

Constructive proof

In mathematics, a **constructive proof** is a method of proof that demonstrates the existence of a mathematical object by creating or providing a method for creating the object. This is in contrast to a **non-constructive proof** (also known as an *existence proof* or *pure existence theorem*) which proves the existence of a particular kind of object without providing an example.

Some non-constructive proofs show that if a certain proposition is false, a contradiction ensues; consequently the proposition must be true (proof by contradiction). However, the principle of explosion(*ex falso quodlibet*) has been accepted in some varieties of constructive mathematics, including intuitionism.

Constructivism is a mathematical philosophy that rejects all but constructive proofs in mathematics. This leads to a restriction on the proof methods allowed (prototypically, the law of the excluded middle is not accepted) and a different meaning of terminology (for example, the term "or" has a stronger meaning in constructive mathematics than in classical).

Constructive proofs can be seen as defining certified mathematical algorithms: this idea is explored in the Brouwer–Heyting–Kolmogorov interpretation of constructive logic, the Curry–Howard correspondence between proofs and programs, and such logical systems as Per Martin-Löf's Intuitionistic Type Theory, and Thierry Coquand and Gérard Huet's Calculus of Constructions

Contents

1	Examples
1.1	Non-constructive proofs
1.2	Constructive proofs
2	Brouwerian counterexamples
3	See also
4	References
5	Further reading
6	External links

Examples

Non-constructive proofs

First consider the theorem that there are an infinitude of prime numbers. Euclid's proof is constructive. But a common way of simplifying Euclid's proof postulates that, contrary to the assertion in the theorem, there are only a finite number of them, in which case there is a largest one, denoted *n*. Then consider the number *n!* + 1 (1 + the product of the first *n* numbers). Either this number is prime, or all of its prime factors are greater than *n*. Without establishing a specific prime number, this proves that one exists that is greater than *n*, contrary to the original postulate.

Now consider the theorem "There exist irrational numbers *a* and *b* such that *a*^{*b*} is rational." This theorem can be proven using a constructive proof, or using a non-constructive proof.

The following 1953 proof by Dov Jarden has been widely used as an example of a non-constructive proof since at least 1970.^[2]

CURIOSA

339. A Simple Proof That a Power of an Irrational Number to an Irrational Exponent May Be Rational.

$\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If it is rational, our statement is proved. If it is irrational $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ proves our statement.

Dov Jarden Jerusalem

In a bit more detail:

- Recall that $\sqrt{2}$ is irrational, and 2 is rational. Consider the number $q = \sqrt{2}^{\sqrt{2}}$. Either it is rational or it is irrational.
- If *q* is rational, then the theorem is true, with *a* and *b* both being $\sqrt{2}$.
- If *q* is irrational, then the theorem is true, with *a* being $\sqrt{2}^{\sqrt{2}}$ and *b* being $\sqrt{2}$, since

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2.$$

This proof is non-constructive because it relies on the statement "Either *q* is rational or it is irrational"—an instance of the law of excluded middle, which is not valid within a constructive proof. The non-constructive proof does not construct an example *a* and *b*; it merely gives a number of possibilities (in this case, two mutually exclusive possibilities) and shows that one of them—but does not show *which* one—must yield the desired example.

It turns out that $\sqrt{2}^{\sqrt{2}}$ is irrational because of the Gelfond–Schneider theorem but this fact is irrelevant to the correctness of the non-constructive proof.

Constructive proofs

A *constructive* proof of the above theorem on irrational powers of irrationals would give an actual example, such as:

$$a = \sqrt{2}, \quad b = \log_2 9, \quad a^b = 3.$$

The square root of 2 is irrational, and 3 is rational. **log₂ 9** is also irrational: if it were equal to $\frac{m}{n}$, then, by the properties of logarithms, 9^n would be equal to 2^m , but the former is odd, and the latter is even.

A more substantial example is the graph minor theorem. A consequence of this theorem is that a graph can be drawn on the torus if, and only if, none of its minors belong to a certain finite set of "forbidden minors". However, the proof of the existence of this finite set is not constructive, and the forbidden minors are not actually specified. They are still unknown.

