Chapter I

A Weak Post's Theorem and the Deduction Theorem Retold

This note is about the *Soundness* and *Completeness* ("Post's Theorem") in Boolean logic.

1. Soundness of Boolean Logic

Soundness is the Property expressed by the statement of the metatheory below:

$$\text{If } \Gamma \vdash A, \text{ then } \Gamma \models_{taut} A \tag{1}$$

1.1 Definition. The statement "Boolean logic is Sound" means that Boolean logic satisfies (1). □

To prove soundness is an easy induction on the length of Γ-proofs:

We prove that proofs preserve truth.

1.2 Lemma. Eqn *and* **Leib** *preserve truth, that is,*

$$A, A \equiv B \models_{taut} B \tag{2}$$

and

$$A \equiv B \models_{taut} C[\mathbf{p} := A] \equiv C[\mathbf{p} := B] \tag{3}$$

Proof. We proved (2) in Assignment #1. We prove (2) now:

So, let a state s make $A \equiv B$ true ($\mathbf{t}$).

We will show that

$$C[\mathbf{p} := A] \equiv C[\mathbf{p} := B] \text{ is } \mathbf{t} \text{ in state } s \tag{4}$$

If $\mathbf{p}$ is not in C then (4) is $C \equiv C$, a tautology, so is true under s in particular.

► Let then the distinct $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{r}', \mathbf{r}'', \ldots$ all occur in C.

Now *in the lhs of (4)* $\mathbf{p}$ gets the value $\overline{s}(A)$, while $\mathbf{q}, \mathbf{r}, \mathbf{r}', \mathbf{r}'', \ldots$ get their values DIRECTLY from s.

Now, *in the RHS of (4)* $\mathbf{p}$ gets the value $\overline{s}(B)$, while $\mathbf{q}, \mathbf{r}, \mathbf{r}', \mathbf{r}'', \ldots$ STILL get their values DIRECTLY from s.

► But $\overline{s}(A) = \overline{s}(B)$.

So both the lhs and rhs of (4) end up with the same truth value after the indicated substitutions.

In short, the equivalence is true. □

We can now prove:

1.3 Metatheorem. *Boolean logic is Sound, that is, (1) on p.1 holds.*

Proof. By induction on the length of proof, n, needed to obtain $\Gamma \vdash A$ we prove

$$\Gamma \models_{taut} A \tag{$\dagger$}$$

So pick a state s that satisfies Γ. (‡)

1. *Basis*. $n = 1$. Then we have just A in the proof.

   If $A \in \Lambda$, then it is a tautology, so in particular is true under s. We have (†).

   If $A \in \Gamma$, then s satisfies A. Again we have (†).

   I.H. Assume for all proofs of length $\leq n$.

   I.S. Prove the theorem in the case (†) needed a proof of length $n + 1$:

$$\underbrace{\overbrace{\ldots}^{length\ =n}, A}_{length\ =n+1}$$

   Now if A is in $\Lambda \cup \Gamma$ we are back to the Basis. Done.

If not

- Case where A is the result of *EQN* on X and $X \equiv Y$ that are in the "...-area".
  By the I.H. s satisfies X and $X \equiv Y$ hence, by the Lemma, satisfies A.
- Case where A is the result of *LEIB* on $X \equiv Y$ that are is the "...-area".
  By the I.H. s satisfies $X \equiv Y$ hence, by the Lemma, satisfies A. □

1.4 Corollary. *If $\vdash A$ then $\models_{taut} A$. A is a tautology.*

Proof. $\Gamma = \emptyset$ here. BUT, EVERY state s satisfies THIS Γ, vacuously:

Indeed, to prove that some state v *does NOT* you *NEED* an $X \in \emptyset$ such that $\overline{v}(X) = \mathbf{f}$; *IMPOSSIBLE*.

