Copyright Notice

The derivation of a proof by J.C.S.P. van der Woude

In the following

- P and Q will be used to denote predicates on some space.
- X and Y will be used to denote functions from the natural numbers to predicates on that space; accordingly, X.i (0≤i) and Y.i (0≤i) denote predicate sequences.
- f will be used to denote a predicate transformer, i.e. a function from predicates to predicates.
- square brackets will be used to denote universal quantification of the enclosed predicate over the space in question.

With the above notational conventions we give the following definitions

- "sequence X.i (0≤i) is monotonic" means "sequence X.i (0≤i) is weakening or strengthening".
- "sequence X.i (0≤i) is weakening" means $(\underline{A}\, i,j : 0 \leq i < j : [X.i \Rightarrow X.j])$.
- "sequence X.i (0≤i) is strengthening" means $(\underline{A}\, i,j : 0 \leq i < j : [X.i \Leftarrow X.j])$.

- "predicate transformer f is monotonic" means $[P \Rightarrow Q] \Rightarrow [f.P \Rightarrow f.Q]$ for all P, Q .
- "predicate transformer f is finitely conjunctive" means $[f.(P \wedge Q) \equiv f.P \wedge f.Q]$ for all P, Q .
- "predicate transformer f is or-continuous" means $[f.(\underline{E}i: 0 \leq i: X.i) \equiv (\underline{E}i: 0 \leq i: f.(X.i))]$ for any monotonic sequence $X.i$ $(0 \leq i)$.
- "predicate transformer f is and-continuous" means $[f.(\underline{A}i: 0 \leq i: X.i) \equiv (\underline{A}i: 0 \leq i: f.(X.i))]$ for any monotonic sequence $X.i$ $(0 \leq i)$.

We can now formulate the

Theorem For any predicate transformer f

(0) (f is finitely conjunctive) $\wedge$ (f is or-continuous) $\Rightarrow$ (f is and-continuous) .

Here, we shall sketch the simple part of the proof and shall derive the exciting part (which we owe to J.C.S.P. van der Woude).

Proof Under the truth of the antecedent of (0) we have to show for monotonic $X.i$ $(0 \leq i)$

(1) $[f.(\underline{A}i: 0 \leq i: X.i) \equiv (\underline{A}i: 0 \leq i: f.(X.i))]$.

To begin with we recall that —not proved here— because f is finitely conjunctive, f is

monotonic. We now distinguish two cases.

X.i (0≤i) is weakening Because f is monotonic, also the predicate sequence f.(X.i) (0≤i) is weakening; consequently – not shown here – both sides of (1) are equivalent to f.(X.0). This concludes the first case.

X.i (0≤i) is strengthening Because f is monotonic – not shown here – LHS(1) ⇒ RHS(1) and we are left with the proof obligation

(2) $[\, f.(\underline{A}\, i: 0\le i: X.i) \Leftarrow (\underline{A}\, i: 0\le i: f.(X.i)) \,]$

for strengthening X.i (0≤i) and an f that is finitely conjunctive and or-continuous.

Meeting the obligation of showing (2) is the exciting part of the proof. Reduced to its bare essentials, it consists of one definition and about a dozen simple steps. But in presenting just that irrefutable formal argument, we would pull several rabbits out of the magical hat. The proof is exciting because of the existence of heuristic considerations that quite effectively buffer these shocks of invention. For that reason, we shall develop this proof instead of just presenting it. To aid the reader in parsing the interleaved presentation of heuristic considerations and proof fragments, the latter will be indented. Here we go!

For the sake of brevity we shall omit from here on the ranges $0 \leq i$ and $0 \leq j$, which are to be understood. We begin with a general remark about the exploitation of or-continuity. The or-continuity of f states

(3) $\quad [f.(\underline{E}i :: Y.i) \equiv (\underline{E}i :: f.(Y.i))]$

for any monotonic sequence $Y.i$. For a strengthening sequence $Y.i$, just monotonicity of f suffices for (3) to hold, and for constant sequences $Y.i$, (3) holds for any f. The relevant conclusion from these observations is that, if f's or-continuity is going to be exploited —and it is a safe assumption that it has to— a truly weakening sequence has to enter the picture.

Armed with this insight, we return to our demonstrandum (2). The simplest way of demonstrating an implication is to start at one side and then to repeatedly manipulate the expression (while either weakening or strengthening is allowed) until the other side is reached. So, let us try that. That decision being taken, at which side should we start?

Both sides are built from the "familiar" universal quantification and the "unfamiliar" application of f, about which our knowledge

is limited, the only difference being that, at the two sides, they occur in opposite order. In such a situation, the side with the "unfamiliar" operation as the outer one counts as the more complicated one and is therefore the preferred starting point. In our case, it is the consequent

---

(4) $\quad f.(\underline{A}i :: X.i)$,

---

so let us start from there. The formal challenge of manipulating (4) while exploiting what we know about f should provide the heuristic guidance as to in which direction to proceed.

