A Proof of the Independence of the Continuum Hypothesis

by

DANA SCOTT[1]

Stanford University

1. Formulating the continuum hypothesis.[2] The conceptual framework required to formulate Cantor's continuum hypothesis is remarkably elementary. The hypothesis is, of course, the assertion:

$$\text{(CH)} \qquad 2^{\aleph_0} = \aleph_1.$$

Even as it stands (CH) is a reasonably simple statement, but reference to the alephs can easily be avoided. In the first place, if we agree to assume the axiom of choice, then every cardinal number is an aleph. Thus $2^{\aleph_0}$ must be equal to some aleph, and (CH) states that it is the next one after $\aleph_0$. In other words, *there is no cardinal strictly between* $\aleph_0$ *and* $2^{\aleph_0}$.

Next, remembering to stress the word "continuum", we recall that the hypothesis has to do with the real numbers; indeed, the set of real numbers is surely the most natural set of cardinality $2^{\aleph_0}$. Therefore, (CH) can be taken as asserting that *every set of real numbers is either countable or of the same cardinality as the whole set of real numbers.*

Finally, again making use of the axiom of choice, we recall that a subset of a set is of the same cardinality as the whole set if and only if the subset can be mapped *onto* the whole set. Thus (CH) is equivalent to the statement that *given any set of reals, either the set of integers can be mapped onto the set, or the set can be mapped onto the whole set of reals.*

To understand this statement we need understand only these familiar mathematical concepts: *integers, reals,* arbitrary *subsets* of the reals, and arbitrary *mappings (functions)* from reals to reals. To see this more clearly, let us formulate the statement in logical symbols. Let lower case variables x, y range over reals; let the upper case variable X range over sets of reals; and let f, g range over real functions. The symbol $\mathbf{N}$ is reserved for the set of integers. Then, using the standard notation for set membership and function value, we can state (CH) in the form:

$$\text{(CH')} \quad \forall X\,[\exists f \forall y \in X\, \exists x \in \mathbf{N}\,[y = f(x)] \vee \exists g \forall y\, \exists x \in X\,[y = g(x)]].$$

[1] Research supported by NSF Grant GP-3926.

[2] This is an expository paper, based on recent work of Solovay and the author. References and credits are collected together in the final section.

MATHEMATICAL SYSTEMS THEORY, Vol. 1, No. 2.
Published by Springer-Verlag New York Inc.

In the above $\forall$ is to be read as the universal quantifier, $\exists$ as the existential quantifier; and $\forall\, y \in X$ is to be read as "*for all y in the set X*", and $\exists\, x \in \mathbb{N}$ as "*for some x in the set* $\mathbb{N}$". The symbol $\vee$ stands for "*or*". Note that for simplicity we can assume without any loss of generality that the real functions have as their domain of definition the *whole* set of real numbers—because the values of the f outside $\mathbb{N}$ and the g outside X are irrelevant to the import of the statement (CH′).

As a matter of fact, if we want to be very economical with our concepts, the notion of a *set* of reals can be reduced to the notion of a *real function* by using the idea of a characteristic function. Of course, the formulation (CH′) suffers some loss of beauty in that a phrase such as

$$\forall\, y \in X[\cdots]$$

would have to be replaced by

$$\forall\, y\ [X(y) = \mathbf{0} \rightarrow \cdots],$$

where $\rightarrow$ stands for "*implies*". Nevertheless, we shall imagine this reduction as having been carried out for the sake of the axiomatic system we wish to present in the next section.

2. Axiomatizing the higher-order theory of real numbers. So far we have only committed ourselves to speaking about reals (and possibly certain special numbers like 0) and real functions (and certain special functions like the characteristic function of the integers). The statements we make about these objects are formulated in a language which permits (at least) equations, the use of the function-value notation, the logical connectives and quantifiers. This bare framework is certainly sufficient for the mere formulation of an equivalent version of the continuum hypothesis as we have seen. But there is much, much more that cannot be stated in such restricted terms.

For example, it is necessary sometimes to speak of *functionals*—mappings from functions to reals—and *operators*—mappings from functions to functions. We even think of functionals on operators or operators on operators on operators from time to time. Could it not be possible that very simple properties of these so-called *higher-type functions,* properties that mathematicians are willing to accept, could be used to give a *proof* of the continuum hypothesis? The fact that mention of these objects is not required in (CH′) is no argument.

Consider the case of ordinary real algebra. We can give a (partial) axiomatization of this theory by stating the usual axioms for an ordered field. Now it is well known that the Archimedean axiom does not follow. The statement of the Archimedean axiom is quite simple, requiring beyond elementary algebra only the idea of an iterated multiple of an element (or equivalently the notion of an integer). On the other hand, if we bring in the concept of an arbitrary subset of the field of elements and invoke the obvious basic axioms about existence of subsets together with the

Dedekind completeness of the ordering, then the Archimedean axiom does follow. The connection is direct, but still it takes a moment's thought to see to which subset the completeness axiom should be applied assuming a counter-example to the Archimedean axiom.

The example just cited involves only isolated axioms which we wish to assume for the reals in any case. However, Gödel in his Incompleteness Theorem has shown that the situation is much worse: suppose we agree to assume all the standard axioms about reals together with the obvious axioms about functions, functionals, functionals on functionals, functionals on functionals on functionals, etc., say to 17 levels. Then by the method of Gödel's Theorem we can show (assuming the consistency of the system) that an extension of the system to allow for 18 levels permits a derivation of a statement about the *integers* which was not previously provable. Therefore the proof of a statement may very well involve notions not mentioned in its formulation. That situation is often met in mathematical practice when someone solves a difficult problem by introducing new notions and nearly as often someone later shows us how to avoid the new concepts by deriving the (now known to be true) fact along familiar lines. Gödel shows us, however, that in certain cases the situation is *unavoidable.* To be sure, Gödel's sentences of arithmetic are somewhat bizarre—but no one proposes a change in the rules that would eliminate them from consideration.

Nevertheless, in the case of the continuum hypothesis Cohen has finally established its unprovability no matter how many levels we would desire to allow. Even the axiom of choice is of no help. To understand this remarkable independence result, it will not be necessary to contemplate the transfinite levels employed in Cohen's original proof, nor to become involved in any ordinal inductions. We will be able to see the essence of the argument while operating on just *two* levels above the reals, that is, using only functions and functionals.

To axiomatize this theory we will use in the first place the notation of ordinary real algebra: real variables x, y, z (possibly with subscripts) and the symbols **0**, **1**, $+$, $\cdot$, $\leqslant$, and $=$. Besides these we will employ function variables f, g, h (possibly with subscripts) and functional variables F, G, H (possibly with subscripts), together with the ordinary functional notation in contexts such as $f(x)$, and $F(f)$. Equations between functions and between functionals are also permitted.

To be more precise, we can say that a *term* (generalized polynomial) is either a real variable, or one of the symbols **0** or **1**, or the result of applying a functional variable to a function variable, or the result of applying a function variable to a previously obtained term, or the sum or product of previously obtained terms. An *atomic formula* is an equation or inequality between terms or an equation between function variables or between functional variables. A *formula* is either an atomic formula or is the result of applying the logical connectives or the quantifiers to previously obtained formulas. The symbols to be used for the logical connectives are $\neg$ (not),

$\vee$ (or), $\wedge$ (and), $\rightarrow$ (implies), $\leftrightarrow$ (if and only if). Round parentheses are used for grouping terms and square brackets for formulas.

