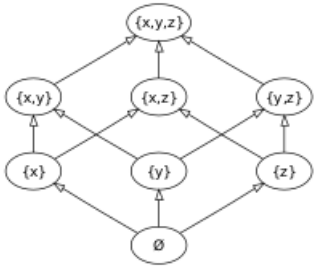
Cantor's theorem

In elementary set theory, **Cantor's theorem** is a fundamental result which states that, for any set A, the set of all subsets of A (the power set of A, denoted by $\mathcal{P}(A)$) has a strictly greater cardinality than A itself. For finite sets, Cantor's theorem can be seen to be true by simple enumeration of the number of subsets. Counting the empty set as a subset, a set with n members has a total of 2^n subsets, so that if $\mathbf{card}(A) = n$, then $\mathbf{card}(\mathcal{P}(A)) = 2^n$, and the theorem holds because $2^n > n$ for all non-negative integers.

Much more significant is Cantor's discovery of an argument that is applicable to any set, which showed that the theorem holds for infinite sets, countable or uncountable, as well as finite ones. As a particularly important consequence, the power set of the set of natural numbers, a countably infinite set with cardinality $\aleph_0 = \mathrm{card}(\mathbb{N})$, is uncountably infinite and has the same size as the set of real numbers, a cardinality larger than that of the set of natural numbers that is often referred to as the cardinality of the continuum: $\mathfrak{c} = \mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathcal{P}(\mathbb{N}))$. The relationship between these cardinal numbers is often expressed symbolically by the equality and inequality $\mathfrak{c} = 2^{\aleph_0} > \aleph_0$.

The theorem is named for German mathematician Georg Cantor, who first stated and proved it at the end of the 19th century. Cantor's theorem had immediate and important consequences for the philosophy of mathematics. For instance, by iteratively taking the power set of an infinite set and applying Cantor's theorem, we obtain an endless hierarchy of infinite cardinals, each strictly larger than the one before it. Consequently, the theorem implies that there is no largest cardinal number (colloquially, "there's no largest infinity").



The cardinality of the set {*x*, *y*, *z*}, is three, while there are eight elements in its power set ($3 < 2^3 = 8$), here ordered by inclusion.

Contents

Proof
When A is countably infinite
Related paradoxes
History
Generalizations
See also
References
External links

Proof

Cantor's argument is elegant and remarkably simple. The complete proof is presented below, with detailed explanations to follow.

Theorem (Cantor). Let f be a map from set A to its power set $\mathcal{P}(A)$. Then $f : A \to \mathcal{P}(A)$ is not surjective. As a consequence, $\mathbf{card}(A) < \mathbf{card}(\mathcal{P}(A))$ holds for any set A.

Proof: Consider the set $B = \{x \in A \mid x \notin f(x)\}$. Suppose to the contrary that f is surjective. Then there exists $\xi \in A$ such that $f(\xi) = B$. But by construction, $\xi \in B \iff \xi \notin f(\xi) = B$. This is a contradiction. Thus, f cannot be surjective. On the other hand, $g : A \to \mathcal{P}(A)$ defined by $x \mapsto \{x\}$ is an injective map. Consequently, we must have $\mathbf{card}(A) < \mathbf{card}(\mathcal{P}(A))$. ■

By definition of cardinality, we have card(X) < card(Y) for any two sets X and Y if and only if there is an injective function but no bijective function from X to Y. It suffices to show that there is no surjection from X to Y. This is the heart of Cantor's theorem: there is no surjective function from any set A to its power set. To establish this, it is enough to show that no function f that maps elements in A to subsets of A can reach every possible subset, i.e., we just need to demonstrate the existence of a subset of A that is not equal to $f(x)$ for any $x \in A$. (Recall that each $f(x)$ is a subset of A.) Such a subset is given by the following construction, sometimes called the *Cantor diagonal set* of f:[1][2]

$$B = \{x \in A \mid x \notin f(x)\}.$$

This means, by definition, that for all $x \in A$, $x \in B$ if and only if $x \notin f(x)$. For all x the sets B and $f(x)$ cannot be the same because B was constructed from elements of A whose images (under f) did not include themselves. More specifically, consider any $x \in A$, then either $x \in f(x)$ or $x \notin f(x)$. In the former case, $f(x)$ cannot equal B because $x \in f(x)$ by assumption and $x \notin B$ by the construction of B. In the latter case, $f(x)$ cannot equal B because $x \notin f(x)$ by assumption and $x \in B$ by the construction of B.

