ON THE FOUNDATIONS OF COMPUTING

Giuseppe Primiero

OXFORD

On the Foundations of Computing

GIUSEPPE PRIMIERO

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

First Edition published in 2020

Impression: 1

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2019947624

ISBN 978–0–19–883564–6 (hbk.)
ISBN 978–0–19–883565–3 (pbk.)

DOI: 10.1093/oso/9780198835646.001.0001

Printed and bound by
CPI Group (UK) Ltd, Croydon, CR0 4YY

Contents

1 Introduction

How Algorithms Control the World. (*The Guardian,* 1 July 2013).
Rise of the Machines. (*The Economist,* 4 April 2018).
Are We Living in a Computer Simulation? (*Scientific American,* 7 April 2016).

These are real headlines appearing on major journalistic outlets during the last few years. They indicate a recurrent and strengthening feeling in the relation between humanity and computing technologies: fear. In the first case, it is fear of opaque structures, faster than we can ever be, and decisive in all aspects of modern life. In the second case, it is fear of complex artefacts, whose reliability is crucial in several daily events in which our lives can be put at stake by not so uncommon errors. In the third case, it is the atavistic fear of our origin and destiny, rephrased and redesigned around the myth of a computational mastermind.

As often with fears that pervade human culture and science in particular, their origins lie in lack of knowledge. The wealth of popular science publications that investigate the effects of computing technologies on work, health, economy, and social life tend to assume one of two tendencies: on the one hand, the enthusiasts who share their visionary future where algorithms and machines will be our companions, friends, and saviours, lifting the burden of hard work and elevating us from the last remnants of our mortal lives; on the other hand, the detractors who paint a bleak vision of malevolent AIs fighting humanity for their right to survive.

Science and its philosophical analysis have in this context a double role: to reduce ignorance on which extremist views grow, and to build the basis for a more realistic, mature, solid, and argumentative position on our current and future relation with machines and computing technologies.

This aim requires a difficult but essential combination of factors. First, computing technologies need to be explained, to all sorts of specialists as well to the general public, to reduce the current algorithmic fever. This means to illustrate the basis of the mathematical and engineering tools that have for decades built up towards the creation of computing machines, and to explain the laws that regulate their progress. Second, everyone,

On the Foundations of Computing. Giuseppe Primiero, Oxford University Press (2020). © Giuseppe Primiero.
DOI: 10.1093/oso/9780198835646.001.0001

and scientists in particular, need to ask the difficult questions concerning technology: how do we define algorithms, and which properties do we ascribe to them? how is a computational error recognized and its negative effects constrained?; what does it mean to know computationally? These questions may appear trivial or too generic at first, but their answers constitute the backbone for any strategy, politics, or ethics involving computing technologies. In turn, this can determine our way of living with them. For this task, the sole scientific approach becomes insufficient. And a pure philosophical analysis risks being too pretentious, presupposing (or worse: ignoring) the technical basics. A combination of solid scientific grounding and consistent philosophical research can lead to an understanding of how computing is affecting our epistemological and ontological worldviews.

Our first task is therefore to locate the origin of the current frenzy in its appropriate historical and formal context: the problem of deciding mechanically which sentences of a mathematical system are true. This problem was sought to be resolved through the definition of computable functions and in turn by modelling this latter idea in the form of a universal machine capable of realizing all such functions. The notion of algorithm and its execution is thus recognized in the mechanical execution of a well-defined function, a concept which matches the notion of program. The connection between programs and proofs (as the standard formal way of determining the truth of propositions in mathematics) is thus at the very heart of the notion of computation. It is nonetheless a lot more complex to establish which properties can be ascribed and should be defining algorithms. It is striking to witness the superficiality and confusion shown by those who do not deal with computing professionally. But it is also amazing to realize that a profound and intense debate concerning the nature of algorithms and their implementations is still ongoing among computing professionals. This points to the difficulty of analysing objects whose nature is at the same time both formal and concrete, abstract and linguistic. Along with their definition, the formal analysis of their correctness becomes essential, a guarantee *in principle* that their intended behaviour is satisfied.

The second task is to highlight the parallel development of machines capable of realizing those same functions identified as computable, a step from the abstract realm of mathematics to the concrete one of engineering. It is in this context that the limitations to (formal) correctness as well as the new laws guiding the evolution of computing machinery emerge, to define a new concept of validity. While the practice of automated testing and formal verification constitute today an essential aspect of controlling computing machinery especially in safety-critical systems, large web-based, robotic, and AI applications, there is still an extensive conceptual void to be filled. It concerns our ability to define, categorize, and explain the limits of functionality, usability, and efficiency for *implemented* programs, i.e. in the passage from formal to physical correctness. Specification (as the expression of intention) and implementation are required to reflect the complex, stratified nature of computing machinery.

A third task consists in clarifying in which way computing machinery can help forming our scientific view of the world, and under which conditions results obtained through computational means can be granted scientific validity. This is an essential step for two reasons: first, more and more of our science is the result of using computing technologies extensively; second, from the previous analysis we should be aware of the limits induced by mechanical processes which are in principle grounded on a formal notion of validity, but whose realization is based on implemented processes with physical and contextual properties. In this sense, the mentioned problem of recognizing our reality as the possible result of a computation is more constructively and realistically rephrased as the task of identifying the characteristics that make a simulation a valid way of knowing any external reality. In this third task, the power and the limits of computational methods need to be fully formulated and qualified to obtain a transparent understanding of computing and its properties.

These three tasks reflect a way to concretely understand computing and its realizations. In doing so, the myths pervading our information society can be dispelled. More interestingly, we can contribute to the important and essential job of building the philosophical analysis required by computation and associated methods, a feature so intrinsic to our culture today that it is hard to imagine a more urgent task for philosophy. A solid and critical understanding of the foundations of computing is a new and essential building block in the relation between society and technology, a task that philosophy and science need to share and act upon urgently.

The present volume is our contribution towards a more balanced scientific understanding of the new information society.

Part I

The Mathematical Foundation

2 A Fundamental Crisis

Summary

This chapter reconstructs the historical background of the mathematical foundation of modern computing. At the beginning of the twentieth century, mathematical correctness and truth were under scrutiny and three main theoretical positions emerged in trying to offer an appropriate methodological answer to their definitions. The resulting debate was the basis for explaining what it means to compute.

2.1 The Foundations of Mathematics Debated

While computing technologies are young by comparison with other efforts of human ingenuity, their origins go back to many early chapters in the human quest for the understanding and realization of mechanical aids to knowledge. An exhaustive history would need to reconstruct the influences of the philosophical views on the mechanization of deductive knowledge in the *Ars Magna* by Ramon Llull from the thirteenth century; in the *Characteristica Universalis* and *Calculus Ratiocinator* by Leibniz in the eighteenth century; and the (only partly realized) engineering efforts for the *Analytical Engine* by Babbage in the nineteenth century.[1] But while philosophy and engineering have been crucial disciplines in the birth and evolution of computing, largely acknowledged in the following part of this book, our recollection of the foundations of computing starts from their roots in mathematics.

