

# Sistemas Concurrentes y Distribuidos



*Escuela Técnica Superior de Ingenierías  
Informática y de Telecomunicación*

**Los Del DGIIM**, [losdeldgiim.github.io](https://losdeldgiim.github.io)

Doble Grado en Ingeniería Informática y Matemáticas  
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

# Sistemas Concurrentes y Distribuidos

Los Del DGIIM, [losdeldgiim.github.io](https://losdeldgiim.github.io)

José Juan Urrutia Milán  
Arturo Olivares Martos

Granada, 2024-2025



# Índice general

<b>1. Introducción a la Programación Concurrente</b>	<b>5</b>
1.1. Conceptos básicos . . . . .	5
1.1.1. Comparación de programas concurrentes con secuenciales . . .	5
1.1.2. Definición de concurrencia . . . . .	6
1.1.3. Axiomas de la programación concurrente . . . . .	6
1.2. Modelos para creación de procesos en un programa . . . . .	8
1.2.1. Grafos de Sincronización . . . . .	8
1.2.2. Definición estructurada de procesos . . . . .	9
1.2.3. Definición no estructurada de procesos . . . . .	9
1.3. Exclusión mutua y sincronización . . . . .	10
1.4. Propiedades de los sistemas concurrentes . . . . .	12
1.4.1. Propiedades de seguridad ( <i>safety</i> ) . . . . .	12
1.4.2. Propiedades de vivacidad ( <i>liveness</i> ) . . . . .	13
1.5. Lógica de programas de Hoare y verificación de programas concurrentes	14
1.5.1. Corrección de los programas concurrentes . . . . .	14
1.5.2. Introducción a la Lógica de Hoare . . . . .	15
1.5.3. Verificación de sentencias concurrentes . . . . .	20
1.5.4. Verificación usando invariantes globales . . . . .	26
<b>2. Sincronización en memoria compartida. Monitores</b>	<b>29</b>
2.1. Definición de un monitor . . . . .	29
2.1.1. Concepto de monitor . . . . .	30
2.1.2. Características de programación con monitores . . . . .	34
2.1.3. Operaciones de sincronización . . . . .	37
2.2. Verificación de programas con monitores . . . . .	39
2.2.1. Invariante de monitor . . . . .	40
2.2.2. Axiomas para operaciones de sincronización con semántica desplazante . . . . .	41
2.2.3. Regla de la concurrencia para la verificación de programas con monitores . . . . .	47
<b>3. Relaciones de problemas</b>	<b>49</b>
3.1. Introducción . . . . .	49



# 1. Introducción a la Programación Concurrente

## 1.1. Conceptos básicos

Hasta ahora, nos hemos dedicado al estudio y desarrollo de programas secuenciales, que podemos entender de forma intuitiva como una ejecución lineal de instrucciones.

En programación concurrente, tendremos ahora múltiples unidades de ejecución independientes, a las que llamaremos procesos (sea un core o un procesador). La programación concurrente trata de coordinar los procesos para que cooperen entre sí con el fin de realizar un problema global de forma mucho más rápida de como lo haría un programa secuencial.

Podemos pensar que un proceso es una unidad de software abstracta conformada por un conjunto de instrucciones a ejecutar y por el contexto del procesador (como los valores de los registros, el contador de programa, el puntero de pila, la memoria Heap, memoria para variables, el acceso a determinados recursos, ...), al que llamamos estado del proceso.

Cuando en esta asignatura aparezca “flujo de control”, debemos pensar en una secuencia de ejecución de instrucciones. Es decir, como si fuera un proceso pero carente de un estado.

Nuestro trabajo en esta asignatura será gestionar la concurrencia, es decir, la ejecución independiente de dichos procesos con el fin de que no sea una sucesión de eventos incontrolados.

### 1.1.1. Comparación de programas concurrentes con secuenciales

Normalmente, en un programa concurrente tendremos más procesos que núcleos donde ejecutar dichos procesos, de donde aparece el concepto de concurrencia: en programación concurrente debe parecer que todos los procesos avanzan de forma simultánea, pese a haber más procesos que núcleos.

Si provocamos cambios de contexto dejando avanzar al resto de flujos de con-

trol, el programa no sufrirá las latencias provocadas por los procesos de E/S (por ejemplo), haciendo que el programa global sea más eficiente gracias a la concurrencia.

En sistemas que simulen el mundo real, podemos asociar un proceso con cada ente que intervenga en nuestro sistema (como una simulación del tráfico en una ciudad, o del movimiento de planetas), con lo que los sistemas de simulación pueden modelarse mejor con procesos concurrentes independientes, más que con programas secuenciales.

### 1.1.2. Definición de concurrencia

Podríamos definir la concurrencia como el paralelismo potencial que existe en los programas que puede aprovecharse independientemente de las limitaciones del hardware en el que se ejecuta el programa.

Como ya hemos mencionado, podremos tener un mayor número de procesos que de cores, y con este modelo cada uno de los procesos se ejecuta aparentemente al mismo tiempo que los demás.

El concepto de concurrencia es un concepto de programación a alto nivel que trata de representar el paralelismo potencial que existe en un programa. Con los compiladores adecuados, podemos programar en función de dichas características sin limitarnos por la arquitectura hardware del ordenador.

El objetivo fundamental de la concurrencia es simplificar toda la parte de la sincronización y comunicación entre los diferentes procesos de un programa, el cual suele ser un problema complejo sin solución fácil. Nos da un nivel algorítmico suficientemente independiente de los detalles del hardware para resolver dichos problemas, facilitando la portabilidad del código entre arquitecturas y lenguajes de programación.

Como beneficios de este modelo abstracto (el de la concurrencia), podemos destacar:

- Da herramientas, instrucciones y sentencias útiles para problemas de sincronización entre procesos.
- Las primitivas de programación en un lenguaje de alto nivel (como son los lenguajes concurrentes) son más fáciles de utilizar que con lenguajes de bajo nivel. Por ejemplo, los semáforos son más complejos que los monitores.
- Evita la dependencia con instrucciones de bajo nivel, haciendo que el programa pueda ejecutarse en otra computadora.

### 1.1.3. Axiomas de la programación concurrente

La programación concurrente es un modelo abstracto definido en base a 5 axiomas que nos dicen si un lenguaje es o no concurrente. En caso de no cumplirse, el código no va a poder ser transportable ni verificable.

Estos axiomas son:



**1. Atomicidad y entrelazamiento de instrucciones atómicas.**

Al menos ciertas instrucciones han de ser atómicas (esto es, instrucciones que no pueden ser interrumpidas, como por ejemplo las lecturas y escrituras en memoria).

**2. Consistencia de los datos tras un acceso concurrente.**

El entrelazamiento de instrucciones atómicas preserva la consistencia de los resultados de las operaciones. Es decir, si tenemos muchos procesos actuando a la vez sobre un conjunto de datos compartidos, debemos estar seguros de que los accesos a los mismos no los estropeen.

**3. Irrepetibilidad de las secuencias de instrucciones.**

Cuando se ejecuta un programa concurrente, se sucede un entrelazamiento de las instrucciones de los procesos que se ejecutan a la vez, con lo que la secuencia de instrucciones que obtenemos como resultado de volver a ejecutar el mismo programa con otros datos es muy probable que no sea la misma.

Esto dificulta el “debugging” de un programa concurrente, ya que podemos tener un error en el programa que repercute en el mal funcionamiento del mismo sólo cuando se suceda una secuencia de instrucciones específica en la ejecución del mismo.

**4. Independencia de la velocidad de los procesos.**

No puede hacerse ninguna suposición en la velocidad de ejecución de un proceso, ya que este puede verse suspendido o ralentizado, salvo que esta es positiva.

La corrección en programas concurrentes no debe depender de la velocidad relativa de los procesos.

**5. Hipótesis del progreso finito.**

- Un proceso debe tratar de avanzar todo lo que pueda. Esto es, si un proceso se está ejecutando, debe tratar de ejecutar tantas instrucciones como sea posible.
- Una vez que un proceso comienza a ejecutar una sección de código, debe terminar dicha sección.
- Todo proceso debe seguir progresando durante la ejecución de un programa.

Cuando se interpreta la ejecución de un programa concurrente como un conjunto de trazas de las cuales elegimos una al ejecutar el programa, estamos ignorando ciertos detalles, como:

- El estado de la memoria asignado a cada proceso.
- El valor de los registros de cada proceso.
- El coste computacional de los cambios de contexto.
- La política de planificación que se emplea de los procesos.
- El desarrollo de los programas es independiente del hardware.

## 1.2. Modelos para creación de procesos en un programa

En relación al número de procesos que se ejecutan en un programa, podemos clasificarlos en:

- Sistemas estáticos: El número de procesos en el programa es el mismo durante su ejecución. Dicho número se define al programarlo y en el momento de la compilación.
- Sistemas dinámicos: El número de procesos es variable, de forma que durante la ejecución del programa pueden crearse y destruirse procesos.

### 1.2.1. Grafos de Sincronización

Un Grafo de Sincronización es un Grafo Dirigido Acíclico (DAG) donde cada nodo representa una secuencia de sentencias del programa (o actividad). Nos sirven para definir situaciones de precedencia en la ejecución de un programa. Tenemos que tener instrucciones en el lenguaje concurrente que nos permitan representar el comienzo de las instrucciones con un DAG.

En un DAG, se suceden dependencias secuenciales, esto es, un proceso no empieza hasta que termina otro: dadas dos actividades  $S_1$  y  $S_2$ , una arista desde la primera hacia la segunda ( $S_1 \rightarrow S_2$ ) significa que  $S_2$  no puede comenzar su ejecución hasta que  $S_1$  haya finalizado.

**Ejemplo.** El DAG de la Figura 1.1 nos indica que la primera actividad que tendrá lugar en nuestro programa será la actividad  $S_1$ . Tras el fin de esta, se sucederán de forma concurrente las actividades  $S_2$  y  $S_3$ . Tras terminar  $S_2$ , comenzará  $S_4$  y, tras esta, se ejecutarán de forma concurrente  $S_5$  y  $S_6$ . Finalmente, tras el final de  $S_5$ ,  $S_6$  y  $S_3$ , el programa terminará con la actividad  $S_7$ .



Figura 1.1: Ejemplo de DAG

En relación a cómo podemos crear los procesos, destacamos dos formas que podemos encontrarnos en los lenguajes paralelos:

### 1.2.2. Definición estructurada de procesos

En programación estructurada, contaremos con dos palabras reservadas del lenguaje que nos permitirán recrear la siguiente funcionalidad a explicar. En pseudocódigo, nos referiremos a ellas como **cobegin** y **coend**.

Dados dos procesos  $P_1$  y  $P_2$  que queremos que se ejecuten de forma concurrente, bastará especificar en pseudocódigo:

```
1  cobegin
    P1;
    P2;
  coend
```

Hasta llegar a la palabra **cobegin** no comenzará ningún proceso. Tras esta, se sucederá un entrelazado de las instrucciones de  $P_1$  y  $P_2$ , y no se saldrá de dicha región hasta que terminen ambos procesos.

**Ejemplo.** Un programa utilizando la definición estructurada de procesos que cumpla el DAG de la Figura 1.1 es el siguiente:

```
1  begin
    S1;
    cobegin
        begin
5      S2;
        S4;
        cobegin
            S5;
            S6;
10     coend
        end
    S3;
    coend
    S7;
15 end
```

### 1.2.3. Definición no estructurada de procesos

En lenguajes concurrentes que no cuenten con palabras reservadas que simulen **cobegin** y **coend**, contaremos con dos llamadas al sistema que nos permitirán replicar dicha funcionalidad para crear procesos:

#### **fork**

Duplica el proceso que actualmente se está ejecutando y lo lanza a ejecución. Si se le especifica una rutina, cambiará el código del clon por dicha rutina.

#### **join**

Espera a que cierto proceso termine de ejecutarse antes de proseguir con la ejecución del resto de instrucciones.

La función **fork** ya se vió en la asignatura de Sistemas Operativos, por lo que el estudiante debería estar familiarizado con ella.

**Ejemplo.** Un programa con definición no estructurada de procesos para el DAG de la Figura 1.1 es el siguiente:

```
1  begin
    S1;
    fork S3;
    S2;
5  S4;
    fork S6;
    S5;
    join S3;
    join S6;
10 S7;
end
```

### 1.3. Exclusión mutua y sincronización

No todas las secuencias de entrelazamiento de un programa concurrente van a ser aceptables. Para impedir que sucedan ciertas secuencias (o trazas) tenemos condiciones de sincronización, relacionadas con instrucciones de lenguajes de programación de tal forma que dichas instrucciones no se ejecutan hasta que no es cierta una condición que depende de las variables del proceso.

De esta forma, una **condición de sincronización** es una restricción en el orden en que se pueden entremezclar las instrucciones que generan los procesos de un programa. Podemos utilizarlas para asegurarnos de que todas las trazas del programa son correctas.

La **exclusión mutua** es un caso particular de sincronización en el que se obliga a que un trozo de código de un proceso sea ejecutado de forma totalmente secuencial de manera que no se permita el entrelazamiento con otros procesos. Este trozo de código (en el que no se permite el entrelazamiento de instrucciones con otros procesos) recibe el nombre de **sección crítica**. Se dice que las secciones críticas se ejecutan en exclusión mutua.

La mayoría de instrucciones en un programa son instrucciones compuestas (esto es, formadas por varias instrucciones en lenguaje máquina). Si queremos establecer secciones críticas para la ejecución de cada una de dichas instrucciones, rodearemos la instrucción por < y >. Notaremos así que se ejecuta de forma atómica.

**Ejemplo.** Por ejemplo, ante el siguiente código concurrente:

```
1  begin
    x := 0;
    cobegin
        x := x+1;
5  x := x-1;
    coend
end
```

El resultado obtenido en la variable  $x$  es indeterminado, ya que puede ser 1,  $-1$  o 0:

- El segundo proceso puede leer la variable  $x$  antes de que el primero escriba en ella, leyendo 0; y podría escribir en ella después de que lo haga el primer proceso, escribiendo finalmente un  $-1$ .
- Podría ejecutarse el primer proceso antes que el segundo, dejando la variable  $x$  a 1 y el segundo le cambiaría el valor a 0.
- El primer proceso puede leer la variable  $x$  antes de que el segundo escriba en ella, leyendo 0; y podría escribir en ella después de que lo haga el segundo proceso, escribiendo finalmente un 1.

Notemos que esto sucede ya que la instrucción  $x := x \text{ OP } a$  es una instrucción compuesta de las instrucciones máquina: `LOAD  $x$ , OP  $a$ ,  $x$`  y `STORE  $x$` .

Sin embargo, ante el siguiente código concurrente:

```

1  begin
    x := 0;
    cobegin
        < x := x+1 >;
5    < x := x-1 >;
    coend
end

```

Obtenemos siempre 0 en  $x$ , ya que las instrucciones de cada instrucción compuesta no se entrelazan, al ser secciones críticas.

## Paradigma del Productor Consumidor

El paradigma del productor/consumidor es una situación de dos procesos que cooperan, uno escribiendo datos en una variable, al que llamaremos productor; y otro que leerá dicha variable y realizará cálculos con ella, al que llamaremos consumidor.

Este paradigma nos sirve de ejemplo para justificar las condiciones de sincronización, así como para ponerlas en práctica.

Son necesarias condiciones de sincronización ya que no todas las trazas de ejecución de un programa con estructura productor/consumidor son correctas.

**Ejemplo.** Si notamos por  $L$  a las lecturas del consumidor y por  $E$  a las escrituras del productor, las tres siguientes trazas de ejecución no son correctas:

1.  $L, E, L, E, \dots$ , porque leemos una lectura de la variable antes de que el productor escriba en ella, leyendo un valor indeterminado y pudiendo provocar el fallo del programa.
2.  $E, L, E, E, L, \dots$ , porque el consumidor se ha perdido una escritura del productor en la variable, que puede hacer que cambie la salida del programa a una errónea.
3.  $E, L, L, E, L, \dots$ , porque el consumidor ha usado un mismo dato dos veces, que también puede resultar en un mal funcionamiento del programa.

Para que el paradigma del productor/consumidor funcione correctamente, han de cumplirse las dos condiciones de sincronización siguientes:

1. El consumidor no puede leer la variable hasta que el productor haya escrito en ella. Cuando el consumidor lee, debe esperar a que el productor proporcione un nuevo dato antes de volver a leer.
2. El productor no puede escribir un nuevo valor hasta que el consumidor haya leído el último dato escrito (salvo en el primer valor a escribir).

Para cumplir con las condiciones de sincronización, deberemos añadir instrucciones en el código para que:

- El consumidor se detenga la primera vez hasta que el productor escriba en la variable.
- Se impida un segundo ciclo del consumidor hasta que se produzca el siguiente dato.
- Se impida un segundo ciclo del productor hasta que el dato anterior no haya sido leído por el consumidor.

