Our proof format

We said earlier that we are in favour of what we called "calculational proofs"; as a result, many of our proofs are, indeed, calculational: the statement of a theorem is in essence a boolean expression, and its proof is in essence a calculation evaluating that boolean expression to the value true . The most straightforward way of evaluating a boolean expression is to subject it to one or more value-preserving transformations until true or false is reached. The reason that a number of consecutive transformations may be needed is because we wish to confine them to manipulations from a restricted repertoire.

Remark We shall not restrict that repertoire to the absolute minimum because that would not be practical for our purposes: it would make our calculations much longer than we would like them to be. It would be like doing mathematics without theorems, reducing each argument down to the axioms, and that is not practical. The reader should bear in mind that our purposes -i.e. using logic- are quite different from those of the logicians that study logics: for their purposes it is appropriate to reduce logical systems to their bare essentials, but not for ours. (End of Remark.)

Let $[A]$ denote the boolean expression to be evaluated, and let the evaluation take, say, 3 steps, which would amount to the occurrence of 2 intermediate results. More precisely, for some expressions $[B]$ and $[C]$:

the first step would establish $[A] \equiv [B]$;
the second step would establish $[B] \equiv [C]$;
the third step would establish $[C] \equiv true$;

then the whole calculation would establish $[A] \equiv true$. (Had the third step established $[C] \equiv false$, the whole calculation would have established $[A] \equiv false$.)

Note that in the above rendering of the calculation, the intermediate expressions $[B]$ and $[C]$ each occur twice. Since, in general, the B and C can be quite elaborate expressions, we need for brevity's sake a format in which such repetitions are avoided. We propose

$$
\begin{array}{ll}
 & [A] \\
= & \{\text{hint why } [A] \equiv [B]\} \\
 & [B] \\
= & \{\text{hint why } [B] \equiv [C]\} \\
 & [C] \\
= & \{\text{hint why } [C] \equiv true\} \\
 & true
\end{array}
$$

<u>Remark</u> The virtue of this format is more than

brevity alone, for it allows us to conclude $[A] \equiv true$ without reading the intermediate expressions. In our former rendering one would have to check that the right-hand side of $[A] \equiv [B]$ is the same expression as the left-hand side of $[B] \equiv [C]$. Our format expresses that sameness by syntactic means. (End of Remark.)

Though in principle sufficient, our proof format can do with some refinement, as the following example shows. Let our proof obligation be of the form $[A \equiv D]$. Rendered in our format, the calculation could be of the form

$$\begin{array}{ll}
 & [A \equiv D] \\
= & \{\text{hint why } [A \equiv B]\} \\
 & [B \equiv D] \\
= & \{\text{hint why } [B \equiv C]\} \\
 & [C \equiv D] \\
= & \{\text{hint why } [C \equiv D]\} \\
 & true
\end{array}$$

<u>Note</u> Compared with the previous example, the first two hints in the above are stronger since -Leibniz- for any X, Y, Z : $[X \equiv Y] \Rightarrow [X \equiv Z] \equiv [Y \equiv Z]$; since $[C \equiv D]$ is the same as $[C \equiv D] \equiv true$, the last hint follows the previous example. [End of Note.]

The above is not very nice if the expression for which D stands is a lengthy one: it has to be repeated from line to line.

We therefore render this argument in the form

$$\begin{array}{ll}
 & A \\
= & \{\text{hint why } [A \equiv B]\} \\
 & B \\
= & \{\text{hint why } [B \equiv C]\} \\
 & C \\
= & \{\text{hint why } [C \equiv D]\} \\
 & D
\end{array}$$

under the new convention that each relational operator at the left is universally quantified by its own pair of square brackets. Hence the above amounts to the assertion

$$[A = B] \wedge [B = C] \wedge [C = D] \quad .$$

<u>Note</u> Since $[[A] \equiv [B]] \equiv ([A] \equiv [B])$, the new convention of the implied square brackets does not change our first example, in which booleans were compared. The new convention has been introduced so as to be able to accommodate on the lines of our proof format boolean structures as well. (End of Note.)

A not uncommon occurrence when we prove $[A \equiv D]$ by means of such a "continued equivalence" is that one of the intermediate expressions is $A \vee D$. In our format we would get something of the form

$$\begin{array}{ll} & A \\ = & \{\text{hint}\} \\ & \dots \\ = & \{\text{hint}\} \\ & A \vee D \\ = & \{\text{hint}\} \\ & \dots \\ = & \{\text{hint}\} \\ & D \qquad\qquad , \end{array}$$

asserting $[A \equiv D]$ on account of

$$[A \equiv A \vee D] \wedge [A \vee D \equiv D] \quad .$$

Since the first conjunct is the same as $[D \Rightarrow A]$ and the second one the same as $[A \Rightarrow D]$, such a proof of equivalence boils down to a proof by "mutual implication", and we often prove the two implications separately. (This is informally known as "a ping-pong argument".)

