KRML 25 -0

A proof in the relational calculus

H. Peter Hofstee, K. Rustan M. Leino
Computer Science
California Institute of Technology
Pasadena, CA 91125
3 December 1993

A problem communicated to us from Burghard von Karger via C.A.R. Hoare is, given the definition of $\Diamond$, for all Q, as

$$[\Diamond Q \equiv true;\ Q;\ true] \qquad ,$$

prove

$$\begin{array}{ll} & [Q \Rightarrow \neg\Diamond P] \ \wedge \\ & [P;\ P \Rightarrow \neg\Diamond Q] \\ \Rightarrow & \\ & [P^* \Rightarrow \neg\Diamond Q] \qquad , \end{array}$$

for all P and Q. The definition of * is that from the regularity calculus, namely, for any P, P^* is the strongest solution of

(0) $\quad X : [X \equiv J \vee P;\ X] \qquad .$

By Knaster Tarski, we can reformulate (0) as: P^* is the strongest solution of

(1) $\quad X : [X \Leftarrow J \vee P;\ X] \qquad .$

The problem also bears a stipulation that the cone rule not be used in the proof.

In examining the problem, we note that for $P : [\neg P]$, the statement does not hold without also using in the antecedent

$$[J \Rightarrow \neg\Diamond Q] \qquad .$$

Hence, we change the problem to add this as a conjunct in the antecedent, and calculate, for any P and Q,

$$
\begin{array}{ll}
 & [P^* \Rightarrow \neg\Diamond Q] \\
\Leftarrow & \{\ P^* \text{ is strongest solution of (1): } [J \vee P;\ X \Rightarrow X] \Rightarrow [P^* \Rightarrow X]\text{, with } X := \neg\Diamond Q\ \} \\
 & [J \vee P;\ \neg\Diamond Q \Rightarrow \neg\Diamond Q] \\
= & \{\ \text{calculus}\ \} \\
 & [J \Rightarrow \neg\Diamond Q] \wedge [P;\ \neg\Diamond Q \Rightarrow \neg\Diamond Q] \\
= & \{\ \text{modified problem statement: } [J \Rightarrow \neg\Diamond Q]\ \} \\
 & [P;\ \neg\Diamond Q \Rightarrow \neg\Diamond Q] \\
\Leftarrow & \{\ [P \Rightarrow \mathit{true}] \text{ and monotonicity}\ \} \\
 & [\mathit{true};\ \neg\Diamond Q \Rightarrow \neg\Diamond Q] \\
= & \{\ \text{right exchange}\ \} \\
 & [\sim \mathit{true};\ \Diamond Q \Rightarrow \Diamond Q] \\
= & \{\ \Diamond \text{ and associativity of } ;\ \} \\
 & [\sim \mathit{true};\ \mathit{true};\ Q;\ \mathit{true} \Rightarrow \Diamond Q] \\
= & \{\ [\mathit{true} \equiv\ \sim \mathit{true}] \text{ and } [\mathit{true};\ \mathit{true} \equiv \mathit{true}]\ \} \\
 & [\mathit{true};\ Q;\ \mathit{true} \Rightarrow \Diamond Q] \\
= & \{\ \Diamond \text{ and calculus}\ \} \\
 & \mathit{true} \qquad .
\end{array}
$$

Suspiciously, we have not in this proof used the antecedent for the original problem. Another curiosity is that in our very first step, we use the substitution $X := \neg\Diamond Q$, and $\neg\Diamond Q$ is not even a solution of (0) for P^*.

We trace the source of the problem as follows. The contrapositive of the statement

If Q is contained in P, then either Q is contained in $P;\ P$, or P is contained in Q.

inspired the problem. Operator $\Diamond$, pronounced "ever", was borrowed from temporal logic, and $\Diamond Q$ was intended to represent those strings that contain some string from Q as a substring. Negation provides set complement, and $[\Rightarrow]$ subset. But to apply the relational calculus to a problem of regular expressions, one needs a model, like the one described in [0], that satisfies the axioms of the relational calculus. Then we have

$$
\begin{array}{ll}
 & [P \Rightarrow \neg\Diamond Q] \\
= & \{\ \text{interpretation}\ \} \\
 & \forall(\, p, q : P.p \wedge Q.q : q \text{ is not a substring of } p\ ) \\
= & \{\ \text{interpretation}\ \} \\
 & \forall(\, p, q : P.p \wedge Q.q : \neg\exists(\, r, s :: r;\ q;\ s \ = \ p\ )\ )
\end{array}
$$

$$= \quad \{ \text{ choose } r, s :=\sim q, p \quad \}$$

$$\quad \mathit{false} \qquad ,$$

which shows that the interpretation of substrings is not what the original problem intended.

References

[0] E.W. Dijkstra. The unification of three calculi. In M. Broy, editor, *Program Design Calculi*, NATO ASI Series F. Springer-Verlag, 1993.