

Ingeniería del Software II

4 – Propiedades de los sistemas reactivos y su análisis

Propiedades de los sistemas concurrentes

Con frecuencia, los programas concurrentes suelen ser reactivos, y sus características diferentes de las de los programas secuenciales convencionales.

Por esto, las propiedades que en general se desea garantizar de programas concurrentes difieren de las propiedades de programas secuenciales. Algunas de estas son:

- No violación de **invariantes** de sistema
- Ausencia de **starvation**
- Ausencia de **deadlock**
- Garantía de **exclusion mutua** en el acceso a recursos compartidos
- Ausencia de **livelock**

Categorías de propiedades

Una clasificación clásica de las propiedades de los sistemas reactivos incluye las siguientes cuatro categorías:

- Propiedades de **alcanzabilidad** ("reachability")
- Propiedades de **seguridad** ("safety")
- Propiedades de **vitalidad** ("liveness")
- Propiedades de **equidad** ("fairness")

Propiedades de alcanzabilidad ("reachability")

"Es posible que el sistema llegue a algún estado de un conjunto dado"

Por ejemplo:

- una (o alguna) componente entra a la region crítica
- es posible llegar a un estado de ERROR (ej: deadlock, violación de exclusión mutua, violación de invariante, etc.)

En este último caso nos interesa que se cumpla la negación de la propiedad. Es usual que la propiedad de interés sea la negación de la alcanzabilidad.

Propiedades de seguridad ("safety")

"Nunca va a pasar nada malo"

Por ejemplo:

- no es posible llegar a un estado de deadlock
- se garantiza exclusión mutua
- el sistema preserva un invariante dado

En general, la negación de una propiedad safety es una propiedad de alcanzabilidad

Propiedades de vitalidad ("liveness")

"Siempre es posible que algo bueno ocurra"

Por ejemplo:

- un (sub)proceso dado termina su ejecución
- es posible alcanzar un estado de estabilidad
- si se llama al ascensor, este llegará en algún momento

Propiedades de equidad ("fairness")

"Siempre ocurrirá algo de manera frecuente"

Por ejemplo:

- siempre que un proceso esté esperando para entrar a una región crítica, entonces logrará entrar
- siempre que un proceso solicite periódicamente un recurso finalmente se le será asignado.
- un proceso dado no sufre de inanición

Pospondremos su estudio en más detalle para la próxima unidad.

Por qué categorizar

Las razones dependen de los distintos puntos de vista:

• Metodología de especificación:

Nos ayuda a buscar las preguntas correctas que debemos hacerle a nuestro sistema, por ejemplo:

- ¿qué necesito para que mi sistema no llegue a una situación no deseada? (safety),
- ¿qué se debe cumplir para que mi sistema progrese en su ejecución? (liveness).

• Metodología de modelado:

En la tarea de modelado uno hace más incapié en ciertos aspectos de acuerdo al objetivo de verificación.

Por ejemplo, se pueden aplicar distintos tipos de simplificaciones según se desee verificar una propiedad de safety o de liveness.

Por qué categorizar (continuación)

● **Economía en la verificación:**

Las distintas clases requieren distintas técnicas de verificación, cada una con su complejidad.

Las propiedades de alcanzabilidad y de seguridad son las más cruciales para la corrección de un sistema y por lo tanto necesitan más atención.

Por suerte son las más fáciles de chequear.

● **Metodología de verificación:**

Algunas técnicas (en particular las de abstracción) sólo sirven para una determinada clase de propiedades.

Propiedades como conjuntos de trazas

La semántica de procesos (en realidad, una de las semánticas más simples para procesos) puede definirse como el conjunto de todas sus ejecuciones. Cada ejecución de un proceso puede verse como la sucesión de eventos en los cuales el proceso se involucra (y en el orden en que lo hace).

Ejemplo: Consideremos el siguiente proceso:

```
MAKER = (make->ready->MAKER).  
USER  = (ready->use->USER).  
  
||MAKER_USER = (MAKER || USER).
```

La única traza posible para **MAKER** es:

```
make, ready, make, ready, make, ...
```

Algunas trazas posibles para **MAKER_USER** son:

```
make, ready, use, make, ready, use, ...  
make, ready, make, use, ready, make, ready, use, ...
```

Propiedades como conjuntos de trazas (cont.)

Al igual que los procesos, las propiedades tienen una semántica dada en términos de conjuntos de trazas. Una propiedad P se identifica con todas las sucesiones de eventos atómicos que exhiben la propiedad P .

Por ejemplo, la propiedad “no ocurren dos producciones (make) sucesivas” contiene las siguientes trazas:

```
use, use, use, use, use, use, use, ...  
make, use, make, use, make, use, make, ...  
ready, ready, ready, ready, ready, ...
```

Lenguajes ω -regulares

Dado un lenguaje regular $A \subseteq \Sigma^*$ definimos

$$A^\omega \stackrel{\text{def}}{=} \{\sigma_1\sigma_2\sigma_3 \dots \mid \forall i \geq 0 : \sigma_i \in A \wedge \sigma_i \neq \epsilon\}$$

es decir, A^ω es el lenguaje conteniendo todas las concatenaciones infinitas de palabras no vacías de A .

