Foundations of Mathematics in the Twentieth Century

V. Wiktor Marek and Jan Mycielski

1. INTRODUCTION AND EARLY DEVELOPMENTS. Logic and foundations are a domain of mathematics concerned with basic mathematical structures (in terms of which one can define all other mathematical structures), with the correctness and significance of mathematical reasoning, and with the effectiveness of mathematical computations. In the twentieth century, these areas have crystallized into three large chapters of mathematics: *set theory, mathematical logic (including model theory)*, and *computability theory*, which are intertwined in significant ways. In this paper we describe the evolution and present state of each of them. In modern times the study of logic and foundations has attracted eminent mathematicians and philosophers such as Cantor, Cohen, Frege, Gödel, Hilbert, Kleene, Martin, Russell, Solovay, Shelah, Skolem, Tarski, Turing, Zermelo, and others, and has given rise to a large body of knowledge. Although our paper is only a brief sketch of this development, we discuss essential results such as Gödel's theorem on the completeness of first-order logic and his theorems on the incompleteness of most mathematical theories, some independence theorems in set theory, the role of axioms of existence of large cardinal numbers, Turing's work on computability, and some recent developments.

There are still many interesting unsolved problems in logic and foundations. For example, logic *does not* explain what "good" mathematics is. We know that mathematics has a very precise structure: axioms, definitions, theorems, proofs. Thus we know what is correct mathematics but not why the works of certain mathematicians delight us while others strike us as downright boring. Nor do foundations tell us *how* mathematicians construct proofs of their conjectures. Since we have no good theoretical model of the process for constructing proofs, we are far from having truly effective procedures for automatically proving theorems, although spectacular successes have been achieved in this area. We mention other unsolved problems at the end of this paper.

We now give a brief sketch of the history of logic and foundations prior to 1900. The ancient Greeks asked: *what are correct arguments?* and: *what are the real numbers?* As partial answers they created the theory of syllogisms and a theory of commensurable and incommensurable magnitudes. These questions resurfaced in the 18th century, due to the development of analysis and to the lack of sufficiently clear concepts of sets, functions, continuity, convergence, etc. In a series of papers (1878–1897) Georg Cantor created set theory. In 1879 Gottlob Frege described a formal system of logic that explained precisely the logical structure of all mathematical proofs. In 1858 Richard Dedekind gave a definitive answer to the question: *what are the real numbers?* by defining them in terms of sets of rational numbers. He proved the axiom of continuity of the real line, an axiom accepted hitherto (beginning with the Greeks) without proof.

As for the question of characterizing correct arguments or proofs, Aristotle created the theory of syllogisms, which codifies certain forms of proof. In terms of modern logic, these were rules pertaining to unary relations. A relevant example is the syllogism: *if Socrates is a Greek and if all Greeks are mortal then Socrates is mortal.* Written in modern logical notation this syllogism takes the form

$$[Greek(Socrates) \wedge \forall x(Greek(x) \Rightarrow mortal(x))] \Rightarrow mortal(Socrates).$$

In this formula $Greek(\cdot)$ and $mortal(\cdot)$ are symbols for unary relations. We used the universal quantifier $\forall x \ldots$, which means *for all x we have* ... Similarly, one introduces the existential quantifier $\exists x \ldots$ which means *there exists x such that* ... For two thousand years the theory of syllogisms was the core of logic. In the 17th century G.W. Leibniz hoped to create a “characteristica universalis”, a language that would make it possible to express all mathematical sentences, and a “calculus ratiocinator”, which would reduce all reasoning to computation. In the middle of the 19th century G. Boole, guided by the algebra of numbers, introduced an algebra of sentences. We owe further evolution of these ideas to A. De Morgan, C.S. Pierce, G. Frege, and other mathematicians and philosophers. In particular, it became clear that the logic used in mathematics goes beyond syllogisms. Indeed, mathematics involves relations between two or more objects. For example, “less than” relates two numbers and is thus a *binary* and not a *unary* relation.

Cantor made the most important steps toward the determination of fundamental mathematical structures. He showed that (almost) all objects used by mathematicians can be thought of as sets. Moreover, it turned out that such an interpretation removed all ambiguities previously encountered in mathematics. For example, Zermelo and von Neumann used the concept of set to define the concept of a natural number. In turn, natural numbers could be used to define integers and rational numbers. B. Bolzano, R. Dedekind, and Cantor showed independently how to use sets of rational numbers to construct the real numbers and to prove their fundamental properties. Then functions were defined as sets consisting of ordered pairs, as we explain in Section 2. This new definition was simpler and more general than the earlier approach, which treated a function f as an algorithm for computing the value $f(x)$ for a given element x in the domain of f. In the 1880s and 1890s Cantor used this general concept of function to prove many theorems of set theory. He extended the concept of a cardinal number to infinite sets, analyzed notions such as linear order, and introduced the concept of well-ordering and the related concept of an ordinal number. He also used transfinite induction in definitions and proofs. This was a new method that went beyond induction over the natural numbers, already used in Euclid’s *Elements*.

There was no theory of computability at the end of the 19th century. The original concept of functions as algorithms was developed only later, beginning with the work of Turing in 1935. However, issues of effectiveness have concerned mathematicians and philosophers since ancient times. There were many examples of algorithms, such as Euclid’s algorithm for finding greatest common divisors, Cardano’s algorithm for solving cubic equations, Newton’s algorithm for finding zeros of differentiable functions, and Gauss’s algorithm involving the arithmetic-geometric mean. Some computing devices existed in antiquity. In many cultures there were types of abaci, some of which are still in use today. Mechanical computing devices for addition and multiplication were developed for use in censuses. Science, artillery, and finance required many accurate computations. The demand for computing devices for astronomy, engineering, taxation bureaus, banks, etc., grew steadily. In the first half of the 19th century C. Babbage proposed the construction of a machine similar to a modern storedprogram computer, but he was not able to complete this project. Up to the middle of the 19th century, many great analysts did not accept existential statements unsupported by algorithms. For example, to show that the initial value problem $y' = -y$, $y(1.3) = 2.4$, has a solution, one had to know how to construct it, i.e., one had to give a general prescription such that given any real number x one could compute the value $y(x)$ of the solution function y. Eventually, in the 20th century, the mathematical concept of a computable function was created by A. Church, K. Gödel, E. Post, and in a more definitive way by A. Turing.

An interesting prelude to the development of logic and foundations in the 20th century occurred in 1900. At the International Congress of Mathematicians in Paris, David Hilbert presented a lecture in which he stated 23 unsolved problems. Three of them, Nos. 1, 2, and 10, deal with logic and foundations:

> Problem 1 belongs to set theory and was originally posed by Cantor. It is called the *continuum hypothesis* and asks: *are there infinite sets of real numbers whose cardinality differs from the cardinality of the set of integers as well as from the cardinality of the set of all reals?*
>
> Problem 2 belongs to logic and asks: *are the axioms of analysis consistent?* In his lecture, Hilbert asked about the consistency of arithmetic. But by arithmetic he meant what is now called analysis: the arithmetic of the integers augmented by set variables and a full comprehension scheme that we discuss in Section 2.
>
> Problem 10 belongs to the theory of computability and asks: *is there an algorithm for deciding the existence of integral solutions of multivariable polynomial equations with integral coefficients*?

Thus the three areas of foundations of mathematics appeared in Hilbert's lecture. In the 20th century these three problems were solved in very surprising ways: K. Gödel and P.J. Cohen showed that the continuum hypothesis is independent of the generally accepted axioms of set theory (Table I). Gödel showed that Problem 2 is unsolvable. Moreover, no consistent theory containing enough combinatorics, whose axioms are explicitly given, can prove its own consistency. And M. Davis, Yu. Matiyasevich, H. Putnam, and J. Robinson showed that Problem 10 has a negative answer: no such algorithm exists.

Before continuing our presentation of logic and foundations we add some remarks about the relationship of this paper to the accounts of other historians and philosophers.

Some authors divide the study of logic and foundations into three orientations: intuitionism, logicism, and formalism. There are reasons to think that this division is misleading; first, because these three concepts are not of the same kind, and second, because logicism and formalism are terminological oxymorons. Specifically, intuitionism is not an attempt to explain what mathematics is, but rather a proposal for an alternative mathematics. On the other hand, logicism and formalism are such attempts, but the difference between them is rather insignificant. Since these terms turn up so frequently in the literature, it makes sense to discuss them in greater detail.

