Preface

My main aim is to make accessible to readers without any specialist training in mathematics, and with only an elementary knowledge of modern logic, complete proofs of the fundamental metatheorems of standard (i.e. basically truth-functional) first order logic, including a complete proof of the undecidability of a system of first order predicate logic with identity.

Many elementary logic books stop just where the subject gets interesting. This book starts at that point and goes through the interesting parts, as far as and including a proof that

> it is impossible to program a computer to give the right answer (and no wrong answer) to each question of the form 'Is — a truth of pure logic?'

The book is intended for non-mathematicians, and concepts of mathematics and set theory are explained as they are needed.

The main contents are: Proofs of the consistency, completeness and decidability of a formal system of standard truth-functional propositional logic. The same for first order monadic predicate logic. Proofs of the consistency and completeness of a formal system of first order predicate logic. Proofs of the consistency, completeness and undecidability of a formal system of first order predicate logic with identity. A proof of the existence of a non-standard model of a formal system of arithmetic.

The reader will be assumed to have an elementary knowledge of truth-functional connectives, truth tables and quantifiers. For the reader with no knowledge of set theory, here are very brief explanations of some notations and ideas that will be taken for granted later on:

1. *The curly bracket notation for sets*

'{Fido, Joe}' means 'The set whose sole members are Fido and Joe'. '{3, 2, 1, 3, 2}' means 'The set whose sole members are the numbers 3, 2, 1, 3, 2' (and this last set is the same set as {1, 2, 3}, i.e. the set whose sole members are the numbers 1, 2 and 3).

2. *The epsilon notation for set-membership*

'$n \in X$' means 'n is a member of the set X'.

3. *The criterion of identity for sets*

A set A is the same set as a set B if and only if A and B have exactly the same members. *Nothing else matters* for set identity.

4. *The empty set*, $\emptyset$

By the criterion of identity for sets [(3) above], if A is a set with no members and B is a set with no members, then A is the same set as B; so if there is a set with no members, there is just one such set. We shall assume that there is such a set.

Further introductory material on set theory can be found in, for example, chap. 9 of Suppes (1957) or chap. 1 of Fraenkel (1961).

The book deals only with (1) *standard* (i.e. basically truth-functional) logic, and (2) *axiomatic* systems.

(1) Standard first order logic, with its metatheory, is now a secure field of knowledge; it is not the whole of logic, but it is important, and it is a jumping-off point for most other developments in modern logic. There seemed to me to be no book that tried to make accessible to non-mathematicians complete proofs of the basic metatheory of standard logic: hence this one.

(2) Axiomless systems (so-called 'natural deduction systems') are nowadays getting more popular than axiomatic systems, for formal proofs of theorems *inside* a system are generally shorter and easier to find with a natural deduction system than with an axiomatic one. But I find that complete proofs of *metatheorems* (theorems *about* a system) are in general longer and more laborious for natural deduction systems than for axiomatic ones; so, since I am mainly concerned with proofs of theorems about systems and not much concerned with proofs inside systems, and since anything you can get with a natural deduction system you can get with an axiomatic one, I have deliberately concentrated on axiomatic systems.

I hope that the book will equip those who are not mathematical specialists not only to tackle more advanced works on standard logic, such as those of Kleene or Mendelson or Shoenfield or Smullyan,[1] but to frame philosophically interesting systems of non-standard logic and to prove metatheorems about them. For I believe that the logician's most urgent tasks at present lie in the field of non-standard logic. There is, for example, a sense of 'if' that is crucial to many everyday arguments; it seems clear to me that 'if' in that sense is not a truth-functional connective; and so I think it a scandal that the sense has not yet been adequately caught in any interpreted formal system with an adequate metatheory. I commend the task to my readers, who may find help in Church (1956) and in Hughes and Cresswell (1968).

The books I have borrowed most from are Mendelson (1964) and Margaris (1967). I thank the following people for ideas, information, or criticisms: Ross Brady, John Crossley, John Derrick, Len Goddard, Jeff Graves, Geoffrey Keene, Martin Löb, Angus Macintyre, Timothy Potts, Rowan Rockingham Gill, Harold Simmons, Dick Smith and Bob Stoothoff. My predecessors and colleagues in the Department of Logic and Metaphysics in the University of St Andrews, and especially Professors J. N. Wright and L. Goddard, made it possible for me to concentrate on this part of logic, and without them the book would not exist.

GEOFFREY HUNTER

St Andrews,
December 1969

For corrections to the first printing I am indebted to Ross Brady, M. J. Cresswell, Rod Girle, John Hall, L. Hodes, Harry Lewis, J. Howard Sobel, and Barry Taylor. I am also indebted to the late Richard Montague, who read part of the book for the University of California Press, for criticism at an earlier stage; to Alan Anderson and Nuel Belnap for their beautiful system in §37; and to Czeslaw Lejewski.

For additional corrections I am indebted to M. C. Bradley, Edwin Hung, Laurence Goldstein, Michael Levin, Hugh Rice, Joe Van de Mortel, and William Wisdom.

G. H.

[1] For detailed references, see pp. 262 ff.

PART ONE

Introduction: General Notions

To get a rough idea of what the metatheory of logic is, start with

(1) *truths of logic.*

Distinguish these from

(2) *sentences used to express truths of logic.*

(Two different sentences, e.g. one in French, one in English, might be used to express the same truth of logic.)

Now consider

(3) *the theory of sentences-used-to-express-truths-of-logic.*

This last is, roughly, *the metatheory of logic.*

The big difference between metatheory in that rough sense and metatheory in the sense of this book is over (2). In this book the sentences-used-to-express-truths-of-logic must be formulas of a *formal language*, i.e. a 'language' that can be completely specified without any reference at all, direct or indirect, to the meaning of the formulas of the 'language'. It was by the insistence on this requirement that the metatheory of logic, after a long and interesting but desultory history of over two thousand years, came in this century to yield exact and new and deep results and to give promise of systematic growth.

So we begin with formal languages.

1 Formal languages

The basic objects of metatheory are *formal languages*.

The essential thing about a formal language is that, even if it is given an interpretation, *it can be completely defined without reference to any interpretation for it*: and it need not be given any interpretation.

A formal language can be identified with the set of its *well-formed formulas* (also called *formulas* or *wffs*). If the set of all wffs of a formal language L is exactly the same as the set of all wffs of a formal language L′, then L is the same formal language as L′. If not, not.

A *formula* is an abstract thing. A *token* of a formula is a mark or a string of marks. Two different strings of marks may be tokens of the same formula. It is not necessary for the existence of a formula that there should be any tokens of it. (We want, for example, to speak of formal languages with infinitely many formulas.)

The set of well-formed formulas of a particular formal language is determined by a fiat of its creator, who simply lays down what things are to be wffs of his language. Usually he does this by specifying

(1) a set of *symbols* (the *alphabet* of his language)

and

(2) a set of *formation rules* determining which sequences of symbols from his alphabet are wffs of his language.

It must be possible to define both sets without any reference to interpretation: otherwise the language is not a formal language.

The word 'symbols' in the last paragraph is a technical term: symbols, in this technical sense of the word, need not be symbols of anything, and they must be capable of being specified without reference to any interpretation for them.

Symbols are abstract things, like formulas. A token of a symbol is a mark or configuration of marks.

Roughly, a formal language could be completely mastered by a suitable machine, without any understanding. (This needs qualification where the formal language has an uncountable alphabet (see §10 below): in such a case it is not clear that the formal language could be completely mastered by anything.)

Given a particular formal language, we may go on to do either or both of the following things:

1. We may define the notion of *an interpretation of the language*. This takes us into *model theory*.
2. We may specify a *deductive apparatus* for the language. This takes us into *proof theory*.

EXERCISES

1. The language W is defined as follows:
   Alphabet: △ □
   Formulas: Any finite string of symbols from the alphabet of W that begins with a '△' is a formula.
   Is W a formal language?
2. The language X is defined as follows:
   Alphabet: a b c d e f g
   Formulas: Any finite string of symbols from the alphabet of X that makes an English word is a formula.
   Is X a formal language?
3. The language Y is defined as follows:
   Alphabet: a b c d e f g
   Formulas: Any finite string of symbols from the alphabet of Y that does not make an English word is a formula.
   Is Y a formal language?

ANSWERS

1. Yes.
2. No. The definition of *formula of X* involves essentially reference to meaning, since a thing is an English word only if it has a meaning. (In order to know that a thing is a word you don't have to know *what* it means, only *that* it has a meaning. But even this weak reference to meaning is enough to prevent X from being a formal language.) (Another way of putting it: You could program a machine to find out if the string of symbols was a word in some specified English dictionary, and the

machine could do this without knowing the meaning of any word. But, with some exceptions which we may neglect, things are included in a dictionary only if they have a meaning or meanings.)

