Notes on Post's paper

Randall Holmes

October 15, 2020

1 Introduction

I have never read this paper before. I think it has a significant place in the history of the subject (it dates from 1921). It is reputed to contain the first proof of the completeness of propositional logic (in the particular form axiomatized in Principia Mathematica, but carried out in a very general way which can be used for other axiomatizations).

It is manifestly related to Russell (and gives me a chance to keep you out of reading too much of Principia Mathematica, which is a hard read). Some of the terminology should also remind you of Frege to some extent.

The point he makes at the bottom of the first page is an important one. Earlier treatments of symbolic logic informally used in their proofs the very propositions whose formal statements they try to prove. In this paper, Post keeps the sentences of propositional logic that we are reasoning about quite distinct from the language in which we are actually conducting our reasoning (though the latter may have the same basic ideas "or" and "not" appearing in it, it is only the appearances of or and not in the expressions that we are reasoning about that we undertake to prove theorems about).

Post says clearly that the theorems of this paper are not theorems in the propositional logic which is their subject. The assertions of propositional logic are theorems in one sense: the main theorems in this paper are not assertions of propositional logic, but assertions of a mathematical theory with more content (arithmetic, or set theory). We will talk later in this class, at least briefly, about what theory Post might be understood to be working in.

2 All the elementary propositions

Post describes the sytem of Principia Mathematica as having as its subject a certain class of expressions. We supply infinitely many propositional variables $p_1, p_2, p_3, \ldots, q_1, q_2, q_3, \ldots, r_1, r_2, r_3, \ldots$ I will assume that these are exactly the ones we have, for concreteness: p, q, r suffixed with numerals.

He then says that we have two elementary function $\sim P$ and $(P \vee Q)$ which can be used to construct further elementary propositions. I think that we are to view these as functions in a rather Fregean way: what is mean is simply that the letters P and Q may freely be replaced with propositions (including complex ones). Parentheses may be dropped where no ambiguity is introduced. So, for example, we are given p_1, q_7, r_{17} as specific functions. We can construct $\sim q_7$ as the negation of a previously given expression. We can construct $\sim q_7 \vee r_{17}$ as the disjunction of two previously given propositions. We can construct $p_1 \vee (\sim q_7 \vee r_{17})$ as the disjunction of two previous given propositions. In this way, we can construct ever more complex propositions.

I use the letters p, q, t_i for variables ranging over atomic propositions (the p_i's, q_i's, and r_i's). Post is less careful about drawing such a distinction, which I think is needed. I use capital letters (such as P, Q in the paragraph above where Post uses p, q) as variables standing for any elementary proposition at all, simple or complex. Again, I think Post is less careful about a very important distinction here.

This is a description of the space of all possible elementary propositions.

3 The asserted elementary propositions (the theorems of propositional logic)

What really interests us is the space of propositions $\vdash P$ which are asserted as theorems. Here I am following my own rule, which is that when I introduce a capital letter, this stands for an undetermined complex elementary proposition; if I use p it varies over p_i's, q_i's, and r_i's.

Post gives a definition of the set of all elementary propositions $\vdash P$ to be asserted.

He first gives rules for deriving new theorems from old, then he gives the theorems we start with.

II. If we have $\vdash f(p)$ (this standing for any expression containing p, which

is any variable) then for any variable q we have $\vdash f(q)$ and $\vdash f(\sim q)$, and for any variables q and r we have $\vdash f(q \vee r)$.

The effect of this is that we can replace any variable p with any complex elementary proposition A throughout an asserted $\vdash P$ to get another asserted $\vdash P'$.

We may in practice need to apply this rule several times to substitute a complex expression A for p. Post never actually exhibits this process, but we give an example.

Start with $\vdash p_1 \vee \sim p_1$ (assuming that we have already derived this).

We can replace p_1 by rule II uniformly with $q_1 \vee r_1$.

Thus we have $\vdash (q_1 \vee r_1) \vee \sim (q_1 \vee r_1)$.

Now we can replace r_1 with $\sim r_1$.

Thus we have $\vdash (q_1 \vee \sim r_1) \vee \sim (q_1 \vee \sim r_1)$.

Notice that we replaced p_1 uniformly with $q_1 \vee \sim r_1$, which is more complex than the expressions that the text of rule II tell us explicitly can replace a variable. In fact, we can replace a variable with any elementary proposition by repeated applications of the rule, and Post always presumes this.

