An introductory example

The purpose of this chapter is to give the reader some idea of what he can expect to find in this book. To this end I shall derive a proof for a theorem that is not completely trivial in the sense that it is easy to come up with a more complicated argument or to spend more time in trial and error to "find" a proof. (And for some people it will even be easy to "find" no proof at all.)

When deriving the proof, I shall follow the rules of the game. For me that is easy because the game is familiar to me; you, however, are invited to follow the derivation before the game has been fully explained. I know that this is not fair and I apologize for it, but I have no choice: the explanation of the game will occupy a major portion of the rest of the book and has to be postponed.

In order to assist you in seeing what is going on, I shall first explain in a prelude the bare minimum needed to understand the theorem, to read the proof, and to follow its derivation. I ask you to remember, while reading this prelude, that almost each of its sentences

should be followed by "about which more later".

Prelude

- I assume you to be familiar with the notion of applying a function f to an argument x; instead of writing $f(x)$ — or just $f\,x$ —, we denote function application explicitly by an infix full stop (= period) and write $f.x$.

- I assume you to be familiar with the notion of "substituting equals for equals", e.g. that $f.x = f.y$ follows from $x = y$ and that also $x+7 = y+7$ follows from $x = y$.

- I invite you to be willing to view expressions such as $3=3$, $3<4$, $3<x$, $3>4$ not necessarily as statements of fact but as "boolean expressions" which — depending on the values of variables occurring in them — take on either the value "true" or the value "false". The first two, $3=3$ and $3<4$, have the value true, the next one, $3<x$, has the value true if x is large enough and the value false if x is small enough, and the last one, $3>4$ — which as statement of fact would be "wrong" — has the value false .

• A "relation" on a domain is a boolean function on the ordered pairs of elements of the domain; relations are often denoted by an infix notation. Familiar examples of relations on integers are $<$, $\leq$, $>$, $\geq$, $=$, and $\neq$. (Warning: later we shall use the symbol $\leq$ to denote some relation on an arbitrary domain.) In view of "substituting equals for equals", equality is an important relation for any domain on which functions are defined.

• Relations on the boolean domain are known as "logical connectives". The predicate calculus comprises the rules for manipulating formulae with logical connectives. Of the logical connectives we need, besides $=$, $\Leftarrow$ (read "follows from" or "if"); For the sake of completeness we mention $\wedge$ (read "and"). Their properties here relevant are that for any boolean A

(0) $A = (A = true)$ $\quad A = (A \Leftarrow true)$ $\quad A = (A \wedge true)$

and that for any boolean A and B

(1) $(A \Leftarrow B) \Leftarrow (A = B)$ $\quad (A \Leftarrow B) \Leftarrow (A \wedge B)$

Moreover it can be shown that (0) is exhaustive, i.e. that in a sense $=$, $\Leftarrow$, and $\wedge$ are the only logical connectives for which true is a unit element.

Mathematical Methodology

• Many a proof obligation can be captured by a boolean expression of the form $A \Leftarrow B$. The obligation can be met by constructing what is called "a strengthening chain" of boolean expressions, starting with A and ending with B. (This is a slight abuse of language: it would have been a little bit more honest to call the chain "nonweakening".) A chain is strengthening if for any boolean expression C with successor D in the chain, $C = D$ or $C \Leftarrow D$ follows from the available rules. The available rules may come from the predicate calculus or from stated properties of atoms of the formulae.

• Relation $\leq$ is reflexive means

(2) $\quad x \leq x \quad$ for all x .

(The clause "for all ...." is short for "for all .... of the domain on which $\leq$ has been defined.) In view of (0) we could also have written as definition of reflexivity of $\leq$

$$(x \leq x) = \text{true} \quad \text{for all } x \ .$$

It gives us a rule for creating a pair of successive boolean expressions C and D in a strengthening chain since $C = D$ follows if the one expression can be formed by replacing for some x the subexpression $x \leq x$ in the other by true .

• There are many ways of stating that relation $\leq$ is transitive; predicate calculus shows their equivalence. For our purposes we take:

Relation $\leq$ is transitive means

(3) $(x \leq z \Leftarrow y \leq z) \Leftarrow x \leq y$ for all x, y, z .

