A problem in the regularity calculus

H. Peter Hofstee

Computer Science Department
California Institute of Technology

Caltech-CS-TR-93-42

HPH27

A problem in the regularity calculus.

H. Peter Hofstee

Computer Science
California Institute of Technology
Pasadena, CA 91125
December 21, 1993

1 Introduction

The problem examined in this note is specified as follows.
Given
(0) $[J \Rightarrow \neg\Diamond Q]$,
(1) $[P; P \Rightarrow \neg\Diamond Q]$,
(2) $[Q \Rightarrow \neg\Diamond P]$,
prove
$[P^* \Rightarrow \neg\Diamond Q]$, where $[P^* = \mu(X : X = J \vee P; X)]$.
The problem was communicated by C.A.R. Hoare.

2 Axioms

Our starting point is the relational calculus (see e.g. R. Dijkstra '92) without the $\sim$ and without the exchange rules or the cone rule. We add the following three axioms (remember $\langle X \rangle = \neg[\neg X]$):

(3) $\forall(A, B :: \langle J \ \wedge \ A\rangle \ \wedge \ \langle J \ \wedge \ B\rangle = \langle J \ \wedge \ A; B\rangle)$

(4) $\forall(A, B :: \langle A; B\rangle = \langle A\rangle \ \wedge \ \langle B\rangle)$

(5) $\forall(A, B, C, D :: \langle A; B \ \wedge \ C; D\rangle =$
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C\rangle \ \wedge \ \langle A1; B \ \wedge \ D\rangle) \vee$
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C0\rangle \ \wedge \ \langle B \ \wedge \ C1; D\rangle))$

Axiom (3) expresses the absence of an inverse w.r.t. ; .

Axiom (4) is a strengthening of a property in the relational calculus: $\langle A; B\rangle \Rightarrow \langle A\rangle \ \wedge \ \langle B\rangle$.

Axiom (5) is inspired by the model of sets of sequences. I am quite unhappy with this ugly axiom and I hope someone will show me a way to replace it with more elegant ones.

We can rewrite (3) as follows,

$$\begin{aligned}
&\langle J \ \wedge \ A\rangle \ \wedge \ \langle J \ \wedge \ B\rangle = \langle J \ \wedge \ A; B\rangle \\
&= \{ \text{ Definition 'somewhere', pred. calculus } \} \\
&\quad \neg[\neg J \vee \neg A] \ \wedge \ \neg[\neg J \vee \neg B] = \neg[\neg J \vee \neg(A; B)] \\
&= \{ \text{ Pred. calc. } \} \\
&\quad \neg[J \Rightarrow \neg A] \ \wedge \ \neg[J \Rightarrow \neg B] = \neg[J \Rightarrow \neg(A; B)] \\
&= \{ \ (A = B) = (\neg A = \neg B) \ \} \\
&\quad [J \Rightarrow \neg A] \vee [J \Rightarrow \neg B] = [J \Rightarrow \neg(A; B)]
\end{aligned}$$

Using (4) we prove:

$$\begin{aligned}
&\langle \Diamond A \ \wedge \ B\rangle \ \wedge \ \langle C\rangle \\
&= \{ \ (4) \ \} \\
&\quad \langle (\Diamond A \ \wedge \ B); C\rangle \\
&\rightarrow \{ \text{ Monotonicity of } ; \ \} \\
&\quad \langle \Diamond A; C \ \wedge \ B; C\rangle \\
&\Rightarrow \{ \ \mathit{true}; C \Rightarrow \mathit{true}, \text{hence } \Diamond A; C \Rightarrow \Diamond A \ \} \\
&\quad \langle \Diamond A \ \wedge \ B; C\rangle
\end{aligned}$$

Hence,

(6) $\langle \Diamond A \ \wedge \ B\rangle \ \wedge \ \langle C\rangle \Rightarrow \langle \Diamond A \ \wedge \ B; C\rangle$

Which we can rewrite as,

$$\begin{aligned}
&\langle \Diamond A \ \wedge \ B\rangle \ \wedge \ \langle C\rangle \Rightarrow \langle \Diamond A \ \wedge \ B; C\rangle \\
&= \{ \text{ Pred. calc. } \} \\
&\quad \neg\langle \Diamond A \ \wedge \ B\rangle \vee \neg\langle C\rangle \Leftarrow \neg\langle \Diamond A \ \wedge \ B; C\rangle \\
&= \{ \text{ Definition } \langle\rangle \ \} \\
&\quad [\neg B \vee \neg\Diamond A] \vee \neg\langle C\rangle \Leftarrow [\neg(B; C) \vee \neg\Diamond A] \\
&= \{ \text{ Pred. calc. } \} \\
&\quad [B; C \Rightarrow \neg\Diamond A] \ \wedge \ \langle C\rangle \Rightarrow [B \Rightarrow \neg\Diamond A]
\end{aligned}$$

