Part II — Logic and Set Theory

Based on lectures by Dr Zsak

Lent 2023

Contents

§1 Propositional logic

We build a language consisting of statements/propositions;
We will assign truth values to statements;
We build a deduction system so that we can prove statements that are true (and only those). These are also features of more complicated languages.

§1.1 Languages

Let P be a set of **primitive propositions**. Unless otherwise stated, we let $P = \{p_1, p_2, \dots\}$ (i.e. countable). The **language** $L = L(P)$ is a set of **propositions** (or **compound propositions**) and is defined inductively by

1. if $p \in P$, then $p \in L$;
2. $\perp \in L$, where the symbol $\perp$ is read 'false'/ 'bottom';
3. if $p, q \in L$, then $(p \Rightarrow q) \in L$.

Example 1.1

$((p_1 \Rightarrow p_2) \Rightarrow (p_1 \Rightarrow p_3)) \in L$. $(p_4 \Rightarrow \perp) \in L$.

If $p \in L$ then $((p \Rightarrow \perp) \Rightarrow \perp) \in L$.

Remark 1. Note that the phrase 'L is defined inductively' means more precisely the following. Let $L_1 = P \cup \{\perp\}$, and define $L_{n+1} = L_n \cup \{(p \Rightarrow q) \mid p, q \in L_n\}$. We set $L = \bigcup_{n=1}^{\infty} L_n$.

Note that the elements of L are just finite strings of symbols from the alphabet $P \cup \{(,), \Rightarrow, \perp\}$. Brackets are only given for clarity; we omit those that are unnecessary, and may use other types of brackets such as square brackets.
We can prove that L is the smallest (w.r.t. inclusion) subset of the set Σ of all finite strings in $P \cup \{(,), \Rightarrow, \perp\}$ s.t. the properties of a language hold.
Note that $L \subsetneq \Sigma$. E.g. $\Rightarrow p_1 p_3 (\in \Sigma \setminus L$.

Note that the introduction rules for the language are injective and have disjoint ranges, so there is exactly one way in which any element of the language can be constructed using rules (i) to (iii).

Every $p \in L$ is uniquely determined by the properties of a language above, i.e. either $p \in P$ or $p = \perp$ or $\exists$ unique $q, r \in L$ s.t. $p = (q \Rightarrow r)$.

We can now introduce the abbreviations $\neg, \wedge, \vee, \top$, which are not, and, or and true/top respectively, defined by

Notation.

$$\neg p = (p \Rightarrow \perp); \quad p \vee q = \neg p \Rightarrow q; \quad p \wedge q = \neg(p \Rightarrow \neg q), \top = (\perp \Rightarrow \perp)$$

§1.2 Semantic implication

Definition 1.1 (Valuation)
A **valuation** is a function $v\colon L \to \{0,1\}$ s.t.

1. $v(\perp) = 0$;
2. If $p, q \in L$ then $v(p \Rightarrow q) = \begin{cases} 0 & v(p) = 1 \text{ and } v(q) = 0 \\ 1 & \text{else} \end{cases}$.

Example 1.2
If $v(p_1) = 1$, $v(p_2) = 0$. Then

$$v\left(\underbrace{(\perp \Rightarrow p_1)}_{1} \Rightarrow \underbrace{(p_1 \Rightarrow p_2)}_{0}\right) = 0$$

Remark 2. On $\{0,1\}$, we can define the constant $\perp = 0$ and the operation $\Rightarrow$ in the obvious way. Then, a valuation is precisely a mapping $L \to \{0,1\}$ preserving all structure, so it can be considered a homomorphism.

Proposition 1.1
Let $v, v'\colon L \to \{0,1\}$ be valuations that agree on the primitives p_i. Then $v = v'$. Further, any function $w\colon P \to \{0,1\}$ extends to a valuation $v : L \to \{0,1\}$ s.t. $v\mid_P = w$.

Remark 3. This is analogous to the definition of a linear map by its action on the basis vectors.