Hence every state satisfies A. Thus a $\models_{taut} A$. □

1.5 Example. Soundness allows us to disprove formulas: To show they are NOT theorems.

- $\vdash \mathbf{p}$ is false. If this were true, then $\mathbf{p}$ would be a tautology!
- $\vdash \bot$ is false! Because $\bot$ is not a tautology!
- $p \vdash p \wedge q$ is false. Because if it were true I'd have to have $p \models_{taut} p \wedge q$.
  Not so: Take a state s such that $s(p) = \mathbf{t}$ and $s(q) = \mathbf{f}$. □

2. Completeness of Boolean logic ("Post's Theorem")

We prove here

(1) A weak form of Post's theorem: If Γ is finite and $\Gamma \models_{\text{taut}} A$, then $\Gamma \vdash A$

and derive as a corollary the *Deduction Theorem*:

(2) If $\Gamma, A \vdash B$, then $\Gamma \vdash A \to B$.

2.1. Some tools

We will employ the TWO results from class/text below:

2.1 Theorem. $\vdash \neg(C \vee D) \vee E \equiv (\neg C \vee E) \wedge (\neg D \vee E)$.

2.2 Theorem. $\neg C \vee E, \neg D \vee E \vdash \neg(C \vee D) \vee E$.

2.3 Main Lemma. *Suppose that A contains none of the symbols $\top, \bot, \rightarrow, \wedge, \equiv$. If $\models_{taut} A$, then $\vdash A$.*

Proof. *The proof is long but easy!*

Under the assumption, A is *an $\vee$-chain*, that is, it has the form

$$A_1 \vee A_2 \vee A_3 \vee \ldots \vee A_i \vee \ldots \vee A_n \qquad (1)$$

where none of the A_i has the form $B \vee C$.

In (1) we assume without loss of generality that $n > 1$, due to the axiom $X \vee X \equiv X$ —that is, *in the contrary case* we can use $A \vee A$ instead, which is a tautology as well.

Moreover, (1), that is A, is written in least parenthesised notation.

Let us call an A_i *reducible* iff it has the form $\neg(C \vee D)$ or $\neg(\neg C)$.

"Reducible", since A_i is not alone in the $\vee$-chain, will be synonymous to *simplifiable.*

Otherwise A_i is *irreducible. Not* simplifiable.

Thus, the only possible irreducible A_i have the form $\mathbf{p}$ or $\neg\mathbf{p}$ (where $\mathbf{p}$ is a variable).

We say that $\mathbf{p}$ "occurs positively in $\ldots \vee \mathbf{p} \vee \ldots$", while it "occurs negatively in $\ldots \vee \neg\mathbf{p} \vee \ldots$".

In, for example, $\mathbf{p} \vee \neg\mathbf{p}$ it occurs *both* positively and negatively.

By **definition** *we will say that A is irreducible iff* ***all*** *its A_i are.*

We define the *reducibility degree*, of EACH A_i —in symbols, $rd(A_i)$— to be the total number, counting repetitions of the $\neg$ and $\vee$ connectives in it, **not counting a possible leading** $\neg$.

The reducibility degree of the entire A is the sum of the reducibility degrees of all its A_i.

For example, $rd(p) = 0$, $rd(\neg p) = 0$, $rd(\neg(\neg p \vee q)) = 2$, $rd(\neg(\neg p \vee \neg q)) = 3$, $rd(\neg p \vee q) = 0$.

By induction on $rd(A)$ we now prove the main lemma, that $\vdash A$ on the stated hypothesis that $\models_{taut} A$.

For the *Basis*, let A be an *irreducible* tautology —so, $rd(A) = 0$.

It must be that A is a string of the form

"$\cdots \vee \mathbf{p} \vee \cdots \neg \mathbf{p} \vee \cdots$"

for some $\mathbf{p}$, otherwise,

if no $\mathbf{p}$ appears *both* "positively" and "negatively",

then we can find a truth-assignment that makes A false ($\mathbf{f}$) —a contradiction to its tautologyhood.