Hence,

(7) $[B; C \Rightarrow \neg\Diamond A] \ \wedge \ \langle C\rangle \Rightarrow [B \Rightarrow \neg\Diamond A]$

Similarly we can prove,

(6') $\langle \Diamond A \ \wedge \ B \rangle \ \wedge \ \langle C \rangle \Rightarrow \langle \Diamond A \ \wedge \ C; B \rangle$
(7') $[C; B \Rightarrow \neg \Diamond A] \ \wedge \ \langle C \rangle \Rightarrow [B \Rightarrow \neg \Diamond A]$

Using the axioms we prove,

$\langle A \ \wedge \ C; D \rangle$
$=$ { J is identity for ; }
$\langle A; J \ \wedge \ C; D \rangle$
$=$ { (5) }
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C \rangle \ \wedge \ \langle A1; J \ \wedge \ D \rangle) \vee$
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C0 \rangle \ \wedge \ \langle J \ \wedge \ C1; D \rangle)$
$=$ { (3), J is identity of ; }
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C \rangle \ \wedge \ \langle A1 \ \wedge \ D \rangle) \vee$
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C0 \rangle \ \wedge \ \langle J \ \wedge \ C1 \rangle \ \wedge \ \langle J \ \wedge \ D \rangle)$
$=$ { Begin subproof }
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C0 \rangle \ \wedge \ \langle J \ \wedge \ C1 \rangle \ \wedge \ \langle J \ \wedge \ D \rangle)$
$=$ { (4) }
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle (A \ \wedge \ C0); (J \ \wedge \ C1) \rangle \ \wedge \ \langle J \ \wedge \ D \rangle)$
$\Rightarrow$ { Monotonicity of ; , J unit of ; }
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C0; C1 \rangle \ \wedge \ \langle J \ \wedge \ D \rangle)$
$\Rightarrow$ { Monotonicity of $\langle\rangle$ }
$\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A \ \wedge \ C \rangle \ \wedge \ \langle J \ \wedge \ D \rangle)$
$=$ { Choose $C0 := C, C1 := J$,term is independent of bound variables }
$\langle A \ \wedge \ C \rangle \ \wedge \ \langle J \ \wedge \ D \rangle$
$\Rightarrow$ { Choose $A0 := A, A1 := J$ }
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C \rangle \ \wedge \ \langle A1 \ \wedge \ D \rangle)$
$=$ { End subproof }
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C \rangle \ \wedge \ \langle A1 \ \wedge \ D \rangle)$

Hence,

(8) $\forall(A, C, D :: \langle A \ \wedge \ C; D \rangle =$
$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ C \rangle \ \wedge \ \langle A1 \ \wedge \ D \rangle))$

We next derive a few variants of (5).

$$
\begin{array}{l}
\quad \langle A;\ B\ \wedge\ C;\ D\rangle \\
= \{\ (5)\ \} \\
\quad \exists(A0, A1 : [A0;\ A1 \Rightarrow A] : \langle A0\ \wedge\ C\rangle\ \wedge\ \langle A1;\ B\ \wedge\ D\rangle) \vee \\
\quad \exists(C0, C1 : [C0;\ C1 \Rightarrow C] : \langle A\ \wedge\ C0\rangle\ \wedge\ \langle B\ \wedge\ C1;\ D\rangle) \\
= \{\ (8)\ \} \\
\quad \exists(A0, A1 : [A0;\ A1 \Rightarrow A] : \langle A0\ \wedge\ C\rangle\ \wedge\ \langle A1;\ B\ \wedge\ D\rangle) \vee \\
\quad \exists(C0, C1 : [C0;\ C1 \Rightarrow C] : \langle A\ \wedge\ C0\rangle\ \wedge \\
\qquad \exists(B0, B1 : [B0;\ B1 \Rightarrow B] : \langle B0\ \wedge\ C1\rangle\ \wedge\ \langle B1\ \wedge\ D\rangle)) \\
= \{\ \text{Pred. calc.}\ \} \\
\quad \exists(A0, A1 : [A0;\ A1 \Rightarrow A] : \langle A0\ \wedge\ C\rangle\ \wedge\ \langle A1;\ B\ \wedge\ D\rangle) \vee \\
\quad \exists(B0, B1 : [B0;\ B1 \Rightarrow B] : \\
\qquad \exists(C0, C1 : [C0;\ C1 \Rightarrow C] : \langle A\ \wedge\ C0\rangle\ \wedge\ \langle B0\ \wedge\ C1\rangle)\ \wedge \\
\qquad \langle B1\ \wedge\ D\rangle)) \\
= \{\ (8)\ \} \\
\quad \exists(A0, A1 : [A0;\ A1 \Rightarrow A] : \langle A0\ \wedge\ C\rangle\ \wedge\ \langle A1;\ B\ \wedge\ D\rangle) \vee \\
\quad \exists(B0, B1 : [B0;\ B1 \Rightarrow B] : \langle A;\ B0\ \wedge\ C\rangle\ \wedge\ \langle B1\ \wedge\ D\rangle))
\end{array}
$$

