The design of a proof of equality

In this chapter we deal with real variables.

Let p, x, y satisfy

(0) $(\underline{A}w :: p \leq w \equiv x \leq w \wedge y \leq w)$;

such triples exist for any pair x, y : take, for instance, for p the maximum of x and y .

Let q, x, y satisfy

(1) $(\underline{A}w :: w \leq q \equiv w \leq x \vee w \leq y)$;

such triples exist for any pair x, y : take, for instance, for q the maximum of x and y .

The purpose of this chapter is to design the formal argument that derives

(2) $p = q$

from (0) and (1) .

* * *

As a heuristic device, we apply what is known as "the nabla trick" — "nabla" is the name of the character ∇ — . It consists of

trying to prove (2) from (3) and (4), which have been obtained from (0) and (1), respectively, by replacing $\leq$ by the unknown relational operator ∇ :

(3) $(\underline{A}w:: \quad p\nabla w \equiv x\nabla w \wedge y\nabla w)$

(4) $(\underline{A}w:: \quad w\nabla q \equiv w\nabla x \vee w\nabla y)$.

As we go along, we discover which properties of ∇ we need for the proof.

Remark The nabla trick serves more than one purpose. Firstly, because the as yet undefined operator ∇ defies interpretation of (3) and (4) in terms of some model, the nabla trick assists us in manipulating formulae without interpreting them. Secondly, the nabla trick is a means for collecting those properties of $\leq$ that are needed to derive (2) from (0) and (1); it is quite possible that, besides $\leq$, other relations have those properties as well and, therefore, could be chosen for ∇. The nabla trick is an aid in keeping track of what is needed for our arguments, and that is also what this chapter is about. (End of Remark.)

How do we derive (2), i.e. $p=q$? The first

observation is that, since there exist different real numbers, $p=q$ cannot be established without constraints on both p and q. Since (3) and (4) are the only constraints given on p and q, both (3) and (4) are needed. In these formulae, p and q only occur as operands of ∇ while we have to establish $p=q$, i.e. we need some property of ∇ that relates it to $=$. Remembering for a short moment that eventually $\leq$ should be an acceptable instantiation for ∇, we postulate that nabla is antisymmetric, i.e. satisfies for any p,q

(5) $$p=q \Leftarrow p\nabla q \wedge q\nabla p \ .$$

Remark Relation (5) is a constraint imposed on ∇, and that is why we have not written the needlessly stronger

$$p=q \equiv p\nabla q \wedge q\nabla p$$

though this relation would have been satisfied with $\leq$ for ∇. Not requiring more than needed is the rule of the game in this chapter. (End of Remark.)

By virtue of (5), demonstrating $p=q$ has been reduced to the independent demonstrations

of the conjuncts $p \nabla q$ and $q \nabla p$. Focussing our attention on the first one, $p \nabla q$, then we see that this term is an instantiation of the left-hand sides of both (3) and (4). We therefore split them up: let it be given that for all w

(3a) $\quad p \nabla w \Leftarrow x \nabla w \wedge y \nabla w$

(3b) $\quad p \nabla w \Rightarrow x \nabla w \wedge y \nabla w$

(4a) $\quad w \nabla q \Leftarrow w \nabla x \vee w \nabla y$

(4b) $\quad w \nabla q \Rightarrow w \nabla x \vee w \nabla y$.

We expect the proof of $p \nabla q$ to use (3a) and (4a), but not the two b-formulae. To prove $p \nabla q$ for any p satisfying (3a) and any q satisfying (4a), we observe

$$
\begin{array}{ll}
 & p \nabla q \\
\Leftarrow & \quad \{(3a) \text{ with } w := q\} \\
 & x \nabla q \wedge y \nabla q \\
\Leftarrow & \quad \{(4a) \text{ with } w := x \,;\, (4a) \text{ with } w := y\} \\
 & (x \nabla x \vee x \nabla y) \wedge (y \nabla x \vee y \nabla y) \\
\Leftarrow & \quad \{\text{pred. calc.}\} \\
 & (x \nabla x \wedge y \nabla y) \\
= & \quad \{(6) \text{ with } w := x \,;\, (6) \text{ with } w := y\} \\
 & \text{true}
\end{array}
$$

where nabla is postulated to be reflexive, i.e. to satisfy for any w

(6) $\quad w \nabla w$.

Remark For completeness' sake we show what would have happened, had we applied (3a) and (4a) in the other order: we would have arrived at another strengthening of $p \nabla q$, for the demonstration of which (6) does not suffice.

$$
\begin{array}{ll}
 & p \nabla q \\
\Leftarrow & \{(4a) \text{ with } w := p\} \\
 & p \nabla x \ \vee \ p \nabla y \\
\Leftarrow & \{(3a) \text{ with } w := x \ ; \ (3a) \text{ with } w := y\} \\
 & (x \nabla x \ \wedge \ y \nabla x) \ \vee \ (x \nabla y \ \wedge \ y \nabla y) \\
= & \{(6)\} \\
 & y \nabla x \ \vee \ x \nabla y \quad .
\end{array}
$$

(End of Remark.)

