Mathematical proof [UNIT-II]

- Article

P. Oxy. 29, one of the oldest surviving fragments of Euclid's *Elements*, a textbook used for millennia to teach proof-writing techniques. The diagram accompanies Book II, Proposition 5.[1]

A **mathematical proof** is a deductive argument for a mathematical statement, showing that the stated assumptions logically guarantee the conclusion. The argument may use other previously established statements, such as theorems; but every proof can, in principle, be constructed using only certain basic or original assumptions known as axioms,[2][3][4] along with the accepted rules of inference. Proofs are examples of exhaustive deductive reasoning which establish logical certainty, to be distinguished from empirical arguments or non-exhaustive inductive reasoning which establish "reasonable expectation". Presenting many cases in which the statement holds is not enough for a proof, which must demonstrate that the statement is true in *all* possible cases. A proposition that has not been proved but is believed to be true is known as a conjecture, or a hypothesis if frequently used as an assumption for further mathematical work.

Proofs employ logic expressed in mathematical symbols, along with natural language which usually admits some ambiguity. In most mathematical literature, proofs are written in terms of rigorous informal logic. Purely formal proofs, written fully in symbolic language without the involvement of natural language, are considered in proof theory. The distinction between formal and informal proofs has led to much examination of current and historical mathematical practice, quasi-empiricism in mathematics, and so-called folk mathematics, oral traditions in the mainstream mathematical community or in other cultures. The philosophy of mathematics is concerned with the role of language and logic in proofs, and mathematics as a language.

History and etymology

: History of logic

The word "proof" comes from the Latin *probare* (to test). Related modern words are English "probe", "probation", and "probability", Spanish *probar* (to smell or taste, or sometimes touch or test),[5] Italian *provare* (to try), and German *probieren* (to try). The legal term "probity" means authority or credibility, the power of testimony to prove facts when given by persons of reputation or status.[6]

Plausibility arguments using heuristic devices such as pictures and analogies preceded strict mathematical proof.[7] It is likely that the idea of demonstrating a conclusion first arose in connection with geometry, which originated in practical problems of land measurement.[8] The development of mathematical proof is primarily the product of ancient Greek mathematics, and

one of its greatest achievements.[9] Thales (624–546 BCE) and Hippocrates of Chios (c. 470–410 BCE) gave some of the first known proofs of theorems in geometry. Eudoxus (408–355 BCE) and Theaetetus (417–369 BCE) formulated theorems but did not prove them. Aristotle (384–322 BCE) said definitions should describe the concept being defined in terms of other concepts already known.

Mathematical proof was revolutionized by Euclid (300 BCE), who introduced the axiomatic method still in use today. It starts with undefined terms and axioms, propositions concerning the undefined terms which are assumed to be self-evidently true (from Greek "axios", something worthy). From this basis, the method proves theorems using deductive logic. Euclid's book, the *Elements*, was read by anyone who was considered educated in the West until the middle of the 20th century.[10] In addition to theorems of geometry, such as the Pythagorean theorem, the *Elements* also covers number theory, including a proof that the square root of two is irrational and a proof that there are infinitely many prime numbers.

Further advances also took place in medieval Islamic mathematics. In the 10th century CE, the Iraqi mathematician Al-Hashimi worked with numbers as such, called "lines" but not necessarily considered as measurements of geometric objects, to prove algebraic propositions concerning multiplication, division, etc., including the existence of irrational numbers.[11] An inductive proof for arithmetic sequences was introduced in the *Al-Fakhri* (1000) by Al-Karaji, who used it to prove the binomial theorem and properties of Pascal's triangle.

Modern proof theory treats proofs as inductively defined data structures, not requiring an assumption that axioms are "true" in any sense. This allows parallel mathematical theories as formal models of a given intuitive concept, based on alternate sets of axioms, for example Axiomatic set theory and Non-Euclidean geometry.

Nature and purpose

As practiced, a proof is expressed in natural language and is a rigorous argument intended to convince the audience of the truth of a statement. The standard of rigor is not absolute and has varied throughout history. A proof can be presented differently depending on the intended audience. To gain acceptance, a proof has to meet communal standards of rigor; an argument considered vague or incomplete may be rejected.