Hence,

$$
\begin{array}{ll}
(9) & \forall(A, B, C, D :: \langle A;\ B\ \wedge\ C;\ D\rangle = \\
& \exists(A0, A1 : [A0;\ A1 \Rightarrow A] : \langle A0\ \wedge\ C\rangle\ \wedge\ \langle A1;\ B\ \wedge\ D\rangle) \vee \\
& \exists(B0, B1 : [B0;\ B1 \Rightarrow B] : \langle A;\ B0\ \wedge\ C\rangle\ \wedge\ \langle B1\ \wedge\ D\rangle))
\end{array}
$$

Similarly one can prove,

$$
\begin{array}{ll}
(10) & \forall(A, B, C, D :: \langle A;\ B\ \wedge\ C;\ D\rangle = \\
& \exists(D0, D1 : [D0;\ D1 \Rightarrow D] : \langle A\ \wedge\ C;\ D0\rangle\ \wedge\ \langle B\ \wedge\ D1\rangle) \vee \\
& \exists(B0, B1 : [B0;\ B1 \Rightarrow B] : \langle A;\ B0\ \wedge\ C\rangle\ \wedge\ \langle B1\ \wedge\ D\rangle))
\end{array}
$$

We next prove a property that will serve us well in the next section.

(11) $\forall(A, B, C, D :: \langle A; B; C \ \wedge \ \Diamond D\rangle \ \wedge \ [D \Rightarrow \neg\Diamond B] \Rightarrow$
$(\langle A; B \ \wedge \ \Diamond D\rangle \ \wedge \ \langle C\rangle) \vee (\langle A\rangle \ \wedge \ \langle B; C \ \wedge \ \Diamond D\rangle))$

$\langle A; B; C \ \wedge \ \Diamond D\rangle$

$=$ { Definition $\Diamond$ }

$\langle A; B; C \ \wedge \ true; D; true\rangle$

$=$ { (5) }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ true\rangle \ \wedge \ \langle A1; B; C \ \wedge \ D; true\rangle) \vee$

$\exists(T0, T1 : [T0; T1 \Rightarrow true] : \langle A \ \wedge \ T0\rangle \ \wedge \ \langle B; C \ \wedge \ T1; D; true\rangle)$

$=$ { (10), Pred. calc. }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ true\rangle \ \wedge$

$(\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle A1; B; C0 \ \wedge \ D\rangle \ \wedge \ \langle C1 \ \wedge \ true\rangle) \vee$

$\exists(T0, T1 : [T0; T1 \Rightarrow true] : \langle A1; B \ \wedge \ D; T0\rangle \ \wedge \ \langle C \ \wedge \ T1\rangle))) \vee$

$\exists(T0, T1 :: \langle A \ \wedge \ T0\rangle \ \wedge \ \langle B; C \ \wedge \ T1; D; true\rangle)$

$\Rightarrow$ { Monotonicity $\exists, \langle\rangle, ;, \ \wedge, \vee$ }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0 \ \wedge \ true\rangle \ \wedge$

$(\exists(C0, C1 : [C0; C1 \Rightarrow C] : \langle true; B; true \ \wedge \ D\rangle \ \wedge \ \langle C1 \ \wedge \ true\rangle) \vee$