Un lenguaje L se dice ω -regular si existen lenguajes regulares A_i y B_i , $0 \leq i \leq k$, tal que $\epsilon \notin B_i \neq \emptyset$ y

$$L = \bigcup_{0 \leq i \leq k} A_i \cdot B_i^\omega$$

donde \cdot denota la concatenación habitual de lenguajes.

Propiedad: Los lenguajes ω -regulares son cerrados por union, intersección y complemento.

Lenguajes ω -regulares

Dado un lenguaje regular A

$$A^\omega \stackrel{\text{def}}{=} \{\sigma_1\sigma_2\sigma_3 \dots\}$$

También las denominaremos
fragmentos de trazas

es decir, A^ω es el lenguaje de las concatenaciones infinitas de palabras no vacías de A .

Un lenguaje L se dice ω -regular si existen lenguajes regulares A_i y B_i , $0 \leq i \leq k$, tal que $\epsilon \notin B_i \neq \emptyset$ y

$$L = \bigcup_{0 \leq i \leq k} A_i \cdot B_i^\omega$$

donde \cdot denota la concatenación habitual de lenguajes.

Propiedad: Los lenguajes ω -regulares son cerrados por unión, intersección y complemento.

Lenguajes ω -regulares

Ejemplo:

La propiedad P sobre el proceso **MAKER_USER** puede escribirse como cualquiera de las siguientes expresiones ω -regulares:

$$\left((\text{make} + \text{ready} + \text{use}) (\text{ready} + \text{use})^+ \right)^\omega$$

$$\left((\text{make} + \varepsilon) (\text{ready} + \text{use}) \right)^\omega$$

$$\left((\text{make} + \text{ready} + \text{use})^* \text{make make} (\text{make} + \text{ready} + \text{use})^\omega \right)$$

Lenguajes ω -regulares

Ejemplo:

La propiedad P sobre el proceso **MAKER_USER** puede describirse como cualquiera de las siguientes expresiones ω -regulares:

$$\left((\text{make} + \text{ready} + \text{use}) (\text{ready} + \text{use})^+ \right)^\omega$$

$$\left((\text{make} + \varepsilon) (\text{ready} + \text{use}) \right)^\omega$$

$$\left((\text{make} + \text{ready} + \text{use})^* \text{make make} (\text{make} + \text{ready} + \text{use})^\omega \right)$$

Los lenguajes ω -regulares son cerrados por complemento

Formalización de propiedades safety

Observar:

- Si una traza viola una propiedad de safety, lo hace en un “instante” finito.
- Si un prefijo de una traza (infinita) viola una propiedad de safety, no hay forma de remediarlo (cualquiera sea la forma en que se continúe, la traza no dejará de violar la propiedad).

Es decir:

Un conjunto de trazas $P \subseteq \Sigma^{\omega}$ es una propiedad de safety si cumple

$$\forall \sigma : \sigma \notin P \Rightarrow \exists i \geq 0 : \forall \beta : \sigma[..i]\beta \notin P$$

o equivalentemente:

donde $\sigma[..i]$ denota el prefijo i -ésimo de σ .

Formalización de propiedades safety

Observar:

- Si una traza viola una propiedad de safety, lo hace en un "instante" finito.
- Si un prefijo de una traza (infinita) viola una propiedad de safety, cualquier forma de remediarlo (cualquiera sea la forma de la propiedad) la traza no dejará de violar la propiedad).

Es decir:

Un conjunto de trazas $P \subseteq \Sigma^{\omega}$ es una propiedad de safety si cumple

$$\forall \sigma : \sigma \notin P \Rightarrow \exists i \geq 0 : \forall \beta : \sigma[..i]\beta \notin P$$

o equivalentemente:

donde $\sigma[..i]$ denota el prefijo i -ésimo de σ .

Una propiedad P es de safety si toda palabra en su complemento tiene un "prefijo malo"

Formalización de propiedades safety

Observar:

- Si una traza viola una propiedad de safety, lo hace en un “instante” finito.
- Si un prefijo de una traza (infinita) viola una propiedad de safety, no hay forma de remediarlo (cualquiera sea la forma en que se continúe, la traza no dejará de violar la propiedad).

Es decir:

Un conjunto de trazas $P \subseteq \Sigma^{\omega}$ es una propiedad de safety si cumple

$$\forall \sigma : \sigma \notin P \Rightarrow \exists i \geq 0 : \forall \beta : \sigma[..i]\beta \notin P$$

o equivalentemente:

$$\forall \sigma : \forall i \geq 0 : \exists \beta : \sigma[..i]\beta \in P \Rightarrow \sigma \in P$$

donde $\sigma[..i]$ denota el prefijo i -ésimo de σ .

