

• Variables nt, st

• Variables de canalización $\begin{cases} \text{free-tunnel-south} \\ \text{free-tunnel-north} \end{cases}$

• Invariante $\{I \wedge st > 0 \rightarrow nt = 0 \wedge nt > 0 \rightarrow st = 0\}$

"Si no hay ningún coche en el túnel que ha entrado desde el sur entonces pueden entrar en el túnel los coches desde el norte y viceversa"

• Métodos

wants-enter(self, direction)

self.mutex.acquire()

$\{INV\} \checkmark$

if direction == NORTH:

$\{INV\} \checkmark$

self.free-tunnel-north.wait_for($nt = 0$)

$\{I \wedge st = 0\} \equiv \{ \underbrace{st > 0 \rightarrow nt = 0}_{\text{no hay que demostrar nada aquí}} \wedge \underbrace{\text{falso} \rightarrow \text{cierto}}_{\checkmark} \} \checkmark$

$nt = nt + 1$

$\{I \wedge nt \geq 1\} \equiv \{ \underbrace{st = 0 \rightarrow nt \neq 0}_{\checkmark} \wedge \underbrace{\text{cierto} \rightarrow st = 0}_{\checkmark} \} \checkmark$

self.mutex.release()

$\{INV\} \checkmark$

else:

$\{INV\} \checkmark$

self.free-tunnel-south.wait_for($st = 0$)

$\{I \wedge st = 0\} \equiv \{ \underbrace{\text{falso} \rightarrow \text{cierto}}_{\checkmark} \wedge \underbrace{nt = 0 \rightarrow st \neq 0}_{\text{no hay nada que demostrar aquí}} \} \checkmark$

$st = st + 1$

$\{I \wedge st \geq 1\} \equiv \{ \underbrace{\text{cierto} \rightarrow nt = 0}_{\checkmark} \wedge \underbrace{nt = 0 \rightarrow st \neq 0}_{\checkmark} \} \checkmark$

self.mutex.release()

$\{INV\} \checkmark$

leaves-tunnel(self, direction)

self.mutex.acquire()

$\{INV\} \checkmark$

if direction == NORTH:

$\{INV\} \checkmark$

$nt = nt - 1$

$\{INV \wedge nt = nt - 1\} \equiv \{ \underbrace{st > 0 \rightarrow nt = 0}_{\text{no hay nada que demostrar aquí}} \wedge \underbrace{\text{cierto} \rightarrow st = 0}_{\checkmark} \} \checkmark$

nt no puede ser menor que cero $\Rightarrow nt - 1 > 0$

⊙ y no podría ser cero en este caso

temprero porque si $nt - 1 < 0 \Rightarrow nt > 0 \equiv \text{falso}$

else:

$\{INV\} \checkmark$

$st = st - 1$

$\{INV \wedge st = st - 1\} \equiv \{ \underbrace{\text{cierto} \rightarrow nt = 0}_{\checkmark} \wedge \underbrace{nt > 0 \rightarrow st = 0}_{\text{no hay nada que demostrar aquí}} \} \checkmark$

por el mismo razonamiento que ⊙ pero para st

$\{INV\} \checkmark$