<u>Remark</u> Many texts on theorem proving seem to suggest that a ping-pong argument is -if not the only way- the preferred way of demonstrating equivalence. This opinion is not confirmed by our experience; avoiding unnecessary ping-pong arguments will turn out to be a powerful way of shortening our arguments. At this stage the methodological advice is to avoid the ping-pong argument if you can, but to learn to recognize

the situation in which the ping-pong argument is appropriate. (End of Remark.)

There are two reasons, why for the genuine ping-pong argument the above format is inadequate. The first reason is revealed by considering a proof of $[A \equiv D]$ in which one of the intermediate expressions is $A \wedge D$:

$$\begin{array}{ll} & A \\ = & \{\text{hint}\} \\ & \dots \\ = & \{\text{hint}\} \\ & A \wedge D \\ = & \{\text{hint}\} \\ & \dots \\ = & \{\text{hint}\} \\ & D \end{array} ,$$

which asserts $[A \equiv D]$ on account of

$$[A \equiv A \wedge D] \;\wedge\; [A \wedge D \equiv D] \quad .$$

The first conjunct, however, is the same as $[A \Rightarrow D]$ and the second one the same as $[D \Rightarrow A]$, so here we have a representation rather different from the previous one of exactly the same proof of equivalence by mutual implication. The availability of just these two options is not nice; it is much nicer to have a more neutral one in between.

The second reason is that the last two examples tend to lead to elaborate expressions with a lot of repetition between the different lines: in the top half, A is repeated all the time, in the bottom half, D is repeated all the time. Since a main purpose of our format is to avoid repetition, we had better do something about it. We can do so by admitting in the left column the implication sign as well. Since

$$[X \equiv Y] \wedge [Y \Rightarrow Z] \;\Rightarrow\; [X \Rightarrow Z] \quad ,$$
$$[X \Rightarrow Y] \wedge [Y \equiv Z] \;\Rightarrow\; [X \Rightarrow Z]$$

and implication is transitive, i.e.

$$[X \Rightarrow Y] \wedge [Y \Rightarrow Z] \;\Rightarrow\; [X \Rightarrow Z] \quad ,$$

a proof of $[A \Rightarrow D]$ could, for instance, have the form

$$\begin{array}{ll}
 & A \\
\Rightarrow & \quad \{\text{hint why } [A \Rightarrow B]\} \\
 & B \\
= & \quad \{\text{hint why } [B \equiv C]\} \\
 & C \\
\Rightarrow & \quad \{\text{hint why } [C \Rightarrow D]\} \\
 & D \qquad\qquad ,
\end{array}$$

which asserts $[A \Rightarrow D]$ on account of

$$[A \Rightarrow B] \wedge [B \equiv C] \wedge [C \Rightarrow D] \quad .$$

Admitting, besides $=$, also $\Rightarrow$ in the left column may greatly reduce the amount of writing needed. So far, so good, but in order to be really pleasant to use, our format needs to accommodate three further, independent refinements.

The first one has nothing to do with the amount of writing; it only allows us to write and read things in a different order. Besides the implication $\Rightarrow$ we admit the consequence $\Leftarrow$ (read: "follows from"), and from a logical point of view it makes no difference whether we write $[A \Rightarrow D]$ or $[D \Leftarrow A]$. (It is a facility analogous to the freedom of writing the same relation either as $x < y$ or as $y > x$.) Consequently, our last proof of $[A \Rightarrow D]$ could equivalently have been rendered in the form

$$\begin{array}{ll}
 & D \\
\Leftarrow & \{\text{hint why } [D \Leftarrow C]\} \\
 & C \\
\equiv & \{\text{hint why } [C \equiv B]\} \\
 & B \\
\Leftarrow & \{\text{hint why } [B \Leftarrow A]\} \\
 & A \qquad\qquad .
\end{array}$$

Often the choice between implications or consequences is irrelevant, but we have encountered many calculations that in the one way require considerable clairvoyance to write down in the sense that the motivation for certain manipulations becomes apparent several lines down in the calculation, where everything miraculously falls into place, whereas written in the other way such calculations often have the pleasant property that each next manipulation is strongly suggested by what has already been written down. Calculations that in the one way strike the reader as pulling rabbits out of hats can often be derived in the opposite direction on the principle that there is really only one thing you can do. In fact we fear that the traditional predominance of the implication over the consequence in combination with our habit of reading from left to right has greatly contributed to the general mystification of mathematics.