Formalización de propiedades safety

Observar:

- Si una traza viola una propiedad de safety, lo hace en un "instante" finito.
- Si un prefijo de una traza (infinita) viola una propiedad de safety, no hay forma de remediarlo (cualquiera sea la forma en que se continúe, la traza no dejará de violar la propiedad).

Es decir:

Un conjunto de trazas $P \subseteq \Sigma^\omega$ es una propiedad

$\forall \sigma : \sigma \notin P \Rightarrow \exists i \geq 0 : \forall \beta : \sigma[..i]\beta \notin P$

o equivalentemente:

$\forall \sigma : \forall i \geq 0 : \exists \beta : \sigma[..i]\beta \in P \Rightarrow \sigma \in P$

donde $\sigma[..i]$ denota el prefijo i -ésimo de σ .

Una propiedad P es de safety si toda traza infinita que se pueda "aproximar" finitamente con trazas de P , también está en P (la recíproca es evidente)

Formalización de propiedades safety

Ejemplos:

$$\left((\text{make} + \varepsilon) (\text{ready} + \text{use}) \right)^\omega$$

o Complemento:

$$(\text{make} + \text{ready} + \text{use})^* \text{make make} (\text{make} + \text{ready} + \text{use})^\omega$$

Prefijos malos

Formalización de propiedades safety

Ejemplos:

$$\left((\text{make} + \varepsilon) (\text{ready} + \text{use}) \right)^\omega$$

o Complemento:

$$(\text{make} + \text{ready} + \text{use})^* \text{make make} (\text{make} + \text{ready} + \text{use})^\omega$$

Prefijos malos

$$\left((\text{make} + \text{ready})^* (\text{use ready}^* (\text{use} + \varepsilon) \text{ready}^* \text{make})^* \right)^\omega$$

Sólo se puede usar hasta dos productos sin que antes se haga otro

Formalización de propiedades safety

Ejemplos:

$$\left((\text{make} + \varepsilon) (\text{ready} + \text{use}) \right)^\omega$$

o Complemento:

$$(\text{make} + \text{ready} + \text{use})^* \text{make make} (\text{make} + \text{ready} + \text{use})^\omega$$

Prefijos malos

$$\left((\text{make} + \text{ready})^* (\text{use ready}^* (\text{use} + \varepsilon) \text{ready}^* \text{make})^* \right)^\omega$$

o Complemento:

$$(\text{make} + \text{ready} + \text{use})^* (\text{use ready}^* \text{use ready}^* \text{use}) (\text{make} + \text{ready} + \text{use})^\omega$$

Prefijos malos

Formalización de propiedades liveness

Observar:

- Ningún fragmento de traza (finito) viola una propiedad de liveness: Si el evento que se esperaba que ocurriera aún no lo hizo, puede suceder más adelante.

Es decir:

Un conjunto de trazas $P \subseteq \Sigma^\omega$ es una propiedad de liveness si cumple

$$\forall \alpha \in \Sigma^* : \exists \beta \in \Sigma^\omega : \alpha\beta \in P$$

Es decir, una propiedad P es de liveness si toda palabra en su complemento **NO** tiene un "prefijo malo"

Formalización de propiedades liveness

Ejemplo:

$(\text{make} + \text{ready})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

En algún momento se puede consumir ("use")

Formalización de propiedades liveness

Ejemplo:

$(\text{make} + \text{ready})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

es equivalente a:

$(\text{make} + \text{ready} + \text{use})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

Todos los posibles
prefijos aparecen en la
propiedad

Formalización de propiedades liveness

Ejemplo:

$(\text{make} + \text{ready})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

es equivalente a:

$(\text{make} + \text{ready} + \text{use})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

Todos los posibles prefijos aparecen en la propiedad

$((\text{ready} + \text{use})^* \text{make})^\omega$

La producción se realiza indefinidamente (se producen infinitos "make" a lo largo de la ejecución)

Formalización de propiedades liveness

Ejemplo:

$(\text{make} + \text{ready})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

es equivalente a:

$(\text{make} + \text{ready} + \text{use})^* \text{use} (\text{make} + \text{ready} + \text{use})^\omega$

Todos los posibles prefijos aparecen en la propiedad

$((\text{ready} + \text{use})^* \text{make})^\omega$

es equivalente a:

$(\text{ready} + \text{use} + \text{make})^* ((\text{ready} + \text{use})^* \text{make})^\omega$

Todos los posibles prefijos aparecen en la propiedad

Safety, liveness y todas las demás

Teorema [Alpern & Schneider 85]:

Toda propiedad puede escribirse como la intersección de una propiedad de safety y una de liveness.

