Soundness Proof of the Transformation Rule used in the WHILE loop

We use Axiomatic Semantics for formulating and proving the rule.

Proposition 1. *Transformation Rule for while loops with conditionals*

$$\frac{\begin{array}{ll}\{I \wedge b1\} & \{I \wedge \neg b1\} \\ \textit{WHILE}[b, & \textit{WHILE}[b, \\ \quad \textit{WHILE}[b \wedge b1, c1]; & \quad \textit{WHILE}[b \wedge \neg b1, c2]; \\ \quad \textit{WHILE}[b \wedge \neg b1, c2]] & \quad \textit{WHILE}[b \wedge b1, c1]] \\ \{I \wedge \neg b\} & \{I \wedge \neg b\}\end{array}}{\{I\}\textit{WHILE}[b, IF[b1, c1, c2]]\{I \wedge \neg b\}} \tag{1}$$

where I denotes the invariant. Also, we assume that the inner WHILEs have the same invariant, i.e.:

$$\{I\}\textit{WHILE}[b \wedge b1, c1]\{I \wedge \neg b \wedge b1\} \tag{2}$$

$$\{I\}\textit{WHILE}[b \wedge \neg b1, c2]\{I \wedge \neg b \wedge \neg b1\} \tag{3}$$

Statement of Soundness Proof:

$$(4) \Leftrightarrow (5),$$

where:

$$\boxed{\{I\}\text{WHILE}[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}, \tag{4}$$

and

$$\boxed{\begin{array}{ll}\{I \wedge b1\} & \{I \wedge \neg b1\} \\ \text{WHILE}[b, & \text{WHILE}[b, \\ \quad \text{WHILE}[b \wedge b1, c1]; & \quad \text{WHILE}[b \wedge \neg b1, c2]; \\ \quad \text{WHILE}[b \wedge \neg b1, c2]] & \quad \text{WHILE}[b \wedge b1, c1]] \\ \{I \wedge \neg b\} & \{I \wedge \neg b\}\end{array}}. \tag{5}$$

Additional Knowledge

Formula manipulation:

$$I \equiv I \wedge (b1 \vee \neg b1) \tag{6}$$

$$\begin{array}{l} I \wedge b \Rightarrow I \\ I \wedge \neg(b \wedge b1) \Rightarrow I \\ I \wedge \neg(b \wedge \neg b1) \Rightarrow I \end{array} \tag{7}$$

Semantic rule for Compositions:

$$\frac{\{P\}c1\{R\} \qquad \{R\}c2\{Q\}}{\{P\}c1; c2\{Q\}} \tag{8}$$

Semantic rule for Conditionals:

$$\frac{\{P \wedge b\}c1\{Q\} \qquad \{P \wedge \neg b\}c2\{Q\}}{\{P\}\text{IF}[b, c1, c2]\{Q\}} \tag{9}$$

Semantic rule for the WHILE loop (for partial correctness):

$$\frac{\{I \wedge b\}c\{I\}}{\{I\}\text{WHILE}[b, c]\{I \wedge \neg b\}} \tag{10}$$

Auxiliary rule:

$$\frac{\{P\}c\{Q\}}{\{P\}\text{IF}[b, c, c]\{Q\}} \tag{11}$$

Proof of (4) $\Rightarrow$ (5)

$$\frac{\dfrac{(NL1)}{\{I \wedge b1\}\text{WHILE}[b, \text{IF}[b1, c1, c2]]\{I \wedge \neg b\}} \qquad \dfrac{(NL2)}{\{I \wedge \neg b1\}\text{WHILE}[b, \text{IF}[b1, c1, c2]]\{I \wedge \neg b\}}}{\{I\}\text{WHILE}[b, \text{IF}[b1, c1, c2]]\{I \wedge \neg b\}}\,6 \tag{12}$$

Deriving the rule for (NL1)

$$\frac{I \wedge b1 \Rightarrow I \qquad \dfrac{\dfrac{(NL1.1)}{\{I \wedge b\}\text{IF}[b1, c1, c2]\{I\}}\,9}{\{I\}\text{WHILE}[b, \text{IF}[b1, c1, c2]]\{I \wedge \neg b\}}\,10}{(NL1)}\,8 \tag{13}$$

$$\frac{\dfrac{\dfrac{\{I\}\text{WHILE}[b \wedge b1,\ c1]\{I \wedge \neg(b \wedge b1)\}}{\{I \wedge b \wedge b1\}c1\{I\}}\,10 \qquad \dfrac{\{I\}\text{WHILE}[b \wedge \neg b1,\ c2]\{I \wedge \neg(b \wedge \neg b1)\}}{\{I \wedge b \wedge \neg b1\}c2\{I\}}\,10}{\{I \wedge b\}\text{WHILE}[b \wedge b1,\ c1]; \text{WHILE}[b \wedge \neg b1,\ c2]\{I\}}\,7+8}{(NL1.1)} \tag{14}$$

Thus, from (13) and (14), we have:

$$\frac{\{I \wedge b1\}\text{WHILE}[b, \text{WHILE}[b \wedge b1,\ c1]; \text{WHILE}[b \wedge \neg b1,\ c2]]\{I \wedge \neg b\}}{(NL1)}\,8 \tag{15}$$

Deriving the rule for (NL2)