## 1.4. Propiedades de los sistemas concurrentes

Una propiedad de un sistema concurrente es un atributo que se cumple en toda la ejecución del sistema, mientras que el conjunto de todas sus ejecuciones (de todas las posibles trazas generadas en la ejecución) nos dan el comportamiento del sistema.

Cualquier propiedad de un sistema concurrente puede ser formulada como combinación de dos tipos de propiedades fundamentales:

- Propiedades de seguridad (*safety*): Una propiedad de este tipo afirma que hay un estado del programa que es inalcanzable.
- Propiedades de vivacidad (*liveness*): Propiedades que afirman que en algún momento se alcanzará un estado deseado.

### 1.4.1. Propiedades de seguridad (*safety*)

Estas propiedades expresan determinadas condiciones que han de cumplirse durante toda la ejecución del programa. Cualquier propiedad que pueda ser formulada por la existencia de un estado inalcanzable, es una propiedad de seguridad. En dicho caso, deberíamos poder definir qué estado es inalcanzable y demostrar que el programa concurrente nunca puede llegar a dicho estado.

Las propiedades de seguridad pueden ya comprobarse en tiempo de compilación, ya que se cumplen independientemente de la ejecución concreta que sigue el sistema en tiempo de ejecución. Es por esto que se trata de una propiedad estática.

Ejemplos de problemas donde vemos propiedades de seguridad son:

- El problema de la exclusión mutua: La condición de que dos procesos del programa no puedan ejecutar simultáneamente las instrucciones de una sección crítica es de seguridad.
- Problema del productor/consumidor: Todos los estados que lleven a una traza distinta de E, L, E, L, ... son estados prohibidos.
- La situación de interbloqueo: Es una de las situaciones más críticas que se dan tras quebrantar una propiedad de seguridad, ya que hay procesos ocupando recursos que no están usando y que no liberarán.

#### 1.4.2. Propiedades de vivacidad (*liveness*)

Las propiedades de vivacidad expresan que el sistema llegará en un futuro a cumplir determinadas condiciones (en un tiempo no indeterminado). En determinados ejemplos, dichas propiedades pueden entenderse como que las condiciones dinámicas de ejecución no lleven a que determinados procesos sean sistemáticamente adelantados por otros, no pudiendo avanzar en la ejecución de instrucciones útiles, de forma que el proceso sufra inanición (*starvation*).

Para demostrar que una propiedad es de vivacidad, debemos definir un “buen estado” del programa, y demostrar que es alcanzable para todos los procesos en un determinado tiempo.

Ejemplos de problemas donde vemos propiedades de vivacidad son:

- El problema de la exclusión mutua: Las secciones críticas se ejecutan por un proceso a vez. El sistema debe garantizar que, en la espera por entrar a una región crítica, no ocurra que un proceso sea siempre adelantado por otros procesos, llevando a que dicho proceso nunca ejecute la región crítica (que es nuestro estado deseado).
- El problema del productor/consumidor: Un proceso que quiera escribir o leer de la variable compartida ha de poder hacerlo en un tiempo finito.

Debemos notar que el axioma de proceso finito expuesto en secciones anteriores no tiene nada que ver con la ausencia de inanición:

- El axioma de proceso finito afirma que los procesos no pueden quedarse parados arbitrariamente, sino que estos deben intentar ejecutar instrucciones conforme les sea posible.
- Un proceso puede estar ejecutando instrucciones en un bucle indefinido pero no avanzar en la ejecución de las instrucciones de su código (es decir, puede estar realizando un trabajo inútil). En este caso, se cumpliría el axioma del proceso finito pero no se cumpliría la propiedad de vivacidad, ya que el proceso sufriría inanición.

Como ya venimos avisando, el no cumplimiento de la propiedad de vivacidad puede llevar a uno o más procesos a un estado de inanición (es indefinidamente pospuesto por otros, de forma que no pueda realizar aquello para lo que está programado). Aunque dicha situación es menos grave que una situación de interbloqueo

(ya que hace que el programa no avance nada), tenemos procesos inoperantes (que no realizan su trabajo), por lo que consideraríamos que el programa concurrente no es correcto.

De esta forma, un programa concurrente solo podrá ser completamente correcto cuando se demuestre que los procesos que lo integran no sufren inanición en ninguna de sus posibles ejecuciones.

**Ejemplo** (Cena de filósofos). Disponemos de cinco filósofos,  $F_0$ ,  $F_1$ ,  $F_2$ ,  $F_3$  y  $F_4$ , que dedican su vida a pensar y en algún momento desean comer. Acceden a una mesa redonda en la que hay un plato del que todos pueden comer, siempre y cuando dispongan de dos palillos. Sólo hay 5 palillos, estos distribuidos de forma que entre dos filósofos hay un palillo.

Los filósofos son cabezotas, por lo que una vez congen un palillo, no están dispuestos a soltarlo. Además, no pueden arrebatarse un palillo a otro filósofo por ir en contra de sus ideales morales.

Ante la situación descrita, podemos llegar a ver los dos ejemplos siguientes:

- Si todos los filósofos cogen a la vez el palillo de su derecha, cada filósofo dispondrá de un palillo y no habrá más palillos libres.

Estamos ante una situación de interbloqueo: ningún filósofo puede comer y no podrá hacerlo jamás. Como resultado, todos los filósofos se morirán de hambre.

- Si, por ejemplo, los filósofos  $F_0$  y  $F_2$  (que rodean al filósofo  $F_1$  en la mesa) conspiran para dejar morir de hambre al filósofo  $F_1$  de forma que cuando  $F_0$  deje el palillo que hay entre  $F_0$  y  $F_1$ ,  $F_2$  coja el palillo que hay entre él y  $F_1$  (y viceversa), conseguirán que  $F_1$  nunca consiga sus dos palillos, llevando al filósofo a un estado de inanición y, posteriormente, la muerte.

Esta asignatura trata de crear protocolos que podamos demostrar que cumplen con las propiedades de seguridad y vivacidad, con el fin de no llevar nunca a situaciones de interbloqueos, inanición de algún(os) proceso(s), o alguna de las malas situaciones comentadas anteriormente.

## 1.5. Lógica de programas de Hoare y verificación de programas concurrentes

### 1.5.1. Corrección de los programas concurrentes

En los programas secuenciales, para comprobar la corrección total de los mismos, debemos probar que el programa **termina** dando **salidas esperadas** ante determinadas entradas.

Diremos que un programa secuencial es *parcialmente correcto* si, supuesto que este termine, entonces los resultados que obtiene tras ejecutarse son esperados.

En un programa secuencial, hay un único conjunto de datos de entrada que provoca un único conjunto de datos de salida. Esto no sucede en programas concurrentes, ya que el indeterminismo en la ejecución provoca distintas trazas posibles



del programa, y es bastante probable que todas las trazas posibles no provoquen los mismos resultados.

Para extender la definición de programa correcto a los programas concurrentes, notemos primero que muchos de ellos están pensado para no terminar nunca, de forma que su fin esté relacionado con alguna situación de error. Los sistemas operativos o los cajeros automáticos son programas concurrentes que están pensados para que nunca terminen, por lo que no podemos decir que una condición necesaria para que un programa concurrente sea correcto es que termine.

Para llevar a cabo la verificación de software, es decir, la demostración de que un programa es correcto, podemos emplear diferentes métodos:

**Depuración de código.** Explorar algunas ejecuciones de un código y comprobar que dichas ejecuciones son aceptables porque se cumplen las propiedades previamente fijadas.

Este método sirve para programas secuenciales, pero no para programas paralelos, ya que nos es imposible depurar un código ante todas las posibles combinaciones de distintas trazas de ejecución.

**Razonamiento operacional.** Realizar un análisis de casos exhaustivo para explorar todas las posibilidades de secuencias de ejecución de un código con el fin de garantizar que todas son correctas.

Es un método inviable para programas concurrentes. Por ejemplo, en un programa que use dos procesos, cada uno con 3 instrucciones atómicas, el número de posibles trazas de ejecución es de 20.

**Razonamiento asertivo.** Realizar un análisis abstracto basado en Lógica Matemática que permita representar de forma abstracta los estados<sup>1</sup> concretos que un programa alcanza.

De esta forma, el único enfoque posible es el razonamiento asertivo.

## 1.5.2. Introducción a la Lógica de Hoare

### Axiomática del lenguaje

Construiremos ahora un sistema lógico formal (SLF) que facilite la elaboración de asertos o proposiciones lógicas ciertas con una base lógico-matemática precisa.

Nuestro SLF estará formado por:

- Símbolos: Como sentencias del lenguaje de programación, variables proposicionales, operadores, ...
- Fórmulas: Secuencias de símbolos bien formadas<sup>2</sup>.

<sup>1</sup>Un estado del programa viene definido por los valores que tienen las variables del programa en determinado instante durante su ejecución.

<sup>2</sup>Entendemos por esto a sucesiones de símbolos con un significado fácilmente entendible.

- Axiomas: Propositiones que mediante un consenso se consideran verdaderas.
- Reglas de inferencia o de derivación: Reglas que nos permiten derivar fórmulas ciertas a partir de axiomas o de fórmulas que ya conocemos que son ciertas.

Podemos pensar en las reglas de inferencia como teoremas matemáticos: tienen unas hipótesis y unas tesis de forma que, en cualquier situación que las hipótesis sean ciertas, las tesis lo serán.

**Notación.** Notaremos a las reglas de inferencia por:

$$(\text{nombre de la regla}) \frac{H_1, H_2, \dots, H_n}{C}$$

De forma que disponemos de  $n$  hipótesis  $(H_1, H_2, \dots, H_n)$  en conjunción que nos llevan a la tesis  $C$ .

Para proseguir con el detallamiento del SLF, es necesario antes la definición de interpretación:

**Definición 1.1** (Interpretación). Sea  $A$  el conjunto de todos los asertos o fórmulas lógicas, una interpretación será una aplicación de dominio  $A$  y codominio el conjunto  $\{V, F\}$ <sup>3</sup>.

De esta forma, dada una interpretación y un aserto  $v$ , podemos ver la veracidad o falsedad de  $v$  gracias a la interpretación.

Para que las demostraciones de nuestro SLF sean confiables, este sistema debe ser seguro y completo. Fijada una interpretación:

- Decimos que un sistema es seguro si todos los asertos son hechos ciertos.
- Decimos que un sistema es completo si todos los hechos ciertos son asertos.

A partir de ahora, supondremos que no hay diferencia entre asertos y hechos ciertos. Es decir, que nuestro sistema es seguro y completo.

## Lógica proposicional

Las fórmulas del SLF que estamos construyendo se llaman proposiciones, y están formadas por:

- Constantes proposicionales  $\{V, F\}$ .
- Variables proposicionales  $\{p, q, r, \dots\}$ .
- Operadores lógicos  $\{\neg, \wedge, \vee, \rightarrow, \leftarrow, \longleftrightarrow\}$ .
- Expresiones formadas por constantes, variables y operadores.

---

<sup>3</sup>Cuyos elementos interpretamos como verdadero y falso.

Al igual que sucedía en la asignatura de Lógica y Métodos Discretos, podemos extender la definición de las interpretaciones y aplicarlas sobre las proposiciones del lenguaje, mediante unas reglas ya conocidas.

De esta forma, diremos que:

- Una fórmula es satisfacible si existe alguna interpretación que la satisfaga.
- Una fórmula será válida si se satisface en cualquier estado del programa (es decir, si cualquier interpretación la satisface). Las llamaremos tautologías.

Dentro de la lógica proposicional de este SLF son tautologías algunas fórmulas ya conocidas, como la distributiva de  $\wedge$  y de  $\vee$  o la conmutatividad de las mismas, por ejemplo.

**Definición 1.2.** Dadas dos fórmulas  $P$  y  $Q$ , diremos que son equivalentes siempre y cuando que  $P$  se satisfaga para una cierta interpretación si y solo si  $Q$  se satisface para la misma interpretación.

Por ejemplo,  $p \rightarrow q$  y  $\neg q \rightarrow \neg p$  son fórmulas equivalentes.

### Lógica de programas

Este SLF trata de hacer afirmaciones sobre la ejecución de un programa. Incluimos por tanto a los triples, que tienen la forma

$$\{P\}S\{Q\}$$

donde  $P$  y  $Q$  son asertos (llamados precondition y poscondition, respectivamente) y  $S$  es una sentencia simple o estructurada de un lenguaje de programación. En  $P$  y  $Q$  podrán aparecer tanto variables lógico-matemáticas como variables del propio programa. Para distinguirlas, notaremos a las primeras con letras mayúsculas y a las segundas con minúsculas.

Un triple  $\{P\} S \{Q\}$  se interpreta como cierto si  $S$  es ejecutado en un estado del programa que satisface  $P$  y, si la ejecución de  $S$  termina, el estado en el que  $S$  termina satisface  $Q$ , independientemente de los efectos producidos por los entrelazamientos de instrucciones atómicas de  $S$ .

Notemos que de esta forma el triple  $\{V\} \text{ while true do begin end } \{F\}$  es siempre cierto, ya que  $S$  se ejecuta en un estado del programa que satisface  $P$  y  $S$  nunca termina.

**Notación.** A partir de la notación de los triples, y siendo  $P$  una fórmula del lenguaje, notaremos por

$$\{P\}$$

Al conjunto de los estados del programa que verifican  $P$ .

De esta forma,  $\{V\}$  es el conjunto de todos los estados de un programa, ya que todos los estados de dicho programa verifican  $V$ . Análogamente,  $\{F\}$  se corresponde con el conjunto vacío.

**Notación.** Dadas  $P$  y  $Q$  asertos equivalentes, entonces obtenemos el mismo conjunto de estados del programa que verifican dichos asertos:

$$\{P\} = \{Q\}$$

Sin embargo, para evitar la confusión con el operador de asignación, notaremos las igualdades entre los conjuntos de estados de un programa con el operador  $\equiv$ .

*Observación.* Notemos que, dados cualesquiera asertos  $\{P\}$  y  $\{Q\}$ , podemos pensar en:

- $\{P \wedge Q\}$  como en  $\{P\} \cap \{Q\}$ .
- $\{P \vee Q\}$  como en  $\{P\} \cup \{Q\}$ .
- $\{P\} \rightarrow \{Q\}$  como en  $\{P\} \subseteq \{Q\}$

De esta forma, notemos que siempre se verifica que:

- $\{V \wedge P\} = \{P\}$ .
- $\{V \vee P\} = \{V\}$ .
- $\{F \wedge P\} = \{F\}$ .
- $\{F \vee P\} = \{P\}$ .
- $\{F\} \rightarrow \{P\} \rightarrow \{V\}$ .
- $\{P \wedge Q\} \rightarrow \{P\} \rightarrow \{P \vee Q\}$ .

**Definición 1.3** (Sustitución textual). Dado un aserto  $P$ , que contiene al menos una aparición libre de la variable  $x$ , y una expresión  $e$ , definimos la sustitución textual de  $x$  por  $e$ , notado por  $P_e^x$ , como la sustitución textual de todas las ocurrencias libres de  $x$  en  $P$  por  $e$ .

Enumeramos ahora los axiomas de nuestra Lógica de programas:

**Axioma de la sentencia nula**  $\{P\} \text{ null } \{P\}$ .

Es decir, si el aserto  $P$  es cierto antes de la ejecución de la sentencia nula (esta es, la que no cambia nada en el programa),  $P$  seguirá siendo cierto tras la ejecución de la misma.

**Axioma de asignación**  $\{P_e^x\} x = e \{P\}$ .

Es decir, la asignación de un determinado valor  $e$  a una variable  $x$  solo cambia en el programa el valor de dicha variable  $x$ .

**Ejemplo.** Un ejemplo de uso del axioma de asignación es el siguiente:

Tratamos de probar que el triple  $\{V\} x = 5 \{x = 5\}$  es cierto. Es decir, que desde cualquier estado del programa, si asignamos 5 a  $x$ , acabaremos en cualquier estado del programa en el que  $x$  valga 5.

*Demostración.* Sea  $P$  la fórmula dada por  $x = 5$  y  $e$  el valor numérico 5, sabemos que el axioma de asignación es cierto, luego se cumplirá que:

$$\{P_e^x\} x = e \{P\}$$

de donde:

$$\{V\} \equiv \{5 = 5\} x = e \{x = 5\}$$

□

Seguidamente, para cada una de las sentencias que afectan al flujo de control en un programa secuencial, contamos con reglas de inferencia para poder formar triples correctos en las demostraciones; además de dos reglas básicas de consecuencia.

**Regla de la consecuencia (1).**

$$\frac{\{P\}S\{Q\}, \{Q\} \rightarrow \{R\}}{\{P\}S\{R\}}$$

Es decir, siempre podemos hacer más débil la poscondición de un triple, de forma que este siga siendo cierto.

**Regla de la consecuencia (2).**

$$\frac{\{R\} \rightarrow \{P\}, \{P\}S\{Q\}}{\{R\}S\{Q\}}$$

Es decir, siempre podemos hacer más fuerte la precondition de un triple, manteniendo su veracidad.