Rewriting (4) so as to exploit f's or-continuity would require rewriting its argument $(\underline{A}i :: X.i)$ as an existential quantification over a truly weakening sequence, but how to do that —I tried in vain— is not clear at all. So, let us try to exploit at this stage f's finite conjunctivity, i.e. let us introduce a P and Q such that

$$[(\underline{A}i :: X.i) \equiv P \wedge Q] \quad .$$

For one of the conjuncts, say P, we may choose any predicate implied by $(\underline{A}i :: X.i)$; the law of instantiation tells us that any $X.j$ would do. (Note that this choice is

less restrictive than it might seem: because X.i is a strengthening sequence, any finite conjunction of some X.i 's yields some X.j .) We could therefore consider for some j the introduction of a predicate Q constrained by

$$[(\underline{A}i :: X.i) \equiv X.j \wedge Q] \quad .$$

But the introduction of one predicate Q for one specific j is unlikely to do the job: for one thing, the universal quantifications in the demonstrandum don't change their value if the range $0 \leq i$ is replaced by $j < i$. This observation suggests, instead of the introduction of a single predicate Q , a predicate sequence Y.j , constrained by

$$(5) \qquad (\underline{A}j :: [(\underline{A}i :: X.i) \equiv X.j \wedge Y.j]) \quad .$$

The introduction of the sequence Y.j will turn out to be the major invention of the proof under design. For the time being, we don't define Y -as would be done immediately in a "bottom-up" proof- but only collect constraints on Y , of which (5) is the first one. We do so in the hope that, eventually, we can construct a Y that meets all the constraints.

A minor problem with the use of (5) as a rewrite rule is that it equates an ex-

pression not depending on j with one that formally does depend on j. The formal dependence on j that would thus be introduced can be eliminated by quantifying over j; because we are rewriting a consequent, we use existential quantification because that yields a formally weaker expression — the range being non-empty! — than universal quantification (and the weaker the consequent, the lighter the task ahead of us). In short, we propose to start our proof under design with

$$
\begin{aligned}
& f.(\underline{A}i :: X.i) \\
= \quad & \{(5) \text{ and range of } j \text{ non-empty}\} \\
& (\underline{E}j :: f.(X.j \wedge Y.j)) \\
= \quad & \{f \text{ is finitely conjunctive}\} \\
& (\underline{E}j :: f.(X.j) \wedge f.(Y.j)) \qquad (6)
\end{aligned}
$$

So far, so good! We have not yet exploited f's $\underline{or}$-continuity and we cannot do so before we have an existential quantification over a truly weakening sequence. In (6) we do have an existential quantification (albeit, as yet, over a constant sequence) and, with $X.i$ a (truly) strengthening sequence, there is a fair chance that (5) permits a (truly) weakening sequence $Y.j$. So let us introduce the second constraint on Y

(7) sequence $Y.j$ $(0 \leq j)$ is weakening

as a next step towards the use of f's or-continuity, i.e. the use of (3) as a rewrite rule.

Comparison of the right-hand side of (3) with (6) shows that we can use (3) as rewrite rule only after we have succeeded in removing in (6) the first conjunct $f.(X.j)$ from the term. We cannot just omit it, as that would weaken the expression and, heading for an antecedent, we are not allowed to do that. We may strengthen it; in particular, strengthening it to something independent of j would allow us to take the constant conjunct outside the existential quantification of (6). In order to strengthen $f.(X.j)$ to something that is independent of j, we propose to quantify universally over j. That is, at (6) we propose to continue our proof under design with

$$
\begin{array}{ll}
 & (\underline{E}j :: f.(X.j) \wedge f.(Y.j)) \\
\Leftarrow & \quad \{\text{instantiation, monotonicity of } \wedge, \underline{E}\} \\
 & (\underline{E}j :: (\underline{A}i :: f.(X.i)) \wedge f.(Y.j)) \\
= & \quad \{\wedge \text{ distributes over } \underline{E}\} \\
 & (\underline{A}i :: f.(X.i)) \wedge (\underline{E}j :: f.(Y.j)) \\
= & \quad \{(3) \text{ and } (7), \text{ i.e. the use of or-continuity}\} \\
(8) & \quad (\underline{A}i :: f.(X.i)) \wedge f.(\underline{E}j :: Y.j)
\end{array}
$$

So far, so very good! Note that the left con-

junct of (8) is the antecedent of (2) we are heading for! Again, we cannot just omit the second conjunct in (8) as that would weaken the expression; the second conjunct has to be subsumed - i.e. implied - by the first one. By the looks of it we can equate (8) with its first conjunct on just the monotonicity of f and some implicative relation between X and Y - which will emerge as our third and last constraint on Y - . But be careful! If the range of i were empty, the first conjunct of (8) would yield true, whereas (8) would yield $f.(\underline{E}j :: Y.j)$ and there is no reason to assume these equivalent. Somewhere along the completion of our formal argument, we have to exploit the non-emptiness of i's range. As we can do it immediately, let us do it immediately. In short, we propose to continue our proof under design at (8) with

$$
\begin{array}{ll}
 & (\underline{A}i :: f.(X.i)) \wedge f.(\underline{E}j :: Y.j) \\
= & \quad \{\text{range of } i \text{ non-empty}\} \\
 & (\underline{A}i :: f.(X.i) \wedge f.(\underline{E}j :: Y.j)) \\
= & \quad \{\text{monotonicity of } f \text{ and } (9)\} \\
 & (\underline{A}i :: f.(X.i))
\end{array}
$$

with, as our third and last constraint on Y,

(9) $\quad (\underline{A}i :: [X.i \Rightarrow (\underline{E}j :: Y.j)])$.

