Facultad de Ciencias Exactas, Ingeniería y Agrimensura
UNIVERSIDAD NACIONAL DE ROSARIO

Ingeniería de Software

Trabajo Práctico Verificación de Software

Cipullo, Inés

2025

1 Requerimientos

Se describen los requerimientos de un planificador de procesos a corto plazo, encargado de planificar los procesos que están listos para ejecución, también llamado *dispatcher*. Este planificador implementará el algoritmo de planificaión "Ronda" (*Round Robin* en inglés), y este sistema tendrá un único procesador.

Un proceso puede estar en alguno de los siguientes estados: *nuevo*, *listo*, *ejecutando*, *bloqueado*, *terminado*. El dispatcher decide entre los procesos que están listos para ejecutarse y determina a cuál de ellos *activar*, y detiene a aquellos que *exceden su tiempo* de procesador, es decir, se encarga de las transiciones entre los estados **listo** y **ejecutando**.

Siguiendo Round Robin, los procesos listos se almacenan en forma de cola, cada proceso listo se ejecuta por un sólo *quantum* y si un proceso no ha terminado de ejecutarse al final de su período, será interrumpido y puesto al final de la cola de procesos listos. Se deben tener en cuenta, también, aquellas transiciones que involucran otros estados de procesos pero inciden sobre alguno de los dos estados que se controlan desde el dispatcher. Los procesos que sean agregados a la cola de listos por estas otras transiciones, se ubicarán al final de la misma.

2 Especificación

Para empezar, se dan las siguientes designaciones.

p es un proceso $\approx p \in PROCESS$

t es un contador de ticks del sistema $\approx t \in TICK$

proceso nulo $\approx$ *nullp*

cantidad de tiempo durante el cual un proceso tiene permiso para ejecutarse en el procesador antes de ser interrumpido $\approx$ *quantum*

procesos en estado listo (para ser ejecutados) $\approx$ *procQueue*

proceso en ejecución $\approx$ *current*

contador de ticks restantes de ejecución que le corresponden a *current* $\approx$ *remTicks*

Luego, se introducen los tipos que se utilizan en la especificación.

$[PROCESS]$

$TICK == \mathbb{N}$

Además, se presentan las siguientes definiciones axiomáticas, donde se define la existencia del proceso *nullp*, que representa el proceso nulo, y la constante *quantum*, que equivale a 5 ticks.

$$nullp : PROCESS$$

$$quantum : TICK$$
$$quantum = 5$$

Se define entonces el espacio de estados del planificador y su estado inicial.

Dispatcher

$$procQueue : \mathbb{N} \rightarrowtail PROCESS$$
$$current : PROCESS$$
$$remTicks : TICK$$

InitDispatcher

Dispatcher

$procQueue = \emptyset$

$current = nullp$

$remTicks = 0$

Como un proceso no puede estar *en ejecución* y *listo* al mismo tiempo, se plantea el siguiente invarinate de estado:

InvDispatcher

Dispatcher

$current \notin \operatorname{ran} procQueue$

$nullp \notin \operatorname{ran} procQueue$

Procedemos con la especificación de las operaciones requeridas. Estas son:

- *NewProcess*: para pasar un proceso de estado *nuevo* (o *bloqueado*) a *listo*.
- *Dispatch*: modela el funcionamiento del planificador, se encarga de las transiciones entre los estados *listo* y *en ejecución*.
- *TerminateProcess*: para pasar un proceso de estado *en ejecución* a *terminado*.