Proof. Clearly, v, v' agree on L_1 as $v(\perp) = v'(\perp) = 0$, the set of elements of the language of length 1. If v, v' agree at $p, q \in L_n$, then they agree at $p \Rightarrow q$. So by induction, v, v' agree on L_{n+1} for all n, and hence on L.

Let $v(p) = w(p)$ for all $p \in P$, and $v(\perp) = 0$ to obtain v on the set L_1. Assuming v is defined on $p, q \in L_n$ we can define it at $p \Rightarrow q$ in the obvious way. This defines v on L_{n+1}, hence v is defined on $\cup L_n = L$. By construction, v is a valuation on L and $v\mid_P = w$. $\square$

Example 1.3

Let v be the valuation with $v(p_1) = v(p_3) = 1$, and $v(p_n) = 0$ for all $n \neq 1, 3$. Then, $v((p_1 \Rightarrow p_3) \Rightarrow p_2) = 0$.

Definition 1.2 (Tautology)

A **tautology** is $t \in L$ s.t. $v(t) = 1 \forall$ valuations v. We write $\models t$.

Example 1.4

$p \Rightarrow (q \Rightarrow p)$ (a true statement is implied by any true statement).

$v(p)$	$v(q)$	$v(q \Rightarrow p)$	$v(p \Rightarrow (q \Rightarrow p))$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Since the right-hand column is always 1, $\models p \Rightarrow (q \Rightarrow p)$.

Example 1.5 (Law of Excluded Middle)

$\neg\neg p \Rightarrow p$, which expands to $((p \Rightarrow \perp) \Rightarrow \perp) \Rightarrow p$.

$v(p)$	$v(\neg p)$	$v(\neg\neg p)$	$v(\neg\neg p \Rightarrow p)$
0	1	0	1
1	0	1	1

Hence $\models \neg\neg p \Rightarrow p$.

Example 1.6

$\neg p \vee p$, which expands to $((p \Rightarrow \perp) \vee p)$.

$v(p)$	$v(\neg p)$	$v(\neg p \vee p)$
0	1	1
1	0	1

Hence $\models \neg p \vee p$.

Example 1.7

$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$. Suppose this is not a tautology. Then we have a valuation v s.t. $v(p \Rightarrow (q \Rightarrow r)) = 1$ and $v((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) = 0$. Hence, $v(p \Rightarrow q) = 1, v(p \Rightarrow r) = 0$, so $v(p) = 1, v(r) = 0$, giving $v(q) = 1$, but then $v(p \Rightarrow (q \Rightarrow r)) = 0$ contradicting the assumption.

Definition 1.3 (Semantic Implication)

Let $S \subseteq L$ and $t \in L$. We say S **entails** or **semantically implies** t, written $S \models t$, if for every valuation v on L, $v(s) = 1 \ \forall\, s \in S \Rightarrow v(t) = 1$.

Example 1.8

$\{p, p \Rightarrow q\} \models q$.

Example 1.9

Let $S = \{p \Rightarrow q, q \Rightarrow r\}$, and let $t = p \Rightarrow r$. Suppose $S \not\models t$, so there is a valuation v s.t. $v(p \Rightarrow q) = 1, v(q \Rightarrow r) = 1, v(p \Rightarrow r) = 0$. Then $v(p) = 1, v(r) = 0$, so $v(q) = 1$ and $v(q) = 0$ ↯.

Definition 1.4 (Model)

Given $t \in L$, say a valuation v **is a model for** t (or t **is true in** v) if $v(t) = 1$.

Definition 1.5 (Model)

We say that v **is a model of** S in L if $v(s) = 1$ for all $s \in S$.

Thus, $S \models t$ is the statement that every model of S is also a model of t/ t is true in every model of S.

Remark 4. The notation $\models t$ is equivalent to $\varnothing \models t$.

§1.3 Syntactic implication

For a notion of proof, we require a system of axioms and deduction rules. As axioms, we take (for any $p, q, r \in L$),

1. $p \Rightarrow (q \Rightarrow p)$;

2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$;
3. $((p \Rightarrow \bot) \Rightarrow \bot) \Rightarrow p$.

