Third Procedure: `transfer()`

Denote the length, head and tail pointers of the two buffers with `NB1`,`h1`,`t1`,`NB2`,`h1`,`t2`, respectively. The variables in `push()` and `pop()` also need replacing accordingly.

```
push():
  wait until t1 - h1 < NB1
  B1[t1 mod NB1] := I[x]
  x := x + 1
  t1 := t1 + 1

transfer():
  wait until h1 < t1 and t2 - h2 < NB2
  B2[t2 mod NB2] := B1[h1 mod NB1]
  h1 := h1 + 1
  t2 := t2 + 1

pop():
  wait until h2 < t2
  O[y]:= B2[h2 mod NB2]
  h2 := h2 + 1
  y := y + 1
```

Interpretations

To write an invariant of the form:

$$S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K,$$

the following interpretations are needed:

$$\begin{aligned} S_I &= I[x, N) & S_{IB_1} &= B_1[t_1 \text{ upto } x) \\ S_{B_1} &= B_1[h_1 \text{ upto } t_1) & S_{B_1B_2} &= B_2[t_2 \text{ upto } h_1) \\ S_{B_2} &= B_2[h_2 \text{ upto } t_2) & S_{B_2O} &= O[y \text{ upto } h_2) \\ S_O &= O[0, y] \end{aligned}$$

Invariant

The updated invariant is

$$S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K$$

with side conditions

$$h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}.$$

Local Correctness

For `push()`, a local invariant $S : x \le N$ is added, $t_1 = x \wedge x < N$ are preconditions, and $t_1 = x$ is a postcondition:

$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge x < N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, t_1 = x$
wait until $t_1 - h_1 < N_{B_1}$
$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + B_1[h_1 \text{ upto } t_1) + [\,] + (I[x] + I[x+1, N)) = K \wedge x < N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 < N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, t_1 = x$
$\mathbf{B_1}[t_1 \bmod N_{B_1}] := I[x]$
$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + B_1[h_1 \text{ upto } t_1) + [\,] + (B_1[t_1 \bmod N_{B_1}] + I[x+1, N)) = K \wedge$
$\quad x < N \wedge h_1 \le t_1 \wedge t_1 - h_1 < N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, t_1 = x$
$\mathbf{x} := x + 1$
$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + B_1[h_1 \text{ upto } t_1) + B_1[t_1 \bmod N_{B_1}] + I[x, N) = K \wedge x \le N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 < N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, t_1 + 1 = x$
$\mathbf{t_1} := t_1 + 1$
$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + B_1[h_1 \text{ upto } t_1) + [\,] + I[x, N) = K \wedge x \le N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, t_1 = x$

For `pop()`, a local invariant $R : y \le N$ is added, $y = h_2 \wedge y < N$ are preconditions, and $y = h_2$ is a postcondition:

$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge y < N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, y = h_2$
wait until $h_2 < t_2$
$\triangleright\, O[0, y) + [\,] + (B_2[h_2 \bmod N_{B_2}] + B_2[h_2 + 1 \text{ upto } t_2)) + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge$
$\quad y < N \wedge h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 < t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, y = h_2$
$\mathbf{O}[y] := B_2[h_2 \bmod N_{B_2}]$
$\triangleright\, O[0, y) + [\,] + (O[y] + B_2[h_2 + 1 \text{ upto } t_2)) + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge y < N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 < t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, y = h_2$
$\mathbf{h_2} := h_2 + 1$
$\triangleright\, O[0, y) + O[y] + B_2[h_2 \text{ upto } t_2) + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge y < N \wedge$
$\quad h_1 \le t_1 \wedge t_1 - h_1 \le N_{B_1} \wedge h_2 \le t_2 \wedge t_2 - h_2 \le N_{B_2}$
$\triangleright\, y + 1 = h_2$

$\mathbf{y} := y + 1$
$\triangleright\, O[0, y) + [\,] + B_2[h_2 \text{ upto } t_2) + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge y \leq N \wedge$
$h_1 \leq t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 \leq N_{B_2}$
$\triangleright\, y = h_2$

Finally, for `transfer()`, $t_2 = h_1$ is both a precondition and a postcondition:

