A comparison of relational proofs

The purpose of this note is to compare different proofs for the same theorem of the relational calculus, so that we may get some feeling for the sources of manipulative advantages and disadvantages. The theorem chosen is simple enough that it can be proved from first principles; yet I hope it is "deep" enough to make the experiment interesting.

Theorem Let t be the strongest solution of

(*) $\quad x: [\,] \vee a;x \Rightarrow x\,]$

i.e. -in view of Knaster-Tarski-

(0) $\quad [\,] \vee a;t \equiv t\,]$

(1) $\quad [\,] \Rightarrow x\,] \wedge [\,a;x \Rightarrow x\,] \Rightarrow [\,t \Rightarrow x\,]$ for all x;

let s be the strongest solution of

(**) $\quad x: [\,b \vee a;x \Rightarrow x\,]$, i.e.

(2) $\quad [\,b \vee a;s \equiv s\,]$

(3) $\quad [\,b \Rightarrow x\,] \wedge [\,a;x \Rightarrow x\,] \Rightarrow [\,s \Rightarrow x\,]$; then

(4) $\quad [\,s \equiv t;b\,]$

Proof 0 In this proof we try to find closed expressions for t and s, whereafter we establish (4) by manipulating these expressions. Comparing (*) with (**), we see that (*) is obtained from (**) with for b the special choice

$\mathcal{J}$; so we focus on (**) and try to find an expression for s in terms of (a,b) . We observe

```
    s
=   {(2)}
    b ∨ a;s
=   {(2)}
    b ∨ a;(b ∨ a;s)
=   { ; over ∨}
    b ∨ a;b ∨ a;a;s
=   {(2) and ; over ∨}
    b ∨ a;b ∨ a;a;b ∨ a;a;a;s      etc.
```

which suggests for s the closed form, viz.

(5) $[\, s \equiv \langle \exists n : n \geq 0 : q.n \,;\, b \rangle \,]$, where

(6) $[\, q.0 \equiv \mathcal{J} \,]$ and $[\, q.(n+1) \equiv a;q.n \,]$ for all n.

To check that conjecture (5) verifies (2) we observe

```
    b ∨ a;⟨∃n: n≥0 : q.n ; b⟩
=     { ; over ∃}
    b ∨ ⟨∃n: n≥0 : a;q.n ; b⟩
=     { (6)}
    q.0;b ∨ ⟨∃n: n≥0 : q.(n+1);b⟩
=     {p.c., transforming the dummy}
    q.0;b ∨ ⟨∃n: n≥1 : q.n ; b⟩
=     { p.c.}
    ⟨∃n: n≥0 : q.n;b⟩      .
```

To check that conjecture (5) verifies (3) for

any x, we observe

$$
\begin{array}{ll}
 & [\langle \exists n: n \geq 0: q.n ; b \rangle \Rightarrow x] \\
= & \quad \{ \text{pred. calc.} \} \\
 & \langle \forall n: n \geq 0: [q.n ; b \Rightarrow x] \rangle \\
\Leftarrow & \quad \{ \text{by mathematical induction, see below} \} \\
 & [b \Rightarrow x] \wedge [a;x \Rightarrow x]
\end{array}
$$

For the mathematical induction we observe for the base:

$$
\begin{array}{ll}
 & [q.0 ; b \Rightarrow x] \\
= & \quad \{ (6) \} \\
 & [\,] ; b \Rightarrow x] \\
= & \quad \{ \text{rel. calc.} \} \\
 & [b \Rightarrow x]
\end{array}
$$

for the step:

$$
\begin{array}{ll}
 & [q.(n+1) ; b \Rightarrow x] \\
= & \quad \{ (6) \} \\
 & [a ; q.n ; b \Rightarrow x] \\
\Leftarrow & \quad \{ [a;x \Rightarrow x] \} \\
 & [a ; q.n ; b \Rightarrow a;x] \\
\Leftarrow & \quad \{ \text{monotonicity } ; \} \\
 & [q.n ; b \Rightarrow x] \,.
\end{array}
$$