Intuitionism was invented in 1908 by L.E.J. Brouwer as a reaction to the freedom of imagination proposed by Cantor, Hilbert, and Poincaré (*in mathematics, to exist is to be free of contradiction*), and to the program of formalizing (that is, defining in mathematical terms) the rules of logic and the axioms of mathematics. Brouwer thought that freedom of imagination and formalization are incompatible; he also thought that many objects of classical mathematics are not sufficiently constructive. Developing these ideas, he rejected the existence of least upper bounds of nonempty bounded sets of reals (that is, the continuity of the real line) and many other nonconstructive statements. He proposed an alternative mathematics, called intuitionism, which was intended to be more meaningful than classical mathematics and to have a more meaningful logic (for example, the general theorem of classical logic *p or not p* was rejected; *p or not p* would be proved only by proving *p* or proving *not p*), and this logic would undergo perpetual development.

This program attracted some outstanding mathematicians, such as H. Poincaré and H. Weyl (although in their practice neither accepted all the strictures of intuitionism) and E. Bishop (who accepted them fully). However, intuitionism proved to be rather unsuccessful. It had two unpleasant technical features: its weak logic made it hard to prove theorems, so that many theorems of classical mathematics were rejected outright; and it has a plethora of concepts that are equivalent in classical mathematics but not under the weak logic of intuitionism. But Brouwer raised an issue that, if valid, would make up for these technical difficulties. He claimed that many concepts and objects of classical mathematics are meaningless. For example, he accepted the integers but rejected well-orderings of the real line.

Even today many mathematicians who are not familiar with logic and foundations would say that this sounds reasonable. But in 1904 Hilbert observed that the infinite sets of pure mathematics are actually imagined, in the sense that they are like containers whose intended content has not yet been constructed (imagined). The same view of sets was also held by Poincaré. This observation removed the existential (ontological) problem of infinite sets. Moreover, in 1923 the logic of Frege was extended by Hilbert to one in which quantifiers cease to be primitive concepts; they become abbreviations for certain quantifier-free expressions. In this way the apparent reference to infinite universes in pure mathematics, suggested by quantifiers, becomes a metaphor for a finite constructive process actually occurring in the human imagination (see Section 3). Thus the critique of classical mathematics raised by Brouwer and his followers collapsed. The authors of this article know of no clear motivation for intuitionism. The integers and their algebra (if we include some very large integers such as $10^{10^{10}}$) are no more constructive and finitary than any other mathematical objects and their "algebras". All we can say today in defense of Brouwer's idea is that some concepts of mathematics are useful in science and others are not; the latter must be regarded as pure art. But both kinds of objects are equally solid constructions of the human imagination and they become more permanent when expressed in writing.

Next we turn to logicism and formalism. Unlike intuitionism, they are attempts to explain what mathematics is. The first is attributed to G. Frege, B. Russell, and A.N. Whitehead, and its spirit is close to the philosophers of the Vienna circle. The second is attributed to D. Hilbert and his collaborators and to Th. Skolem, and is close to the Polish school of logic. The dividing line between logicism and formalism is not very significant because it depends merely on a terminological difference: whether set theory, or some of its variants (such as the theory of types), is included in logic. The term *logic* was used for a long time in the narrower sense (often called *first-order logic*), which does not include set theory; the growth of set theory and of model theory has motivated the modern terminology. An important fact that favors the more inclusive sense of logic (of Frege et al.) is the naturalness of the axioms of set theory; see Table I. They are so intuitive that they belong to the mental logic of almost all people who work in pure mathematics or use mathematics in science. Another reason why the term logicism is not used any more is that its program—to derive mathematics from logic in the wider sense—has been fully accomplished. This fundamental achievement is due mainly to Cantor and Dedekind. We say more about it in the next section.

To complicate matters, the term formalism has several meanings. First, it is associated with the problem posed by Hilbert in 1900 of proving the consistency of stronger (more expressive) theories in weaker theories, because this requires formalization of the stronger theory in the weaker one. Although in 1931 Gödel proved that such proofs do not exist, the idea of Hilbert gave rise to the problem of classification of mathematical theories according to their strength: we say that S is *stronger* than T if T is interpretable in S (e.g., analysis in set theory) but not vice versa. Gödel's results imply that S is stronger than T if the consistency of T can be proved in S. Work on the ensuing classification, which is sometimes called the *Hilbert program*, is still in progress. Second, formalism is used as a name for the philosophy of Hilbert that we discussed previously in connection with intuitionism. Brouwer called Hilbert a *formalist*, meaning that Hilbert professed that pure mathematics is just a formal game of symbols (Stalin levelled the same accusation against western art, which he called bourgeois art). This was unfair, since Hilbert insisted that mathematics is, first and foremost, a structure of thought-objects in our minds rather than of symbols on paper, and, if the word *game* can be applied to it, then the adjectives *interesting*, *beautiful*, and *often applicable* would have to be added as well. Thus, contrary to Brouwer's misnomer *formalism* for Hilbert's philosophy, the role of mathematics as an interface between science and art was essential to Hilbert.

2. SET THEORY. In the first decade of the 20th century, mathematicians clarified the concept of set. A naive approach to this concept, the *full comprehension scheme* of G. Frege and B. Russell, claims that "every class one can think of is a set", in symbols $\exists x \forall y [y \in x \iff \varphi(y)]$, where φ is any property expressed in the language of set theory. Russell himself found that this led to a contradiction when $\varphi(y)$ is the property $y \notin y$. Indeed, suppose that R is the collection $\{y : y \text{ is a set and } y \notin y\}$. It follows immediately from this definition that if R is a set then

$$R \in R \iff R \notin R.$$

This is a contradiction, hence R cannot be a set. It became clear that the concept of set had to be refined so as to avoid such contradictions. This is not to imply that the mathematical community, Cantor in particular, ever accepted the full comprehension scheme. Cantor knew that this scheme was too liberal and he had other examples to prove it. Collections defined by arbitrary formulas φ of the language of set theory are called *classes*. Cantor found that if the class of ordinal numbers were a set, then there would be an ordinal number not in that class—a contradiction; and if the class of all sets were a set, then its power set would have a cardinal number greater than itself—again a contradiction.

Something had to be done to make the concept of set clear and useful. This problem was solved by Russell and Whitehead, who constructed a weak set theory called the *theory of types*, and in a more satisfying way by E. Zermelo. In 1908 Zermelo proposed a system of axioms describing sets and methods for constructing them. These axioms do not imply that Russell's R, or Cantor's other classes, are sets. Zermelo's system, with certain improvements introduced by Th. Skolem and A. Fraenkel, became the generally accepted axiomatization of set theory. Almost all of mathematics can be developed within this theory, called Zermelo-Fraenkel set theory, or ZFC; see Table I.

These axioms describe a hierarchy of sets, among which are the natural numbers $0, 1, 2, \ldots$ First, taking any formula φ that is always false in axiom A4, we get a set with no elements. By axiom A1 this set is unique; we call it the *empty set* and denote it by $\emptyset$ or 0. By axiom A3, we have a set $\mathcal{P}(\emptyset) = \{\emptyset\}$ (also denoted by 1), which has the single element $\emptyset$. Then we have the set $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ (also denoted by 2). And given any two sets u and v we can build the set $\{u, v\}$ by using axiom A4 with

TABLE I. The Axioms of Set Theory ZFC

A1 **Extensionality** (Sets containing the same elements are equal):

$$\forall z[z \in x \leftrightarrow z \in y] \to x = y$$

A2 **Union** (The union u of all elements z of a set x is a set; $u = \bigcup(x)$):

$$\exists u \forall y[y \in u \leftrightarrow (\exists z \in x)[y \in z]]$$

A3 **Powerset** (The collection p of all subsets of a set x is a set; $p = \mathcal{P}(x)$):

$$\exists p \forall y[y \in p \leftrightarrow (\forall z \in y)[z \in x]]$$

A4 **Replacement** (The image r of a set d by a mapping φ is a set):

$$\forall x \exists z \forall y[\varphi(x, y) \to y = z] \to \forall d \exists r \forall y[y \in r \leftrightarrow (\exists x \in d)\varphi(x, y)]$$

(The axiom A4 is a scheme: for each formula φ we get a separate axiom. The formula φ may contain free variables other than x and y but not the variables d, r, or z)

