Logic and Set Theory

January 24, 2018

Contents

0 Miscellaneous

Some introductory speech

1 Propositional logic

Let P denote a set of *primitive proposition*, unless otherwise stated, $P = \{p_1, p_2, ...\}$.

Definition. The *language* or *set of propositions* $L = L(P)$ is defined inductively by:
(1) $p \in L\ \forall p \in P$;
(2) $\perp \in L$, where $\perp$ is read as 'false';
(3) If $p, q \in L$, then $(p \implies q) \in L$. For example, $(p_1 \implies L)$, $((p_1 \implies p_2) \implies (p_1 \implies p_3))$.

Note that at this point, each proposition is only a finite string of symbols from the alphabet $(,), \implies, \perp, p_1, p_2, ...$ and do not really mean anything (until we define so).
By *inductively define*, we mean more precisely that we set $L_1 = P \cup \{\perp\}$, and $L_{n+1} = L_n \cup \{(p \implies q) : p, q \in L_n\}$, and then put $L = L_1 \cup L_2 \cup ....$

Each proposition is built up *uniquely* from 1) and 2) using 3). For example, $((p_1 \implies p_2) \implies (p_1 \implies p_3))$ came from $(p_1 \implies p_2)$ and $(p_1 \implies p_3)$. We often omit outer brackets or use different brackets for clarity.

Now we can define some useful things:
• $\neg p$ (not p), as an abbreviation for $p \implies L$;
• $p \vee q$ (p or q), as an abbreviation for $(\neg p) \implies q$;
• $p \wedge q$ (p and q), as an abbreviation for $(p \implies (\neg q))$.

These definitions 'make sense' in the way that we expect them to.

Definition. A *valuation* is a function $v : L \to \{0, 1\}$ s.t.
(1) $v(\perp) = 0$; (2)

$$v(p \implies q) = \begin{cases} 0 & v(p) = 1, v(q) = 0 \\ 1 & else \end{cases} \quad \forall p, q \in L$$

Remark. On $\{0, 1\}$, we could define a constant $\perp$ by $\perp = 0$, and an operation $\implies$ by $a \implies b = 0$ if $a = 1, b = 0$ and 1 otherwise. Then a valuation is a function $L \to \{0, 1\}$ that preserves the structure ($\perp$ and $\implies$), i.e. a homomorphism.

Proposition. (1) If v, v' are valuations with $v(p) = v'(p)\ \forall p \in P$, then $v = v'$ (on L).
(2) For any $w : P \to \{0, 1\}$, there exists a valuation v with $v(p) = w(p)\ \forall p \in P$.
In short, a valuation is defined by its value on p, and any values will do.

Proof. (1) We have $v(p) = v'(p)\ \forall p \in L_1$. However, if $v(p) = v'(p)$ and $v(q) = v'(q)$ then $v(p \implies q) = v'(p \implies q)$, so $v = v'$ on L_2. Continue inductively we have $v = v'$ on $L_n \forall n$.
(2) Set $v(p) = w(p)\ \forall p \in P$ and $v(\perp) = 0$: this defines v on L_1. Having defined v on L_n, use the rules for valuation to inductively define v on L_{n+1} so we can extend v to L. □

Definition. We say p is a *tautology*, written $\models p$, if $v(p) = 1$ $\forall$ valuations v.
Some examples:
(1) $p \implies (q \implies p)$: a true statement is implies by anything. We can verify this by:

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

So we see that this is indeed a tautology;
(2) $(\neg\neg p) \implies p$, i.e. $((p \implies \bot) \implies \bot) \implies p$, called the "law of excluded middle";

(3) $[p \implies (q \implies r)] \implies [(p \implies q) \implies (p \implies r)]$.
Indeed, if not then we have some v with $v(p \implies (q \implies r)) = 1$, $v(\implies (p \implies q) \implies (p \implies r)) = 0$. So $v(p \implies q) = 1$, $v(p \implies r) = 0$. This happens when $v(p) = 1$, $v(r) = 0$, so also $v(q) = 1$. But then $v(q \implies r) = 0$, so $v(p \implies (q \implies r)) = 0$.

Definition. For $S \subset L$, $t \in L$, say S *entails* or *semantically implies* t, written $S \models t$ if $v(s) = 1 \forall s \in S \implies v(t) = 1$, for each valuation v.
("Whenever all of S is true, t is true as well.")

For example, $\{p \implies q, q \implies r\} \models (p \implies r)$. To prove this, suppose not: so we have v with $v(p \implies q) = v(q \implies r) = 1$ but $v(p \implies r) = 0$. So $v(p) = 1$, $v(r) = 0$, so $v(q) = 0$, but then $v(p \implies q) = 0$.

If $v(t) = 1$ we say t is true in v or that v is a model of t.

For $S \subset L$, v is a model of S if $v(s) = 1$ $\forall s \in S$. So $S \models t$ says that every model of S is a model of t. For example, in fact $\models t$ is the same as $\phi \models t$.

2 Syntactic implication

For a notion of 'proof', we will need axioms and deduction rules. As axioms, we'll take:
1. $p \implies (q \implies p)\ \forall p, q \in L$;
2. $[p \implies (q \implies r)] \implies [(p \implies q) \implies (p \implies r)]\ \forall p, q, r \in L$;
3. $(\neg\neg p) \implies p\ \forall p \in L$.

Note: these are all tautologies. Sometimes we say they are 3 axiom-schemes, as all of these are infinite sets of axioms.