Ejemplo: *a* until *b*

algún evento *b* ocurre inmediatamente precedido por una serie ininterrumpida de eventos *a* (léase: "*a* ocurre hasta que ocurre *b*")

$$a^* b \Sigma^\omega = (a^* b \Sigma^\omega + a^\omega) \cap (\Sigma^* b \Sigma^\omega)$$

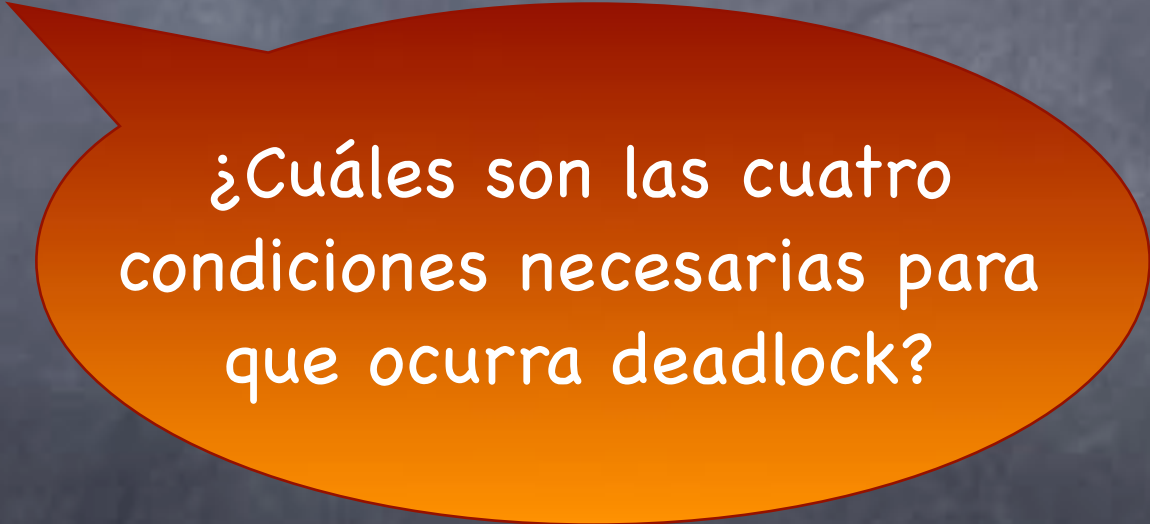
A la izquierda de la intersección se da la propiedad safety y a la derecha, la de liveness.

(¿Qué significa cada una de estas propiedades?)

Análisis de propiedades en FSP

Los distintos tipos de propiedades en FSP se verifican y/o modelan de manera distinta.

Deadlock



¿Cuáles son las cuatro condiciones necesarias para que ocurra deadlock?

Análisis de propiedades en FSP

Los distintos tipos de propiedades en FSP se verifican y/o modelan de manera distinta.

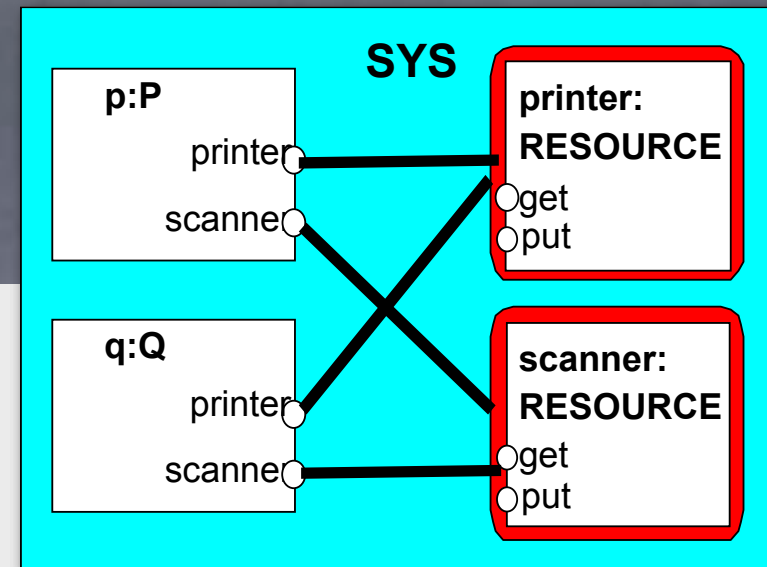
Deadlock

```
RESOURCE = (get -> put -> RESOURCE).
```

```
P = (printer.get -> scanner.get -> copy  
    -> printer.put -> scanner.put -> P).
```

```
Q = (scanner.get -> printer.get -> copy  
    -> printer.put -> scanner.put -> Q).
```

```
||SYS = (p:P || q:Q  
    || {p,q}::printer:RESOURCE  
    || {p,q}::scanner:RESOURCE  
    ).
```



Análisis de propiedades en FSP

Los distintos
modelan de m

LTSA puede chequear
deadlock. Lo hace mediante una
búsqueda exhaustiva.

