Forms of Argument (Part II)

Saeed Kazem

Amirkabir University of Technology

May 22, 2019

A proof by contradiction of a proposition P consists of assuming $\neg P$ and deducing a false statement:

$$\neg P \Rightarrow \texttt{FALSE}.$$

The false statement could be anything, including any assertion that contradicts the assumption $\neg P$.

Theorem 7.1. The number of primes is infinite.

`PROOF BY CONTRADICTION.` Assume there are only finitely many primes, $p_1, \ldots, p_n$. **Follow out.**

To apply the method of contradiction to an implication $P \Rightarrow Q$, we assume the negation of the implication, namely $\neg(P \Rightarrow Q)$. By Theorem 4.1, this is equivalent to $P \wedge \neg Q$, so our proof amounts to establishing that

$$(P \wedge \neg Q) \Rightarrow \texttt{FALSE}.$$

This form of proof by contradiction is called the **both ends method**: to prove that if P then Q, we assume both P and not–Q, and we deduce something impossible.

Suppose that a statement concerning all elements of a set is false. To prove this, is sufficient to exhibit a single element of that set for which the statement fails. This argument is called a **counterexample**.

In symbols, we show that the statement

$$\forall x \in X,\ \mathcal{P}(x)$$

is false by proving its negation, namely

$$\exists x \in X,\ \neg\mathcal{P}(x).$$

Conjecture 1. *For all integers n, $p(n) = n^2 + n + 41$ is prime.*

A conjecture is a statement that we wish were a theorem. Three things may happen to a conjecture:
(i) someone proves it, and the conjecture becomes a theorem;
(ii) someone produces a counterexample, and the conjecture is proved false;
(iii) none of the above, and the conjecture remains a conjecture.

Which one is our case?

Conjecture 2. *For all but finitely many integers n, $p(n)$ is prime.*

Conjecture 3. *There are infinitely many integers n such that $p(n)$ is prime.*

Conjecture 4. *There are infinitely many primes p such that $p + 2$ is also prime.*

Conjecture 5. *Every even integer greater than 2 can be written as a sum of two primes.*

In constructing a mathematical argument it's easy to make mistakes. In this section we identify some common faulty arguments: confusing examples with proofs, assuming what we are supposed to prove, mishandling functions. Awareness of these problems should help us in avoiding them.

The verification of a statement in specific cases does not constitute a form of proof.

Theorem. For all primes p, the integer $2p-2$ is divisible by p.

`WRONG PROOF.`

$$2^2-2=2\cdot 1, \quad 2^3-2=3\cdot 2, \quad 2^5-2=5\cdot 6, \quad 2^7-2=7\cdot 18, \text{etc.} \qquad \square$$

The theorem has been proved only for $p=2,\ 3,\ 5,\ 7$.

Theorem. For all $x,\ y$ and z, if $x+y<x+z$ then $y<z$.

`WRONG PROOF.` Suppose $x+y<x+z$. Take $x=0$. Then

$$y=0+y<0+z=z. \qquad \square$$

The mistake here is that we took x to be 0, which is a special value of x.

Inappropriate handling of implications results in common mistakes. Instead of proving an implication, we may end up proving its converse; or we may assume the statement we are meant to prove, deduce from it a true statement, and believe we've completed the proof. These faulty deductions—of which we now show an example—are sometimes called circular arguments.

Prove that $\sqrt{2}+\sqrt{6}<\sqrt{15}$

`WRONG PROOF.`

$$\begin{aligned}\sqrt{2}+\sqrt{6}<\sqrt{15} &\Rightarrow (\sqrt{2}+\sqrt{6})^2<15\\ &\Rightarrow 8+2\sqrt{12}<15\\ &\Rightarrow 2\sqrt{12}<7\\ &\Rightarrow 48<49. \qquad \square\end{aligned}$$

We were supposed to prove P, where $P=(\sqrt{2}+\sqrt{6}<\sqrt{15})$. Instead we have assumed P, and correctly deduced from it the true statement $48<49$. However, the deduction $P\Rightarrow \texttt{TRUE}$ (unlike the deduction $P\Rightarrow \texttt{FALSE}$) gives us no information about P. Indeed, had we started from the false statement$\sqrt{2}+\sqrt{6}<-\sqrt{15}$, we would have reached exactly the same conclusion.

There are two methods for fixing this problem.

First method: retracing the steps. We regard the chain of deductions displayed above as 'rough work'; then we start from the end and prove the chain of converse implications.