The concept of proof is formalized in the field of mathematical logic.[12] A formal proof is written in a formal language instead of natural language. A formal proof is a sequence of formulas in a formal language, starting with an assumption, and with each subsequent formula a logical consequence of the preceding ones. This definition makes the concept of proof amenable to study. Indeed, the field of proof theory studies formal proofs and their properties, the most famous and surprising being that almost all axiomatic systems can generate certain undecidable statements not provable within the system.

The definition of a formal proof is intended to capture the concept of proofs as written in the practice of mathematics. The soundness of this definition amounts to the belief that a published proof can, in principle, be converted into a formal proof. However, outside the field of automated proof assistants, this is rarely done in practice. A classic question in philosophy asks whether mathematical proofs are analytic or synthetic. Kant, who introduced the analytic–synthetic distinction, believed mathematical proofs are synthetic, whereas Quine argued in his 1951 "Two Dogmas of Empiricism" that such a distinction is untenable.[13]

Proofs may be admired for their mathematical beauty. The mathematician Paul Erdős was known for describing proofs which he found to be particularly elegant as coming from "The Book", a hypothetical tome containing the most beautiful method(s) of proving each theorem. The book *Proofs from THE BOOK*, published in 2003, is devoted to presenting 32 proofs its editors find particularly pleasing.

Methods of proof

Direct proof

: Direct proof

In direct proof, the conclusion is established by logically combining the axioms, definitions, and earlier theorems.[14] For example, direct proof can be used to prove that the sum of two even integers is always even:

> Consider two even integers x and y. Since they are even, they can be written as $x = 2a$ and $y = 2b$, respectively, for some integers a and b. Then the sum is $x + y = 2a + 2b = 2(a+b)$. Therefore $x+y$ has 2 as a factor and, by definition, is even. Hence, the sum of any two even integers is even.

This proof uses the definition of even integers, the integer properties of closure under addition and multiplication, and the distributive property.

Proof by mathematical induction

: Mathematical induction

Despite its name, mathematical induction is a method of deduction, not a form of inductive reasoning. In proof by mathematical induction, a single "base case" is proved, and an "induction rule" is proved that establishes that any arbitrary case implies the next case. Since in principle the induction rule can be applied repeatedly (starting from the proved base case), it follows that all (usually infinitely many) cases are provable.[15] This avoids having to prove each case individually. A variant of mathematical induction is proof by infinite descent, which can be used, for example, to prove the irrationality of the square root of two.

A common application of proof by mathematical induction is to prove that a property known to hold for one number holds for all natural numbers:[16] Let $\mathbf{N} = \{1, 2, 3, 4, ...\}$ be the set of natural numbers, and let $P(n)$ be a mathematical statement involving the natural number n belonging to $\mathbf{N}$ such that

- **(i)** $P(1)$ is true, i.e., $P(n)$ is true for $n = 1$.
- **(ii)** $P(n+1)$ is true whenever $P(n)$ is true, i.e., $P(n)$ is true implies that $P(n+1)$ is true.
- **Then $P(n)$ is true for all natural numbers n.**

For example, we can prove by induction that all positive integers of the form $2n - 1$ are odd. Let $P(n)$ represent "$2n - 1$ is odd":

> **(i)** For $n = 1$, $2n - 1 = 2(1) - 1 = 1$, and 1 is odd, since it leaves a remainder of 1 when divided by 2. Thus $P(1)$ is true.

(ii) For any n, if $2n - 1$ is odd ($P(n)$), then $(2n - 1) + 2$ must also be odd, because adding 2 to an odd number results in an odd number.
But $(2n - 1) + 2 = 2n + 1 = 2(n+1) - 1$, so $2(n+1) - 1$ is odd ($P(n+1)$).
So $P(n)$ implies $P(n+1)$.
Thus $2n - 1$ is odd, for all positive integers n.

The shorter phrase "proof by induction" is often used instead of "proof by mathematical induction".[17]

Proof by contraposition

: Contraposition

Proof by contraposition infers the statement "if *p* then *q*" by establishing the logically equivalent contrapositive statement: "if *not q* then *not p*".

For example, contraposition can be used to establish that, given an integer

, if is even, then is even:

Suppose is not even. Then is odd. The product of two odd numbers is odd,

hence is odd. Thus is not even. Thus, if *is* even, the supposition must

be false, so has to be even.