A5 **Infinity** (There exists an infinite set s):

$$\exists s[\exists x[x \in s] \wedge (\forall x \in s)(\exists y \in s)\forall z[z \in y \leftrightarrow (z \in x \vee z = x)]]$$

A6 **Regularity** (Every non-empty set has an $\in$-minimal member):

$$\exists y[y \in x] \to (\exists y \in x)(\forall z \in y)[z \notin x]$$

A7 **Choice** (Every set x of non-empty, pairwise-disjoint sets y possesses a selector s):

$$\{(\forall y \in x)\exists z[z \in y] \wedge \forall yzt[y \in x \wedge z \in x \wedge t \in y \wedge t \in z \to y = z]\}$$
$$\to \exists s(\forall y \in x)\exists t \forall u[(u \in y \wedge u \in s) \leftrightarrow u = t)]$$

$d = \{\emptyset, \{\emptyset\}\}$ and

$$\varphi(x, y) := [(x = \emptyset \to y = u) \wedge (x = \{\emptyset\} \to y = v)].$$

We denote $\bigcup(\{u, v\})$ by $u \cup v$ and say that $x \subseteq y$ if and only if $x \cup y = y$. The ordered pair (x, y) is $\{\{x\}, \{x, y\}\}$ and the Cartesian product $a \times b$ is $\{(x, y) : x \in a \wedge y \in b\}$.

Another important definition, due to von Neumann, is the class *Ord* of ordinal numbers. These are sets α (such as the sets 0, 1, and 2) with the property:

$$\forall x, y[x \in y \in \alpha \to x \subseteq y \subseteq \alpha].$$

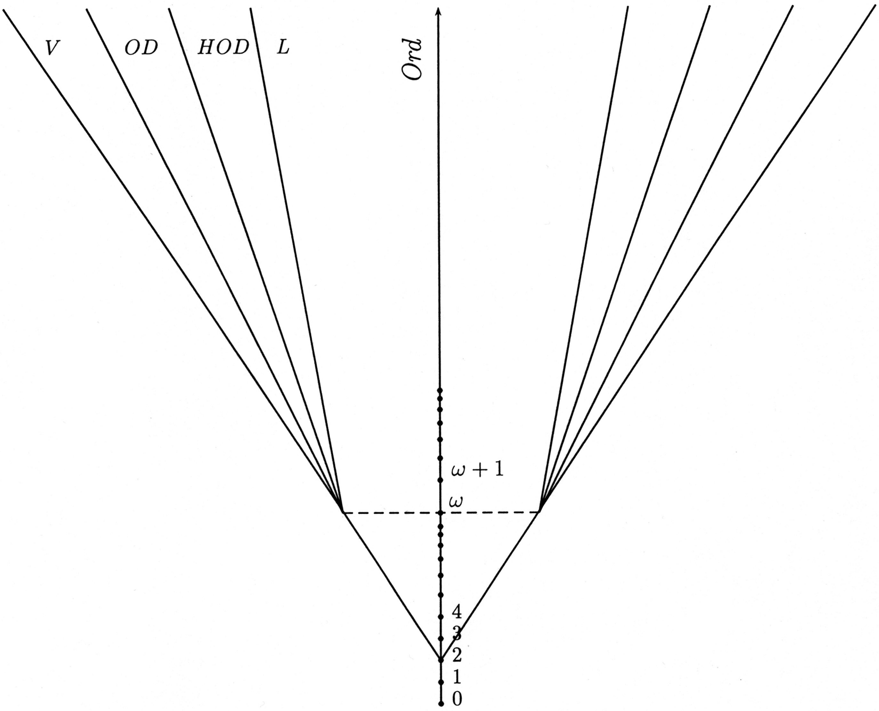
The class *Ord* of ordinal numbers is not a set. One proves that *Ord* is the smallest class containing $\emptyset$, closed under the operation $x + 1 = x \cup \{x\}$ and under arbitrary unions of sets of its elements. An ordinal λ is called a *limit* if $\bigcup(\lambda) = \lambda$. We denote the least infinite ordinal number by ω or N, so $\omega = N = \{0, 1, 2, \ldots\}$.

The members of an ordinal are well-ordered by the $\in$ relation, and in general we define a *well-ordering* to be any ordering isomorphic to an ordinal, or to *Ord* itself. The axiom of choice A7 implies that any set can be well-ordered (and the converse also holds); Zermelo introduced A7 for precisely this purpose.

Every set x can be assigned a unique ordinal number called its *rank* and defined as follows: $rank(\emptyset) = 0$ and $rank(x) = \bigcup(\{rank(y) + 1 : y \in x\})$. The set of all sets of rank at most α exists and is denoted by V_α. We can define V_α (where α is any ordinal) inductively by:

$$V_0 = \emptyset, \qquad V_{\alpha+1} = \mathcal{P}(V_\alpha), \qquad V_\lambda = \bigcup_{\xi<\lambda} V_\xi \text{ for limit } \lambda.$$

The class of all sets is denoted by V, so $V = \bigcup_\alpha V_\alpha$; see Figure 1.



$Ord \subseteq L \subseteq H\ O\ D \subseteq O\ D \subseteq V$;
ZFC is true in V, in $H\ O\ D$, and in L;
ZFC + GCH + V = L is true in L;
It is consistent with ZFC that not all real numbers are in OD;
$Ord : 0 = \emptyset; \quad \xi + 1 = \xi \cup \{\xi\}; \quad \lambda = \bigcup_{\xi<\lambda} \xi, \quad \lambda$ limit;
$V : V_0 = \emptyset; \quad V_{\xi+1} = \mathcal{P}(V_\xi), \quad V_\lambda = \bigcup_{\xi<\lambda} V_\xi, \quad \lambda$ limit;

Figure 1. Ordinal-definable, hereditarily ordinal-definable and constructible sets in the universe of Set Theory

It is a surprising and important fact (established by Cantor, Dedekind, von Neumann, and others) that all mathematical objects can be interpreted in a natural way as sets in V. A simple but important step of this interpretation was the construction (by Wiener and Kuratowski) of ordered pairs (x, y) as $\{\{x\}, \{x, y\}\}$. Later, D. Scott constructed cardinal numbers without using the axiom of choice, by defining the cardinal number of x to be the set of all sets y of least possible rank such that y can be bijectively mapped onto x.

The axiom of choice, A7, troubled some mathematicians. This axiom asserts that for any set x of nonempty and pairwise disjoint sets there is a set with just one element in common with each member of x. This generalizes an obvious property of finite collections of sets, but it leads to sets that are not explicitly definable. Mathematicians now use the axiom of choice in many of its equivalent forms, such as Zorn's lemma or the well-ordering principle, but of course accepting the axiom implies accepting its consequences, such as the *paradoxical decomposition of a ball* found by S. Banach and A. Tarski in 1924. Improving on an earlier theorem of F. Hausdorff, they showed that a ball can be divided into five disjoint sets that can be moved by isometries to form two balls of the same size as the initial ball. Of course, this contradicts physical experience. Thus one can say that the mathematical concept of a set is far more liberal than the concept of a physical body. In general, the consequences of the axiom of choice (for uncountable families of sets) are less relevant to applications of mathematics than are theorems whose proofs do not involve this axiom.

There is a weaker axiom of choice (called the *axiom of dependent choices* or DC) that does not have such odd consequences. DC says that if $A_0, A_1, \ldots$ is a sequence of nonempty sets and $R_i \subseteq A_i \times A_{i+1}$ are relations such that

$$(\forall x \in A_i)(\exists y \in A_{i+1})[(x, y) \in R_i],$$

then there exists a sequence $a_0, a_1, a_2, \ldots$ such that

$$\forall i[(a_i, a_{i+1}) \in R_i].$$

The classification of all sets by rank is paralleled by other classifications, not necessarily of all sets, by *ordinal definability* or *constructibility*. All of these classifications can be defined in the theory ZFC minus the axiom of choice, which is called ZF.

A set x is *ordinal-definable* if, for some ordinal α and some formula $\varphi(y)$, x is the set of elements y of V_α that satisfy the formula $\varphi(y)$ in V_α. The class of ordinal-definable sets is denoted by OD. HOD denotes the class of *hereditarily ordinal-definable sets*, i.e., sets such that they, their elements, the elements of their elements, and so on, are in OD. Gödel showed, without using the axiom of choice, that HOD satisfies all the axioms of ZFC. Thus if ZF is consistent then so is ZFC. The assumption $V = OD$ implies $V = HOD$ and the axiom of choice.