III. If we have $\vdash P$ and $\vdash \sim P \vee Q$, we have also $\vdash Q$. This is an implementation of the familiar rule of *modus ponens*, as one can see if one recalls that implication $P \supset Q$ is defined by Russell as $\neg P \vee Q$.

Now is as good a time as any to remark that I am more used to writing $\neg P$ for negation and $P \rightarrow Q$ for implication, and if either of these symbols appear they should be understood as meaning the same thing as $\sim P$ and $P \supset Q$, respectively. Moroever, you are welcome to use these symbols if you prefer them or cannot help writing them.

IV: Where p, q, r are any variables, the following are initial assertions (axioms):

1. $\sim (p \vee p) \vee p$
2. $\sim q \vee (p \vee q)$
3. $\sim (p \vee q) \vee (q \vee p)$
4. $\sim [p \vee (q \vee r)] \vee (q \vee (p \vee r))$

5. $\sim (\sim q \vee r) \vee (\sim (p \vee q) \vee (p \vee r))$

I write the axioms in a form using parentheses in a style familiar to you (brackets being an acceptable alternative, and I decided I liked Post's brackets in the fourth axiom), with every needed parenthesis being written except those on the outside. There is no need to put negations in parentheses: parentheses or brackets are written only to signal disjunctions.

I do not use the device of dots which Post inherits from its inventors (the authors of Principia Mathematica) but it might be good to have some explanation of them for reading Post's text. $P.Q$ is used simply to mean what we would write $P \wedge Q$, defined as $\sim (\sim P \vee \sim Q)$: I will use dots for conjunctions, though I might use $\wedge$ as well and you are welcome to. A dot or group of dots next to a binary connective is a left or right parenthesis (as appropriate) for which the appropriate right or left parenthesis (respectively) is not written: it will appear as far to the right (or left) as possible with the proviso that one stops before a group of the same number or a larger number of dots, and one must have sensible relationships to any explicit parentheses that are present. It is a tricky device for those not accustomed to it. I'll talk through producing undotted forms of the axioms, and I will be happy to undot any expressions in the paper on request. You are not required to write dots.

The asserted propositions are exactly the ones which can be derived from the axioms by the rules above.

4 Truth table methods

Post introduces the truth values + and −, and is at pains to say that he is simply using these as formal symbols.

He could have inductively defined the truth table of a function $f(t_1, \ldots, t_n)$ (by which he simply means an expression with distinct atomic propositions $t_1, \ldots, t_n$ in it, and with no other atomic propositions in it; I have noted above that I use t_i's as variables ranging over the constant atomic expressions p_i, q_i, r_i; Post is not careful about drawing such a distinction). The table will have 2^n rows, each row beginning with one of the 2^n strings of n

+'s and −'s. Each row will contain one more symbol, which we define by recursion on the structure of $f(t_1, \ldots, t_n)$:

if $f(t_1, \ldots, t_n)$ is an atomic elementary proposition, it will be one of the t_i's, and the last sign in each row will be the same as the ith sign in the row.

If the function $f(t_i, \ldots, t_n)$ is of the form $\neg f_1(t_1, \ldots, t_n)$, first construct the truth table of $f_1(t_1, \ldots, t_n)$: the last sign of each row in the table of f will be $-$ if the last sign of the corresponding row in the table for f_1 is $+$, and $+$ if the last sign of the corresponding row in the table for f_1 is $-$.

If the function $f(t_1, \ldots, t_n)$ is of the form $f_1(t_1, \ldots, t_n) \vee f_2(t_1, \ldots, t_n)$, then compute the tables for f_1 and f_2: the last sign in each row of the table for f will be $-$ if the last signs of the corresponding rows in the tables for f_1 and f_2 are both $-$, and otherwise will be $+$.

Actually our definition is more modern than his, but may make it clearer that the truth table of a function $f(t_1, \ldots, t_n)$ can be computed mechanically from the expression $f(t_1, \ldots, t_n)$ without naively reading $\vee$ and $\sim$ as the words "or" and "not" of the language we are speaking as we carry out the proof.

I will talk through this nasty-looking formal definition in class, and point out that it actually corresponds precisely to a procedure that students can reasonably use to write down truth tables. In fact, there is clear evidence in the paper that this is how Post was thinking of it, too.

Post then proves a theorem which is important. Every possible truth table is actually the truth table of some proposition.