To see that we can do this, just assign $\mathbf{f}$ to $\mathbf{p}$'s that occur ***positively only***, and $\mathbf{t}$ to those that occur ***negatively only***.

Now

$$
\begin{aligned}
& A \\
\Leftrightarrow & \Big\langle \text{commuting the terms of an } \vee\text{-chain} \Big\rangle \\
& \mathbf{p} \vee \neg\mathbf{p} \vee B \quad (\text{what is "}B\text{"?}) \\
\Leftrightarrow & \Big\langle \text{Leib + axiom + Red. } \top \text{ META; Denom: } \mathbf{r} \vee B\text{; fresh } \mathbf{r} \Big\rangle \\
& \top \vee B \quad \text{bingo!}
\end{aligned}
$$

Thus $\vdash A$, which settles the *Basis*-case: $rd(A) = 0$.

We now argue the case where $rd(A) = m+1$, on the I.H. that for any formula Q with $rd(Q) \leq m$, we have that $\models_{taut} Q$ implies $\vdash Q$.

By commutativity (symmetry) of "$\vee$", let us assume without restricting generality that $rd(A_1) > 0$.

We have two cases:

(1) A_1 is the string $\neg\neg C$, **hence** A **has the form** $\neg\neg C \vee D$.

Clearly $\models_{taut} C \vee D$ as well.

Moreover, $rd(C \vee D) < rd(\neg\neg C \vee D)$, hence (by I.H.)

$$\vdash C \vee D \qquad (\dagger)$$

But,

$$\neg\neg C \vee D$$
$$\Leftrightarrow \Big\langle \text{Leib } + \vdash \neg\neg X \equiv X;\ \text{Denom: } \mathbf{r} \vee D;\ \text{fresh } \mathbf{r} \Big\rangle$$
$$C \vee D \quad (\dagger) \text{ above is "bingo"!}$$

Hence, $\vdash \neg\neg C \vee D$, that is, $\vdash A$ in this case.

Lecture #12, Oct. 23

One more case to go:

(2) A_1 is the string $\neg(C \vee D)$, **hence** A **has the form** $\neg(C \vee D) \vee E$**.**

$$\text{We want: } \vdash \neg(C \vee D) \vee E \qquad (i)$$

By 2.1 and from $\models_{taut} \neg(C \vee D) \vee E$ —this says $\models_{taut} A$— we immediately get that

$$\models_{taut} \neg C \vee E \qquad (ii)$$

and

$$\models_{taut} \neg D \vee E \qquad (iii)$$

from the $\equiv$ and $\wedge$ truth tables.

Since the rd of each of (ii) and (iii) is $< rd(A)$, the I.H. yields $\vdash \neg C \vee E$ AND $\vdash \neg D \vee E$.

Apply the RULE 2.2 to the above two theorems to get (i).

We are done, **except for one small detail:**

If we had changed the "original" A into $A \vee A$ (cf. the "without loss of generality" remark just below (1) on p.7), then all we proved above is $\vdash A \vee A$.

The *contraction* rule from (e-)Class, Notes, and Text then yield $\vdash A$. □

But ALL this only proves "$\models_{taut} A$ implies $\vdash A$"

when A does *not* contain $\wedge, \rightarrow, \equiv, \bot, \top$.

WHAT IF IT DOES?

We are now removing the restriction on A regarding its connectives and constants:

2.4 Metatheorem. (Post's Theorem) *If* $\models_{taut} A$*, then* $\vdash A$*.*

Proof. First, we note the following *theorems* stating equivalences, *where* $\mathbf{p}$ *is fresh for* A.

The proof of the last one is in the notes and text but it was too long (but easy) to cover in class.

$$\begin{aligned}
&\vdash \top \equiv \neg\mathbf{p} \vee \mathbf{p}\\
&\vdash \bot \equiv \neg(\neg\mathbf{p} \vee \mathbf{p})\\
&\vdash C \rightarrow D \equiv \neg C \vee D\\
&\vdash C \wedge D \equiv \neg(\neg C \vee \neg D)\\
&\vdash (C \equiv D) \equiv ((C \rightarrow D) \wedge (D \rightarrow C))
\end{aligned} \tag{2}$$

Using (2) above, we eliminate, in order, all the $\equiv$, then all the $\wedge$, then all the $\rightarrow$ and finally all the $\bot$ and all the $\top$.

