1974

Three Papers in Mathematical Logic

Henry P. Miranda '74
College of the Holy Cross, henrypaulmiranda@gmail.com

THREE PAPERS IN MATHEMATICAL LOGIC

by

Henry P. Miranda

An Algebraic Proof
of the
Completeness of Sentential Logic

Godel's Proof of the Incompleteness
of
Axiomatic Number Theory

The Independence
of the
Continuum Hypothesis

Presented in Partial Fulfillment
of the
Requirements for the Fenwick Scholar Program
1973-1974

AN ALGEBRAIC PROOF OF THE COMPLETENESS OF SENTENTIAL LOGIC

I. INTRODUCTION

In this paper we prove the completeness of sentential logic using concepts of Boolean structures. For readers unfamiliar with the terminology, "sentential" or elementary" logic (sometimes called the Statement Calculus) is the usual form of valid reasoning, omitting quantification over variables. For example, statements such as "P or Q" and "if P then not Q and not R" represent such forms. Statements including quantification, such as "if for all x, P(x), then for some y, Q(y)" do not fall into the category discussed here; they belong to the so-called first-order logic. The restriction to elementary logic is reasonable since the proof of completeness in the first order case parallels the proof presented here, though it is technically much more difficult.

The study of elementary logic is primarily concerned with discovering the forms of valid reasoning. As an example, let A be the statement "If P then P or Q" where P and Q are arbitrary assertions. The distinctive feature of statement A is that it is regarded as true independent of the truth or falsity of assertions P and Q, the more basic statements from which is is composed. It is these statements which are true simply on the basis of their form not their content which represent the subject matter of sentential logic. The "completeness" of this logic asserts that if a statement is of such a (tautologous) form then it can be proved. Now, as soon as the concept of proof is mentioned, we begin to ask about axioms, rules of inference, theorems, etc. But first let us establish some ground rules for the formal language.

II. THE STATEMENT CALCULUS

In order, to formalize the discussion of statements such as those mentioned in § I, it is necessary to introduce a symbolic language L in which these statements can be expressed.

The primitive symbols of L are the following:

1. Propositional Variables: a countable set, $P = \{p_1, p_2, \ldots\}$.
2. Connectives: $\rightarrow$, $\neg$ (no commas)
3. Parentheses: (,)

P is our set of basic statement symbols with which other statements are built. "$\longrightarrow$" is interpreted as "if . . . then . . .," and "$\neg$" is the negation symbol. The correct way to build sentences are these:

1. Any propositional variable is a well-formed formula (wff)
2. If A and B are wffs, then $\neg A$ is a wff, and $(A \longrightarrow B)$ is a wff.

Let W be the set of all wffs. As examples, $\neg(P_1 \longrightarrow P_2) \in W$, and $P_1 P_2 \notin W$ (more than one variable but no connective). The element of W referred to above can be interpreted as "not, if P_1 then P_2." The utility of the formal language L in our discussion is obvious. Let us now make rigorous the above assignment of meaning to the statements of L.

<u>Def. 1</u> An <u>interpretation</u> is a map $g: P \longrightarrow \{T, F\}$.

Let I be the set of all interpretations. An interpretation then is an assignment of meaning (but only truth or falsity) to each basic statement of our language. A <u>value map</u> extends these assignments to each wff in W.

<u>Def. 2</u> A <u>value map based on the interpretation g</u> is a map

V_g: $W \longrightarrow \{T,F\}$ defined indictively as follows:

$V_g(p_i) = g(p_i)$ for all $p_i \in P$.

If A is $\neg B$ for some $B \in W$, then

$V_g(A) = F$ iff $V_g(B) = T$

If A is $(B \longrightarrow C)$ for some $B, C \in W$, then

$V_g(A) = F$ iff $V_g(B) = T$ <u>and</u> $V_g(c) = F$.

Using the above, the value map of an interpretation g can be computed for any wff in W.

<u>Def. 3</u> If $A \in W$, and $g \in I$, then

A is <u>true in g</u> if $V_g(A) = T$;

A is <u>false in g</u> if $V_g(A) = F$.

<u>Def. 4</u> $A \in W$ is a <u>tautology</u> if it is true in all interpretations. (Denoted by $\models A$).

<u>Def. 5</u> If $A \in W$, then $g \in I$ is a <u>model</u> of A iff $V_g(A) = T$.

One can see that a statement A is a tautology if and only if every interpretation g is a model of A. In other words A is "true" regardless of whether any of the basic statements $P_1 P_2$, etc., are true or false. Thus, tautologies are of primary interest; they represent those special forms involved with valid reasoning mentioned in I.

Since the completeness theorem concerns the relationship between tautologies and what is "provable," we need a precise notion of what a "proof" is. We begin by presenting certain axioms and rules of inference which will be used in our definition of a proof.

The following are statements of W which we take as axioms:

1. $(A \longrightarrow (B \longrightarrow A))$
2. $((A \longrightarrow (B \longrightarrow C)) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C)))$
3. $((\neg A \longrightarrow \neg B) \longrightarrow (B \longrightarrow A))$
4. $(A \longrightarrow A)$
5. $(\neg\neg A \longrightarrow A)$
6. $(A \longrightarrow \neg\neg A)$

Note that all of these axioms are tautologies. Some of them are familiar. For instance, 3) is a statement of the contra-positive law. It should be noted that these formulas technically are not elements of W in themselves; they are <u>axiom schema</u>. To obtain an axiom, simply substitute a wff for A,B, and C in 1) - 6). As abbreviations we will write

$(A \vee B)$	for	$(\neg A \rightarrow B)$
$(A \wedge B)$	for	$\neg(A \rightarrow \neg B)$
$(A \leftrightarrow B)$	for	$((A \rightarrow B) \wedge (B \rightarrow A))$

Their meanings can be derived from that of $\neg$ and $\rightarrow$ and are described as follows:

$(A \vee B)$ is true if either A or B is true, or both
$(A \wedge B)$ is true if both A and B are true
$(A \leftrightarrow B)$ is true if A and B are either both true, or both false.

The rules of inference which allow us to proceed from axioms to other "theorems" are as follows:

For any $A,B,C \in W$,

	From:	Infer:
1.	A,B	$(A \wedge B)$
2.	$(A \wedge B)$	$(B \wedge A)$
3.	$(A \vee B)$	$(B \vee A)$
4.	$(A \vee (B \vee C))$	$((A \vee B) \vee C)$
5.	$(A \wedge (B \wedge C))$	$((A \wedge B) \wedge C)$
6.	A	$(A \vee B)$
7.	$(A \leftrightarrow B)$, $(B \vee C)$	$((A \vee C) \leftrightarrow (B \vee C))$
8.	$(A \leftrightarrow B)$, $(B \wedge C)$	$((A \wedge C) \leftrightarrow (B \wedge C))$
9.	$(A \vee A)$	A
10.	$(A \wedge A)$	A

From:	Infer:
11. $(A \longrightarrow B)$	$((A \wedge C) \longrightarrow B)$
12. $(A \longrightarrow B)$	$(A \longrightarrow (B \vee C))$
13. $(A \wedge B)$	A
14. $A, (A \longrightarrow B)$	B

The most important property of a rule of inference is that it preserve tautologousness; the reader can check that the above rules satisfy this requirement. This list of rules of inference may seem lengthy. However, <u>all</u> the above rules can in fact be derived from the last rule, commonly known as <u>modus ponens</u> (in Latin, "method of affirming"). For example, we can derive (informally) rule No. 3):

1. $(A \vee B)$	an assumption
2. $(\neg A \longrightarrow B)$	translation of 1.
3. $((\neg A \longrightarrow \neg\neg B) \longrightarrow (\neg B \longrightarrow A))$	contrapositive axiom
4. $(B \longrightarrow \neg\neg B)$	axiom 6)
5. $(\neg A \longrightarrow \neg\neg B)$	2. and 4.
6. $(\neg B \longrightarrow A)$	3., 5., and modus ponens
7. $(B \vee A)$	translation of 6.

We now formalize the above proof process and define what is meant by a proof, a proof from assumptions and a theorem.

<u>Def. 6</u> $W_1, \ldots, W_n \in W$ is a <u>proof sequence from assumptions</u> $\alpha_1, \ldots, \alpha_k$ iff each w_i, $1 \leq i \leq n$, is

1. an axiom, or
2. An assumption from $\{\alpha_1, .., \alpha_k\}$, or
3. inferred from $w_1, \ldots, w_{i-1}$ by a rule of inference.

Def. 7 If A is the last wff in a proof sequence from assumptions, we say A is provable from these assumptions. (Denoted $\{\alpha_1, \ldots, \alpha_k\} \vdash A$, or $\mathcal{A} \vdash A$, if $\mathcal{A} = \{\alpha_1, \ldots, \alpha_k\}$.

Def. 8 An absolute proof sequence is a proof sequence with an empty assumption set.

Def. 9 $A \in W$ is a theorem if it is provable from the empty set of assumptions. (Denoted $\vdash A$).

The relation between the two forms of proof can be formalized into a powerful tool which we simply state without proof as the

Deduction Theorem $\{A\} \vdash B$ iff $\vdash (A \rightarrow B)$.

This theorem formalizes the often used method of assuming as axioms the hypothesis of a theorem, and then proving the conclusion. One hasn't really proved the conclusion; he has proved "if the hypothesis is true, then so is the conclusion."

