Misra's Invariant Theorem

Eric C.R. Hehner, Albert Y.C. Lai

2005 July 6

In a recent email message, Jay Misra made a conjecture concerning the existence of “forward-looking” loop invariants. He did not completely formalize it, and did not prove it. We did formalize it and prove it, so it is now a theorem. Here is Jay's statement of the theorem, in his own words and notations and numbering.

Let x be a set of variables, and $f\colon D\to D$ be a function whose domain is the set of states (possible values of f). Given is the loop **while** $b(x)$ **do** S **od** . Assume that $x\in D$ is a loop invariant. Then $x{=}f(x_0)$ holds at the termination of the loop (assume it terminates) iff for all x in D :

1. $\neg b(x) \Rightarrow x{=}f(x)$
2. $f(x){=}f(x_0)$ is invariant

Staying with Jay's notations, except that we use x and x' instead of x_0 and x , and using Dijkstra's $[\ ]$ to mean $\forall x, x'\colon D\cdot$, here is our statement of the theorem.

$$
\begin{aligned}
\forall D\cdot\ \forall f\colon D\to D\cdot \quad & [b(x) \land x\in D \land S(x,x') \Rightarrow x'\in D] \\
\Rightarrow \quad & [x'{=}f(x) \Leftarrow \textbf{while } b(x) \textbf{ do } S(x,x') \textbf{ od}] \\
= \quad & [(\neg b(x) \Rightarrow x{=}f(x)) \land (b(x) \land S(x,x') \Rightarrow f(x'){=}f(x))]
\end{aligned}
$$

I'll spare you the proof (it's not hard), and instead show Jay's example of the use of the theorem. Let A be an array of length N . In the example,

x	is	s, n
$x\in D$	is	$n\le N$
$b(x)$	is	$n\ne N$
$S(x,x')$	is	$s{:=}\ s{+}A[n];\ \ n{:=}\ n{+}1$
$f(x)$	is	$s + (+i\colon n{\le}i{<}N\colon A[i]), N$

The antecedent in the theorem is $[b(x) \land x\in D \land S(x,x') \Rightarrow x'\in D]$, which becomes

$$[n{\ne}N \land n{\le}N \land s'{=}s{+}A[n] \land n'{=}n{+}1 \Rightarrow n'{\le}N]$$

and it is easily proven. The left side of the equation in the theorem is $[x'{=}f(x) \Leftarrow \textbf{while } b(x) \textbf{ do } S(x,x') \textbf{ od}]$, which becomes

$$[s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N \Leftarrow \textbf{while } n{\ne}N \textbf{ do } s{:=}\ s+A[n];\ \ n{:=}\ n+1 \textbf{ od}]$$

The refinement $P \Leftarrow \textbf{while } b \textbf{ do } S \textbf{ od}$ is a shorthand for

$$P \Leftarrow \textbf{if } b \textbf{ then } S;\, P \textbf{ else } \mathit{skip} \textbf{ fi}$$

which is equivalent to

$$P \;\Leftarrow\; b \wedge (S;\, P) \;\vee\; \neg b \wedge \mathit{skip}$$

which is equivalent to

$$(P \;\Leftarrow\; b \wedge (S;\, P)) \wedge (P \;\Leftarrow\; \neg b \wedge \mathit{skip})$$

so it now becomes

$$\begin{array}{lll}
[& (& s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N \\
 & \Leftarrow & n{\ne}N \wedge (s{:=}\ s+A[n];\ \ n{:=}\ n+1;\ \ s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N) \\
 &) & \\
\wedge & (& s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N \\
 & \Leftarrow & n{=}N \wedge s'{=}s \wedge n'{=}n \\
 &) & \\
] & &
\end{array}$$

The expression $(s{:=}\ s+A[n];\ \ n{:=}\ n+1;\ \ s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N)$ is simplified by first replacing n with $n+1$ and then replacing s with $s+A[n]$ in $s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N$ to obtain

$$s'{=}s+A[n]+(+i\colon n+1{\le}i{<}N\colon A[i]) \wedge n'{=}N$$

which simplifies to $s'{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n'{=}N$ and proves the first implication. The second implication is easy, and that proves the left side of the equation. We weren't trying to prove it, but we happen to have proved it. Now we are obliged to prove the right side

$$[(\neg b(x) \Rightarrow x{=}f(x)) \wedge (b(x) \wedge S(x, x') \Rightarrow f(x'){=}f(x))]$$

which becomes

$$\begin{array}{lll}
[& (& n{=}N \\
 & \Rightarrow & s{=}s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge n{=}N \\
 &) & \\
\wedge & (& n{\ne}N \wedge s'{=}s+A[n] \wedge n'{=}n+1 \\
 & \Rightarrow & s'+(+i\colon n'{\le}i{<}N\colon A[i]) = s+(+i\colon n{\le}i{<}N\colon A[i]) \wedge N{=}N \\
 &) & \\
] & &
\end{array}$$

which is a lot like the left side of the theorem.