NewProcessOk

$\Delta Dispatcher$

$p? : PROCESS$

$procQueue \neq \emptyset$

$p? \notin \operatorname{ran} procQueue$

$p? \neq current$

$p? \neq nullp$

$procQueue' = procQueue \cup \{max\,(\operatorname{dom} procQueue) + 1 \mapsto p?\}$

$current' = current$

$remTicks' = remTicks$

newProcessOkEmptyQueue

$\Delta Dispatcher$

$p? : PROCESS$

$procQueue = \emptyset$

$p? \notin \operatorname{ran} procQueue$

$p? \neq current$

$p? \neq nullp$

$procQueue' = \{1 \mapsto p?\}$

$current' = current$

$remTicks' = remTicks$

NewProcessError

$\Xi Dispatcher$

$p? : PROCESS$

$p? \in \operatorname{ran} procQueue \lor p? = current \lor p? = nullp$

$NewProcess == NewProcessOk \lor newProcessOkEmptyQueue \lor NewProcessError$

Tick

$\Delta Dispatcher$

$remTicks > 0$

$current \neq nullp$

$procQueue' = procQueue$

$current' = current$

$remTicks' = remTicks - 1$

Timeout

$\Delta Dispatcher$

$procQueue \neq \emptyset$

$remTicks = 0$

$current \neq nullp$

$procQueue' = procQueue \cup \{max\,(\mathrm{dom}\, procQueue) + 1 \mapsto current\}$

$current' = nullp$

$remTicks' = remTicks$

TimeoutEmptyQueue

$\Delta Dispatcher$

$procQueue = \emptyset$

$remTicks = 0$

$current \neq nullp$

$procQueue' = \{1 \mapsto current\}$

$current' = nullp$

$remTicks' = remTicks$

DispatchProcess

$\Delta Dispatcher$

$current = nullp$

$procQueue \neq \emptyset$

$procQueue' = procQueue \setminus \{min\,(\mathrm{dom}\, procQueue) \mapsto procQueue(min\,(\mathrm{dom}\, procQueue))\}$

$current' = procQueue(min\,(\mathrm{dom}\, procQueue))$

$remTicks' = remTicks$

Idle

$\Xi Dispatcher$

$current = nullp$

$procQueue = \emptyset$

$Dispatch == Tick \lor Timeout \lor TimeoutEmptyQueue \lor DispatchProcess \lor Idle$

TerminateProcessOk

$\Delta Dispatcher$

$p? : PROCESS$

$current = p?$

$procQueue' = procQueue$

$current' = nullp$

$remTicks' = remTicks$

TerminateProcessError

$\Xi Dispatcher$

$p? : PROCESS$

$current \neq p?$

$TerminateProcess == TerminateProcessOk \lor TerminateProcessError$

3 Simulaciones en *{log}*

Se traduce la especificación a *{log}* (en **planificador.slog**), la cual pasa el **type_check**. A continuación, se presentan dos simulaciones ejecutadas sobre *{log}* y la primera solución de cada una.

1ra simulación

```
dec([PQ0, PQ1, PQ2, PQ3, PQ4, PQ5, PQ6, PQ7, PQ8, PQ9], t_proc_queue) &
dec([C0, C1, C2, C3, C4, C5, C6, C7, C8, C9], process)                &
dec([RT0, RT1, RT2, RT3, RT4, RT5, RT6, RT7, RT8, RT9], t_tick)       &
initDispatcher(PQ0, C0, RT0)                                          &
newProcess(PQ0, C0, RT0, process:p1, PQ1, C1, RT1)                    &
newProcess(PQ1, C1, RT1, process:p2, PQ2, C2, RT2)                    &
dispatch(PQ2, C2, RT2, PQ3, C3, RT3)                                  &
dispatch(PQ3, C3, RT3, PQ4, C4, RT4)                                  &
dispatch(PQ4, C4, RT4, PQ5, C5, RT5)                                  &
dispatch(PQ5, C5, RT5, PQ6, C6, RT6)                                  &
dispatch(PQ6, C6, RT6, PQ7, C7, RT7)                                  &
dispatch(PQ7, C7, RT7, PQ8, C8, RT8)                                  &
dispatch(PQ8, C8, RT8, PQ9, C9, RT9).
```