**Regla de la composición.**

$$\frac{\{P\}S_1\{Q\}, \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}$$

Es decir, podemos condensar dos triples en uno, siempre y cuando la poscondición de uno sea la precondition del otro.

**Regla del *if*.**

$$\frac{\{P \wedge B\}S_1\{Q\}, \{P \wedge \neg B\}S_2\{Q\}}{\{P\} \text{ if } B \text{ then } S_1 \text{ else } S_2 \{Q\}}$$

De esta forma, siempre que queramos probar que una tripleta de la forma

$$\{P\} \text{ if } X \text{ then } S_1 \text{ else } S_2 \{Q\}$$

es cierta, tendremos que probar que las tripletas

$$\{P \wedge X\}S_1\{Q\} \quad \{P \wedge \neg X\}S_2\{Q\}$$

son ciertas.

**Regla de la iteración.** Suponiendo que una sentencia **while** puede iterar un número arbitrario de veces (incluso 0), tenemos que:

$$\frac{\{I \wedge B\}S\{I\}}{\{I\} \text{ while } B \text{ do } S \text{ end do } \{I \wedge \neg B\}}$$

Donde a la proposición  $I$  la llamaremos invariante.

### 1.5.3. Verificación de sentencias concurrentes

Sabemos ya hacer demostraciones para verificar la corrección de programas secuenciales. Será de nuestro interés ahora permitir la ejecución concurrente de dichos flujos de ejecución secuenciales, con el objetivo de probar la corrección de un programa concurrente.

Si entendemos la ejecución de un programa concurrente como un entrelazamiento de las instrucciones atómicas ejecutadas por los procesos del programa, entonces hemos de tener en cuenta para la demostración de corrección que no todas las secuencias de entrelazamiento resultan ser aceptables. Para poder programar correctamente, usamos sentencias de sincronización, tales como:

- Secciones críticas en el código para evitar condiciones de carrera.
- Sincronización con una condición (hacer que un proceso espere hasta que se dé una determinada condición en el estado del programa).

Usando estas operaciones, conseguiremos hacer correctos nuestros programas concurrentes (que es de lo que trata la asignatura), para luego demostrar matemáticamente que, efectivamente, dichos programas son correctos.

Dados varios triples de Hoare que representan secciones de programas secuenciales de los que hemos probado su corrección parcial, tratamos ahora de introducir estas secciones de programa en un programa concurrente.

Sin embargo, puede suceder que un proceso ejecute una instrucción atómica de su región de código que haga falsa la precondition o la poscondición de una sentencia que esté siendo simultáneamente ejecutada por otro proceso, invalidando su corrección.

**Ejemplo.** Por ejemplo, tenemos los dos siguientes triples:

$$\begin{aligned} &\{x = 0\} \ x = x + 2 \ \{x = 2\} \\ &\{V\} \ x = 0 \ \{x = 0\} \end{aligned}$$

cuya corrección puede comprobarse fácilmente usando el axioma de asignación.

Ahora, nos disponemos a ejecutar el siguiente código concurrente:

```
1 x = 0;
  cobegin
    <x = x + 2;> || <x = 0;>
  coend
```

donde podemos ver que la ejecución de una instrucción *interfiere* con la poscondición de la otra instrucción:

- La poscondición  $\{x = 0\}$  de la instrucción de la derecha no se cumple tras la ejecución de  $\langle x = x + 2; \rangle$  (en caso de que esta se ejecute después).
- La poscondición  $\{x = 2\}$  de la instrucción de la izquierda no se cumple tras la ejecución de  $\langle x = 0; \rangle$  (en caso de que esta se ejecute después).

- Notemos que la ejecución de una instrucción no *interfiere* con la precondition de la otra.

La ejecución de una instrucción hace falsa la poscondición de la otra, invalidando la demostración que hicimos del trozo de programa secuencial y, por tanto, del programa concurrente.

Sin embargo, podemos hacer un cambio en los triples iniciales para no tener este problema: usando la primera regla de la consecuencia, podemos relajar las poscondiciones de ambos triples:

$$\begin{aligned} \{x = 0\} \quad x = x + 2 \quad \{x = 0 \vee x = 2\} \\ \{V\} \quad x = 0 \quad \{x = 0 \vee x = 2\} \end{aligned}$$

haciendo que estos sigan siendo correctos. Si ahora tratamos de ejecutar de forma concurrente estas dos instrucciones, observamos que independientemente de la traza de ejecución, la ejecución de una instrucción no hace falsas las pre o poscondición de la otra.

Antes de proceder a la formalización del concepto de interferencia, hemos de comentar ciertos detalles:

- Una acción atómica elemental o sección crítica realiza una transformación indivisible del estado del programa, de forma que cualquier estado intermedio que pudiera existir no sería visible para el resto de los procesos.

En los programas concurrentes, puede suceder que las asignaciones no sean atómicas, por estar típicamente implementadas por varias instrucciones máquina:

```
1 y = 0; z = 0;
  cobegin
    x = y + z; || y = 1; z = 2
  coend
```

El programa superior puede dar como resultados esperados de  $x$  0, 1, 3 (como el lector habrá podido adivinar) y 2. Este último valor sería resultado de haber leído en la instrucción de la izquierda el valor de  $y$ , la ejecución de las dos instrucciones de la derecha, y finalmente añadir  $z$  al valor leído, guardándolo en  $x$ .

Se trata de un ejemplo curioso, ya que  $z + y = 2$  no se corresponde con ningún estado del programa. Esta situación puede resolverse con el uso de secciones críticas, ya que en este caso lo que falla es el programa concurrente, que está mal programado.

- Una expresión que no hace referencia a ninguna variable modificada por otro proceso será evaluada de forma atómica, ya que ninguno de los valores de la variable puede ser modificada mientras la expresión resulta evaluada.

De esta forma, si consideramos el siguiente programa concurrente en el que los procesos se encuentran usando variables disjuntas:

```

1  x = 0; y = 0;
   cobegin x = x + 1; || y = y + 1; coend

```

La ejecución de una instrucción no tiene nada que ver con la ejecución de la otra.

## Interferencia

Dado un triple  $\{P\}S\{Q\}$ , este puede contener varios asertos:  $\{P\}$ ,  $\{Q\}$  y cualquiera que sirva como pre y poscondición entre las acciones atómicas incluidas en la sección de código  $S$ .

**Ejemplo.** De esta forma, el triple

$$\{V\} \ x = 0; \ x = x + 1; \ \{x = 1\}$$

contiene los asertos  $\{V\}$ ,  $\{x = 0\}$  y  $\{x = 1\}$ . Sin embargo, el triple

$$\{V\} \ < x = 0; \ x = x + 1; > \ \{x = 1\}$$

contiene los asertos  $\{V\}$  y  $\{x = 1\}$ , ya que la ejecución de las dos instrucciones se hace de forma atómica y ningún otro proceso puede ver el estado intermedio ( $x = 0$ ) de la variable  $x$ , ya que como hemos mencionado en el primer punto, las regiones críticas realizan una transformación **indivisible** del estado del programa.

**Definición 1.4** (Interferencia). Dado un triple  $\{P\}S\{Q\}$  y una sentencia atómica  $a^4$  con precondition  $pre(a)$ , decimos que  $a$  no interfiere con  $\{P\}S\{Q\}$  si para todo aserto  $A$  del triple se cumple el triple

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

Es decir, si el aserto  $A$  es invariante para la sentencia  $a$ .

*Observación.* Notemos que, en la definición anterior, hemos empleado el símbolo  $\equiv$  para denotar la igualdad entre dos triples. Este abuso de la notación será no obstante fácil de distinguir en el contexto.

**Definición 1.5.** Dados  $n$  triples  $\{P_i\}S_i\{Q_i\}$ , decimos que están libres de interferencia si  $S_i$  no interfiere con  $\{P_j\}S_j\{Q_j\}$ , para cada par  $(i, j)$  con  $i \neq j$ .

La falta de interferencia significa que la ejecución atómica de pasos de un proceso del programa nunca falsifica los asertos usados en las demostraciones individuales de los otros procesos.

Esto es de especial relevancia en los programas concurrentes, ya que para demostrar su corrección, primero hemos de demostrar que la ejecución secuencial de cada proceso es correcta (en caso de no serlo, directamente el programa concurrente no es correcto), para luego demostrar que la ejecución de un proceso no interfiere con otro, para así garantizar que, aunque tengamos varios procesos ejecutándose

<sup>4</sup>Esta puede contener tantas líneas de código como queramos, lo importante es que su ejecución se haga de forma atómica.



de forma concurrente, como no interfieren entre sí, no se modifica la corrección del programa.

Veremos próximamente que con garantizar la corrección secuencial de los procesos y la no interferencia entre los mismos, nos es suficiente para garantizar la corrección de los programas concurrentes, gracias a este razonamiento intuitivo que acabamos de realizar (lo único que cambia al ejecutar los procesos de forma concurrente es que puedan modificar variables de otros procesos, interfiriendo en su ejecución, sin embargo, si no interfieren en la misma, todo saldrá bien).

**Ejemplo.** Recuperando el ejemplo del inicio de la sección, nos disponemos a demostrar que los triples  $\{x = 0\} \ x = x + 2 \ \{x = 0 \vee x = 2\}$ ,  $\{V\} \ x = 0 \ \{x = 0 \vee x = 2\}$  están libres de interferencia. Para ello, hemos de demostrar  $2 \cdot 2 = 4$  triples (ya que tenemos dos instrucciones, cada una con 2 asertos):

$$\begin{aligned} NI(x = 0, \ x = 0) &\equiv \{x = 0 \wedge V\} \ x = 0 \ \{x = 0\} \\ NI(x = 0 \vee x = 2, \ x = 0) &\equiv \{(x = 0 \vee x = 2) \wedge V\} \ x = 0 \ \{x = 0 \vee x = 2\} \\ NI(V, \ x = x + 2) &\equiv \{V \wedge x = 0\} \ x = x + 2 \ \{V\} \\ NI(x = 0 \vee x = 2, \ x = x + 2) &\equiv \{(x = 0 \vee x = 2) \wedge x = 0\} \ x = x + 2 \ \{x = 0 \vee x = 2\} \end{aligned}$$

1. Para el primer triple:

$$\{x = 0 \wedge V\} \ x = 0 \ \{x = 0\}$$

Tenemos que  $\{x = 0 \wedge V\} \equiv \{x = 0\}$ , por lo que basta con probar:

$$\{x = 0\} \ x = 0 \ \{x = 0\}$$

Usando el axioma de asignación:

$$\{V\} \equiv \{0 = 0\} \equiv \{x = 0\}_0^x \ x = 0 \ \{x = 0\}$$

Y como  $\{x = 0\} \rightarrow \{V\}$ , usando la segunda regla de consecuencia, tenemos ya probado  $NI(x = 0, \ x = 0)$ .

2. Para el segundo triple

$$\{(x = 0 \vee x = 2) \wedge V\} \ x = 0 \ \{x = 0 \vee x = 2\}$$

Tenemos que  $\{(x = 0 \vee x = 2) \wedge V\} \equiv \{x = 0 \vee x = 2\}$ , por lo que basta con probar:

$$\{x = 0 \vee x = 2\} \ x = 0 \ \{x = 0 \vee x = 2\}$$

Usando el axioma de asignación:

$$\{V\} \equiv \{V \vee F\} \equiv \{0 = 0 \vee 0 = 2\} \equiv \{x = 0 \vee x = 2\}_0^x \ x = 0 \ \{x = 0 \vee x = 2\}$$

Y como  $\{x = 0 \vee x = 2\} \rightarrow \{V\}$ , tenemos el triple probado usando otra vez la segunda regla de la consecuencia.

3. Para el tercer triple:

$$\{V \wedge x = 0\} \ x = x + 2 \ \{V\}$$

Como  $\{V \wedge x = 0\} \equiv \{x = 0\}$ , probamos:

$$\{x = 0\} \ x = x + 2 \ \{V\}$$

Dado que el triple  $\{x = 0\} \ x = x + 2 \ \{x = 2\}$  es cierto (se comprueba trivialmente con el axioma de asignación) y como  $\{x = 2\} \rightarrow \{V\}$ , tenemos el triple probado usando la primera regla de la consecuencia.

4. Para el cuarto triple:

$$\{(x = 0 \vee x = 2) \wedge x = 0\} \ x = x + 2 \ \{x = 0 \vee x = 2\}$$

Como:

$$\{(x = 0 \vee x = 2) \wedge x = 0\} \equiv \{x = 0\}$$

Tenemos que probar:

$$\{x = 0\} \ x = x + 2 \ \{x = 0 \vee x = 2\}$$

Usando el axioma de asignación:

$$\{x = 0 \vee x = 2\}_{x+2}^x \ x = x + 2 \ \{x = 0 \vee x = 2\}$$

$$\{x = 0 \vee x = 2\}_{x+2}^x \equiv \{x + 2 = 0 \vee x + 2 = 2\} \equiv \{x = -2 \vee x = 0\}$$

Y como  $\{x = 0\} \rightarrow \{x = 0 \vee x = -2\}$ , lo tenemos demostrado usando la segunda regla de consecuencia.

A continuación, veremos una regla de inferencia relacionada con lo que explicamos tras la definición de interferencia, y es que nos es suficiente con demostrar la corrección secuencial de los procesos y la no interferencia entre los mismos para poder garantizar la corrección de un programa concurrente.

Un programa concurrente pueden entenderse como la ejecución secuencial de estructuras **cobegin-coend**, por lo que será suficiente con demostrar la corrección parcial de cada una de estas estructuras para luego demostrar la corrección parcial de todo el programa, que se reducirá a una demostración de un programa secuencial.

### Regla de la composición concurrente segura de procesos.

$$\frac{\{P_i\} \ S_i \ \{Q_i\} \text{ son triples libres de interferencia } 1 \leq i \leq n}{\{P_1 \wedge P_2 \wedge \dots \wedge P_n\} \ \text{cobegin} \ S_1 \ || \ S_2 \ || \ \dots \ || \ S_n \ \text{coend} \ \{Q_1 \wedge Q_2 \wedge \dots \wedge Q_n\}}$$

**Ejemplo.** Aplicamos ahora la regla de la composición concurrente al ejemplo que venimos manejando. Como hemos visto, los triples  $\{x = 0\} \ x = x + 2 \ \{x = 0 \vee x = 2\}$  y  $\{V\} \ x = 0 \ \{x = 0 \vee x = 2\}$  están libres de interferencia, por lo que podemos aplicar la regla de la composición concurrente, llegando a que el triple

$$\begin{aligned} & \{x = 0\} \\ & \text{cobegin} \ x = x + 2; \ || \ x = 0; \ \text{coend} \\ & \{x = 0 \vee x = 2\} \end{aligned}$$

es cierto.

**Ejemplo.** Ante el siguiente código:

```
1 x = 0; y = 0;
  cobegin x = y + 1; || y = x + 1; coend
```

Notemos que los posibles resultados de ejecución del mismo son (donde se ha notado por  $l(x)$  la lectura de la variable  $x$  y por  $e(x)$  a la escritura en la variable  $x$ , respectivamente con  $y$ ):

Traza	$x$	$y$	Traza	$x$	$y$	Traza	$x$	$y$
$l(x)$	0	0	$l(x)$	0	0	$l(y)$	0	0
$l(y)$	0	0	$e(y)$	0	1	$e(x)$	1	0
$e(x)$	1	0	$l(y)$	0	1	$l(x)$	1	0
$e(y)$	1	1	$e(x)$	2	1	$e(y)$	1	2

Vemos en la tabla que hay tres posibles resultados del programa:

1. Uno en el que primero se leen las variables y luego se modifican.
2. Otro en el que primero se modifica  $y$  y luego  $x$ .
3. Un último en el que primero se modifica  $x$  y luego  $y$ .

Vemos que al tener varios procesos que escriben y modifican varias variables, debemos distinguir varias casuísticas para luego determinar los posibles resultados del programa.

Sin embargo, ante el siguiente código:

```
1 x = 0; y = 0;
  z = x;
  cobegin x = y + 1; || y = z + 1; coend
```

obtenemos los siguientes posibles resultados:

Traza	$x$	$y$	Traza	$x$	$y$	Traza	$x$	$y$
$l(z)$	0	0	$l(z)$	0	0	$l(y)$	0	0
$l(y)$	0	0	$e(y)$	0	1	$e(x)$	1	0
$e(x)$	1	0	$l(y)$	0	1	$l(z)$	1	0
$e(y)$	1	1	$e(x)$	2	1	$e(y)$	1	1

Donde sólo hay una única variable compartida que es leída y escrita por un único proceso, el número de casos a tener en cuenta disminuye, ya que sólo debemos distinguir dos casos:

1. Al ejecutar el código de la izquierda, la variable  $y$  todavía no ha sido modificada.
2. Al ejecutar el código de la izquierda, la variable  $y$  ha sido modificada ya.