$\langle A1; B \ \wedge \ D; true\rangle \ \wedge \ \langle C \ \wedge \ true\rangle)) \vee$

$(\langle A \ \wedge \ true\rangle \ \wedge \ \langle B; C \ \wedge \ true; D; true\rangle)$

$=$ { $[D \Rightarrow \neg\Diamond B] = \neg\langle D \ \wedge \ \Diamond B\rangle$ }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0\rangle \ \wedge \ \langle A1; B \ \wedge \ D; true\rangle \ \wedge \ \langle C\rangle) \vee$

$(\langle A\rangle \ \wedge \ \langle B; C \ \wedge \ \Diamond D\rangle)$

$=$ { (4) }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0; (A1; B \ \wedge \ D; true)\rangle \ \wedge \ \langle C\rangle) \vee$

$(\langle A\rangle \ \wedge \ \langle B; C \ \wedge \ \Diamond D\rangle)$

$\Rightarrow$ { Monotonicity of ; }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A0; A1; B \ \wedge \ A0; D; true\rangle \ \wedge \ \langle C\rangle) \vee$

$(\langle A\rangle \ \wedge \ \langle B; C \ \wedge \ \Diamond D\rangle)$

$\Rightarrow$ { Monotonicities }

$\exists(A0, A1 : [A0; A1 \Rightarrow A] : \langle A; B \ \wedge \ true; D; true\rangle \ \wedge \ \langle C\rangle) \vee$

$(\langle A\rangle \ \wedge \ \langle B; C \ \wedge \ \Diamond D\rangle)$

$=$ { $A; J = A$, hence $\exists$... }

$$(\langle A;\, B \ \wedge\ \Diamond D\rangle \ \wedge\ \langle C\rangle)\vee$$
$$(\langle A\rangle \ \wedge\ \langle B;\, C \ \wedge\ \Diamond D\rangle)$$

3 An inductive proof

We prove by induction $\forall(n : n \geq 0 : [P^n \Rightarrow \neg\Diamond Q])$. We observe the theorem is trivially true if $\neg\langle P\rangle$, hence we may assume $\langle P\rangle$.

Case $n = 0$:

$$\begin{aligned} & [P^0 \Rightarrow \neg\Diamond Q] \\ = & \{\ \forall(A :: A^0 = J)\ \} \\ & [J \Rightarrow \neg\Diamond Q] \\ = & \{\ (0)\ \} \\ & \mathit{true} \end{aligned}$$

Case $n = 1$:

$$\begin{aligned} & [P \Rightarrow \neg\Diamond Q] \\ \Leftarrow & \{\ (7)\ \} \\ & \langle P\rangle \ \wedge\ [P;\, P \Rightarrow \neg\Diamond Q] \\ = & \{\ \text{Assumption, (1)}\ \} \\ & \mathit{true} \end{aligned}$$

Induction step:

$$\begin{aligned} & \neg[P^m \rightarrow \neg\Diamond Q] \\ = & \{\ \text{Predicate calculus}\ \} \\ & \langle P^m \ \wedge\ \Diamond Q\rangle \\ = & \{\ m \geq 2\text{, definition } \Diamond\ \} \\ & \langle P;\, P;\, P^{m-2} \ \wedge\ \Diamond Q\rangle \\ \Rightarrow & \{\ (11)\text{: } A := P, B := P, C := P^{m-2}, D := Q\ \} \\ & (\langle P;\, P \ \wedge\ \Diamond Q\rangle \ \wedge\ \langle P^{m-2}\rangle)\vee \\ & (\langle P\rangle \ \wedge\ \langle P;\, P^{m\ -2} \ \wedge\ \Diamond Q) \\ = & \{\ \text{Pred. calc.}\ \} \\ & (\neg[P;\, P \Rightarrow \neg\Diamond Q] \ \wedge\ \langle P^{m-2}\rangle)\vee \\ & (\langle P\rangle \ \wedge\ \neg[P^{m-1} \Rightarrow \neg\Diamond Q]) \\ = & \{\ [P;\, P \Rightarrow \neg\Diamond Q]\text{, Induction hypothesis.}\ \} \\ & \mathit{false} \end{aligned}$$

The proof is completed by the observation $\mu(X : X = J \vee P;\, X) = \exists(n : n \geq 0 : P^n)$ which is a consequence of the fact that $\lambda X.(J \vee P;\, X)$ is continous. A proof can be found in (van de Snepscheut '93, page 45).