We shall need the following concept:

<u>Def. 10</u> $\mathcal{A} \subset W$ is <u>deductively inconsistent</u> iff $\mathcal{A} \vdash \neg(p_1 \longrightarrow p_1)$. Otherwise, $\mathcal{A}$ is <u>deductively consistent</u>.

In other words, $\mathcal{A}$ is deductively inconsistent if, by assuming $\mathcal{A}$, one can prove something which is patently false. One can easily prove the following lemma which says that it does not matter exactly what patently false statement is provable from $\mathcal{A}$.

<u>Lemma 1</u> The following are equivalent:

1. $\mathcal{A}$ is deductively inconsistent;
2. for some $A \in W$ $\mathcal{A} \vdash A$ <u>and</u> $\mathcal{A} \vdash \neg A$;
3. for all $A \in W$ $\mathcal{A} \vdash A$ <u>and</u> $\mathcal{A} \vdash \neg A$.

With the description of the formalization of elementary logic completed, we now know precisely what the objects are that are dealt with in the completeness theorem, which, informally, states that <u>every tautology is a theorem</u>. As the title of this paper suggests, we will use the concepts of Boolean structures in the proof.

III. <u>BOOLEAN STRUCTURES</u>

<u>Def. 11</u> A <u>Boolean ring</u> is a ring with identity in which every element is idempotent, that is, for all b in the boolean ring,

$b^2 = b \cdot b = b$.

As an example, consider the two-element ring {0,1}, with operations defined by:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

This boolean ring is a field; it is the only boolean field and is in fact isomorphic to Z/2Z.

As another example, let X be an arbitrary set. Then the set $2^X = \{f: X \longrightarrow {}^{Z}1/2Z\}$ is a boolean ring, with the operations defined pointwise.

This all serves as an introduction to a more natural formulation of these structures, the boolean algebra:

<u>Def. 12</u> A <u>boolean algebra</u> is a non-empty set B with two binary operations, $\wedge$, $\vee$, and one unary operation, $'$, and two distinct unique elements 0 and 1, satisfying:

1. $p \vee 0 = p$ $\qquad p \wedge 1 = p$
2. $p \wedge p' = 0$ $\qquad p \vee p' = 1$
3. $p \wedge q = q \wedge p$ $\qquad p \vee q = q \vee p$
4. $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ $\qquad p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

for all p,q, and $r \in B$.

The following are well-known theorems about boolean algebras:

5. $0' = 1$ $\qquad$ $1' = 0$
6. $p \wedge 0 = 0$ $\qquad$ $p \vee 1 = 1$
7. $p'' = p$
8. $p \wedge p = p$ $\qquad$ $p \vee p = p$
9. $(p \wedge q)' = p' \vee q'$ $\qquad$ $(p \vee q)' = p' \wedge q'$
10. $p \wedge (q \wedge r) = (p \wedge q) \wedge r$ $\qquad$ $p \vee (q \vee r) = (p \vee q) \vee r$

As an example, consider an arbitrary non-empty set X. Then the set of all subsets of X is a boolean algebra, with distinguished elements $\emptyset$ and X, and with operations defined by

$$P \wedge Q = P \cap Q \quad \text{(intersection)}$$

$$P \vee Q = P \cup Q \quad \text{(union)}$$

$$P' = \overline{P} \quad \text{(complementation)}$$

Boolean algebras and boolean rings can be interdefined. For, if $B = \langle B, +, \cdot \rangle$ is a boolean ring, we can define

$$p \vee q = p + q + pq$$

$$p \wedge q = p \cdot q$$

$$p' = 1 + p$$

for $p,q \in B$. $B = \langle B, \wedge, \vee, ', 0, 1 \rangle$, then becomes a boolean algebra. Similarly, if $B = \langle B, \wedge, \vee, ', 0, 1 \rangle$ is a boolean algebra, we can define

$$p + q = (p \wedge q') \vee (p' \wedge q)$$

$$p \cdot q = p \wedge q$$

$B = \langle B, +, \cdot \rangle$ is then a boolean ring.

We shall take the informal approach of naming the boolean ring or algebra by its underlying set B.

<u>Def. 13</u> A <u>boolean ideal</u> in a boolean algebra B is a subset M of B such that

1. $0 \in M$
2. if $p \in M$ and $q \in M$, then $p \vee q \in M$
3. if $p \in M$ and $q \in B$, then $p \wedge q \in M$.

Boolean ideals have a close relationship to ring ideals.

In fact,

<u>Theorem 1</u> M is a boolean ideal in the boolean algebra B iff M is a ring ideal in the boolean ring B.

The proof of the above theorem is a simple consequence of the definitions.

The concept of a filter will be needed also.

<u>Def. 14</u> A <u>boolean filter</u> in a boolean algebra B is a subset N of B s.t.

1. $\underline{1} \in N$
2. if $p \in N$ and $q \in N$, then $p \wedge q \in N$
3. if $p \in N$ and $q \in B$, then $p \vee q \in N$.

Ideals and filters are dual concepts in that if M is a boolean ideal, then $N = \{p | p' \in M\}$ is a boolean filter. And if N is a boolean filter, then $M = \{p | p' \in N\}$ is a boolean ideal.

Def. 15 An ideal is maximal if it is a proper ideal that is not included in any other proper ideal.

This general definition, which applies to all ideals in all rings, can now be applied to boolean algebras. Maximal boolean ideals have a simple characterization.

Lemma 2 If M is a boolean ideal in a boolean algebra B, then M is maximal iff for all $p \in B$, either $p \in M$ or $p' \in M$, but not both.

PROOF: Assume M is maximal, and that there exists an element $p_o \in B$ s.t. neither $p_o \in M$ nor $p_o' \in M$. Define N by $N = \{p \vee q \mid q \in M, p \vee p_o = p_o\}$. It is easily checked that N is an ideal of B. Also, M is a proper subset of N, since $q = 0 \vee q \in N \quad \forall q \in M$. But $p_o \in N$, and $p_o \notin M$. Therefore, M is not maximal, contradicting the hypothesis.

If M contains p or p' but not both for <u>all</u> $p \in B$, then any ideal N containing M (properly) would contain some $p_o \notin M$. Thus $p_o' \in M \subset N$ and hence N would contain $p_o \wedge p_o' = 1$. But, if any ideal contains 1, it is the entire boolean algebra. Therefore, M is maximal. QED

The above lemma is quite plausible from a ring-theoretic viewpoint. For an ideal M to be maximal in B, it is necessary and sufficient that B/M be a field. But the only boolean field is the two-element field, $Z_1/2Z_1$. Hence we would expect that every maximal ideal would "split" the elements of B right down the middle, so to speak.

A useful lemma concerning maximal boolean ideals will now be proved.

<u>Lemma 3</u> If M is a maximal boolean ideal, then $x \vee y \in M$ iff $x \in M$ and $y \in M$.

<u>PROOF</u>: The "if" part, of course, follows directly from the definition. Assume $x \notin M$, and $x \vee y \in M$. Then $x' \in M$ since

M is maximal, by Lemma 2. Therefore $x' \vee (x \vee y) \in M$, and hence $(x' \vee x) \vee y \in M$ by associativity of $\vee$. But $x' \vee x = 1$, and thus $1 \vee y = 1 \in M$, yielding, a contradiction. Thus, $x \in M$. Similarly, $y \in M$. QED.

The primary theorem about maximal ideals is called, cryptically, the Maximal Ideal Theorem. It assures us that maximal ideals exist under the proper circumstances.

<u>The Maximal Ideal Theorem</u> If B is a boolean algebra, and I is a proper ideal in B, then there exists a maximal ideal M of B containing I.

The proof of the maximal ideal theorem involves Zorn's Lemma, which, of course, is equivalent to the axiom of choice.

We are now ready to begin the proof of the completeness of elementary logic. Up to this point we have dealt on two seemingly unrelated topics, formulization of elementary logic and basic properties of boolean structures. We are now ready to describe their connection.

IV. THE CONSTRUCTION OF THE EQUIVALENCE RELATION ON W

Let W be the set of all wffs of L, as in § 2. Define an equivalence relation on W by:

$$A \equiv B \text{ iff } \vdash (A \longleftrightarrow B)$$

<u>Theorem 2</u> $\equiv$ is an equivalence relation.

<u>PROOF</u>: We must establish reflexivity, symmetry, and transitivity.

1) $\equiv$ is reflexive

1.	$\vdash (A \longrightarrow A)$	axiom 4)
2.	$\vdash ((A \longrightarrow A) \wedge (A \longrightarrow A))$	rule 1) with 1.
3.	$\vdash (A \longleftrightarrow A)$	translation of 2.
4.	$A \equiv A$	definition of $\equiv$.

2) $\equiv$ is symmetric. Assume $A \equiv B$

1.	$\vdash (A \longleftrightarrow B)$	definition of $\equiv$
2.	$\vdash ((A \longrightarrow B) \wedge (B \longrightarrow A))$	translation of 1.
3.	$\vdash ((B \longrightarrow A) \wedge (A \longrightarrow B))$	rule 2) with 2.
4.	$\vdash (B \longleftrightarrow A)$	translation of 3.
5.	$B \equiv A$	definition of $\equiv$.

3) $\equiv$ is transitive. Assume $A \equiv B$ and $B \equiv C$.