3. No. In order to tell whether or not a string of symbols from the alphabet of Y is a formula of Y you have to know whether or not it is an English word, and so whether or not it has a meaning. How, for example, do you tell whether 'bac', or 'deg', or 'ged', or 'gef', or 'geg', or 'gegg', is a formula of Y? Only by finding out if it is a meaningful English word. (In fact 'geg' seems to be the only one that is not an English word, and so the only one that is a formula of Y.)

2 Interpretations of formal languages. Model theory

In rough and very general terms, an *interpretation* of a formal language is an assignment of meanings to its symbols and/or formulas.[1] *Model theory* is the theory of interpretations of formal languages (a *model* of a formula of a language is an interpretation of the language for which the formula comes out true).[2] Among the concepts of model theory are those of *truth for an interpretation*, *semantic* (or *model-theoretic*) *consequence*, and *logical validity*.

EXERCISE

Give an interpretation for the formal language W (§1, exercise 1).

ANSWER

A possible interpretation would be: Take '△' as meaning the same as the (decimal) digit '1', '□' as meaning the same as the digit '0', and each formula accordingly as meaning the same as

[1] In Part 2 we restrict the notion of interpretation to interpretations for which each interpreted formula is either true or false. In Part 3 there is an analogous restriction.

[2] At least in one standard sense of 'model', which we follow in this book. Another sense, closely related to ours, will be mentioned in Part 3.

a decimal numeral composed exclusively of '1's and '0's. So, e.g., '△ □ △' is to mean the same as '1 0 1' in the decimal system.

This shows that, in a very wide sense of 'interpretation', an interpreted formula need not be a proposition, where by 'proposition' we mean a sentence expressing something true or false. It can be, as here, a name of something. Or it can be an adjective, or an adverb, or a preposition, or a phrase, or a clause, or an imperative sentence, or a string of sentences, or a string of names, or . . . Or such meanings might be attached to the symbols that some or all of the interpreted formulas came out as nonsense. Later in the book we restrict the notion of interpretation: see p. 6, fn. 1.

3 Deductive apparatuses. Formal systems. Proof theory

By specifying a deductive apparatus for a formal language we get a formal system.

A *formal system* S is a formal language L together with a *deductive apparatus* given by

(1) laying down by fiat that certain formulas of L are to be *axioms* of S

and/or

(2) laying down by fiat a set of *transformation rules* (also called *rules of inference*) that determines which relations between formulas of L are relations of *immediate consequence* in S. (Intuitively, the transformation rules license the derivation of some formulas from others.)

The deductive apparatus must be definable without reference to any intended interpretation of the language: otherwise the system is not a formal system.

A deductive apparatus can consist of axioms and rules of inference, or of axioms alone, or of rules of inference alone.

Proof theory is that part of the theory of formal systems (i.e. of formal languages with deductive apparatuses) that does not involve model theory in an essential way (i.e. that does not require any reference to interpretations of the languages). Among concepts belonging to proof theory are those of *proof in* *a system* (or *formal proof*), *theorem of a system* (or *formal theorem*), *derivation in a system* (or *formal derivation*), and *syntactic* (or *proof-theoretic*) *consequence*. All these involve essentially reference to a deductive apparatus, and all can be defined without saying anything about interpretations.

A formal language can be identified with the set of all its wffs. But a formal system cannot be identified with the set of all its theorems. For two formal systems S and S′ may have exactly the same theorems and yet differ in some proof-theoretically important way: e.g. a formula A that is a syntactic consequence in S of a formula B may not be a syntactic consequence in S′ of B.

EXERCISES

Let Z be the system defined as follows:

Alphabet: △ □

Formulas: Any finite string of symbols from the alphabet of Z that begins with a '△' is a formula of Z. Nothing else is a formula of Z.

Axiom: △ □ □ □

Rule of Inference: Any formula of Z whose last two symbols are a '△' and a '□', in that order, is an immediate consequence in Z of any formula of Z whose first two symbols are a '△' and a '□', in that order. [E.g. '△ □ □ □ △ △ □' is an immediate consequence in Z of '△ □ △ △ △ □ △'.] Nothing else is an immediate consequence in Z of anything.

1. Is Z a formal system?
2. Is '△ △ □' an immediate consequence in Z of '△ □ □ □'?
3. Is '△ □' an immediate consequence in Z of '△ □'?
4. Is '△ □ □ △' an immediate consequence in Z of '△ □ □ △'?
5. Is '□ □ △ △ □' an immediate consequence in Z of '△ □ △ △ △ △'?
6. Give an example of an immediate consequence in Z of '△ △ △ △ △'.

ANSWERS

1. Yes.
2. Yes.
3. Yes.
4. No. Only formulas that end '. . . △ □' can be immediate consequences in Z.
5. No. '□ □ △ △ □' is not a formula of Z, since it does not begin with a '△'.
6. There are none. Only formulas that begin '△ □ . . .' can have immediate consequences in Z.

4 'Syntactic', 'Semantic'

In this book 'syntactic' and 'semantic' will have the following meanings:

Syntactic: having to do with formal languages or formal systems without essential regard to their interpretation.

Semantic: having to do with the interpretation of formal languages.

'Syntactic' has a slightly wider sense than 'proof-theoretic', since it can be applied to properties of formal languages without deductive apparatuses, as well as to properties of formal systems. 'Semantic' in this book just means 'model-theoretic'.

EXERCISES

1. Is it a syntactic or a semantic property of a formula of the system Z (§3, exercises) that it is an immediate consequence in Z of another formula of Z?
2. Is it a syntactic or a semantic property of a formula that it denotes a number?
3. Is it a syntactic or a semantic property of a formula that it is true?

ANSWERS

1. Syntactic.
2. Semantic: the last part of the question can be paraphrased by '. . . that it can be *interpreted* as denoting a number'.

3. Semantic: the last part of the question can be paraphrased by '. . . that it can be *interpreted* as expressing something true'.

5 Metatheory. The metatheory of logic

Metatheory is the theory of formal languages and systems and their interpretations. It takes formal languages and systems and their interpretations as its objects of study, and consists in a body of truths and conjectures about these objects. Among its main problems are problems about the *consistency*, *completeness* (in various senses), *decidability* (see §8 below) and *independence* of sets of formulas. Both model theory and proof theory belong to metatheory.

The *metatheory of logic* is the theory of those formal languages and systems that for one reason or another matter to the logician. Usually the logician is interested in a formal language because it has formulas that can be interpreted as expressing logical truths; and usually he is interested in a formal system because its theorems can be interpreted as expressing logical truths or because its transformation rules can be interpreted as logically valid rules of inference.

6 Using and mentioning. Object language and metalanguage. Proofs in a formal system and proofs about a formal system. Theorem and metatheorem

In logic the words 'use' and 'mention' [both the nouns and the verbs] are sometimes used in a technical sense to mark an important distinction, which we explain by example:

A. 'London' is a word six letters long.
B. London is a city.

In A the word 'London' is said to be *mentioned*; in B the word 'London' is said to be *used* (and not mentioned).

There are various ways of indicating that an expression is being mentioned; e.g. enclosing it in quotation marks (as in the

example), or printing it in italics, or printing it on a line to itself. We shall use some of these devices, but in order to save quotation marks and also to make the text easier to read, we shall in addition make use of a standard convention. In cases where the context makes it clear that expressions are being mentioned, not used, we shall sometimes omit quotation marks: e.g. instead of writing

'$\supset$' is a truth-functional connective

we shall write simply

$\supset$ is a truth-functional connective

and instead of writing

The set {'$\sim$', '$\wedge$', '$\vee$'}

we shall write simply

The set $\{\sim, \wedge, \vee\}$.

Formal languages are sometimes called *object languages*. The language used to describe an object language is called its *metalanguage*. We use English, supplemented by special symbolism (including the symbolism of set theory), for our metalanguage.

A *proof in a formal system* that has axioms (and all the ones we shall be concerned with have axioms) is a string of formulas of a formal language that satisfies certain purely syntactic requirements and has no meaning.

A *proof about a formal system* is a piece of meaningful discourse, expressed in the metalanguage, justifying a true statement about the system.

Similarly a *theorem of a formal system* is a formula of a formal language that satisfies certain purely syntactic requirements and has no meaning, while a *theorem about a formal system* (also called a *metatheorem*) is a true statement about the system, expressed in the metalanguage.

EXERCISES

1. *Christian lady*: It is enough for my argument if you admit that the existence of God, if not certain, is at least probable; or if not probable, is at least possible.

Infidel: I can make no such admission until I know what you intend by the word 'God'.

Charles Bradlaugh, 'Doubts in Dialogue', *National Reformer*, 23 Jan 1887

(*a*) In the dialogue above, is the Christian lady using or mentioning the word 'God', in the logician's special sense of the words 'using' and 'mentioning'?

(*b*) Is the Infidel using or mentioning the word 'God'?

2. In each of the following cases say whether the sentence 'Shut the door' is used or mentioned:

(*a*) 'Shut the door' is used to make a request or issue a command.

(*b*) Shut the door.

(*c*) I don't know what you mean by 'Shut the door'.

3. In each of the following cases say whether the sentence 'Cruelty is wrong' is used or mentioned:

(*a*) Cruelty is wrong, no matter what the circumstances.