Brouwerian counterexamples

In constructive mathematics a statement may be disproved by giving a counterexample, as in classical mathematics. However, it is also possible to give a **Brouwerian counterexample** to show that the statement is non-constructive. This sort of counterexample shows that the statement implies some principle that is known to be non-constructive. If it can be proved constructively that a statement implies some principle that is not constructively provable, then the statement itself cannot be constructively provable. For example, a particular statement may be shown to imply the law of the excluded middle. An example of a Brouwerian counterexample of this type is Diaconescu's theorem which shows that the full axiom of choice is non-constructive in systems of constructive set theory, since the axiom of choice implies the law of excluded middle in such systems. The field of constructive reverse mathematics develops this idea further by classifying various principles in terms of "how nonconstructive" they are, by showing they are equivalent to various fragments of the law of the excluded middle.

Brouwer also provided "weak" counterexamples^[3] Such counterexamples do not disprove a statement, however; they only show that, at present, no constructive proof of the statement is known. One weak counterexample begins by taking some unsolved problem of mathematics, such as Goldbach's conjecture which asks whether every even natural number larger than 4 is the sum of two primes. Define a sequence *a*(*n*) of rational numbers as follows:^[4]

$$a(n) = \begin{cases} (1/2)^n & \text{if every even natural number in the interval } [4, n] \text{ is the sum of two primes,} \\ (1/2)^k & \text{if } k \text{ is the least even natural number in the interval } [4, n] \text{ which is not the sum of two primes} \end{cases}$$

For each *n*, the value of *a*(*n*) can be determined by exhaustive search, and so *a* is a well defined sequence, constructively. Moreover, because *a* is a Cauchy sequence with a fixed rate of convergence, *a* converges to some real number α, according to the usual treatment of real numbers in constructive mathematics.

Several facts about the real number α can be proved constructively. However, based on the different meaning of the words in constructive mathematics, if there is a constructive proof that "α = 0 or α ≠ 0" then this would mean that there is a constructive proof of Goldbach's conjecture (in the former case) or a constructive proof that Goldbach's conjecture is false (in the latter case). Because no such proof is known, the quoted statement must also not have a known constructive proof. However, it is entirely possible that Goldbach's conjecture may have a constructive proof (as we do not know at present whether it does), in which case the quoted statement would have a constructive proof as well, albeit one that is unknown at present. The main practical use of weak counterexamples is to identify the "hardness" of a problem. For example, the counterexample just shown shows that the quoted statement is "at least as hard to prove" as Goldbach's conjecture. Weak counterexamples of this sort are often related to the limited principle of omniscience

See also

- Errett Bishop - author of the book "Foundations of Constructive Analysis".
- Existence theorem#'Pure' existence results
- Non-constructive algorithm existence proofs
- Probabilistic method

References

- ↑ J. Roger Hindley, "The Root-2 Proof as an Example of Non-constructivity", unpublished paperSeptember 2014, full text (http://www.users.waitrose.com/~hindley/Root2Proof2014.pdf)Archived (https://web.archive.org/web/20141023060917/http://www.users.waitrose.com/~hindley/Root2Proof2014.pdf)2014-10-23 at the Wayback Machine
- ↑ Dov Jarden, "A simple proof that a power of an irrational number to an irrational exponent may be rational", *Curiosa* No. 339 in *Scripta Mathematica***19**:229 (1953)
- ↑ A. S. Troelstra, *Principles of Intuitionism*, Lecture Notes in Mathematics 95, 1969, p. 102
- ↑ Mark van Atten, 2015, Weak Counterexamples(https://plato.stanford.edu/entries/brouwer/weakcounterex.html) Stanford Encyclopedia of Mathematics

Further reading

- J. Franklin and A. Daoud (2011)*Proof in Mathematics: An Introduction* Kew Books, ISBN 0-646-54509-4, ch. 4
- Hardy, G.H. & Wright, E.M. (1979) *An Introduction to the Theory of Numbers* (Fifth Edition). Oxford University Press.ISBN 0-19-853171-0
- Anne Sjerp Troelstra and Dirk van Dalen (1988) "Constructivism in Mathematics: Volume 1" Elsevier Science.ISBN 978-0-444-70506-8

External links

- Weak counterexamples*by Mark van Atten, Stanford Encyclopedia of Philosophy

Retrieved from 'https://en.wikipedia.org/w/index.php?title=Constructive_proof&oldid=795170927'

This page was last edited on 12 August 2017, at 13:51.

Text is available under theCreative Commons Attribution-ShareAlike Licenseadditional terms may applyBy using this site, you agree to theTerms of Use and Privacy Policy. Wikipedia® is a registered trademark of theWikimedia Foundation, Inc, a non-profit organization.