Proof by contradiction

: Proof by contradiction

In proof by contradiction, also known by the Latin phrase *reductio ad absurdum* (by reduction to the absurd), it is shown that if some statement is assumed true, a logical contradiction occurs, hence the statement must be

false. A famous example involves the proof that is an irrational number:

Suppose that were a rational number. Then it could be written in lowest terms

as where *a* and *b* are non-zero integers with no common factor. Thus, .
Squaring both sides yields $2b^2 = a^2$. Since the expression on the left is an integer multiple of 2, the right expression is by definition divisible by 2. That is, a^2 is even, which implies that *a* must also be even, as seen in the proposition above (in #Proof by contraposition). So we can write $a = 2c$, where *c* is also an integer. Substitution into the original equation yields $2b^2 = (2c)^2 = 4c^2$. Dividing both sides by 2 yields $b^2 = 2c^2$. But then, by the same argument as before, 2 divides b^2, so *b* must be even. However, if *a* and *b* are both even, they have 2 as a common factor. This contradicts our previous

statement that *a* and *b* have no common factor, so we must conclude that is an irrational number.

To paraphrase: if one could write as a fraction, this fraction could never be written in lowest terms, since 2 could always be factored from numerator and denominator.

Proof by construction

: Proof by construction

Proof by construction, or proof by example, is the construction of a concrete example with a property to show that something having that property exists. Joseph Liouville, for instance, proved the existence of transcendental numbers by constructing an explicit example. It can also be used to construct a counterexample to disprove a proposition that all elements have a certain property.

Proof by exhaustion

Proof by exhaustion

In proof by exhaustion, the conclusion is established by dividing it into a finite number of cases and proving each one separately. The number of cases sometimes can become very large. For example, the first proof of the four color theorem was a proof by exhaustion with 1,936 cases. This proof was controversial because the majority of the cases were checked by a computer program, not by hand.[18]

Closed chain inference

: Closed chain inference

A closed chain inference shows that a collection of statements are pairwise equivalent.

In order to prove that the statements are each pairwise equivalent,

proofs are given for the implications , , , and .[19][20]

The pairwise equivalence of the statements then results from the transitivity of the material conditional.

Probabilistic proof

: Probabilistic method

A probabilistic proof is one in which an example is shown to exist, with certainty, by using methods of probability theory. Probabilistic proof, like proof by construction, is one of many ways to prove existence theorems.

In the probabilistic method, one seeks an object having a given property, starting with a large set of candidates. One assigns a certain probability for each candidate to be chosen, and then proves that there is a non-zero probability that a chosen candidate will have the desired

property. This does not specify which candidates have the property, but the probability could not be positive without at least one.

A probabilistic proof is not to be confused with an argument that a theorem is 'probably' true, a 'plausibility argument'. The work toward the Collatz conjecture shows how far plausibility is from genuine proof, as does the disproof of the Mertens conjecture. While most mathematicians do not think that probabilistic evidence for the properties of a given object counts as a genuine mathematical proof, a few mathematicians and philosophers have argued that at least some types of probabilistic evidence (such as Rabin's probabilistic algorithm for testing primality) are as good as genuine mathematical proofs.[21][22]

Combinatorial proof

: Combinatorial proof

A combinatorial proof establishes the equivalence of different expressions by showing that they count the same object in different ways. Often a bijection between two sets is used to show that the expressions for their two sizes are equal. Alternatively, a double counting argument provides two different expressions for the size of a single set, again showing that the two expressions are equal.

Nonconstructive proof

: Nonconstructive proof

A nonconstructive proof establishes that a mathematical object with a certain property exists—without explaining how such an object can be found. Often, this takes the form of a proof by contradiction in which the nonexistence of the object is proved to be impossible. In contrast, a constructive proof establishes that a particular object exists by providing a method of finding it. The following famous example of a nonconstructive proof shows that there exist two irrational

numbers *a* and *b* such that is a rational number. This proof uses

that is irrational (an easy proof is known since Euclid), but not

that is irrational (this is true, but the proof is not elementary).