Let us assume that our process eliminates **one** unwanted symbol at a time.

This leads to *the Equational Proof below*.

Starting from A we will generate a sequence of formulae

$$F_1, F_2, F_3, \ldots, F_n$$

where F_n contains no $\top, \bot, \wedge, \rightarrow, \equiv$.

I am using here F_1 as an alias for A. We will also give to F_n an alias A'.

$$
\begin{aligned}
& A \\
\Leftrightarrow & \Big\langle \text{Leib from (2)} \Big\rangle \\
& F_2 \\
\Leftrightarrow & \Big\langle \text{Leib from (2)} \Big\rangle \\
& F_3 \\
\Leftrightarrow & \Big\langle \text{Leib from (2)} \Big\rangle \\
& F_4 \\
& \vdots \\
\Leftrightarrow & \Big\langle \text{Leib from (2)} \Big\rangle \\
& A'
\end{aligned}
$$

Thus, $\vdash A' \equiv A$ $\quad(*)$

By **soundness**, we also have $\models_{taut} A' \equiv A$ $\quad(**)$

So, say $\models_{taut} A$. By $(**)$ we have $\models_{taut} A'$ as well, and by the Main Lemma 2.3 we obtain $\vdash A'$.

By $(*)$ and Eqn we get $\vdash A$. □

Post's theorem is the "*Completeness Theorem*"[†] of Boolean Logic.

It shows that the syntactic manipulation apparatus — proofs— DOES certify the "whole truth" (tautologyhood) in the Boolean case.

[†]Which is really a *Meta*theorem, right?

2.5 Corollary. *If* $A_1, \ldots, A_n \models_{taut} B$*, then* $A_1, \ldots, A_n \vdash B$*.*

Proof. It is an easy semantic exercise to see (see the special case in Problem Set #1, Fall 2020) that

$$\models_{taut} A_1 \to \ldots \to A_n \to B$$

By 2.4,

$$\vdash A_1 \to \ldots \to A_n \to B$$

hence (hypothesis strengthening)

$$A_1, A_2 \ldots, A_n \vdash A_1 \to A_2 \to \ldots \to A_n \to B \qquad (1)$$

Applying modus ponens n times to (1) we get

$$A_1, \ldots, A_n \vdash B$$

□

The above corollary is very convenient.

It says that every (correct) schema $A_1, \ldots, A_n \models_{taut} B$ leads to a *derived rule of inference*, $A_1, \ldots, A_n \vdash B$.

In particular, combining with the transitivity of $\vdash$ metatheorem, we get

2.6 Corollary. *If* $\Gamma \vdash A_i$*, for* $i = 1, \ldots, n$*, and if* $A_1, \ldots, A_n \models_{taut} B$*, then* $\Gamma \vdash B$*.*

Thus —*unless otherwise requested!*— we can, from now on, *rigorously* mix syntactic with semantic justifications of our proof steps.

For example, we have at once $A \wedge B \vdash A$, because (trivially) $A \wedge B \models_{taut} A$ (compare with our earlier, much longer, proof given in class).

3. Deduction Theorem, Proof by Contradiction

3.1 Metatheorem. (The Deduction Theorem) *If* $\Gamma, A \vdash B$, *then* $\Gamma \vdash A \to B$, *where "*Γ, A*" means "all the assumptions in* Γ*, plus the assumption* A*"* (in set notation this would be $\Gamma \cup \{A\}$).

Proof. Let $G_1, \ldots, G_n \subseteq \Gamma$ be a *finite* set of formulae used in a Γ, A-proof of B.

Thus we also have $G_1, \ldots, G_n, A \vdash B$.