The second refinement concerns demonstranda of the form $[E] \Rightarrow [A \equiv D]$. (The following is mutatis mutandis equally applicable to demonstranda of the form $[E] \Rightarrow [A \Rightarrow D]$.) The demonstrandum is equivalent to $[[E] \wedge A \equiv [E] \wedge D]$ and we could have used our earlier format; it is, however, unattractive to repeat $[E]$ on each line, the more so since $[E]$ is often needed for the justification of a single step only. The calculation might therefore be presented in the following form:

$$\begin{array}{ll} & A \\ = & \{\text{hint why } [A \equiv B]\} \end{array}$$

$$
\begin{array}{ll}
 & B \\
= & \{\text{hint why } [E] \Rightarrow [B \equiv C]\} \\
 & C \\
= & \{\text{hint why } [C \equiv D]\} \\
 & D \quad .
\end{array}
$$

This format is often appropriate where $[E]$ would be the formal statement of a (usually named) property of one of the atomic symbols occurring in A and D . At first sight some readers may have the uneasy feeling that the antecedent $[E]$ has been "smuggled in", but we can reassure those readers; what we have done is neither deep , nor fishy: we introduced a convenient shorthand that proved safe to use.

The third convention concerns the omission of universal quantifications. If our demonstrandum is in full $(\underline{A}x::[A.x \equiv D.x])$ we would write:

"We observe for any x

$$
\begin{array}{ll}
 & A.x \\
= & \{\text{hint why } (\underline{A}x:: [A.x \equiv B.x])\} \\
 & B.x \\
= & \{\text{hint why } (\underline{A}x:: [B.x \equiv C.x])\} \\
 & C.x \\
= & \{\text{hint why } (\underline{A}x:: [C.x \equiv D.x])\} \\
 & D.x \quad \text{"}
\end{array}
$$

and similarly if we had to demonstrate a universally quantified implication.

By way of example of how this all works, we shall now prove "A conjunctive predicate transformer is monotonic", a theorem that appeals to the following definitions:

(i) a function from predicates to predicates is (for historical reasons) called "a predicate transformer"

(ii) $(f \text{ is conjunctive}) \equiv$
$(\underline{A}X,Y :: [f.(X \wedge Y) \equiv f.X \wedge f.Y])$

(iii) $(f \text{ is monotonic}) \equiv$
$(\underline{A}P,Q :: [P \Rightarrow Q] \Rightarrow [f.P \Rightarrow f.Q])$.

The proof might be rendered as follows.

Proof We observe for any conjunctive predicate transformer f and any predicates P and Q:

$$
\begin{array}{ll}
 & [f.P \Rightarrow f.Q] \\
= & \quad \{\text{predicate calculus}\} \\
 & [f.P \wedge f.Q \equiv f.P] \\
= & \quad \{f \text{ is conjunctive}\} \\
 & [f.(P \wedge Q) \equiv f.P] \\
\Leftarrow & \quad \{\text{Leibniz}\} \\
 & [P \wedge Q \equiv P] \\
= & \quad \{\text{predicate calculus}\} \\
 & [P \Rightarrow Q] \quad .
\end{array}
$$

(End of Proof.)

The above gives some idea of the degree of detail provided in the hints. The two hints "predicate calculus" both refer to the formula

$$[X \Rightarrow Y] \equiv [X \wedge Y \equiv X]$$

of which the reader is supposed to know that it holds for any predicates X, Y. These hints refer to one of "the manipulations from a restricted repertoire" that we mentioned in the beginning.

The hint "f is conjunctive" is given where the reader can be supposed to know that this means that application of f distributes over conjunction. If the situation is less familiar or the substitution is more complicated, we give the instantiation explicitly. (In this case, we would have referred to the second line of (ii) "with $X,Y := P, Q$".) When a manipulation is confined to a subexpression (as, in this case, to the left-hand side of the equivalence), our hints do not identify the subexpression; the reader is supposed to do so himself by identifying in which subexpression the two related expressions differ.

The hint "Leibniz" refers to

$$[x = y] \Rightarrow [f.x = f.y] \quad ,$$

i.e. that a function applied to equal arguments yields equal values.

Austin, 26 January 1987

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