He proves this by mathematical induction on the order of the truth table (which is one less than the number of symbols in a row: it is the same as the number of variables used).

The four order one tables are handled by functions $p \vee p$, $\neg p$, $p \vee \sim p$, and $\sim (p \vee \sim p)$, as you can demonstrate by building these truth tables.

He then points out that if we have got functions with each order m table, we can construct a function with any desired order $m + 1$ table as follows:

From the order $m+1$ table T you are given, construct two order m tables T^+ and T^-. T^+ is obtained by deleting all the rows from the table which have - in column $m + 1$, then deleting column $m + 1$. T^- is obtained by deleting all the rows from the table which have $+$ in column $m + 1$, then deleting column $m + 1$. The idea is to replace t_{m+1} with either a true statement or a false statement. By inductive hypothesis we have $f_1(t_1, \ldots, t_m)$ with table T^+ and $f_2(t_1, \ldots, t_m)$ with table T^-.

Post of course doesn't use the notations T^+ and T^-. But I am more

explicitly defining the exact operation he uses.

Post then says that it is easy to see that

$$(t_{m+1}.f_1(t_1,\ldots,t_m) \vee (\sim t_{m+1}).f_2(t_1,\ldots.t_m)$$

has T as its table.

One might actually have a better chance of directly verifying Post's last assertion using my formal definition of the truth table of an expression above.

I went through some explicit examples of this procedure in lecture.

I will give a simpler way to produce a function realizing any truth table next time.

5 Discussion of Oct 7

5.1 A sample proof in Post's system

We derive $\vdash p \supset p$ in Post's system. Implication is a defined concept: we are actually deriving $\sim p \vee p$.

1. $\vdash \sim q \vee (p \vee q)$ an axiom (IV number 2)
2. $\vdash \sim [p \vee (q \vee r)] \vee (q \vee (p \vee r))$ an axiom (IV number4)
3. $\vdash \sim [\sim q \vee (p \vee q)] \vee (p \vee (\sim q \vee q))$ II applied to line 2: replace p with $\sim q$, q with p, r with q.
4. $\vdash p \vee (\sim q \vee q)$ III line 1, line 3
5. $\vdash \sim [\sim q \vee (p \vee q)] \vee (\sim q \vee q)$ II line 4: replace p with $\sim [\sim q \vee (p \vee q)]$
6. $\vdash \sim q \vee q$ III 1,5
7. $\vdash \sim p \vee p$ II line 6, replace q with p
8. $\vdash p \supset p$ line 7, definition of $\supset$

6 Another way to get an assertion with a given truth table

We illustrate by example another general method of getting an expression with a desired truth table.

p	q	r	???
$+$	$+$	$+$	$-$
$+$	$+$	$-$	$+$
$+$	$-$	$+$	$+$
$+$	$-$	$-$	$-$
$-$	$+$	$+$	$-$
$-$	$+$	$-$	$+$
$-$	$-$	$+$	$+$
$-$	$-$	$-$	$-$

Above I have given a truth table in the final column of which I have sprinked random $+$'s and $-$'s. There is a uniform way to write down an expression with this truth table, which I now demonstrate using ordinary logical notation.

$(p \wedge q \wedge \neg r)$ from row 2

$\vee(p \wedge \neg q \wedge r)$ from row 3

$\vee(\neg p \wedge q \wedge \neg r)$ from row 6

$\vee(\neg p \wedge \neg q \wedge r)$ from row 7

giving a complete expression $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$ with the given table.

This method will work for any table except one with a column of $-$'s on the right, which can be represented by $p \wedge \neg p$ (for example).

The expression obtained is in a very stereotyped form, being a disjounction (or statement) linking conjunctions (and statements) composed of atomic letters and negations of letters (such an expression is said to be in disjunctive normal form). In addition, each expression contains all three letters in use in a fixed order.

This method could be used to give an alternative proof of Post's theorem that there is an expression with any given truth table.

7 Boolean algebra

There is a presentation of propositional operations (which is at the same time a presentation of certain basic operations on sets) which supports computations which are involved in the motivation of Post's proof of his main theorem.

You may notice Post referring to disjunction (or) as "logical addition" and conjunction (and) as "logical multiplication". In boolean algebra, we write $x + y$ for $x \vee y$ and xy for $x \wedge y$ (and $\overline{x}$ for $\neg x$). The advantage of doing this is that we can present a set of computational rules which suggests a method of taking any expression of propositional logic and converting it to a form which represents its truth table, from which it is easy to see whether it is a theorem or not.