PROOF.

$$\begin{aligned}
48 < 49 \ &\Rightarrow \ \sqrt{48} < \sqrt{49} \\
&\Rightarrow 2\sqrt{12} < 7 \\
&\Rightarrow 8 + 2\sqrt{12} < 15 \\
&\Rightarrow (\sqrt{2} + \sqrt{6})^2 < 15 \\
&\Rightarrow \sqrt{2} + \sqrt{6} < \sqrt{15}
\end{aligned}$$

where in the first and the last implications we have taken the positive square root of each side. We have proved the implication TRUE$\Rightarrow$ P, from which we deduce that P is TRUE.$\Box$

Second method: contradiction.

`PROOF`. Let us assume $\neg P$:

$$\begin{aligned}\sqrt{2}+\sqrt{6} \geq \sqrt{15} &\Rightarrow (\sqrt{2}+\sqrt{6})^2 \geq 15 \\ &\Rightarrow 8+2\sqrt{12} \geq 15 \\ &\Rightarrow 2\sqrt{12} \geq 7 \\ &\Rightarrow 48 \geq 49.\end{aligned}$$

We have proved that $\neg P \Rightarrow$FALSE, which implies that $\neg P$ is FALSE, that is, P is TRUE. $\square$

Many things can go wrong when we deal with functions. For instance, we may apply a function to arguments outside its domain, or invert a function incorrectly (e.g., taking the wrong sign of a square root).

We begin with a proof from calculus which isn't correct, even if it captures the essence of the argument. The chain rule for differentiating the composition of two functions states that if f and g are differentiable, then

$$(g \circ f)'(x) = g'(f(x))f'(x).$$

SLOPPY PROOF. Let ε be a real number. We compute

$$\frac{g(f(x+\varepsilon)) - g(f(x))}{\varepsilon} = \frac{g(f(x+\varepsilon)) - g(f(x))}{f(x+\varepsilon) - f(x)} \times \frac{f(x+\varepsilon) - f(x)}{\varepsilon}.$$

Letting ε tend to zero gives the desired result. $\square$

The right-hand side is obtained by multiplying and dividing by $f(x+\varepsilon)-f(x)$. But this quantity may well be zero for non-zero ε (e.g., if f is constant), which invalidates the argument. A valid proof requires more delicacy.

PROOF. Let $y = f(x)$. Since g is differentiable at y, we write

$$g(y+\delta)-g(y) = g'(y)\delta + h(y,\delta)\delta$$

where h is a continuous function with $h(y,0)=0$.
Specialising to $\delta = f(x+\varepsilon)-f(x)$, we find

$$\begin{aligned}\frac{g(f(x+\varepsilon))-g(f(x))}{\varepsilon} =& g'(f(x))\frac{f(x+\varepsilon)-f(x)}{\varepsilon}\\ & h(y, f(x+\varepsilon)-f(x))\frac{f(x+\varepsilon)-f(x)}{\varepsilon}.\end{aligned}$$

As ε tend to zero, the last term tends to zero, being the product of a function that tends to zero and a function that tends to a finite limit (because f is differentiable). This gives the desired result.

WRONG THEOREM. *Every negative real number is positive.*

WRONG PROOF. Let α be a negative real number. Then

$$\alpha = -|\alpha| = (-1)^1|\alpha| = (-1)^{2\cdot\frac{1}{2}}|\alpha| = [(-1)^2]^{\frac{1}{2}}|\alpha| = |\alpha| > 0. \quad \square$$

What's wrong with this proof?

Proofs come in all shapes and sizes. Correctness is, of course, imperative, but a good proof requires a lot more since the conflicting requirements of clarity and conciseness must be resolved. The level of exposition and the amount of detail will depend on the mathematical maturity of the target audience. There is one general rule, to be applied at all key junctures in a proof:

- `Say what you plan to do.`
- `When you've done it, say so.`

We now examine statements of theorems and proofs that are less than optimal, and we improve them.

BAD THEOREM. *If* $x^2 \neq 0$, *then* $x^2 > 0$.

BAD PROOF. If $x > 0$ then $x^2 = xx > 0$. If $x < 0$ then $-x > 0$, so $(-x)(-x) > 0$, i.e., $x^2 > 0$. $\square$

The statement of the theorem is incomplete, in that there is no information about the quantity x. Furthermore, this is a proof by cases (see Sect. 7.2), and it would be helpful if this were made explicit.

THEOREM. *For all real numbers* x, *if* $x^2 \neq 0$, *then* $x^2 > 0$.

PROOF. Let x be a real number such that $x^2 \neq 0$. Then $x \neq 0$, and we have two cases:

(i) $x < 0$. Then $-x > 0$, so $(-x)(-x) > 0$, that is, $x^2 > 0$.
(ii) $x > 0$. Then $xx = x^2 > 0$. $\square$

BAD THEOREM. $\forall a, b \in \mathbb{R},\ (a \in \mathbb{Q} \wedge b \notin \mathbb{Q}) \Rightarrow a + b \notin \mathbb{Q}$.