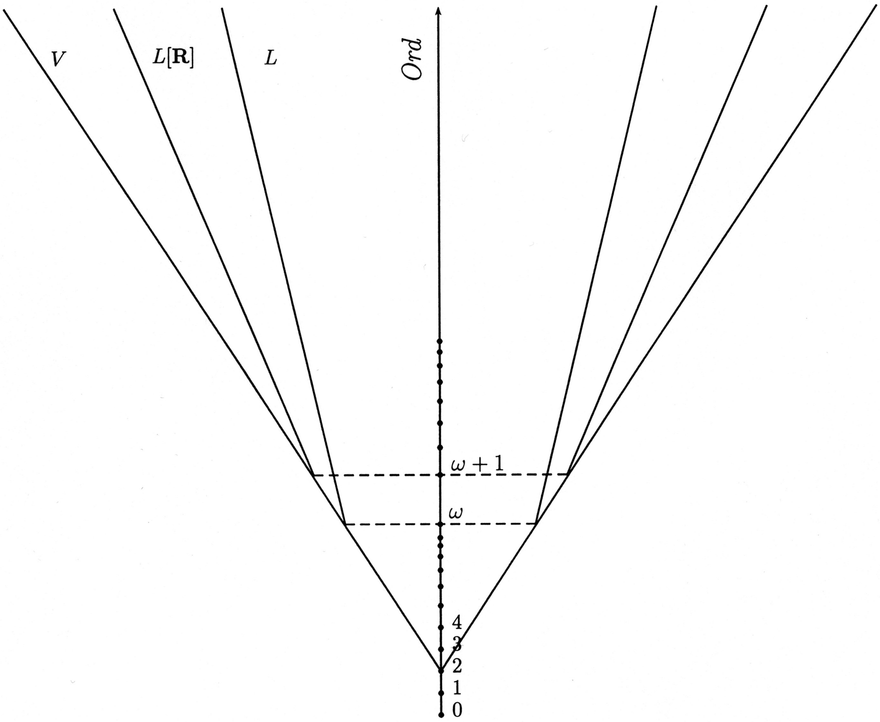
As mentioned in Section 1, the continuum hypothesis says that any infinite set of real numbers has either the cardinal number $\aleph_0$ of the set of integers or else the cardinal number $\mathfrak{c}$ of the set of all real numbers. ZFC implies that this hypothesis is equivalent to $\mathfrak{c} = \aleph_1$, where $\aleph_1$ is the cardinality of the shortest well-ordered uncountable set. Attempts to decide whether $\mathfrak{c} = \aleph_1$ have led to many interesting results. In the late 1930s Gödel showed that the continuum hypothesis is consistent with the axioms of ZFC, and in 1964 Paul J. Cohen showed that the axiom of choice does not follow from ZF and that the continuum hypothesis does not follow from ZFC.

Gödel's technique amounts to reversing the objections to the axiom of choice. Instead of asking how to define choice sets (selectors), he admits only the sets *constructible* by means of the following transfinite process. Working in ZF, we inductively define "constructible levels" L_α so that sets at a particular level are definable in the structure consisting of the objects at previous levels. Thus $L_0 = \emptyset$, $L_{\alpha+1} = Def(L_\alpha)$, and $L_\lambda = \bigcup_{\alpha<\lambda} L_\alpha$ for limit λ. Here $Def(\mathcal{A})$ is the operation that adds to $\mathcal{A}$ new elements, representing all subsets of $\mathcal{A}$ definable in terms of elements of $\mathcal{A}$.

This definition of L_α can be formalized in ZF because definitions are formulas, and formulas can be encoded by natural numbers. In fact, we can even construct a well-ordering of the universe $L = \bigcup_\alpha L_\alpha$ of constructible sets. This is done by induction. It is enough to define the ordering of a given level L_α. First we order "k-tuples" of objects from the previous levels. Then we order the given level by comparing pairs consisting of a code of a formula and a sequence of parameters (from the previous levels). This well-ordering of L shows that the axiom of choice holds in L.

To obtain the continuum hypothesis in L, Gödel proved a deeper theorem: all constructible real numbers occur in levels L_α with indices α that are countable in L. This readily implies the continuum hypothesis in L. What remains to be shown is that all the axioms of ZFC hold in L. We have already shown that the axiom of choice holds in L. Showing the validity of the other axioms of ZF in L is easy. Hence the axioms of ZFC remain consistent after adding the continuum hypothesis. Even the *generalized* continuum hypothesis—$2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for every ordinal α—holds in the universe L of constructible sets. Gödel also showed that all constructible sets (and only those) are constructible in L. Thus all the consequences of ZFC, and of the sentence "$V = L$" asserting that all sets are constructible, are true in L.

Although it is consistent to assume that $V = L$, it is more natural to assume that $V \neq L$, in which case the class L can be enlarged by adding sets from $V \setminus L$ and using them in an inductive definition of a larger universe. For example, inclusion of all the real numbers yields an interesting universe denoted by $L[\mathbf{R}]$; see Figure 2.



$Ord \subseteq L \subseteq L[\mathbf{R}] \subseteq V$;
ZFC is true in V and in L, ZF is true in $L[\mathbf{R}]$;
Under suitable large cardinal axioms ZF + $\forall X[AD(X)]$ + DC is true in $L[\mathbf{R}]$;

Figure 2. Sets that are constructible and constructible from reals in the universe of Set Theory

Cohen's argument for the independence of the axiom of choice and of the continuum hypothesis is more complicated than Gödel's. It can be explained as the construction of a *Boolean model*—a class of functions whose values belong to the Boolean algebra of open-closed subsets of a topological space. For suitable definitions of the membership and equality relations between such functions, the construction assigns the Boolean value **1** to all the axioms of ZFC. For a suitable choice of topological space the value of the continuum hypothesis in this model is **0**. But it can be shown that whatever is provable from formulas of value **1** in this model likewise has value **1**. Hence the continuum hypothesis is an independent sentence—it is not provable from ZFC. In a similar way, Cohen proved the independence of A7 (the axiom of choice) from ZF. His method, called *forcing*, was later used to obtain other independence proofs, for many well-known problems in set theory, real analysis, and algebra.

While these results show the independence of various sentences in ZFC, the truth or falsehood of most of them can be established in the two natural subuniverses L and $L[\mathbf{R}]$. The proofs of these theorems in $L[\mathbf{R}]$, however, require some extensions of ZFC. Specifically, they require cardinal numbers so large that their existence cannot be proved in ZFC.

The role of different universes, i.e., of different models of ZF, becomes particularly clear if we look at the *axiom of determinacy* introduced by J. Mycielski and H. Steinhaus in 1962. Let X be a set of infinite sequences of 0s and 1s, and consider the following game between two players I and II. Player I chooses 0 or 1, then player II chooses 0 or 1, then I again chooses 0 or 1, etc. When making their choices, both players know X and they know the previous choices. Player I wins if the sequence of 0's and 1's belongs to X, while player II wins if the sequence does not belong to X. The axiom of determinacy for X, $AD(X)$, states that one of the players has a winning strategy. Using the axiom of choice, one can show that there are sets X for which $AD(X)$ is false, i.e., for which neither of the players has a winning strategy. But if a model of ZF satisfies $AD(X)$ for all X, then this model is closer to physical reality than any model of ZFC. For example, the Banach-Tarski paradoxical decomposition of a ball is impossible. In 1989, D.A. Martin, J.R. Steel, and H. Woodin showed that if one assumes ZFC plus appropriate large cardinal axioms, then $L[\mathbf{R}]$ satisfies $AD(X)$ for all X, as well as the axiom DC of dependent choices. Whether $AD(X)$ holds for all $X \in OD$ remains an open problem; see the problems at the end of this paper.

The universes HOD, L, and $L[\mathbf{R}]$ are very different. For example, in HOD and L there are definable non-Lebesgue measurable sets of reals, while (under the assumption of the existence of a suitable large cardinal) in $L[\mathbf{R}]$ all sets of reals are Lebesgue measurable and $|\mathbf{R} \cap HOD| = \aleph_0$.