[1] See for example Davis (2012); O'Regan (2012); Tedre (2015) for short recounts of these contributions to computing. For references to the work of Llull, see http://orbita.bib.ub.es/llull/ and Llull (1985). For Leibniz' contribution to the idea of a universal language, see e.g. his *On the General Characteristic* (ca. 1679) in (Leibniz, 1989, pp.221–8). For the works of Babbage, see Babbage (2010).

On the Foundations of Computing. Giuseppe Primiero, Oxford University Press (2020). © Giuseppe Primiero.
DOI: 10.1093/oso/9780198835646.001.0001

Between the end of the nineteenth and the beginning of the twentieth century, a foundational crisis was taking place across the most important mathematical circles in the world. This crisis can be considered (factually and metaphorically) as the root of computing in mathematics. From the ruins left by the titanic clash of different views on mathematical truth, infinity and correctness, the *theory of computation* was born. This term refers today to the field of logical and mathematical research that investigates the concept of *effective computation*, or less abstractly, of *effectively computable mathematical structures*. This discipline, which expresses the essential formal aspect of computing, should be considered in its coexistence with the theory of algorithms, whose origins actually pre-date the theory of computation. Algorithms will be analysed later in their philosophical, mathematical, and programming interpretations. This interplay of ideas, notions and scientific research programmes is a constant in our conceptual reconstruction of computing as a discipline, and should be always recalled by the reader.

In the following part of this chapter, we will offer a reconstruction of the debate on the foundations of mathematics that was at the origin of the notion of computable function and, in turn, of the very idea of computing as a mathematical discipline.

2.2 Logical Roots

Computability theory as the mathematical roots of computing has its own origins in logic. In its most basic formulation, logic studies how to perform correct reasoning. The correctness of this abstract act of knowledge is formally made concrete in the form of two relations between sets of sentences: on the one hand, by the definition of valid *consequence*; on the other, by that of correct *derivation*. These two notions express the current view on, respectively, the semantic and syntactic interpretations of logical reasoning.

The notion of consequence is based on the interpretation of propositions as truth-bearers, expressing (the obtaining of) corresponding states of affairs. This tradition has been codified in the work of Tarski,[2] which in turn goes back to Quine, Frege, and Bolzano. Truth as correspondence relies on the notions of *interpretation* and of *model*, in which truth is realized. While the basic intuition of truth for the propositional translation of sentences only requires an assignment of truth values (true/false) to atoms and their closure under logical connectives, for the aim of developing formal systems in various branches of mathematics the use of predicative calculi was essential, and so the definition of an interpretation for predicative formulae:

Definition 1 (Interpretation) *An interpretation of a formula ϕ is an assignment of meanings to any individual variable x of ϕ or predicative variable $P(x)$ of ϕ for objects and predicates (or relations for predicates ranging over more than one variable) in the language of a system F.*

[2] Tarski (1943).

As for the propositional case, predicative formulae interpretation is completed by the definition of compositional rules for logical connectives and the standard extension to the universal and existential quantifiers. The notion of truth by interpretation is used to define the concept of model:

Definition 2 (Model) *A model $\mathcal{M}$ of a sentence ϕ (or a set of sentences Γ) is an interpretation in which ϕ (or every ϕ member of Γ) is true.*

The semantic notion of consequence uses preservation of truth in a model:

Definition 3 (Semantic Consequence Relation) *Given a set of sentences $\Gamma = \{\phi_1, \ldots, \phi_n\}$ within some formal system F, we say that a formula ψ is a semantic consequence of Γ in F, denoted as $\Gamma \vDash_F \psi$ if and only if there is no model $\mathcal{M}$ of F such that all members of Γ are true in $\mathcal{M}$, but ψ is false in $\mathcal{M}$.*

A different understanding of the notion of correct logical reasoning comes from the syntactic reading of the relation between sentences. Under this reading, the truth of a formula ψ is reduced to its correct derivation by means of a proof procedure as a relation between sentences, the premises, and the conclusion, i.e. the formula ψ at hand. The notion of *proof procedure* (or derivation) therefore grounds the syntactic understanding of correct reasoning:

Definition 4 (Proof Procedure) *A proof procedure $\mathcal{P}$ of a sentence ψ from a set of sentences $\Gamma = \{\phi_1, \ldots, \phi_n\}$ is a finite set of steps in which every formula is either some ϕ_i member of Γ, or is obtained by a previous step by applying a well-defined and explicit rule r of a formal system F, and the last step in $\mathcal{P}$ is the formula ψ.*

With this notion we can define the syntactic notion of derivability:

Definition 5 (Syntactic Derivability Relation) *Given a set of sentences $\Gamma = \{\phi_1, \ldots, \phi_n\}$ within some formal system F, we say that a formula ψ is syntactically derived by Γ in F, denoted as $\Gamma \vdash_F \phi$ if and only if there is a proof procedure $\mathcal{P}$ in F of ψ from Γ.*

When the set Γ of sentences of interest represents some scientific theory (like axioms and laws of geometry, physics, or arithmetic), semantic consequence and syntactic derivability relations tell us what are the truths, respectively theorems, of that theory. Towards the end of the nineteenth century, and during the first decades of the twentieth, mathematicians were interested in knowing how much could be proved by their theories, i.e. whether they were strong enough to validate all the truths of their respective fields. More clearly stated, the main research problem for mathematicians at that time can be formulated as follows:

Problem 1 (Soundness and Completeness) *Can we build logical systems that allow us to discover all (completeness) and only (soundness) the true sentences derivable from the axioms of a given theory?*

It was the main aim of mathematicians to ensure that their designed logical systems would guarantee sound and complete theories. This was true in particular of arithmetic.

The uncertainty surrounding this crucial issue, and the related methodological problems, became known as the *Grundlangenkrisis*, or the crisis of the foundations of mathematics.