La idea de esta simulación es encolar dos nuevos procesos, **p1** y **p2**, en la cola de procesos listos, luego iniciar la ejecución del primero hasta que termine el tiempo de ejecución asignado (1 **quantum**) y sea interrumpido por el dispatcher. El resultado es el esperado:

```
PQ0 = {},
PQ1 = {[1,process:p1]},
PQ2 = {[1,process:p1],[2,process:p2]},
PQ3 = {[2,process:p2]/_N1},
```

```
PQ4 = {[2,process:p2]/_N1},
PQ5 = {[2,process:p2]/_N1},
PQ6 = {[2,process:p2]/_N1},
PQ7 = {[2,process:p2]/_N1},
PQ8 = {[2,process:p2]/_N1},
PQ9 = {[3,process:p1],[2,process:p2]/_N1},
C0 = process:nullp,
C1 = process:nullp,
C2 = process:nullp,
C3 = process:p1,
C4 = process:p1,
C5 = process:p1,
C6 = process:p1,
C7 = process:p1,
C8 = process:p1,
C9 = process:nullp,
RT0 = 0,
RT1 = 0,
RT2 = 0,
RT3 = 5,
RT4 = 4,
RT5 = 3,
RT6 = 2,
RT7 = 1,
RT8 = 0,
RT9 = 0
Constraint: subset(_N1,{[1,process:p1],[2,process:p2]}),
[1,process:p1]nin _N1, set(_N1), dom(_N1,_N2), set(_N2),
foreach(_X in _N2,2>=_X), rel(_N1)
```

2da simulación

```
dec([PQ0, PQ1, PQ2, PQ3, PQ4, PQ5, PQ6], t_proc_queue) &
dec([C0, C1, C2, C3, C4, C5, C6], process)             &
dec([RT0, RT1, RT2, RT3, RT4, RT5, RT6], t_tick)       &
initDispatcher(PQ0, C0, RT0)                           &
newProcess(PQ0, C0, RT0, process:p1, PQ1, C1, RT1)     &
newProcess(PQ1, C1, RT1, process:p2, PQ2, C2, RT2)     &
dispatch(PQ2, C2, RT2, PQ3, C3, RT3)                   &
dispatch(PQ3, C3, RT3, PQ4, C4, RT4)                   &
terminateProc(PQ4, C4, RT4, process:p1, PQ5, C5, RT5)  &
dispatch(PQ5, C5, RT5, PQ6, C6, RT6).
```

La idea de esta simulación es encolar dos nuevos procesos, **p1** y **p2**, en la cola de procesos listos, luego iniciar la ejecución del primero, que ejecute por un tick y que termine su ejecución. Despues se inicia la ejecución del segundo. El resultado es el esperado:

```
PQ0 = {},
PQ1 = {[1,process:p1]},
PQ2 = {[1,process:p1],[2,process:p2]},
PQ3 = {[2,process:p2]/_N1},
PQ4 = {[2,process:p2]/_N1},
PQ5 = {[2,process:p2]/_N1},
C0 = process:nullp,
C1 = process:nullp,
C2 = process:nullp,
C3 = process:p1,
C4 = process:p1,
C5 = process:nullp,
C6 = process:p2,
```

```
RT0 = 0,
RT1 = 0,
RT2 = 0,
RT3 = 5,
RT4 = 4,
RT5 = 0,
RT6 = 5
Constraint: subset(_N1,{[1,process:p1],[2,process:p2]}),
[1,process:p1]nin _N1, set(_N1), dom(_N1,_N2), set(_N2),
foreach(_X in _N2,2=<_X), pfun(_N1), comppf({[2,2]},_N1,{}),
subset(PQ6,{[2,process:p2]/_N1}), subset(_N1,{[2,process:p2]/PQ6}),
[2,process:p2]nin PQ6, rel(_N1), set(PQ6)
```

4 Generado de Condiciones de Verificación

Se utiliza el VCG para generar condiciones de verificación sobre la especificación en *{log}*, lo cual genera el archivo **planificador-vc.slog**. Luego el comando `check_vcs_planificador` realiza todas las descargas de prueba automaticamente.