This says that for some x, y, z and some transitive $\leq$, the left-hand side $x \leq z \Leftarrow y \leq z$ may be followed in a strengthening chain by $x \leq y$ (with the same x, y as in the preceding expression). The significance of this strengthening transformation is that it eliminates the two occurrences of z .

• Function f is monotonic with respect to $\leq$ – or: function f preserves $\leq$ – means

(4) $f.x \leq f.y \Leftarrow x \leq y$ for all x, y .

• In hints we use the symbol := (read "becomes" or "instantiated by") to define instantiations, e.g. were we to conclude from the monotonicity of h for specific arguments u and v

$$h.u \leq h.v \Leftarrow u \leq v$$

the hint "(4) with $f, x, y := h, u, v$" would fully describe the substitutions.

(End of Prelude.)

After the above we are ready to formulate and prove the following theorem.

Theorem Let $\leq$ be a reflexive transitive relation on some domain; let f and g be functions from that domain to that domain satisfying

(5) $(f.x \leq y) = (x \leq g.y)$ for all x,y ;

then f is monotonic. (End of Theorem.)

Example With $\leq$ in its usual interpretation as a relation on the real numbers, we could take for f and g the cube and the cube root respectively since

$$(x^3 \leq y) = (x \leq \sqrt[3]{y}) \quad \text{for all } x,y \ ;$$

the cube is, indeed, a monotonic function. (End of example.)

Our proof obligation is to show that (4) follows from (2), (3), and (5). It can be met by showing that for arbitrary u,v in the domain,

(6) $f.u \leq f.v \Leftarrow u \leq v$

follows from (2), (3), and (5). We try to do so by investigating how (2), (3), and (5) enable us to construct a strengthening

chain from $f.u \leq f.v$ to $u \leq v$. [When a —strengthening or weakening— chain has to be constructed, it is, for good reasons, standard practice to start at the most complicated side.] Viewed this way, our task is to remove from $f.u \leq f.v$ the two f-applications.

Were we to replace in (6) the f applied to u by an arbitrary function, we would get an underivable expression, and the same holds if we replaced the f applied to v by an arbitrary function. In other words, for both f-applications, something given about f has to be used. Since of (2), (3), and (5), only the last one mentions f, we know that -at least- two appeals to (5) will be needed, with instantiations $x := u$ and $x := v$ respectively.

Closer inspection of (5) tells us that indeed it can be used for f-elimination: it equates an expression with an f with an expression without an f. So far, so good, but still closer inspection of (5) reveals that it can only be used for an f-application to the left of $\leq$. In our starting formula $f.u \leq f.v$, the term $f.u$ meets that condition, but the term $f.v$ does not. So the problem becomes: how do we get an expression of the form

$$f.v \leq \ldots$$

to enter the picture in order to prepare ourselves for the use of (5) with $x := v$? So we find our attention drawn to (2) and (3) and observe that, thanks to (2) with $x := f.v$, the introduction of the term

$$f.v \leq f.v$$

amounts to the introduction of the term *true*. So we consider a first step of the form

$$\begin{array}{ll} & f.u \leq f.v \\ = & \quad \{ \leq \text{ is reflexive, i.e. (2) with } x := f.v \} \\ & (f.u \leq f.v) \ \ldots \ (f.v \leq f.v) \quad , \end{array}$$

where (0) tells us that for "..." we can choose between $=$, $\Leftarrow$, and $\wedge$. Which one do we select?

With regard to the above step, the choice is irrelevant on account of the reflexivity of $\leq$. This first step could, however, be our last appeal to the reflexity of $\leq$, in which case the remaining steps should be valid, no matter what the value of the extra term $f.v \leq f.v$ is. Since we are constructing a strengthening chain, we should select our

weakest option, and according to (1) that is $\Leftarrow$. Hence we propose to start our proof with the first step

$$
\begin{array}{ll}
 & f.u \leq f.v \\
= & \quad \{ \leq \text{ is reflexive, i.e. (2) with } x := f.v \} \\
 & (f.u \leq f.v) \Leftarrow (f.v \leq f.v) \quad .
\end{array}
$$

