i}$, then define g as

$$g(x) \to (x_0, x_1, x_2, ...)$$

By CBS Theorem 4.8, [0,1] and $2^{\mathbb{N}}$ are equinumerous.

Example 4.11. Show that

$$[0,1] \sim [0,1)$$

We define injective functions:

$$\begin{aligned} f : [0,1] &\to [0,1) \\ x &\mapsto x/2 \\ g : [0,1) &\to [0,1] \\ x &\mapsto x \end{aligned}$$

Apply CBS Theorem 4.8.

Proposition 4.12. *A set X is countable if and only if X is either empty or there exists a surjection from $\mathbb{N}$ onto X.*

Proof. The "only if" direction is straight-forward: suppose X is countable, then there it is equinumerous with $\mathbb{N}$ or is finite. Construct the surjection when $X \neq \emptyset$. For the "if" direction, $\emptyset$ is countable, assume X is infinite an let $f : \mathbb{N} to X$ be a surjection. We are going to produce another surjection $g : X \to \mathbb{N}$. By induction, choose arbitrarily $a_n \in X$ such that $a_n \notin \{a_0, a_1, ..., a_{n-1}\}$, $g(a_n) = n$. Map everything else to 0, since $\{a_0, a_1, ...\}$ may miss some elements of X. □

Proposition 4.13. *If A_n is countable for each $n \in \mathbb{N}$, then $\bigcup_{n \in \mathbb{N}} A_n$ is countable.*

Proof. (sketch)
For each $n \in \mathbb{N}$, choose surjective function $f_0 : A_n \to \mathbb{N}$, then

$$\begin{aligned} h : \mathbb{N} \times \mathbb{N} &\to \bigcup_{n \in \mathbb{N}} A_n \\ (n, m) &\mapsto f_n(m) \end{aligned}$$

is surjective. □

Proposition 4.14. *Let A, B, C be sets, then*

- *If $B \cap C = \emptyset$, then $A^{B \cup C} \sim A^B \times A^C$.*

- $(A^B)^C \sim A^{B \times C}$.

Example 4.15.

$$\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$$

Since $\mathbb{R}^{\mathbb{N}} \sim (2^{\mathbb{N}})^{\mathbb{N}} \sim 2^{\mathbb{N}\times\mathbb{N}} \sim 2^{\mathbb{N}} \sim \mathbb{R}$.

Exercise 4.16. Show that each of

$$\mathbb{Q} \times \mathbb{Q},\ \mathbb{Z} \times \mathbb{N},\ \bigcup_{n\in\mathbb{N}} \mathbb{Z}^n$$

is countable.

Show that each of

$$\mathbb{N}^{\mathbb{N}},\ \mathbb{Q} \times \mathbb{R},\ [0,1]^{\mathbb{N}}$$

is uncountable.

Here are a few more exercises (requiring much more creativity to solve!), roughly in increasing order of difficulty:[7]

Exercise 4.17. (Lázár, 1936)
For each $x \in \mathbb{R}$, associate a finite set $A(x)$. A set $I \subseteq R$ is said to be *independent* if for any $x, y \in I, x \notin A(y)$, in other words, $I \cap A(I) = \emptyset$. Show that there exists an uncountable independent set. (Hint[8])

Exercise 4.18. Can a countably infinite set contain uncountable many nested subsets? (Hint[9])

Exercise 4.19. (Putnam, 1989)
Can a countably infinite set contain uncountable many subsets whose pairwise intersections are finite? (Hint[10])

[7] These are beyond the level of this course, they are just for fun.

[8] You will need the pigeonhole principle, which basically says if you put an uncountably infinite many pigeons into a countable number of holes, some hole will contain uncountably infinite many pigeons. Now associate an interval $J(x)$ to each pigeon $x \in \mathbb{R}$, the question is, how should you choose these intervals (these are the holes)?

[9] Construct the nested subsets. Index them by real numbers.

[10] Construct sets indexed by irrational numbers; for any number, there's a sequence of rational numbers converging to it.

5 Propositional Calculus

Set of variables: $p, q, r, v_1, v_2, \ldots$;
Set of binary connectives: $\neq, \vee, \wedge, \rightarrow, \leftrightarrow$.

Definition. *Formulas* are defined on the variables recursively as follows:
Each variable v is a formula;
If φ_1 and φ_2 are formulas, then so are $\neg\varphi_1, \varphi_1 \vee \varphi_2, \varphi_1 \wedge \varphi_2, \varphi_1 \rightarrow \varphi_2, \varphi_1 \leftrightarrow \varphi_2$.

Definition. A *truth assignment* is a function $s : V \rightarrow \{0,1\}$. If $|V| = n < \infty$, then there are 2^n truth assignments.
Given a truth assignment $s : V \rightarrow \{0,1\}$, the associated *evaluation* of formula is defined as $\tilde{s} : \mathrm{Form}(V) \rightarrow \{0,1\}$, inductively as follows:

$$\begin{aligned}
\tilde{s}(v) &= s(v) \text{ if } v \in V \\
\tilde{s}(\neg\varphi) &= 1 - \tilde{s}(\varphi) \\
\tilde{s}(\varphi_1 \vee \varphi_2) &= \max(\tilde{s}(\varphi_1), \tilde{s}(\varphi_2)) \\
\tilde{s}(\varphi_1 \wedge \varphi_2) &= \min(\tilde{s}(\varphi_1), \tilde{s}(\varphi_2)) \\
\tilde{s}(\varphi_1 \rightarrow \varphi_2) &= \begin{cases} 0 & \tilde{s}(\varphi_1) > \tilde{s}(\varphi_2) \\ 1 & \tilde{s}(\varphi_1) \leq \tilde{s}(\varphi_2) \end{cases} \\
\tilde{s}(\varphi_1 \leftrightarrow \varphi_2) &= \begin{cases} 0 & \tilde{s}(\varphi_1) \neq \tilde{s}(\varphi_2) \\ 1 & \tilde{s}(\varphi_1) = \tilde{s}(\varphi_2) \end{cases}
\end{aligned}$$

Notation. We often write $\varphi[s]$ for $\tilde{s}(\varphi)$.[11]
Definition. If $|V| = n < \infty$, then for a given formula $\varphi \in \mathrm{Form}(V)$, its *truth table* is a function from the set of all 2^n truth assignments to $\{0,1\}$, $s \mapsto \varphi[x]$.

Example 5.1. $\varphi = p \vee q$

q \ p	0	1
0	0	1
1	1	1

$\varphi = (p \vee q) \vee \neg q$

[11]The reason is, $\tilde{s}(\varphi)$ as defined here, is thought as the function $\tilde{s}$ maps the formula φ to a Boolean value; In writing $\varphi[s]$, we think it has "plugging in" the value of the variables as dictated by s into φ, in the same way we evaluate a polynomial, say $1 + x + x^2|_{x \mapsto 2}$.

q \ p	0	1
0	1	1
1	1	1

$\varphi = (p \to q) \to p$

q \ p	0	1
0	0	1
1	0	1

Definition. A formula $\varphi \in \text{Form}(V)$ is a *tautology* if for every truth assignment $s : V \to \{0,1\}$, we have $\varphi[s] = 1$.[12]

Example 5.2. The followings are all tautologies:

$p \vee \neg p$	Law of excluded middle
$\neg\neg p \leftrightarrow p$	Double negation
$\neg(p \vee q) \leftrightarrow ((\neg p) \wedge (\neg q))$	De Morgan's Laws
$\neg(p \wedge q) \leftrightarrow ((\neg p) \vee (\neg q))$	
$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	Distributivity Laws
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	
$((p \wedge q) \to r) \leftrightarrow (p \to (q \to r))$	Exportation Law
$(\neg p \to p) \to p$	Clavius' Law
$((p \to q) \to p) \to p$	Pierce's Law

Definition. Two formulas φ_1 and φ_2 are *equivalent*, denoted $\varphi_1 \equiv \varphi_2$ if for every truth assignment s, we have

$$\varphi_1[s] = \varphi_2[s]$$

Note that $\varphi_1 \equiv \varphi_2$ if and only iff $\varphi_1 \leftrightarrow \varphi_2$ is a tautology.

Example 5.3. $(p \to q) \to p$ is equivalent to p.

What is special about the connectives $\neg, \wedge, \vee, \to, \leftrightarrow$?

Not much. You only need a few of them to express the others. Since

$$p \vee q \equiv \neg(\neg p \wedge \neg q),$$

[12]These can be verified by checking all truth assignments, despite being long and boring, it's unlike the validity of formulas in first-order logic which is undecidable...

we can remove $\vee$ from all formulas.
Similarly using the equivalences,

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

and

$$p \to q \equiv \neg p \vee q$$

we can write any formula in equivalent form using only $\{\neg, \vee\}$, or $\{\neg, \wedge\}$, or $\{\neg, \to\}$.

We can also form new connectives, for instance

$$p \text{ NOR } q := \neg(p \vee q)$$

Logical connectives are functions from sets of possible truth assignments to $\{0,1\}$. This leads us to...

5.1 Boolean functions

Definition. An *n-ary Boolean function* is a function from $\{0,1\}^n$ to $\{0,1\}$. Binary Boolean functions such as $\vee$, $\wedge$ are called *binary connective*; $\neg$ is *unary*.

Remark 5.4. The variables correspond to *projection function*.

$$\prod_{v_a} : \{0,1\}^V \to \{0,1\}$$

$$\prod_{v_a}(s) = s(v_a)$$

Remark 5.5. The constant functions with values 0 and 1 are treated as 0-ary Boolean function, denoted $\perp$ and $\top$.

5.2 Functional Closure

Now we define functional closure of a set of Boolean function. Crudely speaking, the functional closure is the set of all Boolean functions that can be obtained from Φ or the identity function by "composition" of union types. If you have encountered the notion of closure before, it is what you would expect; but the formal definition just look terrifying.

Definition. Given a set Φ of Boolean functions, define the following sequence of sets of Boolean functions:

$$\Phi_0 = \Phi \cup \{id, \top, \bot\}$$

For every $f_1, f_2, ..., f_k$, if

$$f_1 : \{0,1\}^{d_1} \to \{0,1\}^{c_1}$$
$$\vdots$$
$$f_k : \{0,1\}^{d_k} \to \{0,1\}^{c_k}$$

with $f_1, ..., f_k \in \Phi_n$, and $d_1, d_2, ..., d_k, c_1, c_2, ..., c_k \in \mathbb{N}$, and

$$g : \{0,1\}^{c_1+c_2+...+c_k} \to \{0,1\}^c$$

with $g \in \Phi_n$ and $c \in \mathbb{N}$;
if

$$h : \{0,1\}^d \to \{0,1\}^c$$

$d \in \mathbb{N}$ is such that $d \geq d_1 \geq \cdots \geq d_k$ and

$$h(P_1, P_2, ..., P_d) = g(f_1(P_{11}, ..., P_{1d_1}), ..., f_k(P_{k1}, ..., P_{kd_k}))$$

for some $P_* \in \{0,1\}$, then $h \in \Phi_{n+1}$.

The *functional closure* of Φ is the set

$$\bigcup_{n \in \mathbb{N}} \Phi_n$$

Example 5.6. The binary connective $\wedge$ belongs to the functional closure of $\{\vee, \neg\}$, since

$$\wedge(p, q) = \neg(\vee(\neg(p),\ \neg(q)))$$

in Polish notation.

Here,

$$\begin{aligned} \vee, \neg &\in \Phi_0 \\ (p,q) \mapsto \vee(\neg(p),\ \neg(q)) &\in \Phi_1 \\ (p,q) \mapsto \neg(\vee(\neg(p),\ \neg(q))) &\in \Phi_2 \end{aligned}$$

Definition. A set Φ of Boolean connectives is *n-functionally complete* or simply *n-complete* if every Boolean function from $\{0,1\}^n$ to $\{0,1\}$ belongs to the functional closure of Φ. A set Φ is *functionally complete* or *complete* if Φ is n-complete for every $n \in \mathbb{N}$.

Proposition 5.7. *The set $\{\neg, \vee\}$ is 1-complete and 2-complete.*

Proof. Easy check. □

Proposition 5.8. *If a set Φ of Boolean functions is 1-complete and 2-complete, then it is n-complete for each $n \in \mathbb{N}$.*

Proof. By induction on n. Base cases are given. Suppose the claim holds for n.
Let $F : \{0,1\}^{n+1} \to \{0,1\}$, define $F_0, F_1 : \{0,1\}^n \to \{0,1\}$ as follows:

$$F_0(P_1, ..., P_n) = F(P_1, ..., P_n, 0)$$

and

$$F_1(P_1, ..., P_n) = F(P_1, ..., P_n, 1)$$

F_0 and F_1 belong to the functional closure of Φ by induction hypothesis. Now F can be written as

$$F(P_1, ..., P_n, P_{n+1}) = (P_{n+1} \wedge F_1(P_1, ..., P_n)) \vee (\neg P_{n+1} \wedge F_0(P_1, ..., P_n))$$

Since $\wedge, \vee, \neg$ belong to the functional closure of $\{\neg, \vee\}$, which in turn belongs to the functional closure of Φ, this shows that Φ is $(n+1)$-complete. □

Remark 5.9. Can we find an even smaller set of complete binary connectives?

Yes! {NAND} and {NOR} are both complete. You can verify this claim by using 5.8 and checking each of {NAND} and {NOR} is 1-complete and 2-complete.[13]

Truth table for NAND:

q \ p	0	1
0	1	1
1	1	0

Truth table for NOR:

[13] NAND is also written as $\uparrow$, called "Sheffen stroke"; NOR is also written as $\downarrow$, called "Pierce's arrow". I find these names sound too mythological.

$q \backslash p$	0	1
0	1	0
1	0	0

5.3 Parsing trees

Definition. The *length* of a propositional formula is the number of symbols used in it, including parentheses.

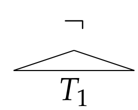
Example 5.10. $\neg((p) \wedge (q))$ has length 10.

Definition. The *parsing tree* of a formula is defined by induction as follows.

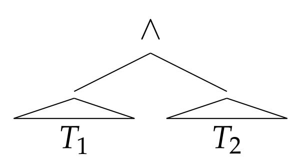
- If φ is a variable, then its parsing tree is

$$\varphi$$

- If $\varphi = \neg\varphi_1$ and the parsing tree of φ_1 is T_1, then the parsing tree of φ is

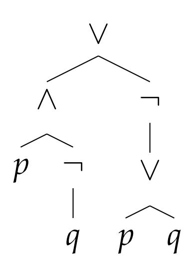


- If $\varphi = \varphi_1 \wedge \varphi_2$ and the parsing tree of φ_1 and φ_2 are respectively T_1 and T_2, then the parsing tree of φ is



  Similarly for other binary connectives.

Example 5.11. The parsing tree of $(p \wedge (\neg q)) \vee (\neg(p \vee q))$ is



5.4 Switching Circuits

5.5 Satisfiability

Definition. A set Φ of propositional formulas is *satisfiable* if there is a truth assignment s such that $\varphi[s] = 1\ \forall \varphi \in \Phi$.

Remark 5.12. If $\Phi = \{\varphi\}$, then Φ is satisfiable $\iff$ $\neg\varphi$ is not a tautology;
If $\Phi = \{\varphi_1, ..., \varphi_n\}$, then Φ is satisfiable $\iff$ $\{\varphi_1 \wedge \cdots \wedge \varphi_n\}$ is not a tautology.

Therefore the following questions are equally difficult:

- determine whether a formula is a tautology;
- determine whether a formula is satisfiable;
- determine whether a finite set of formulas is satisfiable;

Theorem 5.13. *(Compactness Theorem)* [14]
look up Given a set of propositional formulas Φ, the followings are equivalent:
• *Φ is satisfiable;*
• *Every finite subset $\Phi_0 \subset \Phi$ is satisfiable.*

Proof. We will prove that the second statement (for now, call Φ "finitely satisfiable") implies the first only for countable set of variables. Note that Form(V)= $\bigcup_{n\in\mathbb{N}} F_n$ is countable, where F_n is the set of formulas of length $\leq n$. For each n, $F_n = \bigcup_{m\in\mathbb{N}} F_n^m$, where F_n^m is the set of formulas of length $\leq n$ using only the variables $\{v_1, ..., v_m\}$, so each F_n^m is finite.

Step 1. We will produce a finitely satisfiable set $\Psi \supseteq \Phi$, such that for every $f \in \text{Form}(V)$, either $f \in \Psi$ or $\neg f \in \Psi$. We start by producing a sequence of sets Φ^n such that

- $\Phi^0 = \Phi$, the original set;
- Φ^n is finitely satisfiable;
- Either $f_n \in \Psi$ or $\neg f_n \in \Psi$ for $n > 0$.

[14] As its name suggests, this is related to topology of some space. Turns out it is equivalent to the compactness of the Stone space of the Lindenbaum-Tarski algebra 6.2. That also leads to a much shorter and elegant proof, which you can look up online.

Lemma 5.14. *If Δ is a finitely satisfiable set of formulas and $\varphi \in Form(V)$, then at least one of $\Delta \cup \{\varphi\}$ or $\Delta \cup \{\neg\varphi\}$ finitely satisfiable.*

Proof. Suppose not. Then there exist $\Delta_0 \in \Delta \cup \{\varphi\}$ and $\Delta_1 \in \Delta \cup \{\neg\varphi\}$ that are not finitely satisfiable. Note that $\varphi \in \Delta_0$ and $\neg\varphi \in \Delta_1$. then $\Delta_0 = \{\varphi, \varphi_1, \varphi_2, ..., \varphi_n\}$ and $\Delta_1 = \{\neg\varphi, \varphi_{n+1}, ..., \varphi_m\}$ where $\varphi_i \in \Delta\ \forall 1 \leq i \leq m$, and possibly $\varphi_i = \varphi_j$ for some $i \neq j$. Since $\varphi_{i=1}^{m}\{\varphi_i\} \subseteq \Delta$, there exists a truth assignment s such that $\varphi_i[s] = 1$ for all i.
If $\varphi[s] = 1$, then Δ_0 is satisfiable; if $\varphi[s] = 0$, then Δ_1 is satisfiable; □

Let $\Phi^{n+1} = \begin{cases} \Phi \cup \{f_n\} & \text{if it is finitely satisfiable} \\ \Phi \cup \{\neg f_n\} & \text{otherwise} \end{cases}$

where $\{f_1, f_2, ...\}$ is an enumeration of elements of Form(V).

Define
$$\Psi = \bigcup_{n \in \mathbb{N}} \Phi^n$$

Claim 1. Ψ is finitely satisfiable.

Proof. Every finite subset of Ψ is contained in some Φ^n. □

Claim 2. If $\varphi \vee \psi \in \Psi$ then at least one of $\varphi \in \Psi,\ \psi \in \Psi$ holds.

Proof. Suppose not, then by construction, $\neg\varphi \in \Psi,\ \neg\psi \in \Psi$. But $\{\varphi \vee \psi, \neg\varphi, \neg\psi\}$ is not satisfiable. □

Claim 3. If $\varphi \to \psi$ is a tautology and $\varphi \in \Psi$, then $\psi \in \Psi$.

Proof. If $\psi \notin \Psi$, then $\neg\psi \in \Psi$, but $\{\varphi, \neg\psi\}$ is not satisfiable. □

Step 2. Define truth assignment $s : V \to \{0, 1\}$.

$$s(v) = \begin{cases} 1 & \text{if } v \in \Psi \\ 0 & \text{if } v \notin \Psi \end{cases}$$

Claim 4. $\varphi[s] = 1 \iff \varphi \in \Psi$.

Proof. By induction on length of φ. If φ has length 1, claim holds by definition of s.
If $\varphi = \neg\psi$, easy check.
If $\varphi = \psi_1 \vee \psi_2$, and if $\varphi \in \Psi$, then by Claim 2, $\psi_1 \in \Psi$ or $\psi_2 \in \Psi$ or both. By the induction hypothesis, $\varphi[s] = \max(\psi_1[s], \psi_2[s]) = 1$; if $\varphi \notin \Psi$, then $\psi_1 \notin \Psi$ and $\psi_2 \notin \Psi$ (otherwise, $\psi_1 \to \psi_1 \vee \psi_2$ contradicts Claim 3). By the induction hypothesis, $\varphi_1[s] = \varphi_2[s] = 0$, so $\varphi[s] = 0$. □

Claim 4 shows Ψ is satisfiable. Since $\Phi \subseteq \Psi$, Φ is satisfied by the same truth assignment s, and we are done. $\square$

Definition. A formula φ is in *disjunctive normal form* (abbr. DNF) if

$$\varphi = \varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n$$

where each $\varphi_i = \varphi_i^1 \wedge \cdots \wedge \varphi_i^{m_i}$, and φ_i^j is either a variable or negation of a variable.

Definition. A formula φ is in *conjunctive normal form* (abbr. CNF) if

$$\varphi = \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n$$

where each $\varphi_i = \varphi_i^1 \vee \cdots \vee \varphi_i^{m_i}$, and φ_i^j is either a variable or negation of a variable.

Example 5.15. $p,\ p \vee q$ are in both DNF and CNF.

Theorem 5.16. *For every formula Φ, there are φ^{CNF} in CNF and φ^{DNF} in DNF such that $\varphi \equiv \varphi^{CNF} \equiv \varphi^{DNF}$;*

Proof. (Sketch)
By induction on length of φ. Base cases of length 1 (φ is a variable) and length 2 (φ the negation of a variable) hold. Since $\{\neg, \vee\}$ forms a complete set of Boolean functions, any formula φ can be expressed using the connectives $\neg, \vee$, we have two cases to consider:

Case 1. If $\varphi = \neg\psi$ for some ψ, just apply De Morgan's Law 5.2 on ψ^{CNF} or ψ^{DNF}.

Case 2. If $\varphi = \psi_1 \vee \psi_2$, then $\varphi^{DNF} = \psi_1^{DNF} \vee \psi_2^{DNF}$.

For CNF, take

$$\psi_1^{CNF} \vee \psi_2^{CNF} = (\psi_1^1 \wedge \cdots \wedge \psi_1^n) \vee (\psi_2^1 \wedge \cdots \wedge \psi_2^m) = \bigwedge_{i,j} (\psi_1^i \vee \psi_2^j)$$

where we applied the Distributivity Law 5.2 at the last step. $\square$

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, how do we find a propositional formula φ that realizes f? i.e. for any $s \in \{0,1\}^n, f(s) = 1 \iff \varphi[s] = 1$.

Answer: Use DNF form, let $s_1, s_2, ..., s_k$ be all $s \in \{0,1\}^n$ such that $\varphi(s) = 1$. For s_i, let $\varphi_i = \alpha_1^i \wedge \cdots \wedge \alpha_n^i$ where

$$\alpha_j^i = \begin{cases} v_j & \text{if } s_i(v_j) = 1 \\ \neg v_j & \text{otherwise} \end{cases}$$

Finally write $\varphi := \varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_k$.

Example 5.17. Let f be given by the table

$v_1 \backslash v_2$	0	1
... 0	0	1
1	1	1

Then we have

$$\begin{array}{ll} s_1 = (0,1) & \varphi_1 = \neg v_1 \wedge v_2 \\ s_2 = (1,0) & \varphi_2 = v_1 \wedge \neg v_2 \\ s_3 = (1,1) & \varphi_3 = v_1 \wedge v_2 \end{array}$$

so that

$$\varphi = \varphi_1 \vee \varphi_2 \vee \varphi_3 = (\neg v_1 \wedge v_2) \vee (v_1 \wedge \neg v_2) \vee (v_1 \wedge v_2)$$

6 Boolean algebra

Definition. A *Boolean algebra* is a tuple $(B, +, \cdot, -, 0, 1)$ where $+, \cdot$ are functions from B^2 to B, $-$ is a function from B to B, and $0, 1 \in B$, and $\forall a, b, c \in B$,

$$\begin{array}{lll} a \cdot (b + c) = (a \cdot b) + (a \cdot c) & a + b = b + a & a + 0 = a \\ a + (b \cdot c) = (a + b) \cdot (a + c) & a \cdot b = b \cdot a & a + 1 = 1 \\ a \cdot (b \cdot c) = (a \cdot b) \cdot c & a + (-a) = 1 & a \cdot 0 = 0 \\ a + (b + c) = (a + b) + c & a \cdot (-a) = 0 & a \cdot 1 = a \end{array}$$

Example 6.1. Given a set X, $(\mathcal{P}(X), \cup, \cap, {}^c, \emptyset, X)$, where ^{c} denotes the complement, is a Boolean algebra. Every finite Boolean algebra is a subalgebra of this type.

Example 6.2. Let V be the set of variables. Let $\equiv$ be the equivalence relation on Form(V), so $\varphi \equiv \psi$ iff $\varphi \leftrightarrow \psi$ is a tautology.
Let LT(V) = (Form$(V)/_{\equiv}, \vee, \wedge, \neg, \top, \bot$) where

$$\begin{aligned} \top &= [v_1 \vee \neg v_1]_{\equiv} \\ \bot &= [v_1 \wedge \neg v_1]_{\equiv} \\ [\varphi]_{\equiv} \vee [\psi]_{\equiv} &= [\varphi \vee \psi]_{\equiv} \\ [\varphi]_{\equiv} \wedge [\psi]_{\equiv} &= [\varphi \wedge \psi]_{\equiv} \\ \neg[\varphi]_{\equiv} &= [\neg\varphi]_{\equiv} \end{aligned}$$

This is called the *Lindenbaum-Tarski algebra*.

Theorem 6.3. *(Idempotent Law)*
If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, for $a \in B$, we have

$$a + a = a,\ a \cdot a = a$$

Proof.

$$a + a = a \cdot 1 + a \cdot 1 = a \cdot (1 + 1) = a \cdot 1 = a.$$

$$a \cdot a = (a + 0) \cdot (a + 0) = a + (0 \cdot 0) = a + 0 = a.$$

□

Remark 6.4. The Boolean algebra is *self-dual* in the sense that if an equality φ is satisfied in the Boolean algebra, then the equality φ' obtained by exchanging $+$ and $\cdot$ and exchanging 0 and 1 is also satistified.

Lemma 6.5. *(Absorption Law)*
If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, $\forall a, b \in B$,

$$a \cdot (a + b) = a, \qquad a + (a \cdot b) = a$$

Proof.
$$a \cdot (a + b) = (a + 0) \cdot (a + b) = a \cdot (0 + b) = a + 0 = a.$$
By Remark 6.4, $a + (a \cdot b) = a$ also holds. □

Lemma 6.6. *If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, for $a \in B$, $\exists! b \in B$ such that $a \cdot b = 0$, $a + b = 1$. Denote it $-a$.*

Proof. Clearly $-a$ satisfies the equations by axioms, suppose a' and a'' such that

$$a' \cdot a = a'' \cdot a = 0, \quad a' + a = a'' + a = 0,$$

then
$$a' = a' \cdot 1 = a' \cdot (a + a'') = a' \cdot a + a' \cdot a'' = 0 + a' \cdot a'' = a' \cdot a''$$
and
$$a'' = a'' \cdot 1 = a'' \cdot (a + a') = a'' \cdot a + a'' \cdot a = 0 + a'' \cdot a' = a'' \cdot a'$$
therefore $a' = a''$. □

Proposition 6.7. *If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, then $\forall a, b \in B$,*

$$-(a + b) = (-a) \cdot (-b)$$

$$-(a \cdot b) = (-a) + (-b)$$

Proof. . Using the axioms, we have

$$(a + b) + (-a) \cdot (-b) = ((a + b) + (-a)) \cdot ((a + b) + (-b)) = (1 + b) \cdot (1 + a) = 1 \cdot 1 = 1$$

$$(a + b) \cdot (-a) \cdot (-b) = (a \cdot (-a) \cdot (-b)) + (b \cdot (-a) \cdot (-b)) = (0 \cdot (-b)) + (0 \cdot (-a)) = 0 + 0 = 0$$

Now result follows from Lemma 6.6. □

Remark 6.8. If φ and ψ are propositional formulas built using $\vee, \wedge$ and $\varphi \leftrightarrow \psi$ is a tautology, then $a_\varphi = a_\psi$ is satisfied in all Boolean algebra, where a_φ, a_ψ are obtained from φ, ψ by substituting + for $\vee$, $\cdot$ for $\wedge$, $-$ for $\neg$.

Definition. A binary relation is a *partial order* if it is reflexive, antisymmetric and transitive. A partially ordered set is called a *poset*.

Definition. The Boolean algebra$(B, +, \cdot, -, 0, 1)$ has a natural partial order $\leq$ defined as

$$a \leq b \text{ if } a \cdot b = a$$

Proposition 6.9. *If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, then $\forall a, b \in B$,*

$$a \cdot b = a \iff a + b = b$$

Proof. Using the Absorption Law 6.5,
$\Rightarrow$ $\quad a + b = (a \cdot b) + b = b,$
$\Leftarrow$ $\quad a \cdot b = a \cdot (a + b) = a.$ □

Proposition 6.10. *The relation $\leq$ defined on Boolean algebra$(B, +, \cdot, -, 0, 1)$ above is indeed a partial order.*

Proof. • Reflexivity: $a \cdot a = a$ by the Idempotent Law 6.3;
• Antisymmetry: if $a \leq b, b \leq a$ then $a = a \cdot b = b \cdot a = b$;
• Transitivity: $a + b = a, b + c = b$ then $a + c = (a + b) + c = a + (b + c) = a + b = a$. □

Remark 6.11. $0 \leq a \leq 1$ for every element a in a Boolean algebra.

Definition. An element a of a Boolean algebra$(B, +, \cdot, -, 0, 1)$ is called an *atom* if $\nexists b \in B$ such that

$$b \leq a, \ b \neq 0, \ b \neq a$$

Equivalently, we can define an atom to be an element that is minimal along the nonzero elements, or alternatively, an element that *covers* 0. A *coatom* is an element covered by 1.

Definition. A Boolean algebra with no atom is said to be *atomless*.[15] A Boolean algebra in which every element is the join of atoms below it is said to be *atomic*.

Proposition 6.12. *If $(B, +, \cdot, -, 0, 1)$ is a Boolean algebra, and $a, b, c \in B$ are such that $a \leq c, b \leq c$ then $a + b \leq c$.*

Proof.

$$(a + b) \cdot c = a \cdot c + b \cdot c = a + b$$

□

[15] For instance, the Boolean algebra generated by left half-closed intervals is infinite and atomless.

Example 6.13. Atoms in LT(V)
Assume $|V| > 1$. Is $[p]_\equiv$ an atom in LT(V)? No, since $[(p \wedge q)]_\equiv \leq [p]_\equiv$ as $(p \wedge q) \wedge p = (p \wedge q)$. Extending this idea, we infer that if V is finite, say $V = \{v_1, v_2, ..., v_n\}$, then the atoms of LT($V$) are of the form $[a_1 \wedge a_2 \wedge ... \wedge a_n]_\equiv$ where a_i is either v_i or $\neg v_i$ of each $1 \leq i \leq n$.
If V is infinite, then if φ is any formula $\varphi \not\equiv \perp$, and $v \in V$ is a variable that does not appear in φ, then $[\varphi \wedge v]_\equiv \leq [\varphi]_\equiv$, so LT($V$) does not contain an atom.

Proposition 6.14. *If $(B, +, \cdot, -, 0, 1)$ is a finite Boolean algebra, then for any $b \in B, b \neq 0$, there exists an atom $a \in B$ such that $a \leq b$.*

Proposition 6.15. *If $a, b \in B, a \neq b$ are atoms, then $a \cdot b = 0$.*

Definition. Given Boolean algebras A and B, a function $f : A \to B$ is a *homomorphism* if

$$\begin{aligned} f(0_A) &= f(0_B) \\ f(1_A) &= f(1_B) \\ f(-_A a) &= -_B f(a) \\ f(a +_A b) &= f(a) +_B f(b) \\ f(a \cdot_A b) &= f(a) \cdot_B f(b) \end{aligned}$$

If f is also a bijection, then f is an *isomorphism*. We often denote $A \simeq B$.

Lemma 6.16. *If $y \in B$ and $Y := \{a \in X : a \leq y\}$, then $y = +Y := +_{a \in Y} a\}$.*

Proof. Let $Y = \{y_1, y_2, ..., y_k\}$, we want $y_1 + y_2 + \cdots + y_k = y$. Since $y_i \leq y \ \forall i$, $y_1 + y_2 + \cdots + y_k \leq y$ by 6.12. Note that $y = y \cdot (y_1 + y_2 + \cdots + y_k) + y \cdot (-(y_1 + y_2 + \cdots + y_k))$. Let $b = -(y_1 + y_2 + \cdots + y_k)$. If $b \neq 0$, let $a \leq b$ be an atom, so $a \leq b \leq y$ and $a = y_i$ for some i.
Now applying De Morgan's Law, $a = a \cdot b = y_i \cdot y \cdot (-(y_1 + y_2 + \cdots + y_k)) = y \cdot (-y_1) \cdot ... \cdot (y_i) \cdot (-y_i) \cdot ... \cdot (y_k) \leq 0$, contradicting that a is an atom. Thus $b = 0$, so $y = y \cdot (y_1 + y_2 + \cdots + y_k)$ thus $y \leq y_1 + y_2 + \cdots + y_k, y = +Y$. □

Theorem 6.17. *If $(B, +, \cdot, -, 0, 1)$ is a finite Boolean algebra, then there exists a finite set X such that B is isomorphic to $(\mathcal{P}(X), \cup, \cap, ^c, \emptyset, X)$.*[16]

[16] More generally, a Boolean algebra is isomorphic to the powerset of some set X equipped with the usual set-theoretic operations iff it is complete and atomic. This theorem says that every finite Boolean algebra is complete and atomic.

Corollary 6.18. *Any finite Boolean algebra has size* 2^n *for some* $n \in \mathbb{N}$.

Proposition 6.19. *The Lindenbaum-Tarski algebra on a countably infinite set of variables is countably infinite.*

Proof. Exercise. $\square$

7 Partially ordered sets

Recall that a binary relation is a *partial order* if it is reflexive, antisymmetric and transitive. A partially ordered set is called a *poset*.

Definition. Let $(P, \leq)$ be a poset, an element $a \in P$ is called

- *maximal* if $\nexists b \in P,\ b \neq a,\ b \geq a$;
- *minimal* if $\nexists b \in P,\ b \neq a,\ b \leq a$;
- *greatest* if $a \geq b, \forall b \in P$;
- *smallest* if $a \leq b, \forall b \in P$.

Remark.

- If a greatest (or smallest) element exists, it is unique;
- A greatest (resp. smallest) element is maximal (resp. minimal).
- Atoms are the minimal elements in $(B \backslash \{0\}, \leq)$.

Definition. Let $X \subseteq P, b \in P$ is an *upper bound* of X if $b \geq a, \forall a \in X$; b is the *supremum* (also called *join*) of X if b is the smallest upper bound of X.
Similarly, $b \in P$ is an *lower bound* of X if $b \leq a, \forall a \in X$; b is the *infimum* (also called *meet*) of X if b is the greatest upper bound of X.

Example. Consider the poset $(\mathbb{Q}, \leq)$ and $X := \{q \in \mathbb{Q} : q \leq \sqrt{2}\}$. X has an upper bound but it does not have a supremum.

Definition. A subset C of poset $(P, \leq)$ is a *chain* if $(C, \leq\restriction_{C \times C})$ is linear.

Definition. A subset A of poset $(P, \leq)$ is an *antichain* if for every distinct $x, y \in A$, we have $x \not\leq y$, i.e. x and y are incomparable. Thus any antichain can intersect any chain in at most one element.

Example.

- $(\mathbb{R}, \leq)$ is a linear order, thus any subset of $\mathbb{R}$ is a chain.
- $(P(X), \subseteq)$ is not a linear order if $|X| \geq 2$.

- $\{\emptyset, \{1\}, \{1,2\}\}$ is a chain in $P(\{1,2\})$.
- $\{\{1\}, \{2,3\}, \{2,4\}\}$ is an antichain in $P(\{1,2,3,4\})$.[17]

Definition. Given a poset $(P, \leq)$, the *width* of $(P, \leq)$ is the maximum number of elements in an antichain of P.

Theorem 7.1. *(Dilworth)*
If $(P, \leq)$ is a finite poset of width w, then there exist chains $C_1, C_2, ..., C_w$ such that $P = \sqcup_{i=1}^{w} C_i$.

Proof. By induction on the size of P. Base case $|P| = 0$ or 1 trivial.
Induction step, assume claim holds for $|P| < n$. Let $(P, \leq)$ be a poset of size n. Let $a \in P$ be maximal. Let k denote the width of $P' := P \backslash \{a\}$, so there are disjoint chains $C_1, C_2, ..., C_k$ covering P'. For each $i \leq k$, let x_i be the maximal element in C_i that belongs to an antichain of size k.
Claim that $\{x_1, x_2, ..., x_k\}$ is an antichain. Suppose on the contrary $x_i \leq x_j$. Let A_j be an antichain of size k in P' such that $x_j \in A_j$. Let $y \in A_j \cap C_i$, so $y \leq x_i$ by the choice of x_i. By transitivity, $y \leq x_i \leq x_j$, then y and x_j are distinct comparable elements in A_j, contradicting A_j is an antichain.

Case 1: a is not comparable with any x_i; then $\{a, x_1, ..., x_k\}$ is an antichain and $P = \{a\} \sqcup C_1 \sqcup \cdots \sqcup C_k$, so width of P is $k+1$.
Case 2: a is comparable with any x_i, so $x_i \leq a$. Let $C = \{a\} \sqcup \{y \in C_i : y \leq x_i\}$. Consider $P'' := P \backslash C$, P'' cannot contain an antichain of size k because x_i was the greatest element of C_i that belongs to an antichain of size k, so the width of P'' is $k-1$. Let $C'_1, ..., C'_{k-1}$ be disjoint chains covering P''. Then $P = C \sqcup C'_1 \sqcup \cdots \sqcup C'_{k-1}$ and the width of P is k.

□

Definition. Given a poset $(P, \leq)$, the *height* of $(P, \leq)$ is the maximum number of elements in a chain of P.

Theorem 7.2. *(Mirsky)*[18]
The height of a finite poset $(P, \leq)$ equals the smallest number of antichains into which P can be partitioned.

Proof. For any element x, consider the chains having x as their greatest element. Let $N(x)$ denote the size of the largest of these chains. Then each set $N^{-1}(i)$is an antichain,

[17] The largest antichain in $(P(X), \subseteq)$ is the largest Sperner family, which has size $\binom{|X|}{[|X|/2]}$

[18] The dual of Dilworth's theorem. Not covered in this course.

and they partition P into a number of antichains equal to the size of the largest chain. $\square$

7.1 Lattices and Zorn's Lemma

Definition. A poset $(L, \leq)$ is called a *lattice* if every finite subset of L has a supremum and an infimum. Equivalently, $(L, \leq)$ is a *lattice* if every two-element subset has a supremum and an infimum.

Example. Every linearly ordered set is a lattice.

Example. Every Boolean algebra is a lattice, since $\sup(a, b) = a + b$.

Non-Example. $(\{\{1\}, \{2\}\}, \subseteq)$ is not a lattice.

Definition. A poset $(L, \leq)$ is called a *complete lattice* if every subset of L has a supremum.

Example. $(\mathbb{R}, \leq)$ and $([0, 1), \leq)$ are complete lattices.

Claim 7.3. *Let $(P, \leq)$ be a poset. The followings are equivalent:*

- *$(P, \leq)$ is a complete lattice;*
- *Every subset of P has an infimum;*
- *Every subset of P has a supremum and an infimum.*

Proof. $2 \Rightarrow 1$. Let $X \subseteq P$, consider $Y = \{p \in P : p \text{ is an upper bound of } X\}$, then $\inf Y = \sup X$.
$1 \Rightarrow 3$. Analogous.
$3 \Rightarrow 2$. Trivial. $\square$

Theorem 7.4. *(Knaster-Tarski)*
If $(L, \leq)$ is a complete lattice and $f : L \to L$ is order-preserving, i.e. $x \leq y \Rightarrow f(x) \leq f(y)$, then f has a fixed point. [19]

Proof. Let $X = \{x \in L : f(x) \leq x\}$. Let $x_0 = \inf X$, thus $x_0 \leq x \ \forall x \in X$. Then by monotonicity of f and definition of X, $f(x_0) \leq f(x) \leq x$, so $f(x_0)$ is a lower bound of X and $f(x_0) \leq x_0$. Applying f once again, we obtain $f(f(x_0)) \leq f(x_0)$, thus $f(x_0) \in X$. Also $x_0 \leq f(x_0)$ by definition of x_0. Thus $f(x_0) = x_0$, i.e. x_0 is a fixed point of f. $\square$

[19] The set of fixed points of f is also a complete lattice

Lemma 7.5. *Let $(P, \leq)$ be a poset such that every chain in P has a supremum, and let $f : P \to P$ be such that for every $x \in P, x \leq f(x)$*[20]*, then f has a fixed point.*

Proof. First note that $\emptyset$ is a chain and $\sup \emptyset$ is the smallest element of P. Call it a. Define $\mathscr{A} = \{A \subseteq P : a \in A, x \in A \Rightarrow f(x) \in A, \text{chain } L \subseteq A \Rightarrow \sup L \in A\}$.
Now we show through the series of claims that $A_0 = \bigcap \mathscr{A}$ is a chain and $A_0 \in \mathscr{A}$. Then take any element $x \in A_0$, the chain $x \leq f(x) \leq f(f(x)) \leq ...$ has a supremum in A_0. This supremum is a fixed point of f.

Claim 1: $A_0 \in \mathscr{A}$.

Proof. Clearly $a \in A_0$. If $x \in A_0, x \in A \ \forall A \in \mathscr{A}$, so $f(x) \in A$, thus $f(x) \in A_0$. Similarly, if the chain $L \subseteq A_0$, then $L \subseteq A \ \forall A$, so $\sup L \in A \ \forall A$, thus $\sup L \in A_0$. The set A_0 satisfies the three criteria, thus $A_0 \in \mathscr{A}$. $\square$

Claim 2: A_0 is a chain.

Proof. Consider $B = \{x \in A_0 : (y < x, \ y \in A_0) \Rightarrow f(y) \leq x\}$. For $x \in B$, let $B_x = \{z \in A_0 : z \leq z \text{ or } f(x) \leq z\}$. If we show that $A_0 = B = B_x$ for every $x \in A$, then A_0 is a chain, since if $x, y \in A_0$, then either $y \leq x$ or $x \leq f(x) \leq y$, thus x and y are comparable. $\square$

Claim 3: If $x \in B$, then $B_x \in \mathscr{A}$. Consequently, $A_0 = B_x$ for every $x \in A_0$.

Proof. Clearly $a_0 \in B_x$.
Suppose $z \in B_x$, we want $f(x) \in B_x$. Case 1, $z \leq x$, then either (z = x, so $f(z) = f(x) \in B_x$) or ($z < x$, then $f(z) \leq x \in B$, thus again $f(z) \in B_x$). Case 2, $f(x) < z$, but also $z \leq f(z)$, so $f(x) \leq f(z)$.
Suppose $L \subseteq B_x$ is a chain. If every $l \in L$ is such that $l \leq x, \sup L \leq x$, then $\sup L \in B_x$. if for some $l \in L$, $f(x) \leq l \leq \sup L$, then clearly $L \in B_x$.
Since $B_x \subseteq A_0$ and $A_0 := \bigcap \mathscr{A}$, we have $A_0 = B_x$. $\square$

Claim 4: $B \in \mathscr{A}$. Thus $B = A_0$.

Proof. Clearly $a_0 \in B$.
Suppose $x \in B$, i.e. $y < x, \Rightarrow f(y) \leq x\}$. If $y < f(x)$, then $y \leq x$ by Claim 3, thus $f(y) \leq x \leq f(x)$. If $y = x$, then $f(y) \leq f(x)$, so $x \in B \Rightarrow f(x) \in B$, i.e. B is closed under function application.
Now take any chain $L \subseteq B$. Let $y < \sup L$, then $\exists l \in L$ such that $l \nleq y$, so $y < l$ since by Claim 3, $A_0 = B_l$. Since $l \in B, f(y) \leq l \leq \sup L$, this shows $\sup L \in B$.
Thus $B \in \mathscr{A}$, and $B = A_0$. $\square$

[20]Such f is said to be *progressive*

□

Axiom of Choice (abbr. AC)
If X is a nonempty family of sets such that $\emptyset \notin X$ then $\exists f : X \to \bigcup X$ such that for every $a \in X, f(a) \in a$.

Lemma 7.6. *If $(P, \leq)$ be a poset such that every chain in P has an supremum, then P has a maximal element.*

Proof. Suppose not. For each $x \in P$, define $A_x = \{y \in P : y > x\}$. Using AC, we have a function $f : P \to P, f(x) \in A_x$, thus $x \leq f(x)$. By Lemma 7.5, f has a fixed point, contradicting absence of a maximal element. □

Theorem 7.7. *(Hausdorff maximal principle)*
For any poset $(P, \leq)$, there exists a maximal chain in P.

Proof. Consider $S := (\{C \subseteq P : C \text{ is a chain}\}, \subseteq)$. We will show any chain in S has a supremum.
Let $\mathcal{C}$ be a chain in S, we have $\bigcup \mathcal{C} \subseteq P$. Take arbitrary $x, y \in \bigcup \mathcal{C}$, then $\exists C_1, C_2 \in \mathcal{C}$ such that $x \in C_1$, $y \in C_2$. Since $\mathcal{C}$ is a chain, C_1 and C_2 are comparable. Wlog, assume $C_1 \subseteq C_2$, then $x, y \in C_2$; since C_2 is a chain, x, y are comparable. Therefore $\bigcup \mathcal{C}$ is a chain, and $\bigcup \mathcal{C} = \sup \mathcal{C} \in S$. By Lemma 7.6, S has a maximal element, which corresponds to a maximal chain in P. □

Theorem 7.8. *(Kuratowski-Zorn Lemma)*[21]
If $(P, \leq)$ is a poset such that every chain in P has an upper bound, then P has a maximal element.

Proof. Let $C \subseteq P$ be a maximal chain, its existence is guaranteed by 7.7. Let b be an upper bound of C. Note that $b \in C$ since otherwise $C \cup \{b\}$ would be a larger chain. If $\exists c$ such that $c > b$, then again $C \cup \{c\}$ would be a larger chain, contradicting maximality of C. Therefore b is a maximal element in P. □

Corollary 7.9. *For any poset $(P, \leq)$, there exists a linear order $\preccurlyeq$ on P that extends $\leq$, i.e. $(\leq \subseteq \preccurlyeq \subseteq P)$.*

Proof. Consider $S := (\{R \subseteq P \times P : R \text{ is a poset and } \leq \subseteq R\}, \subseteq)$.

Claim 1: Any chain $\mathcal{C}$ in S has an upper bound in S.

[21] What's sour, yellow, and equivalent to the Axiom of Choice? Zorn's lemon.