Sobre la interacción con el VCG

En una primera iteración del comando `check_vcs_planificador`, hubo algunas condiciones de verificación que no fueron descargadas exitosamente. Por lo que fue necesario agregar las siguientes hipótesis en las condiciones de verificación que lo requerían:

- hipótesis `invDispatcher(ProcQueue, Current)` en `dispatch_pi_invIny`
- hipótesis `invIny(ProcQueue)` en `dispatch_pi_invDispatcher`

En ambos casos plantee la negación del enunciado y analicé el contraejemplo que presentaba para saber qué hipótesis era necesario agregar. No fue necesario utilizar el comando `findh`.

También fue necesario aumentar el timeout para que se logren descargar algunas pruebas, esto lo hice modificando el argumento de `def_to`.

5 Demostración en *Z/EVES*

Utilizando el asistente de pruebas *Z/EVES*, vamos a demostrar que la operación `TerminateProcess` preserva el invariante de estado `InvDispatcher`.

theorem TerminateProcessInvDispatcher

$$InvDispatcher \land TerminateProcess \Rightarrow InvDispatcher'$$

proof[*TerminateProcessInvDispatcher*]

invoke TerminateProcess;

split TerminateProcessOk;

simplify;

cases;

invoke TerminateProcessOk;

invoke InvDispatcher;

equality substitute procQueue';

simplify;

next;

invoke TerminateProcessError;

invoke InvDispatcher;

invoke Ξ *Dispatcher*;

rewrite;

next;

■

6 Casos de Prueba con FASTEST

Se generan casos de prubea utilizando la herramienta FASTEST para la operación `NewProcess`.

Comandos utilizados

```
loadspec ../fastest.tex
selop NewProcess
genalltt
addtactic NewProcess_DNF_1 SP \notin p? \notin \ran procQueue
addtactic NewProcess_DNF_3 SP \in p? \in \ran procQueue
genalltt
genalltca
```

Con estos comandos se carga la especificación, se selecciona la operación para la cual generar los casos de prueba y se aplican las tacticas de testing. En primer lugar, se aplica *Disjunctive Normal Form (DNF)*, que lleva la operación a su forma normal disyuntiva, ya que es la táctica por defecto que aplica FASTEST al ejecutar el comando `genalltt`. Esto particiona la operación de acuerdo a las precondiciones de las suboperaciones que la definen, donde *NewProcess_DNF_1* corresponde a *newProcessOk*, *NewProcess_DNF_2* corresponde a *newProcessOkEmptyQueue* y las tres restantes corresponden a las tres alternativas de *newProcessError*. Luego, se aplican las tacticas de partición estándar (*Standard Partition (SP)*) de $\notin$ y $\in$, donde resulta útil. Se obtiene el siguiente árbol:

- *NewProcess_VIS*
  - *NewProcess_DNF_1*
    - *NewProcess_SP_1*
    - *NewProcess_SP_2*
  - *NewProcess_DNF_2*
  - *NewProcess_DNF_3*
    - *NewProcess_SP_3*
    - *NewProcess_SP_4*
  - *NewProcess_DNF_4*
  - *NewProcess_DNF_5*

Finalmente se generan los casos de prueba, obteniendo el siguiente árbol de clases de prueba:

- *NewProcess_VIS*
  - *NewProcess_DNF_1*
    - *NewProcess_SP_2*
      - *NewProcess_SP_2_TCASE*
  - *NewProcess_DNF_2*
    - *NewProcess_DNF_2_TCASE*
  - *NewProcess_DNF_3*
    - *NewProcess_SP_3*
      - *NewProcess_SP_3_TCASE*
    - *NewProcess_SP_4*
      - *NewProcess_SP_4_TCASE*
  - *NewProcess_DNF_4*
    - *NewProcess_DNF_4_TCASE*
  - *NewProcess_DNF_5*
    - *NewProcess_DNF_5_TCASE*

Notamos que no se generó un caso de prueba para la hoja `NewProcess_SP_1`. Esto es porque es una clase de prueba vacía, ya que contiene tanto $procQueue \neq \{\}$ y $procQueue = \{\}$ como precondiciones.

Esquemas Z

Por último, se muestran los esquemas de los casos de prueba abstractos generados por FASTEST.