Since the whole purpose of the above exercise was to create the opportunity for the two appeals to (5), that is what we do next:

$$
\begin{array}{ll}
 & (f.u \leq f.v) \Leftarrow (f.v \leq f.v) \\
= & \quad \{(5) \text{ with } x,y := u, f.v \text{ and } x,y := v, f.v \} \\
 & (u \leq g.(f.v)) \Leftarrow (v \leq g.(f.v)) \quad .
\end{array}
$$

Observing that now all occurrences of g and f are concentrated in two occurrences of the same expression, an appeal to the transitivity of $\leq$ seems indicated, i.e. for the next step I suggest

$$
\begin{array}{ll}
 & (u \leq g.(f.v)) \Leftarrow (v \leq g.(f.v)) \\
\Leftarrow & \quad \{ \leq \text{ is transitive, i.e. (3) with } x,y,z := u, v, g.(f.v) \} \\
 & u \leq v
\end{array}
$$

and, lo and behold, we are done!

Collecting the above I would summarize

the above proof as follows.

Proof We observe for any u,v

$$
\begin{array}{ll}
 & f.u \leq f.v \\
= & \quad \{ \leq \text{ is reflexive} \} \\
 & f.u \leq f.v \Leftarrow f.v \leq f.v \\
= & \quad \{(5) \text{ with } x,y := u, f.v \text{ and } x,y := v, f.v \} \\
 & u \leq g.(f.v) \Leftarrow v \leq g.(f.v) \\
\Leftarrow & \quad \{ \leq \text{ is transitive} \} \\
 & u \leq v \quad .
\end{array}
$$

(End of Proof.)

In the above rendering of the chain

- we have avoided the duplication of the intermediate expressions;
- we have eliminated four parenthesis pairs by giving $\leq$ a higher binding power than $\Leftarrow$;
- we have surrounded, as a visual aid to parsing, $\Leftarrow$ by more blank space than $\leq$;
- in the first and last hint we have exploited the (assumed) familiarity with the notions reflexivity and transitivity to omit the instantiations.

These are minor details, but, as we shall see later, we have to pay attention to them (and to many more) for, together, a lot of minor details can make a big difference.

Remark The above is by no means the only reasonable chain. Its design has been driven by the desire to eliminate f-applications and to combine the two appeals to (5). An alternative chain is

$$
\begin{array}{ll}
 & f.u \leq f.v \\
= & \{(5) \text{ with } x,y := u, f.v\} \\
 & u \leq g.(f.v) \\
\Leftarrow & \{\leq \text{ is transitive}\} \\
 & u \leq v \ \wedge \ v \leq g.(f.v) \\
= & \{(5) \text{ with } x,y := v, f.v\} \\
 & u \leq v \ \wedge \ f.v \leq f.v \\
= & \{\leq \text{ is reflexive}\} \\
 & u \leq v \quad .
\end{array}
$$

The first step fulfils our obligation to instantiate (5) with $x := u$ and creates the "$u \leq$" of our goal; the second step extends that to "$u \leq v$"; the third step fulfils our obligation to instantiate (5) with $x := v$, and the fourth step removes the last conjunct.

Both proofs are minimal in the sense that what has to be used is used exactly once. They are identical in the sense that they use the same instantiations of (2), (3), and (5). The second proof also provides the answer to

the objection my development of the first proof could have evoked: why didn't I start with the immediately possible elimination of the f applied to u ? The answer is: I could have done so.

The second proof was given by Edgar Knapp, but he produced it in the opposite order, starting with

$$\begin{array}{ll} & u \leq v \\ = & \{ \leq \text{ is reflexive} \} \\ & u \leq v \ \wedge \ f.v \leq f.v \end{array}$$

This step -as in our case- would also have been valid with $\wedge$ replaced by $\equiv$ or $\Leftarrow$. Because here a weakening chain is under construction, the strongest option has to be selected, and that is $\wedge$. (Formula (1) could have been extended with

$$(A \equiv B) \Leftarrow (A \wedge B) \quad . \quad)$$

(End of Remark.)

Austin, 2 October 1989

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA