PROOF

S. R. Searle*

Biometrics Unit, Cornell University, Ithaca, New York

BU-530-M

REVISED MAY, 1976

Abstract

Students from applied disciplines taking service courses in mathematics often have difficulty with the concepts and techniques of mathematical proof. This note outlines some ideas that have been used over a period of years in an elementary presentation of the importance of proof and its logic. A short list is given of widely used elementary methods of proof.

---

*Preparation of this manuscript was completed while the author was on leave, 1975-6, at Florida State University.

PROOF

S. R. Searle*

Biometrics Unit, Cornell University, Ithaca, New York

Introduction

Considerable teaching of mathematics is done in service courses to students having major interests such as physical and biological sciences, the humanities, medicine, the social sciences, business, and law. Quite apart from the mathematical content of such courses, a wholly new concept to most of the students involved is that of proof, for which there is little opportunity or need in many disciplines outside of mathematics. However, when students from those disciplines come to learn some mathematics, their texts seldom contain even introductory discussion of the most important of all concepts in mathematics, namely proof. Yet the process of proof is vital, not only to the development of mathematics, but also at all levels of learning mathematics.

Service courses seldom involve full mathematical rigor, nor do they proceed wholly in the manner of theorem, proof, theorem, proof, ...; and the more advanced material may often be presented without proof. Nevertheless, the proving of many results and the asking for proof in homework assignments will always be part of such courses no matter how it is characterized: e.g., "show that ...", "satisfy yourself that ...", or "establish that ...". Although a student

---

*Preparation of this manuscript was completed while the author was on leave at Florida State University, 1975-6.

beginning a service course may feel a need to learn only the mathematics applicable to his discipline and not the techniques of developing (proving) the results he will use, it is because the techniques of proving already-established results are also the techniques he will need in using his new-found mathematics that he does need to learn about the techniques of proof, and about proof itself. The subject of proof is therefore an important starting point for many service courses. Not only should the concept of proof be discussed, but also the importance of proof and the need for it, as well as illustration of some of the widely-used methods of proof. This paper summarizes ideas that have been used in this manner for the past decade in a service course in elementary matrix algebra. Use of them has greatly reduced the difficulties that were previously manifest when students were simultaneously learning about matrices and about mathematical proof.

The nature of proof

Proof, in the mathematical sense, is described in Webster's dictionary as being "that degree of cogency, arising from evidence, which convinces the mind of any truth or fact and produces belief". Three aspects of this definition merit attention. First, proof is "a degree of cogency ... which convinces the mind". Second, the act of convincing the mind must arise "from evidence"; and third, the whole procedure must "produce belief" in the "truth or fact". On the importance of proof to mathematics Bell [1940] writes "without deductive proof, from admitted assumptions, explicitly stated as such, mathematics does not exist". Note the involvement of deduction here, deduction being defined by Webster as "reasoning from given premises to necessary conclusions". The "given premises" upon which the reasoning is to be based are Bell's "admitted assumptions" which, if not explicitly stated, must at the very least be implicitly understood. In

either case, these assumptions are the evidence from which the act of convincing the mind, in the Webster definition, must arise.

Proof is based upon knowledge (the "admitted assumptions" of Bell), and knowledge changes over time. Hence proof is a living process and is not impervious to time. For example, a Babylonian would have proven that the root of the equation $x^2 - x - 12 = 0$ is $x = 4$, perhaps by observing that $4^2 - 4 - 12 = 0$. He would not have known of the root $x = -3$, because in Babylonian times negative numbers were unknown, a belief that existed into the 16th Century when Cardan still described negatives as fictitious. That proof is not impervious to time is also in keeping with the Webster definition which ends with the injunction that proof "produces belief". The Babylonian did not know about negative numbers and when, centuries later, people did believe in them only then could they believe that $x = -3$ is also a root. In this way, proof is a living process.

Proof is seldom a unique procedure. More accurately, there is seldom just one way of proving a true proposition. Proving that $(x-2)(x+2)$ equals $x^2 - 4$ is a simple example: $(x-2)(x+2)$ can be expressed either as $x(x+2) - 2(x+2)$ or as $(x-2)x + (x-2)2$ and both of these expressions simplify to the desired result. Thus, although proof is the process which "convinces the mind" of a truth and therefore has a unique ending, it does not necessarily involve a unique procedure in any particular situation.

Since there may be several proofs of a proposition, it is natural that some get to be described as good and others as bad. A good proof is usually one that is clear and concise, for mathematicians generally admire both clarity and brevity. A bad proof may not have these characteristics, but it is not a wrong proof. Indeed, by the literal meaning of the word "proof" there can be no such thing as a wrong proof. What we are prone to call a wrong proof is a procedure

or line of argument which seeks to "convince the mind" of a truth but which fails to do so. It is therefore no proof at all and so should really be called a non-proof, not a wrong proof.

