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. For avoiding confusion with the stronger concept that follows, such a constrictive proof is sometimes called an **effective proof**.

A **constructive proof** may also refer to the stronger concept of a proof that is valid in Constructive mathematics. Constructivism is a mathematical philosophy that rejects all proof methods that involve the existence of objects that are not explicitly built. This excludes, in particular, the use of the law of the excluded middle, the axiom of infinity, and the axiom of choice, and induces a different meaning for some terminology (for example, the term "or" has a stronger meaning in constructive mathematics than in classical).

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.

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

A historical example

Until the end of 19th century, all mathematical proofs were essentially constructive. The first non-constructive constructions appeared with Georg Cantor theory of infinite set, and the formal definition of real numbers.

The first use of non-constructive proofs for solving previously considered problems seems to be Hilbert's Nullstellensatz and Hilbert's basis theorem. From a philosophical point of view, the former is specially interesting, as implying the existence of a well specified object.

Nullstellensatz may be stated as follows: If $f_1, \ldots, f_k$ are polynomials in n indeterminates with complex coefficients, which have no common complex zeros, then there are polynomial $g_1, \ldots, g_k$ such that

$$f_1 g_1 + \ldots + f_k g_k = 1.$$

Such a non-constructive existence theorem was such a surprise for mathematicians of that time that one of them, Paul Gordan wrote: *"this is not mathematics, it is theology*".

Twenty five years later, Grete Hermann provided an algorithm for computing $g_1, \ldots, g_k$, which is not a constructive proof in the strong sense, as she used Hilbert's result. She proved that, if $g_1, \ldots, g_k$ exist, they can be found with degrees less than 2^{2^n}.

This provides an algorithm, as the problem is reduced to solving a system of linear equations, by considering as unknowns the finite number of coefficients of the g_i.

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:[1][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. $\log_2 9$ 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

1. J. Roger Hindley, "The Root-2 Proof as an Example of Non-constructivity", unpublished paper, September 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.
2. 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)
3. A. S. Troelstra, *Principles of Intuitionism*, Lecture Notes in Mathematics 95, 1969, p. 102
4. 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