BAD PROOF. Suppose $a + b \in \mathbb{Q}$. Then $a + b = m/n$.
If $a \in \mathbb{Q}$, then $a = p/q$, and $b = m/n - p/q \in \mathbb{Q}$. □

The symbolic formulation of the theorem obscures its simple content. The proof is straightforward, but the use of unnecessary symbols and the lack of comments make it less clear than it should be.

THEOREM. *The sum of a rational and an irrational number is irrational.*

PROOF. Let a and z be a rational and an irrational number, respectively. Consider the identity $z = (a + z) - a$. If $a + z$ were rational, then z, being the difference of two rational numbers, would also be rational, contrary to our assumption. Thus $a + z$ must be irrational. □

BAD THEOREM. n *odd* $\Rightarrow 8|n^2-1$.

BAD PROOF.
Suppose $a+b\in\mathbb{Q}$. n *odd* $\Rightarrow \exists j\in\mathbb{Z},\; n=2j-1$;
$\therefore n^2-1=4j(j+1)$;
$\forall j\in\mathbb{Z},\; 2|j(j+1)\Rightarrow 8|n^2-1$. $\square$

This is a clumsy attempt to achieve conciseness via an entirely symbolic exposition. Combining words and symbols and adding some short explanations will improve readability and style. We shall see that a clearer proof need not be longer.

THEOREM. *The square of an odd integer is of the form $8n+1$.*

PROOF. An odd integer k is of the form $k=2j+1$, for some integer j. A straightforward manipulation gives $k^2=4j(j+1)+1$. Our claim now follows from the observation that the product $j(j+1)$ is necessarily even. $\square$

Exercise 8

Exercise 7.1 You are given cryptic proofs of mathematical statements. Rewrite them in a good style, with plenty of explanations.

1. *Prove that the line through the point* $(4, 5, 1) \in \mathbb{R}^3$ *parallel to the vector* $(1, 1, 1)^T$ *and the line through the point* $(5, -4, 0)$ *parallel to the vector* $(2, -3, 1)^T$ *intersect at the point* $(1, 2, -2)$. (The symbol T denotes transposition.)

   BAD PROOF.

$$
\begin{aligned}
&(4,5,1)^T + \lambda\,(1,1,1)^T = (4+\lambda, 5+\lambda, 1+\lambda)^T; \\
&\quad = (5,-4,0)^T + \mu\,(2,-3,1)^T = (5+2\mu, -4-3\mu, \mu)^T. \\
&\therefore\ 4+\lambda = 5+2\mu,\ 5+\lambda = -4-3\mu,\ 1+\lambda = \mu. \\
&\Rightarrow\ 4+\lambda = 5+2(1+\lambda) \ \Rightarrow\ \lambda = -3,\ \mu = -2. \\
&\therefore\ \mathbf{v} = (1,2,-2)^T.
\end{aligned}
$$

□

2. *Prove that the real function $x \mapsto 3x^4 + 4x^3 + 6x^2 + 1$ is positive.*
   BAD PROOF.

   $f'(x) = 12x(x^2 + x + 1) = 0 \Leftrightarrow x = 0;$
   $f''(0) > 0,\ f(0) > 0 \Rightarrow$ positive. $\square$

3. *Prove that for all real values of a, the line*

$$y = ax - \left(\frac{a-1}{2}\right)^2$$

   is tangent to the parabola $y = x^2 + x$.
   BAD PROOF.

   $ax - (a-1)^2/4 = x^2 + x;$
   $\Rightarrow x^2 + x(1-a) + (a-1)^2/4 = 0;$
   $\Rightarrow x = (a-1)/2.$
   For this x, $\mathrm{d}y/\mathrm{d}x$ is the same. $\square$

Exercise 7.2 The following text has several faults: (a) explain what they are; (b) write an appropriate revision.

WRONG THEOREM. *For all numbers x and y,*

$$\frac{x^2 + y^2}{|xy|} > 2.$$

WRONG PROOF. For

$$\begin{aligned} \frac{x^2 + y^2}{|xy|} > 2 &\Rightarrow x^2 + y^2 > 2xy \\ &\Rightarrow x^2 - 2xy + y^2 > 0 \\ &\Rightarrow (x - y)^2 > 0. \end{aligned}$$

The last equation is trivially true, which proves it. □

Exercise 7.4 Write the first few sentences of the proof of each statement, introducing all relevant notation in an appropriate order, and identifying the RTP.

1. On a compact set every continuous function is uniformly continuous.

Let X be a compact set, and let f be a continuous function over X. RTP: f is uniformly continuous.

2. Every valuation of a field with prime characteristic is non-archimedean.
3. No polynomial with integer coefficients, not a constant, can be prime for all integer values of the indeterminate.
4. A real function continuous in a closed interval attains all values between its maximum and minimum.
5. A subset of a metric space is open if and only if its complement is closed.