Equivalently, and slightly more formally, we just proved that the existence of $\xi \in A$ such that $f(\xi) = B$ implies the following contradiction:

$$\begin{aligned} \xi \in f(\xi) &\iff \xi \in B && \text{(by assumption that } f(\xi) = B\text{);} \\ \xi \in B &\iff \xi \notin f(\xi) && \text{(by definition of } B\text{).} \end{aligned}$$

Therefore, by reductio ad absurdum, the assumption must be false.[3] Thus there is no $\xi \in A$ such that $f(\xi) = B$; in other words, B is not in the image of f and f does not map to every element of the power set of A, i.e., f is not surjective.

Finally, to complete the proof, we need to exhibit an injective function from A to its power set. Finding such a function is trivial: just map x to the singleton set $\{x\}$. The argument is now complete, and we have established the strict inequality for any set A that card(A) < card($\mathcal{P}(A)$).

Another way to think of the proof is that B, empty or non-empty, is always in the power set of A. For f to be onto, some element of A must map to B. But that leads to a contradiction: no element of B can map to B because that would contradict the criterion of membership in B, thus the element mapping to B must not be an element of B meaning that it satisfies the criterion for membership in B, another contradiction. So the assumption that an element of A maps to B must be false; and f cannot be onto.

Because of the double occurrence of x in the expression "$x \notin f(x)$", this is a diagonal argument. For a countable (or finite) set, the argument of the proof given above can be illustrated by constructing a table in which each row is labelled by a unique x from $A = \{x_1, x_2, \ldots\}$, in this order. A is assumed to admit a linear order so that such table can be constructed. Each column of the table is labelled by a unique y from the power set of A; the columns are ordered by the argument to f, i.e. the column labels are $f(x_1), f(x_2), \ldots$, in this order. The intersection of each row x and column y records a true/false bit whether $x \in y$. Given the order chosen for the row and column labels, the main diagonal D of this table thus records whether $x \in f(x)$ for each $x \in A$. The set B constructed in the previous paragraphs coincides with the row labels for the subset of entries on this main diagonal D where the table records that $x \in f(x)$ is false.[3] Each column records the values of the indicator function of the set corresponding to the column. The indicator function of B coincides with the logically negated (swap "true" and "false") entries of the main diagonal. Thus the indicator function of B does not agree with any column in at least one entry. Consequently, no column represents B.

For a finite set, the proof can also be illustrated using a more prosaic presentation known as the barber paradox.[4]

Despite the simplicity of the above proof, it is rather difficult for an automated theorem prover to produce it. The main difficulty lies in an automated discovery of the Cantor diagonal set. Lawrence Paulson noted in 1992 that Otter could not do it, whereas Isabelle could, albeit with a certain amount of direction in terms of tactics that might perhaps be considered cheating.[2]

When A is countably infinite

Let us examine the proof for the specific case when A is countably infinite. Without loss of generality, we may take $A = \mathbb{N} = \{1, 2, 3,...\}$, the set of natural numbers.

Suppose that $\mathbb{N}$ is equinumerous with its power set $\mathcal{P}(\mathbb{N})$. Let us see a sample of what $\mathcal{P}(\mathbb{N})$ looks like:

$$\mathcal{P}(\mathbb{N}) = \{\varnothing, \{1,2\}, \{1,2,3\}, \{4\}, \{1,5\}, \{3,4,6\}, \{2,4,6,\ldots\}, \ldots\}.$$

$\mathcal{P}(\mathbb{N})$ contains infinite subsets of $\mathbb{N}$, e.g. the set of all even numbers {2, 4, 6,...}, as well as the empty set.

Now that we have an idea of what the elements of $\mathcal{P}(\mathbb{N})$ look like, let us attempt to pair off each element of $\mathbb{N}$ with each element of $\mathcal{P}(\mathbb{N})$ to show that these infinite sets are equinumerous. In other words, we will attempt to pair off each element of $\mathbb{N}$ with an element from the infinite set $\mathcal{P}(\mathbb{N})$, so that no element from either infinite set remains unpaired. Such an attempt to pair elements would look like this:

$$\mathbb{N}\begin{Bmatrix} 1 & \longleftrightarrow & \{4,5\} \\ 2 & \longleftrightarrow & \{1,2,3\} \\ 3 & \longleftrightarrow & \{4,5,6\} \\ 4 & \longleftrightarrow & \{1,3,5\} \\ \vdots & \vdots & \vdots \end{Bmatrix}\mathcal{P}(\mathbb{N}).$$

Given such a pairing, some natural numbers are paired with subsets that contain the very same number. For instance, in our example the number 2 is paired with the subset {1, 2, 3}, which contains 2 as a member. Let us call such numbers *selfish*. Other natural numbers are paired with subsets that do not contain them. For instance, in our example the number 1 is paired with the subset {4, 5}, which does not contain the number 1. Call these numbers *non-selfish*. Likewise, 3 and 4 are non-selfish.

Using this idea, let us build a special set of natural numbers. This set will provide the contradiction we seek. Let B be the set of *all* non-selfish natural numbers. By definition, the power set $\mathcal{P}(\mathbb{N})$ contains all sets of natural numbers, and so it contains this set B as an element. If the mapping is bijective, B must be paired off with some natural number, say b. However, this causes a problem. If b is in B, then b is selfish because it is in the corresponding set, which contradicts the definition of B. If b is not in B, then it is non-selfish and it should instead be a member of B. Therefore, no such element b which maps to B can exist.

Since there is no natural number which can be paired with B, we have contradicted our original supposition, that there is a bijection between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$.

Note that the set B may be empty. This would mean that every natural number x maps to a subset of natural numbers that contains x. Then, every number maps to a nonempty set and no number maps to the empty set. But the empty set is a member of $\mathcal{P}(\mathbb{N})$, so the mapping still does not cover $\mathcal{P}(\mathbb{N})$.

Through this proof by contradiction we have proven that the cardinality of $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ cannot be equal. We also know that the cardinality of $\mathcal{P}(\mathbb{N})$ cannot be less than the cardinality of $\mathbb{N}$ because $\mathcal{P}(\mathbb{N})$ contains all singletons, by definition, and these singletons form a "copy" of $\mathbb{N}$ inside of $\mathcal{P}(\mathbb{N})$. Therefore, only one possibility remains, and that is that the cardinality of $\mathcal{P}(\mathbb{N})$ is strictly greater than the cardinality of $\mathbb{N}$, proving Cantor's theorem.

Related paradoxes

Cantor's theorem and its proof are closely related to two paradoxes of set theory.

Cantor's paradox is the name given to a contradiction following from Cantor's theorem together with the assumption that there is a set containing all sets, the universal set V. In order to distinguish this paradox from the next one discussed below, it is important to note what this contradiction is. By Cantor's theorem $|\mathcal{P}(X)| > |X|$ for any set X. On the other hand, all elements of $\mathcal{P}(V)$ are sets, and thus contained in V, therefore $|\mathcal{P}(V)| \leqslant |V|$.[1]

Another paradox can be derived from the proof of Cantor's theorem by instantiating the function f with the identity function; this turns Cantor's diagonal set into what is sometimes called the *Russell set* of a given set A:[1]

$$R_A = \{ x \in A : x \notin x \}.$$

The proof of Cantor's theorem is straightforwardly adapted to show that assuming a set of all sets U exists, then considering its Russell set R_U leads to the contradiction:

$$R_U \in R_U \iff R_U \notin R_U.$$

This argument is known as Russell's paradox.[1] As a point of subtlety, the version of Russell's paradox we have presented here is actually a theorem of Zermelo;[5] we can conclude from the contradiction obtained that we must reject the hypothesis that $R_U \in U$, thus disproving the existence of a set containing all sets. This was possible because we have used restricted comprehension (as featured in ZFC) in the definition of R_A above, which in turn entailed that

$$R_U \in R_U \iff (R_U \in U \wedge R_U \notin R_U).$$

Had we used unrestricted comprehension (as in Frege's system for instance) by defining the Russell set simply as $R = \{ x : x \notin x \}$, then the axiom system itself would have entailed the contradiction, with no further hypotheses needed.[5]