We also use 0 to stand for $-$ or false, and 1 to stand for $+$ or true.

Where we say one expression equals another, we say that they have the same truth table.

$$\begin{array}{cc}
x + y = y + x & xy = yx \\
(x + y) + z = x + (y + z) & (xy)z = x(yz) \\
x(y + z) = xy + xz & x + yz = (x + y)(x + z)^* \\
x + 0 = x & x1 = x \\
x + 1 = 1^* & x0 = 0 \\
x + x = x^* & xx = x^* \\
\overline{x + y} = \overline{x}\,\overline{y} & \overline{xy} = \overline{x} + \overline{y}
\end{array}$$

$$\overline{\overline{x}} = x$$

$$\begin{array}{cc}
x + \overline{x} = 1 & x\overline{x} = 0
\end{array}$$

These rules formally resemble algebraic rules for the usual addition and multiplication, though there are some surprises (marked with stars). The negation operation doesn't correspond to any standard arithmetic operation, so we do not star its formulas.

Most of these are common sense if we read addition as intended as "or", multiplication as "and", overstrike as negation, 0 as false and 1 as true.

Something analogous to ordinary algebraic expansion will reduce any expression to a disjunction of conjunctions. The letters can be put in standard order using commutativity and associativity. Repeated letters or negated letters can be shortend to one letter or negated letter ($xx = x, \overline{x}\,\overline{x} = \overline{x}$). Conjunctions with $x\overline{x}$ in them will convert to 0 and can be eliminated. If

a conjunction (such as xy) is missing a letter (such as z) we can add it: $xy = xy1 = xy(z + \overline{z}) = xyz + xy\overline{z}$. So algebraic procedures can convert any expression to the form that would be obtained from its truth table by the procedure of the previous section, and this form can be recognized as true if it contains all lines (and actually can then be reduced to 1 by a boolean algebra calculation: for example, $xy + x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = x(y + \overline{y}) + \overline{x}(y + \overline{y}) = x1 + \overline{x}1 = x + \overline{x} = 1$.)

It is useful to note that implication $x \rightarrow y$ is $\overline{x}y$ in Boolean algebra notation. This corresponds to Post's definition of $P \supset Q$ as $\sim P \vee Q$.

8 Where do these axioms come from? A kind of answer in the proof of the Deduction Theorem

I want to address the origin of the axiom set Post is using (which is originally from Russell and Whitehead, Principia Mathematica, 1910). The best way to see where they come from is to see what can be done with them.

8.1 Axioms and variants

1. $\sim (p \vee p) \vee p$
2. $\sim q \vee (p \vee q)$
3. $\sim (p \vee q) \vee (q \vee p)$
4. $\sim [p \vee (q \vee r)] \vee (q \vee (p \vee r))$
5. $\sim (\sim q \vee r) \vee (\sim (p \vee q) \vee (p \vee r))$

is the set of axioms as it appears in Post's paper. I remind you that $P \supset Q$ (which you may also write $P \rightarrow Q$, the familiar material conditional), is defined as $\sim P \vee Q$. We can rewrite the axioms as

1. $(p \vee p) \supset p$
2. $q \supset (p \vee q)$
3. $(p \vee q) \supset (q \vee p)$

4. $[p \vee (q \vee r)] \supset (q \vee (p \vee r))$

5. $(q \supset r) \supset ((p \vee q) \supset (p \vee r))$

6. Replacing p with $\sim p$ and applying the definition gives another form of 5:

   $(q \supset r) \supset ((\sim p \vee q) \supset (\sim p \vee r))$

   which is equivalent to

   $(q \supset r) \supset ((p \supset q) \supset (p \supset r))$

7. Similarly, replacing p with $\sim p$ in axiom 2 gives

   $q \supset (\sim p \vee q)$

   which is equivalent to

   $q \supset (p \supset q)$

8. Similarly, replace p, q with $\sim p, \sim q$ in axiom 4 to get

   $[\sim p \vee (\sim q \vee r)] \supset (\sim q \vee (\sim p \vee r))$

   which is equivalent to

   $[p \supset (q \supset r)] \supset (q \supset (p \supset r))$

Further notice that rule III (*modus ponens*) can be restated as allowing us to derive $\vdash Q$ from $\vdash P$ and $\vdash P \supset Q$.