Esta propiedad de los programa recibe el nombre de **como máximo una vez**, donde solo encontramos una variable que es leída por varios procesos pero que solo es modificada por uno de ellos. De esta forma, el número de casuísticas disminuye considerablemente, ya que sólo hemos de distinguir el caso de que la variable haya sido modificada y el caso de que todavía no lo haya sido.

#### 1.5.4. Verificación usando invariantes globales

La demostración de verificación de programas concurrentes usando la regla de la composición concurrente es tediosa, ya que es necesario comprobar la veracidad de muchos triples antes de poder aplicarla. Es por tanto que buscamos otra forma predominante de probar los programas concurrentes.

Los invariantes globales (IG) de un programa pueden entenderse como expresiones definidas a partir de las variables globales de un programa. Estas suelen definirse como un predicado de la Lógica de Programas que captura la relación que existe entre las variables compartidas por los procesos de un programa concurrente.

Si cualquier aserto  $\{C\}$  de un triple  $\{P_i\} S_i \{Q_i\}$  se puede escribir como una conjunción del tipo  $\{IG \wedge L\}$  donde  $IG$  es un invariante global del programa y  $\{L\}$  es un predicado en el que intervienen solo variables de un proceso o parámetros de una función, entonces las demostraciones de los procesos secuenciales estarán libres de interferencias.

De esta forma, para que un predicado  $\{I\}$  definido a partir de las variables compartidas entre los procesos pueda ser considerado un IG válido, se ha de cumplir que:

1. Sea cierto para los valores iniciales de las variables del programa que aparecen en  $\{I\}$ .
2. Se ha de poder demostrar la no interferencia de dicho aserto  $I$  con cualquier sentencia atómica de  $S_i$ , es decir, se ha de poder probar el triple

$$NI(I, a) \equiv \{I \wedge pre(a)\} a \{I\}$$

para toda  $a$  sentencia atómica de  $S_i$ .

**Ejemplo.** Si tenemos un programa que sigue el paradigma del productor/consumidor y queremos probar su corrección parcial (esto es, que el programa hace lo que esperamos), suponiendo que ya tenemos demostrada las correcciones parciales del productor y del consumidor, faltaría probar la no interferencia entre ambos. Para ello, y con el fin de evitar comprobar múltiples triples de Hoare, decidimos realizar la prueba mediante un invariante global, de foma que dicho invariante nos dé la corrección parcial de nuestro programa. Si conseguimos probar la invarianza de dicha propiedad, tendremos demostrada la corrección del programa.

Para la corrección parcial, queremos probar que el consumidor no lea una determinada variable  $x$  antes de que el productor no escriba en ella, y que el productor

espere a que el consumidor lea el valor anterior de  $x$  antes de modificarlo. Debemos buscar una forma de representar esto matemáticamente, para así definir  $I$  como la relación matemática que cumpla esto, y proceder a demostrar que  $I$  es un invariante global, para así tener la corrección de nuestro programa probado.

Una forma de hacerlo es contando el número de veces que se lee y escribe en la variable:

Sea  $n$  el número de veces que el productor ha producido y escrito un valor en  $x$  y  $m$  el número de veces que el consumidor ha leído el valor de  $x$ , debe cumplirse que consumidor no lea  $x$  más veces que el productor haya escrito en ella, es decir, que

$$m \leq n$$

Así mismo, el productor no puede escribir en  $x$  más veces de las que el consumidor haya leído  $x$ , sino que sólo puede hacerlo una vez que este lo haya hecho. Es decir, si  $m = n$ , entonces el productor podrá volver a escribir en  $x$ , por lo que tendremos que  $n = m + 1$ . Sin embargo, este no puede volver a escribir hasta que el consumidor haya leído la variable. De esta forma, limitamos al productor de generar más datos de las que el productor pueda consumir, con la expresión:

$$n \leq m + 1$$

En resumen, el buen funcionamiento del programa dependerá del invariante global:

$$I = m \leq n \leq m + 1$$

siendo  $m$  y  $n$  las variables anteriormente definidas.

Pasamos ahora a la demostración de la corrección de nuestro programa:

1. Primero, debemos comprobar que el invariante es cierto al inicio del programa.

Inicialmente, el productor no ha escrito todavía en  $x$ , al igual que el consumidor no ha leído todavía  $x$ , por lo que:

$$0 = m \leq n = 0 \leq m + 1 = 0 + 1$$

Y vemos que se verifica  $I$ .

2. Posteriormente, debemos dividir el programa en bloques de forma que debemos probar que antes y después de cada bloque el invariante sigue siendo válido. Los bloques que consideraremos estarán formados por una iteración del productor y por una del consumidor.

Suponiendo que al inicio de un bloque se verifica  $I$ , es decir, que  $m \leq n \leq m + 1$ , debemos probar que tras la escritura de  $x$  por el productor y tras la lectura de  $x$  por el consumidor se verifica  $m' \leq n' \leq m' + 1$ , siendo  $m'$  y  $n'$  el número actualizado de veces que se ha leído y escrito en la variable, respectivamente.

Para ello, suponemos que se verifica  $I$ . Como demostramos anteriormente la corrección parcial de cada programa (del productor y del consumidor), sabemos que tras un bloque (es decir, una iteración de cada uno de los dos

programas), el productor habrá generado un dato que el consumidor habrá leído (o que el consumidor habrá leído un dato y el productor habrá generado el siguiente). En cualquier traza de ejecución, tendremos que:

$$m' = m + 1 \quad n' = n + 1$$

Y ahora tendremos que comprobar que el invariante se sigue cumpliendo:

$$m \leq n \leq m + 1 \implies m + 1 \leq n + 1 \leq m + 2 \implies m' \leq n' \leq m' + 1$$

Notemos que hemos supuesto que se verificaba  $I$  al inicio del bloque. En principio nada nos garantiza esto, pero como anteriormente probamos que se cumplía al inicio del programa, se cumple antes de la primera ejecución del bloque, y como hemos demostrado que se cumple tras el bloque, se cumplirá antes de la segunda ejecución del bloque, ... Hemos realizado una especie de inducción en nuestro SLF.

Hemos demostrado ya que  $I$  es un invariante global. Como este nos garantiza la corrección de nuestro programa concurrente, tenemos ya demostrada la corrección del mismo.

## 2. Sincronización en memoria compartida. Monitores

Suponiendo que existe una memoria común para los distintos procesos que ejecutan un programa concurrente, este Capítulo trata sobre la sincronización de los mismos usando para ello instrucciones que usan dicha memoria compartida. Nos centraremos en el uso de los monitores, construcciones de alto nivel que nos ofrecen mayor libertad que los semáforos.

El concepto de semáforo se desarrolló previamente en el Seminario 1 de prácticas<sup>1</sup>. Los semáforos presentan dos grandes limitaciones:

1. Están basados en variables compartidas del programa, por lo que no fomentan la modularidad de los programas, impidiendo su reutilización.
2. Las operaciones de los semáforos (`sem_wait` y `sem_signal`) se encuentran dispersas a lo largo del código del programa concurrente. Además, estas instrucciones no solo afectan al bloque de código en el que se encuentran, sino a cualquier otro bloque que use el mismo semáforo.

En definitiva, los semáforos no son un buen mecanismo de programación concurrente, y además la verificación de programas que usan semáforos es muy complicada.

Era necesario encontrar un nuevo mecanismo de programación concurrente que permitiera la encapsulación de la información y de la sincronización entre procesos, así como programar las operaciones de sincronización (como `wait` o `signal`) dentro de bloques o procedimientos que se ejecuten con instrucciones atómicas, para que las instrucciones de sincronización no se encuentren desperdigadas por el programa. Fue Charles Antony Richard Hoare quien inventó los monitores, concepto en el que ahondaremos a lo largo de este Capítulo.

### 2.1. Definición de un monitor

La idea básica de monitor es un módulo que contiene un conjunto de variables a las que llamaremos *variables permanentes*<sup>2</sup>, de forma que dichas variables solo podrán ser alteradas dentro de los procedimientos del módulo monitor. Garantizaremos que la ejecución de cada uno de esos procedimientos se ejecute la mayor parte del tiempo como una única instrucción atómica, salvo que se produzca algo por lo

---

<sup>1</sup>Por lo que el lector debería estar familiarizado con ellos.

<sup>2</sup>A pesar de su nombre, no serán constantes, sino que podremos modificar su valor.

que interrumpir la ejecución del procedimiento.

Podemos pensar en un monitor como en un tipo de dato abstracto que define tipos y variables permanentes propias del monitor, así como un conjunto de procedimientos dentro de dicho módulo. No debemos pensar en los monitores como en una clase, ya que no pueden hacer lo mismo que ellas (no se pueden instanciar y tampoco existe polimorfismo o ligadura dinámica).

### **Ventajas**

A continuación, los programas concurrentes estarán formados tanto por procesos que se ejecutarán de forma concurrente, como por monitores, los cuales velarán por la sincronización y acceso a variables compartidas de dichos procesos, de forma que no se produzcan condiciones de carrera o comportamientos indeseados. Podremos modelar tantas relaciones de interacción entre los procesos de un programa concurrente como queramos. De esta forma, el uso de los monitores o de procedimientos asociados a monitores no restringen las posibilidades del modelado de un sistema concurrente.

Los procesos de un programa concurrente no tendrán que llamar a operaciones de sincronización, sino que llamarán a procedimientos del monitor, los cuales realizarán la funcionalidad deseada sobre las variables compartidas garantizando la sincronización entre los procesos.

Además, los monitores nos permiten una alta reusabilidad de código, ya que podremos reutilizar un monitor ya creado para resolver problemas similares. Sin embargo, la reutilización de código no es similar a la usada en programación orientada a objetos mediante instancias de una misma clase, sino que se hará por copias parametrizables: tendremos una definición de un monitor basada en parámetros, y cuando necesitemos usar un monitor, crearemos una copia de dicha definición parametrizándola (pasándole los parámetros que necesitemos para resolver nuestro problema). De esta forma, no es reutilización por instanciación, sino por *parametrización*.

Los procesos que usemos en los programas concurrentes no verán el acceso a las variables compartidas, sino que será realizado por los procedimientos del monitor, garantizando que se hacen como deben hacerse, evitando condiciones de carrera. De esta forma, los monitores garantizan la ocultación de las variables compartidas, haciéndolas transparentes a los procesos del sistema concurrente.

Finalmente, existen unos axiomas que nos permiten verificar los programas concurrentes que usen monitores de forma sencilla. Dichas demostraciones estarán basadas en el uso de los invariantes globales. Ahondaremos en la verificación de programas concurrentes que utilicen monitores más adelante.

#### **2.1.1. Concepto de monitor**

A modo de resumen para comenzar a definir lo que es un monitor, podemos decir que:



- Es un módulo con un conjunto de variables permanentes que solo pueden ser modificadas por los procedimientos del monitor.
- Cada uno de los procedimientos<sup>3</sup> de un monitor se ejecutan en exclusión mutua (garantizando el acceso a las variables compartidas sin condiciones de carrera). Sin embargo, estos no tienen por qué ejecutarse completamente, sino que pueden interrumpirse y en algún momento futuro seguir ejecutándose en exclusión mutua.
- La ejecución de los procedimientos de un monitor modifican el estado interno del mismo (esto es, el conjunto de las variables permanentes asociadas al monitor).
- El estado inicial del monitor (de sus variables permanentes) se establece mediante la ejecución de un procedimiento especial, al que llamaremos *código de inicialización*. Este se ejecuta tras la declaración de una variable de tipo monitor y da valores iniciales a las variables permanentes.

De esta forma, un monitor puede visualizarse como en la tabla 2.1, como un conjunto que engloba:

- Un conjunto de variables, llamadas *variables permanentes*, que no son accesibles desde fuera del monitor.
- Un conjunto de procedimientos que el monitor proporciona como servicio a los procesos de un programa concurrente (para por ejemplo, acceder a las variables permanentes que serán las variables que compartan dichos procesos), llamados *procedimientos exportados* o *exportables*.
- Un procedimiento especial llamado *código de inicialización*, que permite inicializar las variable permanentes.

Variables permanentes
Procedimientos exportados
Código de inicialización

Tabla 2.1: Esquema de un monitor.

**Ejemplo.** Aunque todavía no entendemos muy bien qué es un monitor, daremos a continuación un ejemplo de uso del mismo, para ilustrar la definición que queremos dar de monitor, pese a que algunas cosas del ejemplo no podamos entenderlas todavía y deberemos dejarlas para más adelante<sup>4</sup>.

<sup>3</sup>Podemos pensar en ellos como en los “métodos” de una clase, haciendo hincapié en que los monitores **no son** clases.

<sup>4</sup>Como el tipo de dato **cond**.

En este ejemplo, queremos solventar un problema mediante el paradigma productor/consumidor. Tendremos dos procesos, un productor y un consumidor, de forma que el productor escribirá en un buffer (o vector) que usaremos como cola cíclica (esto es, que si nos pasamos de la posición final, volvemos al inicio y con planificación FIFO), mientras que el consumidor irá leyendo los datos de dicho buffer. Siendo Buf una variable de tipo monitor que luego definiremos en este ejemplo, el código del productor y del consumidor será el siguiente (pensando en que tenemos que usar procedimientos del monitor para el acceso a las variables compartidas, en este caso el buffer):

```

1  Proceso Prod1::
    var d : tipo_dato;

    while true do begin
5     d = producir();
        Buf.insertar(d); {mete d en el buffer}
    end do

```

```

1  Proceso Cons1::
    var x : tipo_dato;

    while true do begin
5     Buf.retirar(x); {retira del buffer en x}
        consumir(x);
    end do

```

El código del monitor será el siguiente en pseudo-pascal (hemos omitido el código de inicialización):

```

1  Monitor Buf
    var
        -elementos_ocupados : int;
        -frente, atras: 0..N-1;
5     -no_vacio, no_lleno : cond;

        +insertar(d : tipo_dato);
        +retirar(var x : tipo_dato);

```

Donde vemos 5 variables permanentes: **elementos\_ocupados**, que mide la cantidad de posiciones ocupadas del buffer, **frente**, que marca la casilla en la que el productor insertará el próximo dato (por tanto, ha de estar siempre vacía), **atras**, que marca la casilla de la que leerá el consumidor, **no\_vacio** y **no\_lleno**, variables de tipo **cond**, las cuales aprenderemos lo que hacen más adelante.

Contamos además con dos procedimientos: **insertar**, que inserta un dato en el buffer en caso de que haya hueco (si no hay hueco, se bloquea hasta que el consumidor lea un dato y deje un hueco libre):

```

1  procedure insertar(d : tipo_dato) begin
    if((frente + 1) mod N = frente) then no_lleno.wait();
    introducir(buf, frente, d); {inserta d en la posición frente en el buffer}

```

```
5 elementos_ocupados += 1;  
frente = (frente + 1) mod N;  
no_vacio.signal();  
end
```

Y con el procedimiento `retir`, que retira un dato del buffer y lo devuelve como resultado del procedimiento, siempre que esto sea posible (es decir, si no hay ningún dato que leer en el buffer, se bloquea esperando a que el productor ponga algún dato):

```
1 procedure retirar(var x : tipo_dato) begin  
  if(frente = atras) then no_vacio.wait();  
  eliminar(buf, atras, x); {inserta buf[atras] en x y lo borra del buffer}  
  elementos_ocupados -= 1;  
5  atras = atras mod N + 1;  
  no_lleno.signal();  
end
```

Como hemos ya comentado mientras mostrábamos los pseudocódigos del ejemplo, hay que establecer condiciones que identifiquen las dos condiciones inseguras del ejemplo: que el buffer esté lleno o que el buffer esté vacío:

- Si `frente = atras`, entonces el último dato que se ha de consumir está en una casilla vacía en la que el productor escribirá. Se trata de la situación en la que el buffer está vacío. Debemos por tanto, evitar que el consumidor lea un dato del buffer.
- Si  $(frente + 1) \bmod N = atras$ , entonces el siguiente dato a introducir en el buffer está justo delante del dato a consumir. Se trata de la situación en la que el buffer está lleno. Debemos por tanto, evitar que el productor introduzca un dato en el buffer<sup>5</sup>.

Los procesos del programa llaman a los procedimientos del monitor, y no tienen acceso directo al buffer, por lo que no pueden saber cuándo este está lleno o vacío. De esta forma, lo que sucederá es que los procedimientos internos del monitor realizarán una sincronización interna mediante el uso de llamadas bloqueantes:

- Si el buffer está lleno y el productor se dispone a escribir un dato, quedará el proceso bloqueado hasta que un consumidor lea un dato. Este señalará (`signal`) al productor, desbloqueándolo.
- Si el buffer está vacío y el consumidor se dispone a leer un dato, quedará bloqueado el proceso que ejecute el procedimiento del monitor. Cuando el productor escriba un dato, enviará una señal al consumidor, desbloqueándolo.

