An Oxford sequel to EWD1047

In EWD1047 I mentioned

(30) $[P;true \vee true;Q] \Rightarrow [P;true] \vee [true;Q]$

(31) $[P;true] \vee [true;\neg P]$

(32) $[true;\neg X;true] \vee [X]$

and showed how (31) follows from (30) and how (32) follows from (31), and remarked that I did not succeed in proving (30) from (31).

On December 18, 1990, He Jifeng sent me a proof of (30) from (31), which (with a minor correction in a hint) is included here on page EWD1089-1. His references are to the formulae as numbered in EWD1047.

On the 20th December, 1990, Stephen Brien, also from Oxford's Programming Research Group, sent me a derivation of (30) from (32), "thus showing that, given the other axioms of the relational calculus, (30), (31) and (32) are equivalent". His derivation (with a minor correction in a hint) is here included on page EWD1089-2; formula (32) is referred to as "the cone rule".

It is interesting to note that in He Jifeng's proof all steps but 1 are equivalences; (31) is introduced in the same way as (32) in Stephen Brien's proof, viz. as conjunct.

He Jifeng's Proof

A Proof of (30) from (31)

(30) $[P\,;\mathtt{true} \ \vee \ \mathtt{true}\,;Q] \ \Rightarrow \ [P\,;\mathtt{true}] \ \vee \ [\mathtt{true}\,;Q]$

Proof: Let

$$\begin{aligned} X &= \neg(\mathtt{true}\,;Q) \\ Y &= *(P\,;\mathtt{true}) \end{aligned}$$

From (20) and (28) it follows that both X and Y are postconditions. Then one has

$$\begin{aligned}
& [P\,;\mathtt{true} \ \vee \ \mathtt{true}\,;Q] \\
= \quad & \{\textit{predicate calculus and def of } X\} \\
& [X \ \Rightarrow \ P\,;\mathtt{true}] \\
= \quad & \{X \textit{ is a postcondition}\} \\
& [\mathtt{true}\,;X \ \Rightarrow \ P\,;\mathtt{true}] \\
= \quad & \{(15) \textit{ and def of } Y\} \\
& [\mathtt{true} \ \Rightarrow \ *(X\,;Y)] \\
= \quad & \{(0) \textit{ and } (4)\} \\
& [(X\,;Y) \ \Rightarrow \ \mathtt{false}] \\
= \quad & \{\textit{predicate calculus}\} \\
& [\neg(X\,;Y)] \\
= \quad & \{Y \textit{ is a postcondition}\} \\
& [\neg(X\,;\mathtt{true}\,;Y))] \\
= \quad & \{(31) \textit{ and } P := X\} \\
& [\neg(X\,;\mathtt{true}\,;Y)] \ \wedge \ ([X\,;\mathtt{true}] \ \vee \ [\mathtt{true}\,;\neg X]) \\
\Rightarrow \quad & \{\textit{predicate calculus}\} \\
& [\neg(\mathtt{true}\,;Y)] \ \vee \ [\mathtt{true}\,;\neg X] \\
= \quad & \{X \textit{ and } Y \textit{ are } \cancel{\textit{pre}}\textit{conditions and } (28)\} \qquad \text{post} \\
& [\neg Y] \ \vee \ [\neg X] \\
= \quad & \{(20) \textit{ and def of } X \textit{ and } Y\} \\
& [\sim (P\,;\mathtt{true})] \ \vee \ [\mathtt{true}\,;Q] \\
= \quad & \{(20) \textit{ and } [\mathtt{true} \equiv \sim \mathtt{true}]\} \\
& [P\,;\mathtt{true}] \ \vee \ [\mathtt{true}\,;Q]
\end{aligned}$$

* * *

Stephen Brien's Proof

(30) $[P;\ true\ \vee\ true;\ Q]\ \Rightarrow\ [P;\ true]\ \vee\ [true;\ Q]$

Proof (using the cone rule) :

$$
\begin{array}{ll}
 & [P;\ true\ \vee\ true;\ Q] \\
= & \{\textit{Pred Calc}\} \\
 & [\neg(P;\ true)\ \Rightarrow\ true;\ Q] \\
= & \{\neg(P;\ true)\ \textit{is a precondition}\} \\
 & [\neg(P;\ true);\ true\ \Rightarrow\ true;\ Q] \\
\Rightarrow & \{\textit{Monotonicity of ;}\} \\
 & [true;\ \neg(P;\ true);\ true\ \Rightarrow\ true;\ true;\ Q] \\
= & \{\textit{Rel Calc}\} \\
 & [true;\ \neg(P;\ true);\ true\ \Rightarrow\ true;\ Q] \\
= & \{\textit{Cone Rule}\ \cancel{\textit{and}\ (P;\ true) := X}\}\ \text{with}\ X := (P; true) \\
 & ([P;\ true]\ \vee\ [true;\ \neg(P;\ true);\ true])\ \wedge\ [true;\ \neg(P;\ true);\ true\ \Rightarrow\ true;\ Q] \\
\Rightarrow & \{\textit{PredCalc}\} \\
 & [P;\ true]\ \vee\ [true;\ \neg(P;\ true);\ true\ \wedge\ (true;\ \neg(P;\ true);\ true\ \Rightarrow\ true;\ Q)] \\
\Rightarrow & \{\textit{Pred Calc}\} \\
 & [P;\ true]\ \vee\ [true;\ Q]
\end{array}
$$

*   *   *

I thank both gentlemen for their contributions.

Austin, 16 January 1991

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