8.2 State the deduction theorem and introduce notation $\vdash_P$

We state and start to prove the Deduction Theorem: if adding $\vdash P$ as an assumption allows us to derive $\vdash Q$, with the restriction on rule II that no substitutions are made for variables in P, then it is possible to derive $\vdash P \supset Q$ without any additional assumptions or restrictions. In other words, we are allowed to use the method: "suppose P for the sake of argument: if we can then derive Q, then $P \rightarrow Q$ must be true without any assumption.".

We introduce the abbreviation $\vdash_P Q$ for $\vdash P \supset Q$.

We have $\vdash_P P$: we showed $\vdash \sim P \vee P$ which is equivalent to $\vdash P \supset P$, above. If we have(1) $\vdash Q$, then we have (2) $\vdash Q \supset (P \supset Q)$ by the variant 7 of axiom 2 above, followed by rule II to put Q in place of q and P in place

of p. Then rule III applied to (1) and (2) gives us $\vdash P \supset Q$. Thus we have shown that if we have $\vdash Q$ we also have $\vdash_P Q$.

Suppose that we have $\vdash_P f(p)$, where p is a variable not appearing in P. Then we have $\vdash P \rightarrow f(p)$, from which by rule II we can derive $\vdash P \supset f(q)$ and $\vdash P \supset f(q \vee r)$ for any variables q and r, and so we can derive $\vdash_P f(q)$ and $\vdash_P f(q \vee r)$. Thus we have for $\vdash_P$ the ability to apply rule II just as for $\vdash$, as long as we make no substitution which changes P.

8.3 Lemma 1 and the rule of transitivity of implication

We now prove a lemma.

We have

(1) $(q \supset r) \supset ((p \supset q) \supset (p \supset r))$ variant 7 of axiom 5

(2) $[[q \supset r] \supset ([p \supset q] \supset [p \supset r])] \supset ([p \supset q] \supset ([q \supset r] \supset [p \supset r]))$ variant 8 of axiom IV with rule II applied, replacing p with $q \supset r$, q with $p \supset q$, and r with $p \supset r$ (note that these substitutions are being carried out simultaneously, not one after the other).

(Lemma 1) $([p \supset q] \supset ([q \supset r] \supset [p \supset r]))$ rule III (1),(2)

This lemma gives us a very useful rule. Suppose we have derived $\vdash A \supset B$ and $\vdash B \supset C$.

Then we have

(1) $\vdash A \supset B$ given

(2) $\vdash B \supset C$ given

(3) $\vdash (A \supset B) \supset ((B \supset C) \supset (A \supset C))$ rule II applied to Lemma 1

(4) $((B \supset C) \supset (A \supset C))$ III 1,3

(5) $\vdash A \supset C$ III 2,4

So from $\vdash A \supset B$ and $\vdash B \supset C$ we can derive $\vdash A \supset C$. Call this "transitivity of implication".

Simply the idea that from given rules we can derive new rules is of interest.

8.4 Lemma 2

We need to prove another lemma, which we will prove by a series of applications of our derived rule.

(1) $\vdash (\sim p \vee q) \supset (q \vee \sim p)$ rule II applied to axiom 2

(2) $\vdash (\sim p \vee q) \supset (q \vee \sim p) \supset ((p \supset (\sim p \vee q)) \supset (p \supset (q \vee \sim p)))$ rule II applied to variant 6 of axiom 5

(3) $\vdash (((p \supset (\sim p \vee q)) \supset (p \supset (q \vee \sim p)))$ rule III 1,2

(4) $\vdash (((p \supset (p \supset q)) \supset (p \supset (q \vee \sim p)))$ definition of implication 3

(5) $\vdash [\sim p \vee (q \vee \sim p)] \supset [q \vee (\sim p \vee \sim p)]$ rule II applied to variant of axiom 4

(6) $\vdash [p \supset (q \vee \sim p)] \supset [q \vee (\sim p \vee \sim p)]$ def imp 5

(7) $\vdash (((p \supset (p \supset q)) \supset [q \vee (\sim p \vee \sim p)$ trans imp 4,6

(8) $\vdash (\sim p \vee \sim p) \supset \sim p$ rule II axiom 1

(9) $\vdash ((\sim p \vee \sim p) \supset \sim p) \supset ((q \vee (\sim p \vee \sim p)) \supset (q \vee \sim p))$ rule II applied to variant 6 of axiom 5

