Some annotated proofs

Without the work of W.H.J. Feijen, A.J.M van Gasteren and R.M. Dijkstra, the following would not have been written; I owe them a lot.

The topic of this note is the design of formal proofs. Besides giving a number of proofs I shall give the considerations that are of relevance for their construction.

To begin with, we consider the beautiful theorem -from the collection of études composed by WF&AvG, and dubbed "the see-saw lemma by RMD -

(0) $[x \Rightarrow x;\sim x;x]$ for all x ,

to be proven from first principles.

Which first principles? Well, the consequent $x;\sim x;x$ suggests two things: firstly, because of the 2 semicolons, that the associativity of the composition will be involved, and, secondly, that we shall need the exchange rules as they provide the link between composition and transposition.

Because of the involvement of the exchange rules, we follow the suggestion of EWD1141 to switch to composition's conjugate, the confrontation, in terms of which the exchange rules are a little bit cleaner.

Extract I recall from EWD1141, that the "confrontation" is denoted by "!", is defined by $[\, x!y \equiv \neg(\neg x; \neg y)\,]$, and, hence, is associative, has an identity element $\neg\,]\, -$, and is universally conjunctive. In terms of !, the exchange rules are

$$[x!y \vee z] \equiv [z!\sim y \vee x] \qquad \text{left-exchange}$$

$$[x!y \vee z] \equiv [\sim x!z \vee y] \qquad \text{right-exchange.}$$

(End of Extract)

In terms of the confrontation, the see-saw lemma reads

(1) $[\, x!\sim x!x \Rightarrow x\,]$ for all x .

Remark In this note I do not intend to spend much attention to things such as the equivalence of (0) and (1). That part of predicate calculus - including $(f \circ g)^* = f^* \circ g^*$ - I assume here available. (End of Remark).

The three main proof patterns for establishing $[p \Rightarrow q]$ are schematically represented by

(i) $[p \Rightarrow q] \Leftarrow \text{true}$

(ii) $[p \vee z] \Rightarrow [q \vee z]$ for all z

(iii) $[\neg p \vee z] \Leftarrow [\neg q \vee z]$ for all z .

(Under (i) I capture here all notational variations such as

- transforming $p \wedge q$ in a sequence of value-preserving transformations into p
- transforming p in a sequence of weakening transformations into q (or $q \vee \neg p$), etc.

(ii) and (iii) are different for the universal quantification over the new dummy. Note that (ii) and (iii) represent two intrinsically different ways of introducing the dummy z: in (ii) "p" becomes a disjunct, in (iii) "$\neg p$" does so.)

The shape of the exchange rules suggests (ii), i.e. to establish (1) by establishing

(2) $[x\,!\,{\sim}x\,!\,x \vee z] \Rightarrow [x \vee z]$ for all x,z.

Remembering that the whole purpose of the introduction of z was to create the opportunity of applying an exchange rule, we now suggest to apply an exchange rule – for reasons of symmetry it probably does not matter which one –, i.e. to start our weakening chain as follows:

$$
\begin{aligned}
& [x\,!\,{\sim}x\,!\,x \vee z] \\
= & \quad \{\text{right-exchange}\} \\
& [{\sim}x\,!\,z \vee {\sim}x\,!\,x]
\end{aligned}
$$

(The alternative application of the right-exchange rule would have yielded $[\sim(x\,!\sim x)\,!\,z \vee x]$, which looks less inspiring, so we pursue the chosen application first.)

Had $!$ been disjunctive, the next step would have been easy: we would have rewritten our last result as $[\sim x\,!\,(z \vee x)]$. But $!$ is not disjunctive, but conjunctive, i.e. at least monotonic, and this we can exploit, remembering that we are building a weakening chain! We can continue

$$\begin{array}{ll} & [\sim x\,!\,z \vee \sim x\,!\,x] \\ \Rightarrow & \quad \{\,!\ \text{monotonic in its 2nd argument}\} \\ & [\sim x\,!\,(z \vee x)] \quad . \end{array}$$

Remark Here are three alternative formulations for "f is monotonic":

(i) $[p \Rightarrow q] \Rightarrow [f.p \Rightarrow f.q]$ for all p, q

(ii) $[f.p \vee f.q \Rightarrow f.(p \vee q)]$ for all p, q

(iii) $[f.p \wedge f.q \Leftarrow f.(p \wedge q)]$ for all p, q .

Monotonicity is too important a property to be known by (i) only; (ii) and (iii) can be generalized to existential and universal quantification respectively. (End of Remark.)