Remark 5. Sometimes, these three axioms are considered axiom **schemes**, since they are really a different axiom for each $p, q, r \in L$.

These are all tautologies.

For deduction rules, we will have only the rule **modus ponens (MP)**, that from p and $p \Rightarrow q$ one can deduce q.

Definition 1.6 (Proof)
Let $S \subseteq L, t \in L$. A **proof of t from S** is a finite sequence $t_1, \ldots, t_n$ of propositions in L s.t. $t_n = t$ and every t_i is either

1. an axiom;
2. an element of S (t_i is a premise or hypothesis); or
3. follows by MP, where $t_j = p$ and $t_k = p \Rightarrow q$ where $j, k < i$.

We say that S is the set of **premises** or **hypotheses**, and t is the **conclusion**.

We say S **proves** or **syntactically implies** t, written $S \vdash t$, if there exists a proof of t from S.

Example 1.10
We will show $\{p \Rightarrow q, q \Rightarrow r\} \vdash (p \Rightarrow r)$.

1. $q \Rightarrow r$ (hypothesis)
2. $(q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$ (axiom 1)
3. $p \Rightarrow (q \Rightarrow r)$ (modus ponens on lines 1, 2)
4. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ (axiom 2)
5. $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ (modus ponens on lines 3, 4)
6. $p \Rightarrow q$ (hypothesis)
7. $p \Rightarrow r$ (modus ponens on lines 5, 6)

Definition 1.7 (Theorem)
If $\varnothing \vdash t$, we say t is a **theorem**, written $\vdash t$.

Example 1.11

$\vdash (p \Rightarrow p)$.

1. $(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$ (axiom 2)
2. $p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$ (axiom 1)
3. $(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$ (modus ponens on lines 1, 2)
4. $p \Rightarrow (p \Rightarrow p)$ (axiom 1)
5. $p \Rightarrow p$ (modus ponens on lines 3, 4)

§1.4 Deduction theorem

Theorem 1.1 (Deduction Theorem)
Let $S \subseteq L$, and $p, q \in L$. Then $S \vdash (p \Rightarrow q)$ iff $S \cup \{p\} \vdash q$.

Remark 6. This show '$\Rightarrow$' really does behave like implication in formal proofs.

Proof. ($\Rightarrow$): Given a proof of $p \Rightarrow q$ from S, add the line p to the hypothesis and deduce q from modus ponens, to obtain a proof of q from $S \cup \{p\}$.

($\Leftarrow$): Suppose we have a proof of q from $S \cup \{p\}$. Let $t_1, \ldots, t_n$ be the lines of the proof. We will prove that $S \vdash (p \Rightarrow t_i)$ for all i by induction.

- If t_i is an axiom, we write t_i (axiom); $t_i \Rightarrow (p \Rightarrow t_i)$ (axiom 1); $p \Rightarrow t_i$ (modus ponens).
- If $t_i \in S$, we write t_i (hypothesis); $t_i \Rightarrow (p \Rightarrow t_i)$ (axiom 1); $p \Rightarrow t_i$ (modus ponens).
- If $t_i = p$, we write the proof of $\vdash p \Rightarrow p$ given above.
- Suppose t_i is obtained by modus ponens from t_j and $t_k = t_j \Rightarrow t_i$ where $j, k < i$. We may assume by induction that $S \vdash p \Rightarrow t_j$ and $S \vdash p \Rightarrow (t_j \Rightarrow t_i)$. We write
  1. $(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$ (axiom 2)
  2. $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ (modus ponens)
  3. $p \Rightarrow t_i$ (modus ponens)

  giving $S \vdash p \Rightarrow t_i$.

$\square$

Example 1.12

Consider $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$. By the Deduction Theorem, it suffices to prove $\{p \Rightarrow q, q \Rightarrow r, p\} \vdash r$, which is obtained easily from modus ponens.