(10) $\vdash ((q \vee (\sim p \vee \sim p)) \supset (q \vee \sim p))$ III, 8,9

(11)) $\vdash (p \supset (p \supset q)) \supset (q \supset \sim p)$ trans imp 7,10

(12) $\vdash (q \vee \sim p) \supset (\sim p \vee q)$ rule II applied to axiom 2

(13) $\vdash (q \vee \sim p) \supset (p \supset q)$ def imp 12

(Lemma 2) $\vdash (p \supset (p \supset q)) \supset (p \supset q)$ trans imp 11 13

8.5 The proof of modus ponens for $\vdash_P$

Now suppose that we have $\vdash_P Q$ and $\vdash_P Q \supset R$.

Thus we have

(1) $\vdash P \supset Q$ assumption

(2) $\vdash P \supset (Q \supset R)$ assumption

(3) $\vdash (P \supset Q) \supset ((Q \supset R) \supset (P \supset R))$ Lemma 1 above with rule II to replace p with P etc.

(4) $\vdash ((Q \supset R) \supset (P \supset R))$ III (1)(3)

(5) $\vdash (P \supset (Q \supset R)) \supset (((Q \supset R) \supset (P \supset R)) \supset (P \supset (P \supset R)))$ II on the Lemma with p, q, r replaced with P, $Q \supset R$, $P \supset R$.

(6) $\vdash (((Q \supset R) \supset (P \supset R)) \supset (P \supset (P \supset R)))$ III 2,5

(7) $\vdash (P \supset (P \supset R))$ III 4,6

(8) $\vdash ((P \supset (P \supset R)) \supset (P \supset R))$ rule II applied to Lemma 2

(9) $\vdash P \supset R$ III 7,8

Thus from $\vdash_P Q$ and $\vdash_P Q \supset R$ we can derive $\vdash_P R$.

8.6 Remarks on why we have proved the Deduction Theorem at this point

So, we have shown that the collection of statements provable under the hypothesis P contains all statements which are simply derivable, contains P itself, and is closed under applications of rule III and under applications of

rule II which leave P fixed. Thus, if we can prove from theorems of our original system and the hypothesis P that Q follows, without applying rule II to any variable appearing in P (except in subproofs which make no use of the hypothesis P), we have $\vdash_P Q$, from which we have $\vdash P \supset Q$.

8.7 Further remarks

You should see from what I have done that the basic axioms and rules of Russell's system used by Post make for very long and boring proofs. The rule of transitivity of implication which I proved is a basic example of a simplification of the system which can make proofs a lot more reasonable in length (and understandable). Imagine what the proof of Lemma 2 would look like without uses of transitivity of implication! The Deduction Theorem justifies a much more powerful technique for shortening proofs and organizing them intelligibly.

The motivations for the individual axioms can be seen in the manipulations they enable in the proof above. That they are a sufficient set is actually witnessed by the fact that we can prove this theorem, the double negation theorem $\sim\sim P \supset P$, and the standard method of proof of negative statements: if we have $\vdash_P \sim (Q \vee \sim Q)$ then we have $\vdash \sim P$. To get this result it is sufficient to derive $\vdash (P \supset \sim (Q \vee \sim Q)) \supset \sim P$. Notes on these derivations may appear here later.

9 Post's fundamental theorem

I am going to try to present Post's proof in one or more lectures. Post himself divides his proof into four parts.

9.1 Part A: substitution property of biconditionals

Note that Post uses $p \equiv q$ where I would write $p \leftrightarrow q$. Usually $\equiv$ is used now for logical equivalence, but I will follow Post's notation.

$p \equiv q$ is defined as $(p \supset q).(q \supset p)$.

He proves that $(p \equiv q) \supset (f(p) \equiv f(q))$ where the function (expression) f may involve other letters.

He proves this by induction on the complexity of expressions. A variable p is said to be of rank 0, as is a variable q other than p, considered as a

constant function of p. If $f(p)$ is of rank m, $\sim f(p)$ is of rank $m+1$. If $f(p)$ is of rank m and $g(p)$ is of rank n, then $f(p) \vee g(p)$ is of rank $\mathtt{max}(m,n)+1$.