Let us now focus our attention on establishing the second conjunct, $q \nabla p$. There are good reasons to expect the proof of $q \nabla p$ to use (3b) and (4b), but not the two a-formulae. The simplest and most general reason for this expectation is the fact that, in contrast to the a-formulae, the b-formulae have not been used yet, but this is only as compelling as our conviction that the b-formulae have to be used indeed. The con-

vincing reason to use the b-formulae comes from the shape of the demonstrandum $q \nabla p$. How can we use our knowledge about p so as to get a nabla expression with p as its right-hand argument? The only way of doing so is instantiating (3) with $w := p$. On account of (6), however, this instantiation makes (3a) vacuously true, hence useless, and (3b) is the only part that can contribute. Similarly, on account of the q in front of ∇, it is (4b) that has to be instantiated with $w := q$. Finally, to combine p and q in a single nabla expression, we postulate that nabla is transitive, i.e. satisfies for any p, q, w

(7) $\quad q \nabla w \wedge w \nabla p \Rightarrow q \nabla p$.

After the above explorations we observe

$$
\begin{array}{ll}
 & q \nabla p \\
= & \quad \{\text{idempotence of disjunction}\} \\
 & q \nabla p \vee q \nabla p \\
\Leftarrow & \quad \{(7) \text{ with } w := x \text{ ; } (7) \text{ with } w := y\} \\
 & (q \nabla x \wedge x \nabla p) \vee (q \nabla y \wedge y \nabla p) \\
\Leftarrow & \quad \{\text{pred.calc., heading for (3b) with } w := p\} \\
 & (q \nabla x \wedge x \nabla p \wedge y \nabla p) \vee (q \nabla y \wedge x \nabla p \wedge y \nabla p) \\
= & \quad \{\text{pred. calc.}\} \\
 & (q \nabla x \vee q \nabla y) \wedge (x \nabla p \wedge y \nabla p) \\
\Leftarrow & \quad \{(4b) \text{ with } w := q \text{ ; } (3b) \text{ with } w := p\}
\end{array}
$$

$$
\begin{aligned}
& q \nabla q \;\wedge\; p \nabla p \\
= \quad & \{(6) \text{ with } w := q \;;\; (6) \text{ with } w := p\} \\
& \text{true}
\end{aligned}
$$

Remark The first step is not surprising. We use idempotence to duplicate the term so as to be able to exploit the transitivity of ∇ without destroying the symmetry between x and y. The use of the disjunction, rather than the conjunction, is not surprising either: since we are constructing a strengthening chain we choose our next intermediate result as weak as possible. Note that, with in the first step conjunction instead of disjunction, the appeal to (4b), four steps later, would have been impossible. (End of Remark.)

In order to prove $p=q$ from (3) and (4) we had to postulate

- ∇ is antisymmetric, i.e (5)
- ∇ is reflexive, i.e. (6),
- ∇ is transitive, i.e. (7).

Relations enjoying the above three properties are known as "partial orders". We now confine our attention to relations ∇ that are partial orders. However, not every partial relation ∇ is such that for any x,y a pair p,q exists that satisfies (3) and (4) – for instance: $=$ for ∇ –.

Mathematical Methodology.

Assuming that for partial order ∇ and arbitrary x,y, (3) and (4), and hence (2), are satisfied, we observe for any x,y

$$
\begin{array}{ll}
 & \text{true} \\
= & \quad \{\nabla \text{ is reflexive}\} \\
 & p\nabla p \wedge q\nabla q \\
= & \quad \{(3) \text{ with } w:=p;\ (4) \text{ with } w:=q\} \\
 & x\nabla p \wedge y\nabla p \wedge (q\nabla x \vee q\nabla y) \\
= & \quad \{(2), \text{ i.e. } p=q\} \\
 & x\nabla p \wedge y\nabla p \wedge (p\nabla x \vee p\nabla y) \\
= & \quad \{\wedge \text{ distributes over } \vee\} \\
 & (x\nabla p \wedge y\nabla p \wedge p\nabla x) \vee (x\nabla p \wedge y\nabla p \wedge p\nabla y) \\
\Rightarrow & \quad \{\nabla \text{ is reflexive and transitive, twice}\} \\
 & (x=p \wedge y\nabla x) \vee (y=p \wedge x\nabla y) \\
\Rightarrow & \quad \{\text{pred. calc.}\} \\
 & (x=p \vee y=p) \wedge (y\nabla x \vee x\nabla y) \ .
\end{array}
$$

The first conjunct of the last line states that p is one of the values x,y; the second conjunct $y\nabla x \vee x\nabla y$, holding, as it does, for any x,y, states that the partial order ∇ is what is known as a "total order". Examples of a total order on the real numbers are $\leqslant$ and $\geqslant$. With $\leqslant$ for ∇, p (and q) is known as the maximum of x and y, and is denoted by $x \uparrow y$. With $\geqslant$ for ∇, p (and q) is known as the minimum of x and y,

and is denoted by $x \downarrow y$. For the maximum, we have the alternative characterizations

$$(8) \quad x \uparrow y \leq w \;\equiv\; x \leq w \;\wedge\; y \leq w$$

$$(9) \quad w \leq x \uparrow y \;\equiv\; w \leq x \;\vee\; w \leq y \quad ,$$

and – remembering $u \geq w \equiv w \leq u$ – for the minimum

$$(10) \quad w \leq x \downarrow y \;\equiv\; w \leq x \;\wedge\; w \leq y$$

$$(11) \quad x \downarrow y \leq w \;\equiv\; x \leq w \;\vee\; y \leq w \quad .$$

Acknowledgement I am grateful to the anonymous referee of EWD1071 for the "Mathematische Gesellschaft in Hamburg", a remark from whom provided the incentive to show the equivalence between the alternative characterizations for the maximum and the minimum, respectively. (End of Acknowledgement.)

Austin, 24 January 1991

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

Mathematical Methodology