As deduction rules, we'll take just *modus ponens*: from p, and $p \implies q$, we can deduce q.

For $S \subset L$, $t \in L$, a *proof* of t from S cosists of a finite sequence $t_1, ..., t_n$ of propositions, with $t_n = t$, s.t. $\forall i$ the proposition t_i is an axiom, or a member of S, or there exists $j, k < i$ with $t_j = (t_k \implies t_i)$.

We say S is the *hypotheses* or *premises* and t is the *conclusion*.

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

If $\phi \vdash t$, we say t is a *theorem*, written $\vdash t$.

Example. $\{p \implies q, q \implies r\} \vdash p \implies r$.
we deduce by the following:
(1) $[p \implies (q \implies r)] \implies [(p \implies q) \implies (p \implies r)]$; (axiom 2)
(2) $q \implies r$; (hypothesis)
(3) $(q \implies r) \implies (p \implies (q \implies r))$; (axiom 1)
(4) $p \implies (q \implies r)$; (mp on 2,3)
(5) $(p \implies q) \implies (p \implies r)$ (mp on 1,4);
(6) $p \implies q$; (hypothesis)
(7) $p \implies r$. (mp on 5,6)

Example. Let's now try to prove $\vdash p \implies p$. Axiom 1 and 3 probably don't help so look at axiom 2; if we make $(p \implies q)$ and $p \implies (q \implies r)$ something that's a theorem, and make $p \implies r$ to be $p \implies p$ then we are done. So we need to take $p = p, q = (p \implies p), r = p$. Now:
(1) $[p \implies ((p \implies p) \implies p)] \implies [(p \implies (p \implies p)) \implies (p \implies p)]$; (axiom 2)
(2) $p \implies ((p \implies p) \implies p)$; (axiom 1)
(3) $(p \implies (p \implies p)) \implies (p \implies p)$; (mp on 1,2)
(4) $p \implies (p \implies p)$; (axiom 1)
(5) $p \implies p$. (mp on 3,4)

Proofs are made easier by:

Proposition. (2, deduction theorem)
Let $S \subset L$, $p, q \in L$. Then $S \vdash (p \implies q)$ if and only if $(S \cup \{p\}) \vdash q$.

Proof. Forward: given a proof of $p \implies q$ from S, add the lines p (hypothesis), q (mp) to optaion a proof of q from $S \cup \{p\}$.
Backward: if we have proof $t_1, ..., t_n = q$ of q from $S \cup \{p\}$. We'll show that $S \vdash (p \implies t_i) \forall i$, so $p \implies t_n = q$.
If t_i is an axiom, then we have $\vdash t_i \implies (p \implies t_i)$, so $\vdash p \implies t_i$;
If $t_i \in S$, write down t_i, $t_i \implies (p \implies t_i)$, $p \implies t_i$ we get a proof of $p \implies t_i$ from S;
If $t_i = p$: we know $\vdash (p \implies p)$, so done;
If t_i obtained by mp: in that case we have some earlier lines t_j and $t_j \implies t_i$. By induction, we may assume $S \vdash (p \implies t_j)$ and $S \vdash (p \implies (t_j \implies t_i))$. Now we can write down $[p \implies (t_j \implies t_i)] \implies [(p \implies t_j) \implies (t_i)]$ by axiom 2, $p \implies (t_j \implies t_i)$, $p \implies t_j) \implies (p \implies t_i)$ (mp), $p \implies t_j$, $p \implies t_i$ (mp) to obtain $S \vdash (p \implies t_i)$.

These are all of the cases. So $S \vdash (p \implies q)$. □

This is why we chose axiom 2 as we did – to make this proof work.

Example. To show $\{p \implies q, q \implies r\} \vdash (p \implies r)$, it's enough to show that $\{p \implies q, q \implies r, p\} \vdash r$, which is trivial by mp.

Now, how are $\vdash$ and $\vDash$ related? We are going to prove the *completeness theorem*: $S \vdash t \iff S \vDash t$.

This ensures that our proofs are sound, in the sense that everything it can prove is not absurd ($S \vdash t$ then $S \vDash t$), and are adequate, i.e. our axioms are powerful enough to define every semantic consequence of S, which is not obvious ($S \vDash t$ then $S \vdash t$).

Proposition. (3)
Let $S \subset L$, $t \in L$. Then $S \vdash t \implies S \vDash t$.

Proof. Given a valuation v with $v(s) = 1 \ \forall s \in S$, we want $v(t) = 1$.
We have $v(p) = 1 \ \forall p$ axiom as our axioms are all tautologies (proven earier); $v(p) = 1 \ \forall p \in S$ by definition of v; also if $v(p) = 1$ and $v(p \implies q) = 1$, then also $v(q) = 1$ (by definition of $\implies$). So $v(p) = 1$ for each line p of our proof of t from S. □

We say $S \subset L$ consistent if $S \nvdash \perp$. One special case of adequacy is: $S \vDash \perp \implies S \vdash \perp$, i.e. if S has no model then S inconsistent, i.e. if S is consistent then S has a model. This implies adequacy: given $S \vDash t$, we have $S \cup \{\neg t\} \vDash \perp$, so by our special case we have $S \cup \{\neg t\} \vdash \perp$, i.e. $S \vdash ((\neg t) \implies t)$ by deduction theorem, so $S \vdash \neg\neg t$. But $S \vdash ((\neg\neg t) \implies t)$ by axiom 3, so $S \vdash t$ (mp).