Either is a rational number and we are done (take), or is irrational so we

can write and . This then gives , which is thus a rational number of the

form

Statistical proofs in pure mathematics

: Statistical proof

The expression "statistical proof" may be used technically or colloquially in areas of pure mathematics, such as involving cryptography, chaotic series, and probabilistic number theory or analytic number theory.[23][24][25] It is less commonly used to refer to a mathematical proof in the branch of mathematics known as mathematical statistics. See also the "Statistical proof using data" section below.

Computer-assisted proofs

: Computer-assisted proof

Until the twentieth century it was assumed that any proof could, in principle, be checked by a competent mathematician to confirm its validity.[7] However, computers are now used both to prove theorems and to carry out calculations that are too long for any human or team of humans to check; the first proof of the four color theorem is an example of a computer-assisted proof. Some mathematicians are concerned that the possibility of an error in a computer program or a run-time error in its calculations calls the validity of such computer-assisted proofs into question. In practice, the chances of an error invalidating a computer-assisted proof can be reduced by incorporating redundancy and self-checks into calculations, and by developing multiple independent approaches and programs. Errors can never be completely ruled out in case of verification of a proof by humans either, especially if the proof contains natural language and requires deep mathematical insight to uncover the potential hidden assumptions and fallacies involved.

Undecidable statements

A statement that is neither provable nor disprovable from a set of axioms is called undecidable (from those axioms). One example is the parallel postulate, which is neither provable nor refutable from the remaining axioms of Euclidean geometry.

Mathematicians have shown there are many statements that are neither provable nor disprovable in Zermelo–Fraenkel set theory with the axiom of choice (ZFC), the standard system of set theory in mathematics (assuming that ZFC is consistent); see List of statements undecidable in ZFC.

Gödel's (first) incompleteness theorem shows that many axiom systems of mathematical interest will have undecidable statements.

Heuristic mathematics and experimental mathematics

: Experimental mathematics

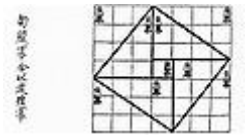
While early mathematicians such as Eudoxus of Cnidus did not use proofs, from Euclid to the foundational mathematics developments

of the late 19th and 20th centuries, proofs were an essential part of mathematics.[26] With the increase in computing power in the 1960s, significant work began to be done investigating mathematical objects beyond the proof-theorem framework,[27] in experimental mathematics. Early pioneers of these methods intended the work ultimately to be resolved into a classical proof-theorem framework, e.g. the early development of fractal geometry,[28] which was ultimately so resolved.

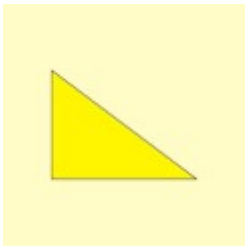
Related concepts

Visual proof

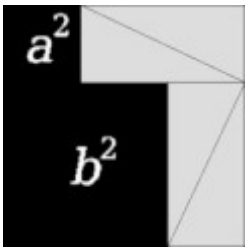
Although not a formal proof, a visual demonstration of a mathematical theorem is sometimes called a "proof without words". The left-hand picture below is an example of a historic visual proof of the Pythagorean theorem in the case of the (3,4,5) triangle.

- 

Visual proof for the (3,4,5) triangle as in the Zhoubi Suanjing 500–200 BCE.

- 

Animated visual proof for the Pythagorean theorem by rearrangement.

- 

A second animated proof of the Pythagorean theorem.

Some illusory visual proofs, such as the missing square puzzle, can be constructed in a way which appear to prove a supposed mathematical fact but only do so by neglecting tiny errors (for

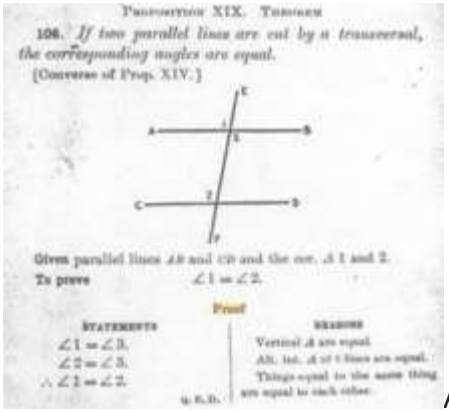
example, supposedly straight lines which actually bend slightly) which are unnoticeable until the entire picture is closely examined, with lengths and angles precisely measured or calculated.