Proof. We will show that $\bigcup \mathcal{C}$ is a poset containing $\leq$. Assume $\bigcup \mathcal{C} \neq \emptyset$, otherwise $\leq$ is an upper bound. Clearly, $\bigcup \mathcal{C}$ contains $\leq$ since any element of $\mathcal{C}$ contains $\leq$. Showing $\bigcup \mathcal{C}$ is a poset is just a routine check:

- $\bigcup \mathcal{C}$ is reflexive since each $R \in \mathcal{C}$ was;
- If x is related to y, and y is related to x in $\bigcup \mathcal{C}$, then x is related to y in R_1, and y is related to x in R_2 for some $R_1, R_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, wlog, $R_1 \subseteq R_2$, thus $x = y$ by antisymmetry property of R_2, thus $\bigcup \mathcal{C}$ is also antisymmetric;
- If x is related to y, and y is related to z in $\bigcup \mathcal{C}$, then x is related to y in R_1 and y is related to x in R_2 for some $R_1, R_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, wlog, $R_1 \subseteq R_2$, so by transitivity of R_2, x is related to z in R_2, thus x is related to z in $\bigcup \mathcal{C}$.

Therefore $\bigcup \mathcal{C} \in S$ and it is an upper bound of $\mathcal{C}$[22]. $\square$

Claim 2: A maximal element in S is a linear order.

Proof. Suppose R is a poset in P which is not linear, so $\exists x, y \in P$ such that $x \not R y, y \not R x$. Let $R' = R \cup \{(a, b) : aRx, yRb\}$[23]. By this construction, $xR'y$ but $x \not R y$, so $R \subsetneq R'$, i.e. R is not maximal; i.e. a maximal element in S has to be a linear order. $\square$

By Kuratowski-Zorn Lemma 7.8 and Claim 1, S has a maximal element; by Claim 2, this maximal element is a linear order. $\square$

Definition. A poset $(P, \leq)$ is *well-founded* if every non-empty set of P has a minimal element.

Definition. A poset $(P, \leq)$ is a *well-order* if it is well-founded and linear.

Example. $\mathbb{N}$ is well-ordered. $(\mathbb{N} \cup \{\omega\}, \leq \cup \{(n, \omega) : n \in \mathbb{N}\})$ is also well-ordered.

Example. Any finite linear order is well-ordered.

Non-Example. $(\mathbb{Q}, \leq)$ and $(\mathbb{R}_+, \leq)$ are not well-ordered.

Theorem 7.10. *(Well-ordering theorem)*
Assuming the Axiom of Choice, for any set X, there exists a well-order on X.

---

[22] In fact, $\bigcup \mathcal{C} = \sup \mathcal{C}$, just as in 7.7.

[23] Again, one should check that R' is indeed a poset. Note that $\{a \in P : aRx\} \cap \{b \in P : yRb\} = \emptyset$.

Definition. A poset $(T, \leq)$ is a *tree* if $|T| \geq 1$ and for every $t \in T$, $\{s \in T : s \leq t\}$ is well-ordered by $\leq$.

Definition. Given a tree $(T, \leq)$ and $t \in T$, we say that $t' \in T$ is an *immediate successor* of t if $t \leq t', t \neq t'$ (for simplicity, we also write $t < t'$) and t' is minimal in $\{s \in T : t \leq s\}$.

Lemma 7.11. *If $(T, \leq)$ is a tree, then for every $t \in T$, either $\{s \in T : t < s\}$ is empty or there exists an immediate successor of t.*

Proof. Suppose $\{s \in T : t < s\}$ is non-empty. Choose any $t'' \in T$ such that $t < t''$. Look at the set $A := \{s \in T : t < s \leq t''\}$. This is a subset of $\{s \in T : s \leq t''\}$, hence there is a minimal element of A, this element is an immediate successor of t'. □

Definition. Given a tree $(T, \leq)$, an *infinite branch* in T is a sequence $(t_0, t_1, t_2...)$ such that t_0 is the least element of T, and t_{i+1} is an immediate successor of t_i for all $i \leq 0$.

Definition. A tree $(T, \leq)$ is *finitely branching* if for every $t \in T$, the set of immediate successors of t is finite.

Theorem 7.12. *(König's Lemma)*
If $(T, \leq)$ is an infinite finitely branching tree, then there exists an infinite branch in T.

Proof. By construction. Let $T =: T_0$ be infinite and finitely branching, and let t_0 be the least element of T. Inductively choose $t_n \in T$, such that t_{n+1} is an immediate successor of t_n and the set $T_{n+1} := \{t \in T_n : t_{n+1} \leq t\}$ is infinite. □

8 Propositional Calculus, revisited

Given a propositional formula $\varphi \in \mathrm{Form}(V)$, we write

$$\vDash \varphi$$

if φ is a tautology.

More generally, given a set Γ of formulas, write[24]

$$\Gamma \vDash \varphi$$

if for every truth assignment s, $\gamma[s] = 1$ for every $\gamma \in \Gamma$ implies $\varphi[s] = 1$.

8.1 Syntactical deduction

Definition. A *deduction system* for propositional logic consists of

- a set A of propositional formulas, called *axioms*;
- a set of finite sequences $(\varphi_1, ..., \varphi_n, \varphi_{n+1})$, written $\dfrac{\varphi_1, ..., \varphi_n}{\varphi_{n+1}}$, called *deduction rules*.

We will consider deduction system for propositional logic where all the deduction rules are of the form, $\dfrac{\varphi \qquad \varphi \to \psi}{\psi}$, called *modus ponens*.

In this section, we will use only the connectives $\{\neg, \to\}$, since this set is functionally complete, there is no compelling reason to use more.

Definition. A *formal proof* or *inference* in a deduction system D from the set of formulas Γ is a sequence of formulas $\varphi_1, \varphi_2, ..., \varphi_n$ such that for each $i \leq n$, either

- φ_i is an axiom of D;
- $\varphi_i \in \Gamma$;
- there are $i_1, i_2, ..., i_k < i$ such that $\dfrac{\varphi_{i_1}, ..., \varphi_{i_k}}{\varphi_i}$ is a deduction rule.

[24] read "Γ semantically entails φ" or "Γ tautologically implies φ"

Definition. We write $\Gamma \vdash_D \varphi$ [25] if there exists a proof $\varphi_1, ..., \varphi_n$ in D from Γ such that $\varphi_n = \varphi$.

Definition. A deduction system D for propositional logic is *sound* if for every formula φ and set of formulas Γ, $\Gamma \vdash_D \varphi \Rightarrow \Gamma \vDash \varphi$. [26]

Proposition 8.1. *If D is a deduction system with only modus ponens as inference rule, then D is sound iff all axioms are tautologies.*

Proof. Suppose D is sound. Clearly $\vdash_D \varphi$ for every axiom φ, then $\vDash \varphi$ by soundness, meaning φ is a tautology.
For the reverse direction, let all axioms be tautologies. Suppose $\Gamma \vdash_D \varphi$, let $\varphi_1, \varphi_2, ..., \varphi_n$ be a proof of φ . We show by induction on i, where $1 \leq i \leq n$, that $\Gamma \vDash \varphi_i$.
Base case, φ_1 must be an axiom of Γ, so $\Gamma \vDash \varphi_1$. For the induction step, suppose $\Gamma \vDash \varphi_j \ \forall j < i$. If φ_i is an axiom, then we are done; otherwise there exist $j, k < i$ such that $\varphi_k = (\varphi_j \to \varphi_i)$, i.e. φ_i is obtained from φ_j and φ_k by modus ponens. By the induction hypothesis, $\Gamma \vDash \varphi_j$ and $\Gamma \vDash \varphi_k$, so we let s be any truth assignment with $\gamma[s] = 1 \ \forall \gamma \in \Gamma$, then $\varphi_j[s] = 1$ and $(\varphi_j \to \varphi_i)[s] = 1$, so we get $\varphi_i[s] = 1$, which means $\Gamma \vDash \varphi_i$. Therefore $\Gamma \vDash \varphi_n$, and D is sound. □

Definition. A deduction system D for propositional logic is *complete* if for every formula φ and set of formulas Γ, $\Gamma \vdash_D \varphi \Leftrightarrow \Gamma \vDash \varphi$

8.2 Completeness of deduction system D_0

Now we will state a few simple lemmas and use them to show that an example deduction system 8.6 is complete.

Lemma 8.2. *A concatenation of two formal proofs is a formal proof.*

Lemma 8.3. *If $\varphi_1, \varphi_2, ..., \varphi_n$ is a formal proof and $i < n$, then $\varphi_1, \varphi_2, ..., \varphi_i$ is a formal proof.*

Lemma 8.4. *If $\Gamma \subseteq \Gamma'$ and $\Gamma \vdash \varphi$, then $\Gamma' \vdash \varphi$.*

Lemma 8.5. *If $\Gamma \vdash \varphi$, then there exists a finite $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \vdash \varphi$.*[27]

---

[25] read "Γ syntactically entails φ" or "Γ entails φ" or "Γ proves φ"

[26] If a deduction system is not sound, then one can prove false statements - so such a deduction system would be worthless.

[27] Compare this lemma with the Compactness theorem 5.13.

Example 8.6. Consider the deduction system D_0 with only modus ponens as inference rule and the following axioms[28]:

(A1) $\varphi \to (\psi \to \varphi)$

(A2) $\varphi \to (\psi \to \chi) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

(A3) $(\neg\varphi \to \psi) \to ((\neg\varphi \to \neg\psi) \to \varphi)$

(A3′) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$

The axioms A3 and A3′ are equivalent. For simplicity, we write $\Gamma \vdash \varphi$ for $\Gamma \vdash_{D_0} \varphi$.

Theorem 8.7. *D_0 is complete.*

Lemma 8.8. *In D_0, $\vdash \varphi \to \varphi$ for every φ.*

Proof. From A1, $\varphi \to (\varphi \to \varphi)$;
From A1, $\varphi \to ((\varphi \to \varphi) \to \varphi)$;
From A2, $\varphi \to ((\varphi \to \varphi) \to \varphi) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$;
By modus ponens, $(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$;
By modus ponens again, $\varphi \to \varphi$. □

Lemma 8.9. *In D_0, $\{\varphi\} \vdash \psi \to \varphi$ for every φ and ψ.*

Proof. From $\{\varphi\}$, we have φ;
From A1, we have $\varphi \to (\psi \to \varphi)$;
By modus ponens, $\psi \to \varphi$ as desired. □

Theorem 8.10. *(Deduction Theorem)*
If Γ is a set of formulas and φ, ψ are formulas, then

$$\Gamma \cup \{\varphi\} \vdash \psi \iff \Gamma \vdash \varphi \to \psi$$

Proof. $\Leftarrow$ If $\varphi_1, \varphi_2, ..., \varphi_n$ is a formal proof from Γ of $\varphi_n = (\varphi \to \psi)$, then $\varphi_1, \varphi_2, ..., \varphi_n, \varphi, \psi$ is a formal proof from $\Gamma \cup \{\varphi\}$ of ψ.

$\Rightarrow$ Suppose $\Gamma \vdash \varphi \to \psi$, let $\varphi_1, \varphi_2, ..., \varphi_n$ be a proof of ψ from $\Gamma \cup \{\varphi\}$. By induction on $i \leq n$, we show that $\Gamma \vdash \varphi \to \varphi_i$. Base case, by Lemma 8.9, $\{\varphi_1\} \vdash \varphi \to \varphi_1$, since φ_1 is either an axiom or an element of Γ, $\Gamma \vdash \varphi \to \varphi_1$ by Lemma 8.4.