But for the demonstration of the existence of Y, we have completed the proof in seven steps (six of which are equivalences). Now for the existence of a Y satisfying (5), (7), and (9).

In order to ease satisfaction of (9), we define Y as the weakest solution of (5), i.e. we define $Y.j$ for any j by

(10) $$[Y.j \equiv (\underline{A}i :: X.i) \vee \neg X.j]$$

In order to verify that this Y indeed satisfies (5), we observe for any j

$$\begin{aligned} & X.j \wedge Y.j \\ = & \quad \{(10)\} \\ & X.j \wedge ((\underline{A}i :: X.i) \vee \neg X.j) \\ = & \quad \{\wedge \text{ distributes over } \vee\} \\ & (X.j \wedge (\underline{A}i :: X.i)) \vee (X.j \wedge \neg X.j) \\ = & \quad \{j \text{ in } i\text{'s range; predicate calculus}\} \\ & (\underline{A}i :: X.i) \end{aligned}$$

In order to verify that condition (7) is met, i.e. that $Y.j$ $(0 \leq j)$ is indeed weakening, we observe for any j and k

$$\begin{aligned} & [Y.j \Rightarrow Y.k] \\ = & \quad \{(10)\} \\ & [(\underline{A}i :: X.i) \vee \neg X.j \Rightarrow (\underline{A}i :: X.i) \vee \neg X.k] \\ \Leftarrow & \quad \{\text{monotonicity of } \underline{\vee}\} \end{aligned}$$

$$
\begin{array}{ll}
 & [\neg X.j \Rightarrow \neg X.k] \\
= & \quad \{\text{counterpositive}\} \\
 & [X.j \Leftarrow X.k] \\
\Leftarrow & \quad \{X.i \ (0 \leq i) \text{ is strengthening}\} \\
 & [j < k] \ .
\end{array}
$$

Finally, in order to verify that Y satisfies (9), we observe

$$
\begin{array}{ll}
 & (\underline{E}j :: Y.j) \\
= & \quad \{(10)\} \\
 & (\underline{E}j :: (\underline{A}i :: X.i) \vee \neg X.j) \\
= & \quad \{j\text{'s range is not empty}\} \\
 & (\underline{A}i :: X.i) \vee (\underline{E}j :: \neg X.j) \\
= & \quad \{\text{de Morgan}\} \\
 & (\underline{A}i :: X.i) \vee \neg(\underline{A}j :: X.j) \\
= & \quad \{\text{Excluded Middle}\} \\
 & \text{true} \ .
\end{array}
$$

And this concludes the exciting part.

(End of Proof.)

Van der Woude's proof is very beautiful and I think it worthwhile to ponder over the question why this is so. It is beautiful in the way in which the proof has been divided into two parts, with Y and its three properties forming the interface between them. It is a meaning-

ful division in the sense that our dealing with f is entirely confined to the first part. Also, the interface between the two parts is the right one, void of any overspecification: it only mentions the existence of a Y with the properties relevant for the first part. Finally, the second part, which no longer deals with f but is concerned with the existence of a Y, is pleasingly constructive. It is really a beautifully structured argument.

I think also our derivation of the proof very beautiful. The development of the first part, which deals with f, is fully driven by the need to exploit that f is given to be finitely conjunctive and or-continuous, and the interface was constructed as we went along. Furthermore, the second part, which constructs a Y meeting the three requirements, does so in the most straightforward manner without pulling a single rabbit out of a hat; finally it contains three mutually independent verifications that the Y constructed meets the three requirements indeed. A very nice disentanglement!

Remark I would like to draw attention to the second step of the final calculation, which establishes $[(\mathbb{E}j: Y.j) \equiv \text{true}]$. Because this

cannot be established if the range for j is empty – existential quantification over an empty range yields false –, the calculation has to exploit that j's range is not empty. The knowledge that disjunction distributes over existential quantification only in the case of a non-empty range – and this belongs to the general knowledge the predicate calculator should have at his disposal – all but dictates that second step. (End of Remark.)

Finally, I would like to point out that, though carried out in great detail, the whole formal proof consists of fewer than twenty steps: the whole calculation is really quite short. I beg the reader to remember this whenever he is faced with a defence of informality on the supposed grounds that formal proofs are too lengthy and too tedious to be of any practical value. This supposition is wrong.

Austin, 27 January 1988

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