INF4140 Models of Concurrency
lecture 7 - page 18-19

Detailed Proof for the Producer / Consumer Example

1 Producer

Proof obligation: $\{I_P \wedge p < n \wedge p == c\} \Rightarrow \{I_P\}_{p \leftarrow p+1, buf \leftarrow a[p]}$

- Proof step1
  $\{c \leq p \leq c+1 \wedge (p == c+1 \Rightarrow buf == a[p-1]) \wedge p \leq n \wedge p < n \wedge p == c\}$
  $\Rightarrow$
  $\{c \leq p+1 \leq c+1 \wedge (p+1 == c+1 \Rightarrow a[p] == a[p+1-1]) \wedge p+1 \leq n\}$
- Proof step2 (simply step1)
  $\{c \leq p \leq c+1 \wedge (p == c+1 \Rightarrow buf == a[p-1]) \wedge p < n \wedge p == c\}$
  $\Rightarrow$
  $\{c \leq p+1 \leq c+1 \wedge (p == c \Rightarrow a[p] == a[p]) \wedge p+1 \leq n\}$

  Now we can prove this implication by showing:

  1. $p == c \Rightarrow c \leq p+1 \leq c+1$
  2. $p == c \Rightarrow (p == c \Rightarrow a[p] == a[p])$
  3. $p < n \Rightarrow p+1 \leq n$

2 Consumer

Proof obligation: $\{I_C \wedge c < n \wedge p > c\} \Rightarrow \{I_C\}_{c \leftarrow c+1, b[c] \leftarrow buf}$

- Proof step1
  $\{c \leq p \leq c+1 \wedge (p == c+1 \Rightarrow buf == a[p-1]) \wedge c \leq n \wedge (b[o:c-1] == a[o:c-1]) \wedge c < n \wedge p > c\}$
  $\Rightarrow$
  $\{c+1 \leq p \leq c+1+1 \wedge (p == c+1+1 \Rightarrow buf == a[p-1]) \wedge c+1 \leq n \wedge (b[o:c+1-1] == a[o:c+1-1])\}_{b[c] \leftarrow buf}$
- Proof step2 (simply step1)
  $\{c \leq p \leq c+1 \wedge (p == c+1 \Rightarrow buf == a[p-1]) \wedge (b[o:c-1] == a[o:c-1]) \wedge c < n \wedge p > c\}$
  $\Rightarrow$
  $\{c+1 \leq p \leq c+2 \wedge (p == c+2 \Rightarrow buf == a[p-1]) \wedge c+1 \leq n \wedge (b[o:c] == a[o:c])\}_{b[c] \leftarrow buf}$
- Proof step3 (apply the substitution of $b[c]$ with buf)
  $\{c \leq p \leq c+1 \wedge (p == c+1 \Rightarrow buf == a[p-1]) \wedge (b[o:c-1] == a[o:c-1]) \wedge c < n \wedge p > c\}$
  $\Rightarrow$
  $\{c+1 \leq p \leq c+2 \wedge (p == c+2 \Rightarrow buf == a[p-1]) \wedge c+1 \leq n \wedge (b[o:c-1] : buf == a[o:c])\}$

Since $(c \leq p \leq c+1 \wedge p > c) \Rightarrow (p == c+1)$ is known from the assumption, we can prove:

1. $p == c+1 \Rightarrow c+1 \leq p \leq c+2$.
2. $p == c+1 \Rightarrow (p == c+2 \Rightarrow buf == a[p-1])$.
   Because $(false \Rightarrow true) == true$ and $(false \Rightarrow false) == true$.
3. Since $p == c+1$, we know from the assumption that $buf == a[p-1] == a[c]$.
   $(b[o : c-1] : buf == a[o : c])$ is then proved by showing:
   $(b[o : c-1] == a[o : c-1]) \wedge buf == a[c]) \Rightarrow (b[o : c-1] : buf == a[o : c])$
4. $c < n \Rightarrow c+1 \leq n$.