The need for proof

A powerful feature of mathematics is that it speaks in generalities. In this context, proof provides us with at least three basic needs: convenience, progress, and safety.

Practical convenience

Consider calculating the area of a rectangular field that is 3 miles long and 2 miles wide. We could mark off individual miles on each side, superimpose a grid, and count the 6 individual square miles. Such counting would be tedious for large fields. Nevertheless, for fields of any length ℓ and width w where ℓ and w are both integers, it is certainly feasible; and the area is ℓw. But what if ℓ and w were not integers; e.g., a field $3\frac{1}{3}$ by $2\frac{1}{2}$? Its area could not be counted in units of a square mile. However, we could then say that the field is 20/6 × 15/6, measure off each side in units of 1/6'th, and count the area as 20 × 15 squares of area 1/36, thus ascertaining the total area to be 300/36 = $8\frac{1}{3}$ square miles. Obviously this is tedious compared to knowing (as we do) that a rectangle of length ℓ and width w always has area ℓw no matter what the values of ℓ and w are, be they integer, rational or irrational. Here is the practical convenience of proof: having once proven that a general rectangle of length ℓ and width w has area ℓw, we can use this result endlessly, without having to prove it again. Once "that degree of cogency" is achieved "which convinces the mind of" the truth of this result "and produces belief" in it,

we can rely upon the result and use it without fear of contradiction. This is the benefit of convenience which proof, combined with the generality of mathematics, provides: we are supplied with results that can be used repeatedly in varied situations with complete assurance of their validity.

Progress

Proof is the basis for growth and development of mathematics. This is not to deny, of course, the value to mathematics of intuition, experience, and just plain guessing. These are all important elements in mathematical development. But as Bell tells us, it is proof which ties these elements together, for "deductive proof is the criterion by which 'guessing' (by whatever name it is dignified) is judged to be or not to be mathematics". One might say that although proof is not the fire that kindles the imagination which contributes so greatly to advances in mathematics, it is the substance upon which development progresses. It is the foundation for each successive new step. It does not of itself provide new steps, but at any point in time it is the means by which all preceding steps have become accepted, and upon which a new step forward can then safely be built. The order of progress is: observations, hunch (intuition or imagination) leading to conjecture and then proof; more observations, imagination and conjecture, and then proof ... and so on. When proof of a conjecture is established that conjecture becomes an accepted fact and can be used as a foundation for a next conjecture. Thus is progress made.

Safety

The designer of a cantilevered balcony uses mathematical proof to convince himself that his structure will not collapse. This need for proof is all too clear. Equally as important is the need in the development of mathematics to be

sure that there are no hidden falsehoods. In particular we must not let mere illustrations deceive us as being proof. For example, Figure 1 represents an 8 × 8 square cut into 4 pieces;

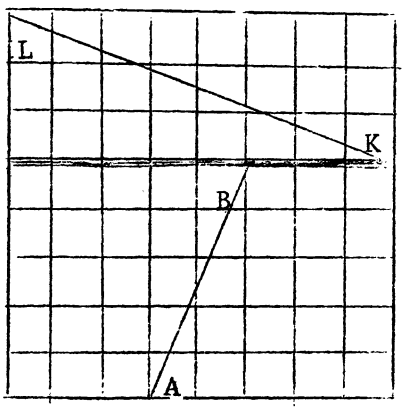

Figure 1

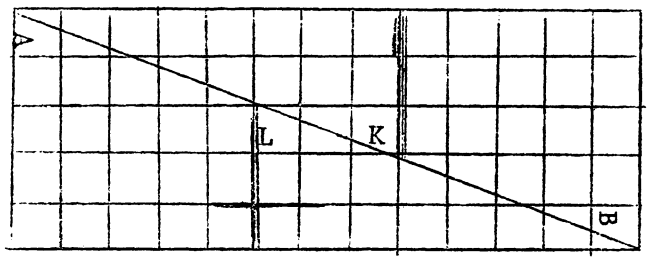

Figure 2

and Figure 2 shows those pieces fitted together again to form a 5 × 13 rectangle. Does this prove that 64 = 65? Clearly not, for it would contradict our whole number system. It is therefore necessary to prove that Figure 2 cannot be derived from Figure 1. A proof is not difficult, and serves as a nice example of the need for proof to safeguard against the deficiencies of its weakling cousin "demonstration".