Lower case letters such as t, u, v will denote terms or possibly function or functional variables, while upper case letters such as A and B will denote formulas. An occurrence of a variable v in a formula is said to be *bound* if it occurs within a context of the form $\forall$ v A or $\exists$ v A, that is, within the scope of a quantifier; other occurrences are called *free.* A formula without free occurrences of variables is sometimes called a *sentence,* because we think of it as being definitely true or false. On the other hand, a formula with free variables (like $[x \leqslant 0 \vee 1 \leqslant x]$) in general cannot be reckoned true or false unless particular values for the free variables are given. Nevertheless, it is convenient to use formulas with free variables (like $[x \cdot y = x \cdot z \rightarrow [x = \mathbf{0} \vee y = z]]$), and when we assert them as axioms or theorems we intend this as a shorthand for universally quantifying the free variables (thus $\forall x \forall y \forall z[x \cdot y = x \cdot z \rightarrow [x = \mathbf{0} \vee y = z]]$ is a true *sentence* of real algebra that we want to be provable from our axioms). Sometimes we will wish to indicate that a formula has free occurrences of variables, and we will write expressions like $A(x, y, z)$ or $B(x_0, x_1, \cdots, x_{n-1})$. Then when we write $B(t_0, t_1, \cdots, t_{n-1})$ we mean to indicate the formula that results by *substituting* the indicated terms or other variables for the original free variables. This notation is *not* unambiguous, but for our purposes a more precise notation would not be worth the additional effort and loss of readability.

Well, just what are the axioms? To have the whole system very clearly in mind we will want to go back to the beginning: the first group of axioms are those of *propositional logic.* We could take all instances of tautologies, or we could select some standard basic list such as:

(PL) (1) $[A \rightarrow [B \rightarrow A]]$
(2) $[[A \rightarrow [B \rightarrow C]] \rightarrow [[A \rightarrow B] \rightarrow [A \rightarrow C]]]$
(3) $[[\neg B \rightarrow \neg A] \rightarrow [A \rightarrow B]]$
(4) $[[A \wedge B] \rightarrow A]$
(5) $[[A \wedge B] \rightarrow B]$
(6) $[A \rightarrow [B \rightarrow [A \wedge B]]]$
(7) $[A \rightarrow [A \vee B]]$
(8) $[B \rightarrow [A \vee B]]$
(9) $[[A \rightarrow C] \rightarrow [[B \rightarrow C] \rightarrow [[A \vee B] \rightarrow C]]$
(10) $[[A \leftrightarrow B] \rightarrow [A \rightarrow B]]$
(11) $[[A \leftrightarrow B] \rightarrow [A \rightarrow B]]$
(12) $[[A \rightarrow B] \rightarrow [[B \rightarrow A] \rightarrow [A \leftrightarrow B]]]$,

where A, B, and C are *arbitrary* formulas. (Some people would call (PL)(1)–(PL)(12) axiom schemata.) Next we have the axioms of *quantifier logic*:

(QL) (1) $[\forall \text{ v } A(\text{v}) \rightarrow A(t)]$
(2) $[A(t) \rightarrow \exists \text{ v } A(\text{v})]$,

where v is a variable and if v is a real [respectively, a function, functional]

variable, then t is a term [function variable, functional variable]. Following these we have the axioms of *equality logic:*

(EL) (1) $t = t$
(2) $t = u \rightarrow [A(t) \leftrightarrow A(u)]$,

where t and u are either both terms or both function or both functional variables. These axiom schemata (PL), (QL), (EL) are, of course, common to *all* theories as are the rules of *logical inference*:

(D) $$\frac{A \qquad [A \rightarrow B]}{\therefore A}$$

(U) $$\frac{[A \rightarrow B(v)]}{\therefore [A \rightarrow \forall\, v\, B(v)]}$$

(E) $$\frac{[B(v) \rightarrow A]}{\therefore [\exists\, v\, B(v) \rightarrow A]}$$

where in (U) and (E) the variable v is not free in the formula A. Rule (D) is called the rule of *detachment* (sometimes *modus ponens*), while (U) and (E) are the rules of *introduction of the universal and existential quantifiers.*

Turning now to the axioms dealing with our specific non-logical primitive notions, we cite first the axioms (OF) of an *ordered field*—axioms so familiar that we need not repeat them in detail here. To these we must adjoin the axiom of a *complete ordering* which can be formulated in many ways. For our system the principle asserting that a bounded function has a least upper bound is probably the simplest:

(CO) $[\exists\, y \forall\, x[f(x) \leqslant y] \rightarrow \exists\, z \forall\, y[z \leqslant y \leftrightarrow \forall\, x[f(x) \leqslant y]]]$.

The formulation of (CO) involves a function variable (the axioms (OF) do not); but since we have as yet no other axioms about functions, the principle (CO) could never be applied to derive any useful consequences (such as the Archimedean axiom). What is required are the following axioms:

(EF) (1) $[f = g \leftrightarrow \forall\, x[f(x) = g(x)]]$
(2) $[F = G \leftrightarrow \forall\, f[F(f) = G(f)]]$

(AC) (1) $[\forall\, x\, \exists\, y\, A(x, y) \rightarrow \exists\, f \forall\, x\, A(x, f(x))]$
(2) $[\forall\, f\, \exists\, y\, B(f, y) \rightarrow \exists\, F \forall\, f\, B(f, F(f))]$.

In the first group are the *axioms of equality* (sometimes, *extensionality*) *for functions and functionals* (actually the implication from right to left is sufficient in view of (EL)). Often these axioms are regarded as definitions, but this economy is not particularly useful nor, in the author's opinion, even conceptually desirable. Equality is such a basic notion that its properties are properly a part of logic. Of course, in a particular theory axioms are needed to give a characterization of equality appropriate to the notions

being axiomatized. Thus among the axioms (OF) we might very well choose to state

$$[x = y \leftrightarrow [x \leqslant y \wedge y \leqslant x]],$$

but hardly any one wishes to elevate this statement to the status of a definition.

In the second group we find the *axioms of choice.* Very often a special consequence of (AC) is singled out: namely, the *axioms of comprehension.* To obtain these weaker axioms we strengthen the hypothesis of (1), say, to

$$\forall\, x\ \exists\, !\, y\ \mathrm{A}(x, y)$$

where $\exists\, !\, y$ is read "there exists a *unique* y". In terms of the other logical symbols this can also be written as

$$\forall\, x\ \exists\, y\ \forall\, y_1[y = y_1 \leftrightarrow \mathrm{A}(x, y_1)].$$

Then the modified axioms simply state: every "rule" (that is, every function-like condition) determines (comprehends) an actual function which follows the rule. We often say "a function is a rule", but it is really the other way around: we make up rules in our mathematical language, and each such determines a well-defined function as an abstract mathematical object. It is just not always recognized that it takes an *axiom* to pass from stating the rule to asserting the existence of the function. The axiom of choice is stronger than the axiom of comprehension, because the "rule" is not assumed to determine uniquely the function value.

Some people feel that these principles about functions and functionals are so basic that they should be considered a part of logic. For one thing the axioms (EF) and (AC) would read the same whether we imagined the variables x, y, z as ranging over reals, or points, or integers, or what have you. In some ways it is just a matter of taste. But since there can be difference of opinion as to the inclusion of the axiom of choice (or the continuum hypotheses!), maybe it is better to draw the line separating logic from mathematics a little further back.

Some readers may have noticed that the functions and functionals we use are just of *one* argument. This is not a serious restriction. Pairs of real numbers could easily be identified with functions: for example, we could define (x, y) to be that function f where

$$f(z) = \begin{cases} x & \text{if } z = 0, \\ y & \text{if } z = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then functions of two arguments could easily be identified with those *functionals* that take the value 0 for functions that are not pairs in the above sense. If that method is felt to be artificial, then a special (real-valued!) pairing function could be added to the list of primitives together with the axiom

$$(x_0, y_0) = (x_1, y_1) \leftrightarrow [x_0 = x_1 \wedge y_0 = y_1].$$

(Actually such a pairing function can be *defined*; it is a Borel function of two arguments obtained from the process of merging decimal expansions. But that is even more artificial than the previous suggestion.) Or functions and functionals of several arguments could be taken as primitive by having special variables for them. Then the axioms (EF) and (AC) would have to be suitably extended in the obvious way. Such extensions (as well as the extensions to higher types of functionals on functionals on functionals) can safely be left to the imagination, for no essentially new ideas about formulation or about the independence proof are required.

In the formulation (CH′) of Section 1, the set of (non-negative) integers was used as the typical denumerably infinite set. There is definitely no need to take the notion of integer as a primitive, because it is so easily defined:

$$\mathbf{N}(y) \leftrightarrow \forall f[f(\mathbf{0}) = \mathbf{0} \wedge \forall x[\mathbf{0} \leqslant x \rightarrow f(x) = f(x + \mathbf{1})] \rightarrow f(y) = \mathbf{0}].$$

Read $\mathbf{N}(y)$ as "*y is an integer*" or simply consider $\mathbf{N}(y)$ as an abbreviation of the formula on the right-hand side of the biconditional.