One historical event can be chosen as representative of this situation. The *Second Conference on Epistemology of the Exact Sciences* took place between 5 and 7 September 1930 in Königsberg: it can be considered a turning point in the history of the philosophy of mathematics and logic. Three lectures were delivered during that conference, conveying the basic research programmes in the foundations of mathematics:[3]

1. Rudolf Carnap, *Die logizistische Grundlegung der Mathematik*;
2. John von Neumann, *Die formalistische Grundlegung der Mathematik*;
3. Arend Heyting, *Die intuizionistiche Grundlegung der Mathematik.*

Each of these lectures illustrated one main position in the debate on the foundations of mathematics: the logicist position by Gottlob Frege with his *Grundgesetze der Arithmetik*; the formalist one by David Hilbert with *Grundlagen der Geometrie*; and the intuionist approach by J.E. Brouwer with *Over de grondslagen der wiskunde.*[4]

2.3 Logicism

Frege's work had been inspired by the idea of grounding mathematics (and arithmetic as a part of it) entirely on logic:

> The most solid way of derivation is clearly that of pure logic which, being abstracted from the particular properties of things is based only on laws, from which all of knowledge comes from.[5]

This programme relied on two main theses:

Thesis 1 (Logical definability) *The concepts of mathematics can be derived from logical concepts through explicit definitions.*

Thesis 2 (Logical derivability) *The theorems of mathematics can be derived from logical axioms through purely logical deduction.*

As a simple example, consider the notion of number, which according to Frege can be explained as the extension of a set: the number 0 is the extension of all concepts that are expressed by empty sets; if you have to explain what 0 means, you can point to all the sets that have zero elements and say that 0 denotes all such sets; the number 1 is the extension of all concepts that are expressed by sets that have just one element;

[3] See respectively Carnap (1931), von Neumann (1983), and Heyting (1983). For an overview of the conference, see Reichenbach and Cohen (1978).

[4] See respectively Frege (1903), Hilbert (1902) and, Brouwer (1907).

[5] (Frege, 1967, ch.1).

and similarly for all other numbers. According to this intuition, the function that selects all the sets of a given cardinality can then be used to determine the extension of the corresponding natural number, i.e. which sets fall under it. Starting from this definition of natural number as extension of concepts with the same cardinality, Frege aims at showing that all arithmetical expressions can be logically derived from other more simple notions. For its universal reliance on logic, Frege's programme became known as *Logicism*.

Notoriously, Frege's programme was crushed by the discovery that one could derive a *paradox* from one of the system's laws in his *Grundgesetze der Arithmetik*. The law in question is formulated as follows:

Definition 6 (Basic Law V) *Given a function $f(x)$, let its extension be $\{x \mid f(x)\}$, and given a function $g(x)$ let its extension be $\{x \mid g(x)\}$; then it holds $f = g$ iff $\forall x(f(x) \leftrightarrow g(x))$.*

If one takes the set of elements x that satisfy the function f, and this set has the same cardinality of the set of elements x that satisfy another function g, then the functions f and g must be extensionally equal, i.e. express concepts identifying the same natural numbers. If one allows f and g to be themselves objects of selection according to cardinality, a paradox famously illustrated by Bertrand Russell in a letter he wrote to Frege in 1902 follows:

> You state that a function, too, can act as the indeterminate element [i.e. it can apply to another function]. This I formerly believed, but now this view seems doubtful to me because of the following contradiction. Let *w* be the predicate: to be a predicate that cannot be predicated of itself. Can *w* be predicated of itself? from each answer its opposite follows. Therefore we must conclude that *w* is not a predicate. Likewise there is no class (as a totality) of those classes which, each taken as a totality, do not belong to themselves. From this I conclude that under certain circumstances a definable collection does not form a totality.[6]

The paradox introduced by Russell is equivalent to the following more informal version:

Proposition 1 (The Barber Paradox) *Suppose there is a town with just one barber, who is male. The barber is a man in town who shaves all those, and only those, men in town who do not shave themselves. In this town, every man keeps himself clean-shaven, and he does so by doing exactly one of two things: shaving himself; or being shaved by the barber. From this, one can ask who shaves the barber. This results in a paradox: the barber can either shave himself, or go to the barber; however, neither of these possibilities are valid. If he shaves himself, then he contradicts his own definition; and if he goes to the barber, then he shaves himself again.*

To see how a paradox follows from the theory of extensions of sets, let us reconsider Russell's argument. Define R as the set of all sets that do not contain themselves. This is the equivalent of the barber's definition as the man who shaves all who do not shave

[6] Russell (1965).

themselves. Then one might ask the question whether R is contained in the set R. This corresponds to asking whether the barber shaves himself, or goes to the barber. If the equivalence holds, then by substitution R is a member of R *ad infinitum*, and the set R uses itself to be defined, a *vicious circle*. If R is not equivalent to R, then for every element X of R, it must hold X is not equivalent to R. In this way, Russell showed that an unrestricted definition of set would lead to contradictions.

This paradox represented the greatest problem for the Fregean ideal of a logic able to provide all principles and rules on which to define all mathematical concepts. This idea of logic referred to the formulation of *one* theory and *one* model of interpretation, such that it would provide a unified axiomatization for arithmetic and all the other sciences. Moreover, the problem was not confined to Frege's system, as similar paradoxes were arising in all branches of mathematics. For a different example, let us consider the paradox by Burali-Forti in naive set theory.[7] It is possible to order the elements of infinite sets by using ordinals numbers:

Definition 7 (Ordinals) *The first ordinal is $\varnothing$ or 0. The successor of some ordinal α is defined as $\alpha \cup \{\alpha\}$, or $\alpha + 1$. The union of all members of a set of ordinals is also an ordinal.*

Suppose that α and β are two ordinals, then $\alpha \leq \beta$ if and only if α is a member of β or α is equal to β and it can be proved that there exists a total order relation $\leq$ on the set of ordinals.[8] Let O be the set of all ordinals. It follows from the definition that

$$
\begin{gathered}
\varnothing = 0 \text{ is a member of } \mathsf{O}\\
\varnothing \cup \{\varnothing\} = \{\varnothing\} = 1 \text{ is a member of } \mathsf{O}\\
\{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = 2 \text{ is a member of } \mathsf{O}\\
\{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = 3 \text{ is a member of } \mathsf{O}\\
\vdots\\
\{1,2,3,4,\ldots\} = \omega \text{ is a member of } \mathsf{O}\\
\omega \cup \{\omega\} = \{\omega, 0, 1, 2, \ldots\} = \omega + 1 \text{ is a member of } \mathsf{O}\\
\omega + 2 \text{ is a member of } \mathsf{O}
\end{gathered}
$$

Definition 8 *The set of all countable ordinals is*

$$\omega_1 = \omega \cup \{\omega, \omega+1, \omega+2, \ldots\} \textit{ is a member of } \mathsf{O}$$

Definition 9 *The set of all ordinals that have the maximal cardinality of the real numbers (or the set of all countable and $\aleph_1$-ordinals) is ω_2, a member of O.*

Consider now the following definition

[7] Burali-Forti (1897).

[8] Recall that an order relation $\leq$ is total over a set X if and only if $\leq$ is reflexive, transitive, antisymmetric and for all α, β members of X, it holds $\alpha \leq \beta$ or $\beta \leq \alpha$.

Definition 10 (Totally Well-Ordered Set) *A totally ordered set is well ordered if and only if every non-empty subset has a least element.*

Every well ordered set is associated with a so-called order type. Two well ordered sets A and B are said to have the same order type if and only if they are order-isomorphic. Every order type is identical to exactly one ordinal.