se verifican y/o

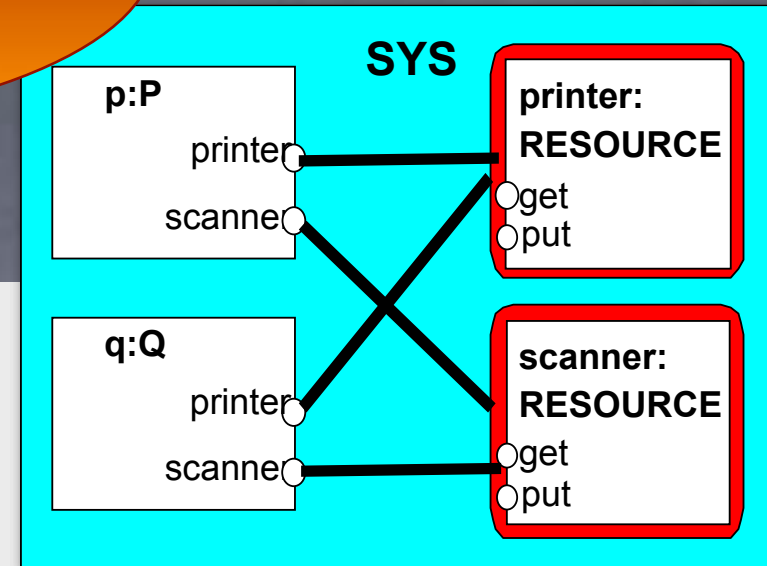
Deadlock

```
RESOURCE = (get -> put -> RESOURCE).
```

```
P = (printer.get -> scanner.get -> copy  
    -> printer.put -> scanner.put -> P).
```

```
Q = (scanner.get -> printer.get -> copy  
    -> printer.put -> scanner.put -> Q).
```

```
||SYS = (p:P || q:Q  
    || {p,q}::printer:RESOURCE  
    || {p,q}::scanner:RESOURCE  
    ).
```



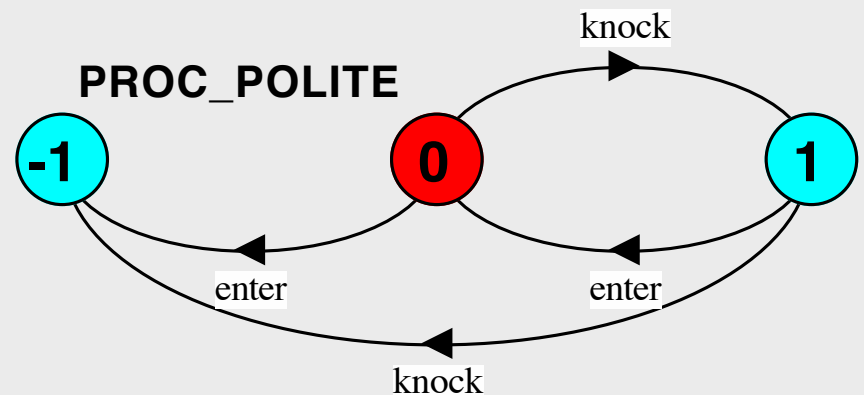
Análisis de propiedades en FSP

Safety

En FSP podemos expresar las propiedades de safety mediante procesos haciendo uso del estado de **ERROR** para indicar cuáles son las trazas que violan esta propiedad (i.e. los prefijos malos).

Ejemplo: Una persona educada golpea sólo una vez antes de entrar y no entra sin golpear.

```
PROC_POLITE = (knock->(enter->PROC_POLITE
                    | knock->ERROR
                )
              | enter->ERROR
            ).
```



Toda ejecución que lleva a **ERROR** es un "prefijo malo"

Análisis de propiedades en FSP

Safety (cont.)

FSP provee una construcción que nos permite obviar el agregado “a mano” de los estados de error:

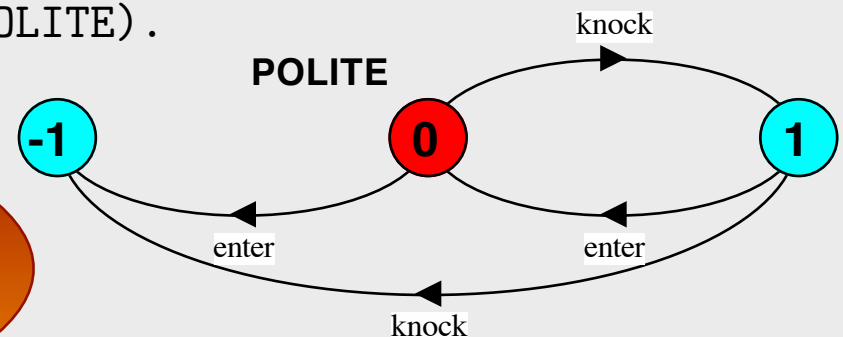
```
property N = P
```

indica que los eventos correspondientes al alfabeto de P deben ocurrir respetando el patrón de ocurrencias definido por P (toda ocurrencia no definida por P lleva al estado de **ERROR**).

