Part II - Logic and Set Theory

Lectured by I. B. Leader

Lent 2015

Contents

1 Propositional calculus

Definition (Propositions)**.** Let P be a set of *primitive propositions*. These are a bunch of (meaningless) symbols, that are usually interpreted to take a truth value. Usually, any symbol (composed of alphabets and subscripts) is in the set of primitive propositions.

The set of *propositions*, written as L or $L(P)$, is defined inductively by

(i) If $p \in P$, then $p \in L$.

(ii) $\perp \in L$, where $\perp$ is "false" (also a meaningless symbol).

(iii) If $p, q \in L$, then $p \Rightarrow q) \in L$.

Example. $p \Rightarrow q$, $p \Rightarrow \perp$, $((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ are propositions.

To define L formally, we let $L_1 = \{\perp\} \cup P$, and for $n \geq 1$, $L_{n+1} = L_n \cup \{(p \Rightarrow q) : p, q \in L_n\}$. Then set $L = L_1 \cup L_2 \cup \cdots$.

In formal language terms, L is the set of finite strings of symbols from the alphabet $\perp$, $\perp$, $\Rightarrow$, (,), p_1, $p_2, \cdots$ that satisfies some formal grammar rule (e.g. brackets have to match).

We define the following abbreviations:

Definition (Logical symbols)**.**

$\neg p$	("not p")	is an abbreviation for	$(p \Rightarrow \perp)$
$p \wedge q$	("p and q")	is an abbreviation for	$\neg(p \Rightarrow (\neg q))$
$p \vee q$	("p or q")	is an abbreviation for	$(\neg p) \Rightarrow q$

1.1 Semantic implication

Definition (Valuation)**.** A *valuation* on L is a function $v : L \to \{0, 1\}$ such that:

- $v(\perp) = 0$,
- $v(p \Rightarrow q) = \begin{cases} 0 & \text{if } v(p) = 1, v(q) = 0, \\ 1 & \text{otherwise} \end{cases}$

We interpret $v(p)$ to be the truth value of p, with 0 denoting "false" and 1 denoting "true".

Note that we do not impose any restriction of $v(p)$ when p is a primitive proposition (that is not $\perp$).

We can also give $\{0, 1\}$ a binary operation $\Rightarrow$ by

$$a \Rightarrow b = \begin{cases} 0 & \text{if } a = 1, b = 0 \\ 1 & \text{otherwise} \end{cases}$$

with a constant $\perp = 0$. Then a valuation $v : K \to \{0, 1\}$ is simply a homomorphism between the two structures that preserve $\perp$ and $\Rightarrow$.

Proposition.

(i) If v and v' are valuations with $v(p) = v'(p)$ for all $p \in P$, then $v = v'$.

(ii) For any function $W : P \to \{0, 1\}$, there is a valuation v such that $v(p) = w(p)$ for all $p \in L$, i.e. we can extend w to a full valuation.

This means "A valuation is determined by its values on P, and any values will do".

Proof. (i) Recall that L is defined inductively. We are given that $v(p) = v'(p)$ on L_1. Then for all $p \in L_2$, p must be in the form $q \Rightarrow r$ for $q, r \in L_1$. Then $v(q \Rightarrow r) = v(p \Rightarrow q)$ since the value of v is uniquely determined by the definition. So for all $p \in L_2$, $v(p) = v'(p)$.

Continue inductively to show that $v(p) = v'(p)$ for all $p \in L_n$ for any n.

(ii) Set v to agree with w for all $p \in P$, and set $v(\perp) = 0$. Then define v on L_n inductively according to the definition.

$\square$

Example. Suppose v is a valuation with $v(p) = v(q) = 1$, $v(r) = 0$. Then

$$v((p \Rightarrow q) \Rightarrow r) = 0.$$

Definition (Tautology)**.** t is a *tautology*, written as $\models t$, if $v(t) = 1$.

Example. (i) $p \Rightarrow (q \Rightarrow p)$ "A true statement is implied by anything".

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

(ii) $(\neg\neg p) \Rightarrow p$. Recall that $\neg\neg p$ is defined as $((p \Rightarrow \perp) \Rightarrow \perp)$.

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

(iii) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.

Instead of creating a truth table, which would be horribly long, we show this by reasoning: Suppose it is not a tautology. So there is a v such that $v(p \Rightarrow q \Rightarrow r)) = 1$ and $v((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) = 0$. For the second equality to hold, we must have $v(p \Rightarrow q) = 1$ and $v(p \Rightarrow r) = 0$. So $v(p) = 1, v(r) = 0, v(q) = 1$. But then $v(p \Rightarrow q) = 0$.

Definition (Semantic entailment)**.** For $S \subseteq L$, $t \in L$, we say S *entails* t, S *semantically implies* t or $S \models t$ if, for any v such that $v(s) = 1$ for all $s \in S$, $v(t) = 1$.

"Whenever all of S is true, t is true as well."

Example. $\{p \Rightarrow q, q \Rightarrow r\} \models (p \Rightarrow r)$.

We want to show that for any valuation v with $v(p \Rightarrow q) = v(q \Rightarrow r) = 1$, we have $v(p \Rightarrow r) = 1$. We prove the contrapositive.

If $v(p \Rightarrow r) = 0$, then $v(p) = 1$ and $v(r) = 0$. If $v(q) = 0$, then $v(p \Rightarrow q) = 0$. If $v(q) = 1$, then $v(q \Rightarrow r) = 0$. So $v(p \Rightarrow r) = 0$ only if one of $v(p \Rightarrow q)$ or $v(q \Rightarrow r)$ is zero.

Definition (Truth and model)**.** If $v(t) = 1$, then we say that t is *true* in v, or v is a *model* of t. For $S \subseteq L$, a valuation v is a *model* of S if $v(s) = 1$. Then $\models t$ means $\emptyset \models t$.

