A Partial Proof of B2a

⟨1⟩1. ASSUME: Inv_B, $Producer_B$
PROVE: $\overline{Send_C}$

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

⟨2⟩1. $Len(\overline{ch}) \neq N$

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

⟨3⟩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 ⟨1⟩1.

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

⟨4⟩1. $p \ominus c \in 0 \,..\, (N - 1)$

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

⟨4⟩2. $p' \ominus c' = (p \ominus c) + 1$

⟨5⟩1. $p' \ominus c' = (p \oplus 1) \ominus c$

PROOF: By definition of $Producer_B$, which is assumed in ⟨1⟩1.

⟨5⟩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 $0 \,..\, (2N - 1)$.

⟨5⟩3. $(p \ominus c) \oplus 1 = (p \ominus c) + 1$

PROOF: By ⟨4⟩1 and definition of $\oplus$.

⟨5⟩4. Q.E.D.

PROOF: By ⟨5⟩1, ⟨5⟩2, and ⟨5⟩3.

⟨4⟩3. Q.E.D.

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

⟨3⟩3. Q.E.D.

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

⟨2⟩3. Q.E.D.

PROOF: By ⟨2⟩1, ⟨2⟩2, and the definition of $Send_C$.

⟨1⟩2. ASSUME: Inv_B, $Consumer_B$
PROVE: $\overline{Rcv_C}$

⟨1⟩3. Q.E.D.

PROOF: By ⟨1⟩1, ⟨1⟩2, and the definitions of $Next_B$ and $Next_C$.

CLOSE