(*b*) The words *Cruelty is wrong* express a true proposition.

(*c*) The sentence 'Cruelty is wrong' is typically used to condemn cruelty.

4. In the following sentence which words are used, which mentioned?

> What *is* means is and therefore differs from *is*, for '*is* is' would be nonsense.

Bertrand Russell, *My Philosophical Development*, p. 63

5. Is the proposition

> Not every string of '△'s and '□'s is a formula of the formal system Z [of §3]

a theorem of Z, a theorem about Z, or a metatheorem?

6. Given that, for any formal system S, anything that is either an axiom of S or an immediate consequence in S of an axiom of S is a *theorem* of S, say for each of the following whether or not it is a theorem of the system Z of §3. [*Note*. This is not intended to be a definition of the notion of *formal theorem*, but merely a simplification for the sake of the exercise. The usual definition allows many more things to be theorems.]

(*a*) △ □ △ □

(*b*) □ □ △ □ [For System Z, see p. 8.]

(*c*) △ □ □ □

(*d*) '△ □ □ □' is a theorem of Z.

7. 'Let A and B be arbitrary formulas of a formal language L.' Explain the function in this sentence of the letters 'A' and 'B'.

8. In the exercises on §3 are the quotation marks in all and only those places where they ought to be?

ANSWERS

1. (*a*) Using.
   (*b*) Mentioning.
2. (*a*) Mentioned.
   (*b*) Used.
   (*c*) Mentioned.
3. (*a*) Used.
   (*b*) Mentioned.
   (*c*) Mentioned.

4. The sentence is 15 words long. I think that the 2nd, 9th, 11th and 12th words are mentioned, the others used. The 2nd and 9th words are names of the word 'is'. The first of the two words in quotation marks is the name of the word 'is'; the second is the word 'is'. So at that point first the name of the word 'is' is mentioned, and then the word 'is' is mentioned.

5. It is both a theorem about Z and a metatheorem (about Z). It is not a formula of Z, so it is not a theorem of Z.

6. (*a*) Yes (immediate consequence of the axiom).
   (*b*) No (not even a formula – it begins with a '□').
   (*c*) Yes (axiom).
   (*d*) No. Not a formula of Z (no formula of any of the formal languages in this book contains an expression in quotation marks). But it is a metatheorem of Z.

7. 'A' and 'B' here are metalinguistic variables, belonging to the metalanguage of the language L.

8. I hope so.

7 The notion of *effective method* in logic and mathematics

Throughout what follows we are concerned with effective methods *in logic and mathematics*, and not, e.g., with methods for telling whether or not something is an acid.

In logic and mathematics, an *effective method* for solving a problem is a method for computing the answer that, if followed correctly and as far as may be necessary, is logically bound to give the right answer (and no wrong answers) in a finite number of steps. An effective method for the solution of a class of problems is an effective method that works for each problem in the class.

This is not a very precise definition, but the concept is not a precise one, even though it belongs to the fields of logic, mathematics and computing.

The paradigm cases of effective methods are mathematical algorithms, such as Euclid's algorithm (Book VII, Prop. 1) for telling whether or not two positive integers have any common divisor other than 1, or his algorithm (Book VII, Prop. 2) for finding the greatest common divisor of two positive integers that are not relatively prime (i.e. that have some common divisor other than 1).

A method can be effective even though it is not possible in practice to follow it as far as is necessary in some (or even any) given case. For instance, there are numbers so large that writing or printing out their names in any suitable notation would take more paper than there is in the world; so (barring quite extraordinary powers of mental arithmetic) it would not be possible in practice to find their greatest common divisor by means of Euclid's algorithm. Nevertheless, even for those numbers Euclid's algorithm is an effective method.

It is not necessary for the existence of an effective method that it should be known to someone at some time. There may exist effective methods that nobody ever discovers in the whole history of the world.

Because an effective method must be capable of being followed mechanically, without requiring any insight or imagination or ingenuity on the part of the user, 'mechanical method' is sometimes used as a synonym for 'effective method'. Our definition ensures that an effective method must not require imagination or ingenuity by making it a condition of a thing's being an effective method that (1) it is a method of *computing* and (2) if it is followed correctly and as far as may be necessary, it is *logically* bound to give the right answer.

An objection to our explanation of 'effective method' is that

we have left unexplained the notions of *computing* and *logically bound* that are crucial to it. Our present answer to this objection is that the notion of an effective method is an informal, intuitive, imprecise one, not a formal and precise one, so that an explanation of the intuitive sense is bound to be imprecise. In a later Part we mention some suggested definitions of effectiveness that are precise and for which it is claimed that they do correspond satisfactorily to the intuitive notion (§52, Church's Thesis).

EXERCISES

1. Is 'Ask God' an effective method for solving a problem?
2. Is 'Ask an oracle' an effective method?
3. Is 'Ask an oracle that always answers and always tells the truth' an effective method?
4. Is 'First say "Yes", then say "No"' an effective method for solving a problem to which the right answer happens in fact to be 'Yes'?
5. Is 'Test it with litmus paper' an effective method (in the sense defined) for telling whether or not something is an acid?
6. 'No solution has been found to this problem, so there is no effective method for solving it.' Is this a valid argument?

ANSWERS

1. No. For (*a*) it is not a method of *computing*, and (*b*) it is not logically bound to give the right answer, for God need not answer.
2. No. Reasons as for 1 above.
3. No. Not a method of *computing*.
4. No. Cf. the requirement in the definition that the method should give *no wrong answers*.
5. No. Not a method of *computing*. Also not *logically* bound to give the right answer.
6. No. It is not necessary for the existence of an effective method that it should be known to someone.

8 Decidable sets

A set is *decidable* if and only if there is an effective method for telling, for each thing that might be a member of the set, whether or not it really is a member.

Some authors require of a formal system that the set of proofs in the system should be decidable. We shall not follow them in this. In each of the main formal systems in this book the set of proofs in the system is in fact decidable. But the metatheory for some of them refers occasionally to systems that may or may not have decidable sets of proofs: it is convenient to call such systems formal systems – and proper too, since they are defined in purely syntactic terms.

Every *finite* set is decidable. Intuitively, think of the members of the set as lined up in a row. Then to determine whether something is a member of the set, check to see whether it is identical with one of the things in the row.

Hereafter we abbreviate 'if and only if' to 'iff'.

EXERCISE

'A set is undecidable iff it has been proved that there is no effective method for telling whether or not a thing is a member of it.' Is there anything wrong with this statement?

ANSWER

Yes. Delete the words 'it has been proved that'.

9 1–1 correspondence. Having the same cardinal number as. Having a greater (or smaller) cardinal number than

There is a 1–1 *correspondence* between a set A and a set B iff there is a way (which need not be known to anyone) of pairing off the members of A with the members of B so that

(1) each member of A is paired with exactly one member of B and

(2) each member of B is paired with exactly one member of A.

(It follows that no member of either set is left unpaired.)

Two sets are said to *have the same cardinal number* or *the same cardinality* iff there is a 1–1 correspondence between them.

A set A *has a greater cardinal number than* a set B iff there is a 1–1 correspondence between B and a proper subset of A but no 1–1 correspondence between B and the whole of A. (A set C is a *proper subset* of a set D [written: $C \subset D$] iff there is no member of C that is not a member of D but there is a member of D that is not a member of C.)

A set A *has a smaller cardinal number than* a set B iff B has a greater cardinal number than A.

The cardinal number of a set is symbolised by writing two parallel lines over a name of the set. Thus the cardinal number of a set A is $\overline{\overline{A}}$, and '$\overline{\overline{A}} = \overline{\overline{B}}$' means 'The sets A and B have the same cardinal number'. (This notation, which is Cantor's, was meant by him to signify a double abstraction: (1) an abstraction from the nature of the members of the set, (2) an abstraction from the order in which they are taken; i.e. so far as the cardinal number of a set is concerned, neither the nature nor the order of the members of the set matters.)

EXERCISE

'Every set has a 1–1 correspondence with itself.' True or false?

ANSWER

True. The point of including this exercise was to bring out that the word 'pairing' in our definition of 1–1 *correspondence* is used in such a way that a thing can properly be said to be 'paired' with itself.

10 Finite sets. Denumerable sets. Countable sets. Uncountable sets

The *natural numbers* are the numbers 0, 1, 2, 3, etc.

A set is *finite* iff it has only a finite number of members; *denumerable* iff there is a 1–1 correspondence between it and the set of natural numbers (so a denumerable set is an infinite set);

countable iff it is either finite or denumerable; *uncountable* iff it is neither finite nor denumerable (so an uncountable set is an infinite set).

0 counts as a finite number, so the empty set is a finite set.

The existence of an uncountable set will be proved in §11, assuming the Power Set Axiom (§11.1). (The existence of some other uncountable sets is proved in Appendix 1, without appeal to the Power Set Axiom.)