NewProcess_VIS

$$
\begin{array}{l}
procQueue : \mathbb{N} \rightarrowtail PROCESS \\
current : PROCESS \\
remTicks : TICK \\
p? : PROCESS \\
\hline
(procQueue \neq \{\} \\
p? \notin \operatorname{ran} procQueue \\
p? \neq current \\
p? \neq nullp) \lor (procQueue = \{\} \\
p? \notin \operatorname{ran} procQueue \\
p? \neq current \\
p? \neq nullp) \lor p? \in \operatorname{ran} procQueue \lor p? = current \lor p? = nullp
\end{array}
$$

NewProcess_DNF_1

$$
\begin{array}{l}
NewProcess\_VIS \\
\hline
procQueue \neq \{\} \\
p? \notin \operatorname{ran} procQueue \\
p? \neq current \\
p? \neq nullp
\end{array}
$$

NewProcess_DNF_2

$$
\begin{array}{l}
NewProcess\_VIS \\
\hline
procQueue = \{\} \\
p? \notin \operatorname{ran} procQueue \\
p? \neq current \\
p? \neq nullp
\end{array}
$$

NewProcess_SP_1

$$
\begin{array}{l}
NewProcess\_DNF\_1 \\
\hline
\operatorname{ran} procQueue = \{\}
\end{array}
$$

NewProcess_DNF_3

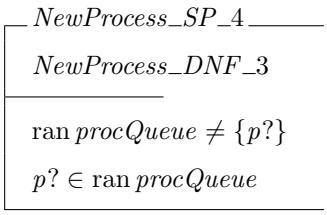
$$
\begin{array}{l}
NewProcess\_VIS \\
\hline
p? \in \operatorname{ran} procQueue
\end{array}
$$

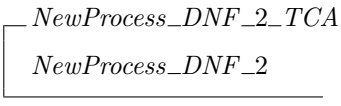
NewProcess_SP_2

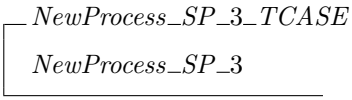
$$
\begin{array}{l}
NewProcess\_DNF\_1 \\
\hline
\operatorname{ran} procQueue \neq \{\}
\end{array}
$$

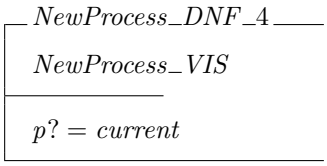
NewProcess_SP_3

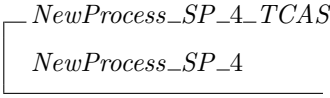
$$
\begin{array}{l}
NewProcess\_DNF\_3 \\
\hline
\operatorname{ran} procQueue = \{p?\}
\end{array}
$$

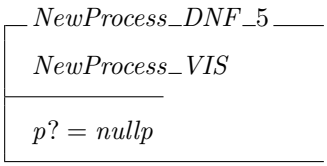

NewProcess_SP_4
NewProcess_DNF_3
ran procQueue ≠ {p?}
p? ∈ ran procQueue

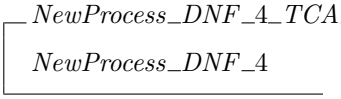

NewProcess_DNF_2_TCASE
NewProcess_DNF_2

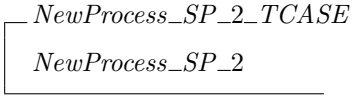

NewProcess_SP_3_TCASE
NewProcess_SP_3

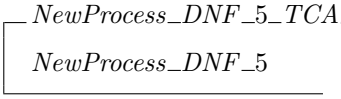

NewProcess_DNF_4
NewProcess_VIS
p? = current


NewProcess_SP_4_TCASE
NewProcess_SP_4


NewProcess_DNF_5
NewProcess_VIS
p? = nullp


NewProcess_DNF_4_TCASE
NewProcess_DNF_4


NewProcess_SP_2_TCASE
NewProcess_SP_2


NewProcess_DNF_5_TCASE
NewProcess_DNF_5