CSSE4603/7032 Models of Software Systems

Assignment 3: MSMIE

Samuel Teed 43211915

May 12, 2016

The required definition of *current_config* is

$$
\begin{array}{|l}
current\_config : Ref \times Ref \to CONFIG \\
\hline
\forall\, r, n : Ref \bullet \\
\quad r = n = null \Rightarrow current\_config(r, n) = wii \\
\quad r \neq null \land n \neq null \Rightarrow current\_config(r, n) = wrn \\
\quad r \neq null \land n = null \Rightarrow current\_config(r, n) = wri \\
\quad r = null \land n \neq null \Rightarrow current\_config(r, n) = wni
\end{array}
$$

The proof of refinement follows.

Initialisation

Lemma 1

$\exists\, MSMIE \bullet MSMIEInit \land R$

$\Leftrightarrow$ [definitions of *MSMIE*, *MSMIEInit* and *R*]

$\exists\, config : CONFIG;\ readers : \mathbb{P}\, PID \bullet$

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$config = wii \land$

$config = current\_config(r, n) \land readers = readers1 \land$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing)$

$\Leftrightarrow$ [one-point-rule (config)]

$\exists\, readers : \mathbb{P}\, PID \bullet$

$(current\_config(r, n) \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$current\_config(r, n) = wii \land$

$readers = readers1 \land$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing)$

$\Leftrightarrow$ [one-point-rule (readers)]

$(current\_config(r, n) \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$current\_config(r, n) = wii \land$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers = \varnothing)$

$\Leftrightarrow$ [simplify (current_config definition)]

$r = n = null \land readers = \varnothing \land$

$w \neq null \land w \neq r \land w \neq n$

Theorem 1

$$MSMIEInit1 \vdash \exists\, MSMIE \bullet MSMIEInit \land R$$

1	$r = n = null$	$MSMIEInit1$
2	$readers = \varnothing$	$MSMEI1$
3	$w \neq null \land w \neq r \land w \neq n$	$MSMEI1$

Applicability

Lemma 2

pre $Write$

$\Leftrightarrow$ [definition of $Write$]

$\exists\, config' : CONFIG;\ readers' : \mathbb{P}\, PID \bullet$

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$(config' \in \{wii, wni\} \Leftrightarrow readers' = \varnothing) \land$

$config' = next\_config(config) \land readers' = readers$

$\Leftrightarrow$ [one-point-rule (config')]

$\exists\, readers' : \mathbb{P}\, PID \bullet$

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$(next\_config(config) \in \{wii, wni\} \Leftrightarrow readers' = \varnothing) \land$

$readers' = readers$

$\Leftrightarrow$ [one-point-rule (readers')]

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$(next\_config(config) \in \{wii, wni\} \Leftrightarrow readers = \varnothing)$

$\Leftrightarrow$ [simplify ($\Leftrightarrow$ *definition*)]

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing)$

Assumption 1: There are at least three non-null values of Ref. That is, if x and y are any values of Ref then the following holds.

$$\exists\, z : Ref \bullet z \neq null \land z \neq x \land z \neq y$$

Lemma 3

pre $Write1$

$\Leftrightarrow$ [definition of $Write1$]

$\exists\, w', r', n' : Ref;\ readers1' : \mathbb{P}\, ID \bullet$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$

$n' = w \land r' = r \land readers1' = readers1$

$\Leftrightarrow$ [Assumption 1]

$\exists\, r', n' : Ref;\ readers1' : \mathbb{P}\, ID \bullet$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$(r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$

$n' = w \land r' = r \land readers1' = readers1$

$\Leftrightarrow$ [one-point-rule (r')]

$\exists\, n' : Ref;\ readers1' : \mathbb{P}\, ID \bullet$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$(r = n' \Rightarrow r = n' = null) \land (r = null \Leftrightarrow readers1' = \varnothing) \land$

$n' = w \land readers1' = readers1$

$\Leftrightarrow$ [one-point-rule (n')]