Bringing together all our conventions we can finally state the version of the continuum hypothesis that in the next sections will be shown independent:

(CH″)

$$\forall h[\exists f \forall y[h(y) = \mathbf{0} \rightarrow \exists x[\mathbf{N}(x) \wedge y = f(x)]] \vee \exists g \forall y \exists x[h(x) = \mathbf{0} \wedge y = g(x)]].$$

3. Constructing the model. The usual method of showing that a certain statement is not derivable from given axioms is to exhibit a model in which the axioms are true but the statement is false. We shall do just that—except our model will require the re-interpretation of the logical as well as the non-logical primitives. The re-interpretation is not really a drastic one, however, and it uses a quite familiar mathematical notion: namely, the idea of an *event* in a probability space.

This is not too surprising. If we ask ourselves what mathematical structure is very much like the real numbers but still different enough to be interesting, one answer is *the random variables of a probability space.* We use random variables as if they were ordinary numbers—except they are not quite precisely placed in the continuum. They are just a little random (or maybe *very* random!). Still we can add and multiply them freely and can compare one to another. Unfortunately they are only partially ordered, not totally ordered, and as a ring they have zero divisors and do not form a field. So the analogy seems to break down. But it really does *not* break down, and this is just the point where the re-interpretation of the logical connectives is required.

Let $(\Omega, \mathscr{A}, P)$ be a probability space in the usual sense: Ω is the non-empty set of *sample points,* $\mathscr{A}$ is the σ-field of subsets of Ω called the *field of events,* and P is a countably additive measure on $\mathscr{A}$ taking on non-negative values and giving Ω measure 1 and is called the *probability measure.* Let $\mathbf{R}$ be

the set of ordinary real numbers, and let $\mathscr{R}$ be the set of *random real numbers* (random variables). The elements $\xi \in \mathscr{R}$ are just those functions $\xi: \Omega \to \mathbb{R}$ such that for all reals $r \in \mathbb{R}$

$$\{\omega \in \Omega: \xi(\omega) \leqslant r\} \in \mathscr{A}.$$

We make a slight abuse of language and identify the ordinary real numbers in $\mathbb{R}$ with the *constant* functions in $\mathscr{R}$. Then $\mathbf{0}$, $\mathbf{1}$, $+$, and $\cdot$ are interpreted in the obvious way. It is in the interpretation of $=$ and $\leqslant$ that we must exercise some care—but the idea is not unnatural.

If ξ and η are two random reals, then the statement

$$\xi = \eta$$

should *not* be regarded as having only two possible truth values—*true* or *false*. With random phenomena, answers cannot be set forth in such black and white terms. For example, as functions ξ and η might be equal almost everywhere, and then the equality statement should be regarded as true. In case the functions are equal on only 63% of the sample points, the statement must be regarded as partially false but not totally false (37% false to be exact). This idea can be made precise by introducing the *(reduced) algebra of events,* that is, the Boolean algebra

$$\mathscr{B} = \mathscr{A}/[P = 0]$$

which is the quotient algebra of the σ-field $\mathscr{A}$ modulo the σ-ideal $[P = 0]$ of events in $\mathscr{A}$ of P-measure zero. We shall refer to the elements of $\mathscr{B}$ simply as *events* from now on.

By dividing out the null sets we not only eliminate the distinction between *everywhere* and *almost everywhere* but most importantly: *$\mathscr{B}$ is a complete Boolean algebra.* This last remark is well known and is essential for the success of our method. Clearly $\mathscr{B}$ is a Boolean σ-algebra, but since the measure P lifts to a *strictly positive* measure on $\mathscr{B}$, it follows that $\mathscr{B}$ satisfies the *countable chain condition* (not more than countably many pairwise disjoint elements in $\mathscr{B}$). As a consequence, finding the *sup* of a family of elements of $\mathscr{B}$ can be reduced to finding the *sup* of a suitable countable subfamily, and in fact the *sup* will exist.

We shall use the symbols $\cup$, $\cap$, $\sim$, $\mathbb{0}$, $\mathbb{1}$ for the Boolean operations of union, intersection, and complement in $\mathscr{B}$ and for the zero and unit element of $\mathscr{B}$. Thus

$$\mathbb{0} = \varnothing/[P = 0],$$
$$\mathbb{1} = \Omega/[P = 0],$$

and if $E_0, E_1 \in \mathscr{A}$, then

$$E_0/[P = 0] \cup E_1/[P = 0] = E_0 \cup E_1/[P = 0].$$

We also use the symbols $\bigcup$ and $\bigcap$ for the infinite *sup* and *inf* of elements of $\mathscr{B}$, but in general if $E_i \in \mathscr{A}$ for $i \in I$, the equation

$$\bigcup_{i \in I} (E_i/[P = 0]) = (\bigcup_{i \in I} E_i)/[P = 0]$$

is *not* true. Of course it is true if the index set I is countable. The left side of the equation always makes sense, but notice that on the right side the union of E_i does not in general belong to $\mathscr{A}$ since $\mathscr{A}$ is only a σ-field.

Our re-interpretation of the logical notions is based on the idea that we can use $\mathscr{B}$ as a system of *generalized truth values*. $\mathbb{1}$ and $\mathbb{0}$ can be identified with *absolute* truth and falsity, but $\mathscr{B}$ permits in addition many other truth values intermediate between $\mathbb{0}$ and $\mathbb{1}$. Every statement A will be given a truth value in $\mathscr{B}$ which we will denote by $[\![A]\!]$. In particular the equility statement $\xi = \eta$ is given its obvious truth value as follows:

$$[\![\xi = \eta]\!] = \{\omega \in \Omega\colon \xi(\omega) = \eta(\omega)\}/[P = 0].$$

Similarly for $\xi \leqslant \eta$ we want

$$[\![\xi \leqslant \eta]\!] = \{\omega \in \Omega\colon \xi(\omega) \leqslant \eta(\omega)\}/[P = 0],$$

and for $\xi + \eta = \zeta$ we want

$$[\![\xi + \eta = \zeta]\!] = \{\omega \in \Omega\colon \xi(\omega) + \eta(\omega) = \zeta(\omega)\}/[P = 0],$$

and so on for any similar elementary equation or inequality relating polynomial combinations of random real numbers.

Suppose statements A and B already have well-determined Boolean truth values. Then we compute the truth values of their various propositional combinations by these simple rules:

$$\begin{aligned}
[\![\mathrm{A} \vee \mathrm{B}]\!] &= [\![\mathrm{A}]\!] \cup [\![\mathrm{B}]\!],\\
[\![\mathrm{A} \wedge \mathrm{B}]\!] &= [\![\mathrm{A}]\!] \cap [\![\mathrm{B}]\!],\\
[\![\neg \mathrm{A}]\!] &= \sim [\![\mathrm{A}]\!],\\
[\![\mathrm{A} \to \mathrm{B}]\!] &= [\![\mathrm{A}]\!] \Rightarrow [\![\mathrm{B}]\!],\\
[\![\mathrm{A} \leftrightarrow \mathrm{B}]\!] &= [\![\mathrm{A}]\!] \Leftrightarrow [\![\mathrm{B}]\!],
\end{aligned}$$

where for $E_0, E_1 \in \mathscr{B}$

$$\begin{aligned}
(E_0 \Rightarrow E_1) &= \sim E_0 \cup E_1,\\
(E_0 \Leftrightarrow E_1) &= (E_0 \Rightarrow E_1) \cap (E_1 \Rightarrow E_0).
\end{aligned}$$

By way of example consider the statement $[\xi \leqslant \eta \vee \eta \leqslant \xi]$. In view of the above rules the truth value of this statement is:

$$\{\omega \in \Omega\colon \xi(\omega) \leqslant \eta(\omega)\} \cup \{\omega \in \Omega\colon \eta(\omega) \leqslant \xi(\omega)\}/[P = 0].$$

But the union of those sets is clearly Ω, and we have shown

$$[\![\xi \leqslant \eta \vee \eta \leqslant \xi]\!] = \mathbb{1}.$$

In other words, even though neither of the statements $\xi \leqslant \eta$ nor $\eta \leqslant \xi$ need be absolutely true, they each have to be sufficiently partially true to make their *disjunction* absolutely true. A similar result holds for *any* elementary statement of real algebra involving random reals—provided the statement has no quantifiers and provided it is true for arbitrary ordinary reals. This applies to all the axioms for an ordered semi-ring: the associative, commutative, and distributive laws for $+$ and $\cdot$, and the laws of the neutral

elements 0 and 1, and the axioms of linear ordering for $\leqslant$ together with the monotonic laws for $+$ and $\cdot$ under $\leqslant$.

