A Partial Proof of B2a

I use the ASSUME, PROVE to avoid an extra level of proof.

$\langle 1 \rangle 1.$ ASSUME: Inv_B, $Producer_B$
PROVE: $\overline{Send_C}$

$\langle 2 \rangle 1.$ $Len(\overline{ch}) \neq N$

$\langle 2 \rangle 2.$ $\exists v \in Msg : \overline{ch}' = Append(\overline{ch}, v)$

$\langle 3 \rangle 1.$ Pick $v \in Msg$ such that $buf' = [buf \text{ EXCEPT } ![p \,\%\, N] = v]$

PROOF: Such a v exists by definition of $Producer_B$, which holds by the assumption of $\langle 1 \rangle 1$.

$\langle 3 \rangle 2.$ $\overline{ch}' = Append(\overline{ch}, v)$

$\langle 4 \rangle 1.$ $p \ominus c \in 0 \,..\, (N-1)$

PROOF: Inv_B implies $p \ominus c \in 0 \,..\, N$, and $Producer_B$ implies $p \ominus c \neq N$.

$\langle 4 \rangle 2.$ $p' \ominus c' = (p \ominus c) + 1$

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

PROOF: By definition of $Producer_B$, which is assumed in $\langle 1 \rangle 1$.

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

PROOF: By Inv_B, which implies that p and c are in $0 \,..\, (2N-1)$, and the properties of $\oplus$ and $\ominus$ as operators on $0 \,..\, (2N-1)$.

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

PROOF: By $\langle 4 \rangle 1$ and definition of $\oplus$.

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

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

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

PROOF: By $\langle 3 \rangle 1$, $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, and the definition of $\overline{ch}$.

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

PROOF: By $\langle 3 \rangle 1$ (which asserts $v \in Msg$) and $\langle 3 \rangle 2$.

$\langle 2 \rangle 3.$ Q.E.D.

PROOF: By $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, and the definition of $Send_C$.

$\langle 1 \rangle 2.$ ASSUME: Inv_B, $Consumer_B$
PROVE: $\overline{Rcv_C}$

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

PROOF: By $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, and the definitions of $Next_B$ and $Next_C$.

CLOSE