Chapter 1

A Weak Post's Theorem and the Deduction Theorem Retold

This note retells

(1) A weak form of Post's theorem: If $\underline{\Gamma \text{ is finite}}$ and $\Gamma \models_{\text{taut}} A$, then $\Gamma \vdash A$. This is adequate <u>in practice</u>. It also derives as a corollary the Deduction Theorem:

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

1.1. Some tools

We will employ below the following Lemma.

1.1.1 Lemma. $\neg A \vee C, \neg B \vee C \vdash \neg(A \vee B) \vee C$.

Proof. Here $\Gamma = \{\neg A \vee C, \neg B \vee C\}$.

$$
\begin{aligned}
& \neg(A \vee B) \vee C \\
\Leftrightarrow & \left\langle \text{Leib: } r \vee C + \text{deMorgan} \right\rangle \\
& (\neg A \wedge \neg B) \vee C \\
\Leftrightarrow & \left\langle \text{distrib. of } \vee \text{ over } \wedge \right\rangle \\
& (\neg A \vee C) \wedge (\neg B \vee C) \\
\Leftrightarrow & \left\langle \text{Leib: } r \wedge (\neg B \vee C), \text{ and } \Gamma \vdash \neg A \vee C \equiv \top \right\rangle \\
& \top \wedge (\neg B \vee C) \\
\Leftrightarrow & \left\langle \text{by } \vdash \top \wedge X \equiv X \right\rangle
\end{aligned}
$$

$$\neg B \vee C \quad \text{bingo!}$$ □

1.1.2 Corollary. $\vdash \neg(A \vee B) \vee C \equiv (\neg A \vee C) \wedge (\neg B \vee C)$.

Proof. In the previous proof just use the first five lines (first two $\Leftrightarrow$). □

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

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

$$A_1 \vee A_2 \vee A_3 \vee \ldots \vee A_i \vee \ldots \vee A_n \tag{1}$$

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 by virtue of the axiom 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 $\neg(\neg C)$. Otherwise it is *irreducible*. Thus, the only possible irreducible A_i have the form p or $\neg p$ (where p is a variable). We say that p "occurs positively in $\ldots \vee p \vee \ldots$", while it "occurs negatively in $\ldots \vee \neg p \vee \ldots$". In, for example, $p \vee \neg p$ it occurs *both* positively and negatively.

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

We define the *reducibility degree*, of A_i—in symbols, $rd(A_i)$—to be the number of $\neg$ or $\vee$ connectives in it, *not counting a possible leading* $\neg$. The reducibility degree of 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, on the stated hypothesis that $\models_{taut} A$.

For the basis, let A be an irreducible tautology ($rd(A) = 0$). It must be that A is a string of the form "$\cdots \vee p \vee \cdots \neg p \vee \cdots$" for some p, otherwise, if no 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 p's that occur ***positively only***, and $\mathbf{t}$ to those that occur ***negatively only***.

Now

$$\begin{array}{ll} & A \\ \Leftrightarrow & \big\langle \text{commuting terms of an } \vee\text{-chain} \big\rangle \\ & p \vee \neg p \vee B \quad (\text{what is ``}B\text{''?}) \end{array}$$

$$\Leftrightarrow \Big\langle \text{Leib: } r \vee B + \text{excluded middle, plus Red. } \top \text{ metathm.} \Big\rangle$$
$$\top \vee B \quad \text{bingo!}$$

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

We now argue the case where $rd(A) = n + 1$, on the I.H. that for any formula Q with $rd(Q) \leq n$, 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 $\models_{taut} C \vee D$. Moreover, $rd(C \vee D) < rd(\neg\neg C \vee D)$, hence

$$\vdash C \vee D$$

by the I.H. But,

$$\neg\neg C \vee D$$
$$\Leftrightarrow \Big\langle \text{Leib: } r \vee D + \vdash \neg\neg X \equiv X \Big\rangle$$
$$C \vee D \quad \text{bingo!}$$