Methods of proof

Organizing a proof

One aspect of proof in algebraic work that sometimes confuses students is the organization of the actual steps involved. Appeal to a traditional presentation of proof in Euclidean geometry can often be helpful in alleviating this confusion. First recall, perhaps by use of the trite schoolboy mnemonic "Don't talk constant piffle", that four familiar headings are (i) Data (or what is given): the assumptions, axioms and definitions stated or implied, (ii) To prove: the

proposition whose verity we hope to establish (iii) Construction: artifacts that will help in establishing a proof, often the formal expression of known facts or data such as "let n = 2p+1" when n is known to be an odd number, and (iv) Proof: deductive use of the data and construction to "convince the mind" of the truth of the proposition.

Although these four steps of a proof are familiar in Euclidian geometry they are also implicit in algebra and analysis. An illustration emphasizes the formal logic that is needed in algebra just as in geometry. For example, consider proving "the rule of 4": that any integer whose right-hand 2 digits form a 2-digit integer that is divisible by 4 is itself divisible by 4. (i) The data are definitions of integer, of digit and of "divisible by 4". (ii) To prove "the rule of 4" is our task. (iii) Construction is to let N be any integer, to let β and γ each be any digit 0, 1, 2, ..., or 9, and to let α be zero or some integer. Then for appropriate α, β and γ, we can write N as $N = 100\alpha + 10\beta + \gamma$. (iv) Proof is now simple: $N/4 = (100\alpha + 10\beta + \gamma)/4 = 25\alpha + (10\beta + \gamma)/4$ which is integer if $(10\beta + \gamma)/4$ is. As a formal ending to a proof we could write Q.E.D., for "quad erat demonstrandum" as the Roman would have said, or for "quite easily done" as the schoolboy now puts it.

Perhaps student confusion in organizing algebraic proofs arises from omissions in the literature. Not only is there an absence of the formal structure just discussed but also of steps (i) and (iii), Data and Construction. This is because data may be more implicit in analytic situations than in Euclidean geometry, and so are less likely to be stated explicitly; and such statements as "let N be an integer" may not be recognizable as construction in the sense used in geometry. Nevertheless, these reminders can help students gain

appreciation of proof in algebra, from seeing the connection to proof in geometry, which is (presumably) a familiar context.

The fallacy of "if p implies q then q implies p"

The following "proof" has been seen in student work on many occasions.

Prove: For real numbers y and k,

$$(y^2 - k^2)(y + 4k) = (y + k)(y^2 + 3ky - 4k^2) \tag{1}$$

"Proof":

$$(y^2 - k^2)(y + 4k) = (y + k)(y^2 + 3ky - 4k^2) \tag{2}$$

$$\therefore y^3 + 4ky^2 - k^2y - 4k^3 = y^3 + 3ky^2 - 4k^2y + ky^2 + 3k^2y - 4k^3$$

$$\therefore y^3 + 4ky^2 - k^2y - 4k^3 = y^3 + 4ky^2 - k^2y - 4k^3 \tag{3}$$

$$\therefore 0 = 0 \qquad \text{Q.E.D.} \tag{4}$$

The algebra is correct. But as a general method of proof the logic which ends with $0 = 0$ is not universally valid. Consider the following example.

Prove: $$9 = 4 \tag{5}$$

"Proof": $$9 = 4 \tag{6}$$

$$\therefore -9 = -4 \tag{7}$$

$$\therefore 9 - 9 = 4 - 4 \tag{8}$$

$$\therefore 0 = 0 \qquad \text{Q.E.D.} \tag{9}$$

The unreasonableness of the proposition $9 = 4$ shows that something about this "proof" must be wrong. And yet, on applying to (6) and (9) the same argument as

was used on (2) and (4) we would have to conclude that (6) is true. In each case we have developed a statement q (namely 0 = 0) as a consequence of some statement p, and used this to argue that p is a consequence of q. Using => for "implies" we have used the argument "if p => q then q => p". It is an argument that is not universally valid.

In one case the argument works and in the other it does not. What then is the difference between the two "proofs"? It is the concept of reversibility. Any time we try to use p => q as an argument to support q => p, each step used in proving p => q must be reversible in order to conclude that q => p. In the second case this reversibility does not exist. The argument going from (6) to (9) contains a step which is not reversible when trying to argue in reverse from (9) to (6), namely the step between (7) and (8). Going from (7) to (8) is valid, but from (8) to (7) is not. (If it were then 15 - 12 = 26 - 23 would imply 15 = 26 and -12 = -23; but the laws of algebra allow no such conclusions.) Hence the logic implied in trying to conclude from (6) => (9) that (9) => (6) breaks down; i.e., (9) does not => (6).