Definition 11 (Cardinal Number) *The cardinal number of a set A is the smallest ordinal α such that α and A are equinumerous.*

The paradox affecting the theory of ordinal numbers is formulated as follows:

Definition 12 (Burali-Forti Paradox) *In the theory of transfinite ordinal numbers every well-ordered set has a unique ordinal number; every segment of ordinals (i.e. any set of ordinals arranged in natural order which contains all the predecessors of each of its elements) has an ordinal number which is greater than any ordinal in the segment. Assuming by contradiction that the class Ω of all ordinals could be linearly ordered, Ω carries all properties of an ordinal number, namely it would be itself well-ordered and it would possess an ordinal ω member of Ω. Thus Ω would be order-isomorphic to a proper initial segment of itself, the one determined by ω. Then, we can construct its successor $\omega + 1$, which is strictly greater than Ω. However, this ordinal number must be an element of Ω since Ω contains all ordinal numbers, and we arrive at $\Omega < \Omega + 1 \leq \Omega$.*

The definition of set in Frege's paradox and the definition of the class of ordinals in Burali-Forti's paradox both rely on the notion of totality of a collection. Poincaré was the first to recognize the Vicious Circle Principle as the basis of what is known as an *impredicative definition*, i.e. a definition in which a member of a set is defined in a way that presupposes the entire set to be defined already.[9] According to the French epistemologist, to avoid being defined circularly, a mathematical entity was to be defined inductively only on the basis of constructions from starting given objects. Also Russell aimed at restricting the formulation of such totalities, through the analysis of the Vicious Circle Principle:

> If, provided a certain collection had a total, it would have members only definable in terms of that total, then the said collection has no total.[10]

The Russellian solution to the paradox in Frege's system is notoriously formulated within the Theory of Types. The definitional procedure which avoids the vicious circle requires to stratify the objects of predication within the theory so that a predicate can never be applied at the same level of an object for which it is defined. The ramified version of the Theory of Types went beyond this restriction:[11] it allowed non-strictly predicative definitions through the formulation of an axiom to reduce any propositional function to a predicative one.

[9] Poincaré (1909).

[10] (Russell, 1903, Appendix B), (Whitehead and Russell, 1962, vol.1, Introduction, ch. 2, p.1).

[11] Russell (1956).

Definition 13 (Axiom of Reducibility) *Given any function ϕ, there is exactly one predicative function μ equivalent to ϕ for any value of the variable x:*

$$\vdash \exists\mu\forall x(\phi x \leftrightarrow \mu!x).$$

The Axiom of Reducibility expresses the principle according to which every definable function ϕ is correctly applied to an object x if and only if it has exactly one predicative formulation μ for each object x to which it applies. The existential claim presupposed by the formulation of μ was the main point of critique in the epistemological value of this axiom. Two further axioms in use in the *Principia* raised doubts because of their existential nature. The Axiom of Choice was formulated as follows:

Definition 14 (Axiom of Choice) *Let C be a collection of non-empty sets. Then there exists a function f defined on C with the property that, for each set S member of C, $f(S)$ is a member of S.*

By the Axiom of Choice, for every well-defined collection of non-empty sets there is one function selecting an element from each set in the collection. This is equivalent to saying that the Cartesian product of a collection of non-empty sets is always non-empty.

The second relevant axiom is formulated as follows:

Definition 15 (Axiom of Infinity) *There is a set I (the infinite set) such that $\varnothing$ is a member of I and such that for every x member of I it holds that $(x \cup \{x\})$, i.e. the union of x with the singleton set containing x is a member of I.*

Consider a standard definition of natural numbers in terms of sets, for example the recursive definition of natural numbers used in Zermelo-Fraenkel set theory:[12]

$$\begin{aligned} 0 &= \varnothing \\ 1 &= 0' = \{0\} \\ 2 &= 1' = \{0,1\} \\ 3 &= 2' = \{0,1,2\} \\ &\vdots \end{aligned}$$

Then the Axiom of Infinity asserts the existence of all natural numbers and by the Axiom of Choice we can construct the set of all its members step by step (as well as the set of all its subsets). The problematic nature of these assumptions, in particular the assertion of the existence of some property, and their use involving the *mathematical infinite*, represented an obstacle to the methodological reliability of the logicist programme.

The method of explicit definitions, i.e. the rejection of the impredicative ones, was meant to overcome the existential assumption by producing *constructions* corresponding

[12] We investigate recursive definitions more closely in Chapter 4.

to name-giving procedures for objects whose existence is already established. This illustrates the reduction of the existential claim to a definitional procedure. Hence, the Axiom of Reducibility represents the greatest difficulty, because it *presupposes* the possibility of definining a predicative function of interest. Carnap in his lecture in Königsberg attempted a consistent way to remove this axiom, using Ramsey's theory from *The Foundations of Mathematics*.[13] In order to remove the Axiom of Reducibility, Ramsey was in turn constrained to the assumption of existence of all properties, before they can be identified by definition. This means, again, to allow impredicative definitions. In rejecting this idea, Carnap maintains that this step means essentially to believe in a Platonic realm of ideas, whereas one should keep the Fregean requirement of accepting only what has been proven *in finitely many steps*. Carnap aimed at explaining how it is possible to give inductive general definitions without retaining conceptual absolutism, i.e. the idea of concepts existing before they can be constructed. In line with the general logicist approach, Carnap writes:

> [t]he verification of a universal logical or mathematical sentence does not consist in running through a series of individual cases, for impredicative definitions usually refer to infinite totalities. The belief that we must run through all the individual cases rests on a confusion of 'numerical' generality, which refers to objects already given, with 'specific' generality. We do not establish specific generality by running through individual cases but by logically deriving certain properties from certain others.[14]

In the formalist programme, the rejection of case-by-case analyses required reducing the complete verification of a statement about an arbitrary property to its *logical validity*, i.e. it being inferred by logical principles alone. The validity of a property defined impredicatively might be difficult or impossible only in individual cases, depending on the specific system in which one is working. Accordingly, formal theories require that definitions must be intended as *constructive* procedures and that those including totalities are valid as long as these can be guaranteed not to involve vicious circles or other paradoxical properties. Moreover, inside a system of deduction there is no primitive reference to the meaning of symbols (for this aspect, the programme has also passed in the literature with the name 'formalist').

2.4 Finitism

A second methodological approach to the problem of truth and correctness was proposed by the *finitist programme*: this was characterized by a stronger requirement on the notion of valid procedure in mathematics, requiring that everything involved in a mathematical definition needs to be reduced to *finite* properties, and everything should be proven by

[13] Ramsey (1926).

[14] (Carnap, 1931, p.51).

pure, *in principle mechanizable,* symbol manipulation techniques. This programme was started by David Hilbert on the assumption that the notion of infinity undermines the validity of deduction procedures and inferential methods.