A denumerable infinity is the smallest sort of infinity: no infinite set has a smaller cardinal number than a denumerable set. So $\aleph_0$ [aleph nought], which is, by definition, the cardinal number of the set of natural numbers, is the smallest transfinite cardinal number. (The cardinal numbers of infinite sets are known as transfinite cardinals.)

It is a characteristic property[1] of any infinite set that there is a 1–1 correspondence between it and at least one of its own proper subsets. For example, there is a 1–1 correspondence between the set of natural numbers and the set of squares of natural numbers, which is a proper subset of the set of natural numbers:

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 4 & 9 & 16 & 25 & 36 & 49 & \dots \end{array}$$

This particular correspondence was known to Galileo (1638). The more or less clear recognition that an infinite set can have a 1–1 correspondence with (some of) its own proper subsets seems to go back at least to the Stoics (Chrysippus?) in the third century B.C. For references, see e.g. Kleene (1967, p. 176, fn. 121).

No finite set can have a 1–1 correspondence with any of its own proper subsets. Accordingly C. S. Peirce in 1885 [*Collected Papers*, iii, §402] took the non-existence of such a correspondence as a defining property of finite sets, while Dedekind took its existence as a defining property of infinite ones. (Dedekind published his definition in 1888. He says that he submitted it to

[1] Strictly this holds only under the assumption of the Axiom of Choice, an axiom that commends itself both because of its intuitive plausibility and because it 'has so many important applications in practically all branches of mathematics that not to accept it would seem to be a wilful hobbling of the practicing mathematician' (Mendelson, 1964, p. 201). [For the Axiom of Choice, see §59.]

Cantor in September 1882 and to Schwarz and Weber several years earlier: cf. Dedekind (1887, fn. to §64).)

EXERCISES

1. Show that the following sets are denumerable:
   (*a*) The set of positive integers, {1, 2, 3, 4, . . .}.
   (*b*) The set of even numbers, {2, 4, 6, 8, . . .}.
   (*c*) The set of odd numbers, {1, 3, 5, 7, . . .}.
   (*d*) The set of integers, {. . . , −3, −2, −1, 0, 1, 2, 3, . . .}.
   (*e*) The set of positive rational numbers.[1]
   (*f*) The set of rational numbers.
2. Show how each of the sets in the last exercise can be put in 1–1 correspondence with one of its own proper subsets.
3. Show that the set of squares of an infinite chessboard of one-inch squares is denumerable.
4. Show that $\aleph_0 - 1 = \aleph_0$ and that $\aleph_0 + 1 = \aleph_0$, and that therefore $\aleph_0 \pm n = \aleph_0$, where n is a natural number.
5. Show that $\aleph_0 . \aleph_0 = \aleph_0$.

ANSWERS

1. (*a*) Here is the start of a 1–1 correspondence between the set of natural numbers and the set of positive integers:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \end{array}$$

In order to prove the existence of a 1–1 correspondence between a set A and the set of natural numbers, it is enough to show how to generate an infinite sequence of members of A that will contain, without repetitions, all the members of A and nothing that is not a member of A. So for the remaining proofs we simply write down the first few terms of appropriate rule-generated sequences, with occasional explanations. [For more on sequences, see §12.]

(*b*) 2, 4, 6, 8, . . .
(*c*) 1, 3, 5, 7, . . .

[1] A *rational number* is a number that can be expressed as a *ratio* of two integers, $\frac{a}{b}$, where $b \neq 0$: e.g. $\frac{1}{2}$, $\frac{22}{17}$, -15 $[=\frac{-15}{1}]$.

(*d*) 0, 1, -1, 2, -2, 3, -3, . . . [Here we abandon any attempt to take the members of the set in order of magnitude.]

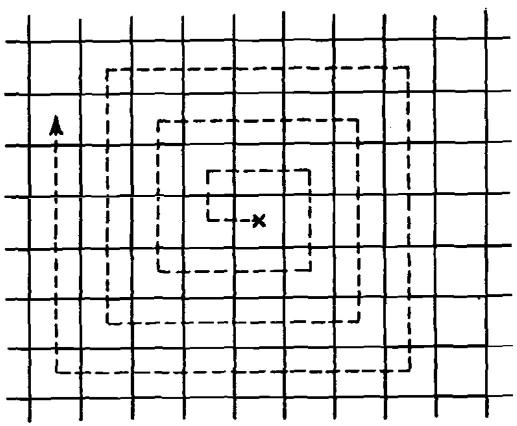
(*e*) $\frac{1}{1}$, $\frac{1}{2}$, $\frac{2}{1}$, $\frac{1}{3}$, [$\frac{2}{2}$,] $\frac{3}{1}$, $\frac{1}{4}$, $\frac{2}{3}$, $\frac{3}{2}$, $\frac{4}{1}$, $\frac{1}{5}$, [$\frac{2}{4}$,] [$\frac{3}{3}$,] [$\frac{4}{2}$,] $\frac{5}{1}$, $\frac{1}{6}$, . . .
(We write down first every positive rational whose numerator and denominator add up to 2. There is only one, viz. $\frac{1}{1}$. Then we write down every one whose numerator and denominator add up to 3, putting numbers with smaller numerators before numbers with larger ones. Then we do the same for rationals whose numerator and denominator add up to 4, and so on. Each time in this process that we come across a number that has already appeared in the sequence, we omit it: so the numbers in square brackets are not in the sequence; they were put in simply to show how the sequence is obtained.)

(*f*) 0, 1, -1, $\frac{1}{2}$, $-\frac{1}{2}$, 2, -2, $\frac{1}{3}$, $-\frac{1}{3}$, 3, -3, $\frac{1}{4}$, $-\frac{1}{4}$, $\frac{2}{3}$, $-\frac{2}{3}$, $\frac{3}{2}$, $-\frac{3}{2}$, 4, -4, . . .
(The sequence for (*e*) expanded by inserting after each term the corresponding negative number, and adding 0 at the beginning.)

2. In each case simply pair off the first term in the sequence given in the answer to exercise 1 with the second term, the second with the third, and so on. E.g. in case (*a*):

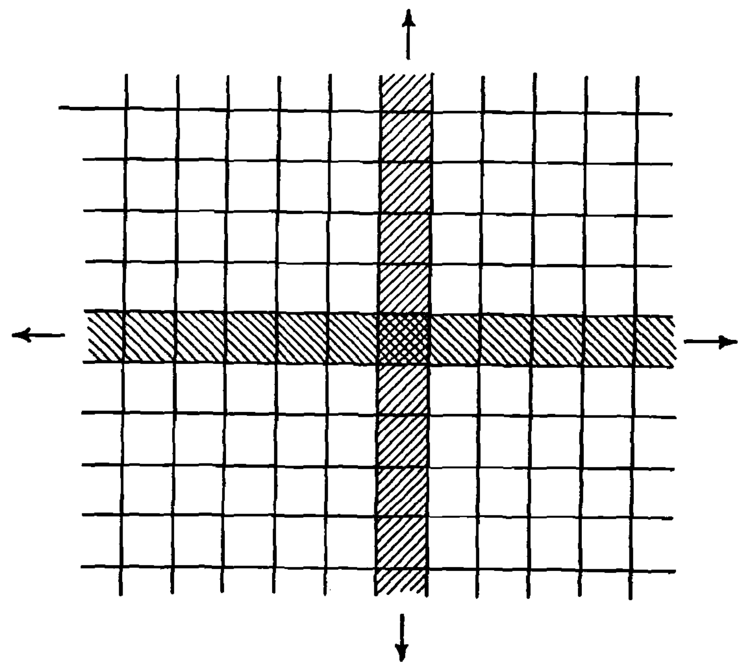
$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & \dots \end{array}$$

3. They can be enumerated by starting from an arbitrary square and following the spiral path indicated in the following figure:



4.. Consider the answer to exercise 2.

5. Consider the answer to exercise 3. The number of squares on the infinite chessboard is the product of the number of squares along some arbitrary line on the board and the number of squares along a line at right-angles, which is the product of $\aleph_0$ and $\aleph_0$:



11 Proof of the uncountability of the set of all subsets of the set of natural numbers

A set A is a *subset* of a set B [written: $A \subseteq B$] iff there is no member of A that is not a member of B. The empty set, $\emptyset$, is a subset of every set, since for any set C there is no member of $\emptyset$ that is not a member of C, simply because there is no member of $\emptyset$. Also, every set is a subset of itself. (By contrast, no set is a *proper* subset of itself.)

The set of all subsets of a set A is known as the *power set* of A.

It seems intuitively obvious that the set of natural numbers *has* its power set, i.e. that there *is* a set that has for its members all subsets of the set of natural numbers and nothing else. But we have not proved this. It is usual to appeal here to a more general axiom, viz.

11.1 (*The Power Set Axiom*) *For any set there exists its power set*

This axiom cannot be taken to be certainly true, but it looks very plausible, and we shall assume it from now on.

11.2 *The set of all subsets of the set of natural numbers is uncountable*

Proof. Clearly the set of all subsets of the set of natural numbers is not finite. For to each natural number there corresponds the set that has that natural number as its sole member; there are denumerably many such sets, and each is a subset of the set of natural numbers.