§1.5 Soundness

We aim to show $S \models t$ iff $S \vdash t$. The direction $S \vdash t$ implies $S \models t$ is called **soundness**, which is a way of verifying that our axioms and deduction rule make sense. The direction $S \models t$ implies $S \vdash t$ is called **adequacy**, which states that our axioms are powerful enough to deduce everything that is (semantically) true.

Proposition 1.2 (Soundness Theorem)

Let $S \subseteq L$ and $t \in L$. Then $S \vdash t$ implies $S \models t$.

Proof. We have a proof $t_1, \dots, t_n$ of t from S. We aim to show that any model of S is also a model of t, so if v is a valuation that maps every element of S to 1, then $v(t) = 1$. We show this by induction on the length of the proof. $v(p) = 1$ for each axiom p and for each $p \in S$. Further, $v(t_i) = 1, v(t_i \Rightarrow t_j) = 1$, then $v(t_j) = 1$. Therefore, $v(t_i) = 1$ for all i. □

§1.6 Adequacy

Consider the case of adequacy where $t = \perp$. If our axioms are adequate, $S \models \perp$ implies $S \vdash \perp$, so $S \nvdash \perp$. We say S is **consistent** if $S \nvdash \perp$. Therefore, in an adequate system, if S has no models then S is inconsistent; equivalently, if S is consistent then it has a model.

In fact, the statement that consistent axiom sets have a model implies adequacy in general. Indeed, if $S \models t$, then $S \cup \{\neg t\}$ has no models, and so it is inconsistent by assumption. Then $S \cup \{\neg t\} \vdash \perp$, so $S \vdash \neg t \Rightarrow \perp$ by the deduction theorem, giving $S \vdash t$ by axiom 3.

We aim to construct a model of S given that S is consistent. Intuitively, we want to write

$$v(t) = \begin{cases} 1 & t \in S \\ 0 & t \notin S \end{cases}$$

but this does not work on the set $S = \{p_1, p_1 \Rightarrow p_2\}$ as it would evaluate p_2 to false.

We say a set $S \subseteq L$ is **deductively closed** if $p \in S$ whenever $S \vdash p$. Any set S has a **deductive closure**, which is the (deductively closed) set of statements $\{t \in L \mid S \vdash t\}$

that S proves. If S is consistent, then the deductive closure is also consistent. Computing the deductive closure before the valuation solves the problem for $S = \{p_1, p_1 \Rightarrow p_2\}$. However, if a primitive proposition p is not in S, but $\neg p$ is also not in S, this technique still does not work, as it would assign false to both p and $\neg p$.

Theorem 1.2 (model existence lemma)
Every consistent set $S \subseteq L$ has a model.

Proof. First, we claim that for any consistent $S \subseteq L$ and proposition $p \in L$, either $S \cup \{p\}$ is consistent or $S \cup \{\neg p\}$ is consistent. If this were not the case, then $S \cup \{p\} \vdash \perp$, and also $S \cup \{\neg p\} \vdash \perp$. By the deduction theorem, $S \vdash p \Rightarrow \perp$ and $S \vdash (\neg p) \Rightarrow \perp$. But then $S \vdash \neg p$ and $S \vdash \neg\neg p$, so $S \vdash \perp$ contradicting consistency of S.

Now, L is a countable set as each L_n is countable, so we can enumerate L as $t_1, t_2, \dots$. Let $S_0 = S$, and define $S_1 = S_0 \cup \{t_1\}$ or $S_1 = S_0 \cup \{\neg t_1\}$, chosen s.t. S_1 is consistent. Continuing inductively, define $\overline{S} = \bigcup_{i \in \mathbb{N}} S_i$. Then, for all $t \in L$, either $t \in \overline{S}$ or $\neg t \in \overline{S}$. Note that $\overline{S}$ is consistent; indeed, if $\overline{S} \vdash \perp$, then this proof uses hypotheses only in S_n for some n, but then $S_n \vdash \perp$ contradicting consistency of S_n. Note also that $\overline{S}$ is deductively closed, so if $\overline{S} \vdash p$, we must have $p \in \overline{S}$; otherwise, $\neg p \in \overline{S}$ so $\overline{S} \vdash \neg p$, giving $\overline{S} \vdash \perp$, contradicting consistency of $\overline{S}$. Now, define the function

$$v(t) = \begin{cases} 1 & t \in \overline{S} \\ 0 & t \notin \overline{S} \end{cases}$$