The "proof" between (6) and (9) clearly had to be false and we have seen that it is on grounds of irreversibility. However, the "proof" between (2) and (4) has no obvious falsity and indeed no irreversibility. All steps going from (4) back to (2) are valid. Thus (4) => (2), but it does so <u>not</u> because (2) => (4) [an argument which (6) and (9) show is not always valid] but because the individual steps back from (4) to (2) <u>are</u> valid; i.e., the factorizations evident in going from (2) to (4) can also be validly done in reverse order. The proof of (2) depends only on these, not upon 0 = 0, and should therefore be re-arranged solely

in terms of these factorizations, excluding 0 = 0. The re-arranged proof would then not even appear to depend on the "if p => q then q => p" fallacy.

It is unfortunate that irreversible steps are not always so easily identifiable as is that between (7) and (8). Consider the following example in matrix algebra.

Prove:
$$\begin{bmatrix} 6 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 6 \end{bmatrix}$$

"Proof":
$$\begin{bmatrix} 6 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} \begin{bmatrix} 6 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 4 & 6 \end{bmatrix}$$

i.e.
$$\begin{bmatrix} 10 & 13 \\ -10 & -13 \end{bmatrix} = \begin{bmatrix} 10 & 13 \\ -10 & -13 \end{bmatrix}$$

Only if the irreversibility of the multiplication by $\begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix}$ is recognized will the invalidity of this kind of "proof" be apparent. This is true generally, and is the reason why the form of "proof" between (2) and (4) should not be used. If reversibility exists, the "proof" can be reorganized to remove its apparent dependence on the "if p => q then q => p" fallacy; and if reversibility does not exist then the "proof" is no proof at all.

The starting point of this method of "proof" is that of writing down p, the statement which we wish to prove. This is tantamount to saying "Assume p". Although the end point q of the "proof" is the obvious truth 0 = 0 it is the

principle of reversibility which prevents us from always implying that p is true. But suppose the end point q turns out to be 0 = 17, or some other contradiction. On presuming the argument for p => q to be valid, finding q to be false removes the desire for trying to show q => p, and so reversibility is not involved. The only conclusion is that p is false. This is the basis of proof by contradiction. (See method 12 in the list which follows.)

Some elementary methods of proof

Having decried a popular student form of "proof" we list some widely-used, simple and valid methods of proof, dealing first with establishing equality of two expressions, x and y.

1. Manipulate x until it becomes y.

2. Manipulate x until it becomes t say; then manipulate y until it also becomes t.

3. Manipulate the difference x - y until it becomes zero.

4. If $y \neq 0$, manipulate x/y until it becomes unity.

5. For an appropriately chosen $m \neq 0$, manipulate $[(x + m) - m]$ until it becomes y. This is the well known method of "add and subtract".

6. For an appropriately chosen $k \neq 0$, manipulate xk/k until it becomes y.

7. When x has the form t/s, manipulate sy until it becomes t.

More general methods of proof include the following.

8. Proof by "construction": introduce equations to represent available data.

9. Proof by substitution: useful in solving equations, where intelligent guessing sometimes locates a solution.

10. Proof by induction: useful in situations that depend on the sequence of integers. This is often found to be a difficult form of proof to understand, when first encountered.

New developments in mathematics are often achieved through repeated use of observations, conjecture and proof, as described earlier. In this context, although not confined to it, the following two methods of proof find considerable use.

11. Proof by exhaustion: a conjecture can be proven by illustrating its truth for all possible special cases to which it applies.

12. Proof by contradiction (sometimes also called proof by reductio ad absurdum). The conclusion from p => q and q being false is that p is false - as has been discussed. Thus any special case of a conjecture that leads to a contradiction, or which contradicts the conjecture, is sufficient to conclude that the conjecture is false. (For example, n = 4 proves the falsity of the conjecture that $2^n - 1$ is prime.)

Insofar as establishing proof by the use of examples is concerned, notice that a true conjecture can be proven not by a single example or even a few examples but only by using all possible examples; this is proof by exhaustion. When there is an infinite number of such examples then some other method of proof must be used. In contrast, to disprove a conjecture which is indeed false, it takes only a single example, namely one that contradicts the conjecture; this is proof by contradiction. In terms of the development of new mathematics through time, if such an example can be exhibited promptly after posing the conjecture then its falsity and rejection become evident just as promptly. In this way, establishing the falsity of false conjectures often occurs more quickly than

proving the validity of true ones. Fermat's conjecture is a time-honoured illustration.

These twelve methods of proof are only a selection from the many available, but they form a useful nucleus for students - especially students from applied disciplines taking their first service courses in mathematics.

Acknowledgment

Thanks go to D. L. Solomon for profitable discussions on reversibility.

Reference

Bell, E. T. (1940). The Development of Mathematics. McGraw-Hill, New York and London.