A Partial Proof of R2 for the Bounded Buffer

THEOREM $Inv \wedge Inv' \wedge Next \Rightarrow [C!Next]_{C!vars}$

$\langle 1 \rangle 1.$ ASSUME: Inv, Inv', $Producer$
PROVE: $C!Send$

$\langle 2 \rangle 1.$ $Len(chBar) \neq N$

PROOF: $TypeOK$ and the definition of $chBar$ implies $Len(chBar) = p \ominus c$, so $\langle 2 \rangle 1$ follows from $Producer$.

$\langle 2 \rangle 2.$ $chBar' = Append(chBar, IHead(in))$

$\langle 3 \rangle 1.$ $(chBar \in Seq(Msgs)) \wedge (Len(chBar) = p \ominus q)$

PROOF: By $TypeOK$ and definition of $chBar$.

$\langle 3 \rangle 2.$ $(chBar' \in Seq(Msgs)) \wedge (Len(chBar') = (p \ominus q) + 1)$

$\langle 4 \rangle 1.$ $p' \ominus q' = (p \ominus q) + 1$

$\langle 5 \rangle 1.$ $p' \ominus q' = (p \oplus 1) \ominus q$

PROOF: By $Producer$.

$\langle 5 \rangle 2.$ $(p \oplus 1) \ominus q = (p \ominus q) \oplus 1$

PROOF: By $TypeOK$ and the arithmetic properties of $\oplus$ and $\ominus$.

$\langle 5 \rangle 3.$ $(p \ominus q) \oplus 1 = (p \ominus q) + 1$

PROOF: $p \ominus q < N$ by $Producer$, so $(p \ominus q) + 1 < 2N$ (by the assumption on N). By definition of $\oplus$, this implies $(p \ominus q) + 1 = (p \ominus q) \oplus 1)$.

$\langle 5 \rangle 4.$ Q.E.D.

PROOF: By $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, and $\langle 5 \rangle 3$.

$\langle 4 \rangle 2.$ Q.E.D.

PROOF: By Inv', the definition of $chBar$, and $\langle 4 \rangle 1$.

$\langle 3 \rangle 3.$ $\wedge\ chBar'[(p \ominus q) + 1] = IHead(in))$
$\wedge\ \forall i \in 1 \,..\, (p \ominus q) : chBar'[i] = chBar[i]$

$\langle 4 \rangle 1.$ The set $\{(c \oplus (i-1))\%N : i \in 1 \,..\, ((p \ominus c) + 1)\}$ contains $(p \ominus c) + 1$ distinct numbers.

PROOF: By $TypeOK$ and Property BB, since $Producer$ implies $p \ominus c < N$, so $(p \ominus c) + 1 \leq N$.

$\langle 4 \rangle 2.$ $(c \oplus (i-1))\%N$ equals $p\%N$ for $i = (p \ominus c) + 1$

PROOF: The arithmetical properties of $\oplus$ and $\ominus$ imply $c \oplus (p \ominus c) = p$.

$\langle 4 \rangle 3.$ Q.E.D.

PROOF: By $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, and the definition of $chBar$, since $Producer$ and $TypeOK$ imply

$$\forall j \in 0 \,..\, (N-1) : buf'[j] = \text{IF } j = p\%N \text{ THEN } IHead(in) \text{ ELSE } buf[j$$

$\langle 3 \rangle 4.$ Q.E.D.

PROOF: By $\langle 3\rangle 1$, $\langle 3\rangle 2$, and $\langle 3\rangle 3$.

$\langle 2\rangle 3.$ $(in' = ITail(in)) \land (out' = out)$

PROOF: By *Producer*.

$\langle 2\rangle 4.$ Q.E.D.

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, and the definition of *Send*.

$\langle 1\rangle 2.$ ASSUME: *Inv*, *Consumer*
PROVE: $C!Rcv$

PROOF: Left as an exercise.

$\langle 1\rangle 3.$ Q.E.D.

PROOF: By $\langle 1\rangle 1$, $\langle 1\rangle 2$, and the definitions of *Next* and $C!Next$.

CLOSE