By *soundness*, $G_1, \ldots, G_n, A \models_{taut} B$.
But then,

$$G_1, \ldots, G_n \models_{taut} A \to B$$

By 2.5, $G_1, \ldots, G_n \vdash A \to B$ and hence $\Gamma \vdash A \to B$ by hypothesis strengthening. □

The mathematician, or indeed the mathematics practitioner, uses the Deduction theorem all the time, without stopping to think about it. Metatheorem 3.1 above makes an honest person of such a mathematician or practitioner.

The everyday "style" of applying the Metatheorem goes like this:

Say we have all sorts of assumptions and we want, *under these assumptions*, to "prove" that "if A, then B" (verbose form of "$A \to B$").

We start by ***adding*** A *to our assumptions*, often with the words, "*Assume* A". We then proceed and prove *just* B (not $A \to B$), and at that point we rest our case.

Thus, we may view an application of the Deduction theorem as a simplification of the proof-task. It allows us to "split" an implication $A \to B$ that we want to prove, moving its premise to join our other assumptions. We now have to prove a *simpler formula*, B, with the help of *stronger* assumptions (that is, all we knew so far, plus A). That often makes our task so much easier!

An Example. Prove

$$\vdash (A \to B) \to A \vee C \to B \vee C$$

By DThm, suffices to prove

$$A \to B \vdash A \vee C \to B \vee C$$

instead.

Again By DThm, suffices to prove

$$A \to B, A \vee C \vdash B \vee C$$

instead.

Let's do it:

1.	$A \to B$	$\langle$hyp$\rangle$
2.	$A \vee C$	$\langle$hyp$\rangle$
3.	$A \to B \equiv \neg A \vee B$	$\langle \neg\vee$ thm$\rangle$
4.	$\neg A \vee B$	$\langle 1 + 3 +$ Eqn$\rangle$
5.	$B \vee C$	$\langle 2 + 4 +$ Cut$\rangle$

□

3.2 Definition. A set of formulas Γ is *inconsistent* or *contradictory* iff Γ *proves every* A *in* WFF. □

Why "contradictory"? For if Γ proves everything, then it also proves $\mathbf{p} \land \neg\mathbf{p}$.

3.3 Lemma. Γ *is inconsistent iff* $\Gamma \vdash \bot$

Proof. only if-part. If Γ is as in 3.2, then, in particular, it proves $\bot$ since the latter is a well formed formula.

if-part. Say, conversely, that we have

$$\Gamma \vdash \bot \tag{9}$$

Let now A be any formula in WFF whatsoever. We have

$$\bot \models_{taut} A \tag{10}$$

Pause. Do you believe (10)?

By Corollary 3.4, $\Gamma \vdash A$ follows from (9) and (10). □

3.4 Metatheorem. (Proof by contradiction) $\Gamma \vdash A$ *iff* $\Gamma \cup \{\neg A\}$ *is inconsistent.*

Proof. if-part. So let (by 3.3)

$$\Gamma, \neg A \vdash \bot$$

Hence

$$\Gamma \vdash \neg A \to \bot \tag{1}$$

by the Deduction theorem. However $\neg A \to \bot \models_{taut} A$, hence, by Corollary 2.6 and (1) above, $\Gamma \vdash A$.

only if-part. So let

$$\Gamma \vdash A$$

By hypothesis strengthening,

$$\Gamma, \neg A \vdash A \tag{2}$$

Moreover, trivially,

$$\Gamma, \neg A \vdash \neg A \tag{3}$$

Since $A, \neg A \models_{taut} \perp$, (2) and (3) yield $\Gamma, \neg A \vdash \perp$ via Corollary 2.6, and we are done by 3.3. □

3.4 legitimises the tool of “proof by contradiction” that goes all the way back to the ancient Greek mathematicians: To prove A assume instead the “opposite”, $\neg A$. Proceed then to obtain a contradiction. This being accomplished, it is as good as having proved A.