4 A proof without induction (for the brave).

We use the definition of P^* as a least (strongest) fixpoint.

$$[P^* = \mu(X : X = J \vee P; X)]$$

Using Knaster Tarski,

$$[P^* = \mu(X : X \Leftarrow J \vee P; X)]$$

and, since P^* is the least solution,

$$\forall(X :: [J \vee P; X \Rightarrow X] \Rightarrow [P^* \Rightarrow X])$$

.

To prove $[P^* \Rightarrow \neg\Diamond Q]$ we are thus inspired to prove,

$$[J \vee P; \neg\Diamond Q \rightarrow \neg\Diamond Q]$$

which is equivalent to

$$[J \rightarrow \neg\Diamond Q] \ \wedge \ [P; \neg\Diamond Q \rightarrow \neg\Diamond Q]$$

.

Unfortunately, the r.h.s. of this formula is not true in all models, and hence unprovable. Choose for instance regular expressions (or sets of sequences), $P = \lambda x.x =' ba'$ $Q = \lambda x.x =' aa'$. These choices satisfy (0),(1), and (2) above. With this choice $\neg\Diamond Q.'a'$ and hence $(P; \neg\Diamond Q).'baa'$, but $\neg(\neg\Diamond Q).'baa'$.

Our next attempt is a strengtening of X, containing $\neg\Diamond Q$ as a conjunct, i.e. $[X = R \ \wedge \ \neg\Diamond Q]$. Using Knaster Tarski again we find it suffices to prove:

$$\exists(R :: [J \vee P; (\neg\Diamond Q \ \wedge \ R) \Rightarrow (\neg\Diamond Q \ \wedge \ R)])$$

In the following calculation we 'discover' the choice $R = J \vee P; \neg\Diamond Q$, which corresponds to the right hand side of the fixpoint equation.

We have,

$$\begin{aligned} & [J \vee P; (X \ \wedge \ (J \vee P; X)) \Rightarrow (X \ \wedge \ (J \vee P; X))] \\ = & \ \{ \text{ Predicate calculus } \} \\ & [J \Rightarrow X] \ \wedge \ [P; (X \ \wedge \ (J \vee P; X)) \Rightarrow X] \end{aligned}$$

Now, if indeed $[P^* \Rightarrow X]$ then the first conjunct is true, whereas according to the fixpoint equation the left hand side of the second conjunct is indeed a strengthening.