According to Hilbert, to overcome the problems posed by paradoxes it was essential to guarantee an axiomatic formalization of theories in which only a completely clarified notion of infinity would be admitted. Under this stipulation, infinite objects and potentially infinite procedures were to be allowed only if reduced (or reducible in principle) to finite counterparts.[15] In particular, Hilbert refers to the use of infinite numerical series to define real numbers and the concept of real number itself, thought of as a completed totality. The introduction of the so-called method of *ideal elements* is Hilbert's way of clarifying the notion of infinity in cases like infinitely long lines and points at infinity from geometry; complex-imaginary magnitudes and ideal numbers from algebra; the entire analysis and Cantor's set theory:

> in analysis we deal with the infinitely large and the infinitely small only as limiting concepts, as something becoming, happening, i.e. with the potential infinite. But this is not the true infinite. We meet the true infinite when we regard the totality of numbers $1, 2, 3, 4, \dots$ itself as completed unity, or when we regard the points of an interval as a totality of things which exists all at once. This kind of infinity is known as actual infinity.[16]

Errors arise in the misapplication of the infinite: in particular, material logical deduction produces errors in the form of arbitrary abstract definitions involving infinitely many objects. For the relation of logical deduction to be valid, properties of the extra-logical objects to which logical signs are applied need to be clearly established. For the rest, logic (and mathematics with it) is a pure, completely determined game of signs, with finitary and directly constructive procedures:

> [a]lthough the content of a classical mathematical sentence cannot always (i.e. generally) be finitely verified, the formal way in which we arrive at the sentence can be. Consequently, if we wish to prove the validity of classical mathematics, which is possible in principle only by reducing it to the a priori valid finitistic system [...], then we should investigate, not statements, but methods of proof.[17]

As an effect of this paradigmatic shift from the logicist inspired unique system of thought to the finitist system of manipulable symbols, logic becomes a way of axiomatizing independent theories, with valid inferential structures built on finitistic, arithmetic-combinatorial bases. To this aim, the Hilbertian method can be reduced to the following basic steps:

- the formulation of a logical vocabulary;
- the unambiguous characterization of a combination of symbols (meaningful formulas);

[15] Hilbert (1983).

[16] (Hilbert, 1983, p.188).

[17] (von Neumann, 1983, p.62).

- the description of a construction procedure called 'proving' allowing to formulate all the valid formulas;
- the acceptance of mathematical statements only on the basis finitary proving methods.

Given this formulation of a logical method for the sciences, Hilbert illustrated his programme at the Congress of Mathematics held in 1928 in Bologna, Italy, with the aim of proving the following results:

Thesis 3 (Completeness) *All true mathematical statements can be proven.*

Thesis 4 (Consistency) *Only true mathematical statements can be proven.*

Thesis 5 (Decidability) *A decision procedure exists to decide the truth or falsity of any given mathematical proposition.*

The birth of logic as meta-theoretical analysis of scientific theories, i.e. the ability to prove completeness and consistency, is based on the last requirement. The effective check provided by decidability, together with consistency, will ensure that no formula derivable in the system can ever be an equation of the form $1 = 0$. Such a proof must of course be characterized by those finitary terms that the method requires:

> The real problem is then that of finding a finitary combinatorial proof of consistency.[18]

It is on the identification of the essential conditions for such a procedure that intuitionism will proceed.

2.5 Intuitionism

The third approach to determine truth and correctness in mathematics would focus in particular on the need to redefine the former notion on a procedural basis, with the aim of maintaining control of the definitional process. Brouwer's philosophy is at the basis of this idea of truth defined by assertion conditions on contents. A formal semantic translation was offered by Heyting's interpretation of intuitionistic logic from around 1930. Kolmogorov further interpreted it in terms of problems and their solutions. The so-called Brouwer-Heyting-Kolmogorov semantics defines the truth of a proposition as the existence of a proof-object for it.[19] According to the intuitionistic perspective, to reduce a definition to a well-defined and complete procedure might not be sufficient if its result does not reduce to determining the conditions under which contents can be known.

[18] (von Neumann, 1983, p.64).

[19] See Brouwer (1925a,b) for the theoretical foundation of intuitionism, Heyting (1930) for its formal translation, and Kolmogorov (1932) for the problem-task interpretation. Details on the BHK formal semantics of proofs are provided in Chapter 7, but for now we are only interested in presenting the guiding principles of intuitionism to the problem of determining true sentences in mathematics.

To illustrate this point, Heyting in his lecture considers the definition of a real number in terms of assigning to every rational number either the predicate LEFT or RIGHT, in order to preserve the natural order of rationals. Its reduction to the procedure enclosing the Euler's constant C within an arbitrarily small rational interval can be obtained by computing an always smaller series of rational intervals. The procedure is still insufficient to decide for an arbitrary rational number A whether it lies left or right of C or is perhaps equal to C.[20] The reason for this uncertainty is the generalized application of the Aristotelian law of excluded middle, i.e. that any proposition either it is true or it is false, formally $A \vee \neg A$. In its application for the calculation of C, the rejection of this law means it is impossible to affirm that either a number n of computation steps proves that $A < C$ or $A > C$, or that such n does not exist until that is actually shown to be the case, and hence the contradictory case can be excluded. The clue to reject the famous Aristotelian principle is given again in terms of the notion of infinity:

> We can drop the requirement that the series of predicates be determined to infinity by a rule. It suffices if the series is determined step by step in some way, e.g. by free choices. I call such sequences 'infinitely proceeding'.[21]

This description of infinite objects such as choice sequences, i.e. in terms of step-by-step procedures, has an effect on their definition. An infinite object cannot be regarded as the collection of its members, which is a meaningless statement if such object is not considered as existing in itself. Instead, an object is defined by the construction on the basis of previously defined elements, down to elementary ones:

> Impredicative definitions are made impossible by the fact, which intuitionists consider self-evident, that only previously defined objects may occur as members of a species [set].[22]

To admit no infinitely proceeding sequence in mathematics means, in other words, to admit only rule-determined sequences, to which a number belongs if and only if there is a rule which allows one to actually determine all predicates of the sequence successively. When applied to some specific case like 'whether or not the sequence 0123456789 occurs in the decimal expansion of π'[23] this requirement corresponds to the formulation of a binary YES/NO problem and the task of finding a solution (proof) to it. A problem is formulated by an intention (expectation) to find its fulfilment (solution): the solution is obtained if a construction is provided, or else it must be proved that the intention leads to a contradiction. This amounts to a reduction of solvability to provability. Truth, as the property of propositions providing solutions to problems, is thus in turn reduced to proofs:

[20] (Heyting, 1983, p.54).
[21] (Heyting, 1983, p.55).
[22] (Heyting, 1983, p.57).
[23] (Heyting, 1983, p.58).