By substituting $b := [\,]$ we derive for t

(7) $\quad [t \equiv \langle \exists n: n \geq 0: q.n \rangle]$,

and now we are ready to establish (4)

$$
\begin{array}{ll}
 & s \\
= & \quad \{ (5) \} \\
 & \langle \exists n: n \geq 0: q.n ; b \rangle \\
= & \quad \{ ; \text{ over } \exists \} \\
 & \langle \exists n: n \geq 0: q.n \rangle ; b \\
= & \quad \{ (7) \} \\
 & t ; b
\end{array}
$$

(End of Proof 0)

Proof 0 uses that relational composition is associative, sufficiently disjunctive and has J as its neutral element. It is the type of proof that I may have preferred 15 years ago, but now it annoys me a little, as its mathematical induction over the naturals strikes me as a foreign element.

Proof 1 Here (4) is established by means of a ping-pong argument; ping is easy.

$$
\begin{array}{ll}
 & [\, s \Rightarrow t;b \,] \\
\Leftarrow & \quad \{ (3) \text{ with } x := t;b \} \\
 & [\, b \Rightarrow t;b \,] \;\wedge\; [\, a;t;b \Rightarrow t;b \,] \\
\Leftarrow & \quad \{ \text{monotonicity of } ; \} \\
 & [\, \mathsf{J} \Rightarrow t \,] \;\wedge\; [\, a;t \Rightarrow t \,] \\
= & \quad \{ (0) \} \\
 & \text{true} \quad .
\end{array}
$$

Pong uses the exchange rules, primarily to get t all by itself in the antecedent position:

$$
\begin{array}{ll}
 & [\, t;b \Rightarrow s \,] \\
= & \quad \{ \text{left exchange} \} \\
 & [\, \neg s;\sim b \Rightarrow \neg t \,] \\
= & \quad \{ \text{contrapositive} \} \\
 & [\, t \Rightarrow \neg(\neg s;\sim b) \,] \\
\Leftarrow & \quad \{ (1) \text{ with } x := \neg(\neg s;\sim b) \} \\
 & [\, \mathsf{J} \Rightarrow \neg(\neg s;\sim b) \,] \;\wedge\; [\, a;\neg(\neg s;\sim b) \Rightarrow \neg(\neg s;\sim b) \,] \\
= & \quad \{ \text{contrapositive ; right exchange} \} \\
 & [\, \neg s;\sim b \Rightarrow \neg \mathsf{J} \,] \;\wedge\; [\, \sim a;\neg s;\sim b \Rightarrow \neg s;\sim b \,]
\end{array}
$$

$\Leftarrow$ {left exchange and monotonicities}

$[\ ];b \Rightarrow s] \ \wedge \ [\neg a;\neg s \Rightarrow \neg s]$

$=$ {$[\ ]$ and right exchange}

$[b \Rightarrow s] \wedge [a;s \Rightarrow s]$

$=$ {(2)}

true

(End of Proof 1).

In a global sense, Proof 1 isn't too bad: the way in which ping uses (0) & (3) and pong uses (1)&(2) is absolutely standard, and since, say, 1985, I can write that down without thinking. There is, however, a dual problem with pong: firstly, all those negations giving rise to contrapositives that don't really contribute to the argument — Rutger M. Dijkstra's objection — and the $\neg$, which now can be regarded as a foreign element.

Proof 2 Ping as above. For pong, we first observe that on account of monotonicities

$$[t \Rightarrow u] \wedge [u;b \Rightarrow s] \Rightarrow [t;b \Rightarrow s] \ .$$

In order to ease the demonstration of $[t \Rightarrow u]$, we want to choose a weak u. Fortunately, $x: [x;b \Rightarrow s]$ has a weakest solution (because $;$ is universally disjunctive); calling it u we have

(8) $\quad [u;b \Rightarrow s]$

(9) $\quad [x;b \Rightarrow s] \Rightarrow [x \Rightarrow u]$ for all x .