Esta funcionalidad se consigue mediante las variables de tipo `cond`. Se verán a continuación, pero para entenderlas por ahora digamos que necesitamos tener una variable

---

<sup>5</sup>Definimos anteriormente que `frente` siempre apunta a una casilla vacía, por lo que como máximo el buffer tendrá ocupados  $N - 1$  elementos.

de tipo `cond` por cada razón por la que queremos bloquear un proceso<sup>6</sup>.

El código de los procedimientos es ejecutado por los propios procesos que ejecutan cada proceso (productor o consumidor, en este caso) del programa concurrente. Por tanto, si el productor ejecuta un procedimiento del monitor con un `wait`, dicho proceso se bloqueará y no podrá ejecutar código hasta desbloquearse.

Para que el código que hemos visto funcione adecuadamente, nos falta introducir un último concepto en los monitores, y es que mientras se ejecuta un procedimiento de un monitor, no se puede ejecutar ningún otro, sino que han de ejecutarse en **exclusión mutua**.

### 2.1.2. Características de programación con monitores

Una vez ilustrado el uso de la herramienta que estamos construyendo en este Capítulo mediante el ejemplo anterior, vamos ahora a introducir la noción de que sólo puede ejecutarse a la vez un único procedimiento de un monitor.

Como ya hemos visto, los procedimientos de los monitores no tienen por qué ejecutarse de principio a fin, sino que un proceso puede comenzar a ejecutar un procedimiento, bloquearse (dejando por tanto libre al monitor) y que otro proceso comience a ejecutar un procedimiento de dicho monitor, sucediéndose un entrelazamiento de las trazas de ejecución de los procedimientos.

Cuando un proceso se encuentra ejecutando un procedimiento del monitor, decimos que el monitor está *ocupado*. En caso contrario, diremos que este está *libre*. Notemos que si un proceso se bloquea mientras ejecuta un procedimiento del monitor, el monitor tiene que quedar libre, ya que si no no habría forma de volver a despertar a dicho proceso (tenemos que ejecutar un `signal` sobre la misma variable `cond` que bloqueó al proceso<sup>7</sup>). La situación de bloquear a un proceso y dejar que entre otro al monitor es delicada y debe hacerse con cuidado, para garantizar que sólo haya un único proceso ejecutando un procedimiento del monitor al mismo tiempo.

Los monitores son objetos *pasivos*. Esto es, no tienen una hebra dentro que ejecute su código, sino que simplemente proporciona código (sus procedimientos) a otros procesos para que sean ellos quien ejecuten el código del monitor.

Para implementar una librería con monitores en un lenguaje de programación base, este debe tener la propiedad de ser *reentrante*.

**Definición 2.1.** Un lenguaje de programación tiene la propiedad de ser reentrante si, siempre que tengamos un proceso ejecutando una función y este se bloquea, sea capaz de conservar la siguiente instrucción a ejecutar y el valor de sus variables

---

<sup>6</sup>En el caso de productor/consumidor, queremos bloquear un proceso si sucede alguno de los dos puntos superiores, condiciones inseguras, luego nos harán falta dos variables de tipo `cond`. En otros problemas, el número de variables de tipo `cond` podría ser otro.

<sup>7</sup>Se explicará más adelante.

locales tras desbloquearse. Es decir, el proceso no debe enterarse localmente de que nada haya cambiado mientras estaba bloqueado.

Notemos que debemos tener esta propiedad en el lenguaje de programación con el que trabajemos para poder hacer uso de funciones bloqueantes (como `wait`) dentro de los procedimientos de un monitor, algo básico en el funcionamiento de este. Afortunadamente, actualmente todos los lenguajes de programación que encontramos en el mercado son reentrantes.

### Instanciación de monitores

El siguiente ejemplo nos ilustra cómo funciona la instanciación de un monitor:

**Ejemplo.** Aunque los monitores están pensado para programas concurrentes (ya que no tiene sentido su uso en programas secuenciales), usaremos en este ejemplo un monitor en un programa secuencial, ya que sólo nos interesa la forma en la que los monitores se inicializan<sup>8</sup>.

Tenemos un programa en el que necesitamos dos variables, las cuales queremos consultar e incrementar mediante un incremento previamente fijado que no cambiará. Para ello, creamos un monitor de acceso a una variable, con parámetros de entrada, para luego poder crear dos copias parametrizadas del mismo. El código del monitor será algo parecido a:

```

1  class monitor VariableProtegida(inicio, incremento : integer);
    var x, inc : integer;

    procedure incremento();
5   begin
        x = x + inc;
    end

    procedure valor(var v : integer);
10  begin
        v = x;
    end

    begin
15  x = inicio; inc = incremento;
    end

```

De esta forma, podemos usar dos copias del monitor de la forma:

```

1  var mv1 : VariableProtegida(0,1);    {empieza en 0 e incrementa en 1}
    mv2 : VariableProtegida(10,4);    {empieza en 10 e incrementa en 4}
    a, b : integer;
    begin
5  mv1.incremento();    {+=1}

```

<sup>8</sup>Además, no hemos terminado de desarrollar cómo es que solo puede ejecutarse a la vez un único procedimiento del monitor, por lo que no entendemos hasta ahora cómo es que sirven para sincronizar programas concurrentes.

```

mv1.valor(a);      {a=1}
mv2.incremento();  {+=4}
mv2.valor(b);      {b=14}
end

```

### Exclusión mutua en los procedimientos de un monitor

Si tenemos varios procesos del programa concurrente que quieren hacer uso de procedimientos del monitor a la vez, sólo podremos dejar pasar a un proceso al monitor (suponiendo que este se encuentre libre). Para los otros procesos, almacenamos su llamada al procedimiento.

Para ello, todos los monitores tienen implementada una cola con planificación FIFO, llamada *cola de entrada al monitor*. Si tenemos dos procesos que quieren acceder a un procedimiento de un monitor libre, sólo podrá hacerlo un proceso. La llamada al procedimiento del monitor del otro proceso quedará almacenada en la cola de entrada al monitor, y este pasará a ejecutar el procedimiento deseado una vez el proceso anterior haya dejado libre el monitor.

En esta asignatura, supondremos que la cola de entrada al monitor es suficientemente larga como para albergar a todos los procesos que necesiten esperar a que el monitor quede libre.

Podemos representar la vida de un proceso de un programa concurrente que hace uso de monitores para sincronizar a sus procesos con el siguiente diagrama:

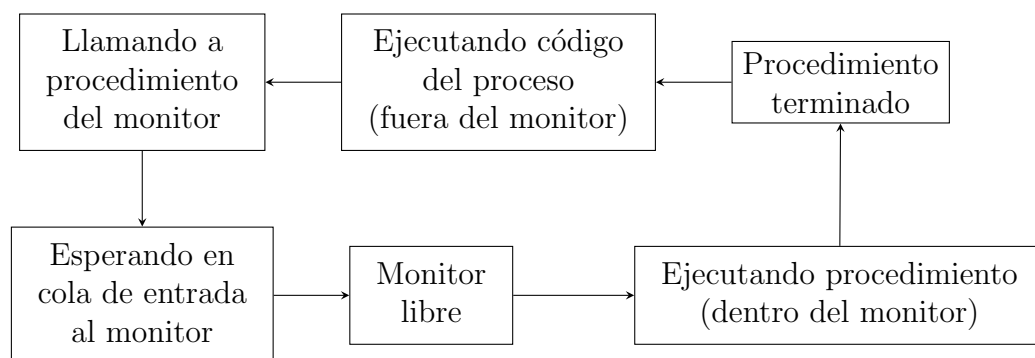


Figura 2.1: Vida de un proceso en un programa concurrente con monitores.

De esta forma, podemos ahora reescribir la descripción gráfica de monitor que hicimos en la tabla 2.1, incluyendo ahora la cola de entrada al monitor, tal y como vemos en la tabla 2.2

Cola del monitor
Variables permanentes
Procedimientos exportados
Código de inicialización

Tabla 2.2: Esquema de un monitor incluyendo la cola de entrada.

### 2.1.3. Operaciones de sincronización

Las operaciones de sincronización entre los procesos de un programa concurrente se programan, como ya hemos visto, dentro de los procedimientos del monitor. Son instrucciones que permiten detener la ejecución de un procedimiento de un monitor y bloquear en una cola al proceso que ha hecho la llamada del procedimiento del monitor. Tenemos para realizar esta acción dos operaciones principales: **wait** y **signal**.

Sin embargo, las operaciones **wait** y **signal** que manejamos en monitores no se parecen a las que usábamos en los semáforos:

- En los semáforos, la ejecución de **wait** ofrecía la posibilidad de bloquear al proceso, ya que no lo hacía si el entero de dentro del semáforo era mayor estricto que 0. Por contra, en monitores la llamada **wait** siempre será bloqueante.
- Las operaciones **wait** y **signal** eran relativas a un semáforo: hacía falta usar un semáforo por cada razón que tuviéramos dentro de un programa concurrente para bloquear a uno o varios procesos (en el caso del productor/consumidor, usar dos semáforos). Sin embargo, con un solo monitor podremos bloquear procesos por tantas razones como queramos, usando un nuevo tipo de dato.

#### Tipo de dato **cond**

En los monitores, para poder usar las operaciones de **wait** y **signal**, será necesario utilizar una variable de tipo de dato condición, o **cond**.

Las variables tipo **cond** sólo se encuentran junto con las variables permanentes de un monitor. Estas no se inicializan a ningún valor.

En nuestro monitor, tendremos varias razones por las que queremos bloquear a los procesos concurrentes de nuestro programa por alguna determinada razón hasta que se cumpla una condición determinada. Por ejemplo, en el problema del productor/consumidor:

- Queremos bloquear a cualquier productor que intente escribir si la estructura de datos intermedia que usamos está llena. Desbloquearemos a un proceso productor cuando se vacíe un hueco en dicha estructura.

- Además, queremos bloquear a cualquier consumidor que intente leer de la estructura de datos intermedia cuando esta esté vacía. Desbloquearemos a un consumidor cuando algún productor haya escrito algún dato.

Por cada razón o condición distinta por la que queramos bloquear a los procesos de un programa concurrente en relación a una misma variable compartida (para evitar estados inseguros), crearemos una variable de tipo **cond**. Es decir, una variable por cada una de las razones por las que queramos que esperen los procesos. En el ejemplo del productor/consumidor, son necesarias únicamente dos variables de tipo **cond**.

Las variables de tipo **cond** admiten 4 métodos (aunque sólo recomendamos usar los dos primeros):

**wait** Bloquea al proceso que ejecuta este método. Dicho proceso pasa a una cola asociada a la variable condición correspondiente con planificación FIFO.

**signal** En caso de haber algún proceso bloqueado en la cola asociada a la variable condición correspondiente, lo desbloquea. Si esta cola está vacía, es equivalente a una operación nula<sup>9</sup>.

**queue** Devuelve un booleano que indica (**true**) si la cola asociada a la variable condición contiene al menos un proceso bloqueado.

**signal\_all** Desbloquea de una sola vez a todos los procesos bloqueados en la cola asociada a la variable condición. El orden de dicha cola no se mantiene para realizar la petición de acceso al monitor, por lo que se produce competencia entre los procesos para entrar al monitor, incumpliendo la propiedad de equidad entre procesos. Depende de la semántica de las señales del lenguaje<sup>10</sup>. Se recomienda **no usarla**.

De esta forma, la representación gráfica final de un monitor es la que se muestra en la tabla 2.3:

Cola del monitor
Variables permanentes
Variables condición y colas de procesos bloqueados
Procedimientos exportados
Código de inicialización

Tabla 2.3: Esquema de un monitor incluyendo las variables condición.

<sup>9</sup>Esto es, equivalente a la instrucción ;.

<sup>10</sup>Se explicará más adelante qué es esto.



### Semántica desplazante

Como hemos comentado ya, los monitores solo permiten que un único proceso se encuentre ejecutando un procedimiento del mismo. En este caso, decíamos que el monitor está ocupado. En caso de que un proceso que estaba ejecutando el procedimiento ejecute un `wait` (o salga del procedimiento), hay que dejar el monitor libre para dejar pasar a otro. Se trata de un momento muy delicado, ya que se pueden producir condiciones de carrera entre los procesos que quieran conseguir el monitor. Esta situación la hemos solucionado ya con la cola de entrada al monitor, ya que con la planificación FIFO, solo podrá entrar un único proceso al monitor.

Si ahora el proceso nuevo que ejecuta el monitor ejecuta un `signal`, desbloqueará al anterior proceso de la cola de la variable condición correspondiente. Si en dicho momento este proceso sale del procedimiento, dejará el monitor abierto, por lo que podría suceder que un proceso de la cola de entrada al monitor entre antes que el proceso recién desbloqueado, sucediéndose un *robo de señal*, y llegaríamos a una situación de falta de equidad.

Para solucionar este segundo problema, algunos lenguajes implementan una *semántica desplazante* en las señales: el proceso que ejecuta el `signal` le pasa el monitor al proceso que recibió la señal (el primero en la cola de bloqueados de la variable condición correspondiente), sin liberar en ningún momento el monitor, de forma que el proceso señalado tiene prioridad. Se dice que la señal usada con la operación `signal` tiene *semántica desplazante*.

Cabe destacar que **no todos los lenguajes con monitores tienen señales con semántica desplazante**, por lo que en dichos lenguajes pueden sucederse robos de señales. De hecho, para demostrar luego la corrección de nuestros programas concurrentes que usan monitores, supondremos que estamos usando un `signal` que envía una señal con semántica desplazante.

Como comentario final a la descripción de un monitor y para motivar la siguiente sección:

- Se presupone que el programador de monitores es un programador experto, de forma que el compilador en ningún momento se dedicará a comprobar si hemos programado de forma correcta un monitor o un procedimiento de él, más allá de la sintaxis del código.
- No deben programarse operaciones `wait` indebidas ni omitirse operaciones `signal` innecesarias. Para comprobar esto, usaremos nuestro sistema de verificación formal.

## 2.2. Verificación de programas con monitores

En la verificación de los programas concurrentes que hemos manejado hasta ahora, hemos primero demostrado la corrección secuencial de cada proceso que forma

parte de un programa secuencial, para luego demostrar la no interferencia entre los mismos.

Sin embargo, ahora que introducimos los monitores, esto no podrá ser nunca más así, ya que un programador nunca puede conocer a priori la traza que genera un proceso que forma parte de un programa concurrente con monitores, ya que al ejecutar procedimientos de monitores, estos pueden quedar bloqueados y se ejecutarían en medio instrucciones de otros procesos que podrían alterar las variables compartidas del programa, falseando alguna precondition o poscondición del proceso bloqueado, por lo que tras desbloquearse, no podemos esperar nada de dicho proceso.

Es por tanto que ahora la estrategia a seguir en las demostraciones es mediante un Invariante de Monitor.

### 2.2.1. Invariante de monitor

**Definición 2.2** (Invariante de Monitor). Un Invariante de Monitor (IM) es una relación entre las variables permanentes de un monitor que debe ser cierta en cualquier estado del programa concurrente, excepto cuando un proceso esté ejecutando código de un procedimiento del monitor.

De esta forma, un IM puede no ser cierto durante la ejecución de un procedimiento por parte de un proceso, pero este ha de cumplirse antes y después de la ejecución de dicho procedimiento.

Si conseguimos probar la existencia de un IM en un programa concurrente, entonces bastará con probar cada una de las secciones de código secuenciales entre llamadas a procedimientos del monitor. Para probar finalmente la corrección de los procesos, usaremos que los IM se mantienen antes y después de las llamadas a procedimientos, para conseguir probar finalmente la corrección de cada uno de los procesos. Si nuestro IM estaba relacionado con la solución al problema, como el acceso a variables compartidas estará controlado por los monitores, al final del programa todos los IMs demostrados se seguirán cumpliendo, por lo que tendremos probada la corrección de nuestro programa concurrente.

Es decir, primero demostraremos que por cada monitor que usamos se verifica un IM, y luego pasaremos a probar la corrección de cada proceso que interviene en el programa concurrente, usando para ello dichos IMs. Finalmente, tendremos probado el programa concurrente.

### Esquema de demostración

Suponiendo que hemos encontrado una relación matemática entre las variables permanentes de un monitor y queremos probar que se trata de un IM<sup>11</sup>, lo primero será probar que  $IM$  se cumple en el estado inicial del monitor, esto es, justo después de la inicialización de las variables permanentes, por lo que tendremos que probar que se verifica el **triple de inicialización de variables**:

$$\{V\} \text{ código de inicialización } \{IM\}$$

<sup>11</sup>A continuación, llamaremos a dicha condición IM, pese a no haber demostrado que se trate de verdad de un IM.

Posteriormente, deberemos probar que  $IM$  se mantiene antes y después de la llamada a cada procedimiento. Es decir, notando por  $IN$  a las precondiciones que tenemos antes de la ejecución de un procedimiento y por  $OUT$  a las poscondiciones que deseamos tener tras dicho procedimiento, debemos demostrar los **triples de procedimientos del monitor**, es decir, demostrar un triple

$$\{IM \wedge IN\} \text{ procedimiento } \{IM \wedge OUT\}$$

por cada procedimiento que tenga nuestro monitor.