Definition 16 (Truth as Proof) *Proposition A is true if and only if there exists a proof a of A.*

The constructive interpretation of the infinite by means of so-called *lawlike sequences* reflects this concept of the truth of a property being reduced to a construction answering its validity:

> [a lawlike sequence] might be described as a sequence [a mapping associating with every natural number a mathematical object belonging to a certain well-defined set] which is completely fixed in advance by a law, i.e. a prescription (algorithm) which tells us how to find for any n member of $\mathbb{N}$ the n^{th} member of the sequence.[24]

When this problem is generalized to theories, Hilbert's aim of determining the truth of any proposition A within a given set of axioms Γ corresponds to constructing a finite proof procedure to check whether A is a theorem within the theory described by Γ. In view of the restriction required by the intuitionistic foundation, several theorems and axioms of classical mathematics could not be proven valid, because not 'constructible', as for example the Law of Excluded Middle and the Fixed Point Theorem of Topology. In view of the idea of providing a 'foundation' (rather than a method or instrument of proceeding in the construction of science), the intuitionistic programme failed in that all classical mathematics cannot be 'constructed'. On the other hand, the failure of formalism was determined by the impossibility of reducing all mathematics to logical sentences. And the failure of formalism was dictated by Gödel's First Incompleteness Theorem.[25]

The foundational crisis of mathematics amounted to the quest for establishing all valid formulas of theories, avoiding the various traps of paradoxes, circular definitions, and the infinity. In particular, Hilbert was looking for a *mechanical way* to determine the provability of every possible mathematical sentence of any given system. The formalization of this task requires set-theoretical tools which we overview in Chapter 3.

Exercises

Exercise 1 *Explain informally how consequence and inference differ in explaining mathematical truths.*

Exercise 2 *Explain informally what the soundness and completeness problems for mathematical theories are.*

Exercise 3 *Illustrate the main principles of the logicist programme in the foundations of mathematics.*

[24] (Troelstra, 1969, p.17).

[25] Gödel (1931).

Exercise 4 *Assuming the definition of the cardinality of a set as the number of its elements, and Frege's definition of number as the extension of a concept, which concepts are expressed by the cardinality of an empty set and of an infinite set?*

Exercise 5 *Consider the following sentence: 'This sentence is false.' Explain how this generates a paradox.*

Exercise 6 *Illustrate the main principles of the finitist programme in the foundations of mathematics.*

Exercise 7 *Explain informally what decidability for sentences of mathematical theories means.*

Exercise 8 *Consider the following definition of the set S: the set of all sets that are greater than S. What type of definition is this and what problems can arise in connection to it?*

Exercise 9 *Illustrate the main principles of the intuitionist programme in the foundations of mathematics.*

Exercise 10 *Why is a mechanical procedure essential according to Hilbert for deciding truth?*

3 Computing and Deciding

Summary

This chapter illustrates the basic tools of computability theory, essential to the formulation of the decision problem and the definition of the notion of computable function.

3.1 Enumerability

The limits to validity identified during the foundational crisis were mainly due to the role that infinity played in the definition of mathematical concepts. This notion of infinity has been crucial in mathematics since antiquity, and it had been the source of paradoxes at least since Zeno. Its presence would return crucially in the seventeenth century with the development of calculus by Newton and Leibniz, and later in the theory of sets by Georg Cantor (1845–1918). His famous theorem based on the diagonalization method is a milestone for mathematics and it allows us to review some essential techniques in the formulation of limiting results related to computability. The method involves essentially the use of the infinite by referring to the enumeration of an infinite list of objects. Such enumeration is expressed in terms of a well-defined function which returns the intended set as result. As required by Hilbert, this notion of infinite list is then reduced to an effectively computable method if it can be guaranteed that each entry of the list comes at a certain point after a finite number of members of the list has been enumerated after the first one. Cantor's diagonal method shows that even in this way it is not possible to arrange all sets of positive integers in a single infinite list.

Let us start by some fundamental notions of naive set theory. Recall that a set is formally intended as a collection of objects, known as the elements or members of the set. We denote the membership of an object s in the set S by the formula $s \in S$. A set is

On the Foundations of Computing. Giuseppe Primiero, Oxford University Press (2020). © Giuseppe Primiero.
DOI: 10.1093/oso/9780198835646.001.0001

well defined if and only if, for any given object s, we can say for certain object whether or not it is a member of the set, i.e. whether $s \in S$ or $s \notin S$. This means to be able to list all elements of S, or enumerate them.

Definition 17 (Enumerable Set) *An enumerable or countable set S is one whose members can be enumerated or arranged in a list.*

The list has to include all and only the elements of the set, in a way such that after some finite number of steps, one can reach any of the elements in that set. The list is unordered, i.e. its members do not have a fixed position in the list, and copies of members do not count. An example is the set of natural numbers smaller than 10, or that of numbers which can divide 2 without returning a rational. A set with an infinite number of elements can also be arranged as a list, e.g. the set of natural numbers $\mathbb{N}$:

Definition 18 (Denumerable Set) *A denumerable or enumerably infinite set is one with an infinite number of members arranged in a list.*

Sets can be enumerated by functions as well:[1]

Definition 19 (Function) *A function f is an assignment of values to arguments. The set of all valid arguments of a function is the domain D of the function f. The set of all the values the function assigns to D is the range R of the function f.*

Definition 20 (Total Function) *A total function $f(d)$ from the domain D to the range R is defined for every element $d \in D$.*

The enumeration of a set by a function needs to be complete: every element in the set needs to appear at least once. By the definition of set, a redundant list of elements obtained by a well-defined function is still an enumeration of the elements in that set. On the other hand, there are functions which are not defined over every possible element:

Definition 21 (Partial Function) *A partial function $f(d)$ from the domain D to the range R is defined for some element $d \in D$.*

Definition 22 (Surjective or Onto Function) *A surjective function $f(d)$ from the domain D to the range R has at least one element $d \in D$ assigned for every element $r \in R$.*

Definition 23 (Injective or 1–1 Function) *An injective function $f(d)$ from the domain D to the range R has at most one element $d \in D$ for every element $r \in R$.*

Definition 24 (Inverse Function) *The inverse function $f^{-1}(d)$ from the domain D to the range R is defined by letting $f^{-1}(r)$ be the one and only d such that $f(d) = r$, if such an element d exists.*

[1] In the following we use the terms *domain* and *range* to denote respectively the set of possible input and output values of functions; totality (or partiality) of a function is determined by the domain being well defined. Another terminology distinguishes the *source* and the *target* as input and output sets, while *domain* and *range* are strictly used to refer to subsets of source and target containing respectively valid input and actual outputs.