And now we observe

$$
\begin{array}{ll}
 & [t;b \Rightarrow s] \\
\Leftarrow & \quad \{\text{monotonicities}\} \\
 & [t \Rightarrow u] \wedge [u;b \Rightarrow s] \\
= & \quad \{(8)\} \\
 & [t \Rightarrow u] \\
\Leftarrow & \quad \{(1) \text{ with } x := u\} \\
 & [\,] \Rightarrow u] \wedge [a;u \Rightarrow u] \\
\Leftarrow & \quad \{(9) \text{ with } x := \,] \text{ , with } x := a;u\} \\
 & [\,];b \Rightarrow s] \wedge [a;u;b \Rightarrow s] \\
\Leftarrow & \quad \{\,] \text{ and } (8)\} \\
 & [b \Rightarrow s] \wedge [a;s \Rightarrow s] \\
= & \quad \{(2)\} \\
 & \text{true}
\end{array}
$$

(End of Proof 2)

Formulae (8) and (9) capture in the traditional manner that u is the weakest solution of $x: [x;b \Rightarrow s]$. They do not capture the consequence of the fact that $[x;b \Rightarrow s]$ is an antimonotonic function of x, i.e. that any predicate stronger than the weakest solution solves the equation as well. We take that in account by replacing (9) by

(10) $\quad [x;b \Rightarrow s] \equiv [x \Rightarrow u]$ for all x

which reduces (8) to a consequence (instantiate (10) with $x := u$).

The tradition is emerging to eliminate the identifier u and to write s/b instead - read: "s over b" - . The infix operator $/$ is now defined by

(11) $[x;y \Rightarrow z] \equiv [x \Rightarrow z/y]$ for all x,y,z.

(Notice the difference between (10) and (11): (10) was used to define u in terms of b and s, (11) defines the operator $/$.) The analogue of (8),

(12) $[(z/y);y \Rightarrow z]$ for all y,z ,

becomes a consequence, known as the law of "cancelation". We can now rewrite our last calculation as follows

$[t;b \Rightarrow s]$

$=$ { def. of $/$ }

$[t \Rightarrow s/b]$

$\Leftarrow$ { (1) with $x := s/b$ }

$[\,] \Rightarrow s/b] \;\wedge\; [a;(s/b) \Rightarrow s/b]$

$=$ { def. of $/$, twice }

$[\,];b \Rightarrow s] \;\wedge\; [a;(s/b);b \Rightarrow s]$

$\Leftarrow$ { $[\,]$ and cancelation + monotonicities }

$[b \Rightarrow s] \;\wedge\; [a;s \Rightarrow s]$

$=$ { (2) }

true .

We could do without the step that introduced u, as the monotonicities exploited have now been captured by the introduction of $/$.

Similarly, we can define $\backslash$ -read "under"- by

(13) $[x;y \Rightarrow z] \equiv [y \Rightarrow x\backslash z]$

with its own law of cancelation

(14) $[x;(x\backslash z) \Rightarrow z]$.

The fact that using formulae like (8) and (9) or (10) is a general technique raises the question: are the equations $x:[x;y\Rightarrow z]$ and $y:[x;y\Rightarrow z]$ so special that their solutions deserve special operators (or functions) to denote them?

(11) is of the form $[f.x \Rightarrow z] \equiv [x \Rightarrow g.z]$, i.e. the form of a Galois connection, and so is (13). Given an f, the introduction of its Galois partner g may be a simple way of capturing that it exists (and that f is universally disjunctive), but it is most rewarding if g has much nicer manipulative properties than f. It looks as if the answer to the question raised can only be given by the outcome of a systematic study of how we can manipulate with $/$ and $\backslash$.

Austin, 16 October 1992

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