Turning now to quantified statements, we consider first how statements with quantifiers over real variables should be evaluated. Since the universally quantified statement is very much like a *conjunction* of all its instances, and the existentially quantified statement is like a disjunction, there is only one obvious way in which Boolean values can be assigned:

$$[\![\forall\, x\ \mathrm{A}(x)]\!] = \bigcap_{\xi\in\mathscr{R}} [\![\mathrm{A}(\xi)]\!],$$

$$[\![\exists\, x\ \mathrm{A}(x)]\!] = \bigcup_{\xi\in\mathscr{R}} [\![\mathrm{A}(\xi)]\!],$$

and similarly for variables other than the symbol x. Noting that an *inf* of Boolean values is $\mathbb{1}$ if and only if each of the values is $\mathbb{1}$, we see from our remarks in the last paragraph that

$$[\![\forall\, x\ \forall\, y[x \leqslant y \vee y \leqslant x]]\!] = \mathbb{1},$$

and likewise

$$[\![\forall\, x\ \forall\, y\ \forall\, z[x \leqslant y \to x + z \leqslant y + z]]\!] = \mathbb{1}.$$

A typical statement involving the existential quantifier is:

$$\forall\, x\ \exists\, y[x + y = \mathbf{0}].$$

Now a *sup* in a Boolean algebra may be equal to $\mathbb{1}$ without any of the terms being equal to $\mathbb{1}$; on the other hand, if one of the terms *is* $\mathbb{1}$, then so is the *sup*. Thus, if for each $\xi \in \mathscr{R}$ we can find an $\eta \in \mathscr{R}$ where

$$[\![\xi + \eta = \mathbf{0}]\!] = \mathbb{1},$$

then the value of the above quantified statement will also be $\mathbb{1}$. Obviously, we need only take $\eta = -\xi$. The general principle here is this: Consider a sentence of the form

$$(*) \qquad \forall\, x_0\ \forall\, x_1 \cdots \forall\, x_{n-1}\ \exists\, y\ \mathrm{A}(x_0, x_1, \cdots, x_{n-1}, y),$$

where the A part involves no quantifiers. If there is a *Borel* function φ such that for any n-tuple $(r_0, r_1, \cdots, r_{n-1})$ of *ordinary* real numbers the statement

$$\mathrm{A}(r_0, r_1, \cdots, r_{n-1}, \varphi(r_0, r_1, \cdots, r_{n-1}))$$

is *true*, then the Boolean value of the quantified statement is $\mathbb{1}$. The reason is that assuming the hypothesis, we have for all $\xi_0, \xi_1, \cdots, \xi_{n-1} \in \mathscr{R}$

$$[\![\mathrm{A}(\xi_0, \xi_1, \cdots, \xi_{n-1}, \varphi(\xi_0, \xi_1, \cdots, \xi_{n-1}))]\!] = \mathbb{1}.$$

Here $\eta = \varphi(\xi_0, \xi_1, \cdots, \xi_{n-1})$ is the *composition* of the random reals $\xi_0, \xi_1, \cdots, \xi_{n-1}$ with the Borel function φ. (We need to assume that φ is Borel to know that η actually belongs to $\mathscr{R}$.) Thus all the axioms (OF) for *ordered fields* obtain the value $\mathbb{1}$.

(As a matter of fact much more obviously holds. The sentences of the form (*) are called $\forall\exists$-*sentences*. If the A part involves only $\mathbf{0}$, $\mathbf{1}$, $+$, $\cdot$, and $\leqslant$,

we call them *algebraic* $\forall\exists$-sentences. The axioms for *real-closed fields* are just of this form. It follows from Tarski's decision method for the theory of real-closed fields that for each algebraic $\forall\exists$-sentence true of the reals, we can take the function φ that gives the desired values to the existentially quantified variable to be not only a Borel function but even to be piecewise algebraic. Thus all axioms for real-closed fields have Boolean value $\mathbf{1}$. But since *any* algebraic statement involving only $\mathbf{0}$, $\mathbf{1}$, $+$, $\cdot$, and $\leqq$ and quantifiers only over real variables which is true of the reals can be proved from these axioms by formal logical deduction, we see that all such statements have Boolean value $\mathbf{1}$. However, this conclusion is slightly premature, because we have not yet discussed the axioms of logic.)

Let us call a statement *valid* (maybe better: *Boolean valid*) if its Boolean value computed according to our rules is $\mathbf{1}$. So far we have seen that many statements that we know to be *true* of the ordinary reals are also *valid*. In other words, the random reals do form a reasonable model for the theory of real numbers (at least as far as the algebra goes) if we talk of valid sentences. This point of view resolves the problem of zero divisors among the random reals. It may very well happen that a product $\xi \cdot \eta$ is 0 almost everywhere, while neither ξ nor η is 0 almost everywhere. Thus the random reals as a ring (taken modulo equality almost everywhere, say) are *not* a model even for the axioms of an integral domain—in the usual sense of the word "model". On the other hand, if we assign to statements Boolean values rather than just simple truth values, then there is a perfectly natural sense in which the random reals are a model for the theory of ordered (even real-closed) fields.

To understand how well this new idea of a model works, we must discuss in detail the axioms of logic. If a statement is one of the axioms in the group (PL), then it is quite clear that it is valid. Even Boole knew that any law of propositional logic translates into an equation (some combination $=\mathbf{1}$) that holds in *all* Boolean algebras.

Next, for the discussion of the axioms of quantifier logic, we must at last face a slightly tiresome point about the use of variables and constants and the distinction between an object and its name. Up to now we have been rather free and easy in saying such things as:

$$\textit{If } \forall\, x\ \mathrm{A}(x) \textit{ is valid, then for all } \xi \in \mathscr{R},\ [\![\mathrm{A}(\xi)]\!] = \mathbf{1}.$$

Strictly speaking, this mode of expression is incorrect. In the first place, our formal language has no *names* for random reals. It does allow the formation of names of certain integers (viz. $\mathbf{0}$, $\mathbf{1}$, $\mathbf{1}+\mathbf{1}$, $(\mathbf{1}+\mathbf{1})+\mathbf{1}$, and so on), but even for the negative integers there is no direct way of naming them. Of course, the sentence

$$\mathrm{A}(-2)$$

is equivalent to

$$\exists\, x[x + (\mathbf{1}+\mathbf{1}) = \mathbf{0} \wedge \mathrm{A}(x)],$$

but that is indirect reference. Even allowing this, at most a countable number of reals can be serviced because there are only countably many combinations of our basic symbols. The answer is (possibly only temporarily) to extend the language by the introduction of new constant symbols to be used in formal combinations as the names of various objects. There is absolutely no difficulty in imagining such an extension. In particular, once we have determined that our model is going to use the specific random reals in $\mathscr{R}$, then we can set about introducing names for them.

Now the second difficulty lies in the anomaly of the phrase

$$[\![\mathrm{A}(\xi)]\!] = \mathbb{1}.$$

For $\mathrm{A}(x)$ is a formula which is only a string of symbols. The variable x is just a symbol. The random real ξ is a special kind of function; it is *not* a symbol. Therefore, it does not make good sense to ask to substitute a non-symbol ξ for a symbol x. Well, that problem, once faced, is not too serious. We need only have a way of constructing arbitrarily many new symbols, and then to the random reals we associate in a one-to-one manner these new symbols to be used as the *names* of the elements of $\mathscr{R}$. The exact way in which this construction is done is not very important. Therefore, having realized that it is necessary, we simply refuse to mention it. If someone questions us when we use $\mathrm{A}(\xi)$, we answer: Oh, that wasn't what was actually meant. What we really mean here is the result of substituting the *name* of ξ for the free occurrences of the variable. When we mention the equation $\xi = \eta$ we really mean the result of placing an equals sign between the *names* of ξ and η, and so on. This has to be done not only for random reals, but also for the objects whose names we will later on substitute for the function and functional variables.