1.	$\vdash (A \longleftrightarrow B)$, $\vdash (B \longleftrightarrow C)$	by definition of $\equiv$, translation of , and rule 13)
2.	$\{A\} \vdash B$	deduction theorem
3.	$\{A\} \vdash (B \longrightarrow C)$	nature of proof sequence
4.	$\{A\} \vdash C$	Modus ponens with 2. and 3.
5.	$\vdash (A \longrightarrow C)$	deduction theorem

Similarly we have $\vdash (C \longrightarrow A)$, from which we infer $\vdash (A \longleftrightarrow C)$

and thus $A \equiv C$. QED.

Thus $\equiv$ is an equivalence relation. We next form $\overline{W}$, the set of equivalence classes of $\equiv$. Let the equivalence class of a wff A be denoted by [A]. We shall make $\overline{W}$ into a boolean algebra.

V. THE BOOLEAN ALGEBRA $\overline{W}$

We first define the three operations and the two distinct elements 0 and 1 on $\overline{W}$. We do this as follows in the natural way:

$$[A] \wedge [B] = [(A \wedge B)]$$
$$[A] \vee [B] = [(A \vee B)]$$
$$[A]' = [\neg A]$$
$$0 = [\neg B] \quad \text{where} \vdash B$$
$$1 = [B] \quad \text{where} \vdash B$$

Of course, it must be shown that $\wedge$, $\vee$, $'$, 0, and 1 are all well-defined, and that the boolean algebra axioms are satisfied. We show that $\wedge$ is well-defined and leave the rest to the reader.

In order to verify that $\wedge$ is well-defined we assume

$A_1 \equiv A_2$, and $B_1 \equiv B_2$, and show that $(A_1 \wedge B_1) \equiv (A_2 \wedge B_2)$

1.	$\vdash (A_1 \longleftrightarrow A_2)$	definition of $\equiv$
2.	$\vdash (B_1 \longleftrightarrow B_2)$	" "
3.	$\vdash (A_1 \longrightarrow A_2)$, $\vdash (A_2 \longrightarrow A_1)$	definition of , rule 13)
4.	$\vdash (B_1 \longrightarrow B_2)$, $\vdash (B_2 \longrightarrow B_1)$	" "
5.	$\vdash ((A_1 \wedge B_1) \longrightarrow A_2)$	rule 11)
6.	$\vdash ((B_1 \wedge A_1) \longrightarrow B_2)$	rule 11)
7.	$\{(A_1 \wedge B_1)\} \vdash A_2$, $\{(B_1 \wedge A_1)\} \vdash B_2$	deduction theorem
8.	$\{(A_1 \wedge B_1)\} \vdash A_2$, $\{(A_1 \wedge B_1)\} \vdash B_2$	commutativity of $\wedge$
9.	$\{(A_1 \wedge B_1)\} \vdash (A_2 \wedge B_2)$	rule 1)
10.	$\vdash ((A_1 \wedge B_1) \longrightarrow (A_2 \wedge B_2))$	deduction theorem
11.	$\vdash ((A_2 \wedge B_2) \longrightarrow (A_1 \wedge B_1))$	similarly
12.	$\vdash ((A_1 \wedge B_1) \longleftrightarrow (A_2 \wedge B_2))$	definition of $\longleftrightarrow$
13.	$(A_1 \wedge B_1) \equiv (A_2 \wedge B_2)$	definition of $\equiv$

QED

Assuming now that the operations $\wedge$, v, and $'$ are well defined, we still need to verify the boolean algebra axioms. We check two and leave the rest to the reader.

<u>Claim</u> $[A] \vee 0 = [A]$

<u>PROOF</u>: $[A] \vee 0 = [A] \vee [\neg B]$ where $\vdash B$.

but	$[A] \vee [\neg B] = [(A \vee \neg B)]$	
now:	$\{(A \vee \neg B)\} \vdash (\neg A \longrightarrow \neg B)$	by definition of v
also:	$\vdash ((\neg A \longrightarrow \neg B) \longrightarrow (B \longrightarrow A))$	axiom 3)
Thus	$\{(A \vee \neg B)\} \vdash (B \longrightarrow A)$	modus ponens.
but	$\vdash B$	assumption

then $\{(A \vee \neg B)\} \vdash A$ by modus ponens

hence $\vdash ((A \vee \neg B) \longrightarrow A)$ by deduction theorem

clearly, $\vdash (A \longrightarrow (A \vee \neg B))$ by rule 12)

Thus $\vdash (A \longleftrightarrow (A \vee \ B))$ translation of .

hence $A \equiv (A \vee \neg B)$ by definition of $\equiv$

Therefore, $[A] = [(A \vee \ B)]$

$= [A] \vee [\neg B]$

$= [A] \vee 0$ QED

Claim $[A] \wedge [A'] = 0$

PROOF: $[A] \wedge [A'] = [A] \wedge [\neg A] = [(A \wedge \neg A)]$

$= [\neg(A \longrightarrow \neg\neg A)]$ by definition of $\wedge$

$= 0$ since $\vdash (A \longrightarrow \neg\neg A)$ (axiom 6))

QED.

VI. THE KEY LEMMA

Recalling the development of elementary logic in II, the "proof theory" and the "model theory" were treated quite separately and were practically unrelated. Yet the completeness theorem deals with precisely this relationship. Hence, we would like a bridge between the two concepts. This bridge is the following lemma, and it is the key step in the proof of completeness.

<u>Lemma 4</u> If $A \in W$ is deductively consistent, then A has a model (i.e., there exists an interpretation g which makes A true).

<u>PROOF</u>: The proof of this Lemma involves several claims.

Let A be a statement in W, and assume A is deductively consistent. Thus, there does not exist a statement B such that $A \vdash B$ and $A \vdash \neg B$. Let $F = \{[B] \in \overline{W} \mid \vdash (A \rightarrow B)\}$. F is a subset of the boolean algebra $\overline{W}$. It is not simply a subset however.

<u>Claim</u> F is a boolean filter.

<u>PROOF</u>: $1 \in F$, since $1 = [B]$ where $\vdash B$.
but if $\vdash B$, then $\{A\} \vdash B$, and $\vdash (A \rightarrow B)$
by the deduction theorem. Thus $1 = [B] \in F$.
Assume next $[B], [C] \in F$. Hence

$$\vdash (A \rightarrow B), \vdash (A \rightarrow C).$$

or $\{A\} \vdash B$, $\{A\} \vdash C$ by the deduction theorem
thus $\{A\} \vdash (B \wedge C)$ by rule 1)
therefore $[(B \wedge C)] \in F$, and $[B] \wedge [C] \in F$.
Assume finally $[B] \in F$, and $[C] \in \overline{W}$.
Therefore $\vdash (A \rightarrow B)$.
And so $\vdash (A \rightarrow (B \vee C))$ by rule 12)
thus $[(B \vee C)] \in F$, hence $[B] \vee [C] \in F$.
also $0 \notin F$, since A is deductively consistent.

Thus F is a proper boolean filter in $\overline{W}$, Also, $[A] \in F$, since $\vdash (A \longrightarrow A)$ (axiom 4).

Recall now that "filter" is the dual concept to an ideal (III). We shall now define the dual ideal to F: Let $I = \{[B] \in \overline{W} \mid [B]' \in F\}$. I is an ideal, by duality. It is a proper ideal, since $1 \notin I$. From the Maximal Ideal Theorem, we know that there exists a maximal ideal in $\overline{W}$ containing I. Let M be such a maximal ideal. We now construct the model of A which is called for in the Lemma.

Let $g: P \longrightarrow \{T,F\}$ be defined by $g(p_i) = T$ iff $[p_i] \notin M$. g is then an interpretation. But is g a model of A? The following claim gives a complete characterization of those statements which are true in g.

<u>Claim</u> The value map V_g, of g, satisfies the following: $V_g(B) = T$ iff $[B] \notin M$.

<u>PROOF</u>: We shall prove this inductively, from the definition of a value map. First, note that $V_g(p_i) = T$ iff $g(p_i) = T$ iff $[p_i] \notin M$. Assume now that B is $\neg C$ for some $C \in W$. Then $V_g(B) = T$ iff $V_g(\neg C) = T$ iff $V_g(C) = F$ iff $[C] \in M$ iff

$[\neg B] \in M$ (by axiom 5) iff $[B]' \in M$ (by definition of ') iff $[B] \notin M$ (since M is maximal). Finally assume B is $(C \rightarrow D)$.

Then $V_g(B) = F$ iff $V_g(C) = T$ and $V_g(D) = F$ iff $[C] \notin M$ and $[D] \in M$ iff $[C]' \in M$ and $[D] \in M$ (since M is maximal) iff $[\neg C] \in M$ and $[D] \in M$ iff $[\neg C] \vee [D] \in M$ (by Lemma 3) iff $[(\neg C \vee D)] \in M$ iff $[(C \rightarrow D)] \in M$ (by definition of v) iff $[B] \in M$. Thus $V_g(b) = F$ iff $[B] \in M$. Or, $V_g(B) = T$ iff $[B] \in M$. QED.

We are left with one unfinished step: to prove that g is a model of the statement A.

<u>Claim</u> g is a model of A.

<u>PROOF</u>: We know that $[A] \in F$. Therefore, $[A]' \in I$ since F and I are dual. But then $[A]' \in M$, since $I \subseteq M$. Hence $[A] \notin M$, since M is a proper maximal ideal. Therefore, $V_g(A) = T$, by previous claim. Hence g is a model of A, by definition. QED.

Hence for any deductively consistent statement A, we can exhibit a model. Or, in the contrapositive form:

<u>Lemma 5</u> If a statement $A \in W$ has no models, then it is

deductively inconsistent.

This lemma, as mentioned above, is the big link between proof theory and model theory, and it is the key step in the proof of the completeness theorem, which can now be proved quite easily.