We show that v is a valuation, then the proof is complete as $v(s) = 1$ for all $s \in S$. Since $\overline{S}$ is consistent, $\perp \notin \overline{S}$, so $v(\perp) = 0$.

Suppose $v(p) = 1, v(q) = 0$. Then $p \in \overline{S}$ and $q \notin \overline{S}$, and we want to show $(p \Rightarrow q) \notin \overline{S}$. If this were not the case, we would have $(p \Rightarrow q) \in \overline{S}$ and $p \in \overline{S}$, so $q \in \overline{S}$ as $\overline{S}$ is deductively closed.

Now suppose $v(q) = 1$, so $q \in \overline{S}$, and we need to show $(p \Rightarrow q) \in \overline{S}$. Then $\overline{S} \vdash q$, and by axiom 1, $\overline{S} \vdash q \Rightarrow (p \Rightarrow q)$. Therefore, as $\overline{S}$ is deductively closed, $(p \Rightarrow q) \in \overline{S}$.

Finally, suppose $v(p) = 0$, so $p \notin \overline{S}$, and we want to show $(p \Rightarrow q) \in \overline{S}$. We know that $\neg p \in \overline{S}$, so it suffices to show that $p \Rightarrow \perp \vdash p \Rightarrow q$. By the deduction theorem, this is equivalent to proving $\{p, p \Rightarrow \perp\} \vdash q$, or equivalently, $\perp \vdash q$. But by axiom 1, $\perp \Rightarrow (\neg q \Rightarrow \perp)$ where $(\neg q \Rightarrow \perp) = \neg\neg q$, so the proof is complete by axiom 3. □

Remark 7. We used the fact that P was a countable set in order to show that L was countable. The result does in fact hold if P is uncountable, but requires more tools to prove. Some sources call this theorem the 'completeness theorem'.

Corollary 1.1 (adequacy)
Let $S \subseteq L$ and let $t \in L$, s.t. $S \models t$. Then $S \vdash t$.

Proof. Follows from the remarks before the model existence lemma. □

§1.7 Completeness

Theorem 1.3 (completeness theorem for propositional logic)
Let $S \subseteq L$ and $t \in L$. Then $S \models t$ if and only if $S \vdash t$.

Proof. Follows from soundness and adequacy. □

Theorem 1.4 (compactness theorem)
Let $S \subseteq L$ and $t \in L$ with $S \models t$. Then there exists a finite subset $S' \subseteq S$ s.t. $S' \models t$.

Proof. Trivial after applying the completeness theorem, since proofs depend on only finitely many hypotheses in S. □

Corollary 1.2 (compactness theorem, equivalent form)
Let $S \subseteq L$. Then if every finite subset $S' \subseteq S$ has a model, then S has a model.

Proof. Let $t = \bot$ in the compactness theorem. Then, if $S \models \bot$, some finite $S' \subseteq S$ has $S' \models \bot$. But this is not true by assumption, so there is a model for S. □

Remark 8. This corollary is equivalent to the more general compactness theorem, since the assertion that $S \models t$ is equivalent to the statement that $S \cup \{\neg t\}$ has no model, and $S' \models t$ is equivalent to the statement that $S' \cup \{\neg t\}$ has no model.

Theorem 1.5 (decidability theorem)
Let $S \subseteq L$ and $t \in L$. Then, there is an algorithm to decide (in finite time) if $S \vdash t$.

Proof. Trivial after replacing $\vdash$ with $\models$, by drawing the relevant truth tables. □