En el ejemplo anterior:

```
property POLITE = (knock -> enter -> POLITE).
```

La declaración de un proceso P como **property** determina que la omisión de una acción en un estado de P interpretado como **proceso** induce una transición errónea en P como **propiedad**.



Análisis de propiedades en FSP

Safety (cont.)

Ejemplo

```
const Max = 3
range Int = 0..Max
```

```
SEMAPHORE(N=0) = SEMA[N] ,
SEMA[v:Int]    = (up->SEMA[v+1]
                  |when(v>0) down->SEMA[v-1]
                  ) .
```

```
LOOP = (mutex.down->enter->exit->mutex.up->LOOP) .
```

```
||SEMADEMO = (p[1..3]:LOOP
              || {p[1..3]}::mutex:SEMAPHORE(1)) .
```


Análisis de propiedades en FSP

Safety (cont.)

Ejemplo

```
const Max = 3
range Int = 0..Max
```

```
SEMAPHORE(N=0) = SEMA[N] ,
SEMA[v:Int]    = (up->SEMA[v+1]
                  |when(v>0) down->SEMA[v-1]
                  ) .
```

```
LOOP = (mutex.down->enter->exit->mutex.up->LOOP) .
```

```
||SEMADEMO = (p[1..3]:LOOP
              || {p[1..3]}::mutex:SEMAPHORE(1)) .
```

```
property MUTEX
= (p[i:1..3].enter->p[i].exit->MUTEX) .
```

```
||CHECK = (SEMADEMO || MUTEX) .
```



Propiedad de
exclusión mututua

Análisis de propiedades en FSP

Safety (cont.)

Ejemplo

```
const Max = 3
range Int = 0..Max
```

```
SEMAPHORE(N=0) = SEMA[N] ,
SEMA[v:Int]    = (up->SEMA[v+1]
                  |when(v>0) down->SEMA[v-1]
                  ) .
```

```
LOOP = (mutex.down->enter->exit->mutex.up->LO
```

```
||SEMADEMO = (p[1..3]:LOOP
              || {p[1..3]}::mutex:SEMAPHORE(1)) .
```

```
property MUTEX
= (p[i:1..3].enter->p[i].exit->MUTEX) .
```

```
||CHECK = (SEMADEMO || MUTEX) .
```

LTSA puede chequear safety.
También lo hace mediante búsqueda exhaustiva.

Verificar cambiando
la inicialización del
semáforo a 2.

Propiedad de
exclusión mututua

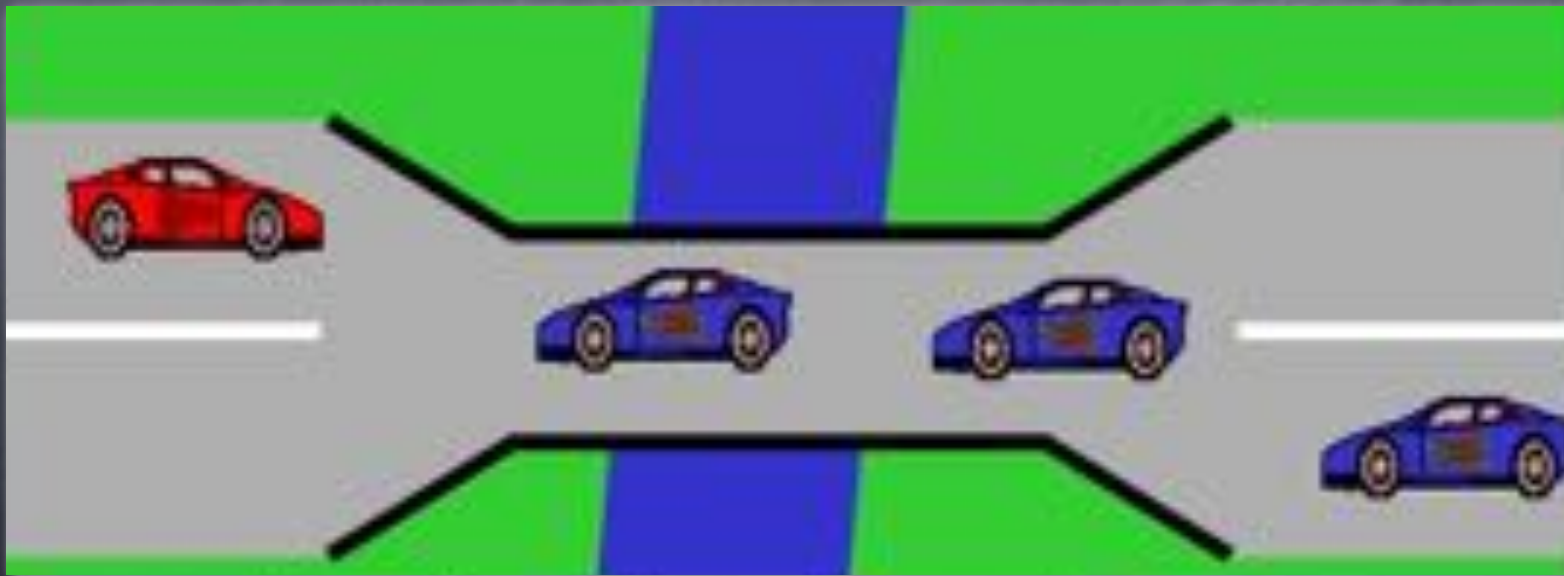
Análisis de propiedades en FSP

Safety (cont.)