VII. THE COMPLETENESS THEOREM

The completeness theorem states that any tautology is provable; i.e., any statement which is true in all interpretations can actually be proved from the axioms and rules of inference described in 2. In our notation, this becomes <u>The Completeness Theorem</u>. If $A \in W$ and $\models A$, then $\vdash A$.

<u>PROOF</u>: Assume $\models A$, that is, A is a tautology.

Hence, A is true in every interpretation.

Thus, $\neg A$ is false in every interpretation

or, $\neg A$ has no models.

Therefore, $\neg A$ is deductively inconsistent (by Lemma 5)

Hence $\{\neg A\} \vdash \neg(p_1 \to p_1)$ by definition.

Then $\vdash (\neg A \to \neg(p_1 \to p_1))$ by deduction theorem

But $\vdash ((\neg A \to \neg(p_1 \to p_1)) \to ((p_1 \to p_1) \to A)$ is axiom 3) so $\vdash ((p_1 \longrightarrow p_1) \longrightarrow A)$ by modus ponens

Also, $\vdash (p_1 \longrightarrow p_1)$ is axiom 4)

Thus $\vdash A$ by modus ponens.

QED.

REFERENCES

P. Halmos. *Lectures on Boolean Algebras, Lecture Notes, 1960.*

D. Hilbert and W. Ackerman. *Principles of Mathematical Logic*, Chelsea Publishing Company, New York, 1950.

E. Mendelson. *Introduction to Mathematical Logic*, D. Van Nostrand Company, Inc., 1964.

J.R. Schoenfield. *Mathematical Logic*, Addison-Wesley Publishing Company, Reading, Mass., 1967.

R.R. Stoll. *Sets, Logic, and Axiomatic Theories*, W.H. Freeman and Company, San Francisco and London, 1961.

GÖDEL'S PROOF OF THE INCOMPLETENESS OF AXIOMATIC NUMBER THEORY

I. INTRODUCTION

The well known theorem discussed in this paper, Gödel's Incompleteness Theorem, is a landmark in the Foundations of Mathematics and has meaning for mathematicians, logicians, and philosophers alike. It dramatically exposes the limitations of the axiomatic approach which Hilbert had hoped would be the mathematicians' final apology.

Although the meaning of several of the terms in our title may be unknown to some readers, we offer some introductory remarks explaining the subject without becoming too technical. Essentially Gödel's Incompleteness Theorem says that there exist statements about natural numbers which are neither provable nor disprovable from the axioms of number theory. The use of the word "statement" requires some explanation of the language in which sentences about number theory are expressed. The concept of provability is perhaps intuitively vague but can be formulated precisely. The axioms of number theory are the Familiar Peano's Postulates about which more will be said later.

II. THE LANGUAGE

The language which is used in Godel's proof for expressing sentences about natural numbers is commonly called a first-order language. The primitive symbols (which are analagous to the alphabet of a conventional language) are listed and explained in Table I. There are a countably infinite set of variables and constants. The reader will notice that we have used "outfix" notation for the function symbols, writing $+(x,y)$ instead of $x+y$. Also, other familiar logical connectives can be defined in terms of these. A & B is an abbreviation of $\neg(\neg A \vee \neg B)$, and $A \rightarrow B$ an abreviation of $\neg A \vee B$, the former being logical conjunction "A and B" and the latter the conditional statement "if A then B".

These symbols can be combined in an infinite number of ways to form strings of symbols only some of which are meaningful.

TABLE I

The Primitive Symbols of the Language

Symbol	Explanation
(	Left parenthesis
)	Right parenthesis
$\neg$	Negation symbol $\neg A$ (= "not A")
V	Logical disjunction AvB (= "A or B")
=	Logical equality x = y (= "x equals y")
$\forall$	Universal Quantifier $\forall xA(x)$ (= "for all x, A(x)")
$\exists$	Existential Quantifier $\exists xA(x)$ (="there exist an x, such that A(x)
$<$	Less than $x<y$ (= "x is less than y")
S	Successor function symbol Sx (= "the successor of x")
+	Addition function symbol +(x,y) (="x plus y")
$\cdot$	Multiplication function symbol $\cdot(x,y)$ (= "x times y")
e	Exponentiation function symbol e(x,y) (= "x^y")
x_i	Variable
c_i	Constant standing for N.N.i ($c_o = 0, c_1=1$, etc.)
,	Comma

There are a countable number of variables and constants.

We shall now describe exactly which of these strings are "formulas."

The <u>terms</u> of the language are the following

1. x_i Any variable
2. c_i Any constant
3. Sa Where a is any term
4. +(a,b) a,b are terms
5. •(a,b) a,b are terms
6. e(a,b) a,b are terms

The <u>Atomic Formulas</u> of the language are the following:

1. $(t = s)$ Where t,s are any terms
2. $(t \angle s)$ Where t,s are any terms

For example, $(+(C_2,C_3) < SC_8)$ is an atomic formula. (It expresses the statement $2 + 3 \angle$ successor of 8). The class of <u>formulas</u> of the language can now finally be described:

1. All atomic formulas are formulas.
2. $\neg A$ is a formula if A is a formula
3. (A v B) is a formula if A,B are formulas
4. $(\forall x_i)A$ and $(\exists x_i)A$ are formulas if A is a formula containing x_i and if A does not already contain the symbols $\forall x_i$ or $\exists x_i$

For example, $((x_1 = C_5) \vee (+(C_1,C_3) < x_1))$ is a formula.

It expresses the statement "$x_1 = 5$ or $1 + 3 < x_1$". As another example, we have $(\exists x_1)(+(x_1,c_5) = c_7)$ which says "there exists an x s.t. x + 5 = 7. We may often omit the outermost parentheses of a formula when no confusion is possible.

This language, though somewhat limited, is quite powerful in that with it one can express most of the common properties of the natural numbers. For instance, the statement that addition is commutative can be written as $(\forall x_1)(\forall x_2)(+(x_1,x_2) = +(x_2,x_1))$. There are statements, however, which one cannot express in this language; for instance, "the set of even natural numbers is infinite" cannot be (try it!) The reader may be interested in discovering other "unexpressible" statements.

II. GÖDEL NUMBERING

Kurt Gödel in the mid-1930's invented a clever method of assigning natural numbers to the formulas of this formal language in such a way that the language could in effect talk about itself. This procedure has since been called Gödel numbering in his honor. He needed a rule or function assigning to each formula of number theory (abbreviated N) and to each finite sequence of formulas a natural number. The reader can easily convince himself that this is plausible, since there are a countable number of symbols, and a countable number of formulas, and also a countable number of finite sequences of formulas. Finite sequences of formulas are important since a proof will be defined as such a sequence satisfying certain properties. This Gödel numbering function (let us call it g) must satisfy the following two properties:

1. g must be 1 - 1
2. g must be "computable," i.e., for any formula or sequence of formulas we could effectively compute its Gödel number, and for each natural number we could effectively compute the formula (if any) associated with it.

How can we construct this mapping? Let us first define g on the symbols of N, (which are listed in Table I):

g[(] = 3	g[=] = 13	g[+] = 23
g[)] = 5	g[$\forall$] = 15	g[$\cdot$] = 25
g[,] = 7	g[$\exists$] = 17	g[e] = 27
g[$\neg$] = 9	g[$<$] = 19	g[x_i] = 29+4i
g[v] = 11	g[S] = 21	g[c_i] = 31+4i i = 0,1,...

In this manner every symbol has a natural number associated to it in a 1-1 way.

Assign to every finite string of symbols $\sigma_1 . . . \sigma_n$ (and thus to every formula) the natural number $\prod_{j=1}^{n} P_j^{g(\sigma_i)}$ where P_j is the j^{th} prime number. Therefore, $g(\sigma_1 \ldots \sigma_n) =$

$2^{g(\sigma_1)} \cdot 3^{g(\sigma_2)} \cdot 5^{g(\sigma_3)} \cdot \; . \; . \; . \; P_n^{g(\sigma_n)}$.

g is 1-1 on the strings, by the unique factorization of natural numbers.

Now assign to each sequence of strings $S_1 \; . \; . \; . \; S_n$ the number $\prod_{j=1}^{n} P_j^{g(S_j)}$ g in the same manner as above. g is still 1-1 on the strings and sequences of strings. (Notice that no string of symbols has the Gödel number as any sequence of strings). Finally, note that g is "computable" in the sense described above.

<u>Ex. 1:</u> $g[(S\ C_o = C_1)] = 2^3 \cdot 3^{21} \cdot 5^{31} \cdot 7^{13} \cdot 11^{35} \cdot 13^5$

<u>Ex. 2:</u> $g[+(x_o,S(x_1)) = S(+(x_o,x_1))]$

translation: $x_o + S(x_1) = S(x_o + x_1)$

$g[-] = 2^{23} \cdot 3^3 \cdot 5^{29} \cdot 7^7 \cdot 11^{21} \cdot 13^3 \cdot 17^{33} \cdot 19^5 \cdot 23^5 \cdot 29^{13} \cdot 31^{21}$

$\cdot 37^3 \cdot 41^{23} \cdot 43^3 \cdot 47^{29} \cdot 53^7$

$\cdot 57^{31} \cdot 59^5 \cdot 67^5$ whew!