[28]Check that all these axioms are tautologies

Now suppose $\Gamma \vdash \varphi \to \varphi_j$ for all $j < i$. If φ_i is an axiom or element of Γ, then we are done. Otherwise φ_i is obtained by modus ponens from φ_j, $\varphi_k = (\varphi_j \to \varphi_i)$, where $j, k < i$, and by induction hypothesis, $\Gamma \vdash \varphi \to \varphi_j$ and $\Gamma \vdash \varphi \to (\varphi_j \to \varphi_i)$. By A2, we have $\varphi \to (\varphi_j \to \varphi_i) \to ((\varphi \to \varphi_j) \to (\varphi \to \varphi_i)) =: \chi$. Now if P_1 is a proof of $\varphi \to \varphi_j$ from Γ, and P_2 is a proof of $\varphi \to (\varphi_j \to \varphi_i)$ from Γ, then $P_1, P_2, \chi, (\varphi \to \varphi_j) \to (\varphi \to \varphi_i)$, $\varphi \to \varphi_i$ is a proof of φ_i from Γ, thus $\Gamma \vdash \varphi \to \varphi_i$. $\square$

Lemma 8.11. *For every φ, ψ,*

$$\{\varphi, \neg\varphi\} \vdash \psi \text{ and } \{\neg\varphi\} \vdash \varphi \to \psi.$$

Proof. From the set of formulas $\{\varphi, \neg\varphi\}$, we have $\neg\psi \to \varphi$, since by Lemma 8.9 $\{\varphi\} \vdash \psi \to \varphi$. Similarly we have $\neg\psi \to \neg\varphi$, again by Lemma 8.9.
From A3, $(\neg\psi \to \varphi) \to ((\neg\psi \to \neg\varphi) \to \psi)$; by modus ponens, $(\neg\psi \to \neg\varphi) \to \psi$; applying modus ponens agains, we get ψ. The second statement in this Lemma follows from Theorem 8.10. $\square$

Definition. A set of formulas Γ is *consistent* if $\exists\psi$ such that $\Gamma \nvdash \psi$.
A set of formulas Γ is *inconsistent* if $\forall\psi$, $\Gamma \vdash \psi$.

Lemma 8.12. *If Γ is inconsistent, then there exists a finite $\Gamma_0 \subseteq \Gamma$ which is inconsistent.*

Proof. Fix Γ and φ. Since Γ is inconsistent, $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$. By Lemma 8.5, there exists finite $\Gamma_0, \Gamma_1 \subseteq \Gamma$ such that $\Gamma_0 \vdash \varphi$ and $\Gamma_1 \vdash \neg\varphi$.
Since $\Gamma_0 \cup \Gamma_1 \vdash \varphi$ and $\Gamma_0 \cup \Gamma_1 \vdash \neg\varphi$, by Lemma 8.4 and Lemma 8.11, $\{\varphi, \neg\varphi\} \vdash \psi$, thus $\Gamma_0 \cup \Gamma_1 \vdash \psi$. Therefore $\Gamma_0 \cup \Gamma_1$ is an inconsistent finite subset of Γ. $\square$

Lemma 8.13. *If $\Gamma \cup \{\neg\varphi\}$ is inconsistent, then $\Gamma \vdash \varphi$.*
If Γ is consistent, then at least one of $\Gamma \cup \{\varphi\}$ or $\Gamma \cup \{\neg\varphi\}$ is consistent.

Proof.

$\Gamma \cup \{\neg\varphi\} \vdash \neg(\varphi \to \varphi)$	using A3'
$\Gamma \vdash \neg\varphi \to \neg(\varphi \to \varphi)$	by Deduction Theorem 8.10
$(\neg\varphi \to \neg(\varphi \to \varphi)) \to ((\varphi \to \varphi) \to \varphi)$	using A3'
$\Gamma \vdash ((\varphi \to \varphi) \to \varphi)$	by modus ponens
$\vdash \varphi \to \varphi$	by Lemma 8.8
$\Gamma \vdash \varphi$	by modus ponens

If $\Gamma \cup \{\neg\varphi\}$ is inconsistent, then $\Gamma \vdash \varphi$, so $\Gamma \cup \{\varphi\}$ is consistent. $\square$

Lemma 8.14. *If Γ is consistent, then there exists a consistent set Δ such that $\Gamma \subseteq \Delta$ and for every formula φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$.*

Proof. Consider the set $P := \{S \subseteq \text{Form}(V) : S \text{is consistent and } \Gamma \subseteq S\}$. Consider the relation of inclusion $\subseteq$ on P so $(P, \subseteq)$ is a poset.

Claim 1: if $\Delta \in P$ is a maximal element, then for every φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$.

Proof. If $\Delta \cup \{\neg\varphi\}$ is consistent, then $\Delta \cup \{\neg\varphi\} \in P$, so $\Delta \cup \{\neg\varphi\} = \Delta$ by the maximality of Δ, hence $\neg\varphi \in \Delta$. If $\Delta \cup \{\neg\varphi\}$ is inconsistent, by Lemma 8.13, $\Delta \vdash \varphi$, so $\Delta \cup \{\varphi\}$ is consistent, thus $\varphi \in \Delta$. $\square$

Now use Zorn's Lemma 7.8 to show that P contains a maximal element.

Claim 2: Every chain C has an upper bound in P.

Proof. Suppose $C \neq$, otherwise Γ is an upper bound. Clearly $\bigcup C$ contains Γ and s for every $s \in C$. If $\bigcup C$ is not consistent, then $\bigcup C \vdash \psi$ and $\bigcup C \vdash \neg\psi$ for some ψ. By 8.12, there exists a finite $T \subseteq \bigcup C$ so that $T \vdash \psi$ and $T \vdash \neg\psi$. Then there exists $c_1, c_2, ..., c_n \in C$ such that $T \subseteq c_1 \cup c_2 \cup ... \cup c_n$. Since C is a chain, without loss of generality c_n is the greatest among $c_1, c_2, ..., c_n$. So $c_n \vdash \psi$ and $c_n \vdash \neg\psi$, contradicting $c_n \in P$. Therefore $\bigcup C$ is an upper bound of C. $\square$

$\square$

Theorem 8.15. *(Completeness Theorem)*

- Γ *is satisfiable* $\iff$ Γ *is consistent.*
- $\Gamma \vdash \varphi \iff \Gamma \vDash \varphi$.

Proof. The "only if" direction follows from soundness 8.1. For the "if" direction, suppose Γ is consistent. We construct a truth assignment satisfying all formulas of Γ. By lemma 8.14, there exists a consistent set $\Delta \supseteq \Gamma$ and for every φ either $\varphi \in \Delta$ or $\neg\varphi \in \Delta$.

Let $s(v) = \begin{cases} 1 & \text{if } v \in \Delta \\ 0 & \text{if } v \notin \Delta \end{cases}$

We claim that s satisfies all formulas in Δ. By induction on the length of formula φ that

$$\varphi[s] = 1 \text{ if } \varphi \in \Delta \quad \text{and} \quad \varphi[s] = 0 \text{ if } \varphi \notin \Delta.$$

Base case trivial.

- If $\varphi = \neg\psi$ for some ψ, then claim follows from assumption on ψ.
- Say $\varphi = \psi \to \chi$.
  - If $\varphi[s] = 0$, then $\psi[s] = 1$ and $\chi[s] = 0$. So by induction hypothesis $\psi \in \Delta$ and $\chi \notin \Delta$. If $\varphi \in \Delta$ then by modus ponens $\chi \in \Delta$, contradiction. Thus $\varphi \notin \Delta$ as desired.
  - If $\varphi[s] = 1$, then $\psi[s] = 0$ and $\chi[s] = 1$. In the first case, $\psi \notin \Delta$, so $\neg\psi \in \Delta$; by Lemma 8.11, $\neg\psi \vdash \psi \to \chi$, so $\varphi = \psi \to \chi \in \Delta$. In the second case, $\chi \in \Delta$. By Lemma 8.8, $\chi \vdash \psi \to \chi$, so again $\varphi = \psi \to \chi \in \Delta$.

  Therefore s satisfies all formulas in Δ.

For the second claim, suppose for a contradiction that $\Gamma \nvdash \varphi$, then $\Gamma \cup \{\neg\varphi\}$ is consistent by Lemma 8.13, which means $\Gamma \cup \{\neg\varphi\}$ is satisfiable by the first claim, thus there exists a truth assignment s satisfying $\Gamma \cup \{\neg\varphi\}$, implying $\Gamma \nvDash \varphi$. $\square$

9 First-order logic

9.1 Languages and models

Definition. A *model* or *structure* is a tuple $M = (A, f_1, ..., f_k, P_1, ..., P_n, C_1, ..., C_l)$ where A is a nonempty set, called the *universe* of M, sometimes denoted $\|M\|$ and

- each f_i is a function such that $f_i : A_i^{r_i} \to A$ for some $r_i > 0$;
- each P_i is a relation such that $P_i \subseteq A_i^{s_i}$ for some $s_i > 0$;
- each C_i is an element of A known as a constant.

If $n = 0$, i.e. there are no relations, then M is called an *algebraic structure*.
If $k = 0$, i.e. there are no functions, then M is called an *relational structure*.

Example 9.1. For any nonempty set A, $(A, \in)$ is a structure with one binary relation $\in$, namely the set-theoretic inclusion relation.

Example 9.2. A poset $(P, \leq)$ is a relational structure.

Example 9.3. A Boolean algebra $(B, +, \cdot, {}^c, 0, 1)$ is an algebraic structure, where $+, \cdot, {}^c$ are the functions and 0, 1 are the constants.

How to talk about models:

Definition. A *language* is a tuple $L = (f_1, ..., f_k, P_1, ..., P_n, C_1, ..., C_l)$, where each f_i, P_i, C_i is called a symbol of the language, equipped with an *arity* function $a : \{f_1, ..., f_k, P_1, ..., P_n\} \to \mathbb{N}^+$.[29]

Definition. Given a model $M = (A, f_1, ..., f_k, P_1, ..., P_n, C_1, ..., C_l)$ and a language $L = (f_1, ..., f_{k'}, P_1, ..., P_{n'}, C_1, ..., C_{l'})$, we say that M is an *L-structure/model for L* if $k = k', n = n', l = l'$ and each $f_i : A^{a(f_i)} \to A$ and each $P_i \subseteq A^{a(P_i)}$.

Example 9.4. Let $L = \{R\}$ where R is a binary relation symbol, then $(P, \leq)$ and $(A, \in)$ are L-structures.

To speak language L, we need

[29] A function or relation of arity n is said to be *n-ary*. Unary is the common name for 1-ary, and binary is the common name for 2-ary, because they sound much better.

- symbols of the language
- logical symbols
  - connectives $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$
  - quantifiers $\exists, \forall$
- auxiliary symbols
  - parentheses
  - commas
- variables $x, y, z, ...$
- equality symbol $=$

Definition. *Terms* are defined inductively:

- Any constant symbol is a term;
- Any variable symbol is a term;
- If $\tau_1, \tau_2, ..., \tau_n$ are terms and f is a function symbol of arity n, then $f(\tau_1, \tau_2, ..., \tau_n)$ is a term;
- Nothing else is a term.

A *constant term* is a term that does not contain any variables.

Interpretation of constant terms in a structure:

If τ is a constant term in L and M is a L-structure, then interpretation of τ in M, denoted τ^M, is defined by induction as follows:

- If $\tau = C_i$, then $\tau^M = C_i$ as well;
- If $\tau = f_i(\tau_1, \tau_2, ..., \tau_n)$, then $\tau^M = f_i^M(\tau_1^M, \tau_2^M, ..., \tau_n^M)$.

Definition. *Formulas* in L are also defined inductively: [30]

- If τ_1 and τ_2 are terms, then $\tau_1 = \tau_2$ is a formula;

[30] In some texts, these are called *well-formed formulas*; for us, a formula is always well-formed.

- If $\tau_1, \tau_2, ..., \tau_n$ are terms and P is an n-ary relation then $P(\tau_1, \tau_2, ..., \tau_n)$ is a formula;
- If φ and ψ are formulas, then $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$, $\varphi \leftrightarrow \psi$, $\neg\varphi$ are formulas;
- If v is a variable and φ is a formula, then $\exists v\ \varphi$ and $\forall v\ \varphi$ are formulas;
- Nothing else is a formula.

Example 9.5. Let $L = \{-, \leq\}$, where $-$ is a unary function and $\leq$ is a binary function. Then $-(x)$ and $-(-x)$ are terms, and $x \leq -(y)$, $\forall x\ \exists y\ x \leq -(y)$ are formulas.