$\triangleright\, S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K \wedge$
$h_1 \leq t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 \leq N_{B_2}$
$\triangleright\, t_2 = h_1$
wait until $h_1 < t_1$ **and** $t_2 - h_2 < N_{B_2}$
$\triangleright\, S_O + S_{B_2O} + B_2[h_2 \text{ upto } t_2) + [\,] + (B_1[h_1 \bmod N_{B_1}] + B_1[h_1 + 1 \text{ upto } t_1)) + S_{IB_1} + S_I = K \wedge$
$h_1 < t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 < N_{B_2}$
$\triangleright\, t_2 = h_1$
$\mathbf{B_2}[t_2 \bmod N_{B_2}] := B_1[h_1 \bmod N_{B_1}]$
$\triangleright\, S_O + S_{B_2O} + B_2[h_2 \text{ upto } t_2) + [\,] + (B_2[t_2 \bmod N_{B_2}] + B_1[h_1 + 1 \text{ upto } t_1)) + S_{IB_1} + S_I = K \wedge$
$h_1 < t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 < N_{B_2}$
$\triangleright\, t_2 = h_1$
$\mathbf{h_1} := h_1 + 1$
$\triangleright\, S_O + S_{B_2O} + B_2[h_2 \text{ upto } t_2) + B_2[t_2 \bmod N_{B_2}] + B_1[h_1 \text{ upto } t_1) + S_{IB_1} + S_I = K \wedge$
$h_1 \leq t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 < N_{B_2}$
$\triangleright\, t_2 + 1 = h_1$
$\mathbf{t_2} := t_2 + 1$
$\triangleright\, S_O + S_{B_2O} + B_2[h_2 \text{ upto } t_2) + [\,] + B_1[h_1 \text{ upto } t_1) + S_{IB_1} + S_I = K \wedge$
$h_1 \leq t_1 \wedge t_1 - h_1 \leq N_{B_1} \wedge h_2 \leq t_2 \wedge t_2 - h_2 \leq N_{B_2}$
$\triangleright\, t_2 = h_1$

For all three functions, the statements at every point are at least as strong as the invariant, so the local correctness is maintained.

Noninterference Proof

The noninterference proof is still easy. All assertions are a conjunction of predicates of 5 forms:

- $S_O + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K$, which is included in the invariant, and proved to hold everywhere as long as other conjuncts hold.
- $x < N, x \leq N, y < N, y \leq N$, which only involve local variables x, y and the constant N, so interference is impossible.
- $t_1 = x, t_1 + 1 = x, y = h_2, y + 1 = h_2, t_2 = h_1, t_2 + 1 = h_1$, which involve shared variables t_1, h_2, t_2, h_1, but they are only ever updated by the concerned process itself: only **S** touches t_1, only **R** touches h_2, and only **T** (the process calling `transfer()`) touches t_2 and h_1.

- $h_1 \leq t_1, t_1 - h_1 \leq N_{B_1}, h_2 \leq t_2, t_2 - h_2 \leq N_{B_2}$, which are also parts of the invariant, so already covered.

This leaves only $t_1 - h_1 < N_{B_1}$, $h_2 < t_2$, $h_1 < t_1$ and $t_2 - h_2 < N_{B_2}$ as predicates that might suffer interference:

1. $t_1 - h_1 < N_{B_1}$ only appears in **S**, and the only statement outside **S** that might invalidate it is $h_1 := h_1 + 1$ in **T**, with the following annotation:

   $\triangleright\, t_1 - h_1 < N_{B_1}$
   $\mathbf{h_1} := h_1 + 1$
   $\triangleright\, t_1 - h_1 < N_{B_1}$

   T only makes S_{B_1} shorter, so if it was not full, it still is not.

2. $h_2 < t_2$ only appears in **R**, and the only statement outside **R** that might invalidate it is $t_2 := t_2 + 1$ in **T**, with the following annotation:

   $\triangleright\, h_2 < t_2$
   $\mathbf{t_2} := t_2 + 1$
   $\triangleright\, h_2 < t_2$

   T only makes S_{B_2} longer, so if it was not empty, it still is not.

3. $h_1 < t_1$ only appears in **T**, and the only statement outside **T** that might invalidate it is $t_1 := t_1 + 1$ in **S**, with the following annotation:

   $\triangleright\, h_1 < t_1$
   $\mathbf{t_1} := t_1 + 1$
   $\triangleright\, h_1 < t_1$

   S only makes S_{B_1} longer, so if it was not empty, it still is not.

4. $t_2 - h_2 < N_{B_2}$ only appears in **T**, and the only statement outside **T** that might invalidate it is $h_2 := h_2 + 1$ in **R**, with the following annotation:

   $\triangleright\, t_2 - h_2 < N_{B_2}$
   $\mathbf{h_2} := h_2 + 1$
   $\triangleright\, t_2 - h_2 < N_{B_2}$

   R only makes S_{B_2} shorter, so if it was not full, it still is not.

Partial Correctness

From initialization $x, y, h_1, t_1, h_2, t_2 := 0, 0, 0, 0, 0, 0$ and the extended invariant, we know that $[\,] + [\,] + [\,] + [\,] + [\,] + [\,] + I[0, N) = K$, so $K = I[0, N)$.

The extended invariant plus the termination condition $(y = N)$ for **R** implies that

$$O[0, N) + S_{B_2O} + S_{B_2} + S_{B_1B_2} + S_{B_1} + S_{IB_1} + S_I = K = I[0, N),$$

which implies

$$N + |S_{B_2O}| + |S_{B_2}| + |S_{B_1B_2}| + |S_{B_1}| + |S_{IB_1}| + |S_I| = |I[0, N)| = N,$$

therefore

$$|S_{B_2O}| = |S_{B_2}| = |S_{B_1B_2}| = |S_{B_1}| = |S_{IB_1}| = |S_I| = 0,$$

thus

$$O[0, N) = I[0, N).$$