IV. SOME PROOF THEORY

At the intuitive level the question "what is a proof?" is not trivial and borders on the philosophical. However, we can formulate a formal working definition which corresponds nicely to our intuition. A proof, in mathematics as in any other logical discipline, must start somehwere. There is a basic set of axioms, from which other statements are proved. Once the place to start or axiom set is given, one must know the method of moving from one statement to the next, i.e., the rules of inference. Let us prescribe these concepts more precisely in our system of axiomatic number theory.

First, the axioms. The axioms of N, also known as Peano's Postulates, are the following formulas:

1. $\neg(Sx_o = C_o)$ [0 is not the successor of any natural number]
2. $((Sx_o = Sx_1) \rightarrow (x_o = x_1))$ [the successer function is 1-1]
3. $(+(x_o,C_o) = x_o)$ [0 is identity for addition]
4. $(+(x_o,Sx_1) = S(+(x_o,x_1)))$ [inductive definition of addition]
5. $(\cdot(x_o,C_o) = C_o)$ [0 times any natural number is 0]
6. $(\cdot(x_o,Sx_1) = +(\cdot(x_o,x_1),x_o))$ [inductive definition of multiplication]

7. $\neg(x_0 < c_0)$ [no natural number is less 0]

8. $((x_0 < Sx_1) \leftrightarrow ((x_0 < x_1) \vee (x_0 = x_1)))$

9. $((A(c_0) \& (\forall x_0)(A(x_0) \rightarrow A(Sx_0))) \rightarrow (\forall x_1)(A(x_1)))$

[induction axiom for any formula A]

These axioms are, of course, additions to the purely logical axioms of first-order logic, an example of which is the logical equality axiom:

$$x_1 = x_2 \rightarrow (\varphi(x_1) \leftrightarrow \varphi(x_2))$$

where φ is any statement with one free variable. Among the logical rules of inference are the following:

R1): Generalization - from $A(x_0)$
infer $(\forall x_0)(A(x_0))$

R2): Specification - from $(\forall x_0)(A(x_0))$
infer $A(t)$ where t is any term of L.

R3): Modus Ponens - from A, $A \rightarrow B$
infer B.

With the above defined, we can now give an explicit definition of a proof.

Def: A proof sequence from assumptions $\mathcal{Q}$ (a set of formulas of N) is a finite sequence of formulas $\alpha_1, \ldots, \alpha_n$, satisfying the following: Each α_i, $i=1,\ldots,n$, is either

1. an axiom,
2. a formula in $\mathcal{A}$ (an assumption), or
3. derivable from $\{\alpha_1,\ldots,\alpha_{i-1}\}$ by one of the rules of inference.

This is quite a natural definition, and leads also to the following:

<u>Def</u>: A formula A is a <u>theorem</u> from assumptions $\mathcal{A}$ if it is the last formula of a proof sequence from assumptions $\mathcal{A}$. We write $\mathcal{A} \vdash A$.

Thus a theorem is any formula which is "provable," in the sense described above. Let us denote our set of axioms by P (for Peano's Postulates). Thus if A is a theorem of axiomatic number theory, we write $P \vdash A$.

An important Meta-theorem in Proof Theory is the <u>Deduction Theorem</u>. It is stated below:

<u>The Deduction Theorem</u> From $\mathcal{A} \vee \{A\} \vdash B$ one may infer $\mathcal{A} \vdash (A \rightarrow B)$, and from $\mathcal{A} \vdash (A \rightarrow B)$ one can infer $\mathcal{A} \vee \{A\} \vdash B$.

The proof of the deduction theorem is not difficult, but it will not be given here. For a proof in the general first-order case, see Schoenfield, p. 33. This metatheorem is quite powerful as a derived rule of inference, as will be seen shortly.

V. SOME DEFINITIONS

In order to accurately state Gödel's theorem, we shall need a few definitions.

Def A set of formulas Σ is inconsistent if there exists a formula A of N s.t. $\Sigma \vdash A$ and $\Sigma \vdash \neg A$.

Def Σ is consistent otherwise. Def Σ is w-inconsistent if there exists a formula $\varphi(x_o)$ (i.e., with an unquantified variable) s.t.

$$\Sigma \vdash \varphi(c_o),\ \Sigma \vdash \varphi(c_1),\ \ldots,\ \Sigma \vdash \varphi(c_i), \ldots$$

for all i = 0, 1, . . ., but $\Sigma \vdash \neg(\forall x_o)(\varphi(x_o))$.

Σ is w-consistent otherwise. Notice that if Σ is inconsistent then Σ is w-inconsistent, by the specification rule. Hence if Σ is w-consistent then Σ is consistent.

Def: Σ is incomplete if there exists a formula φ of N s.t. neither φ nor its negation is provable from Σ. In symbols, Σ is incomplete if there exists a formula φ if N s.t. not $\Sigma \vdash \varphi$ and not $\Sigma \vdash \neg \varphi$.

VI. STATEMENT OF THE THEOREM

We now have at hand all of the facts necessary to formulate Gödel's theorem.

Gödel's Incompleteness Theorem If P is w-consistent, then P is incomplete.

We would expect a reasonable formulation of axiomatic number theory to be w-consistent. w-inconsistency is a somewhat paradoxical property. Therefore Gödel's theorem can be restated informally as follows. If Peano's Postulates satisfy certain quite natural conditions, there are statements expressible in our language which can neither be proved nor disproved. We shall now present the proof of Gödel's theorem.

VII. THE KEY LEMMA

Before stating the key lemma needed in the proof, we shall require some new terminology, incorporated in the following definitions.

Def: Define a relation Sub(x,y,z) on the natural numbers to be true if and only if x is the Godel number of a formula A with one free variable and z is the Godel number of the formula obtained from A by replacing every occurrence of the free vaiiable in A by the constant c_y. For example, $sub(2^{29},0,2^{31})$ is true. (A = "x_o", and the transformed statement is "c_o"). Sub is thus a substitution relation. Define Pr(L,n) to be true if and only if the formula with Godel number n is the last line of a proof sequence which has Godel number L.

The key Lemma can now be stated:

Lemma 1 There exists formulas in our formal language denoted by $\overline{sub}\ (x_1,x_2,x_3)$ and $\overline{pr}(x_1,x_2)$, such that:

if Sub(n,i,m) is true, then $P \vdash \overline{sub}\ (c_n,c_i,c_m)$ and
if Sub(n,i,m) is false, then $P \vdash \neg\, \overline{sub}\ (c_n,c_i,c_m)$ and
if Pr(L,n) is true, then $P \vdash \overline{pr}\ (c_1,c_n)$ and
if Pr(L,n) is false, $P \vdash \neg\, \overline{pr}\ (c_i,c_n)$.

This lemma, sometimes referred to as the expressibility Lemma, is very powerful. It essentially translates statements about substitution and proof to statements about natural numbers; this link-up is the primary application of Gödel numbering and is difficult to prove -- the proof will not be given here. However, the fact that this Lemma is true is not unreasonable, since our Godel function g was "computable," and the notion of proof is finitary. Hence given any two natural numbers N, m we can "decode" both into the strings of symbols they represent and actually determine in a finite number of steps whether or not the two strings satisfied the required properties. Since we can carry out this procedure, it also becomes possible to "prove" formally the statements whose existence the Lemma guarantees. A formalization of this procedure is in fact what is used in the proof of Lemma 1. Its function in the proof of the main theorem will become clear shortly.

There is another lemma which will be needed in the proof. It is more intuitive than the expressibility lemmas and we shall also omit its proof.

Lemma 2 $P \vdash \overline{sub}(c_n, c_n, x_1) \rightarrow (\overline{sub}(c_n, c_n, x_2) \rightarrow x_1 = x_2)$ for all n.

This lemma expresses the 1-1ness of the $\overline{sub}$ formula, and will also be needed below.

VIII. THE MAIN THEOREM

Let φ be any formula of N with one free variable, x_2, say $\varphi(x_2)$. Let A_n be the formula $(\forall x_2)(\overline{\mathrm{sub}}(x_1,x_1,x_2) \rightarrow \varphi(x_2))$. Let n be the Gödel number of A_n. Let A_m be the formula $(\forall x_2)(\overline{\mathrm{sub}}(c_n,c_n,x_2) \longrightarrow \varphi(x_2))$, and let m be the Gödel number of A_m. Note: Notice that Sub(n,n,m) is true. The main theorem is then:

Theorem 1 $P \vdash \varphi(c_m) \leftrightarrow A_m$

PROOF:

1. $P, \varphi(c_m), \overline{\mathrm{sub}}(c_n,c_n,x_2) \vdash \overline{\mathrm{sub}}(c_n,c_n,c_m) \longrightarrow (\overline{\mathrm{sub}}(c_n,c_n,x_2) \rightarrow (x_2=c_m))$

   by Lemma 2.