For these reasons, and because of their intrinsic interest, large cardinals have become an important topic. What are they? Here we introduce one type, called *measurable cardinals*. We call a cardinal number κ *measurable* if there is a measure, with values 0 and 1, defined on the family of all subsets of a set X of cardinality κ, such that the measure of every one-element set is 0, the measure of the whole set X is 1, and the measure of the union of fewer than κ sets of measure 0 is still 0. $\aleph_0$ is the smallest measurable cardinal. In ZFC it is not possible to prove the existence of measurable cardinals greater than $\aleph_0$. In fact, D. Scott showed in 1961 that $V = L$ implies that they do not exist. Thus we see that $V \neq L$ is a more natural assumption than $V = L$ since it does not rule out the natural idea of measurable cardinals.

But why are measurable cardinals called "large"? The reason is a 1930 theorem of Ulam that any measurable cardinal κ can "model the universe", i.e., the sets of rank less than κ satisfy all the axioms of ZFC. This, like the theorem of Scott just mentioned, implies that existence of measurable cardinals cannot be proved in ZFC. However, their existence (and that of other large cardinals) has interesting and deep consequences in real analysis, in the combinatorics of infinite sets, and even in the combinatorics of finite sets.

Practicing mathematicians, whether algebraists, geometers, or analysts, almost never use axioms beyond ZFC. This is surprising, since set theory was invented by Cantor more than 100 years ago and ZFC expresses only Cantor's assumptions. It is even more surprising, since mathematics is constantly enriched by definitions and theorems suggested by the physical sciences. Nonetheless, famous problems such as the four-color conjecture, Fermat's last theorem, Bieberbach's conjecture, and many others, were solved in ZFC; in fact, in weak subtheories of ZFC. It may be of some interest that large cardinal existence axioms (e.g., those used by Martin et al.) are not inspired by physical experience, but rather by concepts arising in the human imagination for which there are no ready physical interpretations. On the other hand, the axiom of determinacy was motivated by H. Steinhaus' wish to build a system of mathematics closer to physical experience than ZFC.

Independence of a sentence in set theory tells us nothing about its future, since it is possible that new developments in mathematics will decide this sentence. Independence tells us only that the sentence is false in some model of ZFC and true in another. If we limit ourselves to the universe of constructible sets, then we obtain theorems about sets of real numbers that are very different from those true in the universe of sets with a measurable cardinal.

Today, set theory plays a role similar to that played by Euclidean geometry for over 15 centuries (up to the time of the construction of mathematical analysis by Newton and Leibniz). Namely, it is a universal axiomatic theory for modern mathematics. It bears repeating that its axiomatization is not complete, and that new fundamental principles about sets are sometimes discovered or invented. Large cardinal axioms and the axiom of determinacy for the class $L[\mathbf{R}]$ are relevant examples. The evolution of mathematics decides which axioms become generally accepted.

Some axiomatic theories weaker than ZFC are still very strong in the sense that large chapters of mathematics can be developed in them. The simplest is PA (*Peano arithmetic*; see Table II). PA is so powerful that it allows us to prove all known theorems of classical number theory. However, there are theorems of finite combinatorics (which can be expressed somewhat artificially as number-theoretic statements) that are provable in ZFC but not in PA. We meet such theorems in the next two sections.

TABLE II. The Axioms of Peano's Arithmetic, PA
(Primitive symbols 1, $+$, $\cdot$)

PA1:	$x + 1 \neq 1$;
PA2:	$x \neq y \to x + 1 \neq y + 1$;
PA3:	$x + (y + 1) = (x + y) + 1$;
PA4:	$x \cdot 1 = x$;
PA5:	$x \cdot (y + 1) = (x \cdot y) + x$;
PA6:	$\varphi(1) \wedge \forall x[\varphi(x) \to \varphi(x+1)] \to \forall x \varphi(x)$, for every formula $\varphi(x)$, which may contain free variables other than x.

TABLE III. The Axioms of Second Order Arithmetic, Z_2
(Primitive symbols 1, $+$, $\cdot$ and $\in$)

$Z_2 1$–$Z_2 5$:	Formulas PA1–PA5 of table II;
$Z_2 6$:	$\forall x[x \in X \leftrightarrow x \in Y] \to [X = Y]$;
$Z_2 7$:	$\exists X \forall y[y \in X \leftrightarrow \psi(y)]$ where ψ is any formula of the extended language without the free variable X;
$Z_2 8$:	$1 \in X \wedge \forall x[x \in X \to x + 1 \in X] \to \forall x[x \in X]$.

The theory PA has a natural extension called Z_2 or *second order arithmetic*; see Table III. Z_2 is obtained from PA by adding a second sort of variables X, Y, ... called *set variables*, a binary symbol $\in$, an axiom of extensionality, the comprehension scheme, and the set form of the induction axiom PA6.

The theory Z_2 is a natural framework for the development of mathematical analysis, but it is much weaker than ZFC.

3. LOGIC AND MODEL THEORY. We now turn to mathematical logic and model theory, and to Hilbert's second problem. While Frege discovered the formalism of logic as early as 1879, introduction of a good system of notation took considerable time. In their *Principia Mathematica*, the first volume of which appeared in 1910, B. Russell and A.N. Whitehead popularized the modern notation for the Fregean syntax of logic. However, their system of logic also included a part of set theory. The first truly modern textbook of mathematical logic, written by D. Hilbert and W. Ackermann, was published in 1928. Then, in 1929, Gödel showed in his doctoral dissertation that Frege's rules of proof suffice to prove all logically valid sentences. We call this result the *completeness theorem for first-order logic.* It motivated the modern terminology according to which logic is the system of axioms and rules of Frege.

In 1924 Hilbert extended Frege's system by adding an operator ϵ for creating functions. If $\varphi(\bar{x}, y)$ is any formula (here $\bar{x}$ denotes any finite sequence of free variables), then Hilbert's operator gives a function symbol $\epsilon y\varphi$ of the variables $\bar{x}$; see axiom L6 of Table IV. This formalizes the mathematical practice of naming new objects and functions with desired properties: in this case, "a y such that $\varphi(\bar{x}, y)$ holds". If there is no such y, then the value $(\epsilon y\varphi)(\bar{x})$ does not matter and L6 holds automatically. Similarly, L7 allows any formula $\varphi(\bar{x})$ to be abbreviated by a single relation symbol $R_\varphi(\bar{x})$. Hilbert's extension has three advantages: (a) it simplifies the rules of logic, (b) choice functions are part of logic, so the axiom of choice follows from the remaining axioms of ZFC, and, most importantly, (c) it allows us to solve the ontological mystery of quantification over infinite universes.

TABLE IV. The Axioms and Rules of First Order Logic
(Essentially after G. Frege and D. Hilbert)

Primitive symbols: $\neg$ negation; $\to$ implication; $=$ equality symbol; sequences of variables $\bar{x} = (x_1, \dots, x_n)$ and $\bar{y} = (y_1, \dots, y_n)$, $(n \geq 0)$; ϵ an operator such that if $\varphi(\bar{x}, y)$ is any formula then $\epsilon y\varphi$ is a function symbol of n arguments (or a constant symbol if $n = 0$).

L1: $(\varphi \to \psi) \to [(\psi \to \chi) \to (\varphi \to \chi)]$;
L2: $\varphi \to (\neg\varphi \to \psi)$;
L3: $(\neg\varphi \to \varphi) \to \varphi$;
L4: If φ and $\varphi \to \psi$ are proved then ψ is proved;
L5: If $\varphi(x)$ is proved, then $\varphi(f(\bar{y}))$ is proved, where $f(\bar{y})$ is any term;
L6: $\varphi(\bar{x}, y) \to \varphi(\bar{x}, (\epsilon y\varphi)(\bar{x})))$;
L7: $R_\varphi(\bar{x}) \leftrightarrow \varphi(\bar{x})$;
L8: $x = x$;
L9: $x = y \to y = x$;
L10: $x = y \to (y = z \to x = z)$;
L11: $[x_1 = y_1 \wedge \dots \wedge x_n = y_n] \to [R(\bar{x}) \leftrightarrow R(\bar{y})]$, where R is any relation symbol of n variables;
L12: $[x_1 = y_1 \wedge \dots \wedge x_n = y_n] \to [f(\bar{x}) = f(\bar{y})]$, where f is any term of n variables.