Terminaremos de ver esto más adelante, pero es necesario darnos cuenta de un detalle, y es que si un procedimiento modifica el valor de alguna variable compartida que se usa en otro proceso, debemos demostrar la no interferencia entre dichas instrucciones. Ilustramos esto con el siguiente ejemplo.

**Ejemplo.** Si tenemos un monitor llamado `Buf` con un procedimiento `retirar(x)`, de forma que modifica el valor del parámetro que le pasamos, ante el siguiente código (si  $x$  es una variable compartida):

```
1 cobegin y = x; || Buf.retirar(x); coend
```

Tenemos que probar que al cambiar el valor de  $x$  con el procedimiento `retirar`, no hay interferencia con la instrucción de la izquierda. Es decir, tenemos que probar:

$$NI(pre(y = x), Buf.retirar(x))$$

$$NI(pos(y = x), Buf.retirar(x))$$

Sin embargo, en caso de ejecutar el siguiente código:

```
1 z = x;
  cobegin y=z; || Buf.retirar(x); coend
```

No tendríamos que hacerlo, ya que el uso de variables disjuntas nos garantiza la no interferencia entre dichas instrucciones.

### 2.2.2. Axiomas para operaciones de sincronización con semántica desplazante

Sabemos ya demostrar toda la corrección de un programa secuencial que usa monitores, salvo por un detalle, y es que no sabemos nada sobre cómo demostrar los triples:

$$\{P\} c.wait(); \{Q\}$$

$$\{P\} c.signal(); \{Q\}$$

para cualesquiera asertos  $P$  y  $Q$ .

En esta subsección, trataremos de dar axiomas para la comprobación de dichos triples, razonándolos de forma intuitiva y mediante el uso de Invariantes de Monitores.

### Axioma de operación wait

Comenzaremos primero con el triple  $\{P\} c.wait(); \{Q\}$ . Para necesitar ejecutar una instrucción **wait** en un procedimiento de un monitor, lo que sucede es que estamos cerca de un estado inseguro del programa (intuitivamente, que  $IM$  está a punto de incumplirse), pero no llegamos a él, porque para ello ejecutamos esta operación, para impedir que el proceso ejecute una instrucción que falsee el  $IM$ . Por tanto, el proceso se bloquea, dejando libre el monitor, por lo que entra otro proceso a ejecutar otro procedimiento.

Solo podremos desbloquear al proceso cuando nos alejemos de dicho estado inseguro, por lo que además de cumplirse el  $IM$ , deberá cumplirse una condición un tanto más estricta que el  $IM$  (que nos indique que estamos lejos de aquel estado inseguro por el cual se bloqueó el proceso). Dicha condición recibe el nombre de *condición de sincronización*, y la notaremos por  $C$ <sup>12</sup>.

Resumiendo:

- Antes de ejecutar la operación **wait**, hemos de estar en un estado seguro del programa, por lo que ha de cumplirse el  $IM$ .
- Tras ejecutar la operación **wait** (es decir, después de que el proceso haya sido desbloqueado), ha de cumplirse la condición de sincronización  $C$ .

Teniendo en cuenta que además se puede cumplir un invariante local al que llamamos  $L$  (esto es, relaciones entre variables permanentes del monitor que se cumplen en un determinado momento) antes y después de dicha instrucción **wait**.

De esta forma, acabamos de razonar de forma intuitiva el **Axioma de la operación wait**:

$$\{IM \wedge L\} c.wait(); \{C \wedge L\}$$

### Axioma de operación signal

Si nos disponemos a ejecutar una instrucción **signal** en nuestro código, es porque el estado del programa se ha alejado de la condición insegura de la que hablábamos en la subsección anterior, que falsearía el valor de verdad de  $IM$ . Por tanto, el programa ha llegado a un punto en el que se cumple la condición de sincronización  $C$ , y ya puede desbloquear al proceso que anteriormente bloqueó. Tras su desbloqueo, este proceso podría ejecutar una instrucción que volviera a acercarnos a un estado inseguro, pero sin llegar a él (ya que  $C$  era suficientemente restrictiva), por lo que como poscondición de la instrucción **signal** no podremos garantizar  $C$ , sino sólo podremos asegurar que se sigue cumpliendo  $IM$ .

Añadiendo la posibilidad de tener un invariante local  $L$  y que si la cola de la variable condición está vacía, la operación **signal** es una instrucción nula, llegamos al **Axioma de la operación signal**:

$$\{\neg vacio(c) \wedge C \wedge L\} c.signal(); \{IM \wedge L\}$$

o equivalentemente:

$$\{c.queue() \wedge C \wedge L\} c.signal(); \{IM \wedge L\}$$

---

<sup>12</sup>Notemos que según hemos definido  $C$ , ha de verificarse que  $IM \rightarrow C$ .

En caso de cumplirse que  $c.queue() = false$ , entonces negaría la precondition del triple, haciéndolo la regla cierta por un razonamiento por vacuidad.

*Observación.* Notemos que el axioma de la operación signal funciona porque hemos supuesto que **tenemos semántica desplazante**, y es que  $IM$  se cumple inmediatamente de desbloquear al proceso que tenemos bloqueado, ya que tras ejecutar **signal** hemos cedido el monitor al proceso anteriormente bloqueado, en vez de liberar el monitor y dejar paso a otro proceso cualquiera, donde nada nos garantizaría que  $C$  se siguiera cumpliendo tras la ejecución del procedimiento de dicho proceso, pudiendo ahora ejecutar el proceso que se bloqueó bajo una precondition que no es  $C$ , lo que podría llevar al programa a adoptar un estado inseguro.

Una vez vistos ya todos los axiomas sobre verificación de operaciones de sincronización de semáforos, estamos listos para desmotrar la corrección de un  $IM$ . Lo haremos en el siguiente ejemplo.

**Ejemplo.** En este ejemplo, queremos programar un monitor que simule el funcionamiento de un semáforo. Para ello, se nos ha ocurrido el siguiente código:

```
1  Monitor Semaforo;
   var s : integer;
   c : cond;

5  procedure P;
   begin
     if s=0 then
       c.wait;
     else
10    null;
     end if
     s = s - 1;
   end

15  procedure V;
   begin
     s = s + 1;
     c.signal;
   end

20  begin {código de inicialización}
     s = 0;
   end
```

Donde hemos llamado P a la función `sem_wait` del semáforo y por V a la función `sem_signal`.

Procedemos a realizar la demostración de que existe un Invariante de Monitor que se mantiene tras la inicialización de las variables permanentes de nuestro monitor y antes y después de cada procedimiento, con la finalidad de poder usar dicho IM en las demostraciones de cualquier programa concurrente que use el semáforo que acabamos de implementar mediante un monitor.

*Demostración.* Tratamos de demostrar que este monitor tiene como IM el aserto

$$IM \equiv \{s \geq 0\}$$

1. Primero, tenemos que demostrar el triple de inicialización de variables:

$$\{V\} \ s = 0; \ \{s \geq 0\}$$

Como el triple  $\{V\} \ s = 0; \ \{s = 0\}$  es cierto por el axioma de asignación y tenemos que  $\{s = 0\} \rightarrow \{s \geq 0\}$ , usando la primera regla de la consecuencia tenemos demostrado el triple.

2. Posteriormente, demostraremos el triple de procedimiento del monitor para el procedimiento P:  $\{IM\} \ P \ \{IM\}$ . Para ello, primero tendremos que probar el triple

$$\{IM\} \ \text{if } s = 0 \ \text{then } c.\text{wait}; \ \text{else } \text{null}; \ \text{end if } \{s > 0\}$$

Luego usaremos la regla del **if**, por lo que será suficiente con probar los triples:

$$\begin{aligned} \{IM \wedge s = 0\} \ c.\text{wait}; \ \{s > 0\} \\ \{IM \wedge s > 0\} \ \text{null}; \ \{s > 0\} \end{aligned}$$

- a) Comenzamos por el segundo, por ser más sencillo. Como

$$\{IM \wedge s > 0\} \equiv \{s \geq 0 \wedge s > 0\} \equiv \{s > 0\}$$

basta probar el triple  $\{s > 0\} \ \text{null}; \ \{s > 0\}$ , que es cierto por el axioma de la sentencia nula.

- b) Para el primer triple, buscamos aplicar el axioma de la operación **wait**, por lo que tenemos que buscar la condición de sincronización. Para ello, buscamos la precondition del **signal** asociado a la misma variable condición, que se encuentra en el procedimiento **V**. Para hallar la precondition de la instrucción **c.signal**, tendremos que demostrar alguna instrucción de dicho procedimiento, con el fin de hallar la precondition.

Sobre el código de **V**, vemos que antes de **c.signal** se ejecuta una primera instrucción **s=s+1**; . Suponemos que **V** tiene como precondition **IM**, por lo que buscamos una poscondición para **s=s+1**;

$$\{IM\} \equiv \{s \geq 0\} \ s = s + 1;$$

Puede comprobarse con el axioma de asignación que la poscondición buscada es  $\{s > 0\}$ . Por tanto, esta será la condición de sincronización de la variable condición **c**:

$$C \equiv \{s > 0\}$$

Como  $\{IM \wedge s = 0\} \equiv \{s = 0\}$ , acabamos de probar el primer triple usando el axioma de la operación **wait**:

$$\{s = 0\} \ c.\text{wait}; \ \{s > 0\}$$

Una vez demostrados los dos triples, tenemos probado el triple del `if`, por lo que sólo faltará probar el triple

$$\{s > 0\} \ s = s - 1; \ \{IM\}$$

Para tener probado el triple del procedimiento `P`.

Como  $\{IM\} \equiv \{s \geq 0\}$ , basta aplicar el axioma de asignación, para obtener  $\{s > 0\} \ s = s - 1; \ \{s \geq 0\}$ .

Aplicando finalmente la regla de composición sobre el triple del `if` y este último triple, tenemos ya probado  $\{IM\} \ P \ \{IM\}$ .

3. Finalmete, hemos de probar el triple  $\{IM\} \ V \ \{IM\}$  para garantizar al fin que `IM` es un IM. Para ello, hemos de probar el triple

$$\{IM\} \ s = s + 1; c.signal; \ \{IM\}$$

Basta con probar los triples

$$\begin{aligned} &\{IM\} \ s = s + 1; \ \{s > 0\} \\ &\{s > 0\} \ c.signal; \ \{IM\} \end{aligned}$$

y aplicar la regla de composición. El primer triple ya lo demostramos en la demostración del triple del procedimiento `P`, luego bastará probar el segundo, el cual es cierto gracias al axioma de la operación `signal`.

Acabamos de probar que  $\{IM\} \ V \ \{IM\}$ , que era el último procedimiento del monitor, luego `IM` es un IM.

□

**Ejercicio 2.2.1.** Se pide demostrar que el siguiente monitor funciona como un semáforo de Habermann.

En un semáforo de Habermann, queremos llevar la cuenta de:

- El número de recursos que han estado disponibles en algún momento, `nv`.
- El número de procesos que han podido hacer uso de un recurso, `np`.
- El número de procesos que han solicitado hacer uso de un recurso, `na`.

```

1  Monitor Semaforo;
   var na, np, nv : int;
       c : cond;

5  procedure P;
   begin
       na = na + 1;
       if(na > nv) then c.wait();
       np = np + 1;
10 end

   procedure V;
```

```

begin
  nv = nv + 1;
15  if(na > np) then c.signal();
end

begin
  na = 0; np = 0; nv = 0;
20 end

```

- Como para poder hacer uso de un recurso hay que haber solicitado acceso a él previamente, siempre tendremos que  $na \geq np$ .
- Como un proceso solo puede hacer uso de un recurso a la vez, el número de recursos que en algún momento han estado disponibles debe ser menor o igual al número de recursos que en algún momento han sido utilizados por algún proceso:  $nv \geq np$ .
- Ahora, destacamos dos casos:
  - Si el número de peticiones para un recurso es mayor que el número de recursos que en algún momento han estado libre,  $na \geq nv$ , entonces es que no se han podido cumplir todas las peticiones, por lo que tienen que haber más procesos que han podido hacer uso de un recurso que recursos disponibles, es decir,  $np \geq nv$ .
  - Por otra parte, si el número de peticiones es menor al número de recursos que en algún momento han estado disponibles,  $na \leq nv$ , entonces todas las peticiones se han podido completar, por lo que  $np \geq na$ .

Combinando estos dos puntos finales, deducimos que  $np \geq \min(na, nv)$ .

Procedemos a demostrar que el monitor que simula el funcionamiento del semáforo de Habermann tiene como IM:

$$\{IM\} = \{np \leq na \wedge np \leq nv \wedge np \geq \min(na, nv)\}$$

En primer lugar, tendremos que demostrar el triple de inicialización de variables,  $\{V\}$  código de inicialización  $\{IM\}$ :

$$\begin{aligned} \{V\} \quad na = 0; \quad np = 0; \quad nv = 0; \quad \{na = 0 \wedge np = 0 \wedge nv = 0\} \\ \{na = 0 \wedge np = 0 \wedge nv = 0\} \rightarrow \{IM\} \end{aligned}$$

Ahora, tendremos que probar los triples de los procedimientos del monitor:

$$\begin{aligned} \{IM\} \quad P \quad \{IM\} \\ \{IM\} \quad V \quad \{IM\} \end{aligned}$$

1. Para el primero:

$$\begin{aligned} \{IM\} \equiv \{np \leq na \wedge np \leq nv \wedge np \geq \min(na, nv)\} \\ na = na + 1; \\ \{np \leq na - 1 \wedge np \leq nv \wedge np \geq \min(na - 1, nv)\} \\ \text{if } (na > nv) \text{ then } c.wait(); \\ np = np + 1; \end{aligned}$$



2.

### 2.2.3. Regla de la concurrencia para la verificación de programas con monitores

Dado un programa concurrente en el que tenemos  $n$  procesos ejecutándose que podemos representar como triples ciertos de Hoare ciertos  $\{P_i\} S_i \{Q_i\}$  con  $i \in \{1, \dots, n\}$  de forma que ninguna variable en  $P_i$  o en  $Q_i$  es modificada por ningún  $S_j$  con  $i \neq j$ . Si en dicho código tenemos  $m$  monitores de forma que para cada uno hemos conseguido probar un IM  $IM_k$  con  $1 \leq k \leq m$ , entonces podemos aplicar la **regla de concurrencia para programas con monitores**:

$$\frac{\{P_i\} S_i \{Q_i\} \quad 1 \leq i \leq n}{\begin{array}{l} \{MI_1 \wedge \dots \wedge MI_m \wedge P_1 \wedge \dots \wedge P_n\} \\ cobegin S_1 \parallel S_2 \parallel \dots \parallel S_n coend \\ \{MI_1 \wedge \dots \wedge MI_m \wedge Q_1 \wedge \dots \wedge Q_n\} \end{array}}$$

Obteniendo así la verificación de nuestro programa concurrente.



## 3. Relaciones de problemas

### 3.1. Introducción

**Ejercicio 3.1.1.** Considerar el siguiente fragmento de programa para 2 procesos P1 y P2: Los dos procesos pueden ejecutarse a cualquier velocidad. ¿Cuáles son los posibles valores resultantes para la variable  $x$ ? Suponer que  $x$  debe ser cargada en un registro para incrementarse y que cada proceso usa un registro diferente para realizar el incremento.

```

1  {variables compartidas}
   var x : integer := 0 ;
   Process P1;
   var i: integer;
5  begin
   begin
       for i:= 1 to 2 do begin
           x:= x + 1;
       end
10  end
   end

```

```

1
   Process P2;
   var j: integer;
5  begin
   begin
       for j:= 1 to 2 do begin
           x:= x + 1;
       end
10  end
   end

```

Observando el código, cada proceso hace 2 lecturas y dos escrituras (incrementos) en  $x$ .

- Como cada proceso aumenta dos veces el valor de  $x$ , el valor de  $x$  ha de ser, como mínimo, 2.
- Como en total se hacen 4 incrementos, el valor de  $x$  ha de ser 4 como máximo.

Notando por  $l_{ij}$  a la  $j$ -ésima lectura del proceso  $i$  y por  $e_{ij}$  a la  $j$ -ésima escritura del proceso  $i$ , ambas referidas a la variable  $x$ , podemos obtener cualquiera de las siguientes trazas de ejecución:

P1	P2	x	P1	P2	x	P1	P2	x	P1	P2	x
$l_{11}$	-	0	$l_{11}$	-	0	$l_{11}$	-	0	$l_{11}$	-	0
$e_{11}$	-	1	-	$l_{21}$	0	$e_{11}$	-	1	-	$l_{21}$	0
-	$l_{21}$	1	$e_{11}$	-	1	-	$l_{21}$	1	$e_{11}$	-	1
-	$e_{21}$	2	-	$e_{21}$	1	-	$e_{21}$	2	-	$e_{21}$	1
$l_{12}$	-	2	$l_{12}$	-	1	$l_{12}$	-	2	$l_{12}$	-	1
$e_{12}$	-	3	$e_{12}$	-	2	-	$l_{22}$	2	-	$l_{22}$	1
-	$l_{22}$	3	-	$l_{22}$	2	$e_{12}$	-	3	$e_{12}$	-	2
-	$e_{22}$	4	-	$e_{22}$	3	-	$e_{22}$	3	-	$e_{22}$	2

Luego los posibles valores resultantes para  $x$  son: 2, 3 y 4.