$\exists\, readers1' : \mathbb{P}\, ID \bullet$

$w \neq null \land w \neq r \land w \neq n \land (r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$(r = w \Rightarrow r = w = null) \land (r = null \Leftrightarrow readers1' = \varnothing) \land$

$readers1' = readers1$

$\Leftrightarrow$ [one-point-rule (readers1')]

$w \neq null \land w \neq r \land w \neq n \land$

$(r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$(r = w \Rightarrow r = w = null) \land (r = null \Leftrightarrow readers1 = \varnothing)$

$\Leftrightarrow$ [simplify duplication]

$w \neq null \land w \neq r \land w \neq n \land$

$(r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing) \land$

$(r = w \Rightarrow r = w = null)$

$\Leftrightarrow$ [simplify (w $\neq null$)]

$w \neq null \land w \neq r \land w \neq n \land$

$(r = n \Rightarrow r = n = null) \land (r = null \Leftrightarrow readers1 = \varnothing)$

Theorem 2

$R \land \text{pre } Write \vdash \text{pre } Write1$

1	$w \neq null \land w \neq r \land w \neq n$	$MSMEI1$
2	$(r = n \Rightarrow r = n = null)$	$MSMEI1$
3	$(r = null \Leftrightarrow readers1 = \varnothing)$	$MSMEI1$

Correctness

Lemma 4

$\exists\, MSMIE' \bullet Write \land R'$

$\Leftrightarrow$ [definitions of $MSMIE'$, $Write$ and R']

$\exists\, config' : CONFIG;\ readers' : \mathbb{P}\, PID \bullet$

$(config' \in \{wii, wni\} \Leftrightarrow readers' = \varnothing) \land$

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$

$config' = next\_config(config) \land readers' = readers \land$

$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$

$config' = current\_config(r', n') \land readers' = readers1'$

$\Leftrightarrow$ [one-point-rule (config')]

$\exists\, readers' : \mathbb{P}\, PID \bullet$

$(current\_config(r', n') \in \{wii, wni\} \Leftrightarrow readers' = \varnothing) \land$

$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$
$current\_config(r', n') = next\_config(config) \land readers' = readers \land$
$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$
$readers' = readers1'$

$\Leftrightarrow$ [one-point-rule (readers')]

$(current\_config(r', n') \in \{wii, wni\} \Leftrightarrow readers1' = \varnothing) \land$
$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$
$current\_config(r', n') = next\_config(config) \land readers1' = readers \land$
$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$

$\Leftrightarrow$ [simplify (current_config definition)]

$(r' = null \Leftrightarrow readers1' = \varnothing) \land$
$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$
$current\_config(r', n') = next\_config(config) \land readers1' = readers \land$
$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null) \land (r' = null \Leftrightarrow readers1' = \varnothing) \land$

$\Leftrightarrow$ [simplify duplication]

$(r' = null \Leftrightarrow readers1' = \varnothing) \land$
$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$
$current\_config(r', n') = next\_config(config) \land readers1' = readers \land$
$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null)$

$\Leftrightarrow$ [simplify (next_config definition)]

$(r' = null \Leftrightarrow readers1' = \varnothing) \land$
$(config \in \{wii, wni\} \Leftrightarrow readers = \varnothing) \land$
$current\_config(r', n') \in \{wni, wrn\} \land readers1' = readers \land$
$w' \neq null \land w' \neq r' \land w' \neq n' \land (r' = n' \Rightarrow r' = n' = null)$

Theorem 3

$R \land \text{pre } Write \land Write1 \vdash \exists\, MSMIE' \bullet Write \land R'$

1	$config \in \{wii, wni\} \Leftrightarrow readers = \varnothing$	$lemma2(preWrite)$
2	$n' = w \land r' = r$	$write1$
3	$w \neq null$	
4	$n' \neq null$	2, 3
5	$current\_config(r', n') \in \{wni, wrn\}$	4
6	$r' = null \Leftrightarrow readers1' = \varnothing$	$MSMIE1'$
7	$r' = n' \Rightarrow r' = n' = null$	$MSMIE1'$
8	$w' \neq null \land w' \neq r' \land w' \neq n'$	$MSMIE1'$