In the following, we constrain ourselves to functions whose domain is the set of positive integers:

Definition 25 (Function of Positive Integers) *A function f of positive integers $\mathbb{Z}$ encodes an arrangement of the members of its range R.*

Let us consider some examples:

- the set E of even positive integers is encoded by the function $f(n) = 2(n)$;
- the set O of odd positive integers is encoded by the function $f(n) = (2n - 1)$;
- the whole set $\mathbb{Z}$ of positive integers is encoded by the function $f(n) = n$ (i.e. the identity function);
- the whole set $\mathbb{Z}$ of positive integers is (also) encoded by the function

$$g(n) = \begin{cases} n + 1, \text{ if } n \text{ is odd} \\ n - 1, \text{ if } n \text{ is even} \end{cases}$$

Every function can be defined as partial. Consider the following examples:

- the set E of even positive integers is encoded by the partial function $j(n)$

$$j(n) = \begin{cases} n, \text{ if n is even} \\ \text{undefined otherwise} \end{cases}$$

- any subset S of the set $\mathbb{Z}$ positive integers is encoded by the partial function $k(n)$

$$k(n) = \begin{cases} n, \text{ if } n \text{ is in the set S} \\ \text{undefined otherwise} \end{cases}$$

Every subset of the set of positive integers is enumerable, i.e. a function can be defined for every subset such that the function gives that set as its range. Hence, the following definition:

Definition 26 (Enumerable Set by a Function) *A set S is enumerable if and only if for every $s \in S$ there is at least one positive integer $n \in \mathbb{Z}$ such that $f(n) = s$.*

In view of the definition of an enumerable set as the ordered list that can be obtained as the result of applying a function to integers, one also has the following:

Definition 27 (Enumerable Set) *A set S is enumerable if and only if S is the range of some function f of positive integers, i.e. $f(n) = s$ for every $s \in S$.*

Such function f defining the elements in S is called the characteristic function of S:

Definition 28 (Characteristic Function) *A function f is called the characteristic function of a set S if and only if*

$$f(s) = \begin{cases} 1, \ if\, s \in S \\ 0, \ if\, s \notin S \end{cases}$$

3.2 Encoding

The notion of function is generalized by defining it for more than one argument. A function $f(m,n)$ can be conveniently defined as a one-place function with ordered pair of integers as argument (and so for many arguments). The inverse generalization is to look at a function of one argument as the code that yields any given pair (or set) of values as its range. In this case we call the argument of that function the code for the given pair:

Definition 29 (Code Number) *Given a function f which enumerates pairs of positive integers (m,n), any argument s such that $f(s)=(m,n)$ may be called the code number for the pair (m,n). Applying the function f means to decode s; the other way round means to encode the pair (m,n).*

In order to define a function that takes a pair of integers as argument and yields an integer as value, one can encode the set of ordered pairs of positive integers. A possible method to do this consists in listing all the pairs of positive integers according to the following rule:[2]

1. enter all the pairs the sum of whose entries is 2;
2. enter the pairs the sum of whose entries is 3 and so on;
3. for entries with equal sum, enter first the pair with lower first entry:

$$(1,1),(1,2),(2,1),(1,3),(2,2),(3,1),(1,4)\ldots$$

Then a code for (m,n) is the number s corresponding to the position in which the pair (m,n) is located. That number is obtained by counting all the pairs $m+n-2$ whose sum is $m+n-1$. For example, for the pair $(m=1,n=1)$ there are $1+1=2-2=0$ pairs to go through whose sum is $1+1-1=1$. The general formula is given as

$$[1+2+\ldots(m+n-2)]+m$$

The code J for any item in this list is as follows:

$$J(m,n)=(m^2+2mn+n^2-m-3n+2)/2$$

A generalization of the previous case is to encode the set of finite sequences of positive integers. Take $G_1(n)$ to be the 1-term sequence n. G_2 is the function enumerating all the 2-tuples or pairs from Cantor's zig-zag list:

$$(1,1),(1,2),(2,1),(1,3),(2,2),(3,1),(1,4)\ldots$$

[2] This method is illustrated in (Boolos et al., 2002, chapter 1).

G_3 is the function enumerating the triples obtained by substituting in the previous list the second entry n with the nth component in the same list:

$$(1,(1,1)),(1,(1,2)),(2,(1,1)),(1,(2,1)),(2,(1,2)),(3,(1,1)),(1,(1,3))\ldots$$

and so on for every G_i. An encoding of all these sequences by a pair of positive integers can be obtained by encoding any sequence G of length k by the pair (k,a) where $G_k(a) = s$. In other words: start by the original listing of pairs and replace any pair (k,a) by the ath item on the list of k-tuples:

- replace $(1,1)$ by the first item 1 in the list of 1-tuples;
- replace $(1,2)$ by the second item 2 in the list of 1-tuples;
- replace $(2,1)$ with the first item $(1,1)$ in the list of 2-tuples:

$$(1),(2),(1,1),(3),(1,2),(1,1,1),(4)\ldots$$

3.3 Diagonalization

Given the definition of enumerable set, it is easy to understand the notion of a nonenumerable set, i.e. a set for which no function can be given whose range contains all the elements in that set. The existence of such sets is exemplified by the following theorem:

Theorem 1 (Cantor's Theorem) *The set P^* of all sets of positive integers is not enumerable.*

Proof. The proof is by contradiction. Build the infinite list L of sets of positive integers $S_1, S_2, S_3, \ldots$. This will contain all the possible subsets of the set of integers (odd, even, and so on). Then define the set $\Delta(L)$ as follows:

Definition 30 (Diagonal List) *For each positive integer n, n is in the diagonal list $\Delta(L)$ if and only if n is not in S_n.*

Let us proceed by constructing $\Delta(L)$. Let us assume that S_1 is the list of prime positive integers $S_1 = \{2,3,5,\ldots\}$; then $1 \in \Delta(L)$ because $1 \notin S_1$. Take now S_2 and assume this is the list of even positive integers $S_2 = \{2,4,6,\ldots\}$; then $2 \notin \Delta(L)$ because $2 \in S_2$. Take now S_3 and assume this is the list of odd positive integers $S_3 = \{1,3,5,\ldots\}$, then $3 \notin \Delta(L)$ because $3 \in S_3$. And so on. Then, provided L is the list of *all* sets of integers, $\Delta(L) \in L$ i.e. $\exists m.S_m = \Delta(L)$ for some positive integer m. But for the definition of $\Delta(L)$

Definition 31 *$m \in \Delta(L)$ if and only if $m \notin S_m$.*

This contradicts the following:

Definition 32 *$m \in \Delta(L)$ if and only if $m \in S_m$.*

Hence if $\Delta(L) \in L$ we have a contradiction, therefore $\Delta(L)$ cannot be in L. This demonstrates that the set L of all sets of positive integers is not enumerable. □