1.2 Syntactic implication

While semantic implication captures the idea of truthfulness, syntactic implication captures the idea of proofs. To do so, we need to have axioms and deduction rules.

Our system of deduction composes of the following axioms:

(i) $p \Rightarrow (q \Rightarrow q)$

(ii) $[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$

(iii) $(\neg\neg p) \Rightarrow p$

and the deduction rule of *modus ponens*: from p and $p \Rightarrow q$, we can deduce q.

Note that every axiom is a tautology.

Definition (Proof and syntactic entailment)**.** For any $S \subseteq L$, a *proof* of t from S is a finite sequence $t_1, t_2, \cdots t_n$ of propositions, with $t_n = t$, such that each t_i is one of the following:

(i) An axiom

(ii) A member of S

(iii) A proposition t_i such that there exist $j, k < i$ with $t_j = (t_k \Rightarrow t_i)$.

If there is a proof of t from S, we say that S *proves* or *syntactically entails* t, written $S \vdash t$.

If $\emptyset \vdash t$, say t is a *theorem* and write $\vdash t$.

In a proof of t from S, t is the *conclusion* and S is the set of *hypothesis* or *premises*.

Example. $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$

"Go for $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ via Axiom 2.

1. $[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$ Axiom 2
2. $q \Rightarrow r$ Hypothesis
3. $(q \Rightarrow r) \Rightarrow [q \Rightarrow (q \Rightarrow r)]$ Axiom 1
4. $p \Rightarrow (q \Rightarrow r)$ MP on 2,3
5. $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ MP on 1, 4
6. $p \Rightarrow q$ Hypothesis
7. $p \Rightarrow r$ MP on 5, 6

Example. $\vdash (p \Rightarrow p)$

"Go for $[p \Rightarrow (p \Rightarrow p)] \Rightarrow (p \Rightarrow p)$"

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. $[p \Rightarrow (p \Rightarrow p)] \Rightarrow (p \Rightarrow p)$ MP on 1, 2

4. $p \Rightarrow (p \Rightarrow p)$ Axiom 1

5. $p \Rightarrow p$ MP on 3, 4

This seems like a really tedious way to prove things. We now prove that the *deduction theorem*, that can usually help to prove $S \vdash t$.

Proposition (Deduction theorem)**.** Let $S \subset L$ and $p, q \in L$. Then $S \vdash (p \Rightarrow q)$ if and only if $S \cup p \vdash q$.

"$\vdash$ behaves like the connective $\Rightarrow$ in the language"

Proof. ($\Rightarrow$) Given a proof of $p \Rightarrow q$ from S, append the lines

- p Hypothesis
- q MP

to obtain a proof of q from $S \cup \{q\}$.

($\Leftarrow$) Let $t_1, t_2, \cdots, t_n = q$ be a proof of q from $S \cup \{p\}$. We'll show that $S \vdash p \Rightarrow t_i$ for all i.

We consider different possibilities of t_i:

- t_i is an axiom: Write down
  - $t_i \Rightarrow (p \Rightarrow t_i)$ (Axiom 1)
  - t_i Axiom
  - $p \Rightarrow t_i$ MP
- $t_i \in S$: Write down
  - $t_i \Rightarrow (p \Rightarrow t_i)$ (Axiom 1)
  - t_i Hypothesis
  - $p \Rightarrow t_i$ MP

  To get $S \models (p \Rightarrow t_i)$
- $t_i = p$: Write down our proof of $p \Rightarrow p$ from our example above.
- t_i is obtained by MP: we have some $j, k < i$ such that $t_k = (t_k \Rightarrow t_i)$. We can assume that $S \vdash (p \Rightarrow t_j)$ and $S \vdash (p \Rightarrow t_k)$ by induction on i. Now we can write down
  - $[p \Rightarrow (t_j \Rightarrow t_i)] \Rightarrow [(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)]$ Axiom 2
  - $p \Rightarrow (t_j \Rightarrow t_i)$ Known already
  - $(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$ MP
  - $p \Rightarrow t_j$ Known already
  - $p \Rightarrow t_i$ MP

  to get $S \models (p \Rightarrow t_i)$.

This is why Axiom 2 is as it is - it enables us to prove the deduction theorem. $\square$

Example. We want to show $\{p \Rightarrow q, q \Rightarrow r\} \vdash (p \Rightarrow r)$. By the deduction theorem, it is enough to show that $\{p \Rightarrow q, q \Rightarrow r, p\} \vdash r$, which is trivial by applying MP twice.

Now we have two notions: $\models$ and $\vdash$. How are they related? We want to show that they are equal: if something is true, we can prove it; if we can prove something, it must be true.
Aim. Show that $S \vdash t$ if and only if $S \models t$. This is the *completeness theorem*, made up of two directions:

(i) Soundness: If $S \vdash t$, then $S \models t$. "Our axioms aren't absurd"

(ii) Adequacy: If $S \models t$, $S \vdash t$. "Our axioms are strong enough to be able to deduce, from S, *all* semantic consequences of S."

Proposition (Soundness)**.** If $S \subset L$, $t \in L$, then if $S \vdash t$, then $S \models t$.

Proof. Given valuation v with $v(s) = 1$ for all $s \in S$, we need to show that $v(t) = 1$. But $v(p) = 1$ for all axioms p, and $v(p) = 1$ for all $p \in S$, and if $v(p) = 1$ and $v(p \Rightarrow q) = 1$, then $v(q) = 1$. Hence each line t_i in a proof $t_1, \cdots, t_n$ of from S has $v(t_i) = 1$. $\square$

This works because we know that all axioms of tautologies.