MODULE *naive*

EXTENDS *Integers*
CONSTANT $N$, $STOP$, $EPSILON$
ASSUME $N \in Nat \setminus \{0, 1\}$
$Procs \triangleq 1 \,..\, N$
$SetMax(S) \triangleq$ CHOOSE $i \in S : \forall\, j \in S : i \geq j$

Hybrid Logical Clocks naive algorithm

```
--algorithm naive{
   variable pt = [j ∈ Procs ↦ 0], lc = [j ∈ Procs ↦ 0], mailbox = [j ∈ Procs ↦ 0] ;
   fair process ( j ∈ Procs ) {
      J0: while ( pt[self] < STOP ) {
            either   local or receive event
            J1: {    phy clocks cannot diverge more than EPSILON
                 await (∀ k ∈ Procs : pt[self] < pt[k] + EPSILON) ;
                 pt[self] := pt[self] + 1 ;
                 lc[self] := SetMax({lc[self] + 1, mailbox[self] + 1, pt[self]}) ;
             }
            or   send event
            J2: {    phy clocks cannot diverge more than EPSILON
                 await (∀ k ∈ Procs : pt[self] < pt[k] + EPSILON) ;
                 pt[self] := pt[self] + 1 ;
                 lc[self] := lc[self] + 1 ;
                 mailbox[(self%N) + 1] := lc[self] ;
             }
          }
    }
}
```

BEGIN TRANSLATION

VARIABLES $pt$, $lc$, $mailbox$, $pc$

$vars \triangleq \langle pt, lc, mailbox, pc\rangle$

$ProcSet \triangleq (Procs)$

$Init \triangleq$ Global variables
$\land\, pt = [j \in Procs \mapsto 0]$
$\land\, lc = [j \in Procs \mapsto 0]$
$\land\, mailbox = [j \in Procs \mapsto 0]$
$\land\, pc = [self \in ProcSet \mapsto$ "J0"$]$

$J0(self) \triangleq \land\, pc[self] =$ "J0"
$\land$ IF $pt[self] < STOP$
THEN $\land \lor \land\, pc' = [pc$ EXCEPT $![self] =$ "J1"$]$
$\lor \land\, pc' = [pc$ EXCEPT $![self] =$ "J2"$]$
ELSE $\land\, pc' = [pc$ EXCEPT $![self] =$ "Done"$]$
$\land$ UNCHANGED $\langle pt, lc, mailbox\rangle$

$$
\begin{aligned}
J1(self) \triangleq\ & \land\ pc[self] = \text{“J1”} \\
& \land\ (\forall\, k \in Procs : pt[self] < pt[k] + EPSILON) \\
& \land\ pt' = [pt \text{ EXCEPT } ![self] = pt[self] + 1] \\
& \land\ lc' = [lc \text{ EXCEPT } ![self] = SetMax(\{lc[self] + 1,\ mailbox[self] + 1,\ pt'[self]\})] \\
& \land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“J0”}] \\
& \land \text{UNCHANGED } mailbox
\end{aligned}
$$

$$
\begin{aligned}
J2(self) \triangleq\ & \land\ pc[self] = \text{“J2”} \\
& \land\ (\forall\, k \in Procs : pt[self] < pt[k] + EPSILON) \\
& \land\ pt' = [pt \text{ EXCEPT } ![self] = pt[self] + 1] \\
& \land\ lc' = [lc \text{ EXCEPT } ![self] = lc[self] + 1] \\
& \land\ mailbox' = [mailbox \text{ EXCEPT } ![(self\%N) + 1] = lc'[self]] \\
& \land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“J0”}]
\end{aligned}
$$

$$j(self) \triangleq J0(self) \lor J1(self) \lor J2(self)$$

$$
\begin{aligned}
Next \triangleq\ & (\exists\, self \in Procs : j(self)) \\
& \lor \text{ Disjunct to prevent deadlock on termination} \\
& \quad ((\forall\, self \in ProcSet : pc[self] = \text{“Done”}) \land \text{UNCHANGED } vars)
\end{aligned}
$$

$$
\begin{aligned}
Spec \triangleq\ & \land\ Init \land \Box[Next]_{vars} \\
& \land\ \forall\, self \in Procs : \mathrm{WF}_{vars}(j(self))
\end{aligned}
$$

$$Termination \triangleq \Diamond(\forall\, self \in ProcSet : pc[self] = \text{“Done”})$$

END TRANSLATION

$$TypeOK \triangleq (\forall\, k \in Procs : lc[k] \geq pt[k])$$
$$Sync \triangleq (\forall\, k,\ l \in Procs : pt[k] \leq pt[l] + EPSILON)$$
$$Bounded \triangleq (\forall\, k \in Procs : lc[k] < pt[k] + N * (EPSILON + 1))$$

\ * Modification History
\ * Last modified *Thu Oct* 30 21:00:51 *EDT* 2014 by *Siddharth*
\ * Created *Thu Oct* 30 08:26:40 *EDT* 2014 by *Siddharth*

For the model with:
$EPSILON = 3$
$N = 3$
$STOP = 20$

We see that the property, $Bounded \triangleq (\forall\, k \in Procs: lc[k] < pt[k] + N * (EPSILON + 1))$ Get's violated on running the model check.

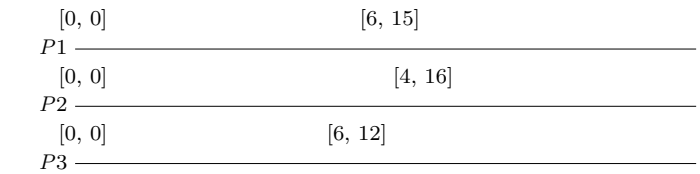
An instance of the counter example obtained by TLA+ model checker is given below:

Starting with Initial predicate: Since there exist three process, the physical times are $< 0,0,0 >$ for Process 1, Process 2 and Process 3 respectively. Similarly, the Logical times are $< 0,0,0 >$.

We see that for the bound gets violated after 33 states for the given instance:
$PT = < 6,4,6 >$

$LC = <15,16,12>$

We see that for Process 2, $LC = 16$ is not less than the bound, 16 $((PT + N * (EPSILON + 1) = (4 + 3 * (3 + 1)))$
$\{LC < PT + N * (EPSILON + 1) results\ to$ FALSE$\}$




*Hence the bound gets violated in the naive algorithm implementation of Hybrid Logical Clocks.*

*This proves that' $l - pt'$ diverges as we continue the message loop.*

---

*Project submitted by Siddharth Krishna Sinha(ssinha4@buffalo.edu)*

---