What is (in) a proof?

Bas Luttik

November 20, 2009

A *proof* of some precise (usually mathematical) statement is a convincing argument that the statement is true.

In the first part of the course[1], the statements to be proved were given in the form of abstract logical formulas. Whenever a proof of the truth of a formula was requested, it was always made very precise what we would accept as a proof: we either asked for a *calculation* (a proof according to the methods discussed in part I of the book [1]) or for a *derivation* (a proof according to the methods discussed in part II of the book [1]).

In the second part of the course[2], the statements to be proved were still formulated as logical formulas, expressing general facts about sets, relations and functions. When proving them, there was a lot more freedom: as proofs we accepted any combination of methods from part I and part II of the book [1], as long as it represented a logically correct reasoning and as as long as it was clear which method was applied where.

There is a great advantage of requiring proofs to be presented in a precisely specified format such as a calculation or a derivation: as soon as one has agreed on the rules and on how to use them, then it is clear what constitutes a correct proof (i.e., a convincing argument) and what does not.[3] But there are also disadvantages; we mention two:

1. A proof presented as a derivation puts a lot of emphasis on standard logical reasoning, and this often distracts from the crux of the argument.

2. The statement to be proved and other notions involved in the proof, may not be presented as logical formulas. It can be quite cumbersome to translate them into logical formulas that can be used in a derivation.

If the goal is to convince another person with sufficient knowledge of logical reasoning that some statement is true, then there is usually no need to first translate the statement into a logical formula and to present the reasoning as a derivation. In fact, this is then usually undesirable, since most people prefer to read text rather

[1] the part about Chapters 1–15 of the book [1]

[2] the part about Chapters 16–18 of the book [1]

[3] Incidentally, to be able to work within a formal framework and stick precisely to the rules of the framework is an important skill.

than logical formulas, and most people prefer a textual presentation of a reasoning over a derivation. Of course, although statements in a textual presentation of a proof are not (all) formulated as formulas, they should nevertheless be so precise that, perhaps with some effort, it would be possible to translate them into logical formulas. Furthermore, the proof, even if it is not completely explicit about which logical rule is applied when, should convey sufficient information about the logical structure of the reasoning.

In the last part of the course, we encourage you to present proofs in a textual fashion, putting less emphasis on the rules for standard logical reasoning that you have learned in blocks A and B. (Of course, to be able to deliver a logically correct reasoning you still need to be aware of those rules and know how to apply them, but when you present your proof you need not mention them explicitly). We shall illustrate the notion of 'textual proof' in the remainder of this document by discussing an example. Let us prove the following statement:

> Any integer postage greater than 7 cents can be formed by using only 3-cent and 5-cent stamps.

We first give a textual proof, and then present the same reasoning in the form of a derivation.

A textual proof

Proof. We prove the statement with induction on $b > 7$.

(Basis) If $b = 8$, then b can be formed with one 3-cent stamp and one 5-cent stamp.

(Step) Let b be an arbitrary postage greater than 7 and suppose that b can be formed using only 3-cent and 5-cent stamps (the Induction Hypothesis). Clearly, the formation of the postage b either *does* or *does not* include a 5-cent stamp. To prove that also $b + 1$ can be formed using only 3-cent and 5-cent stamps, we distinguish these two cases:

Case 1: Suppose that the formation of the postage b, which exists by the Induction Hypothesis, *does* include a 5-cent stamp. Then we can form the postage $b + 1$ by replacing, in the formation of b, one 5-cent stamp by two 3-cent stamps.

Case 2: Suppose that the formation of the postage b, which exists by the Induction Hypothesis, *does not* include a 5-cent stamp. Then it consists entirely of 3-cent stamps, and hence, since $b > 7$, it must include at least three 3-cent stamps. By replacing, in the formation of b, three 3-cent stamps by two 5-cent stamps, we form the postage $b + 1$.

Thereby, the statement is proved. □

We make a few comments about the statement and its textual proof:

1. Note that the statement to be proved is actually a universal quantification in disguise; we want to prove a property *for all* amounts of postage greater than 7.

2. We have learned two methods to prove a universally quantified predicate over a domain consisting of all integers from some starting point. The first method is to prove the predicate for some arbitrary integer about which we assume nothing else than that it is in the domain, and then apply the $\forall$-intro rule. The second method is to apply (some form of) induction. Our textual proof begins with the announcement that we choose the latter.

3. A proof by induction of some universally quantified predicate consists of two parts. The first part, referred to as the (Basis), consists of establishing that the predicate holds for the smallest number in the domain of the universal quantification, which is 8 in this case. The second part, referred to as the (Step), consists of establishing that, for all b in the domain, if the predicate holds for b, then it also holds for $b + 1$.

   Note that (Step) involves another universal quantification: we have to show that if b can be formed then so can $b + 1$ *for all* $b > 7$. Note that the explicit universal quantification is omitted from our textual proof. We deal with it by means of the first method we have learned for proving universal quantification: the $\forall$-intro rule. Recall that this involves the declaration of an arbitrary b in the domain (i.e., an integer b such that $b > 7$), which is done explicitly in our textual proof with the statement "let b be an arbitrary postage greater than 7". The application of $\forall$-intro itself, however, is not mentioned explicitly in our textual proof; it is assumed that anyone with sufficient knowledge of standard logical reasoning will know that proving the universally quantified statement can be done by proving the statement for the arbitrary integer $b > 7$ declared in the proof.