Now suppose that someone claims that he has found a 1–1 correspondence between the set of natural numbers and the set of all subsets of the set of natural numbers. We shall show how any such claim can be refuted.

Suppose the alleged 1–1 correspondence starts off like this:

	0	1	2	3	4	5	6	7	8	...
0 ↔ the set of all natural numbers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	...
1 ↔ the empty set	No	No	No	No	No	No	No	No	No	...
2 ↔ the set of all even numbers	No	No	Yes	No	Yes	No	Yes	No	Yes	...
3 ↔ the set of all odd numbers	No	Yes	No	Yes	No	Yes	No	Yes	No	...
4 ↔ the set of all prime numbers	No	No	Yes	Yes	No	Yes	No	Yes	No	...
5 ↔ the set of all squares of n.n.s.	Yes	Yes	No	No	Yes	No	No	No	No	...
6 ↔ the set of all cubes of n.n.s.	Yes	Yes	No	No	No	No	No	No	Yes	...
. . .	.	.	.	.	.	.	.	.	.	

[On the right-hand side of the table we write 'Yes' under a number if it is a member of the set mentioned at its left, and 'No' if it is not.]

We use *Cantor's diagonal argument* to show that our imaginary claimant's supposed 1–1 correspondence is not a 1–1 correspondence after all. For we can define a subset of the set of natural numbers that does not occur in his pairing, viz. the subset defined by starting at the top left-hand corner of the array

on the right and going down the diagonal changing each 'Yes' to 'No' and each 'No' to 'Yes', thus:

0	1	2	3	4	5	6	7	8	...
No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	...
No	Yes	No	No	No	No	No	No	No	...
No	No	No	No	Yes	No	Yes	No	Yes	...
No	Yes	No	No	No	Yes	No	Yes	No	...
No	No	Yes	Yes	Yes	Yes	No	Yes	No	...
Yes	Yes	No	No	Yes	Yes	No	No	No	...
Yes	Yes	No	No	No	No	Yes	No	Yes	...
.	.	.	.	.	.	.	.	.	

Going down the diagonal we see that among the members of this subset will be the numbers 1, 4, 5 and 6. The set so defined is a subset of the set of natural numbers that differs from each set in the original pairing in at least one member.

This was only a particular example. It is clear, however, that for *any* alleged 1–1 pairing of the subsets of the set of natural numbers with the natural numbers a similar diagonal argument would yield a subset of the set of natural numbers *not* in the pairing. So we have quite generally:

> There is no 1–1 correspondence between the set of natural numbers and the set of all subsets of the set of natural numbers.

So the set of all subsets of the set of natural numbers is not denumerable. We have seen that it is not finite. So it is uncountable. Q.E.D.

The reader may for a moment think that we could get round the diagonal argument by adding the new subset at the top of the list, pairing it off with the number 0, and shifting each of the other subsets down a place. This would not help. For a fresh application of the diagonal argument to the new list would produce another subset not in the list. And so on, without end. Any attempt to pair off the subsets of the set of natural numbers with the natural numbers leaves out not just one but infinitely many subsets (indeed, uncountably many: cf. 13.6 below).

There is a 1–1 correspondence between the set of natural numbers and the set whose members are {0}, {1}, {2}, {3} and so on. This last set is a proper subset of the set of all subsets of the set of natural numbers. So we have: There is a 1–1 correspondence between the set of natural numbers and a proper subset of the set of all subsets of the set of natural numbers, but no 1–1 correspondence between the set of natural numbers and the set of all subsets of the set of natural numbers. Therefore *the set of all subsets of the set of natural numbers has a greater cardinal number than the set of natural numbers* (cf. the definition of *having a greater cardinal number than* in §9).

By using a general and abstract form of the diagonal argument, Cantor showed that *the power set of a set always has a greater cardinal number than the set itself.* This is known as *Cantor's Theorem.* A proof of it is given in small print below; below that there is an example that may help towards understanding it.

Given the existence of any infinite set whatever, the truth of the Power Set Axiom, and Cantor's Theorem, it follows that there is an unending succession of different and ever greater infinite sets – 'the paradise that Cantor created for us' (Hilbert, 1925).

The following proof of Cantor's Theorem might be skipped at a first reading:

Cantor's Theorem: The power set of a set has a greater cardinal number than the set itself

Proof

1. Let A be any set. Consider *any* pairing-off of members of A with members of the power set of A that assigns to each distinct member of A a distinct subset of A. Let S be the set of all members of A that are not members of the subset assigned to them. S is a subset of A. But S is not assigned to any member of A. For suppose it were assigned to a member, say x, of A. Then x would be a member of S if and only if it were not a member of S. This is a contradiction. So any pairing-off of distinct members of A with distinct members of the power set of A leaves some member of the power set unpaired. So there is no 1–1 correspondence between A and its power set.

2. It remains to show that there is a 1–1 correspondence between A and a proper subset of the power set of A. This is easy. Take as the proper subset the set of all sets that have as their sole member a member of A.

Example. Let A be the set {1, 2, 3}. Then the power set of A is the set

$$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \emptyset\}.$$

A has three members. The power set of A has eight members. There is no 1–1 correspondence between A and its power set; but there is a 1–1 correspondence between A and a proper subset of its power set: take, e.g., the subset {{1}, {2}, {3}}.

Cantor's Theorem is more or less obvious for finite sets. What Cantor did was to show that it held for infinite sets as well.

12 Sequences. Enumerations. Effective enumerations

In mathematics a sequence is a function of a certain sort. But we shall use the word in an intuitive way. A *sequence* is an ordering of objects, called the *terms* of the sequence. The same thing may occur more than once in the ordering; e.g. $\langle 1, 2, 3, 1\rangle$ is a sequence of four terms with the number 1 occurring as the first term and as the fourth term. A sequence s is the same as a sequence s' iff s and s' have exactly the same number of terms and the first term of s is the same as the first term of s', the second term of s is exactly the same as the second term of s', and so on. So, e.g., $\langle 1, 2, 1\rangle \neq \langle 1, 2\rangle$, and $\langle 1, 2, 3\rangle \neq \langle 3, 2, 1\rangle$.

A sequence of n terms is also known as an n-tuple.

A sequence may be finite or infinite. A denumerable sequence is a sequence with denumerably many terms, and may be symbolised by giving the first few terms and then putting dots; e.g. $\langle 1, 2, 3, \ldots\rangle$ and $\langle 1, 1, 1, \ldots\rangle$ and $\langle 1, 2, 1, 2, 1, 2, \ldots\rangle$ and $\langle 4, 9, 13, 5, 5, 5, \ldots, 5, \ldots\rangle$ are denumerable sequences. In the last one every term from the fourth on is the number 5.

In the examples given above all the terms in all the sequences are numbers. But just as there are sets with things other than numbers as members, so there are sequences with things other than numbers as terms.

An *enumeration* of a set A is a finite or denumerable sequence of which every member of A is a term and every term is a member of A. For example, the sequences $\langle 3, 1, 2\rangle$ and $\langle 1, 2, 3, 1\rangle$ are both enumerations of the set $\{1, 2, 3\}$.

An *effective enumeration* is an enumeration which is finite or for which there is an effective method for telling what the *n*th term is, for each positive integer n. (Every finite enumeration is effective, because there is an effective method – remember it need not be known to anyone – for enumerating the members of any finite set.)

EXERCISES

1. 'If there is an enumeration with repetitions of a set A, then there is an enumeration without repetitions of the set A.' True or false?
2. (*a*) If in exercise 1 above 'effective enumeration' was substituted for 'enumeration' both times, would the resulting statement be true?
   (*b*) If it would be, describe a method for calculating the *n*th term of the new enumeration. If not, say why not.

ANSWERS

1. True. Simply delete repetitions.
2. (*a*) Yes.
   (*b*) Calculate the first term of the old sequence. Put it down as the first term of the new. Calculate the second term of the old. Put it down as the second term of the new *unless* it is identical with an earlier term in the new sequence. After each addition to the new sequence, check how many terms you have put in it. Sooner or later you are bound to come to the *n*th term of the new sequence (if there is an *n*th term), and you will know it to be the *n*th term.

13 Some theorems about infinite sets

13.1 *Any subset of a countable set is countable*

Proof. Let A be an arbitrary countable set and B be an arbitrary subset of A.

(*a*) If A is finite, then obviously B is finite and so countable.

(*b*) If A is denumerable, then (by definition) there is a 1–1 correspondence between it and the set of natural numbers, and so there is a denumerable sequence that enumerates A without repetitions. Delete from this sequence all terms that are not members of B, and the result is a finite or denumerable sequence that enumerates B without repetitions. So B is countable.

The *union* of two sets A and B [written: $A \cup B$] is the set that has for its members all the members of A and all the members of B.