Let us use the word *sentence* to refer to formulas without free variables and without any occurrences of these new names. The word *statement* will be used for formulas without free variables but which may contain the names (call these names *constants*). The axiomatic *theory* is only interested in the sentences. Investigation of the *model*, however, requires us to use these statements about its elements (or some equivalent device) in determining what is valid in the model—even if we only want to discuss the validity of certain particular sentences (such as (CH″), for example).

Actually, we do employ some formulas with free variables in setting up the axiomatic theory. This is not essential, however. We can always imagine these formulas with prefixed universal quantifiers on the free variables. Similarly, a formula with free variables is *valid* in our model if and only if each instance resulting by substitution of constants for the free variables in a valid statement. With these conventions in mind, we can return to the discussion of the axioms of quantifier logic.

A typical example of (QL)(1) is

$$[\forall\, x\ \mathrm{A}(x) \to \mathrm{A}((y + f(z)))].$$

To show that an implication is valid it is enough to show that the Boolean

value of its hypothesis is included in the Boolean value of its conclusion. Since the formula we have chosen has free variables (y, z, and f, at least), we imagine first that constants for specific objects have been substituted in for them. Now we have not yet determined how we are to interpret the notion of function in this model (that will be taken care of in the next section), but, no matter how it is done, the term $(y + f(z))$ will have some specific value after the substitution of the values for the variables. Say the value is ξ_0. By the rule for the universal quantifier, the Boolean value of the hypothesis is

$$\bigcap_{\xi \in \mathscr{R}} [\![A(\xi)]\!]$$

while the Boolean value of the conclusion is

$$[\![A(\xi_0)]\!].$$

Obviously, then, the first is included in the second. The dual argument establishes the validity of (QL)(2).

The preservation of validity by the rules (D), (U), (E) is as easily proved. In the case of (D), if every instance of A is valid, and every instance of $[A \rightarrow B]$ is valid, then the Boolean value of A is always $\mathbf{1}$ and is always included in the Boolean value of B, which is therefore valid. In the case of (U), let us suppose by way of example that $[A \rightarrow B(x)]$ is valid, where the variable x is not free in A. Thus the choice of an instance of A does not force any particular substitution for x. Hence the Boolean value of an instance of A is always included in the corresponding instance of $B(\xi)$, no matter which $\xi \in \mathscr{R}$ is used. Therefore, the Boolean value of the instance of A is included in the Boolean value of the instance of $\forall\, x\, B(x)$, which establishes the validity of the implication. The dual argument applies to (E). Notice that (QL)(1) and (U) correspond *exactly* to our interpretation of the universal quantifier as a Boolean *inf* in the complete algebra $\mathscr{B}$, and dually for (QL)(2) and (E).

The axioms of equality (EL) could be partially checked at this time, but it will be more interesting to discuss them within the context of our interpretation of functions and functionals to which we now turn.

4. Construction of the model continued: the concept of random functions and functionals. We have already seen that many functions on the ordinary reals $\mathbb{R}$ naturally extend to functions on the random reals $\mathscr{R}$. In particular, all Borel functions extend in this simple way. Suppose $\varphi: \mathbb{R} \rightarrow \mathbb{R}$ is a Borel function of one argument and let us use the same notation for its extension $\varphi: \mathscr{R} \rightarrow \mathscr{R}$. (Remember $\varphi(\xi)$ for $\xi \in \mathscr{R}$ is actually the composition $\varphi \circ \xi$, because the random reals are functions on the probability space.) Thus the extended φ is a function from $\mathscr{R}$ to $\mathscr{R}$ in the ordinary sense of the word, but does it not have some additional property that is not too specifically connected with its Borel character? The property we are seeking has to do with the behaviour of φ in combination with our

interpretation of equality. Given ξ and η, the event $[\![\xi = \eta]\!]$ can be quite arbitrary, but it is obvious that

$$(\#) \qquad [\![\xi = \eta]\!] \subseteq [\![\varphi(\xi) = \varphi(\eta)]\!]$$

holds for all $\xi, \eta \in \mathscr{R}$. In words: the mapping φ cannot make arguments less equal than they already are. Clearly there are many badly behaved functions from $\mathscr{R}$ into $\mathscr{R}$ that do *not* have the property (#). All Borel functions have this property. Suppose that $\psi: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is a Borel function of two arguments. Extend it to $\psi: \mathscr{R} \times \mathscr{R} \to \mathscr{R}$. Let $\eta_0 \in \mathscr{R}$ be fixed. Define $\varphi: \mathscr{R} \to \mathscr{R}$ by the equation

$$\varphi(\xi) = \psi(\xi, \eta_0)$$

for all $\xi \in \mathscr{R}$. Very likely φ will not be the extension of any ordinary Borel function, but it is quite clear that the φ so defined also has property (#). We call arbitrary functions from $\mathscr{R}$ into $\mathscr{R}$ having property (#) *random functions* and denote the class of all such functions by $\mathscr{R}^{\mathscr{R}}$.

Property (#) was discovered by considering that the axioms (EL) imply the formula

$$[x = y \to f(x) = f(y)].$$

This is such a basic truth of logic that there is no question that its validity must be preserved in choosing our interpretation of the notion of function. What seems remarkable is that this minimal requirement (namely, the property (#)) is sufficient to single out the proper class. But maybe it is not so remarkable: what else does one want of a function in general other than the fact that its values are uniquely determined by its arguments?

Before we can define what we mean by a *random functional* we must know the meaning of equality applied to functions. Clearly axiom (EF) forces us to define

$$[\![\varphi = \psi]\!] = \bigcap_{\xi \in \mathscr{R}} [\![\varphi(\xi) = \psi(\xi)]\!]$$

for all $\varphi, \psi \in \mathscr{R}^{\mathscr{R}}$. Then in strict analogy to (#) we call a mapping $\Phi: \mathscr{R}^{\mathscr{R}} \to \mathscr{R}$ a *random functional* if it satisfies

$$(\#\#) \qquad [\![\varphi = \psi]\!] \subseteq [\![\Phi(\varphi) = \Phi(\psi)]\!]$$

for all $\varphi, \psi \in \mathscr{R}^{\mathscr{R}}$. And equality between functionals is defined by

$$[\![\Phi = \Psi]\!] = \bigcap_{\varphi \in \mathscr{R}^{\mathscr{R}}} [\![\Phi(\varphi) = \Psi(\varphi)]\!]$$

for all $\Phi, \Psi \in \mathscr{R}^{\mathscr{R}^{\mathscr{R}}}$, the class of all random functionals. We could now easily go on to define what we mean by random functionals on random functionals, etc. In any case, the interpretation of the quantifiers on the function and functional variables is now specified.

The axioms of group (EF) are valid by definition and the axioms of (EL) are dismissed almost as easily. From our definition it is immediate that $[\![t = t]\!] = \mathbb{1}$ no matter what kind of term or constant t is. Thus (EL)(1) is valid. In our formulation of (EL)(2) we have used arbitrary formulas; however, it is enough to check only the cases of atomic formulas. In fact, the following particular cases are sufficient:

$$
\begin{aligned}
&[x = y \rightarrow [x = z \leftrightarrow y = z]],\\
&[x = y \rightarrow [z = x \leftrightarrow z = y]],\\
&[x = y \rightarrow [x \leqslant z \leftrightarrow y \leqslant z]],\\
&[x = y \rightarrow [z \leqslant x \leftrightarrow z \leqslant y]],\\
&[x = y \rightarrow [x + z = y + z]],\\
&[x = y \rightarrow [z + x = z + y]],\\
&[x = y \rightarrow [x \cdot z = y \cdot z]],\\
&[x = y \rightarrow [z \cdot x = z \cdot y]],\\
&[x = y \rightarrow [f(x) = f(y)]],\\
&[f = g \rightarrow [f(z) = g(z)]],\\
&[f = g \rightarrow [F(f) = F(g)]],\\
&[F = G \rightarrow [F(f) = G(f)]].
\end{aligned}
$$

Now the first eight of these formulas we already knew to be valid from the previous section's work, while the remaining four are valid by definition. Any other case of this *principle of replacement of equals by equals* can be built up by using various substitution instances of these and by combining them with the other laws of logic.