For any rank 0 function, we have the theorem: if $f(p)$ is a rank 0 function of p, then $p \equiv q \supset f(p) \equiv f(q)$ simplifies to either $(p \equiv q) \supset (p \equiv q)$ (if $f(p) = p$) or $(p \equiv q) \supset (r \equiv r)$ (if $f(p) = r$, a constant function where r is distinct from p). Both of these are theorems (facts Post leaves the reader to prove for themselves or look up in Principia Mathematica).

Suppose that the theorem is true for any function of rank $\leq m$ (this is an argument by strong induction). A formula $f(p)$ of rank m is of the form either $\sim g(p)$ or $g(p) \vee h(p)$, where g, h are of rank $\leq m$.

We have $(p \equiv q) \supset (g(p) \equiv g(q))$ and $(p \equiv q) \supset (h(p) \equiv h(q))$ by inductive hypothesis. Post tells us that (1) $r \equiv s \supset (\sim r \equiv \sim s)$ is a theorem.

The case where $f(p)$ is defined as $\sim g(p)$:

(1) $\vdash (r \equiv s) \supset (\sim r \equiv \sim s)$ claimed to be a theorem of PM by Post (we might revisit this)

(2) $\vdash (g(p) \equiv g(q)) \supset (\sim g(p) \equiv \sim g(q))$ rule II applied to (1)

(3) $\vdash (p \equiv q) \supset (g(p) \equiv g(q))$ inductive hypothesis (g is of rank $\leq m$)

(4) $\vdash (p \equiv q) \supset (\sim g(p) \equiv \sim g(q))$ trans imp 3,2

(5) $\vdash (p \equiv q) \supset (f(p) \equiv f(q))$ in the case where $f(p)$ is defined as $\sim g(p)$.

Post tells us that $(r \equiv s) \supset (t \equiv u) \supset ((r \vee t) \equiv (s \vee u))$ is a theorem of the system of PM.

The case wher $f(p)$ is defined as $g(p) \vee h(p)$:

(1) $\vdash (r \equiv s) \supset (t \equiv u) \supset ((r \vee t) \equiv (s \vee u))$ Post claim

(2) $\vdash (g(p) \equiv g(q)) \supset ((h(p) \equiv h(q)) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q))))$ rule II applied to (1)

(3) $\vdash (p \equiv q) \supset (g(p) \equiv g(q)$ ind hyp (g is of rank $\leq m$)

(4) $\vdash (p \equiv q) \supset ((h(p) \equiv h(q)) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q))))$ trans imp 3,2

I am going to pause and introduce a rule: from $\vdash A \supset (B \supset C)$ derive $\vdash B \supset (A \supset C)$: this is easily justified using a combination of the basic rules and a variant of axiom 4, and I think I will assign this as homework. I'll call it "hypothesis reordering".

(5) $\vdash (h(p) \equiv h(q)) \supset ((p \equiv q) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q))))$ hypothesis reordering, 4

(6) $\vdash (p \equiv q) \supset (h(p) \equiv h(q))$ ind hyp (h is of rank $\leq m$)

(7) $\vdash (p \equiv q) \supset ((p \equiv q) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q))))$ trans imp 6,5

(8) $\vdash ((p \equiv q) \supset ((p \equiv q) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q))))) \supset ((p \equiv q) \supset ((g(p) \equiv h(p)) \equiv (g(q) \vee h(q))))$ rule II applied to Lemma 2

(9) $\vdash ((p \equiv q) \supset ((g(p) \vee h(p)) \equiv (g(q) \vee h(q)))$ rule III 7,8

(10) $\vdash (p \equiv q) \supset (f(p) \equiv f(q))$ in the case where $f(p)$ is defined as $g(p) \vee h(p)$.

One could remove line 8 if one also had a rule of hypothesis collapse, from $\vdash A \supset (A \supset B)$ derive $A \supset B$. This can be derived using Lemma 2 much as hypothesis reordering is derived from a variant of axiom 4.

This completes the proof of the theorem of part A, by mathematical induction.

9.2 Part B

The second part is basically a Boolean algebra calculation. This is why I mentioned Boolean algebra. The purpose of Part A is in effect to allow us to use biconditionals as equations for purposes of calculation.