$$
\begin{array}{l}
\quad \exists(R :: [J \vee P; (\neg\Diamond Q \ \wedge \ R) \Rightarrow (\neg\Diamond Q \ \wedge \ R)]) \\
= \{ \text{ Pred. calc. } \} \\
\quad \exists(R :: [J \Rightarrow \neg\Diamond Q] \ \wedge \ [J \Rightarrow R] \ \wedge \\
\qquad\quad [P; (\neg\Diamond Q \ \wedge \ R) \Rightarrow \neg\Diamond Q] \ \wedge \\
\qquad\quad [P; (\neg\Diamond Q \ \wedge \ R) \Rightarrow R]) \\
\Leftarrow \{ \text{ Choose } R = R' \vee J, (0) \ \} \\
\quad \exists(R' :: [J \Rightarrow R' \vee J] \ \wedge \\
\qquad\quad [P; (\neg\Diamond Q \ \wedge \ (R' \vee J)) \Rightarrow \neg\Diamond Q] \ \wedge \\
\qquad\quad [P; (\neg\Diamond Q \ \wedge \ (R' \vee J)) \Rightarrow (R' \vee J)]) \\
= \{ \text{ Pred. calc. } \} \\
\quad \exists(R' :: [P; (\neg\Diamond Q \ \wedge \ (R' \vee J)) \Rightarrow \neg\Diamond Q] \ \wedge \\
\qquad\quad [P; (\neg\Diamond Q \ \wedge \ (R' \vee J)) \Rightarrow (R' \vee J)]) \\
\Leftarrow \{ \text{ Choose } R' = P; \neg\Diamond Q \ \} \\
\quad [P; (\neg\Diamond Q \ \wedge \ (P; \neg\Diamond Q \vee J)) \Rightarrow \neg\Diamond Q] \ \wedge \\
\quad [P; (\neg\Diamond Q \ \wedge \ (P; \neg\Diamond Q \vee J)) \Rightarrow (P; \neg\Diamond Q \vee J)] \\
= \{ \ [A; (B \ \wedge \ C) \Rightarrow (A; B \vee D)] \ \} \\
\quad [P; (\neg\Diamond Q \ \wedge \ (P; \neg\Diamond Q \vee J)) \Rightarrow \neg\Diamond Q] \\
= \{ \text{ Pred. calc. } \} \\
\quad [P; ((\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \vee (\neg\Diamond Q \ \wedge \ J)) \Rightarrow \neg\Diamond Q] \\
= \{ \ [J \Rightarrow \neg\Diamond Q] \ \} \\
\quad [P; ((\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \vee J) \Rightarrow \neg\Diamond Q] \\
= \{ \ ; \text{ is disjunctive,[ ] is conjunctive } \} \\
\quad [P; (\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \Rightarrow \neg\Diamond Q] \ \wedge \ [P; J \Rightarrow P; \neg\Diamond Q] \\
= \{ \ [J \Rightarrow \neg\Diamond Q] \Rightarrow [P; J \Rightarrow P; \neg\Diamond Q], \text{ definition } \langle\rangle \ \} \\
\quad \neg\langle P; (\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \ \wedge \ true; Q; true\rangle \\
= \{ \ (5) \ A := P, B := \neg\Diamond Q \ \wedge \ P; \neg\Diamond Q, C := true, D := Q; true \ \} \\
\quad \neg\exists(P0, P1 : [P0; P1 \Rightarrow P] : \langle (P0 \ \wedge \ true); (P1; (\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \ \wedge \ Q; true)\rangle) \ \wedge \\
\quad \neg\exists(T0, T1 : [T0; T1 \Rightarrow true] : \langle (P \ \wedge \ T0); (\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q \ \wedge \ T1; Q; true)\rangle) \\
\Leftarrow \{ \ \neg(true; Q; true) \ \wedge \ (T1; Q; true) = false, \langle A; B\rangle = \langle A\rangle \ \wedge \ \langle B\rangle \ \} \\
\quad \neg\exists(P0, P1 : [P0; P1 \Rightarrow P] : \langle P0\rangle \ \wedge \ \langle (P1; (\neg\Diamond Q \ \wedge \ P; \neg\Diamond Q) \ \wedge \ Q; true)\rangle)
\end{array}
$$

continued on next page ..

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] : \langle P0\rangle \ \wedge\ \langle (P1;\ (\neg\Diamond Q \ \wedge\ P;\ \neg\Diamond Q) \ \wedge\ Q;\ true)\rangle)$$

$\Leftarrow$ { $A;\ (B \ \wedge\ C) \Rightarrow A;\ C$ }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] : \langle P0\rangle \ \wedge\ \langle (P1;\ P;\ \neg\Diamond Q \ \wedge\ Q;\ true)\rangle)$$

$=$ { (5) $A := P1;\ P, B := \neg\Diamond Q, C := Q, D := true$ }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] : \langle P0\rangle$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle (P2 \ \wedge\ Q);\ (P3;\ \neg\Diamond Q \ \wedge\ true)\rangle)\vee$$
$$\exists(Q0, Q1 : [Q0;\ Q1 \Rightarrow Q] : \langle (P1;\ P \ \wedge\ Q0);\ (\neg\Diamond Q \ \wedge\ Q1;\ true)\rangle))$$

$\Leftarrow$ { $\langle A;\ B\rangle \Rightarrow \langle A\rangle$ }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle P2 \ \wedge\ Q\rangle)\vee$$
$$\exists(Q0, Q1 : [Q0;\ Q1 \Rightarrow Q] : \langle P1;\ P \ \wedge\ Q0\rangle))$$

$\Leftarrow$ { $[A \Rightarrow \Diamond A], [A;\ B \Rightarrow \Diamond B]$ }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle P2 \ \wedge\ \Diamond Q\rangle)\vee$$
$$\exists(Q0, Q1 : [Q0;\ Q1 \Rightarrow Q] : \langle \Diamond P \ \wedge\ Q0\rangle))$$

$=$ { (6): $\langle \Diamond A \ \wedge\ B\rangle \ \wedge\ \langle C\rangle \Rightarrow \langle \Diamond A \ \wedge\ B;\ C\rangle$ }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle P2;\ P3 \ \wedge\ \Diamond Q\rangle)\vee$$
$$\exists(Q0, Q1 : [Q0;\ Q1 \rightarrow Q] : \langle \Diamond P \ \wedge\ Q0;\ Q1\rangle))$$