2. $P, \varphi(c_m), \mathrm{sub}(c_n,c_n,x_2) \vdash \overline{\mathrm{sub}}(c_n,c_n,c_m)$

   by note and expressibility

3. $P, \varphi(c_m), \overline{\mathrm{sub}}(c_n,c_n,x_2) \vdash \overline{\mathrm{sub}}(c_n,c_n,x_2) \rightarrow x_2 = c_m$

   1),2), and modus ponens

4. $P, \varphi(c_m), \overline{\mathrm{sub}}(c_n,c_n,x_2) \vdash \overline{\mathrm{sub}}(c_n,c_n,x_2)$

   ; an assumption

5. $p, \varphi(c_m), \overline{\mathrm{sub}}(c_n,c_n,x_2) \vdash x_2 = c_m$

   3),4), and modus ponens

6. $P, \varphi(c_m) \vdash \mathrm{sub}(c_n,c_n,x_2) \rightarrow x_2 = c_m$

   5), deduction theorem

7. $P, \varphi(c_m), \overline{\mathrm{sub}}(c_n,c_n,x_2) \vdash x_2 = c_m \rightarrow (\varphi(c_m) \leftrightarrow \varphi(x_2))$

   - a logical axiom of equality

8. $P, \varphi(c_m), \overline{sub}(c_n,c_n,x_2) \vdash \varphi(c_m) \leftrightarrow \varphi(x_2)$

6),7) modus ponens

9. $P, \varphi(c_m), \overline{sub}(c_n,c_n,x_2) \vdash \varphi(c_m)$

an assumption

10. $P, \varphi(c_m), \overline{sub}(c_n,c_n,x_2) \vdash \varphi(x_2)$

8),9), and modus ponens

11. $P, \varphi(c_m) \vdash \overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2)$

by 10), deduction theorem

12. $P, \varphi(c_m) \vdash (\forall x_2)(sub(c_n,c_n,x_2) \rightarrow \varphi(x_2))$

11), generalization rule

13. $P, \varphi(c_m) \vdash A_m$

12), by definition of A_m

14. $P \vdash \varphi(c_m) \rightarrow A_m$

13), and deduction theorem

The other direction is slightly shorter:

1. $(\Leftarrow)$ $P, \overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2) \vdash \overline{sub}(c_n,c_n,c_m) \rightarrow \varphi(c_m)$

Rule of specialization

2. $P, \overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2) \vdash \overline{sub}(c_n,c_n,c_m)$

by note and expressibility Lemma

3. $P, \overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2) \vdash \varphi(c_m)$

1 ,2), modus ponens

4. $P \vdash (\overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2)) \rightarrow \varphi(c_m)$

3), deduction theorem

5. $P \vdash (\forall x_2)(\overline{sub}(c_n,c_n,x_2) \rightarrow \varphi(x_2)) \rightarrow \varphi(c_m)$

generalization rule

6. $P \vdash A_m \rightarrow \varphi(c_m)$ definition of A_m QED

IX. GÖDEL'S THEOREM

Gödel's Theorem which we restate now is a corollary to Theorem 1.

Gödel's Incompleteness Theorem If P is w-consistent, then P is incomplete.

The proof is constructive in that we exhibit the required statement φ s.t. not $P \vdash \varphi$ and not $P \vdash \neg\varphi$.

PROOF: Assume P is w-consistent. Define $\varphi(x_2)$ of theorem 1 to be $(\forall x_3)(\neg \overline{pr}(x_3,x_2))$. Loosely speaking, $\varphi(x_2)$ states that there is no proof for the formula of N with Godel number x_2. Let A_n, A_m be as in Theorem 1.

Case I: Assume $P \vdash A_m$. Then we can prove A_m from Peano's Postulates and thus, there exists a proof sequence for A_m. Let L be the Godel number of this proof sequence. Since m is the Godel number of A_m, Pr(L,m) is true. Therefore, by the expressibility Lemma, $P \vdash \overline{pr}(c_L,c_m)$ but $P \vdash A_m \rightarrow \varphi(c_m)$ by Theorem 1. So, $P \vdash A_m \rightarrow (\forall x_3)(\neg \overline{pr}(x_3,c_m))$ but we are assuming $P \vdash A_m$. Therefore, by modus ponens, $P \vdash (\forall x_3)(\neg pr(x_3,c_m))$. Consequently, $P \vdash \neg pr(c_L,c_m)$ by rule of specialization. This contradicts the consistency of P. Therefore, our assumption that $P \vdash A_m$ is intennable.

Case II: Assume $P \vdash \neg A_m$

1. $P \vdash \varphi(c_m) \rightarrow A_m$ by Theorem 1
2. $P \vdash \neg A_m \rightarrow \neg \varphi(c_m)$
   1), law of contrapositives
3. $P \vdash \neg \varphi(c_m)$
   assumption, 2), modus ponens
4. $P \vdash \neg (\forall x_3) \neg \overline{pr}(x_3, c_m)$
   3), Definition of $\varphi(c_m)$
5. $P \vdash (\exists x_3)\ \overline{pr}(x_3, c_m)$
   4), Algebra of quantifiers.
6. But we know not $P \vdash A_m$.

   Therefore Pr(L,m) is false for every L.

   Therefore $P \vdash \neg \overline{pr}(c_o, c_m)$, $P \vdash \neg \overline{pr}(c_i, c_m)$ . . . $\forall i$

   by expressibility Lemma.

   Thus, since P is w-consistent, we must have not:

   $$P \vdash \neg (\forall x_3) \neg \overline{pr}(x_3, c_m)$$

   or, not $P \vdash (\exists x_3)\ \overline{pr}(x_3, c_m)$, which contradicts 5).

Therefore, we have not $P \vdash \neg A_m$.

We have shown that A_m is neither provable nor disprovable from Peano's Postulates. Thus if P is w-consistent, there are formulas which can neither be proved nor disproved. P is therefore incomplete and Gödel's theorem is established.

The reader may wonder whether Peano's Postulates are a crucial factor in this proof, and whether other axioms for natural number theory can be found which somehow circumvent the process described above. The answer is NO. It follows from Gödel's proof that any axiom system which is of sufficient power to capture the elementary notions of addition, multiplication, and order in the natural numbers will be incomplete.

X. ATTEMPTS AT CONSISTENCY PROOFS

As another corollary to Theorem 1, we obtain the following interesting result, due to Tarski:

Theorem One cannot prove the consistency of Peano's Postulates within the framework of axiomatic number theory.

PROOF: Define a relation Neg(i,j) on the natural numbers by Neg(i,j) is true if and only if i is the Gödel number of a formula A and j is the Godel number of $\neg A$. As one might suspect, there is also an expressibility lemma associated to Neg, i.e., there exists a formula of N, say $\overline{Neg}\ (x_1,x_2)$, s.t. if Neg(i,j) is true, then $P \vdash \overline{neg}\ (c_i,c_j)$; and if Neg (i,j) is false, then $P \vdash \neg\,\overline{neg}(c_i,c_j)$. Let C be the formula expressing consistency, in terms of $\overline{pr}$ and $\overline{Neg}$:

$$C = (\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)(\overline{pr}(x_1,x_2)\&\overline{pr}(x_3,x_4)\rightarrow \neg\,\overline{neg}(x_2,x_4))$$

then

$$\neg C = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(\overline{pr}(x_1,x_2)\&\overline{pr}(x_3,x_4)\&\overline{neg}(x_2,x_4))$$

Let $\varphi(x_2)$ be as in Gödel's Theorem, i.e.,

$$\varphi(x_2) = (\forall x_3)(\neg\,\overline{pr}\ (x_3,x_2))$$

1. We know $P \vdash \varphi\ (c_m) \rightarrow A_m$
   definition of A_m, Theorem 1.
2. $P, \neg\varphi\ (c_m) \vdash \neg\varphi\ (c_m) \rightarrow \neg\ A_m$
   1), law of contrapositives
3. $P, \neg\varphi\ (c_m) \vdash \neg\varphi\ (c_m)$
   assumption
4. $P, \neg\varphi(c_m) \vdash \neg A_m$
   2),3), modus ponens
5. but $P, \neg\varphi\ (c_m) \vdash A_m$
   by definition of $\neg\varphi(c_m)$.

Let m' be the Godel number of $\neg A_m$.

Then

6. $P, \neg \varphi(c_m) \vdash (\exists x_1)(\exists x_2)(\overline{pr}(x_1, c_m), \& \overline{pr}(x_2, c_m{}') \& \overline{Neg}(c_m, c_m{}'))$

4),5), and by expressibility of $\overline{pr}$, $\overline{neg}$

7. $P, \neg \varphi(c_m) \vdash \neg C$

6), definition of C.

8. $P \vdash \neg \varphi(c_m) \rightarrow \neg C$

7), deduction theorem

<u>Now assume</u> $P \vdash C$

9. $P \vdash C \rightarrow \varphi(c_m)$

8), law of contrapositives

10. $P \vdash \varphi(c_m)$

8),9), modus ponens

11. $P \vdash \varphi(c_m) \rightarrow A_n$

Theorem 1 .

12. $P \vdash A_m$

10), 11), modus ponens

This is a contradiction to Gödel's Theorem -- we have just shown A_m is unprovable. Thus <u>not</u> $P \vdash C$.

Thus we have shown that we cannot prove C from Peano's Postulates, and the theorem is established. The reader may wonder whether this particular formula expressing consistency is crucial to the proof; the answer here is NO. Given any formula A which "represents" consistency in any reasonable sense, we would be able to prove that $P \vdash A \rightarrow C$; Hence if A were provable, so would C be -- but we have seen above that C is not.

XI. OTHER EXPOSITORY AND HISTORICAL REMARKS

Consider the English sentence "I am not provable." Let us suppose informally that there exists some notion of proof and provability in English. Then we would of course insist that whatever one "proved" would be true. If one could then prove the above sentence, it would be true, and hence one would not be able to prove it -- a clear contradiction. This, then, is an example of a sentence in English which cannot be proved. (Notice then that it is a true sentence). Godel's numbering system took this statement, a "meta-statement" in that it does not belong to the formal language L, and expressed it in the formal language, in this way using the language to speak about itself. The reader may find it quite helpful to refer to this English conterpart when attempting to understand more fully the nature of the Incompleteness

Theorem.