All of the checking up to this point has been rather trivial because we made everything work out more or less by definition; however, the proof of validity of (OC) and (AC) requires somewhat more labor. To check (AC)(1) let $A'(x, y)$ be the formula

$$[\forall\, x_1\, \exists\, y_1\, A(x_1, y_1) \rightarrow A(x, y)],$$

where $A(x, y)$ is the given formula. Note that by logic alone the formula

$$\forall\, x\, \exists\, y\, A'(x, y)$$

is valid and that the formula

$$\exists\, f \forall\, x\, A'(x, f(x))$$

is equivalent to (AC)(1). Hence we can drop the prime and be content with checking (AC)(1) in the case where the hypothesis of the implication is valid.

Let $\{\xi_\alpha\colon \alpha < \rho\}$ be a well-ordering of the set $\mathscr{R}$. (We are invoking the axiom of choice in the ordinary sense to validate the axiom of choice in the model. There is nothing wrong with doing this. Our job here is not to prove the consistency of the axiom of choice; Gödel has already done that.

Hence, we can feel free to employ the axiom.) Since we are assuming that $\forall\, x\, \exists\, y\, \mathrm{A}(x, y)$ is valid, we have for each $\alpha < \rho$:

$$\bigcup_{\beta<\rho} [\![\mathrm{A}(\xi_\alpha, \xi_\beta)]\!] = \mathbb{1}.$$

Let $E_{\alpha\beta} \in \mathscr{B}$ be defined by the equation

$$E_{\alpha\beta} = [\![\mathrm{A}(\xi_\alpha, \xi_\beta)]\!] \sim \bigcup_{\gamma<\beta} [\![\mathrm{A}(\xi_\alpha, \xi_\gamma)]\!].$$

Clearly for fixed α, the family

$$\{E_{\alpha\beta} \colon \beta < \rho\}$$

is a *partition of* $\mathbb{1}$ into pair-wise disjoint events. To be able to define the required function, we shall prove a

LEMMA. *For each $\alpha < \rho$, there exists an $\eta_\alpha \in \mathscr{R}$ such that for all $\beta < \rho$,*

$$E_{\alpha\beta} \subseteq [\![\eta_\alpha = \xi_\beta]\!].$$

Proof. Since at most countably many of the events $E_{\alpha\beta}$ are non-zero, we can find a partition of the space Ω by a family

$$\{\Lambda_{\alpha\beta} \colon \beta < \rho\}$$

where for each $\beta < \rho$,

$$E_{\alpha\beta} = \Lambda_{\alpha\beta}/[P = 0].$$

Define $\eta_\alpha \colon \Omega \to \mathbb{R}$ so that for all $\beta < \rho$,

$$\eta_\alpha \restriction \Lambda_{\alpha\beta} = \xi_\beta \restriction \Lambda_{\alpha\beta}.$$

The desired conclusion now follows.

Let $\varphi \colon \mathscr{R} \to \mathscr{R}$ be that function such that $\varphi(\xi_\alpha) = \eta_\alpha$ for all $\alpha < \rho$. The proof that $\varphi \in \mathscr{R}^{\mathscr{R}}$ reduces to showing

$$[\![\xi_{\alpha_0} = \xi_{\alpha_1}]\!] \subseteq [\![\eta_{\alpha_0} = \eta_{\alpha_1}]\!]$$

for all $\alpha_0, \alpha_1 < \rho$. Now by the definition of the events $E_{\alpha\beta}$ it is clear that

$$[\![\xi_{\alpha_0} = \xi_{\alpha_1}]\!] \subseteq (E_{\alpha_0\beta} \Leftrightarrow E_{\alpha_1\beta}).$$

(The validity of (EL)(2) is used here!)

Therefore, by our lemma:

$$[\![\xi_{\alpha_0} = \xi_{\alpha_1}]\!] \cap E_{\alpha_0\beta} \subseteq [\![\eta_{\alpha_0} = \xi_\beta]\!] \cap [\![\eta_{\alpha_1} = \xi_\beta]\!],$$

and so

$$[\![\xi_{\alpha_0} = \xi_{\alpha_1}]\!] \cap E_{\alpha_0\beta} \subseteq [\![\eta_{\alpha_0} = \eta_{\alpha_1}]\!].$$

Taking the *sup* over β gives us the result we need. Finally we note that the lemma also implies that

$$E_{\alpha\beta} \subseteq [\![\mathrm{A}(\xi_\alpha, \eta_\alpha)]\!],$$

so again taking the *sup* over β we have $A(\xi, \varphi(\xi))$ valid for all $\xi \in \mathscr{R}$. In particular, $\exists f \forall x\ A(x, f(x))$ must also be valid.

The proof of (AC)(2) is exactly the same. In fact, we could use the method to show that for any statement of the form $\exists y\ B(y)$, there exists a particular $\eta \in \mathscr{R}$ such that

$$[\![\exists y\ B(y)]\!] = [\![B(\eta)]\!].$$

The same is true for statements of the forms $\exists g\ C(g)$ and $\exists G\ D(G)$.

Finally we must check (CO). It is left to the reader to verify that it is sufficient to consider only those $\varphi \in \mathscr{R}^{\mathscr{R}}$ such that the statement

$$\exists y \forall x\ [\varphi(x) \leqslant y]$$

is *valid.* Assuming this, let $\eta_0 \in \mathscr{R}$ be chosen so that

$$\forall x[\varphi(x) \leqslant \eta_0]$$

is valid. For each rational number $q \in \mathbf{Q}$, the set of all rational numbers, define

$$E_q = [\![\forall x[\varphi(x) \leqslant q]]\!].$$

If we can show that there is a $\zeta \in \mathscr{R}$ such that for all $q \in \mathbf{Q}$

$$E_q = [\![\zeta \leqslant q]\!],$$

then it rather easily follows that

$$\forall y[\zeta \leqslant y \leftrightarrow \forall x[\varphi(x) \leqslant y]]$$

is valid, and (CO) is thereby verified. This last step is possible in view of the equation

$$[\![\zeta \leqslant \eta]\!] = \bigcap_{q \in \mathbf{Q}} [\![\eta \leqslant q \rightarrow \zeta \leqslant q]\!],$$

which is obvious from the definition of the Boolean value of an inequality. Checking these details is a simple exercise.

To complete the work and find the required ζ, we shall show that the E_q form a Boolean-valued analogue of a Dedekind cut in the rationals and that every such cut (uniquely) determines a random real (indeed this would be another way of defining random reals). First notice that

$$[\![\eta_0 \leqslant q]\!] \subseteq E_q \subseteq [\![\varphi(0) \leqslant q]\!]$$

for all $q \in \mathbf{Q}$. It follows that

(i) $$\bigcap_{q \in \mathbf{Q}} E_q = \mathbb{0},$$

(ii) $$\bigcup_{q \in \mathbf{Q}} E_q = \mathbb{1}.$$

From the definition it also follows that

(iii) $$E_q = \bigcap_{r > q} E_r$$

for all $q \in \mathbb{Q}$. Any system of Boolean values satisfying (i)–(iii) may be called a *Boolean-valued cut.* (The reader may check the sense of this by consideration of the extreme case where $E_q = \mathbb{o}$ or $\mathbb{1}$, and an ordinary cut is determined.)