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

One more case to go:

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

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

By 1.1.2 and from $\models_{taut} \neg(C \vee D) \vee E$—this says $\models_{taut} A$—we immediately get that

$$\models_{taut} \neg C \vee E \tag{ii}$$

and

$$\models_{taut} \neg D \vee E \tag{iii}$$

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

Since the rd of each of (ii) and (iii) is smaller than that of A, by I.H. we obtain

$$\vdash \neg C \vee E$$

and

$$\vdash \neg D \vee E$$

which by 1.1.1 yield the validity of (i).

We are done, except for one small detail: If we had changed an "original" A into $A \vee A$ (cf. the "without loss of generality" remark below (1)), then we have proved $\vdash A \vee A$. The idempotent axiom and Eqn then yield $\vdash A$. □

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

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

Proof. First, we note the following equivalences. The ones to the left of "also" follow from the ones to the right by soundness. The ones to the right are known from class (or follow trivially thereof): The first is the Excluded Middle Axiom augmented by "Redundant $\top$". The one below it follows from simple manipulation[†] and $\vdash \bot \equiv \neg\top$. All the others have been explicitly covered.

$$
\begin{aligned}
\models_{taut} \top \equiv \neg p \vee p, &\text{ also } \vdash \top \equiv \neg p \vee p \\
\models_{taut} \bot \equiv \neg(\neg p \vee p), &\text{ also } \vdash \bot \equiv \neg(\neg p \vee p) \\
\models_{taut} C \to D \equiv \neg C \vee D, &\text{ also } \vdash C \to D \equiv \neg C \vee D \\
\models_{taut} C \wedge D \equiv \neg(\neg C \vee \neg D), &\text{ also } \vdash C \wedge D \equiv \neg(\neg C \vee \neg D) \\
\models_{taut} (C \equiv D) \equiv ((C \to D) \wedge (D \to C)), &\text{ also } \vdash (C \equiv D) \equiv ((C \to D) \wedge (D \to C))
\end{aligned}
\tag{1.1}
$$

Using the I.1 above, we eliminate, *in order*, all the $\equiv$, then all the $\wedge$, then all the $\to$ and finally all the $\bot$ and all the $\top$. Let us assume that our process eliminates ***one*** unwanted symbol at a time. Thus, starting from A we will generate a sequence of formulae

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

where F_n contains no $\top, \bot, \wedge, \to, \equiv$. I am using here F_1 as an alias for A. We will also give to F_n the alias A'.

Now in view of the provable equivalences of I.1, each transformation step is the result of a Leib application, thus we have

$$
\begin{array}{ll}
 & F_1 \\
\Leftrightarrow & \Big\langle \text{Leib from I.1} \Big\rangle \\
 & F_2 \\
\Leftrightarrow & \Big\langle \text{Leib from I.1} \Big\rangle \\
 & F_3 \\
\Leftrightarrow & \Big\langle \text{Leib from I.1} \Big\rangle \\
 & F_4 \\
 & \vdots \\
\Leftrightarrow & \Big\langle \text{Leib from I.1} \Big\rangle \\
 & F_n
\end{array}
$$

Hence,

$$\vdash A \equiv A' \tag{1}$$

[†] Recall that $\vdash \neg(A \equiv B) \equiv \neg A \equiv B$ and also $\vdash \neg(A \equiv B) \equiv A \equiv \neg B$.

By soundness, I also get (from (1))

$$\models_{taut} A \equiv A' \tag{2}$$

Now, we are given that $\models_{taut} A$. By (2) and the fact that Eqn propagates truth I get $\models_{taut} A'$. As A' is free from $\top, \bot, \wedge, \to, \equiv$, 1.1.3 yields $\vdash A'$. Eqn and (1) yield $\vdash A$. □

Post's theorem is often called the "Completeness Theorem"[†] of Propositional Calculus. It shows that the syntactic manipulation apparatus completely captures the notion of "truth" (tautologyhood) in the propositional case.