Ejemplo: Un puente de una sola vía

Un puente sobre un río tiene el ancho suficiente para permitir tráfico en sólo una dirección. Por consiguiente, los autos sólo pueden cruzar el puente concurrentemente si viajan en la misma dirección.

Cuando dos autos que viajan en direcciones opuestas ingresan al puente al mismo tiempo ocurre una **violación de seguridad**.



Ejemplo: Un puente de una sola vía

```
const N = 3 // number of each type of car
range T = 0..N // type of car count
range ID= 1..N // car identities
```

```
CAR = (enter->exit->CAR).
```

```
/* cars may not overtake each other */
NOPASS1   = C[1],
C[i:ID]   = ([i].enter -> C[i%N+1]).
```

```
NOPASS2   = C[1],
C[i:ID]   = ([i].exit -> C[i%N+1]).
```

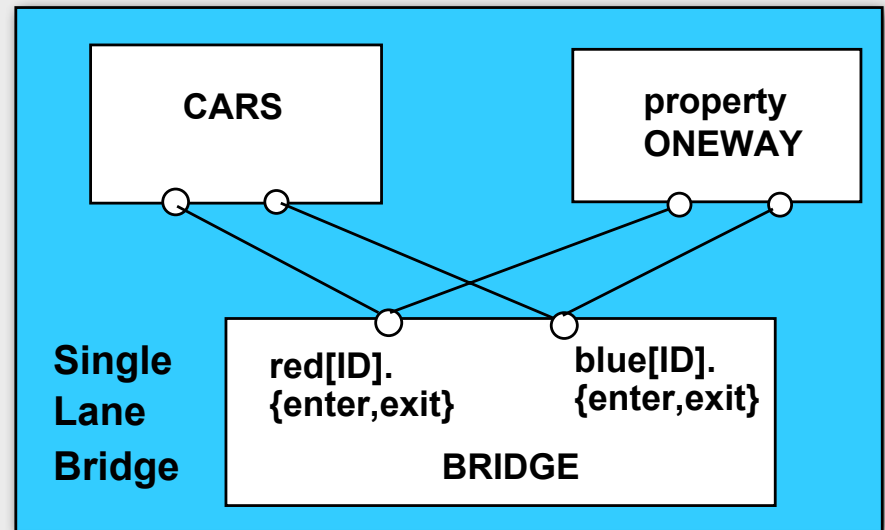
```
||CONVOY = ([ID]:CAR || NOPASS1 || NOPASS2).
```

```
||CARS = (red:CONVOY || blue:CONVOY).
```

```
property ONEWAY = ( red[ID].enter -> RED[1]
                    | blue[ID].enter -> BLUE[1]
                    ),
RED[i:ID] = (red[ID].enter -> RED[i+1]
             |when(i==1)red[ID].exit -> ONEWAY
             |when( i>1)red[ID].exit -> RED[i-1]
             ),
BLUE[i:ID] = (blue[ID].enter -> BLUE[i+1]
              |when(i==1)blue[ID].exit -> ONEWAY
              |when( i>1)blue[ID].exit -> BLUE[i-1]
              ).
```

```
BRIDGE = BRIDGE[0][0],
BRIDGE[nr:T][nb:T] =
    (when (nb==0)
      red[ID].enter -> BRIDGE[nr+1][nb]
    |red[ID].exit   -> BRIDGE[nr-1][nb]
    |when (nr==0)
      blue[ID].enter -> BRIDGE[nr][nb+1]
    |blue[ID].exit   -> BRIDGE[nr][nb-1]
    ).
```

```
||SingleLaneBridge = (CARS || BRIDGE || ONEWAY ).
```



Análisis de propiedades en FSP

Liveness

LTSA solo puede manejar un conjunto reducido de propiedades de liveness:

```
progress N = { a1, a2, ... }
```

Esto indica que, en toda ejecución fuertemente equitativa (strongly fair), alguna de la acciones a_1, a_2, \dots debe ejecutarse infinitas veces

Ejemplo:

```
COIN = ( toss -> heads -> COIN  
        | toss -> tails -> COIN ).  
progress HEADS = {heads}
```

Análisis de progreso

LTSA puede chequear progreso. En este caso, el algoritmo se basa en la búsqueda de ciclos que atrapen las acciones en N

Liveness

LTSA solo puede manejar un caso de liveness:

```
progress N = { a1, a2, ... }
```

Esto indica que, en toda ejecución fuertemente equitativa (strongly fair), alguna de las acciones a_1, a_2, \dots debe ejecutarse infinitas veces

Ejemplo:

```
COIN = ( toss -> heads -> COIN
        | toss -> tails -> COIN ).
progress HEADS = {heads}
```


Análisis de progreso

Liveness

LTSA solo puede manejar un caso de liveness:

```
progress N = { a1, a2, ... }
```

Esto indica que, en toda ejecución finita (es decir, finita y justa), alguna de las acciones a_1, a_2, \dots de N debe ocurrir.