Given (i)–(iii) for $E_q \in \mathscr{B}$ we want to choose $\Lambda_q \in \mathscr{A}$ such that

$$E_q = \Lambda_q/[P = 0]$$

and to have the Λ_q satisfy (i)–(iii) in $\mathscr{A}$. First make an arbitrary choice of Λ_q in the equivalence class E_q. By subtracting a set of measure 0 from all Λ_q for $q < 0$ (namely, the set $\bigcap_{q \in \mathbb{Q}} \Lambda_q$), and by adding a set of measure 0 to all Λ_q for $q \geqslant 0$ (namely, the set $\Omega \sim \bigcup_{q \in \mathbb{Q}} \Lambda_q$), we can assure (i) and (ii). But note that in view of (iii) for E_q,

$$E_q = (\bigcap_{r>q} \Lambda_r)/[P = 0].$$

Thus by replacing the set Λ_q by the set $\bigcap_{r>q} \Lambda_r$ all three of (i)–(iii) are obtained; hence we can assume (i)–(iii) for the Λ_q.

We may now define $\zeta\colon \Omega \to \mathbb{R}$ by the equation

$$\zeta(\omega) = \mathit{inf}\,\{q \in \mathbb{Q}\colon \omega \in \Lambda_q\}.$$

By (i)–(iii) for the Λ_q, we see that

$$\{\omega \in \Omega\colon \zeta(\omega) \leqslant q\} = \Lambda_q$$

holds for all $q \in \mathbb{Q}$. Therefore, for $q \in \mathbb{Q}$,

$$E_q = [\![\zeta \leqslant q]\!],$$

as was to be proved. This completes the checking of the validity of the axioms in the model.

5. The failure of the continuum hypothesis in a suitable model. Up to this point we have made no special assumptions on the probability space $(\Omega, \mathscr{A}, P)$. Thus Ω could have been a one-point space; the Boolean algebra $\mathscr{B}$ would then have degenerated to the two-element algebra with just $\mathbb{o}$ and $\mathbb{1}$; and the model constructed would have been the *standard model,* because $\mathscr{R}$ would be simply $\mathbb{R}$ and the functions and functionals would be arbitrary. But at least the previous sections show that *any* probability space leads to a model of the axioms in this Boolean-valued sense.

We want now to construct somehow a space where the random reals will fail to satisfy the continuum hypothesis. This would seem to be possible if we could only find a space with a very *large* number of random reals. Now a product space has a large number of random reals: the projections onto the coordinate spaces, and these are generally fairly independent functions. So this is our plan: let

$$\Omega = [0, 1]^I,$$

where $[0, 1]$ is the unit interval, and I is an index set of cardinality *strictly greater than* $2^{\aleph_0}$. We use ordinary Lebsegue measure on $[0, 1]$, and let P be the product measure which is defined on the σ-field of Baire subsets of Ω. For each $i \in I$, we let $\xi_i: \Omega \to [0, 1]$ be projection on the ith coordinate. These are random reals because they are measureable functions. For i, $j \in I$ we have

$$[\![\xi_i = \xi_j]\!] = \{\omega \in \Omega: \omega_i = \omega_j\}/[P = 0].$$

If $i \neq j$, this diagonal set has measure 0; thus

$$[\![\xi_i = \xi_j]\!] = \mathbb{0}.$$

The reason that the continuum hypothesis will fail in this model is roughly that, in view of the large number of random reals available, it is possible to select a portion of them to form a set that is neither countable nor in a one-to-one correspondence with all of them. This may seem at first sight self-contradictory. To resolve the seeming contradiction, remember that *two* notions of cardinality must be kept in mind: the ordinary one and the notion interpreted in the model. From the *outside* our model has more than a continuum number of random reals (in the ordinary sense of the word *continuum*), but *inside* the model the word *continuum* simply refers to *all* the random reals. By allowing our truth-value space to expand from $\{\mathbb{0}, \mathbb{1}\}$ to $\mathscr{B}$, we allow the notion of real number to undergo a corresponding expansion. By controlling this expansion (through the use of the product space construction which gives a large Boolean algebra which nevertheless satisfies the countable chain condition) we find that even the corresponding expanded notion of function will not permit us to avoid intermediate sets.

The intermediate set is going to be the set of zeros of a certain random function $\chi: \mathscr{R} \to \mathscr{R}$. To construct this function, let $J \subseteq I$ be a subset of I which is *uncountable* but still *not* of the same cardinality as I. (Recall that I is chosen to have more than a continuum number of elements.) We want χ to have the property that

$$\chi(\xi_j) = \begin{cases} 0 \text{ if } j \in J, \\ 1 \text{ if } j \notin J. \end{cases}$$

This can be done in the following way: For each $\xi \in \mathscr{R}$, let $\Lambda_\xi \subseteq \Omega$ be such that

$$\bigcup_{j \in J} [\![\xi = \xi_j]\!] = \Lambda_\xi/[P = 0].$$

We let

$$\chi(\xi)\ (\omega) = \begin{cases} 0 \text{ if } \omega \in \Lambda_\xi, \\ 1 \text{ if } \omega \notin \Lambda_\xi. \end{cases}$$

It is easy to check that χ is a random function. Also χ has the further property that for $\xi \in \mathscr{R}$,

$$[\![\chi(\xi) = \mathbf{0}]\!] = \bigcup_{j \in J} [\![\xi = \xi_j]\!].$$

We will show first that

$$[\![\exists\, g\, \forall\, y\, \exists\, x[\chi(x) = \mathbf{0} \wedge y = g(x)]]\!] = \mathbf{o}.$$

Assume the contrary. Choose a random function $\psi\colon \mathscr{R} \to \mathscr{R}$ such that

$$[\![\forall\, y\, \exists\, x[\chi(x) = \mathbf{0} \wedge y = \psi(x)]]\!] = E \neq \mathbf{o}.$$

For each $i \in I$, we have

$$E \subseteq [\![\exists\, x[\chi(x) = \mathbf{0} \wedge \xi_i = \psi(x)]]\!] = \bigcup_{\xi \in \mathscr{R}} \bigcup [\![\xi = \xi_j \wedge \xi_i = \psi(\xi)]\!] =$$

$$\bigcup_{j \in J} [\![\xi_i = \psi(\xi_j)]\!].$$

Thus for each $i \in I$, there is a $j_i \in J$ where $E \cap [\![\xi_i = \psi(\xi_{j_i})]\!] \neq \mathbf{o}$. Inasmuch as the set J has smaller cardinality than I and I is uncountable, there must be a fixed $k \in J$ such that the set $K = \{i \in I\colon j_i = k\}$ is *uncountable*. Now the events

$$D_i = E \cap [\![\xi_i = \psi(\xi_k)]\!]$$

for $i \in K$, are all non-zero, pair-wise disjoint, and uncountable in number. (They are pair-wise disjoint because for $i \neq i'$ we have $[\![\xi_i = \xi_{i'}]\!] = \mathbf{o}$.) We have thus contradicted the countable chain condition on $\mathscr{B}$, and therefore $E = \mathbf{o}$.

$$[\![\exists\, f\, \forall\, y[\chi(y) = \mathbf{0} \to \exists\, x[\mathbf{N}(x) \wedge y = f(x)]]]\!] = \mathbf{o}$$

is very similar. One must check first that

$$[\![\mathbf{N}(\xi)]\!] = \bigcup_{n \in \mathbb{N}} [\![\xi = n]\!],$$

where $\mathbf{N}(x)$ is the formula that gives the formal definition of being an integer and $\mathbb{N}$ is the set of ordinary (non-negative) integers. In this part of the argument the assumption that J is uncountable will be used. Therefore, the Boolean value of (CH′) is indeed $\mathbf{o}$, and our independence proof is complete.

6. Discussion of the proof and historical remarks. To those readers familiar with Cohen's original proof [1], [2] and [3], our approach may seem at first very different. Actually it is not. It was R. M. Solovay who first pointed out to the author [private communication, September 1965] that Cohen's definition of *forcing* could be viewed as a way of assigning Boolean values to formulas. (He had discovered this idea in a particular case by using Borel sets of positive measure as forcing conditions.) Indeed by associating with a formula the pair of sets consisting first of those conditions (weakly) forcing the formula and secondly, of those (weakly) forcing

the negation of the formula, Solovay noticed in general that these pairs formed a *complete Boolean algebra.* More important, the well-known properties of Boolean algebras, like distributive laws and the countable chain condition, could be shown to be responsible for the desirable properties of the models being constructed.