**Ejercicio 3.1.2.** ¿Cómo se podría hacer la copia del fichero  $f$  en otro  $g$ , de forma concurrente, utilizando la instrucción concurrente `cobegin-coend`? Para ello, suponer que:

1. Los archivos son una secuencia de items de un tipo arbitrario  $T$ , y se encuentran ya abiertos para lectura ( $f$ ) y escritura ( $g$ ). Para leer un ítem de  $f$  se usa la llamada a función `leer(f)` y para saber si se han leído todos los ítems de  $f$ , se puede usar la llamada `fin(f)` que devuelve verdadero si ha habido al menos un intento de leer cuando ya no quedan datos. Para escribir un dato  $x$  en  $g$  se puede usar la llamada a procedimiento `escribir(g,x)`.
2. El orden de los items escritos en  $g$  debe coincidir con el de  $f$ .
3. Dos accesos a dos archivos distintos pueden solaparse en el tiempo.

La copia del fichero  $f$  en el fichero  $g$  se podría realizar siguiendo el paradigma productor/consumidor que hemos visto en teoría en el Tema 1, mediante el uso de dos procesos:

- Uno que lea un ítem del fichero  $f$  y lo escriba en una variable compartida.
- Otro que lea dicha variable compartida y escriba el ítem en el fichero  $g$ .

En dicho código, debemos garantizar que:

- El consumidor no lea la variable antes de que el productor escriba en ella.
- En la segunda escritura del productor, debemos esperar a que antes la haya leído el consumidor.
- En la segunda lectura del consumidor, debemos esperar a que antes haya modificado la variable el productor.

Siguiendo estos pasos, obtendríamos un código como el siguiente:

```
1 process CopiaFicheros ;
  var ant, sig : T ;
  begin
    sig = leer(f) ;
5   while not fin(f) do begin
      ant = sig ;
      cobegin
        escribir(g, anterior) ;
        sig = leer(f) ;
10    coend
      end
  end
```

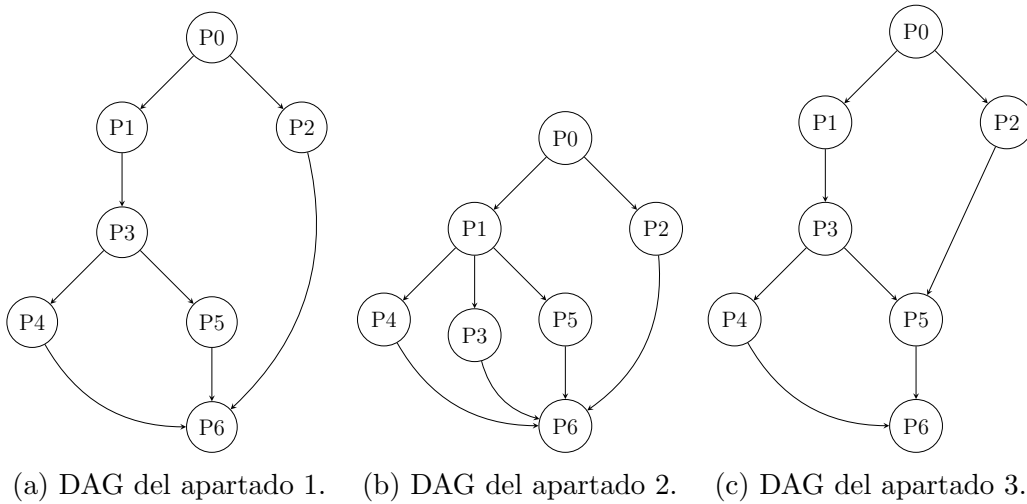


Figura 3.1: Grafos de precedencia del ejercicio 3.1.3.

**Ejercicio 3.1.3.** Construir, utilizando las instrucciones concurrentes `cobegin-coend` y `fork-join`, programas concurrentes que se correspondan con los grafos de precedencia que se muestran en la figura 3.1.

1. Grafo de precedencia de la figura 3.1a:

```

1  begin
    P0;
    fork P2; P1;
    P3;
5  fork P5; P4;
    join P2; join P5;
    P6;
end

```

```

1  begin
    P0;
    cobegin
        P2;
5    begin
        P1;
        P3;
        cobegin P4; P5; coend
    end
10   coend
    P6;
end

```

2. Grafo de precedencia de la figura 3.1b:

```

1  begin
    P0;
    fork P2; P1;
    fork P5; fork P3; P4;
5  join P2; join P5; join P3;
    P6;
end

```

```

1  begin
    P0;
    cobegin
        P2;
5    begin
        P1;
        cobegin P4; P3; P5; coend
    end
10   coend
    P6;
end

```

## 3. Grafo de precedencia de la figura 3.1c:

```

1  begin
    P0;
    fork P2; P1;
    P3;
5  fork P4; join P2; P5;
    join P4;
    P6;
end

```

Sin embargo, no podemos hacer al 100% el DAG de la figura 3.1c, ya que tras P3 debemos crear una estructura `cobegin-coend`. Sin embargo, este debe esperar a P2, por lo que la estructura `cobegin-coend` tendrá que esperar a P2, pero es que P4 no necesita que P2 termine.

Por tanto, no se puede programar con creación de hebras de forma estructurada. Sin embargo, podemos ofrecer dos soluciones, cada una que impone algo que el grafo no nos dice:

- a) Si obligamos a que P4 también espere a P2, obtendríamos el código:

```

1  begin
    P0;
    cobegin
        P2;
5  begin
        P1; P3;
        end
    coend
    cobegin P4; P5; coend
10 P6;
end

```

- b) Si ahora queremos ejecutar de forma concurrente el flujo que tiene a P1, P3 y P4 con el flujo que tiene a P2, entonces obligamos a que P5 espere a P4 (que no nos lo especifica el DAG, pero lo necesitamos para poder programarlo de forma estructurada):

```

1  begin
    P0;
    cobegin
        begin P1; P3; P4; end
5  P2;
    coend
    P5;
    P6;
end

```

**Ejercicio 3.1.4.** Dados los siguientes fragmentos de programas concurrentes, obtener sus grafos de precedencia asociados:

```

1  begin
    P0 ;
    cobegin
        P1 ;
5    P2 ;
        cobegin
            P3 ; P4 ; P5 ; P6 ;
        coend ;
10   P7 ;
    coend
    P8 ;
end

```

```

1  begin
    P0 ;
    cobegin
        begin
5            cobegin
                P1 ; P2 ;
            coend
            P5 ;
        end
10       begin
            cobegin
                P3 ; P4 ;
            coend
            P6 ;
        end
15       end
    coend
    P7 ;
end

```

(a) Programa 1.

(b) Programa 2.

Figura 3.4: Programas concurrentes del ejercicio 3.1.4.

1. Programa de la figura 3.4a.

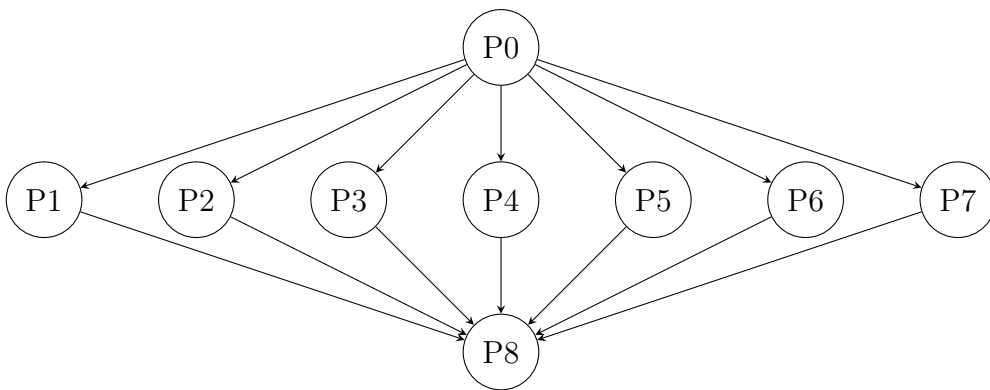


Figura 3.5: DAG para la figura 3.4a.

2. Programa de la figura 3.4b.

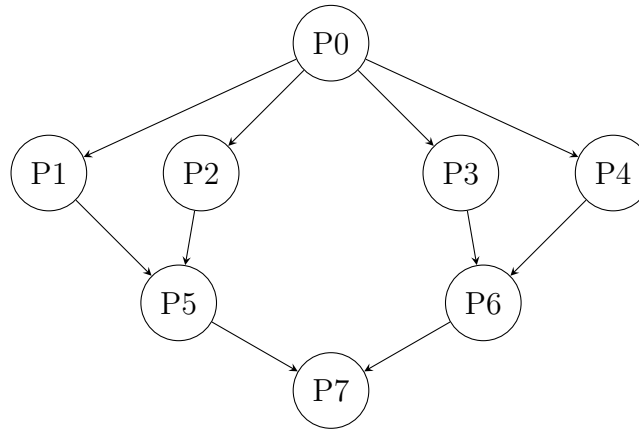


Figura 3.6: DAG para la figura 3.4b.

**Ejercicio 3.1.5.** Suponer un sistema de tiempo real que dispone de un captador de impulsos conectado a un contador de energía eléctrica. La función del sistema consiste en contar el número de impulsos producidos en 1 hora (cada Kwh consumido se cuenta como un impulso) e imprimir este número en un dispositivo de salida. Para ello se dispone de un programa concurrente con 2 procesos: un proceso acumulador (lleva la cuenta de los impulsos recibidos) y un proceso escritor (escribe en la impresora). En la variable común a los 2 procesos  $n$  se lleva la cuenta de los impulsos. El proceso acumulador puede invocar un procedimiento `Espera_impulso` para esperar a que llegue un impulso, y el proceso escritor puede llamar a `Espera_fin_hora` para esperar a que termine una hora. El código de los procesos de este programa podría ser el descrito en el Código Fuente 1.

*Observación.* En el programa se usan sentencias de acceso a la variable  $n$  encerradas entre los símbolos  $<$  y  $>$ . Esto significa que cada una de esas sentencias se ejecuta en exclusión mutua entre los dos procesos, es decir, esas sentencias se ejecutan de principio a fin sin entremezclarse entre ellas. Supongamos que en un instante dado el acumulador está esperando un impulso, el escritor está esperando el fin de una hora, y la variable  $n$  vale  $k$ . Después se produce de forma simultánea un nuevo impulso y el fin del periodo de una hora.

Obtener las posibles secuencias de interfoliación de las instrucciones (1),(2), y (3) a partir de dicho instante, e indicar cuales de ellas son correctas y cuales incorrectas (las incorrectas son aquellas en las cuales el impulso no se contabiliza).

En primer lugar, notemos que la instrucción 2 siempre se ejecutará antes que la instrucción 3, ya que están ambas en el mismo proceso (el escritor). Por tanto, las secuencia de instrucciones que se pueden dar son las intercalaciones de la instrucción 1 con las otras dos instrucciones; es decir: A) 1 – 2 – 3, B) 2 – 1 – 3 y C) 2 – 3 – 1. El análisis de cada una de ellas está en la Tabla 3.1. Notemos que tanto la opción A como la C son válidas, ya que en ambas se contabiliza el impulso. No obstante, difieren entre sí, puesto que en la opción A se contabiliza el impulso en la hora que termina (imprimiéndose entonces), mientras que en la opción C se contabiliza el impulso en la hora siguiente (no imprimiéndose entonces en esta salida). No obstante, la opción B es incorrecta, ya que no se contabiliza el impulso en la hora que termina ni en la siguiente.



```

1  { variable compartida: }
   var n : integer; { contabiliza impulsos }
   begin
   while true do begin
5     Espera_impulso();
      < n := n+1 > ; { (1) }
      end
   end
   process Escritor ;
10  begin
   while true do begin
      Espera_fin_hora();
      write( n ) ; { (2) }
      < n := 0 > ; { (3) }
15  end
   end

```

Código fuente 1: Código acumulador-escritor del ejercicio 3.1.5.

Opción A			Opción B			Opción C		
Operación	n	Salida	Operación	n	Salida	Operación	n	Salida
—	$k$	—	—	$k$	—	—	$k$	—
$1 \rightarrow n := n+1$	$k+1$	—	$2 \rightarrow \text{write}(n)$	$k$	$k$	$2 \rightarrow \text{write}(n)$	$k$	$k$
$2 \rightarrow \text{write}(n)$	$k+1$	$k+1$	$1 \rightarrow n := n+1$	$k+1$	$k$	$3 \rightarrow n := 0$	0	$k$
$3 \rightarrow n := 0$	0	$k+1$	$3 \rightarrow n := 0$	0	$k$	$1 \rightarrow n := n+1$	1	$k$

Tabla 3.1: Tabla de opciones del ejercicio 3.1.5.

```

1  procedure Sort( s,t : integer );
    var i, j : integer ;
    begin
        for i := s to t do
            for j:= s+1 to t do
2              if a[i] < a[j] then
3                  swap( a[i], b[j] ) ;
            end
        end
10 procedure Copiar( o,s,t : integer );
    var d : integer ;
    begin
        for d := 0 to t-s do
            b[o+d] := a[s+d] ;
15 end

```

Código fuente 2: Procedimientos `Sort` y `Copiar` del ejercicio 3.1.6.

**Ejercicio 3.1.6.** Supongamos un programa concurrente en el cual hay, en memoria compartida dos vectores `a` y `b` de enteros y con tamaño par, declarados como sigue:

```

1  var a,b : array[1..2*n] of integer ; { n es una constante predefinida }

```

Queremos escribir un programa para obtener en `b` una copia ordenada del contenido de `a` (nos da igual el estado en que queda `a` después de obtener `b`). Para ello disponemos de la función `Sort` que ordena un tramo de `a` (entre las entradas `s` y `t`, ambas incluidas). También disponemos la función `Copiar`, que copia un tramo de `a` (desde `s` hasta `t`) en `b` (a partir de `o`). Estas funciones se muestran en el Código Fuente 2.

El programa para ordenar se puede implementar de dos formas:

1. Ordenar todo el vector `a`, de forma secuencial con la función `Sort`, y después copiar cada entrada de `a` en `b`, con la función `Copiar`.
2. Ordenar las dos mitades de `a` de forma concurrente, y después mezclar dichas dos mitades en un segundo vector `b` (para mezclar usamos un procedimiento `Merge`).

En el Código Fuente 3 se muestra el código de ambas versiones.

El código de la función `Merge`, disponible en el Código Fuente 4, se encarga de ir leyendo las dos mitades de `a`, en cada paso, seleccionar el menor elemento de los dos siguientes por leer (uno en cada mitad), y escribir dicho menor elemento en la siguiente mitad del vector mezclado `b`.

Llamaremos  $T_s(k)$  al tiempo que tarda el procedimiento `Sort` cuando actúa sobre un segmento del vector con  $k$  entradas. Suponemos que el tiempo que (en media) tarda cada iteración del bucle interno que hay en `Sort` es la unidad (por definición).

Es evidente que ese bucle tiene  $\frac{k(k-1)}{2}$  iteraciones, luego:

$$T_s(k) = \frac{k(k-1)}{2} = \frac{1}{2} \cdot k^2 - \frac{1}{2} \cdot k$$

```
1 procedure Secuencial() ;  
  var i : integer ;  
  begin  
    Sort( 1, 2*n ); { ordena a }  
5    Copiar( 1, 2*n ); { copia a en b }  
  end  
  
procedure Concurrente() ;  
  begin  
10    cobegin  
      Sort( 1, n );  
      Sort( n+1, 2*n );  
    coend  
    Merge( 1, n+1, 2*n );  
15  end
```

Código fuente 3: Procedimientos `Secuencial` y `Concurrente` del ejercicio 3.1.6.

```
1 procedure Merge( inferior, medio, superior: integer ) ;  
  { siguiente posicion a escribir en b }  
  var escribir : integer := 1 ;  
  { siguiente pos. a leer en primera mitad de a }  
5  var leer1 : integer := inferior ;  
  { siguiente pos. a leer en segunda mitad de a }  
  var leer2 : integer := medio ;  
  begin  
    { mientras no haya terminado con alguna mitad }  
10    while leer1 < medio and leer2 <= superior do begin  
      if a[leer1] < a[leer2] then begin { minimo en la primera mitad }  
        b[escribir] := a[leer1] ;  
        leer1 := leer1 + 1 ;  
      end else begin { minimo en la segunda mitad }  
15      b[escribir] := a[leer2] ;  
        leer2 := leer2 + 1 ;  
      end  
      escribir := escribir+1 ;  
    end  
20    { se ha terminado de copiar una de las mitades,  
      copiar lo que quede de la otra }  
    if leer2 > superior then  
      { copiar primera } Copiar( escribir, leer1, medio-1 );  
    else Copiar( escribir, leer2, superior ); { copiar segunda }  
25  end
```

Código fuente 4: Procedimiento `Merge` del ejercicio 3.1.6.