13.2 *The union of a denumerable set and a finite set is denumerable*

Proof. Let A be any denumerable set and B be any finite set. Let B have exactly n members. Then the members of B can be paired off with the first n natural numbers (viz. $0, 1, \ldots, n-1$), and the members of A with the natural numbers from n on, first deleting any members of A that are also members of B.

13.3 *The union of a denumerable set and a denumerable set is a denumerable set*

Proof. Take members from each set alternately, deleting any repetitions. Example: Let A be the set of prime numbers, $\{2, 3, 5, 7, 11, 13, 17, \ldots\}$, and B be the set of odd numbers, $\{1, 3, 5, 7, 9, 11, 13, 15, \ldots\}$. Then the union of A and B can be enumerated in the following way:

$$\langle 2, 1, 3, \cancel{3}, 5, \cancel{5}, 7, \cancel{7}, 11, 9, 13, \cancel{11}, 17, \cancel{13}, 19, 15, \ldots\rangle$$

Given the proofs of 13.2 and 13.3, the proofs of the next two theorems are easy, and they are left to the reader:

13.4 *The union of a countable set and a finite set is countable*

13.5 *The union of a countable set and a countable set is countable*

A – B is the set that has for its members all those members of A that are not members of B.

13.6 *The removal from an uncountable set of countably many members leaves an uncountable set remaining*

Proof

(*a*) [The case where finitely many members are subtracted.]

Let A be any uncountable set, and B be any finite set of members of A. Suppose A – B were countable. Then by 13.4 the union of A – B with B would be countable. But the union of A – B with B is A itself, and by hypothesis A is uncountable. So A – B must be uncountable.

(*b*) [The case where denumerably many members are subtracted.] Let A be any uncountable set, and B be any denumerable set of members of A. Suppose A – B were countable. Then by 13.5 the union of A – B with B would be countable. But the union of A – B with B is A itself, and by hypothesis A is uncountable. So A – B must be uncountable.

14 Informal proof of the incompleteness of any finitary formal system of the full theory of the natural numbers

By 'finitary formal system' we shall mean a formal system with a finite or denumerable alphabet of symbols, wffs only finitely long, and rules of inference (if any) using only finitely many premisses. (In recent years logicians have worked on systems with uncountable alphabets, with infinitely long wffs, with rules of inference having infinitely many premisses, etc.)

A formal system of the full theory of the natural numbers is a formal system (some or all of) whose theorems can be interpreted as expressing truths of the full theory of the natural numbers. Such a system will be said to be *incomplete* if there are truths of the full theory of the natural numbers that are not theorems of the system [i.e. truths that are not expressed by any theorem of the system, on its intended interpretation].

The full theory of the natural numbers is here taken to include, among other things, all truths to the effect that a particular natural number is a member of some particular set of natural numbers. Remember that a set A is identical with a set B if and only if A has exactly the same members as B, and that this identity is not affected by quite radical differences in the specifications of A and B. [E.g. if the only number I am now thinking of is the number 17, then the set of numbers-I-am-now-thinking-of is identical with the set whose sole member is the number 17.]

14.1 *Any finitary formal system has only countably many wffs and therefore only countably many theorems*

Proof

Stage 1. A denumerable alphabet has no greater powers of expression than a finite alphabet, or even than a two-symbol alphabet. For suppose we have a denumerable alphabet with symbols a_1, a_2, a_3, . . . Then there is a 1–1 correspondence between it and the set {10, 100, 1000, . . .} of strings of symbols from the alphabet whose only symbols are 0 and 1; and these strings from the finite alphabet can be used to do whatever can be done with the symbols from the denumerable alphabet.

Stage 2. The set of distinct finitely long wffs that can be got from a finite alphabet is countable. *Proof.* Replace each symbol of the alphabet by a '1' followed by a string of one or more zeros, as in Stage 1. Each wff then becomes a numeral composed exclusively of ones and zeros and beginning with a one.[1] To each distinct wff there corresponds a distinct numeral. Each of these distinct numerals stands for a distinct natural number. There are only denumerably many natural numbers, so there are at most denumerably many wffs. So the set of wffs of any finitary formal system is countable. In any formal system every theorem is a wff. So the set of theorems of any finitary formal system is also countable.

14.2 *There are uncountably many truths of the full theory of the natural numbers*

Proof. To each of the uncountably many subsets of the set of natural numbers [see 11.2] there corresponds a distinct truth of the full theory of the natural numbers, viz. the truth that zero[2] is (or is not, as the case may be) a member of that subset. Therefore there are at least as many truths of the full theory of the

[1] E.g. suppose that the alphabet consists of the four symbols

$$p \quad \supset \quad (\quad)$$

Replace these in any wff by

$$10 \quad 100 \quad 1000 \quad 10000$$

respectively. Then (e.g.) the wff

$$(p \supset p)$$

becomes

$$1000101001010000.$$

[2] There is nothing special about zero here; any other natural number would do.

natural numbers as there are subsets of the set of natural numbers, and so there are uncountably many such truths.

14.3 *Any finitary formal system of the full theory of the natural numbers is incomplete, in the sense explained* [*see paragraph 2 of this section*]

Proof. By 14.1 any finitary formal system of the full theory of the natural numbers has only countably many (formal) theorems. On the intended interpretation each formal theorem will have just one definite unambiguous meaning and, if it is true on the intended interpretation, it will express just one truth. For simplicity's sake we shall assume that on the intended interpretation each distinct theorem expresses a distinct truth of the full theory of the natural numbers. [There are other possibilities: e.g. two distinct theorems might express the same truth, or some theorems might express falsehoods, or some might express truths that were not truths of the full theory of the natural numbers. A full proof would cover these possibilities, using the theorem 13.1 that any subset of a countable set is countable.] Also for simplicity's sake we shall identify interpreted theorems with the truths they express. Then we get: Any finitary formal system of the full theory of the natural numbers will include among its interpreted theorems only countably many truths of the full theory of the natural numbers. But by 14.2 there are uncountably many such truths. So by 13.6 any finitary formal system will fail to include among its interpreted theorems uncountably many such truths. Therefore any finitary formal system of the full theory of the natural numbers is incomplete.

Q.E.D.

Appendix 1: Intuitive theory of infinite sets and transfinite cardinal numbers

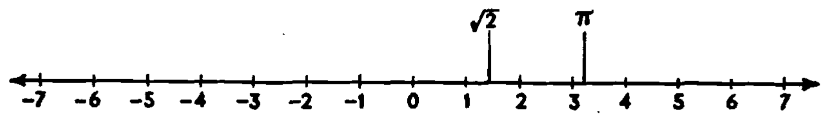
Proofs informal throughout. Some theorems left unproved. The material is not essential to the rest of the book.

Real numbers. Consider an infinite straight line marked off in units, as in the figure on page 31. To each rational number (i.e., number that can be expressed as a ratio of two integers) there corresponds a point on the line. But there are many points

on the line to which no rational number corresponds, e.g. the points marked $\sqrt{2}$ and π. Neither $\sqrt{2}$ nor π can be expressed as a ratio of two integers, and yet $\sqrt{2}$ and π correspond to points on the line. Numbers that correspond in this way to points on a line but that are not expressible as ratios of two integers are known as *irrational numbers*. The set of *real numbers* is the union of the set of rational numbers and the set of irrational numbers, and it can be thought of as the set of numbers corresponding to the points on an infinite line.

The (real) *continuum* is the set of real numbers, in their natural order.

The *linear continuum* is the set of all points on an infinite line.



Theorem A1. *The cardinal number of the* (*real*) *continuum is the same as the cardinal number of the linear continuum*

So from now on we may speak simply of 'the cardinal number of the continuum'.

Notation. The cardinal number of the continuum is $\mathfrak{c}$ [the lower-case German 'c']

We shall make a good deal of use of the following two theorems, which we state without proof:

Theorem A2. *The addition to, or subtraction from, an infinite set of finitely many things yields a set with the same cardinal number as the original*

This is an extension of 13.2, which covered only denumerable sets. A2 covers uncountable sets as well, and its proof involves the Axiom of Choice, which is beyond the scope of this book.

Theorem A3. *The subtraction of a denumerable set from an uncountable set leaves a set with the same cardinal number as the uncountable set*

Theorem A4. *The set of real numbers is uncountable* [Cantor, 1873]

Proof. Three stages:

1. Every real number can be uniquely represented by a non-terminating decimal numeral. Those that it would be natural to represent by terminating decimals are to be represented by non-terminating equivalents: e.g. the real number $3\frac{1}{4}$ by 3·24999999 . . ., not by 3·25; the number 1 by 0·99999 . . . .

