Lección 4:
Semántica de la composición concurrente

- Acciones atómicas: condicionales e incondicionales
- Regla de la composición concurrente
- Aserciones críticas
- Sobre la ausencia de interferencias

Acciones atómicas

- Terminología:
  - **acción atómica incondicional**: B es TRUE
  - **acción atómica condicional**: la que no es incondicional
    - Importante: dada la "atomicidad", si B es FALSE, sólo la ejecución de otro proceso puede hacerla TRUE
- Regla del await:

$$\frac{\{Q \wedge B\}\ S\ \{R\}}{\{Q\}\ \langle await\ (B)\ S\rangle\ \{R\}}$$

¡¡OJO: para corrección parcial!!

- ¿Cuándo es correcto?

```
-- s>=0
<await (s>0) s:=s-1>
-- s>=0
```

- ¿Casos particulares interesantes?

Semántica de la composición concurrente

- ¿"$\{Q_i\}\ S_i\ \{R_i\}$", $i \in \{1..n\}$, permite asegurar ... ?

```
-- Q1 ∧ ... ∧ Qk
PCo S1 || ... || Sk FCo
-- R1 ∧ ... ∧ Rk
```

- Depende:

```
Vars x:Ent := 0
-- x=0 ∧ x=0
PCo <x:=x+1> || <x:=x+1> FCo
-- ¿x=1 ∧ x=1?
```

¡¡NO!!

```
Vars x:Ent := 0
     y:Ent := 0
-- x=0 ∧ y=0
PCo <x:=x+1> || <y:=y+1> FCo
-- ¿x=1 ∧ y=1?
```

¡¡SI!!

Aserciones críticas

- Causa: problema de **interferencias**
- Acción **elegible**:
  - un proceso como secuencia de acciones atómicas
  - una acción atómica es "elegible" si es la siguiente a ejecutar
- Problema: las acciones "elegibles" en un estado dado se pueden ejecutar en cualquier orden
  - ¿qué pasa si, cuando una se empieza a ejecutar, la ejecución de otra ha hecho la Pre de la primera FALSE?
- Para una acción elegible, el predicado necesario para su **Pre** se denominará **aserción crítica**

Aserciones críticas

- Considerar el teorema "`{Q} S {R}`"

AC1 | **R** es una **aserción crítica**

AC2 | para cada instrucción A, fuera de un "await", tal que "`{pre(A)} A {post(A)}`" se ha usado en la verificación, "`pre(A)`" es una **aserción crítica**

Aserciones críticas

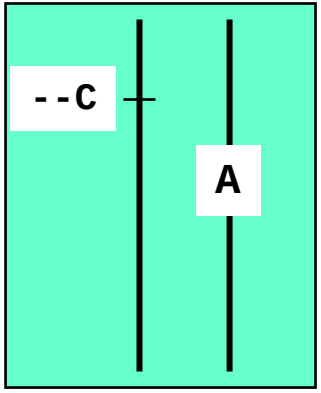
- Se puede matizar (AC2):

AC2' | para cada instrucción A, fuera de un "await", tal que "`A {post(A)}`" se ha usado en la verificación, "`{pmd(A,post(A))}`" es una aserción crítica

- Comentarios:
  - ¿Por qué solo instrucciones fuera de un "await"?
  - Notar que asumimos procesos completamente anotados

Ausencia de interferencias

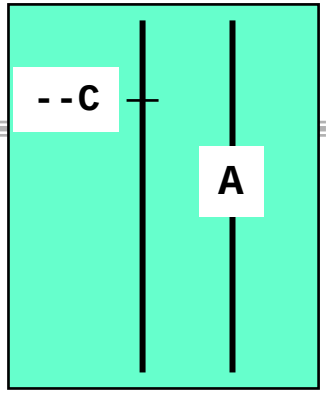
- Una manera de asegurar que la corrección de cada proceso implique la corrección de su ejecución concurrente:
  - que ninguna aserción crítica sea interferida por otro proceso
- ¿Quién puede interferir?
  - acciones de asignación (incluye invoc. a procedimientos)
  - por lo tanto, nos vamos a centrar en las asignaciones
- Principio de **no interferencia**:
  - sean A una asignación, y C una aserción crítica
  - entonces



NI(A,C): {pre(A) $\wedge$ C} A {C}

"C" es invariante para "A" bajo "pre(A)"

Ausencia de interferencias



- Procesos **libres de interferencias** (L.I.):
  - las verificaciones "$\{Q_i\}\ S_i\ \{R_i\}$", $i \in \{1..n\}$ son L.I.
  - cuando

```
Para cada asignación A de Si
  Para cada aserción crítica C de Sj,(j<>i)
     NI(A,C)
```

- Una regla de inferencia para la ejecución concurrente:

$$\frac{\{Q_i\}\ S_i\ \{R_i\}, i \in \{1..n\},\ \text{L.I.}}{\{Q_1 \wedge \ldots \wedge Q_k\}\ \mathit{PCo}\ S_1||\ldots||S_k\ \mathit{FCo}\ \{R_1 \wedge \ldots \wedge R_k\}}$$

¡¡OJO: para corrección parcial!!

Ausencia de interferencias

- Verificar la L.I. puede ser muy costoso, pero es mejor que verificar cada uno de los posibles entrelazados
  - el número de entrelazados puede ser "exponencial" (¿en qué?)
  - el número de comprobaciones de NI es "cuadrático" (¿en qué?)
- Una solución: poder asegurar, por otros métodos, que se cumple la propiedad:
  - uso de variables disjuntas
  - debilitamiento de aserciones
  - uso de invariantes globales