   For the declared b we need to prove an implication: if the predicate holds for b, then it also holds for $b + 1$. For implications we know just one method: $\Rightarrow$-intro. So, we assume the left-hand side of the implication, and prove the right-hand side. The assumption is called the Induction Hypothesis and it is important to state it clearly. In our textual proof above, the Induction Hypothesis is introduced with the phrase

   > "suppose that b can be formed using only 3-cent and 5-cent stamps".

4. The remainder of the proof consists of an application of case distinction. Recall that a very important prerequisite for correctly applying case distinction is that the disjunction of the cases is a true statement (in the context of the proof). Here, the disjunction corresponds with the obvious fact that the formation of the postage b using only 3-cent and 5-cent stamps either does or does not include a 5-cent stamp. Here, for clarity, we have mentioned this obvious fact before the case distinction, but, since it is so obvious, we could also have chosen to leave it implicit. By the remark that we distinguish two cases, it is already

implied that the disjunction of the cases we are going to mention is indeed true.

5. Note that the proof of (BASIS) is straightforward: the postage b considered is concrete ($b = 8$), so we can just say which combination of 3-cent and 5-cent stamps does the job. The proof of (STEP) is more involved. The idea is that we already know by the INDUCTION HYPOTHESIS that a postage b can be formed using only 3-cent and 5-cent stamps, and using this combination of stamps we can make a proper combination of stamps for $b + 1$. This is actually the crux of the proof, the main crucial idea.

A derivation

We shall now also present the reasoning in the textual proof as a derivation. To be able to do so, we need to reformulate the statement to be proved as a formula. First observe that it is irrelevant that the statement is about 'postage'; we can reformulate it as the (more general) purely mathematical statement: for every integer b greater than 7 there exist natural numbers k and l such that $b = k \cdot 3 + l \cdot 5$. Now this mathematical statement corresponds with the formula

$$\forall_b[b \in \mathbb{Z} \wedge b > 7 : \exists_{k,l}[k, l \in \mathbb{N} : b = k \cdot 3 + l \cdot 5]] \ .$$

Before we give our derivation, it is convenient to introduce an abbreviation for the existential quantification: we define the one-place predicate P on integers by

$$P(b) := \exists_{k,l}[k, l \in \mathbb{N} : b = k \cdot 3 + l \cdot 5] \ .$$

We now give a derivation of the formula $\forall_b[b \in \mathbb{Z} \wedge b > 7 : P(b)]$.

{ Mathematics: }

$8 = 1 \cdot 3 + 1 \cdot 5$

{ $\exists^*$-intro (2×) + Def. P: }

$P(8)$

var $i; i \in \mathbb{Z} \wedge i \geq 8$

| $P(i)$

| { Def. P + $\exists^*$-elim (2×) }

| Pick $k, l \in \mathbb{N}$ with $i = k \cdot 3 + l \cdot 5$

| { Mathematics ($l \in \mathbb{N} \stackrel{val}{\Longrightarrow} l = 0 \vee l > 0$): }

(1) | $l = 0 \vee l > 0$

$\boxed{l = 0}$

{ Mathematics: }

$i + 1 = (k \cdot 3) + 1 = (k - 3) \cdot 3 + 10 = (k - 3) \cdot 3 + 2 \cdot 5$

{ Mathematics (if $k \cdot 3 = i \geq 8$, then $k \geq 3$): }

$(k - 3), 2 \in \mathbb{N}$

{ $\exists^*$-intro ($2\times$) + Def. P: }

$P(i + 1)$

(2) $l = 0 \Rightarrow P(i + 1)$

$\boxed{l > 0}$

{ Mathematics: }

$i + 1 = (k \cdot 3 + l \cdot 5) + 1 = k \cdot 3 + (l - 1) \cdot 5 + 6 = (k + 2) \cdot 3 + (l - 1) \cdot 5$

$(k + 2), (l - 1) \in \mathbb{N}$

{ $\exists^*$-intro ($2\times$) + Def. P: }

$P(i + 1)$

(3) $l > 0 \Rightarrow P(i + 1)$

{ Case distinction on (1), (2) and (3): }

$P(i + 1)$

$P(i) \Rightarrow P(i + 1)$

$\forall_i[i \in \mathbb{Z} \wedge i \geq 8 : P(i) \Rightarrow P(i + 1)]$

{ Induction from the integer 8: }

$\forall_b[b \in \mathbb{Z} \wedge b \geq 8 : P(b)]$

{ Mathematics ($b \in \mathbb{Z} \wedge b \geq 8 \stackrel{val}{=\!=} b \in \mathbb{Z} \wedge b > 7$): }

$\forall_b[b \in \mathbb{Z} \wedge b > 7 : P(b)]$

References

[1] Rob Nederpelt and Fairouz Kamareddine. *Logical Reasoning: A First Course*, volume 3 of *Texts in Computing*. King's College Publications, 2004.