2. We concentrate first on the set of real numbers greater than 0 and less than or equal to 1. This set is clearly not finite. Now suppose that each distinct natural number is paired off with a distinct real number, represented by a non-terminating decimal. It is easy to show by a diagonal argument that any such pairing leaves some real number unpaired. For any such pairing will begin like this:

$$\begin{array}{ll} 0 & 0\cdot d\,d\,d\,d\,d\,d\,d\ldots \\ 1 & 0\cdot d\,d\,d\,d\,d\,d\,d\ldots \\ 2 & 0\cdot d\,d\,d\,d\,d\,d\,d\ldots \end{array}$$

where each d is some digit or other (i.e. numeral from 0 to 9), possibly all the same, possibly not. And it is clear that any numeral got by starting off with a zero, then a decimal point, then a digit different from the first d on the diagonal (but not 0), then a digit different from the second d on the diagonal (but not 0), and so on, will represent a real number greater than 0 and less than or equal to 1 that is not paired off with any natural number. So the set of real numbers greater than 0 and less than or equal to 1 is uncountable.

3. By Theorem A2 the set of real numbers greater than 0 and less than or equal to 1 has the same cardinal number as the set of real numbers greater than 0 and less than 1, which has the same cardinal number as the set of points, other than the end-points, on a line one unit long. The figure at the bottom of page 36 shows that there is a 1-1 correspondence between this last set and the set of points on an infinite line, and hence between it and the set of all real numbers. So the set of real numbers is uncountable.

Q.E.D.

Since the set of natural numbers is a proper subset of the set of real numbers, we have as a corollary of Theorem A4:

Theorem A5. $c > \aleph_0$

Theorem A6. Each of the following sets has the cardinal number of the continuum:

A. The set of real numbers x such that $0 \leqslant x \leqslant 1$
B. The set of real numbers x such that $0 < x \leqslant 1$
C. The set of real numbers x such that $0 \leqslant x < 1$
D. The set of real numbers x such that $0 < x < 1$
E. The set of non-negative real numbers

Proof

(Sets A, B, C, D) A is B with one extra thing, viz. the number 0. C is A with one member less, viz. the number 1. D is C with one member less, viz. the number 0. We have already proved that B has the cardinal number of the continuum [in the course of proving Theorem A4]. So A has, by Theorem A2. So C has, by Theorem A2 applied to the result for A. So D has, by A2 applied to the result for C.

(Set E) E has D as a proper subset. So if there is no 1–1 correspondence between E and D, $\overline{\overline{D}} < \overline{\overline{E}}$ (by the definition of $<$ for transfinite cardinals); and if there *is* a 1–1 correspondence, $\overline{\overline{D}} = \overline{\overline{E}}$. But either there is or there is not a 1–1 correspondence between E and D. So $\overline{\overline{D}} \leqslant \overline{\overline{E}}$. Similarly $\overline{\overline{E}} \leqslant \overline{\overline{R}}$, where R is the set of all real numbers. But $\overline{\overline{D}} = \overline{\overline{R}} = c$. So we have:

$$c = \overline{\overline{D}} \leqslant \overline{\overline{E}} \leqslant \overline{\overline{R}} = c.$$

So $$c \leqslant \overline{\overline{E}} \leqslant c.$$

So $$\overline{\overline{E}} = c.$$

(A geometrical proof of the same result is given below: Theorem A8*H*.)

Theorem A7. *The set of all subsets of the set of natural numbers (the power set of the set of natural numbers) has the cardinal number of the continuum*

Proof

Every set of natural numbers can be uniquely represented by a denumerable string of 'Yes'es and 'No's, as in the tables in §11. For example, the string that begins with

Yes Yes No No Yes No

and goes on with nothing but 'No's represents the set {0, 1, 4}. So there is a 1–1 correspondence between the set of all subsets of the set of natural numbers and the set of denumerable strings of 'Yes'es and 'No's. And there is a 1–1 correspondence between this last set and the set of denumerable strings of '1's and '0's. For example, the string of 'Yes'es and 'No's mentioned above corresponds to the string that begins with

$$1\,1\,0\,0\,1\,0$$

and goes on with nothing but '0's.

Put the binary equivalent of a decimal point in front of a denumerable string of '1's and '0's and you get an expression that, in the binary system, denotes a real number $\geqslant 0$ and $\leqslant 1$. For example, the expression that starts off with

$$\cdot 1\,1\,0\,0\,1\,0$$

and goes on with nothing but '0's denotes the real number

$$\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{0}{8}+\tfrac{0}{16}+\tfrac{1}{32}+\tfrac{0}{64}+0$$

i.e. the real number $\frac{25}{32}$. Each denumerable string of '1's and '0's, preceded by a binary point, represents a real number $\geqslant 0$ and $\leqslant 1$, and each real number $\geqslant 0$ and $\leqslant 1$ is represented by some string. But it is not a 1–1 correspondence, since some numbers are represented by more than one string. For example, the number $\frac{1}{4}$ is represented both by

$$\cdot 0\,1\,0\,0\,0\,0\,0\,\ldots$$

and by

$$\cdot 0\,0\,1\,1\,1\,1\,1\,\ldots$$

However, if we took away from the set of strings the set of all strings that from some point on consist wholly of '0's, there *would* be a 1–1 correspondence between the set of strings that was left and the set of real numbers >0 and $\leqslant 1$. But the set of all denumerable strings of '1's and '0's that from some point on consist wholly of '0's can be *enumerated* (we leave this to the reader as an exercise). And the subtraction of a denumerable set from an uncountable set leaves a set with the same cardinality as the uncountable set [Theorem A3]. So we have, using '$\simeq$' for 'has a 1–1 correspondence with':

> The set of subsets of the set of natural numbers $\simeq$ The set of denumerable strings of 'Yes'es and 'No's $\simeq$ The set of denumerable strings of '1's and '0's $\simeq$ The set of denumerable strings of '1's and '0's other than those strings that from some point on consist wholly of '0's $\simeq$ The set of real numbers >0 and $\leqslant 1$ $\simeq$ The set of real numbers.

So the set of subsets of the set of natural numbers has the cardinal number of the continuum.

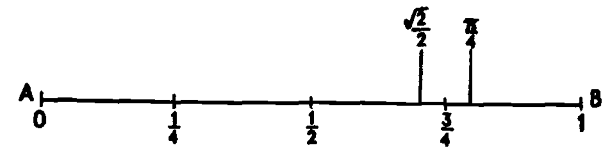
Q.E.D.

Theorem A8. *Each of the following sets has the cardinal number of the continuum*:

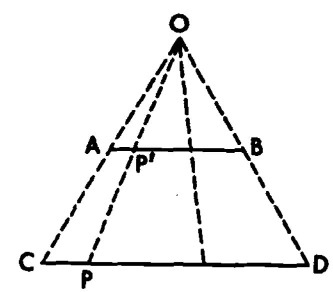
F. The set of points on a line one arbitrary unit long
G. The set of points on a line two arbitrary units long
H. The set of points on the (infinite) half-line
I. The set of points on the (infinite) line

Proof

F. Use Theorem A6*A* and the familiar 1–1 correspondence illustrated by the figure (let *AB* be one arbitrary unit long):

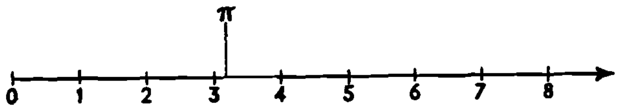


G. One proof is by letting the line *AB* in the proof for *F* be two units long. More intuitive is the following geometrical proof:

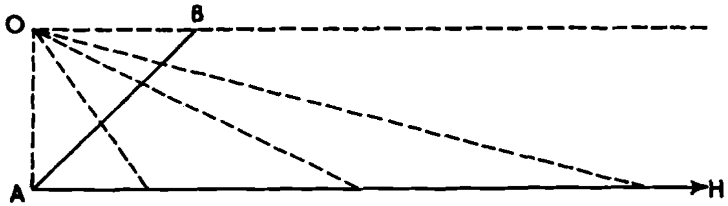


To each point on the two-unit-long line *CD* there corresponds a unique point on the one-unit-long line *AB*, and vice versa. For example, to the point *P* on *CD* there corresponds the unique point *P′* on *AB*, and vice versa.

H. One proof is by the familiar 1–1 correspondence between the set of points on the (infinite) half-line and the set of non-negative real numbers (already shown to have the cardinal $\mathfrak{c}$: Theorem A6*E*):

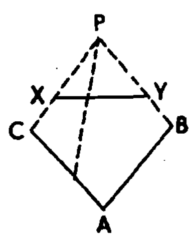


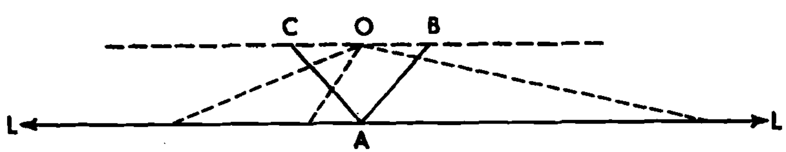
Another is geometrical:



There is a 1–1 correspondence between the points on the infinite half-line AH and the points on AB other than B (no point on AH corresponds to the point B, for OB is parallel to AH). By Theorem A2 the number of points on AB is the same as the number of points on AB other than B. So there is the same number of points on the infinite half-line as on a finite line.