This proof can be illustrated applying the diagonalization method. Let the list of sets of positive integers

$$L = S_1, S_2, S_3, \ldots$$

be represented by functions $s_1, s_2, s_3, \ldots$ ranging over $\{0, 1\}$ according to the following definition:

$$s_n(p) = \begin{cases} 1, \text{ if } p \text{ is in } S_n \\ 0, \text{ if } p \text{ is not in } S_n \end{cases}$$

As an example, for S_3 the list of odd positive integers $S_3 = \{1, 3, 5, \ldots\}$, the function s_3 will give the following values:

$$s_3(1) = 1; s_3(2) = 0; s_3(3) = 1; \ldots$$

Order now vertically the list of functions $s_1, s_2, s_3, \ldots$ and let the list

$$s_n(1), s_n(2), s_n(3), \ldots$$

be the nth row in that list. Then this row will be a list of 0, 1, according to the presence of each entry p at $s_n(p)$ in the set s_n. The *diagonal list* is obtained by taking the following elements:

$$s_1(1), s_2(2), s_3(3), \ldots s_n(n).$$

i.e. the first entry in the first list, the second entry in the second list, up to the n^{th} entry in the n^{th} list. Then the *anti-diagonal list* is obtained by inverting the values of each entry: change to zero the values one and to one the values zero of the items in the diagonal list. This can be obtained as follows:

$$\begin{aligned} s_m(1) &= 1 - s_1(1), \\ s_m(2) &= 1 - s_2(2), \\ s_m(3) &= 1 - s_3(3), \\ &\vdots \end{aligned}$$

where each $s_n(n)$ is a zero or a one. The sequence defined as the antidiagonal list does not appear in any place of the list L. If it should, at row m we would have

$$\begin{aligned} s_m(1) &= 1 - s_1(1), \\ s_m(2) &= 1 - s_2(2), \\ s_m(3) &= 1 - s_3(3), \\ &\vdots \\ s_m(m) &= 1 - s_m(m) \end{aligned}$$

The mth item in this list S_m gives the identity $1 = 0$, because if $s_m(m) = 1$ then $1 - s_m(m) = 0$ and if if $s_m(m) = 0$ then $1 - s_m(m) = 1$.

The argument at the basis of Theorem 1 can be offered now in a short version as follows:

Proof. For every set S the power set $P(S)$ of S, i.e. the set of all subsets of S is larger than S itself. Let f be a function $f : S \mapsto P(S)$, then it is not the case that for every element $p \in P(S)$ there is an element in $s \in S$ such that $f(s) = p$, i.e. some subset of S is not in the image of the function. Let us consider the set

$$T = \{ s \in S \mid s \notin f(s) \}.$$

T is not in the image of f: for all $s \in S$, either s is in T or it is not. In both cases, $f(s) \neq T$, because: if $s \in T$, then by definition of T, $s \notin f(s)$, so $T \neq f(s)$ since $s \in T$ but $s \notin f(s)$; if $s \notin T$, then by definition of T, $s \in f(s)$, so $T \neq f(s)$, since $s \notin T$ but $s \in f(s)$. □

3.4 The Decision Problem

The result of Cantor's Theorem leads to the idea that there are sets whose elements cannot be enumerated. Provided enumerability allows one to define a characteristic function for the relevant set, nonenumerability means nondefinability. Consider the set S of all sets: according to the previous argument, then its power set $P(S)$ is the set of all subsets of all sets. As S is the set of all sets, it is supposed to include $P(S)$ to be complete; but $P(S)$ should also be bigger than S. This shows informally that the notion of 'set of all sets' is inconsistent. This is what Russell's paradox has shown: if any definable subclass of a set is a set, contradictions arise. This last claim can be shown by the use of the following principle:

Definition 33 (Comprehension Principle) *Given any set S and predicate ϕ, there is a set S' which is a subset of S such that x is a member of S' if and only if $x \in S$ and $\phi(x)$ holds. By the axiom of extensionality this set is unique.*

The unrestricted version of the Comprehension Principle let impredicativity arise, because it says that every subset defined by a predicate is itself a set:

Definition 34 (Unrestricted Comprehension Principle) *Given any predicate ϕ, there is a set S such that x is a member of S if and only if $\phi(x)$ holds. By the axiom of extensionality this set is unique.*

The basic answer to the problem of impredicativity and paradoxes obtained by the diagonalization method is represented by the notion of *effective computability*. Accordingly, the problem of enumerability and of definability, reduces to the problem of establishing whether the characteristic function for any given set can be in some sense qualified as effectively computable. The computability of the characteristic function for the set of theorems and (assuming soundness and completeness) of the consequence set of any given theory is the precise formulation of Hilbert's problem of decidability (see Thesis 5):

Proposition 2 (Decision Problem) *Can an effective method be formulated that applied to any finite set of sentences Γ and a sentence ϕ within a system of logic F would establish in a finite amount of time whether $\Gamma \vDash_F \phi$?*

For example: one wants to decide given a formula ϕ of number theory whether it holds for any number x, i.e. if it is valid.

One can also understand the question in purely mechanical terms: imagine the system of reference as a set of axioms and rules denoted by Γ; a system of axioms and rules is logically equivalent to a 'machine'; and take *any* output ϕ. We want to check, if any such ϕ is or is not an output of our 'machine' Γ. Hence, one is looking for a method that can always establish if something is or is not a valid output of a given program for any machine. This gives us the mechanical version of the decision problem:

Proposition 3 (Mechanical Decision Problem) *Could there be a generalized 'calculation procedure' that would tell us whether any output ϕ can be obtained by any machine Γ with a given input ι?*

The notion of effective method or calculation procedure at the basis of the decision problem needed clarification. In other words, the following question emerged: what does it mean that a function is effectively calculable? Our next task is to formulate a mathematically precise answer to this question.

Exercises

Exercise 11 *Give at least one example of an enumerable set and one of a denumerable set with elements in $\mathbb{N}$.*

Exercise 12 *Give at least one example of a total function and one of a partial function with domain in $\mathbb{Z}$.*

Exercise 13 *Consider the following function with domain in $\mathbb{N}$:*

$$f(n) = \begin{cases} 1, \text{ if } n = 1 \\ n - 1, \text{ if } n > 1 \end{cases}$$

Qualify this function as either injective or surjective and explain why.

Exercise 14 *Give at least one example of an injective function over $\mathbb{Z}$.*

Exercise 15 *Give at least one example of a function over $\mathbb{Z}$ and define its inverse.*

Exercise 16 *Enumerate the set of the successors of the odd numbers by a function.*

Exercise 17 *Define a subset of $\mathbb{Z}$ by its characteristic function.*

Exercise 18 *Show formally how the characteristic function of the diagonal list generates an arithmetical contradiction.*

Exercise 19 *What does it mean for a set to be nonenumerable?*

Exercise 20 *Explain the decision problem.*