Ejemplo:

```
COIN = ( toss -> heads -> COIN
        | toss -> tails -> COIN ).
progress HEADS = {heads}
```

LTSA puede chequear progreso. En este caso, el algoritmo se basa en la búsqueda de ciclos que atrapen las acciones en N

Explicación: LTSA verifica bajo la suposición de **strong fairness**. Sin esta suposición, la propiedad es falsa.

LTSA la verifica verdadera

Análisis de progreso

Liveness

LTSA solo puede manejar un caso de liveness:

```
progress N = { a1, a2, ... }
```

Esto indica que, en toda ejecución finita (es decir, finita y *fair*), alguna de las acciones a_1, a_2, \dots de N debe ocurrir.

Ejemplo:

```
COIN = ( toss -> heads -> COIN
        | toss -> tails -> COIN ).
progress HEADS = {heads}
```

Ejemplo: para el puente de una sola vía

```
progress BLUECROSS = {blue[ID].enter}
progress REDCROSS = {red[ID].enter}
```

LTSA puede chequear progreso. En este caso, el algoritmo se basa en la búsqueda de ciclos que atrapen las acciones en N

Explicación: LTSA verifica bajo la suposición de **strong fairness**. Sin esta suposición, la propiedad es falsa.

LTSA la verifica verdadera

Análisis de progreso

Liveness

LTSA solo puede manejar un caso de liveness:

```
progress N = { a1, a2, ... }
```

Esto indica que, en toda ejecución finita (es decir, que no sea *fair*), alguna de las acciones a_1, a_2, \dots debe ocurrir.

Ejemplo:

```
COIN = ( toss -> heads -> COIN
        | toss -> tails -> COIN ).
progress HEADS = {heads}
```

Ejemplo: para el puente de una sola vía

```
progress BLUECROSS = {blue[ID].enter}
progress REDCROSS = {red[ID].enter}
```

LTSA puede chequear progreso. En este caso, el algoritmo se basa en la búsqueda de ciclos que atrapen las acciones en N

Explicación: LTSA verifica bajo la suposición de **strong fairness**. Sin esta suposición, la propiedad es falsa.

LTSA la verifica y la declara verdadera

LTSA las verifica correctas!! :-)

Prioridades entre acciones

LTSA asume en general que la elección es equitativa (fair), por eso no reporta error de progreso en el ejemplo de la moneda o en el puente de una sola vía.

Sin embargo, sabemos que es posible que los autos azules (o los rojos) acaparen el puente haciendo que los rojos (o los azules) esperen por siempre.

Entonces, para detectar problemas de progreso debemos imponer políticas de scheduling en las acciones que modele la situación en la que el puente (o cualquier otro sistema en general) es sometido a usos extremos.

Operador de alta prioridad: $||C = (P||Q) \ll \{a_1, \dots, a_n\}$ especifica una composición en la cual las acciones a_1, \dots, a_n tienen mayor prioridad que cualquier otra acción en $P||Q$, incluyendo τ .

Operador de baja prioridad: $||C = (P||Q) \gg \{a_1, \dots, a_n\}$ especifica una composición en la cual las acciones a_1, \dots, a_n tienen menos prioridad que cualquier otra acción en $P||Q$, incluyendo τ .

Análisis de propiedades en FSP

Liveness (cont.)

Ejemplo: Siguiendo con el puente de una sola vía deseamos modelar que el puente se encuentra congestionado.

Para ello daremos menor prioridad a los eventos de salida del puente. De esta manera se prioriza a la entrada sobre la salida forzando la congestión del puente:

```
||CongestedBridge =  
    SingleLaneBridge >> {red[ID].exit,blue[ID].exit}.
```

Al verificar las propiedades de progreso, LTSA nos indicará ahora una situación de error.

Análisis de propiedades en FSP

Liveness (cont.)

Ejemplo: Siguiendo con el puente de un solo carril, vamos a modelar que el puente se encorcha. Para ello daremos menor prioridad a los procesos que cruzan el puente. De esta manera se priorizará a los procesos que se quedan forzando la congestión del puente.

Otros model checkers permiten elegir si se desea realizar la verificación bajo **fairness** o no.

```
||CongestedBridge =  
    SingleLaneBridge >> {red[ID].exit, blue[ID].exit}.
```

Al verificar las propiedades de progreso, LTSA nos indicará ahora una situación de error.