First order logic generalizes the languages of ZFC, whose primitives are the relation symbols $\in$ and $=$, and of PA, whose primitives are the constant 1, the function symbols $+$ and $\cdot$, and the relation symbol $=$, to an arbitrary system of relation symbols R_i $(i \in I)$ and function symbols f_j $(j \in J)$. Our generalized language allows us to express properties of structures (called *interpretations* of the language), of the form:

$$M = \langle A, \tilde{R}_i, \tilde{f}_j \rangle_{i \in I,\ j \in J},$$

where A is a nonempty set and the $\tilde{R}_i$ and $\tilde{f}_j$ are relations and functions on A. Given any interpretation M of the language and any sentence σ in the language (for example, an axiom of ZFC or PA) we can talk about the *truth of σ in M*. M is called a *model* of a theory T if all the axioms of T are true in M.

In Table IV we list all the rules and axioms of logic. Notice that L1–L7, L11, and L12 are rules since φ, ψ, and χ are arbitrary formulas and R and f are arbitrary relation or function symbols. Similarly, A4 in Table I and PA6 in Table II were also rules; the other statements in Table I and II are single statements (axioms). The system presented in Table I and Table IV formalizes almost all of mathematics.

It is natural to add various abbreviations to Hilbert's system. The following are particularly important, and some of them have been used already.

$$\begin{aligned}
(\varphi \vee \psi) &:= (\neg\varphi \to \psi);\\
(\varphi \wedge \psi) &:= \neg(\varphi \to \neg\psi);\\
(\varphi \leftrightarrow \psi) &:= (\varphi \to \psi) \wedge (\psi \to \varphi);\\
(x \neq y) &:= \neg(x = y);\\
(x \notin y) &:= \neg(x \in y);\\
\{y : y \in z \wedge \varphi(\bar{x}, y)\} &= \epsilon t \forall y[y \in t \leftrightarrow y \in z \wedge \varphi(\bar{x}, y)](\bar{x}) \text{ (in the case of ZFC);}\\
\exists y \varphi(\bar{x}, y) &:= \varphi(\bar{x}, (\epsilon y \varphi)(\bar{x}));\\
\forall y \varphi(\bar{x}, y) &:= \varphi(\bar{x}, (\epsilon y(\neg\varphi))(\bar{x})).
\end{aligned}$$

Since this formalism avoids any reference to infinite universes, it defuses Brouwer's criticism of classical mathematics. Indeed, variables are merely places for substituting constant terms. And the quantifiers $\exists$ and $\forall$ are defined by the last two formulas. This elimination of quantifiers in favor of Hilbert's ϵ terms can be used to prove the completeness of first order logic, by first showing that any consistent set T of sentences has a model; this justifies Hilbert's slogan that *existence is freedom from contradiction*.

In 1929, Gödel proved the following fundamental theorem. If A is a set of sentences (axioms) then a sentence σ is derivable by rules L1–L12 from A if and only if for every model M of A, σ is true in M. This result is called the *completeness theorem for first order logic*. This result justifies the current significance of the word *logic*.

In 1950 Alfred Tarski initiated a systematic study of first-order theories and their models. Model theory has applications in algebra, algebraic geometry, functional analysis, and other areas of mathematics. One such application is *nonstandard analysis*. While 17th and 18th-century mathematicians used infinitesimals without defining them in a clear way, and while Cauchy introduced the ϵ–δ definition of continuity that allowed mathematicians to avoid their use, in the 1960s Abraham Robinson used model theory to introduce infinitesimals by clear and precise definitions and he made good use of them. However, nonstandard analysis is conservative in the sense that if a theorem is stated in the standard concepts and can be proved using nonstandard concepts, then it can also be proved without them.

In mathematical practice we almost always use many-sorted logic, that is, a language with various sorts of variables restricted to appropriate kinds of objects. Second order arithmetic, defined at the end of Section 2, is a good example. Likewise, when we analyze a ring, then, as a rule, we discuss not only the set of its elements but also the set of its ideals, which is a family of its subsets. Thus again we use two sorts of variables. However, one can reduce many-sorted logics to first-order logic with additional unary relation symbols.

Hilbert's second problem was to prove the consistency of the theory Z_2 of Section 2. How could this consistency be established? Hilbert recognized that as soon as a theory T is axiomatized and its rules of proof are spelled out, the consistency of T becomes a combinatorial problem. Since PA can express all problems of finite combinatorics, Hilbert proposed proving the consistency of Z_2 in PA. PA appears to be consistent, because its only problematic part is the induction scheme PA6, and PA6 is corroborated by the following experiment: if one knocks down the first in a row of dominoes, and if every falling piece knocks down the next, then, no matter how many pieces there are, they all fall down.

Generalizing, we can ask for a proof of the consistency of ZFC, i.e., of most of mathematics, in PA. Hilbert thought that PA is complete and so he believed that such proofs can be found. But in 1931 Gödel proved that PA is *not* complete and, moreover, that one cannot prove the consistency of PA *within* PA. Hence it is impossible to prove the consistency of Z_2 or of ZFC in PA, and the solution sought by Hilbert does not exist.

The theorems that wrecked Hilbert's program are called Gödel's *first* and *second incompleteness theorems*. He proved them by encoding symbols, formulas, and sequences of formulas by numbers. When this is done appropriately we can say, *in the language of* PA, what it means for a number to be the code of a correct proof. Then the language of PA can express a sentence Con(PA) that says that PA is consistent; Con(PA) says "There is no proof of the formula $1 \neq 1$ from the axioms of PA."

Gödel showed that if PA is consistent, then it contains no proof of Con(PA)! More generally, he showed that a consistent theory T containing PA, in which the consistency of T can be expressed by a sentence $\mathrm{Con}(T)$, cannot prove $\mathrm{Con}(T)$. Of course, we can prove Con(PA) in ZFC. We can also show in ZFC that the negation $\neg$Con(PA) has no proof in PA (because ZFC proves that PA has a model). Hence PA is not a complete theory, and neither is any consistent extension of PA by a set of axioms whose set of codes is definable in the language of PA. In particular, none of these theories proves its own consistency. In this strong sense, Gödel showed that Hilbert's second problem of proving consistency cannot be solved.

This brings us to an important ordering of theories, in which $S < T$ means that $\mathrm{Con}(S)$ is provable in T:

$$\mathrm{RCF} < \mathrm{PA} < \cdots < \mathrm{A}_i < \cdots < \mathrm{ZFC} < \cdots < \mathrm{ZFC} + \mathrm{LC}_i < \cdots$$

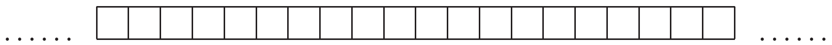
RCF (called the theory of real closed fields) is the theory of the field of real numbers $\langle \mathbf{R}, +, \cdot, < \rangle$, which happens to be a complete theory. PA was defined in Table II; A_i are various axiomatic systems of analysis (Z_2 among them); ZFC was defined in Table I; LC_i are various axioms of existence of large cardinals (some were discussed in Section 2).

Various interesting combinatorial theorems of ZFC that can be stated in the language of PA have been found to be independent of PA. This is the case for some strong forms of Ramsey's theorem on the coloring of graphs. In fact, H. Friedman, L. Harrington, R. Laver, J. Paris, and R. Solovay have proved that some such sentences are intimately related to the existence of large cardinals.

4. COMPUTABILITY THEORY. Now we turn to problems of computability, and to Hilbert's 10th problem. While proving the incompleteness theorem discussed in Section 3, Gödel considered a class of functions now called computable or recursive (though without claiming that they captured the intuitive notion of computability). A function $f : N \to N$ is *computable* if there exists a formula $\varphi(x, y)$ of the language of PA such that $\varphi(n, m)$ is a theorem of PA if $f(n) = m$, and $\neg\varphi(n, m)$ is a theorem of PA if $f(n) \neq m$. Here m and n denote any terms of the form $1 + \cdots + 1$ and $f(n)$ is also represented in this way. This definition of computability is robust in the sense that replacing PA by a stronger theory, e.g., by ZFC, gives the same class of computable functions. Around 1935, Post, Church, and Turing proposed alternative definitions of computable functions and later all these definitions were proved to be equivalent.