In 1936 Barkley Rosser strengthened Godel's theorem by weakening the hypothesis from w-consistency to consistency. He proved the following:

<u>Theorem</u> If P is consistent, then P is incomplete.

The proof of the above theorem is more technical but uses the same fundamental principles as that of the theorem proved in this paper.

REFERENCES

1. E. Mendelson. Introduction to Mathematical Logic, D. Van Nostrand Company, Inc., 1964.

2. J.R. Schoenfield. Mathematical Logic, Addison-Wesley Publishing Company, Reading, Massachusetts, 1967.

THE INDEPENDENCE OF THE CONTINUUM HYPOTHESIS

I. INTRODUCTION

The question of whether or not the Continuum Hypothesis can be proved from the other axioms of axiomatic set theory has been an open question for many years. Recently, the problem has been solved by Cohen and simpler arguments presented by Scott, Solovay, and others. We intend here to discuss the nature of independence proofs and to briefly describe the boolean valued logic used to obtain the independence results.

A. General Axiomatics

The peculiar feature of mathematics as a science is its deductive nature: while other sciences rely most heavily on observation for the justification and verification of their results, mathematicians demand proof. Yet no mathematician would argue that mindless cranking-out of "theorems" without any regard for their meaning or importance is a part of mathematics. They, too, are concerned with a "real" world -- the world of ideas, intuition, and relationships between concepts. This serves to motivate two aspects of the proof process: the decisions of what to try to prove and on what to base the proof. The latter is the subject of the immediate discussion. The choice of axioms is a central and illuminationg facet of all of modern mathematics.

Axiomatic theories are formally all of the same mold; they have a set of axioms which refer to some (possibly unspecified) "universe of discourse", and rules of inference for deriving other statements from the axioms. But in motivation, axiomatic theories break into two classes. Let us refer to them as "pure" and "approximate" theories -- the reason will soon be clear. As an example of the first type let me cite abstract group theory. A group is a set G with a binary operation + satisfying the following axioms:

1. For all a and b in G, a+b is in G.
2. For all a, b, and c in G, (a+b)+c = a+(b+c).
3. There exists an element e in G such that a+e = e+a = a for all a in G.
4. For every a in G there exists an element b in G such that a+b = e.

These axioms describe groups completely. By the Completeness Theorem for first-order logic, any statement that is true in every group is provable from these axioms. One might say then that the abstract study of groups is identical with the study of these axioms and what can or cannot be proved from them. In this sense then the axiomatic theory is pure. These axioms are not designed to describe groups, but groups are defined as any object satisfying these axioms.

In contrast to this type of theory is that best represented by axiomatic number theory. The intuitive notion of natural numbers is not conceived as a set of axioms which describe them, but as an entity which in some ways defies description. In order to capture the concept and axiomatize it, one chooses properties of the natural numbers which are intuitively obvious and takes these as axioms. Hopefully these axioms will describe numbers completely in the sense that any true statement about natural numbers is provable from them. The axioms most commonly chosen are called Peano's Postulates and refer to a universe N with one unary function symbol S.

1. There exists a distinguished element 0 of N.
2. If n is in N, then S(n) is in N.
3. There does not exist an n in N such that S(n) = 0.

4. If $S(n) = S(m)$ for m and n in N, then $m = n$.
5. If A is a subset of N containing 0 and closed under S, then $A = N$.

Interpreting the function S as the successor function, these axioms are seen to be obiously true in the intuitive natural numbers. But we cannot be sure that all true statements about the natural numbers are provable from them -- in fact, Gödel's Incompleteness Theorem states that they cannot. These axioms then do not capture the concept of natural number entirely -- they are only "approximate", and in this sense are distinctly different from the axioms for group theory.

A similar process is carried out in Euclidean geometry. Euclid, the first proponent of the axiomatic method, tried to describe the intuitive notion of plane geometry by means of five axioms which he felt were self-evident. He was not interested in describing all "geometries" which satisfy certain postulates, but only geometry in the plane. One can see that the motivation for the axiomatization is the same as that for number theory.

B. <u>What is Independence?</u>

The most desirable situation in any axiomatic theory would be to have as simple an axiom set as possible without altering the body of theorems which are derivable. What is self-evident to one may seem incomprehensible to another; therefore, in keeping the list of axioms simple one would lessen the probability of disagreement and in general simplify the entire subject. Hence the search for a minimal axiom set is of some importance.

If a statement is neither provable nor disprovable from a given axiom set, it is said to be <u>independent</u>. For example, in group theory the statement

5. For all a and b in G, $a+b = b+a$

is independent of the four axioms given above. One way to prove that a statement is not provable from a set of axioms (this is not a contradiction!) is to exhibit a structure in which the axioms are true but the given statement is not. (Since the proof process preserves truth, if the statement were provable then it would have to be true in that structure also.) The existence of non-commutative groups (and commutative ones) proves that the above statement is independent. In the pure type of axiomatic theory this is not so interesting: one simply obtains another theory, the theory of abelian groups in this case. In the approximate type, however, the addition of a new independent axiom may not simply change the subject, but may allow one to prove new theorems about the same subject.

Euclid, in formulating his postulates for plane geometry, found that he needed the parallel postulate to prove many theorems which he felt were true. This postulate, which states that there is one and only one line through a given point parallel to a given line, was felt to lack the attribute of being "self-evident" which his other postulates had, and for over 2000 years mathematicians attempted to prove it from the other postulates. None succeeded. It was not until the nineteenth century that people began to wonder whether it was provable at all from these other postulates; the denial of this axiom led to non-Euclidean geometries which were distinctly different, yet not inconsistent.

How could one <u>prove</u> that the parallel postulate was not provable? One such proof which is especially relevant to the discussion is that given by Young, and it proceeds as follows. We start with the Euclidean plane. This disarms all who wish to deny the existence of "non-Euclidean" geometry. We take as "points" the points of the plane interior to the unit circle, and take as "lines" chords of the circle. Many postulates hold immediately, for instance, that through two distinct "points" there passes one and only one "line". However, defining "parallel" as non-intersecting, we see that the parallel postulate fails. It is possible to define "distance" in such a way as to validate all the other postulates except this one; this makes it conclusive that it cannot be derived from the others.

Note that in the sketch above we assumed a Euclidean plane to start with, i. e., assumed the parallel postulate. In the proof of the independence of the Continuum Hypothesis (CH) in set theory we also assume the CH, and then modify the notion of "set", "well-ordering", "cardinal number", etc. In fact, powerful principles like the axiom of choice and the CH are needed to prove that the unorthodox sets have the desired properties. Before getting ahead of ourselves, however, let us acquire the proper framework for the discussion.

II. AXIOMATIC SET THEORY

A. Foundations

Set theory is another example of an "approximate" axiomatic theory. Intuitive set theory was simply too imprecise for the mathematicians of the twentieth century. Paradoxes were emerging for which there seemed no solution. The ultimate result of this problem was a complete overhaul of the foundations of set theory and many attempts at axiomatization. The most common and widely accepted of these is Zermelo-Fraenkel set theory, the axioms of which are reproduced here.

1. The Axiom of Extensionality: If two sets A and B have the same elements, then they are the same set.
2. The Null Set Axiom: There exists a set $\emptyset$ which contains no other set.
3. The Sum Axiom: For any two sets A and B, there exists a set C containing all and only the members of A and B.
4. The Power Set Axiom: Given any set A there exists a set B such that B contains as members all and only the subsets of A.

5. The Axiom of Regularity: Every non-empty set A contains an element x such that x and A are disjoint.
6. The Axiom of Infinity: There exists a set A containing the empty set such that whenever B is an element of A, the set $B \cup \{B\}$ is an element of A.
7. The Axiom of Replacement: The range of any function is a set.

All of the above axioms can be formulated in a first-order language with one binary relation $\in$, denoting set membership. For instance, the axiom of extensionality can be written as

$$(\forall x)(x \in A \leftrightarrow x \in B) \rightarrow A=B$$

The reader may be interested in formulating the other axioms similarly. In this paper the symbolic form will have to be resorted to in certain cases.

How intuitive and self-evident are these axioms? It is generally accepted that they are quite satisfactory in this respect, and in nearly every form of axiomatic set theory these statements appear as either axioms or theorems. The following axiom, over which there has been much controversy, does not share this property.

8. The Axiom of Choice: Given any set A there exists a function f from the set of subsets of A to A such that $f(x) \in x$ for every subset x of A.

The primary objection to this axiom is that it is not constructive; the choice function f is not explicitly given -- only its existence is assured. This objection is quite valid and can only be refuted by refering to the power of this theorem -- without it, for example, one cannot prove that every set has a cardinal number.

B. Cardinal Number Theory

Two sets A and B are equipollent if there exists a one-to-one, onto function f from A to B. Equipollence is an equivalence relation and intuitively classifies sets as to their size; for example, two finite sets are equipollent if and only if they have the same number of elements. Cardinal Numbers are special sets which are meant to represent equipollence classes in the following way: two sets have the same cardinal number associated to them if and only if they are equipollent. To construct these special sets is no easy matter and it shall not be attempted here. However, it is a consequence of the axiom of choice that one can construct a cardinal number for every set such that the above property holds. It is also a theorem that any set of cardinal numbers is well-ordered in a natural way.