Using the biconditional theorems $\sim (p \vee q) \equiv (\sim p. \sim q)$ and $\sim\sim p \equiv p$ repeatedly with the result of Part A, and also the theorem $(p \equiv q) \supset ((q \equiv r) \supset (p \equiv r))$ (these are theorems that Post simply claims can be derived), we can for any function $f(t_1, \ldots, t_n)$ prove $f(t_1, \ldots, t_n) \equiv f'(t_1, \ldots, t_n)$, where $f'(t_1, \ldots, t_n)$ does not contain any negation except of a single letter, and is otherwise formed of disjunctions and conjunctions.

9.3 Part C

We then apply what Post actually calls the distributive law of logical multiplication, $p.(q \vee r) \equiv ((p.q) \vee (p.r))$, repeatedly, along with $(p \equiv q) \supset ((q \equiv r) \supset (p \equiv r))$, to get $f(t_1, \ldots, t_n) \equiv f''(t_1, \ldots, t_n)$, where $f''(t_1, \ldots, t_n)$ is a disjunction of conjunctions of single variables and negations of single variables (it is in disjunctive normal form).

If any of these conjunctions contains neither t_i nor $\sim t_i$, this can fixed using $p \equiv ((p.q) \vee (p. \sim q))$.

The products can then be rewritten using commutative and associative laws of logical multiplication = conjunction (which I invite you to write as biconditionals to which the result of Part A can be applied), along with the theorem $\vdash p.p \equiv p$, into forms in which each product contains at most one t_i and at most one $\sim t_i$ for each i: we end up with the biconditional $\vdash f(t_1, \ldots, t_n) \equiv f'''(t_1, \ldots, t_n)$ where f''' is a disjunction of conjunctions

of products of variables and negations of variables in which each product contains at least one of t_i and $\sim t_i$ and at most one of each of these.

9.4 Part D

We can prove by induction that any asserted $\vdash A$ has A positive (its truth table consists entirely of +'s).

Suppose that the original function $f(tt_1, \ldots, t_n)$ is positive (has a truth table consisting entirely of +'s). Then $\vdash f(t_1, \ldots, t_n) \equiv f'''(t_1, \ldots, t_n)$ is positive because it is asserted. It follows that $f'''(t_1, \ldots, t_n)$ must be positive (looking at the truth table of the biconditional.

We then complete the proof that $f(tt_1, \ldots, t_n)$ can be asserted by induction on the number of letters used.

In the case of $n = 1$, f'' must be either $t_1 \vee \sim t_1$ or $t_1 \vee \sim t_1 \vee t_1. \sim t_1$ (up to reordering), because these are the only candidate f'''s which have truth table all +'s, and both of these are asserted ($\vdash t_1 \vee \sim t_1$ and $\vdash t_1 \vee \sim t_1 \vee t_1. \sim t_1$ are both fairly easy from things we have already shown).

Suppose we have shown that $f(t_1, \ldots, t_k)$ having positive truth table implies $\vdash f(t_1, \ldots, t_k)$. We show that this follows for $k + 1$.

$\vdash f(t_1, \ldots, t_k, t_{k+1}) \equiv f''(t_1, \ldots, t_k, t_{k+1})$ for f'' with properties stated in Part C. Use the distributive property of logical multiplication over logical addition and part A methods (and commutativity and associativity of disjunction) to get $\vdash f(t_1, \ldots, t_k, t_{k+1}) \equiv f'''(t_1, \ldots, t_k, t_{k+1})$ where $f'''(t_1, \ldots, t_{k+1})$ is of the form $(t_{k+1}.f_1(t_1, \ldots, t_k)) \vee (\sim t_{k+1}.f_2(t_1, \ldots, t_k)) \vee (t_{k+1}. \sim t_{k+1}.f_3(t_1, \ldots, t_k))$.

Truth table analysis reveals that f_1 and f_2 must be positive (it doesn't matter what f_3 is). It follows by inductive hypothesis that $\vdash f_1(t_1, \ldots, t_k)$ and $\vdash f_2(t_1, \ldots, t_k)$. The theorem $p \supset q \supset (r.p \vee \neg r.q \vee r.\neg r.s$ then allows us to see that $\vdash f'''$ is derivable. The theorem $(p \equiv q) \rightarrow q \supset p$ then allows us to show that, because $\vdash f'''$ is derivable, so is $\vdash f''$, and so is$\vdash f$. Every function with positive truth table is derivable.

So the propositional calculus as described in PM is a complete realization of the propositional calculus as described by the method of truth tables. Tautologies (positive statements) can be proved, and no other statement can be proved.