We proceed in a similar way as for (NL1), namely:

$$\dfrac{I \wedge \neg b1 \Rightarrow I \quad \dfrac{\dfrac{(NL2.1)}{\{I \wedge b\}\text{IF}[b1, c1, c2]\{I\}}9}{\{I\}\text{WHILE}[b, \text{IF}[b1, c1, c2]]\{I \wedge \neg b\}}10}{(NL2)}8 \tag{16}$$

$$\dfrac{\dfrac{\dfrac{\{I\}\text{WHILE}[b, \text{WHILE}[b \wedge \neg b1,\ c2]; \text{WHILE}[b \wedge b1,\ c1]]\{I \wedge \neg b\}}{\{I \wedge b\}\text{WHILE}[b \wedge \neg b1,\ c2]; \text{WHILE}[b \wedge b1,\ c1]\{I\}}10}{\dfrac{\{I\}\text{WHILE}[b \wedge \neg b1,\ c2]\{I \wedge \neg(b \wedge \neg b1)\}}{\{I \wedge b \wedge \neg b1\}c2\{I\}}10 \quad \dfrac{\{I\}\text{WHILE}[b \wedge b1,\ c1]\{I \wedge \neg(b \wedge b1)\}}{\{I \wedge b \wedge b1\}c1\{I\}}10}7+8}{(NL2.1)} \tag{17}$$

Thus, from (16) and (17), we have:

$$\dfrac{\{I \wedge \neg b1\}\text{WHILE}[b, \text{WHILE}[b \wedge \neg b1,\ c2]; \text{WHILE}[b \wedge b1,\ c1]]\{I \wedge \neg b\}}{(NL2)}8 \tag{18}$$

Hence, from using (15) and (18) in (12), we have:

$$\dfrac{\begin{array}{ll}\{I \wedge b1\} & \{I \wedge \neg b1\}\\ \text{WHILE}[b, & \text{WHILE}[b,\\ \quad \text{WHILE}[b \wedge b1, c1]; & \quad \text{WHILE}[b \wedge \neg b1, c2];\\ \quad \text{WHILE}[b \wedge \neg b1, c2]] & \quad \text{WHILE}[b \wedge b1, c1]]\\ \{I \wedge \neg b\} & \{I \wedge \neg b\}\end{array}}{\{I\}\text{WHILE}[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}.$$

Thus, we have proved: (4)⇒(5).

Proof of (5) ⇒ (4)

$$\dfrac{\begin{array}{l}I \wedge b1 \Rightarrow I \quad \dfrac{(NL3)}{\begin{array}{l}\text{WHILE}[b,\\ \{I\}\ \ \text{WHILE}[b \wedge b1, c1];\quad \{I \wedge \neg b\}\\ \quad\ \text{WHILE}[b \wedge \neg b1, c2]]\end{array}}8\\ \quad \{I \wedge b1\}\\ \quad \text{WHILE}[b,\\ \quad\ \text{WHILE}[b \wedge b1, c1];\\ \quad\ \text{WHILE}[b \wedge \neg b1, c2]]\\ \quad \{I \wedge \neg b\}\end{array} \qquad \begin{array}{l}I \wedge \neg b1 \Rightarrow I \quad \dfrac{(NL4)}{\begin{array}{l}\text{WHILE}[b,\\ \{I\}\ \ \text{WHILE}[b \wedge \neg b1, c2];\ \{I \wedge \neg b\}\\ \quad\ \text{WHILE}[b \wedge b1, c1]]\end{array}}8\\ \quad \{I \wedge \neg b1\}\\ \quad \text{WHILE}[b,\\ \quad\ \text{WHILE}[b \wedge \neg b1, c2];\\ \quad\ \text{WHILE}[b \wedge b1, c1]]\\ \quad \{I \wedge \neg b\}\end{array}}{(3)} \tag{19}$$

Deriving the rule for (NL3)

$$\dfrac{\dfrac{I \wedge b \Rightarrow I \quad \dfrac{\dfrac{\dfrac{\{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}{\{I \wedge b\}IF[b1, c1, c2]\{I\}}10}{\{I \wedge b \wedge b1\}c1\{I\} \quad \{I \wedge b \wedge \neg b1\}c2\{I\}}9}{\{I\}\text{WHILE}[b \wedge b1, c1]\{I \wedge \neg(b \wedge b1)\}}10 \quad \{I\}\text{WHILE}[b \wedge \neg b1, c2]\{I \wedge \neg(b \wedge \neg b1)\}}{\{I\}\text{WHILE}[b \wedge b1, c1]\{I \wedge \neg(b \wedge b1)\}}7 \quad I \wedge \neg(b \wedge b1) \Rightarrow I \quad \{I\}\text{WHILE}[b \wedge \neg b1, c2]\{I \wedge \neg(b \wedge \neg b1)\} \quad I \wedge \neg(b \wedge \neg b1) \Rightarrow I}{\{I\}\text{WHILE}[b \wedge b1, c1]; \text{WHILE}[b \wedge \neg b1, c2]\{I\}}8 + 2 + 3}{\{I \wedge b\}\text{WHILE}[b \wedge b1, c1]; \text{WHILE}[b \wedge \neg b1, c2]\{I\}}8}{(NL3)}10 \tag{20}$$

Hence, from (20) we have:

$$\dfrac{\dfrac{\{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}{I \wedge b \Rightarrow I \quad \{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}7}{(NL3)}20 \tag{21}$$

Deriving the rule for (NL4)

We proceed in a similar way as for (NL4), namely:
and we obtain:

$$\dfrac{\dfrac{\{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}{I \wedge b \Rightarrow I \quad \{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}7}{(NL4)} \tag{22}$$

Hence, using (21) and (22) in 19, we have:

$$\dfrac{\dfrac{\dfrac{\{I\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}{\{I\}IF[b1, WHILE[b, IF[b1, c1, c2]], WHILE[b, IF[b1, c1, c2]]]\{I \wedge \neg b\}}11}{\{I \wedge b1\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\} \quad \{I \wedge \neg b1\}WHILE[b, IF[b1, c1, c2]]\{I \wedge \neg b\}}9}{(3)}8 \tag{23}$$

Thus, we have proved: (5)$\Rightarrow$ (4), and we are done.