The author then suggested turning the tables and using the simple conditions on the assignment of the Boolean values as a way of avoiding the forcing definition. From this point of view it became very clear how an arbitrary complete Boolean algebra could be used for the values of formulas. This was already known to Solovay, because an abstract construction of forcing conditions could lead to any desired Boolean algebra as the algebra of pairs of sets of conditions. Of course, all in all, this is nothing more than a *reformulation* of Cohen's original method. It did have the advantage, however, that the use of the *countable* models of set-theory could be avoided if one was willing to work with Boolean values of formulas. This same advantage was also noticed by Vopěnka in his reformulation of Cohen's method in [10] and [11]. (Vopěnka's idea did not work as smoothly as Solovay's because he used strong forcing which requires the values of formulas to lie in a certain complete lattice which is not a Boolean algebra. The more useful Boolean algebra is simply a sublattice of Vopěnka's lattice.)

Then on January 1, 1966, it occurred to the author that once one accepts the idea of Boolean values there is really no need to make the effort of constructing a model for full transfinite set theory. In particular, the use of Gödel's method of constructible sets, which seemed so necessary for the transfinite recursive definition of forcing, could be completely avoided. In other words, Cohen's original method as re-interpreted by Solovay could be looked at as the construction of some very special Boolean-valued extensions of ordinary notions. But then when their simplest properties were recognized, we could take *all* the objects with those properties to form just as good a model as Cohen's (as we have done in defining random functions). It seems that by November 1965 Solovay had himself noticed that a Boolean-valued version of the power-set construction would lead to models for type theory and set theory; and, as he later pointed out, when Easton's version [4] of Cohen's method is used, the objects constructed by transfinite recursion will essentially give *all* the objects of the Boolean model. Still, it may just be possible that the use of Gödel's notion of constructibility in Cohen's style is necessary for some of the more delicate independence proofs, but most of the outstanding results seem to be adequately handled by the simpler construction. (In particular, the author found that the symmetry arguments needed for the independence proofs for the axiom of choice could be translated into automorphism arguments in the Boolean model. Thus the older idea of the Fraenkel-Mostowski proof could be reinstated almost intact. Cf. also [12] and [13].) A detailed report with a full demonstration of the connection with forcing is planned for [8].

The reader will have no doubt noticed that very little use was made of the probability measure P. Mainly, its role was to produce complete Boolean algebras as the quotient of a σ-field modulo the σ-ideal $[P = 0]$. This is a convenient device because it is so familiar, particularly in the construction of the product measure on $[0, 1]^I$. On the other hand, given any complete Boolean algebra $\mathscr{B}$ one can find a space Ω (the Stone space of $\mathscr{B}$), a σ-field of sets $\mathscr{A}$ (the σ-field generated by the clopen subsets of Ω), and an ideal $\mathscr{I}$ (the meager sets in $\mathscr{A}$) such that $\mathscr{B}$ is isomorphic to $\mathscr{A}/\mathscr{I}$ (cf. Halmos [5] for all facts about Boolean algebras needed in this paper). This means that an arbitrary complete Boolean algebra $\mathscr{B}$ can be used to construct a model in the way we have illustrated with the measure algebras. Indeed, the model obtained from the σ-field of Borel subsets of $[0, 1]^I$ modulo the ideal of meager sets gives a proof that is essentially Cohen's original method as will be explained in detail in [8]. The idea of using measure instead of category is due to Solovay [9] and has also been exploited by Sacks [7]. (Solovay's notion of *random real* mentioned in [9] is somewhat different from the author's since it was to be analogous to Cohen's *generic reals.* The comparison will be discussed in [8].)

Another point that may have troubled the reader is that we have not constructed a model for full set theory. He need not worry, however, for our model is just the initial segment of a model for set theory. In other words, the adjunction of random functionals of functionals of functionals . . . of functionals (iterated into the transfinite!) will lead to a model of set theory. This construction of the higher-type objects does *not* require, however, the introduction of *new* random reals or functions or functionals. Hence, the results we obtained regarding the continuum hypothesis will be in no way affected by the extension of the model. In particular, we can have models with classes (in the sense of von Neumann) which satisfy the full comprehension axiom without the cost of additional labor. This extension is not so easy with the original Cohen method. Vopěnka has a partial result in [11] in this direction.

Another confusing matter is our avoidance of countable models which Cohen in [2] thought were essential for his method. The answer is that our models are Boolean-valued and not $\{\mathfrak{o}, \mathbb{1}\}$-valued (i.e., ordinary) models. Cohen is quite right that if you want well-founded ordinary models you must keep everything countable. By working with forcing alone without going over to a model, he could have avoided countable models. This is the same as working with Boolean values and not demanding $\mathfrak{o}$-$\mathbb{1}$ values. On the other hand, if we want ordinary models, we can apply a homomorphism to the Boolean algebra to get them (Vopěnka does this in [10] and [11].) But an arbitrary homomorphism will give non-standard (non-well-founded) models. What one must do is first apply the Löwenheim-Skolem theorem to the Boolean model to obtain a suitable countable submodel (this is possible because in our Boolean model the value of every existential statement is equal to one of its instances). Then one applies the Rasiowa-Sikorski Lemma to obtain a homomorphism of the Boolean algebra onto

$\{\mathbf{o}, \mathbf{1}\}$ which preserves enough *sup*s to map the countable submodel onto a standard model. (Cohen's complete set of conditions does just this in the forcing framework.) To summarize, Cohen performs his homomorphism first, we do it last—if at all. But it amounts to the same thing.

Logicians may be irritated that the author chose in this paper to discuss the theory of real numbers rather than the formally simpler higher-order theory of the arithmetic of the integers. The main reason for the choice is notational. For readers not too familiar with logic, the author thought it would be easier for them to be able to stick to the *primitive notation*. That was also the reason for our choice of *functions* over *sets*. (By the way, the author is indebted to Professor Gödel who suggested that (CH′) is simpler to check than the version (CH) that uses countable ordinals (i.e., the construction of $\aleph_1$) which the author earlier employed.) Of course, we had to pay for this choice by our having to check (CO) which would have been avoided in the theory of the integers. However, now that the idea is exhibited, the reader ought to be able to carry through for himself the proof for the simple theory of types over the integers. On the other hand, the real numbers are always of mathematical interest, their construction from the integers is tiresome, so possibly it is better to see at once how they look in the model by our device of using the measurable functions. In particular, the author hopes that these Boolean models of real number theory may eventually be of interest in themselves apart from their role in the independence proofs.

REFERENCES

[1] COHEN, PAUL J., The independence of the continuum hypothesis, I, II. *Proc. Nat. Acad. Sci. U.S.A.* **50** (1963), 1143–1148; *ibid.* **51** (1964), 105–110.

[2] ——, Independence results in set theory. *The Theory of Models*, Proc. 1963 Internat. Symposium, Berkeley, Amsterdam, 1965, pp. 39–54.

[3] ——, Set theory and the continuum hypothesis. New York (1966).

[4] EASTON, WILLIAM B., *Powers of regular cardinals*. Ph.D Thesis, Princeton, 1964.

[5] HALMOS, PAUL R., *Lectures on Boolean algebras*. Van Nostrand Mathematical Studies, Princeton, 1963.

[6] RASIOWA, HELENA and ROMAN SIKORSKI, *The mathematics of metamathematics*. Monografie Matematyczne, Vol. 41, Warsaw, 1963.

[7] SACKS, GERALD E., Measure-theoretic uniformity. *Bull. Amer. Math. Soc.* **73** (1967), 169–174.

[8] SCOTT, DANA and ROBERT SOLOVAY, Boolean algebras and forcing, (in preparation).

[9] SOLOVAY, ROBERT, The measure problem. Abstract 65T-62, *Notices Amer. Math. Soc.* **12** (1965), 217.

[10] VOPENKA, PETR, The limits of sheaves and applications on constructions of models. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **13** (1965), 189–192.

[11] ——, On ∇-model of set theory. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **13** (1965), 267–272.

[12] JECH, T. and A. SOCHOR, On Θ-model of the set theory. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **14** (1966), 297–303.

[13] MAREK, W., A remark on independence proofs. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **14** (1966), 543–545.

(Received 17 December 1966)