In view of the fact that our target expression $[x \vee z]$ contains no $\sim$, our last trans-

formation was a step in the right direction: the number of ~'s has been reduced from 2 to 1. The right-exchange is a proper mechanism for that, but is only applicable after we have made the confrontation into a disjunct. So we proceed

$$
\begin{array}{ll}
 & [\sim x\,!\,(z \vee x)] \\
= & \quad \{\text{predicate calculus}\} \\
 & [\sim x\,!\,(x \vee z) \vee \text{false}] \\
= & \quad \{\text{right-exchange}\} \\
 & [x\,!\,\text{false} \vee x \vee z]
\end{array}
$$

Remark An alternative for the first step, that would have turned the confrontation into a disjunct would have been an appeal to the idempotence of $\vee$: it would have yielded

$$[\sim x\,!\,(z \vee x) \vee \sim x\,!\,(z \vee x)] \quad ,$$

reintroducing a second ~ (and more complication). (End of Remark)

Now the only thing left is to get rid of the first disjunct x!false. However,

$$[x\,!\,\text{false} \vee x \vee z] \Rightarrow [x \vee z] \quad \text{for all } z$$

is equivalent to

$$[x\,!\,\text{false} \vee x \Rightarrow x]$$

or

$$[x\,!\,\text{false} \Rightarrow x]$$

which holds because ! has a neutral element. (Vide the conjugate relation [x ⇒ x;true].) So our proof can be completed:

```
    [ x!;false ∨ x ∨ z ]
=     { [ x!;false ⇒ x ]}
    [ x ∨ z ]
```

Summarizing the proof, we observe for any x,z

```
    [ x!;~x!;x ∨ z ]
=     { right-exchange }
    [~x!;z ∨ ~x!;x ]
⇒     {!, monotonic in second argument}
    [~x!;(z ∨ x)]
=     {predicate calculus}
    [~x!;(x ∨ z) ∨ false]
=     { right-exchange }
    [ x!;false ∨ x ∨ z]
=     { [ x!;false ⇒ x ]}
    [ x ∨ z]
```

Remark in retrospect The only rôle of the associativity of the composition has been to give us the choice between using the left- or the right-exchange. (End of Remark in retrospect.)

The reader is kindly invited to note that my "annotated" version of a 5-step argument took about 5 pages of manuscript. The moral of the story is that a formal proof can be a very

compact deposit of our considerations. Furthermore I would like to point out that most of our considerations seemed more general than just the relational calculus. The only really specific element was the lemma $[x!, false \Rightarrow x]$, but the need for that was the result of calculation.

* * *

The next theorem - also from WF&AvG - I want to deal with is

For any right-condition q

(3) $\quad [q; true; \neg q \equiv q; \neg q]$.

A moment's consideration shows that a ping-pong argument is indicated since for pong we don't even need to know that q is a right-condition:

$$
\begin{array}{ll}
 & [q; true; \neg q \Leftarrow q; \neg q] \\
\Leftarrow & \quad \{ \; ; \text{ monotonic} \} \\
 & [q; true \Leftarrow q] \\
= & \quad \{ \text{lemma} \} \\
 & true
\end{array}
$$

(The lemma follows thus:

$$
\begin{array}{ll}
 & x; true \\
\Leftarrow & \quad \{ [true \Leftarrow J] \text{ and } ; \text{ monotonic} \} \\
 & x; J \\
= & \quad \{ J \text{ neutral element of } ; \} \\
 & x \quad .
\end{array}
$$

)

With proving ping

(4) $[q;\mathit{true};\sim q \Rightarrow q;\sim q]$

I had serious problems, which in retrospect could be traced to an unsufficiently convenient characterization of "q is a right-condition". The original characterization was

$$[\mathit{true};q \equiv q] \quad ,$$

which is good to know, but since $[\mathit{true};x \Leftarrow x]$ holds for any x, the specific quality of being a right-condition is expressed by

$$[\mathit{true};q \Rightarrow q] \equiv (q \text{ is a right-condition}) \quad ,$$

and it was this equivalence with which I started my work on the current theorem. But it is more convenient its mutual implications separately, depending on whether one wants to show or to use that q is a right-condition. In the former case we use

(5) $[\mathit{true};q \Rightarrow q] \Rightarrow (q \text{ is a right-condition})$;

in the latter case we also exploit the monotonicity of composition, and get that for any x

(6) $[x;q \Rightarrow q] \Leftarrow (q \text{ is a right-condition})$

with the immediate consequence that for any x

(6') $[\sim q;x \Rightarrow \sim q] \Leftarrow (q \text{ is a right-condition})$.

The charm of (6), which almost looks like an

absorption rule, is the dummy x that we can instantiate as we see fit. In particular we can conclude (4) from

(7) $[q;\mathit{true};\sim q \Rightarrow q;\sim q;x]$

In particular -and here is still some sort of rabbit - : if x starts with "q;" we see in the consequent of (7) as subexpression the consequent of the see-saw lemma. So let us start with that:

$$
\begin{array}{ll}
 & \mathit{true} \\
= & \quad \{\text{see-saw lemma}\} \\
 & [q \Rightarrow q;\sim q;q] \\
\Rightarrow & \quad \{\text{monotonicity of ; in 1st argument}\} \\
 & [q;\mathit{true};\sim q \Rightarrow q;\sim q;q;\mathit{true};\sim q] \\
\Rightarrow & \quad \{(6') \text{ with } x := q;\mathit{true};\sim q \text{ and monotonicities}\} \\
 & [q;\mathit{true};\sim q \Rightarrow q;\sim q] \quad .
\end{array}
$$

After the introduction of the see-saw lemma, we compose both sides with "true;~q" to get the target antecedent, in the proces constructing the x with which to apply (6') in the last step.

Austin, 9 November 1992

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