# Logic & Set Theory

## Logic

Originated in ancient Greece with Aristotle. Studies the process of making deductions. The most basic form of logic is *propositional logic*, which concerns itself with ways of combining propositions using words such as "and", "or", "if ... then", "not" etc., and rules for deducing new statements from old ones. A more elaborate system of logic is *predicate logic*, which allows propositions that depend on a variable, and can have different truths for different values of the variable. Examples of such predicates are "$x$ is a man" or "$x$ has brown eyes". The power of this type of logic then comes from the introduction of quantifiers "for all $x$" and "there exists some $x$". These allow the use of statements such as "all men have brown eyes", or even "every man has a father." (this uses two quantifiers, and a predicate with two variables.) These sorts of statements are common in everyday life, and even more common throughout mathematics.

In the 1840s, George Boole viewed the propositional logic of truth values as being an algebraic structure. In fact, this algebra also has a numerical interpretation, being equivalent to the usual algebra of addition, and multiplication modulo 2, with an additional operation, which corresponds to subtraction from 1. This algebraic structure permits more general models of truth values with more than just two truth values. This later lead to generalisations of this logic using different axioms, in particular *intuitionistic logic*, where the double-negation axiom is no longer valid, so that proof by contradiction (and important mathematical technique) can no longer be used. This is a natural thing to consider because it eliminates most non-constructive proofs, which can be unsatisfactory, particularly from a computer science point of view.

Logic is based on the idea that mathematics consists of the study of what can be deduced from a fixed set of axioms and rules of deduction. In the late 1800s and early 1900s, mathematicians hoped to find a good set of axioms for mathematics, so that all of mathematics could be reduced to use a fixed set of axioms and logical deductions. Set theory was used as the basis for this construction. Many of the concepts studied in mathematics can be represented in clever ways as sets. A major work in this area is *Principia Mathematica* by Bertrand Russell and Alfred North Whitehead. However, in 1931 Kurt Gödel proved that their objective was impossible — he showed that any logical system which is powerful enough to contain arithmetic must either be incomplete or inconsistent. He also showed that it is not possible for a logical system to prove its own consistency (that is, that it is not possible to both prove and disprove something). This means that the consistency of mathematics must be taken on faith, and there will always be things which are true, but cannot be proved.

Gödel's proof involved coding statements in the logical system as numbers in such a way that statements such as "$n$ encodes a proof of the proposition encoded by $m$" could be expressed as arithmetical statements. Then he was able to construct a statement which effectively said that there was no way to prove it.

Despite this, set theory can still be used as a basis for all the mathematics that is currently studied. New axioms will sometimes be introduced in restricted contexts. The origins of set theory go back before this time: naive set theory had an important tool for mathematics since Aristotle. A lot of this theory was developped by Georg Cantor in the late 1800s, in particular, many of the counterintuitive properties of infinite sets, such as the difference between ordinals and cardinals, and the different infinite cardinalities.

Cardinality is a way to measure the size of a set — we say that two sets *have the same cardinality* if we can pair up elements, one from each set, so that neither set has any elements left over. [Such a pairing is called a *bijection*.] For finite sets, this is a straightforward process, and any attempt to pair up the elements either works or doesn't work, depending whether the sets have the same cardinality. The possible cardinalities of finite sets are the *natural numbers* $0, 1, 2, \ldots$.

For infinite sets, the situation is not straightforward, because it is possible to have elements left over if paired up one way, but not another way — for example, if we try to pair up the natural numbers with themselves (obviously the same cardinality) by pairing 0 with 1, 1 with 2, 2 with 3, etc. then the element 0 of the second set is left over.