Definition. The set of *free occurrences* of variables in a formula φ is defined by induction:[31]

- If φ is atomic, then all occurrences of variables are free;
- If $\varphi = \varphi_1 \wedge \varphi_2$ or $\varphi_1 \vee \varphi_2$ or $\varphi_1 \to \varphi_2$ or $\varphi_1 \leftrightarrow \varphi_2$ or $\neg\varphi_1$, then the set of free occurrences of variables in φ are those of φ_1 and[32] those of φ_2.
- If $\varphi = \exists x\ \varphi'$ or $\forall x\ \varphi'$, the set of free occurrences of variables in φ are those of φ', except for the occurrence of x.

Definition. *Substitution.* If t is a term and x is a variable, $\varphi(t/x)$ denotes the formula with all free occurrences of x replaced with t.

We use the notation $\varphi(x_1, ..., x_n)$ if all free occurrences of variables in φ are occurrences of the variables $x_1, ..., x_n$.

Example 9.6.

$$\varphi(x, y) = (\forall x\ x \leq y) \wedge (\exists y\ \forall z\ x < y + z)$$

Definition. A substitution is *correct* if no variable of t becomes bounded in $\varphi(t/x)$.[33]

Example 9.7. Let $t = v + x$, then

$$\varphi(t/y) = (\forall x\ x \leq x + v) \wedge (\exists y\ \forall z\ x < y + z)$$

is not a *correct* substitution.

---

[31] If you know about λ-calculus, this definition and the ones below are exactly what you would expect them to be.

[32] Natural language "and", meaning the union of the two sets involved

[33] This is the terminology introduced in class. Some texts only allow for substitution when it is "correct"; in other words, we can perform this substitution only if *t is free to substitute for x in φ.*

Definition. A *sentence* is a formula without free variables.

Definition. Suppose M is a L-structure, the language $L(M)$ is the language $L \cup \{a : a \in M, a \text{ is a constant}\}$.

Interpretation of constant terms of $L(M)$ in M:

- If τ is a constant term of $L(M)$
  - If τ is a constant c of L, then $\tau^M = c^M$;
  - If $\tau = a$ for some constant a of M, then $\tau^M = a$;
- If $\tau = f(\tau_1, \tau_2, ..., \tau_n)$, then $\tau^M = f^M(\tau_1^M, \tau_2^M, ..., \tau_n^M)$.

Definition. If M is an L-structure and φ is an $L(M)$-sentence,

$$M \vDash \varphi$$

is defined by induction as follows:

- If φ is atomic,
  - $\varphi = (t_1 = t_2)$, $M \vDash \varphi$ if $t_1^M = t_2^M$;
  - $\varphi = P(t_1, ..., t_n)$, $M \vDash \varphi$ if $P^M(t_1^M, ..., t_n^M)$;
- If $\varphi = \varphi_1 \wedge \varphi_2$, $M \vDash \varphi$ if ($M \vDash \varphi_1$ and $M \vDash \varphi_2$).
  Similarly for other connectives.
- If $\varphi = \forall x\ \varphi'(x)$, $M \vDash \varphi$ if for all constants $a \in M, M \vDash \varphi'(a/x)$.
- If $\varphi = \exists x\ \varphi'(x)$, $M \vDash \varphi$ if there exists a constant $a \in M$ such that $M \vDash \varphi'(a/x)$.

Convention. If $\varphi = \varphi(x_1, ..., x_n)$, then $\bar{\varphi} := \forall x_1, ..., x_n\ \varphi(x_1, ..., x_n)$, and it is called the *universal closure* of φ. We say $M \vDash \varphi$ if $M \vDash \bar{\varphi}$.

Definition. We say φ is a *valid* L-formula if for every L-structure M, $M \vDash \varphi$.
Given a set Γ of L-formulas, $\Gamma \vDash \varphi$ if for every L-structure M, ($\forall \gamma \in \Gamma\ M \vDash \gamma \Rightarrow M \vDash \varphi$.)

9.2 Application to game theory

Consider a two-player game in which players I and II alternatively choose their moves. Let M be the set of all possible moves, and we assume that each game ends after a given finite number of moves. If M is finite, the game is finite iff each play (one instance of the game) is finite.
Let n be the number of moves in a game G. A winning condition for player I is a subset $A_I \subseteq M^n$, and similarly, a winning condition for player II is a subset $A_{II} \subseteq M^n$; we assume that there is no draw, thus $A_I \sqcup A_{II} = M^n$.

A *winning strategy* for player I is a function

$$s_I : \bigcup_{k:\text{even } k \leq n} M^k \to M$$

so that for every sequence $(m_1, m_2, ..., m_n) \in M^n$, if $m_k = s_I(m_1, ..., m_{k-1})$ for each k <u>odd</u> then $(m_1, ..., m_n) \in A_I$.

A *winning strategy* for player II is a function

$$s_{II} : \bigcup_{k:\text{odd } k \leq n} M^k \to M$$

so that for every sequence $(m_1, m_2, ..., m_n) \in M^n$, if $m_k = s_{II}(m_1, ..., m_{k-1})$ for each k <u>even</u> then $(m_1, ..., m_n) \in A_{II}$.
Clearly it is impossible for both players to have a winning strategy, but we can say more:

Theorem 9.8. *In any finite two-player game, one of the players has a winning strategy.*

Proof. Consider the language L consisting of one n-ary relation R. Let M be the L-structure with A_I being the interpretation of R. Consider the sentence

$$\sigma = \exists x_1 \forall x_2 \exists x_3 ... Q x_n \; R(x_1, ..., x_n)$$

where Q is $\exists$ if n is odd and Q is $\forall$ is n is even.
Observe that if $M \models \sigma$ then player I has a winning strategy; if $M \not\models \sigma$ then

$$M \models \forall x_1 \exists x_2 \forall x_3 ... Q' x_n \; \neg R(x_1, ..., x_n)$$

where Q' is $\forall$ if n is odd and Q is $\exists$ is n is even. In this case, player II has a winning strategy. $\square$

9.3 Axioms and inference rules

Axioms.

(A0) All instances of tautologies of propositional logic

(A1) $(\forall x\ (\varphi \to \psi)) \to (\varphi \to \forall x\ \psi)$ if x does not occur free in φ;

(A2) $\forall x\ \varphi \to \varphi(t/x)$ if t is a term and $\varphi(t/x)$ is a correct substitution;

(A3) $x = x$ for all variable x,

$(x = y) \to (t(x/z) = t(y/z))$ where t is a term and the substitution is correct;

$(x = y) \to (\varphi(x/z) = \varphi(y/z))$ where φ is an L-formula and the substitution is correct;

Inference rules.

(modus ponens) $\dfrac{\varphi \qquad \varphi \to \psi}{\psi}$

($\forall$-rule) $\dfrac{\varphi}{\forall x\ \varphi}$, also called *the generalization rule*

Let From(L) denote the set of L-formulas.
Define $\exists x\ \varphi := \neg\forall x\ \neg\varphi$.

Proposition 9.9. *This proof system is sound, i.e. for any language L and an L-formula φ, if $\vdash \varphi$ then φ is valid.*

Proposition 9.10. $\vdash (\forall x\ \varphi) \to (\exists x\ \varphi)$ *for every formula φ with one free variable x.*

Proof.

$\alpha 1$	$\forall x\ \varphi(x) \to \varphi(y/x)$	by A2, y is a variable not appearing in φ
$\alpha 2$	$\forall x\ \neg\varphi(x) \to \neg\varphi(y/x)$	by A2, y is a variable not appearing in φ
$\alpha 3$	$\alpha 2 \to (\forall x\ \neg\varphi(x) \to \neg\varphi(y/x))$	by the contrapositive law in A0,
$\alpha 4$	$\forall x\ \neg\varphi(x) \to \neg\varphi(y/x)$	by modus ponens on $\alpha 3, \alpha 2$
$\alpha 5$	$\alpha 1 \to (\alpha 4 \to ((\forall x\ \varphi) \to (\exists x\ \varphi)))$	by A0, we have $(p \to q) \to (q \to r) \to (p \to r)$
$\alpha 6$	$\alpha 4 \to ((\forall x\ \varphi) \to (\exists x\ \varphi))$	by modus ponens on $\alpha 1, \alpha 5$
$\alpha 7$	$(\forall x\ \varphi) \to (\exists x\ \varphi)$	by modus ponens on $\alpha 4, \alpha 6$

$\square$

Proposition 9.11. *For any formula φ, $\varphi \vdash \bar{\varphi}$ and $\bar{\varphi} \vdash \varphi$.*

Proof. $\varphi \vdash \bar{\varphi}$ by the $\forall$-rule.
By A2, $\vdash \bar{\varphi} \to \varphi(x/x)$, so $\bar{\varphi} \vdash \varphi$ by modus ponens. □

We also have the analogues of some theorems and lemmas from propositional logic:

Theorem 9.12. *(Deduction Theorem)*
If Γ is a set of L-formulas and φ, ψ are L-formulas, then

$$\Gamma \cup \{\varphi\} \vdash \psi \iff \Gamma \vdash \varphi \to \psi$$

Lemma 9.13. *If $\Gamma \cup \{\neg\varphi\}$ is inconsistent, then $\Gamma \vdash \varphi$.*

Theorem 9.14. *(Completeness Theorem for first-order logic, Gödel 1930)*[34]
If φ is an L-sentence and Γ is a set of L-sentences, then

$$\Gamma \vdash \varphi \iff \Gamma \vDash \varphi$$

In particular, Γ is consistent $\iff$ Γ has a model.[35]

Proof. (by L. Henkin) The "only if" direction follows from soundness. For the "if" direction, fix the language L, assume it's countable, then Form(L) is countable as well. Let $\{c_n : n \in \mathbb{N}\}$ be a set of new constants, i.e. not appearing in L.
Let $L' = L \cup \{c_n : n \in \mathbb{N}\}$, let $S := \{\varphi_n(x) : n \in \mathbb{N}\}$ be the set of all L'-formulas which has one free variable, they do not need to have the same free variable, we just use x for whatever the free variable is. Pick a bijective increasing function $f : \mathbb{N} \to \mathbb{N}$ such that $c_{f(n)}$ does not appear in $\{\varphi_1(x), ..., \varphi_n(x)\}$. Define $S_n = S \cup \{\exists x\ \varphi_i(x) \to \varphi_i(c_{f(i)}/x)\}$[36].
Note that by definition,

$$S \subseteq S_1 \subseteq S_2 \subseteq ... \subseteq S_\infty := \bigcup_{n \in N} S_i$$

For each $n \in \mathbb{N}$, S_n is consistent. Otherwise, choose the smallest n such that S_n is not consistent, then $S_{n-1} \vdash \neg(\exists x\ \varphi_n(x) \to \varphi_n(c_{f(n)}/x))$, equivalently, $S_{n-1} \vdash \exists x\ \varphi_n(x)$ and $S_{n-1} \vdash \neg\varphi_n(c_{f(n)})$. Since $c_{f(n)}$ does not occur in S_{n-1}, we can apply the $\forall$-rule, and get $S_{n-1} \vdash \forall x\ \neg\varphi_n(x)$. Since $\exists x\psi$ is equivalent to $\neg\forall x \neg\psi$, $S_{n-1} \vdash \neg\forall x \neg\varphi_n(x)$ and

[34] Not to be confused with the even more famous Gödel's Incompleteness Theorem 9.24
[35] Meaning there exists an L-structure M such that $M \vDash \gamma\ \forall\gamma \in \Gamma$.
[36] The formulas $\exists x\ \varphi_i(x) \to \varphi_i(c_{f(i)}/x)$ are called *Henkin axioms.*

$S_{n-1} \vdash \forall x \neg\varphi_n(x)$ contradict the consistency of S_{n-1}. Therefore S_n is consistent for each n, and S_∞ is consistent by Compactness Theorem 5.13.
Apply Zorn's Lemma 7.8, let $S' \supseteq S_\infty$ be a maximal consistent set of L'-sentences.
Given S', we define an L'-structure M from S' as follows:
Consider the equivalent relation $\sim$ defined on $C =_{\{} c_n : n \in \mathbb{N}\}$ as $c_n \sim c_m$ if $S' \vdash c_n = c_m$. Let $M = C/_\sim\ = \{[c_n] : n \in \mathbb{N}\}$. Given $L = \{R_1, ..., R_k, f_1, ..., f_l, \text{constants } C\}$, then

$$R_j^M([c_1], ..., [c_n]) \text{ if } S' \vdash R_j(c_1, ..., c_n)$$

$$f_j^M([c_1], ..., [c_n]) = [c_m] \text{ if } S' \vdash f_j(c_1, ..., c_n) = c_m$$

$$c_j^M = c_j$$

Claim 1. For an term t in L', there exists an n such that $S' \vdash t = c_n$.