Turing's definition constitutes a theoretical model of the modern computer. In 1935 he introduced the concept of a machine, now called a *Turing machine*, and proved the existence of a *universal machine*: a machine that, given an appropriate code, is capable of simulating the work of any other Turing machine. Turing's definition of computability does not depend on the notion of proof and leads to many interesting concepts, theorems, and still unsolved problems.

A *Turing machine* M is a function $M : A \times S \to A \times S \times C$, where A is a finite set called an *alphabet*. We assume without loss of generality that A consists of only three letters, 0, 1, and the blank symbol $\Box$. S is a finite set called the *set of states* or *memory* of M, and C consists of three symbols: R, L, Q called *right*, *left*, and *quit*, which we call *commands*. The letter $\Box$ and a certain state s_0 in S play special roles. Such a machine M acts upon an infinite tape



whose squares are filled with single letters of A. At time 0 we have a doubly infinite string of letters $\ldots a_{-1}^0 \; a_0^0 \; a_1^0 \ldots$. The machine always starts at the location 0 and in the state s_0; thus it first looks at a_0^0 and evaluates $M(a_0^0, s_0) = (a_0^1, s_1, c)$. It erases a_0^0, and puts a_0^1 in its place. Then it moves left or right or quits depending on the value of the command c. If it quits, it declares that its job is finished. If it moves right, it looks at the current content of the cell with the index 1, and if it moves left, it looks at the current content of the cell with the index -1. Then, if this content is a, it evaluates $M(a, s_1)$, and acts again in the same way. M works in this way until (if ever) the third component c becomes Q, in which case it halts. Notice that only a single cell on the tape is affected at each time step. The machine creates the sequence of consecutive tapes $\ldots a_{-1}^n \; a_0^n \; a_1^n \ldots$ where $n = 0, 1, \ldots$ is the number of steps.

The initial tape $\ldots a_{-1}^0 \; a_0^0 \; a_1^0 \ldots$ is called the *input*, and the final tape (if M reaches Q) is called the *output*. From now on we assume that the input is of the form $\ldots \Box\Box w \Box\Box \ldots$ where w is a finite string of letters from the alphabet A, which we denote briefly by w. We also assume that at time 0 the first letter of w is at the location 0.

Any machine M is determined by a table of function values proportional in size to its set S of states, hence M can be coded by a finite sequence of 0s and 1s of length at most $K|S|\log|S|$, where K is an absolute constant. We denote the code of the machine M by $code(M)$.

A *universal* machine M_0 is one that, given any input of the form $code(M)\Box w$, works like M on the input w. Thus M_0 halts for the input $code(M)\Box w$ if and only if M halts for the input w, and it yields the same output. An important theorem of Turing says that universal Turing machines exist.

The concept of a Turing machine has philosophical significance because of the following suggestive analogies:

$$\frac{\text{Turing machine}}{\text{its tape}} = \frac{\text{organism}}{\text{its environment}}$$

$$\frac{\text{universal Turing machine}}{\text{the code part of its input}} = \frac{\text{human being}}{\text{its knowledge}}.$$

These analogies are supported by the fact that for every real-world computational procedure (algorithm) there exists a Turing machine that can perform that procedure. A universal Turing machine M_0 is a theoretical model for a programmable computer.

Turing machines permit us to define the concept of computable function as follows. A function $f : D \to N$, where $D \subseteq N$, is called *computable* if there is a Turing machine M which converts any input $n \in D$ to output $f(n)$, and does not halt for input $n \notin D$. Turing proved that if $D = N$ then this definition is equivalent to Gödel's definition stated at the beginning of this section: the main difficulty was to show that there is a Turing machine that enumerates all the codes (Gödel numbers) for theorems of PA and only such numbers.

The idea of a machine enumerating objects is formalized by the concept of a *recursively enumerable set*, which may be defined as the domain of a computable function. The set of consequences of a finite set of axioms is a typical example of a recursively enumerable set. More generally, the consequences of a recursively enumerable set of axioms (such as PA) are recursively enumerable. The latter set is one for which the membership problem is *undecidable*: although there is a Turing machine that lists all theorems of PA, there is no machine that lists all nontheorems, and hence no machine that correctly distinguishes theorems from nontheorems.

The negative solution of Hilbert's 10th problem comes from a new characterization of recursive enumerability, achieved by the efforts by many mathematicians in the years 1950–1970. M. Davis, Y. Matiyasevich, H. Putnam, and J. Robinson showed that for every recursively enumerable set $X \subseteq N$ there is a polynomial $p(x, x_1, \ldots, x_n)$ with integer coefficients such that $x \in X$ if and only if there exist integers $y_1, \ldots, y_n$ such that $p(x, y_1, \ldots, y_n) = 0$. It follows (by taking p to represent a set X with undecidable membership problem) that there is no algorithm for deciding, for each x, whether the equation $p(x, x_1, \ldots, x_n) = 0$ has an integer solution. Thus even elementary number theory is a profound subject, so profound that there is no uniform method for solving its most natural problems.

Another important concept of computability theory, due independently to Solomonoff, Kolmogorov, and Chaitin, is that of an *incompressible sequence*. This formalizes the idea of a sequence that cannot be generated by a program shorter than itself. Let $|w|$ denote the length of the sequence w. Then a finite sequence v of 0s and 1s is *incompressible* relative to a universal Turing machine M_0 if, for every code w such that M_0 with the input $w\Box 0$ yields the output v, we have $|w| \geq |v|$. Since there are 2^n sequences of length n and $2^n - 1$ sequences of length $< n$, there exists an incompressible sequence of any length n.

Chaitin showed that for every theory T with a recursively enumerable set of axioms, and every universal machine M_0, there are only finitely many sequences that T can prove to be incompressible relative to M_0. This is another concrete form of the Gödel incompleteness theorem: only *finitely many* sentences of a certain type can be proved, although infinitely many of them are true. Thus proving such sentences always remains an art, rather than a science.

Here is Chaitin's interesting proof. Let M_T be a Turing machine that enumerates the theorems of T. For each natural number c we upgrade M_T to a Turing machine M_T^c that, given the input 0, searches for a sequence s with $|s| \geq c$ that T proves to be incompressible relative to M_0, and if it finds such a sequence it prints s and stops. We can define M_T^c so that the code of M_T^c relative to M_0 is no longer than

$$|code(M_T)| + K_1 \log_2 c + K_2,$$

where K_1, K_2 are constants independent of c. Now choose c so that

$$|code(M_T)| + K_1 \log_2 c + K_2 < c.$$

Then M_0 applied to the input $code(M_T^c)\Box 0$ does not halt; otherwise its output s would be compressible, contrary to the definition of M_T^c. Therefore, T proves no theorem of the form "s is incompressible" for $|s| \geq c$.

We now turn to some other important concepts of computability theory, formalizing the *time and space complexity* of problems. An algorithmic problem in mathematics typically consists of an infinite set L of questions, each of which may be encoded by a finite sequence of 0s and 1s. A solution may be embodied in a Turing machine M that takes each such question w as input and eventually gives the answer (say, giving output 1 for "yes" and 0 for "no"). In this case the set L is said to be *decidable*. Similarly, a theory T is called decidable if the set of its theorems is decidable.

If we are interested not only in the existence of a solution, but also in its *feasibility*, then we impose a bound on the time or space used in the computation. We say that L is *decidable in polynomial time* ($L \in$ PTIME) if there is a Turing machine M and a polynomial $p(x)$ such that M decides whether $w \in L$ in no more than $p(|w|)$ steps. An example is the problem of checking multiplication of integers: given an equation $c = ab$ of length n, we can multiply the numbers a and b, and can then compare the result with c, in around n^2 steps. Hence checking multiplication is a PTIME problem.

The class PSPACE (*polynomial space*) is defined similarly, except that now we require M to visit no more than $p(|w|)$ cells of the tape; the number of steps does not matter.

Finally, we say that $L \in$ NPTIME (*nondeterministic polynomial time*) if there is a Turing machine M and a polynomial $p(x)$ such that $w \in L$ if and only if there is a v such that, given the input $w\Box v$, M stops in at most $p(|w|)$ steps.

The classes PTIME and PSPACE are natural candidates for classes of *feasibly decidable* problems, with respect to time and space, respectively. The significance of NPTIME is that M is allowed to incorporate a "guess" v in its computation. This is the nondeterministic ingredient, and we illustrate its naturalness by two examples.