We can show that the positive rational numbers have the same cardinality as the natural numbers by arranging them in a grid, and filling in the diagonals. The real numbers, however, do not have the same cardinality. To show this, suppose we produce a pairing of the elements, 0 with $a_0$, 1 with $a_1$, etc. We can construct a real number which is left unpaired as follows: We will choose a number between 0 and 1. In the first decimal place, we will take the first decimal place of $a_0$, and add 2 to it (modulo 10, so that 8 becomes 0 and 9 becomes 1). For the second decimal place, we take the second decimal digit of $a_1$ and add 2 to it, and so on. Now our new number differs from $a_n$ in the $n + 1$th decimal place (possibly also in other places) so it cannot be $a_n$. This applies for any $n$ in the list. Therefore, our new number is not in the list. By a similar argument, we can show that the set of subsets of any set is not of the same cardinality. This demonstrates that there are an infinite number of possible cardinalities for an infinite set.

Another place in which infinite sets differ from finite ones is the distinction between cardinals and ordinals. In mathematics, a cardinal refers to the size of a set, while an ordinal refers to the size of a set with a particular type of ordering on its elements. In the finite case, there is a one-to-one correspondence between these notions, because any two ways to order the elements of a finite set are equivalent. For an infinite set, this is no longer the case. For example, for the set of natural numbers, we could order the elements in the usual way $0, 1, 2, \ldots$, or we could put 0 at the end, $1, 2, 3, \ldots, 0$. These two orders are essentially different — in the first one, each number occurs after only a finite set of other numbers. In the second one, there are an infinite set of numbers before 0. Similarly, we could put 1 at the end of this new order: $2, 3, 4, \ldots, 0, 1$ and this would be another order which is not equivalent. We can even order the set so that all the odd numbers come before all the even numbers, so that there are infinitely many numbers that have infinitely many numbers before them.

Set theory was originally based on the intuition that a set represented any collection of objects with a clear membership rule, and that two sets are the same if and only if they have the same members. The trouble with this naive approach is that it can lead to paradoxes (inconsistent statements). The most well-known example is *Russell's paradox* which considers the set of all sets which are not members of themselves. Russell asked whether this set is a member of itself. If it is, then by definition it should not be, but if it is not, then by definition it should be. Another paradox is *Cantor's paradox* that there is no set of all sets, because if there were, then it must contain all its subsets as members, but Cantor's diagonal argument shows that any set has more subsets than members.

A number of solutions to this paradox have been given, such as Russell's theory of types, where a set is assigned a *type* and is only allowed to contain sets of smaller type. The solution that is most commonly used in mathematics is an axiomatic theory known as *Zermelo-Fraenkel* (ZF) set-theory, which has (among other axioms) an axiom of foundation, which effectively implements the notion of types where the type can be any ordinal, rather than just a finite number.

In addition to the axioms of ZF set theory, most mathematicians use an additional axiom called the *axiom of choice*. This axiom asserts that given any collection of non-empty sets, we can choose one element from each of them. This is clearly true for finite collections, but for infinite collections, it asserts the existence of many sets which cannot be explicitly described. For example, it asserts the existence of a set of real numbers such that every real number differs by a rational number from exactly one of them. It has a number of counterintuitive consequences, including:

- There are sets of numbers with no notion of length.
- It is possible to break a sphere into 5 pieces and rotate the pieces to create two copies of the original sphere. [Banach-Tarski paradox]
- There are two-player games where neither player has a winning strategy (that is, no strategy exists, not just that there is no known winning strategy).

The axiom of choice is different in character from other axioms, because it asserts the existence of sets which cannot be explicitly described. For this reason, some logicians reject this axiom, and study what can be deduced without it. It is, however, fundamental to much of mathematics, and mathematics without it is very different.

Another example of a statement which is independent of the axioms is the continuum hypothesis, which was suggested by Cantor in 1878. It states that there is no cardinality which is smaller than the real numbers, but larger than the natural numbers. In 1940, Gödel showed that the continuum hypothesis is consistent with ZF set theory with the axiom of choice (ZFC) — that is, it cannot be proven to be false in that set theory. In 1963, Paul Cohen proved that the continuum hypothesis also cannot be proven in ZFC.