Despite the syntactical similarities between the Russell set (in either variant) and the Cantor diagonal set, Alonzo Church emphasized that Russell's paradox is independent of considerations of cardinality and its underlying notions like one-to-one correspondence.[6]

History

Cantor gave essentially this proof in a paper published in 1891 "Über eine elementare Frage der Mannigfaltigkeitslehre", where the diagonal argument for the uncountability of the reals also first appears (he had earlier proved the uncountability of the reals by other methods). The version of this argument he gave in that paper was phrased in terms of indicator functions on a set rather than subsets of a set. He showed that if f is a function defined on X whose values are 2-valued functions on X, then the 2-valued function $G(x) = 1 - f(x)(x)$ is not in the range of f.

Bertrand Russell has a very similar proof in *Principles of Mathematics* (1903, section 348), where he shows that there are more propositional functions than objects. "For suppose a correlation of all objects and some propositional functions to have been affected, and let phi-x be the correlate of x. Then "not-phi-x(x)," i.e. "phi-x does not hold of x" is a propositional function not contained in this correlation; for it is true or false of x according as phi-x is false or true of x, and therefore it differs from phi-x for every value of x." He attributes the idea behind the proof to Cantor.

Ernst Zermelo has a theorem (which he calls "Cantor's Theorem") that is identical to the form above in the paper that became the foundation of modern set theory ("Untersuchungen über die Grundlagen der Mengenlehre I"), published in 1908. See Zermelo set theory.

Generalizations

Cantor's theorem has been generalized to any category with products.[7]

See also

- Schröder–Bernstein theorem
- Cantor's first uncountability proof
- Controversy over Cantor's theory

References

1. Abhijit Dasgupta (2013). *Set Theory: With an Introduction to Real Point Sets*. Springer Science & Business Media. pp. 362–363. ISBN 978-1-4614-8854-5.
2. Lawrence Paulson (1992). *Set Theory as a Computational Logic* (https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-271.pdf) (PDF). University of Cambridge Computer Laboratory. p. 14.
3. Graham Priest (2002). *Beyond the Limits of Thought*. Oxford University Press. pp. 118–119. ISBN 978-0-19-925405-7.
4. Albert Geoffrey Howson (1990). *The Popularization of Mathematics*. Cambridge University Press. p. 197. ISBN 978-0-521-40319-1.
5. Heinz-Dieter Ebbinghaus (2007). *Ernst Zermelo: An Approach to His Life and Work* (https://archive.org/details/ernstzermeloappr00ebbi_571). Springer Science & Business Media. pp. 86 (https://archive.org/details/ernstzermeloappr00ebbi_571/page/n97)–87. ISBN 978-3-540-49553-6.
6. Church, A. [1974] "Set theory with a universal set." in *Proceedings of the Tarski Symposium. Proceedings of Symposia in Pure Mathematics XXV,* ed. L. Henkin, Providence RI, Second printing with additions 1979, pp. 297−308. ISBN 978-0-8218-7360-1. Also published in *International Logic Review* 15 pp. 11−23.
7. F. William Lawvere; Stephen H. Schanuel (2009). *Conceptual Mathematics: A First Introduction to Categories* (https://archive.org/details/conceptualmathem00lawv). Cambridge University Press. Session 29. ISBN 978-0-521-89485-2.

- Halmos, Paul, *Naive Set Theory*. Princeton, NJ: D. Van Nostrand Company, 1960. Reprinted by Springer-Verlag, New York, 1974. ISBN 0-387-90092-6 (Springer-Verlag edition). Reprinted by Martino Fine Books, 2011. ISBN 978-1-61427-131-4 (Paperback edition).
- Jech, Thomas (2002), *Set Theory*, Springer Monographs in Mathematics (3rd millennium ed.), Springer, ISBN 3-540-44085-2

External links

- Hazewinkel, Michiel, ed. (2001) [1994], "Cantor theorem" (https://www.encyclopediaofmath.org/index.php?title=p/c020260), *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Weisstein, Eric W. "Cantor's Theorem" (https://mathworld.wolfram.com/CantorsTheorem.html). *MathWorld*.