1.1.5 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 that the hypothesis yields (indeed we have done so in class) that

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

By 1.1.4,

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

hence (by Hypothesis Strengthening)

$$A_1, \ldots, A_n \vdash A_1 \to \ldots \to A_n \to B \tag{1}$$

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 any (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 known from class and text, we get

1.1.6 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).

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

1.2. Deduction Theorem, Proof by Contradiction

1.2.1 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. Assume then $\Gamma, A \vdash B$. Let

$$A_1, A_2, \ldots, A_n$$

be a Γ, A-proof that contains B. Since it is a finite sequence it can only contain a subset of Γ: $\{G_1, \ldots, G_m\} \subseteq \Gamma$.

Thus,

$$G_1, \ldots, G_m, A \vdash B \text{ as well} \tag{1}$$

(1) and soundness yield $G_1, \ldots, G_m, A \models_{taut} B$. The latter yields

$$G_1, \ldots, G_m \models_{taut} A \to B \tag{2}$$

Indeed, a state v that makes the lhs of (2) $\mathbf{t}$ should make the rhs $\mathbf{t}$: If A is $\mathbf{f}$, then there is no work to do; if A is $\mathbf{t}$, then by (1), B is $\mathbf{t}$, thus $A \to B$ is $\mathbf{t}$. By 1.1.5, $G_1, \ldots, G_m \vdash A \to B$. By Hypothesis Strengthening, $\Gamma \vdash A \to B$. □

It is noteworthy (and very easy to establish) that the opposite implication of 1.2.1 holds:

1.2.2 Proposition. *If* $\Gamma \vdash A \to B$*, then* $\Gamma, A \vdash B$*.*

Proof. By Hypothesis Strengthening, $\Gamma, A \vdash A \to B$. By MP, we obtain $\Gamma, A \vdash B$. □

The mathematician, or indeed the mathematics practitioner, uses the Deduction theorem all the time, without stopping to think about it. Metatheorem 1.2.1 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 (nonlogical axioms) 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!

1.2.3 Definition. A set of formulas Γ is *inconsistent* or *contradictory* iff Γ *proves every formula* A.

The following Lemma justifies the term “contradictory” for a Γ such as described above:

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

Proof. only if-part. If Γ is as in 1.2.3, then in particular it proves $\bot$ since the latter is a wff.

if-part. Say, conversely, that we have

$$\Gamma \vdash \bot \tag{1}$$

Let now A be any formula whatsoever. We have

$$\bot \models_{taut} A \tag{2}$$

Pause. Do you believe (2)?

By Corollary 1.1.6, $\Gamma \vdash A$ follows from (1) and (2). $\square$

Why “contradictory”? For example, because we know that $\models_{taut} \bot \equiv A \wedge \neg A$, and hence (1.1.4) $\vdash \bot \equiv A \wedge \neg A$.

1.2.5 Metatheorem. (Proof by contradiction) $\Gamma \vdash A$ *iff* $\Gamma, \neg A$ *is inconsistent.*

Proof. By 1.2.4, $\Gamma, \neg A$ is inconsistent iff

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

By 1.2.1 and 1.2.2, (1) is equivalent to

$$\Gamma \vdash \neg A \to \bot \tag{2}$$

But

$$\begin{aligned}
& \neg A \to \bot \\
\Leftrightarrow & \left\langle \text{known thm} \right\rangle \\
& \neg\neg A \vee \bot \\
\Leftrightarrow & \left\langle \text{known thm} \right\rangle \\
& \neg\neg A \\
\Leftrightarrow & \left\langle \text{double neg} \right\rangle \\
& A
\end{aligned}$$

Thus, (2)—and hence (1)—is equivalent to $\Gamma \vdash A$. $\square$

Metatheorem 1.2.5 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.