The finite cardinals are isomorphic to the set of natural numbers. Hence their properties are well-known. The first infinite cardinal, denoted $\aleph_0$, is the cardinal number of the set of integers (and of every countable set). All infinite cardinals are denoted by these alephs, and they are such that $\aleph_1$ is the next cardinal number after $\aleph_0$, and so forth. Being "the next cardinal number" means that there is no set whose cardinality is greater than $\aleph_0$ but less that $\aleph_1$. This is by definition of the alephs, and in fact is their main property.

Cantor, the man who founded modern cardinal number theory and in so doing revolutionized a good part of mathematics, proved the following theorem:

<u>Cantor's Theorem</u> If A is a set, then the set of all subsets of A, denoted 2^A, has cardinality strictly greater than that of A.

This theorem, applied to the set $\aleph_0$, states that $2^{\aleph_0} > \aleph_0$. Since $\aleph_1$ is the next infinite cardinal after $\aleph_0$, we must then have

$2^{\aleph_0} \geq \aleph_1 > \aleph_0$. It can be shown that while $\aleph_0$ is the cardinality of the integers, $2^{\aleph_0}$ is the cardinality of the continuum. The Continuum Hypothesis is that $2^{\aleph_0} = \aleph_1$, i.e., that there is no set of real numbers with cardinality strictly greater than that of the integers, but strictly less than that of the continuum. This fascinating conjecture was the object of many attempts at proof, but none succeeded. Yet neither could anyone find an appropriate set of real numbers to disprove it. The proof that it was independent of the axioms for set theory (even including the powerful axiom of choice) was a startling and dramatic result, in all ways analogous to the corresponding discovery concerning Euclid's infamous parallel postulate.

III. <u>THE CONSTRUCTION OF THE MODEL</u>

A. <u>Boolean Preliminaries</u>

We shall proceed shortly to a definition of a universe V of objects, which will correspond to the "sets" of our theory. Simultaneously with the definition of V will be given a definition of the predicates ϵ and $=$, in the following way: for each pair of objects a and b of V we associate two elements P and Q of a given Boolean algebra, which elements are to be associated with the statements $a \epsilon b$ and $a=b$, respectively. These shall be called the "Boolean values" of $a \epsilon b$ and $a=b$, and will be denoted $||a \epsilon b||$ and $||a=b||$, respectively.

With the Boolean values of the atomic formulas of the language so defined, the Boolean values for other statements without free variables can be given as follows:

$$||\neg X|| = ||X||'$$

$$||X \& Y|| = ||X|| \wedge ||Y||.$$

If F(x) is a statement containing no free occurrences of any variable except x, then $||(\forall x)F(x)|| = \bigwedge_{a \epsilon V} ||F(a)||$. (We choose the Boolean algebra to be complete, thereby assuring the existence of the above infimum). Then:

$$||X \vee Y|| = ||X|| \vee ||Y||$$

$$||X \rightarrow Y|| = ||X||' \vee ||Y||$$

$$||(\exists x)F(x)|| = \bigvee_{a \epsilon V} ||F(a)|| .$$

If X contains free variables $x_1, \ldots, x_n$, and no matter how these are replaced by members of V the resulting statement without free variables has Boolean Value 1, we then set $||X|| = 1$.

The procedure in proving that some specific statement X_o is not derivable in set theory is to establish two results:

(1) Every statement derivable in set theory has Boolean value 1.

(2) The statement X_o does not have Boolean value 1.

Let us first outline how (1) is established. This is done by showing that if X is an axiom of set theory, then $||X|| = 1$, and if Z can be derived from X and Y by the rules of set theory, and $||X|| = ||Y|| = 1$, then $||Z|| = 1$.

B. <u>The Logical Axioms and Rules</u>

Set theory can be formulated such that the only rule of inference is modus ponens. Thus the application of the rules of set theory is taken care of by the following theorem:

<u>Theorem</u> If $||X|| = 1$ and $||X \rightarrow Y|| = 1$ then $||Y|| = 1$.

The proof is essentially the following argument. If $||X \rightarrow Y|| = 1$ then $||X||' \vee ||Y|| = 1$. But $||X||' = 0$, since $||X|| = 1$. Hence

$||Y|| = 1$. In a similar manner all of the axioms of first-order logic can be shown to have Boolean value 1. For example, let us establish that the axiom $(\forall x)F(x,b) \rightarrow F(b,b)$ has Boolean value 1. We must show that $[||(\forall x)F(x,b)|| \Rightarrow ||F(b,b)||] = 1$, or equivalently, that $[\bigwedge_{a \in V} ||F(a,b)|| \Rightarrow ||F(b,b)||] = 1$. This is if and only if $\bigwedge_{a \in V} ||F(a,b)|| \leq ||F(b,b)||$, which is obvious, since $\bigwedge$ acts as an infimum operation with respect to the partial ordering .

It remains then to investigate the axioms of set theory and to show that they have Boolean value 1. We must define the universe V and the Boolean values of the atomic statements in order to do this, as one might expect.

C. <u>The Construction of the Model</u>

Let us recall the proof of the independence of the parallel postulate. To invalidate the postulate, "points" and "lines" were introduced which differed slightly from the classical points and lines -- however, as few changes as possible were made, since the other postulates were to remain valid. We are at a similar point.

We shall need to modify the notion of "set" and "set membership", but only so much as to invalidate the Continuum Hypothesis, while keeping the other axioms valid.

To every classical set A there is associated a characteristic function f_A such that $f_A(x) = 1$ if $x \in A$, and $f_A(x) = 0$ if $x \notin A$. Identifying 1 with truth and 0 with falsity, we might say that the statement $x \in A$ takes the value $f_A(x)$. With this in mind the generalization to a Boolean valued logic is evident. A "set" will be a function f whose values are elements of the given Boolean algebra. Thus the Boolean value of the statement $a \in f$ is $f(a)$.

$$||a \in f|| = f(a)$$

Once this is defined, equality is not difficult to define. Since we have $a=b$ if and only if $(\forall x)(x \in a \leftrightarrow x \in b)$, define

$$||a=b|| = ||(\forall x)(x \in a \leftrightarrow x \in b)||$$

$$= \bigwedge_{x \in V} ||a(x) \Leftrightarrow b(x)||$$

It is not practicable to introduce all our "sets" at once. Thus, when we introduce a new "set" f, we can define f(a) for those a's which have already been introduced. For other a's, f(a) will be left undefined. We can still define $a \epsilon f$ and $g=f$, however; this is done by setting

$$||a\epsilon f|| = ||(\exists x)(a=x \,\&\, x\epsilon f)||$$

and by restricting the domain of the infimum operation $\bigwedge$ in the definition of $g=f$ to the domain of f and g.

This paper is not the place to enter into the details of the construction of the model. The principle, however, should be clear: our "sets" will not correspond to functions into $\{0,1\}$, but to functions into a given Boolean algebra. The modification is slight enough to assure that the axioms of set theory have Boolean value 1, but is great enough to force the Continuum Hypothesis not to have value 1.

D. The Key Result

Let us assume that the Boolean algebra used in the construction satisfies the countable chain condition. This assures us of several necessary results, among which is that the "set" corresponding to the set of integers is well-behaved, and that "cardinality" inside the model is the same as cardinality in classical set theory.

Let then g be a function from the classical set of integers to the given Boolean algebra. If g is the constant function 1, then g corresponds to the set of integers itself. But if g is arbitrary, it then refers to a "subset" of the integers, just as a function from the integers to $\{0,1\}$ defines a subset in the classical sense ($\{x|g(x) = 1\}$ is the subset in the classical case). How many such "subsets" of the integers exist? Clearly if the Boolean algebra has a large number of elements, such subsets will be quite numerous -- numerous enough, in fact, to force "$2^{\aleph_0}$", the "cardinality" of the set of all "subsets" of the integers, (all refering to the Boolean valued model) to be strictly greater than $\aleph_1$, thereby refuting the Continuum Hypothesis.

The main question is this: can a Boolean algebra be found which is of large enough cardinality to obtain the above result while still satisfying the countable chain condition? The answer is yes. In fact, Boolean algebras with arbitrarily large cardinalities exist which satisfy the countable chain condition.

Thus, with a suitable choice of the Boolean algebra, we can force the Continuum Hypothesis to have Boolean value 0. Also, since every axiom of set theory has Boolean value 1 and the rules of inference preserve Boolean value 1, every statement derivable in set theory has Boolean value 1. Thus, the Continuum Hypothesis is not derivable in set theory and hence is independent of the axioms.

IV. FINAL REMARKS

The proof sketched above actually only shows that the Continuum Hypothesis is not provable from the axioms of set theory -- it does not show that it is not disprovable, or, in other words, that it is consistent. This was done, however, in the late 1930's by Kurt Gödel and his proof used methods which are quite different from those described in this paper. With his result, independence is established.

Boolean valued logic can also be used to prove that the axiom of choice is independent of the other axioms for set theory. The relationship between these arguments and Cohen's original "forcing" techniques are subtle but can be discovered. However, Boolean arguments seem to be of more general application than the forcing arguments used in the original proof.

REFERENCES

1. P.J. Cohen. Set Theory and the Continuum Hypothesis, William A. Benjamin, Inc., New York, 1966.

2. J. B. Rosser. Simplified Independence Proofs, Academic Press, New York, 1969.

3. J. R. Schoenfield. Mathematical Logic, Addison-Wesley Publishing Company, Reading, Mass., 1967.

4. D. Scott. A Proof of the Independence of the Continuum Hypothesis, Mathematical Systems Theory, Vol. 1, No. 2, 1968.

5. P. Suppes. Axiomatic Set Theory, D. Van Nostrand Company, Inc., 1960.