I. Proved already (Theorem A1). It could also be proved by the following two figures, with the help of Theorem A8*F*, e.g., [let XY be one unit long] and A2 [the number of points on the angled line CAB is the same as the number of points on CAB other than the points B and C]:





There is the same number of points on the one-unit-long line XY as there is on the angled line CAB, and the same number on CAB as on L [using Theorem A2].

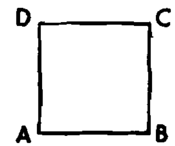
Theorem A9. *Each of the following sets has the cardinal number of the continuum:*

J. The set of all points of a square [Cantor, 1877]
K. The set of all points in a cube
L. The set of all points in an infinite plane
M. The set of all points in infinite three-dimensional Euclidean space

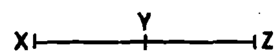
Proof

J. Four stages:

1. Let $ABCD$ be a square with sides one arbitrary unit long:



We concentrate on the points of the square other than those on the sides AB or AD. If we can show that the set of all remaining points of the square has the cardinal number $\mathfrak{c}$, then the union of that set with the set of all points on AB will also have the cardinal number $\mathfrak{c}$, and the union of this last set with the set of all points on AD will also have the cardinal number $\mathfrak{c}$. For the union of two sets each having the cardinal number of the continuum has the cardinal number of the continuum. [As an illustration, consider a line two units long:

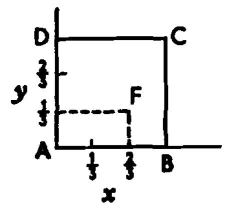


The set of points on XY has the cardinal number $\mathfrak{c}$. The set of points on YZ has the cardinal number $\mathfrak{c}$. The union of these sets is the set of all points on XZ, which also has the cardinal number $\mathfrak{c}$. So $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$.]

In 2, 3 and most of 4 below we shall write, for brevity, 'point of the square' meaning 'point of the square not on AB or AD'.

2. The first basic idea of the proof is that any point of the square $ABCD$ corresponds to a pair of non-terminating decimals

denoting real numbers >0 and $\leqslant 1$, viz. the numbers that are the Cartesian co-ordinates of the point when for axes we choose *AB* and *AD*:



In our illustration the co-ordinates of F are $x = 0{\cdot}6666\ldots$, $y = 0{\cdot}3333\ldots$

3. The second basic idea is to reduce these two non-terminating decimals to a single non-terminating decimal by interlacing their digits. In our illustration the new decimal will be 0·6363636363 . . . So to each distinct point of the square there corresponds a distinct non-terminating decimal denoting a real number >0 and $\leqslant 1$.

4. But there are some non-terminating decimals which do not split up into two non-terminating decimals, viz. all those decimals in which the digit 0 occurs alternately and infinitely many times from some point on: e.g. 0·6360606060606060 . . ., which splits up into 0·6666 . . . and 0·3. Terminating decimals were not allowed in the correspondence we set up in Stage 2. So we have not yet got a 1–1 correspondence between the points of the square and the non-terminating decimals denoting real numbers >0 and $\leqslant 1$: to each distinct point of the square there corresponds a distinct non-terminating decimal denoting a real number >0 and $\leqslant 1$, but not vice versa. To deal with this complication we need the third basic idea of the proof. In getting back from the single decimal to the pair of decimals we take single digits alternately as before *unless* the digit is a zero: if it is a zero, we take the *group* of digits that begins with the zero and ends with the first digit that is not a zero. So

0·6|3|6|06|06|06|06| . . .

splits up into

0·660606 . . .

and

0·30606 . . .

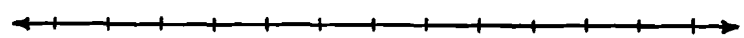
So terminating decimals are avoided and we get our 1–1 correspondence between the set of points of the square (other than the points on *AB* or *AD*) and the set of all non-terminating decimals denoting real numbers >0 and $\leqslant 1$. We know already that this last set has the cardinal number $\mathfrak{c}$. In view of the remarks in Stage 1, it follows that the set of *all* points of the square has the cardinal number $\mathfrak{c}$.

Q.E.D.

(For remarks on the trouble Cantor had in getting this result, see Fraenkel (1961, p. 103).)

K. As for *J*, but interlacing *three* non-terminating decimals, the decimals denoting the co-ordinates of the point in the (three-dimensional) cube.

L. Think of the plane as the infinite chessboard of §10, exercise 3, which we there showed to have only denumerably many one-inch squares. We have already seen that the union of two sets each of which has the cardinal number $\mathfrak{c}$ has the cardinal number $\mathfrak{c}$ [Proof of Theorem A9*J*, Stage 1]. So the union of n sets each of which has the cardinal number $\mathfrak{c}$ will also have the cardinal number $\mathfrak{c}$. But the same is true for the union of denumerably many sets each of which has the cardinal number $\mathfrak{c}$. [As an illustration, consider the infinite line divided into unit segments:



There are denumerably many segments each having $\mathfrak{c}$ points. So the line has $\aleph_0 . \mathfrak{c}$ points. So $\aleph_0 . \mathfrak{c} = \mathfrak{c}$.] The plane consists of the denumerably many one-inch squares, and the number of points in it is therefore $\aleph_0 . \mathfrak{c}$, which is $\mathfrak{c}$. So there is the same number of points in a plane as there is on (e.g.) a one-inch line.

M. As for *L*, but this time with one-inch cubes, and instead of a simple two-dimensional spiral path we take a more complicated three-dimensional path.

Later proofs can be shortened by using the following theorems of the arithmetic of transfinite cardinals:

Theorem A10. $\aleph_0 \cdot \aleph_0 = \aleph_0$

Proof. Cf. §10, answer to exercise 5.

Theorem A11. $c = c \cdot c = c^2 = c \cdot c \cdot c = c^3 = \ldots = c^n$, *where n is any positive integer*

Proof. For $c^2 = c$ consider the result A9*J*. [The number of the set of all points in a square is the product of the number of points on one side and the number of points on an adjacent side $= c \cdot c = c$.] For $c^3 = c$ consider A9*K*. And so on.

Theorem A12. *If a set has the finite cardinal number n, then its power set has the finite cardinal number* 2^n

Illustration:

		Members of the set		
		1	2	3
Subsets of the set	1. {1, 2, 3}	Yes	Yes	Yes
	2. {2, 3}	No	Yes	Yes
	3. {1, 3}	Yes	No	Yes
	4. {3}	No	No	Yes
	5. {1, 2}	Yes	Yes	No
	6. {2}	No	Yes	No
	7. {1}	Yes	No	No
	8. The empty set, ∅	No	No	No

$2^3 = 8$.

Theorem A13. (Generalisation of A12 to transfinite cardinals.)[1] *If a set has the transfinite cardinal number* α, *then its power set has the transfinite cardinal number* 2^α

Theorem A14. $2^\alpha > \alpha$, *for each transfinite cardinal number* α

Proof. From Cantor's Theorem (proved in §11) and Theorem A13.

Theorem A15. *The power set of the set of natural numbers has the cardinal number* $2^{\aleph_0}$

Proof. From A13 and the definition of $\aleph_0$.

Theorem A16. $c = 2^{\aleph_0}$

Proof. From A7 and A15.

[1] The justification of Theorem A13 is more complicated than this remark suggests: see, e.g., Fraenkel (1961, chap. II, §7).

Theorem A17. *The set of all points in* $\aleph_0$*-dimensional space has the cardinal number of the continuum*

Proof. The set of all points in three-dimensional space (e.g.) has the number c^3. The set of all points in $\aleph_0$-dimensional space has the number $c^{\aleph_0}$. Then 'with a few strokes of the pen' (Cantor) we get:

$$c^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} \text{ [A16] } = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} \text{ [A10] } = c.$$

Or in other words: The number of points in infinite space of $\aleph_0$ dimensions is the same as the number of points on a line a billionth of an inch long.

Cantor conjectured that there is no cardinal number α such that $\aleph_0 < \alpha < c$. This conjecture is known as

The Continuum Hypothesis. There is no cardinal number greater than $\aleph_0$ *and smaller than* $c[2^{\aleph_0}]$

In 1938 Kurt Gödel showed that the Continuum Hypothesis cannot be disproved from the usual axioms of set theory, and in 1963 Paul Cohen showed that it cannot be proved from them either. The Continuum Hypothesis is thus *independent* of the usual axioms of set theory. (These results are under the hypothesis that the usual axioms of set theory are consistent. So far nobody has proved that they are, but most workers in the field think that they are.)

The Generalised Continuum Hypothesis (which implies the Continuum Hypothesis). *For each transfinite cardinal number* α, *there is no cardinal number greater than* α *and smaller than* 2^α

EXERCISE

Are there sets with cardinal numbers greater than c?

ANSWER

Yes, assuming the Power Set Axiom [i.e. the axiom that for each set there exists its power set]. E.g. the set of all subsets of the set of real numbers has the cardinal number 2^c, which is greater than c. The power set of the power set of the set of natural numbers also has the cardinal number 2^c. The power sets of these sets have the still greater cardinal number, $2^{(2^c)}$, and so on.