Claim 2. For any L'-sentence φ, $M \vDash \varphi \iff S \vdash \varphi$.
Proof: By induction on the length of φ. Exercise. □

The deduction system studied so-far in this section is an example of *Hilbert-style system*. Let's briefly take a look at another proof-system:

9.4 Natural deduction

The objects that we prove are so-called *sequents*, which have form

$$\Delta \vdash \alpha$$

where Δ is a set of formulas. For propositional logic, there is only one axiom,

$$\Delta, \alpha \vdash \alpha$$

For first-order logic, one adds the following rules:

$$\frac{}{\forall x\ \varphi \vdash \varphi(t/x)}$$ *Rule of universal specification*

$$\frac{\psi \vdash \varphi}{\psi \vdash \forall x\ \varphi}$$ *Rule of universal generalization*

$$\frac{}{\varphi(t/x) \vdash \exists x\ \varphi(x)}$$ *Rule of existential generalization*

$$\frac{\varphi \vdash \psi}{\exists x\ \varphi \vdash \psi(x)}$$ *Rule of existential specification*

Theorem 9.15. *If Γ is a set of sentences and φ is a sentence, then $\Gamma \vdash \varphi$ is a sequent provable in the natural deduction system if and only if $\Gamma \vdash \varphi$ is provable in the Hilbert system.*

Definition. Given a set A of L-sentences, the set of *consequences* is

$$Con(A) := \{\sigma \in \text{Sent}(L) : A \vdash \sigma\}$$

Definition. A set T of L-sentences is called a *theory* if $T = Con(T)$. A theory T is *complete* if for each sentence σ, either $\sigma \in T$ or $\neg\sigma \in T$.
Note that T is complete iff it is maximal consistent.

Definition. If $T = Con(A)$, then A is said to be a set of *axioms* for T.

Definition. Given two sentences σ, τ and a set of sentences T, we say that σ is T-equivalent to τ, denoted $\sigma \equiv_T \tau$, if $T \vdash \sigma \leftrightarrow \tau$.

We simply write $\equiv$ for $\equiv_\emptyset$.

Definition. Given a set of sentences T, the Lindenbaum-Tarski algebra of T is defined as the set $\{[\sigma]_{\equiv_T} : \sigma \in \text{Sent}(L)\}$ with the same operations as in 6.2, with

$$0 = [\forall x\ x \neq x]_{\equiv_T} \text{ and } 1 = [\exists x\ x = x]_{\equiv_T}$$

We denote this as LT(T); if $T \neq \emptyset$, it is call the *Lindenbaum-Tarski algerbra of first-order logic*.

Definition. A sentence σ is in *prenex normal form* if

$$\sigma = Q_1 x_1 Q_2 x_2 ... Q_n x_n\ \varphi(x_1, x_2, ..., x_n)$$

where each Q_i is either a $\exists$ or $\forall$ and φ does not contain any quantifiers.

Example 9.16.
$$\forall x \forall y \exists z\ (x < y \wedge z = x) \wedge (\exists t\ t > y)$$
is not in prenex normal form;
$$\forall x \forall y \exists z \exists t\ (x < y \wedge z = x) \wedge (t > y)$$
is in prenex normal form;

Theorem 9.17. *For any sentence σ, there exists a sentence σ' such that $\sigma \equiv \sigma'$ and σ' is in prenex normal form.*

Proof. Let σ' be obtained from σ by changing the variables to new ones such that no variable appears more than once after a quantifier and moving all quantifiers to the front without switching order, then $\sigma \equiv \sigma'$ follows from the Completeness Theorem since any model satisfying σ also satisfies σ' and vice-versa. □

Definition. Given a model M, a subset $A \subseteq M$ is *definable*[37] if there exists a formula $\varphi(x)$ with one free variable x such that
$$A = \{a \in M : M \vDash \varphi(a/x)\}$$
Similarly, a relation $B \subseteq M$ is *definable* if there exists a formula $\varphi(x_1, ..., x_n)$ with n free variables $x_1, ..., x_n$ such that
$$B = \{(a_1, ..., a_n) \in M^n : M \vDash \sigma(a_1/x_1, ..., a_n/x_n)\}$$

9.5 Zermelo-Fraenkel set theory with the axiom of choice

Language $L = \{\in\}$.

1. Axiom of extensionality
$$\forall x \forall y\ (\forall z\ (z \in x \leftrightarrow z \in y) \to x = y)$$

2. Axiom of regularity
$$\forall x[\exists a\ (a \in x) \to \exists y\ (y \in x) \wedge \neg \exists z\ (z \in y \wedge z \in x)]$$

[37] By cardinality consideration, "almost all" subsets of $\mathbb{N}$ are not definable.

3. Axiom schema of specification

   Given a formula $\varphi(x, z, w_1, ..., w_n)$,

$$\forall z \forall w_1, ..., \forall w_n \exists y \forall x \ (x \in y \leftrightarrow (x \in z \wedge \varphi))$$

4. Axiom of pairing

$$\forall x \forall y \exists z \ (x \in z \wedge y \in z)$$

5. Axiom of union

$$\forall F \exists A \forall Y \forall x \ ((x \in Y \wedge Y \in F) \rightarrow x \in A)$$

6. Axiom schema of replacement

   Given a formula $\varphi(x, z, w_1, ..., w_n)$, let $\exists! y \ \varphi$ denote $(\exists y \varphi) \wedge ((\forall x \forall z \ \varphi(x) \wedge \varphi(z)) \rightarrow x = z)$.

$$\forall A \forall w_1, ..., \forall w_n [\forall x \ x \in A \rightarrow \exists! y \ \varphi \rightarrow \exists B \forall x \ (x \in A \rightarrow \exists y \ (y \in B \wedge \varphi))]$$

7. Axiom of infinity

   Let $S(w)$ denote $w \cup \{w\}$,

$$\exists X \ (\in X \wedge \forall y \ (y \in X) \in S(y) \in X)$$

8. Axiom of powerset

   Let $z \subseteq x$ denote $\forall y \ y \in z \rightarrow y \in x$,

$$\forall x \exists y \forall z \ (z \subseteq x \rightarrow z \in y)$$

9.6 Peano arithmetic

$L_{PA} = \{+, \cdot, S, 0, <\}$; $L_{PE} = L_{PA} \cup \{\exp\}$

Axioms.

1. $xS = yS \rightarrow x = y$
2. $xS \neq 0$

3. $x + 0 = x$

4. $x + yS = (x + y)S$

5. $x \cdot 0 = 0$

6. $x \cdot (yS) = x \cdot y + y$

7. $x \leq 0 \to x = 0$

8. $x \leq yS \to (x \leq y \vee x = yS)$

9. $x \leq y \vee y \leq x$

10. $x^0 = 0$

11. $x^{yS} = x^y + x$

Induction schema:

$$[Z(0) \wedge (\forall x\ A(x) \to A(xS))] \to \forall x\ A(x)$$

The theory generated by these axioms is called *Peano arithmetic*, abbreviated PA.

Definition. A set $A \subseteq N$ is *arithmetic* if it is definable in $\mathbb{N}$.

Write EXP for the set of all finite sequences of symbols of L_{PE} except those starting with the symbol S. For $n \in \mathbb{N}$, we write $\bar{n}$ to mean $0 \underbrace{SS...S}_{n-\text{many } S}$.

For an expression $\sigma = a_1 \cdots a_n$, we will associate a natural number called the *Gödel number* of σ, denoted $g(\sigma)$ in base 19 as follows:

Use this table to assign a unique Gödel number to each individual symbol.

Symbol s	0	S	+	$\cdot$	exp	$\leq$	=	x	$'$	$\perp$	$\exists$	$\forall$	$\neg$	$\to$	$\wedge$	$\vee$	(	)	#
Number $g(s)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

where # plays the role of a white space to separate formulas, and $'$ is for creating variables $x,\ x',\ x''$ etc.

Then for the expression σ, $g(\sigma) := (g(a_1) \cdots g(a_n))_{19}$, i.e. the Gödel number of an expression is the concatenate of the code number $g(.)$ of its symbols in base 19.

Example 9.18. For $\sigma = x + (x)'$, $g(\sigma) = (7\ 2\ 16\ 7\ 17\ 8)_{19}$.

Example 9.19. $g(\bar{n}) = g(\underbrace{0SS...S}_{n-\text{many } S}) = (\underbrace{0\ 1\ 1\ ...1}_{n-\text{many } 1's})_{19}$.

Let * denote concatenation of numbers in base 19.

Proposition 9.20. *The following relations are arithmetic.*

1. *x is a power of 19, abbr. $Pow_{19}(x)$*
   $\exists y\ x = \bar{19}^y$
2. *y is the smallest power of 19 bigger than x*
   $Pow_{19}(x) \wedge (x < y) \wedge \forall z\ (Pow_{19}(z) \wedge x < z) \to y < z.$
3. $y = 19^x$
   $(x = 0 \wedge y = \bar{19}) \vee (x \neq 0 \wedge S(x, y))$
4. $z = x * y$
   $\exists u \exists v\ u = 19^{length(y)} \wedge (v = u \cdot x \wedge z = v + y)$
5. $z = x_1 * ... * x_n$

Diagonalization.

Definition. Given a set $A \subseteq \mathbb{N}$, we say that γ is a Gödel sentence for A if

$$\gamma \text{ is true} \iff g(\gamma) \in A$$

We write E_n for the expression whose Gödel number is n.
Given $m \in \mathbb{N}$, write $E_n(m)$ for $\forall x\ (x = \bar{m}) \to E_n$.

Consider the following function, $\gamma(n, m)$ is defined to be the Gödel number of $E_n(m)$.
Proposition 9.21. *$\gamma(\cdot, \cdot)$ is arithmetic (i.e. $\gamma(x, y) = z$ is arithmetic).*

Proof.

$$z = g(\forall) * g(x) * g(() * g(x) * g(=) * g(y) * g(\to) * g(n) * g())$$

$\square$

Consider the function $d(\cdot)$ defined as $d(n) := r(n, n)$. For $A \subseteq \mathbb{N}$, denote $A^* := d^{-1}(A)$.
If A is arithmetic, then so is A^*.

Theorem 9.22. *(Tarski's undefinability theorem, 1936)*
The set T of Gödel numbers of sentences which are true in $\mathbb{N}$ is not arithmetic.

Proof. (sketch)
Suppose for a contradiction that T is arithmetic so it is defined by some formula $t(x)$. Its complement $\mathbb{N} \backslash T$ is also arithmetic and defined by $\neg t(x)$, so then $\mathbb{N} \backslash T$ is a Gödel sentence. Contradiction. $\square$

Proposition 9.23. *The set of sentences P provable in PE is arithmetic.*

The set of true statements T in number theory is beyond the arithmetic hierarchy, so $P \subsetneq T$.

Theorem 9.24. *(Gödel's First Incompleteness Theorem)*
PA is not complete.

Theorem 9.25. *(Gödel's Second Incompleteness Theorem)*

$$PA \nvdash Con(PA)$$

Index