Elementary proof

: Elementary proof

An elementary proof is a proof which only uses basic techniques. More specifically, the term is used in number theory to refer to proofs that make no use of complex analysis. For some time it was thought that certain theorems, like the prime number theorem, could only be proved using "higher" mathematics. However, over time, many of these results have been reproved using only elementary techniques.

Two-column proof



PROPOSITION XIX. THEOREM

106. *If two parallel lines are cut by a transversal, the corresponding angles are equal.*

[Converse of Prop. XIV.]

Given parallel lines AB and CD and the corr. ∠s 1 and 2.

To prove ∠1 = ∠2.

Proof

STATEMENTS	REASONS
∠1 = ∠3.	Vertical ∠s are equal.
∠2 = ∠3.	Alt. int. ∠s of ‖ lines are equal.
∴ ∠1 = ∠2.	Things equal to the same thing are equal to each other.

Q. E. D.

A two-column proof published in 1913

A particular way of organising a proof using two parallel columns is often used as a mathematical exercise in elementary geometry classes in the United States.[29] The proof is written as a series of lines in two columns. In each line, the left-hand column contains a proposition, while the right-hand column contains a brief explanation of how the corresponding proposition in the left-hand column is either an axiom, a hypothesis, or can be logically derived from previous propositions. The left-hand column is typically headed "Statements" and the right-hand column is typically headed "Reasons".[30]

Colloquial use of "mathematical proof"

The expression "mathematical proof" is used by lay people to refer to using mathematical methods or arguing with mathematical objects, such as numbers, to demonstrate something about everyday life, or when data used in an argument is numerical. It is sometimes also used to mean a "statistical proof" (below), especially when used to argue from data.

Statistical proof using data

: Statistical proof

"Statistical proof" from data refers to the application of statistics, data analysis, or Bayesian analysis to infer propositions regarding the probability of data. While *using* mathematical proof to establish theorems in statistics, it is usually not a mathematical proof in that the *assumptions* from which probability statements are derived require empirical evidence from outside mathematics to verify. In physics, in addition to statistical methods, "statistical proof" can refer to the specialized *mathematical methods of physics* applied to analyze data in a particle physics experiment or observational study in physical cosmology. "Statistical proof" may also refer to raw data or a convincing diagram involving data, such as scatter plots, when the data or diagram is adequately convincing without further analysis.

Inductive logic proofs and Bayesian analysis

: Inductive logic and Bayesian analysis

Proofs using inductive logic, while considered mathematical in nature, seek to establish propositions with a degree of certainty, which acts in a similar manner to probability, and may be less than full certainty. Inductive logic should not be confused with mathematical induction.

Bayesian analysis uses Bayes' theorem to update a person's assessment of likelihoods of hypotheses when new evidence or information is acquired.

Proofs as mental objects

: Psychologism and Language of thought

Psychologism views mathematical proofs as psychological or mental objects. Mathematician philosophers, such as Leibniz, Frege, and Carnap have variously criticized this view and attempted to develop a semantics for what they considered to be the language of thought, whereby standards of mathematical proof might be applied to empirical science.

Influence of mathematical proof methods outside mathematics

Philosopher-mathematicians such as Spinoza have attempted to formulate philosophical arguments in an axiomatic manner, whereby mathematical proof standards could be applied to argumentation in general philosophy. Other mathematician-philosophers have tried to use standards of mathematical proof and reason, without empiricism, to arrive at statements outside of mathematics, but having the certainty of propositions deduced in a mathematical proof, such as Descartes' *cogito* argument.

Ending a proof

[edit]

Main article: Q.E.D.

Sometimes, the abbreviation *"Q.E.D."* is written to indicate the end of a proof. This abbreviation stands for *"quod erat demonstrandum"*, which is Latin for *"that which was to be demonstrated"*. A more common alternative is to use a square or a rectangle, such as □ or ■, known as a "tombstone" or "halmos" after its eponym Paul Halmos. Often, "which was to be shown" is verbally stated when writing "QED", "□", or "■" during an oral presentation. Unicode explicitly provides the "end of proof" character, U+220E (■) (220E(hex) = 8718(dec)).