4.1 The problem of deciding whether an n-digit integer c is composite is not known to be PTIME. However, a Turing machine M can solve this problem in around n^2 steps with the help of a correct "guess" $c = ab$, i.e., by giving M the guess $a\Box b$. Then M needs to check only the multiplication, so the problem of recognizing composite numbers is in NPTIME.

4.2 Gödel's incompleteness theorem implies that no consistent, recursively enumerable theory containing PA is decidable. We can of course decide, given a sentence σ and integer n, whether σ has a proof with fewer than n symbols. In fact, this is an NPTIME problem, because if a correct proof is guessed, one can check it in polynomial time. But again we do not know whether this problem is in PTIME. Gödel posed this question in a letter to von Neumann; most mathematicians believe that the answer is negative.

It is easily seen that

$$\text{PTIME} \subseteq \text{NPTIME} \subseteq \text{PSPACE}.$$

An important theorem of S. Cook says that if problem 4.2 is in PTIME, then PTIME = NPTIME. There are many other such problems (called NP-*complete*), which are important in combinatorics, computer science, and applications of mathematics.

5. CONCLUDING REMARKS. What is mathematics? Mathematical practice and logic and foundations indicate that mathematics is the *art*, rather than the *science*, of constructing deductive theories. For example, while the Goldbach conjecture (every even number greater than 2 is a sum of two primes) is a well established empirical fact, mathematicians do not include it as an axiom because it is not a basis for an interesting theory. Also, it may turn out to be provable in PA or ZFC. Thus mathematics is the art of deduction rather than a list of facts. On the other hand, the study of nature often suggests new mathematical conjectures and sometimes even their proofs, and from time to time it suggests new fundamental axioms that yield interesting theories. In particular, logic is a study of ways in which nature has prepared us to describe reality, a study of natural intelligence. Even the concept of infinite sets is suggested by some apparently unending processes, and by the physical space-time continuum. Thus mathematics is not based on human imagination alone. Mankind in contact with nature generates the art of mathematics.

The main achievements of logic and foundations in the 20th century are:

(A) A precise language for mathematics has been constructed, so that we know what mathematical sentences are and what is a proof of a sentence based on a set of axioms and definitions. Gödel's completeness theorem for first-order logic shows that this concept of proof matches the set-theoretic semantics developed later by Tarski. When proving theorems, mathematicians have always appealed to logical intuition. In the 20th century this intuition has been fully and precisely described; see Table IV.

(B) An axiomatic set theory ZFC, whose primitive notions are those of logic plus the membership relation, has been constructed. Modern mathematics is based on this theory. Its axioms are so simple that they can be presented on a single page; see Table I. On the other hand, as shown by Gödel in 1931, and later by Cohen and others, many questions in finite combinatorics, in the arithmetic of natural numbers, in analysis, and in set theory cannot be decided in ZFC. The work of extending ZFC by new axioms with interesting consequences continues.

(C) A theory of computable functions and algorithms has been constructed. We have a clear distinction between the general classes of functions and their subclasses of computable functions, defined by means of Turing machines. More concrete classes concerned with the time and space complexity of computation, such as PTIME, NPTIME, and PSPACE, are also being investigated.

Thus the fundamental questions posed in the 19th century have been answered. Those answers are surprising and beautiful. One can ask whether mathematics and computer science in the 21st century will be founded on the same concepts as in the 20th century. We conjecture that set theory will remain the most useful and inspiring universal theory on which all of mathematics can be based.

Finally, let us formulate three open problems in logic and foundations that seem to us of special importance.

1. *To develop an effective automatic method for constructing proofs of mathematical conjectures, when these conjectures have simple proofs!* Interesting methods of this kind already exist but, thus far, automated theorem proving procedures are not dynamic: they do not use large lists of axioms, definitions, theorems, and lemmas that mathematicians could provide to the computer. Also, the existing methods are not yet powerful enough to construct most proofs regarded as simple by mathematicians, and conversely, the proofs constructed by these methods do not seem simple.
2. *Are there natural large cardinal existence axioms LC such that* ZFC + LC *implies that all OD sets X of infinite sequences of* 0*s and* 1*s satisfy the axiom of determinacy $AD(X)$?* This question is similar to the continuum hypothesis, in the sense that it is independent of ZFC plus all large cardinal axioms proposed thus far.
3. *Is it true that* PTIME $\neq$ NPTIME, or at least, that PTIME $\neq$ PSPACE*?* An affirmative answer to the first of these questions would tell us that the problem of constructing proofs of mathematical conjectures in given axiomatic theories (and many other combinatorial problems) cannot be fully mechanized in a certain sense.

   In May 2000 the Clay Mathematics Institute announced a prize of one million dollars for a proof or disproof of the conjecture PTIME $\neq$ NPTIME. See `http://www.claymath.org/prize_problems/index.htm` for details.

Acknowledgements This paper grew out of a shorter version published in the popular Polish magazine *Delta* in the issues 9 and 11 of 1999, and 1 and 3 of 2000. We are indebted to Abe Shenitzer, who translated the *Delta* version into English.

Suggested further reading

1. General Information

- J. Barwise, ed., *Handbook of Mathematical Logic*, North Holland, Amsterdam and New York, 1977.
  A comprehensive presentation of all three areas of logic and foundations at the beginning of the fourth quarter of the 20th century.
- Y.L. Ershov, S.S. Goncharov, A. Nerode, and J.B. Remmel, eds., *Handbook of Recursive Mathematics*, Elsevier, Amsterdam and New York, 1998, Vol. I and II.
  An extensive and comprehensive presentation of effective mathematics.
- D. Gabbay and F. Guenther, eds., *Handbook of Philosophical Logic*, Reidel, Dordrecht and Boston, 1985, vols. I–IV.
  A very extensive presentation of aspects of logic and foundations as studied by philosophers (often inconsistent with the views expressed in our paper).

- J. van Heijenoort, ed., *From Frege to Gödel, A Source Book in Mathematical Logic, 1879-1931*, Harvard University Press, Cambridge, MA and London, 1967.
  Translations and commentary on most of the important papers in logic up to 1931.
- J. van Leeuven, ed., *Handbook of Theoretical Computer Science*, Elsevier, Amsterdam and New York, and MIT Press, Cambridge, MA, 1990, vols. I and II.
  A very extensive presentation of syntactic and semantic issues of modern theoretical computer science.

2. Set Theory
   - P.J. Cohen, *Set Theory*, W.A. Benjamin, New York and Amsterdam, 1966.
     An excellent introduction to axiomatic set theory and independence proofs.
   - A.A. Fraenkel, Y. Bar-Hillel, and A. Levy, *Foundations of Set Theory*, North Holland, Amsterdam, 1976.
     An interesting treatment of the history of axiomatic set theory.
   - T. Jech, *Set Theory*, Academic Press, New York, 1977.
     A comprehensive course on classical set theory.
   - K. Kunen, *Set Theory, An introduction to independence proofs*, North Holland, Amsterdam and New York, 1980.
     A very useful course on set theory and on Cohen's method of forcing.
   - K. Kuratowski and A. Mostowski, *Set Theory: with an introduction to descriptive set theory*, 3rd ed., North Holland, Amsterdam and New York, 1976.
     An advanced course on axiomatic set theory.
3. Model Theory
   - C.C. Chang and H.J. Keisler, *Model Theory*, North Holland, Amsterdam and New York, 1990.
     A very beautiful exposition of model theory.
   - W. Hodges, *Model Theory*, Cambridge University Press, Cambridge and New York, 1993.
     A comprehensive monograph on model theory with a large bibliography.
4. Computability Theory
   - P. Odifreddi, *Classical Recursion Theory*, vols. I and II, North Holland, Amsterdam and New York, 1989-1999.
     An extensive presentation of classical recursion theory.
   - H. Rogers, Jr., *Theory of Recursive Functions and Effective Computability*, MIT Press, Cambridge, MA, 1987.
     A very beautiful presentation of computable function theory up to 1967.
   - R.I. Soare, *Recursively Enumerable Sets and Degrees: a Study of Computable Functions and of Computably Generated Sets*, Springer-Verlag, Berlin and New York, 1987.
     A comprehensive study of degrees of computability.

Department of Computer Science, University of Kentucky, Lexington, Kentucky
marek@cs.uky.edu

University of Colorado, Boulder, Colorado
jmyciel@euclid.colorado.edu