$\Leftarrow$ { Calculus }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle P1;\ P \ \wedge\ \Diamond Q\rangle)\vee$$
$$\exists(Q0, Q1 : [Q0;\ Q1 \Rightarrow Q] : \langle \Diamond P \ \wedge\ Q\rangle))$$

$\Leftarrow$ { $[Q \Rightarrow \neg\Diamond P] = \neg\langle Q \ \wedge\ \Diamond P\rangle$,(4) }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \rightarrow P1;\ P] : \langle P0;\ P1;\ P \ \wedge\ \Diamond Q\rangle))$$

$\Leftarrow$ { Calculus }

$$\neg\exists(P0, P1 : [P0;\ P1 \Rightarrow P] :$$
$$\exists(P2, P3 : [P2;\ P3 \Rightarrow P1;\ P] : \langle P;\ P \ \wedge\ \Diamond Q\rangle))$$

$=$ { $[P;\ P \Rightarrow \neg\Diamond Q] \Rightarrow \neg\langle P;\ P \ \wedge\ \Diamond Q\rangle$ }

true

5 Discussion

The following calculation shows a relation between (9) and (4).

$$
\begin{array}{ll}
 & \langle A;\ B\rangle \\
= & \{\ \text{Pred. calc.}\ \} \\
 & \langle \mathit{true}\ \wedge\ A;\ B\rangle \\
= & \{\ \text{Rel. calc.}\ \} \\
 & \langle \mathit{true};\ \mathit{true}\ \wedge\ A;\ B\rangle \\
= & \{\ (9)\ \} \\
 & \exists(T0, T1 : [T0;\ T1 \Rightarrow \mathit{true}] : \langle T0\ \wedge\ A\rangle\ \wedge\ \langle T1;\ \mathit{true}\ \wedge\ B\rangle) \vee \\
 & \exists(T0, T1 : [T0;\ T1 \Rightarrow \mathit{true}] : \langle \mathit{true};\ T0\ \wedge\ A\rangle\ \wedge\ \langle T1\ \wedge\ B\rangle) \\
= & \{\ \text{Pred. calc.}\ \} \\
 & \exists(T0, T1 :: \langle T0\ \wedge\ A\rangle\ \wedge\ \langle T1;\ \mathit{true}\ \wedge\ B\rangle) \vee \\
 & \exists(T0, T1 :: \langle \mathit{true};\ T0\ \wedge\ A\rangle\ \wedge\ \langle T1\ \wedge\ B\rangle) \\
= & \{\ \Leftarrow, \text{choose } \mathit{true} \text{ for } T0, T1.\ \Rightarrow, \text{monotonicity of } \exists, ;, \langle\rangle\ \} \\
 & (\langle \mathit{true}\ \wedge\ A\rangle\ \wedge\ \mathit{true};\ \mathit{true}\ \wedge\ B\rangle) \vee (\langle \mathit{true};\ \mathit{true}\ \wedge\ A\rangle\ \wedge\ \langle \mathit{true}\ \wedge\ B\rangle) \\
= & \{\ \mathit{true};\ \mathit{true} = \mathit{true},\ \text{Pred. calc.}\ \} \\
 & \langle A\rangle\ \wedge\ \langle B\rangle
\end{array}
$$

However, I have not (yet) succeeded in proving (5) from (9) without using (4), so I am still stuck with three axioms.

This note was a preliminary excursion into axiomatic 'string theory', as E.C.R. Hehner calls it. It was motivated by a problem from Burghard von Karger, communicated to me by C.A.R. Hoare.

It seems the axioms I have added do not imply that J is a point predicate, hence the algebra does not use all properties of the model of sets of strings.

Clearly, much work remains.

Acknowledgement

A discussion with Rustan Leino convinced me that I had to add condition (0), and that the relational calculus (without the cone rule) was inappropriate for this problem. Rustan has consolidated our excursions within the relational calculus in KRML 25.

Jan van de Snepscheut scrutinized an earlier version of the paper. If the paper is now error free, it is because of his efforts, if it is not, I am to blame. The observation in section four about the choice for R is Jan's.

References

Rutger M. Dijkstra.
Relational calculus and relational program semantics.
Masters thesis, Universität zu Köln, 1992.

Jan L. A. van de Snepscheut
On lattice theory and program semantics.
Caltech-CS-TR-93-19, California Institute of Technology, 1993.