El tiempo que tarda la versión secuencial sobre  $2n$  elementos (llamaremos  $S$  a dicho tiempo) será evidentemente  $T_s(2n)$ , luego:

$$S = T_s(2n) = \frac{1}{2} \cdot (2n)^2 - \frac{1}{2} \cdot 2n = 2n^2 - n$$

Con estas definiciones, calcular el tiempo que tardará la versión paralela, en los dos siguientes casos. Para esto, hay que suponer que cuando el procedimiento **Merge** actúa sobre un vector con  $p$  entradas, tarda  $p$  unidades de tiempo en ello, lo cual es razonable teniendo en cuenta que en esas circunstancias **Merge** copia  $p$  valores desde **a** hacia **b**. Si llamamos a este tiempo  $T_m(p)$ , podemos escribir  $T_m(p) = p$ . Escribe también una comparación cualitativa de los tres tiempos ( $S$ ,  $P_1$  y  $P_2$ ).

1. Las dos instancias concurrentes de **Sort** se ejecutan en el mismo procesador (llamamos  $P_1$  al tiempo que tarda).

En este caso, tenemos que hay ganancia de tiempo, ya que las dos instancias de **Sort** no pueden ejecutarse simultáneamente. Por tanto, tenemos que:

$$P_1 = 2 \cdot T_s(n) + T_m(2n) = 2 \cdot \left( \frac{1}{2} \cdot n^2 - \frac{1}{2} \cdot n \right) + 2n = n^2 - n + 2n = n^2 + n$$

2. Cada instancia de **Sort** se ejecuta en un procesador distinto (lo llamamos  $P_2$ ).

Al poder ejecutarse ahora de forma simultánea, tenemos que:

$$P_2 = \max\{T_s(n), T_s(n)\} + T_m(2n) = \left( \frac{1}{2} \cdot n^2 - \frac{1}{2} \cdot n \right) + 2n = \frac{1}{2} \cdot n^2 + \frac{3}{2} \cdot n$$

Como podemos ver, en los tres casos la eficiencia es del orden cuadrático. No obstante, el coeficiente de  $n^2$  es distinto en cada caso, siendo el mayor en la versión secuencial. Deducimos por tanto que las versiones concurrentes son más eficientes que la secuencial, y estas mejoras son significativas para valores de  $n$  grandes.

**Ejercicio 3.1.7.** Supongamos que tenemos un programa con tres matrices (**a**, **b** y **c**) de valores flotantes declaradas como variables globales. La multiplicación secuencial de **a** y **b** (almacenando el resultado en **c**) se puede hacer mediante un procedimiento **MultiplicacionSec** declarado como aparece aquí:

```

1  var a, b, c : array[1..3,1..3] of real ;
   procedure MultiplicacionSec()
       var i,j,k : integer ;
       begin
5          for i := 1 to 3 do
               for j := 1 to 3 do begin
                   c[i,j] := 0 ;
                   for k := 1 to 3 do
10                      c[i,j] := c[i,j] + a[i,k]*b[k,j] ;
                   end
               end
       end

```

Escribir un programa con el mismo fin, pero que use 3 procesos concurrentes. Suponer que los elementos de las matrices **a** y **b** se pueden leer simultáneamente, así

```

1  var a, b, c : array[1..3,1..3] of
    real ;
    process CalcularFila[ i : 1..3] ;
        var j, k : integer ;
        begin
5      for j := 1 to 3 do begin
            c[i,j] := 0 ;
            for k := 1 to 3 do
                c[i,j] := c[i,j] +
                    a[i,k]*b[k,j] ;
            end
10     end
    end
end

```

(a) Procesos concurrentes para calcular por filas.

```

1  var a, b, c : array[1..3,1..3] of
    real ;
    process CalcularColumna[j : 1..3] ;
        var i, k : integer ;
        begin
5      for i := 1 to 3 do begin
            c[i,j] := 0 ;
            for k := 1 to 3 do
                c[i,j] := c[i,j] +
                    a[i,k]*b[k,j] ;
            end
10     end
    end
end

```

(b) Procesos concurrentes para calcular por columnas.

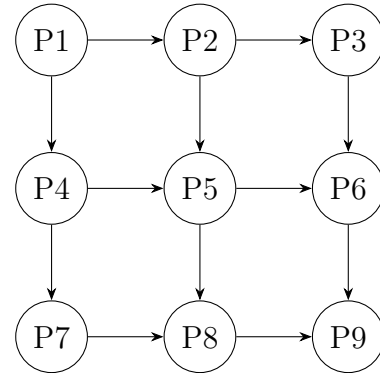
Figura 3.7: Códigos para el ejercicio 3.1.7.

```

1  while true do
    cobegin
        P1 ; P2 ; P3 ;
        P4 ; P5 ; P6 ;
5    P7 ; P8 ; P9 ;
    coend

```

(a) Código del ejercicio 3.1.8.



(b) DAG del ejercicio 3.1.8.

Figura 3.8: Figuras del ejercicio 3.1.8.

como que elementos distintos de  $c$  pueden escribirse simultáneamente.

Esta solución puede llevarse a cabo de dos formas (tal y como vimos en la asignatura de AC). Crearemos tres procesos, y cada uno puede calcular una fila de la matriz  $c$  (Código Fuente 3.7a) o bien cada uno puede calcular una columna de la matriz  $c$  (Código Fuente 3.7b). No obstante, en la asignatura de AC se vio que, por norma general, es más eficiente calcular por filas que por columnas, ya que en el primer caso se accede a la matriz  $a$  de forma secuencial, aprovechando así la localidad espacial y provocando un número menor de fallos de caché.

**Ejercicio 3.1.8.** Un trozo de programa ejecuta nueve rutinas o actividades ( $P_1, P_2, \dots, P_9$ ), repetidas veces, de forma concurrentemente con `cobegin-coend` (ver trozo de código de la figura 3.8a), pero que requieren sincronizarse según determinado grafo (ver la figura 3.8b).

Supón que queremos realizar la sincronización indicada en el grafo, usando para ello llamadas desde cada rutina a dos procedimientos (`EsperarPor` y `Acabar`). Se dan los siguientes hechos:

- El procedimiento **EsperarPor**(*i*) es llamado por una rutina cualquiera (la número *k*) para esperar a que termine la rutina número *i*, usando espera ocupada. Por tanto, se usa por la rutina *k* al inicio para esperar la terminación de las otras rutinas que corresponda según el grafo.
- El procedimiento **Acabar**(*i*) es llamado por la rutina número *i*, al final de la misma, para indicar que dicha rutina ya ha finalizado.
- Ambos procedimientos pueden acceder a variables globales en memoria compartida.
- Las rutinas se sincronizan única y exclusivamente mediante llamadas a estos procedimientos, siendo la implementación de los mismos completamente transparente para las rutinas.

Escribe una implementación de **EsperarPor** y **Acabar** (junto con la declaración e inicialización de las variables compartidas necesarias) que cumpla con los requisitos dados.

Usaremos para ello un vector de variables booleanas **finalizado**, donde **finalizado**[*i*] indica si la rutina *i* ha finalizado o no. Inicialmente estará inicializado a **false**, puesto que ningún proceso ha finalizado. Es decir:

```
1 var finalizado : array[1..9] of boolean := (false,...,false) ;
```

El procedimiento **EsperarPor** se implementa de la siguiente forma:

```
1 procedure EsperarPor( i : integer ) ;
  begin
    while not finalizado[i] do
      begin
5       { no hacer nada }
      end;
    end.
```

Respecto a la función **Acabar**, podríamos pensar que tan solo se necesita cambiar el valor de la variable **finalizado**[*i*] a **true**. No obstante, hemos de tener en cuenta que este programa de ejecuta de forma repetida, por lo que si no se reinicia el vector **finalizado** al final de cada ejecución, en la siguiente ejecución ya no habrá la sincronización necesaria. Por tanto, tras el fin del proceso **P9**, se reinicia el vector **finalizado** a **false**.

```
1 procedure Acabar( i : integer ) ;
  begin
    finalizado[i] := true ;
    if i >= 9 then
5     finalizado := (false,...,false) ;
  end
```

**Ejercicio 3.1.9.** En el ejercicio 3.1.8 los procesos **P1**, **P2**, ..., **P9** se ponen en marcha usando **cobegin-coend**. Escribe un programa equivalente, que ponga en marcha

todos los procesos, pero que use declaración estática de procesos, usando un vector de procesos  $P$ , con índices desde 1 hasta 9, ambos incluidos. El proceso  $P[n]$  contiene una secuencia de instrucciones desconocida, que llamamos  $S_n$ , y además debe incluir las llamadas necesarias a **Acabar** y **EsperarPor** (con la misma implementación que antes) para lograr la sincronización adecuada. Se incluye aquí una plantilla:

```

1 Process P[ n : 1..9 ]
  begin
    ..... { esperar (si es necesario) a los procesos que corresponda }
    S_n ; { sentencias especificas de este proceso (desconocidas) }
5    ..... { senalar que hemos terminado }
  end

```

En primer lugar, hemos de especificar, en función de  $n$ , a qué procesos ha de esperar cada uno, lo cual se hará mediante una matriz compartida. Tenemos que:

```

1 var espera : array[1..9,1..2] of integer := (
    (-1, -1), { P1 }
    (1, -1),   { P2 }
    (2, -1),   { P3 }
5    (1, -1),   { P4 }
    (2, 4),    { P5 }
    (3, 5),    { P6 }
    (4, -1),   { P7 }
    (5, 7),    { P8 }
10   (6, 8)    { P9 }
  ) ;
  Process P[ n : 1..9 ]
  begin
    for i := 1 to 2 do
15     if espera[n,i] <> -1 then { != -1 }
        EsperarPor( espera[n,i] ) ;

    S_n ;
    Acabar( n ) ;
20  end

```

**Ejercicio 3.1.10.** Para los siguientes fragmentos de código, obtener la *poscondición* adecuada para convertirlo en un triple demostrable con la Lógica de Programas:

1.  $\{i < 10\} \quad i = 2 * i + 1 \quad \{\}$

Obtenemos la poscondición de este triple razonando matemáticamente:

$$i < 10$$

$$2 * i < 20$$

$$i' = 2 * i + 1 < 21$$

donde hemos notado por  $i'$  al nuevo valor que adopta la variable  $i$ .

Por tanto, la poscondición del triple es:  $i < 21$ .

Pasamos ahora a demostrar el triple siguiente:

$$\{i < 10\} \quad i = 2 * i + 1 \quad \{i < 21\}$$

Usando el axioma de asignación, tenemos que:

$$\{i < 21\}_{2*i+1}^i \quad i = 2 * i + 1 \quad \{i < 21\}$$

No obstante, de la definición de Sustitución Textual, tenemos que:

$$\{i < 21\}_{2*i+1}^i \equiv \{2 * i + 1 < 21\} \equiv \{i < 10\}$$

Uniando ambas ecuaciones, obtenemos que el triple es cierto.

$$\{i < 10\} \quad i = 2 * i + 1 \quad \{i < 21\}$$

2.  $\{i > 0\} \quad i = i - 1; \quad \{\}$

Obtenemos la poscondición de este triple razonando matemáticamente:

$$i > 0$$

$$i' = i - 1 > -1$$

donde hemos notado por  $i'$  al nuevo valor que adopta la variable  $i$ .

Por tanto, la poscondición del triple es:  $i > -1$ .

Pasamos ahora a demostrar el triple siguiente:

$$\{i > 0\} \quad i = i - 1; \quad \{i > -1\}$$

Usando el axioma de asignación, tenemos que:

$$\{i > -1\}_{i-1}^i \quad i = i - 1 \quad \{i > -1\}$$

No obstante, de la definición de Sustitución Textual, tenemos que:

$$\{i > -1\}_{i-1}^i \equiv \{i - 1 > -1\} \equiv \{i > 0\}$$

Uniando ambas ecuaciones, obtenemos que el triple es cierto.

$$\{i > 0\} \quad i = i - 1 \quad \{i > -1\}$$

3.  $\{i > j\} \quad i = i + 1; \quad j = j + 1 \quad \{\}$

De forma matemática y notando por  $i'$  y  $j'$  a las modificaciones de  $i$  y  $j$ , respectivamente:

$$i > j$$

$$i' = i + 1 > j + 1 = j'$$

$$i' > j'$$

Por tanto, la poscondición del triple es:  $i > j$ . Pasamos a demostrar el triple:

$$\{i > j\} \quad i = i + 1; \quad j = j + 1 \quad \{i > j\}$$

Usando la regla de la composición, tenemos que:

$$\frac{\{P\}S_1\{Q\}, \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}$$

Identificando  $Q$  con  $i > j + 1$ , tenemos que bastará con probar los triples:



$$a) \{i > j\} \ i = i + 1 \ \{i > j + 1\}$$

Mediante el axioma de asignación, tenemos que:

$$\{i > j\} \equiv \{i + 1 > j + 1\} \equiv \{i > j + 1\}_{i+1}^i \ i = i + 1 \ \{i > j + 1\}$$

$$b) \{i > j + 1\} \ j = j + 1 \ \{i > j\}$$

Mediante el axioma de asignación, tenemos que:

$$\{i > j + 1\} \equiv \{i > j\}_{j+1}^j \ j = j + 1 \ \{i > j\}$$

Como ambos son ciertos, el triple que queríamos demostrar también lo es gracias a la regla de composición.

$$4. \ \{\text{falso}\} \quad a = a + 7; \quad \{\}$$

En este caso, partimos de un estado del programa inalcanzable, por lo que en la poscondición podemos poner cualquier estado del programa, es decir,  $\{\text{verdad}\}$ .

$$5. \ \{\text{verdad}\} \quad i = 3; \ j = 2 * i \quad \{\}$$

Como partimos de cualquier estado del programa y sólo se realizan asignaciones, es fácil intuir cuál será la poscondición:

$$\begin{aligned} i &= 3 \\ j &= 2 * i = 2 * 3 = 6 \end{aligned}$$

Pasamos a demostrar el triple

$$\{\text{verdad}\} \quad i = 3; \ j = 2 * i \quad \{i = 3 \ \wedge \ j = 6\}$$

Usando la regla de composición, nos será suficiente probar los triples:

$$\{\text{verdad}\} \ i = 3 \ \{i = 3\} \quad \{i = 3\} \ j = 2 * i \ \{i = 3 \ \wedge \ j = 6\}$$

a) Para el primer triple, usamos el axioma de asignación:

$$\{\text{verdad}\} \equiv \{3 = 3\} \equiv \{i = 3\}_3^i \ i = 3 \ \{i = 3\}$$

b) Para el segundo, volvemos a usar el axioma de asignación:

$$\{i = 3 \ \wedge \ j = 6\}_{2*i}^j \ j = 2 * i \ \{i = 3 \ \wedge \ j = 6\}$$

No obstante, de la definición de Sustitución Textual, tenemos que:

$$\begin{aligned} \{i = 3 \ \wedge \ j = 6\}_{2*i}^j &\equiv \{i = 3 \ \wedge \ 2 * i = 6\} \equiv \{i = 3 \ \wedge \ 2 * 3 = 6\} \equiv \\ &\equiv \{i = 3 \ \wedge \ 6 = 6\} \equiv \{i = 3\} \end{aligned}$$

Uniando ambas ecuaciones, obtenemos que el triple es cierto.

Ambos triples son ciertos, luego por la regla de la composición tenemos demostrado nuestro triple.

6.  $\{\text{verdad}\} \quad c = a + b; \quad c = c/2 \quad \{\}$

Notando por  $c'$  al nuevo valor de  $c$ , tenemos que:

$$\begin{aligned} c &= a + b \\ c' &= c/2 = \frac{a + b}{2} \end{aligned}$$

Tratamos por tanto de probar el siguiente triple

$$\{\text{verdad}\} \quad c = a + b; \quad c = c/2 \quad \left\{ c = \frac{a + b}{2} \right\}$$

Usando la regla de la composición, basta con probar los triples:

$$\{\text{verdad}\} \quad c = a + b; \quad \{c = a + b\} \quad \{c = a + b\} \quad c = c/2; \quad \left\{ c = \frac{a + b}{2} \right\}$$

a) Para el primero, usamos el axioma de asignación:

$$\{\text{verdad}\} \equiv \{a + b = a + b\} \equiv \{c = a + b\}_{a+b}^c \quad c = a + b \quad \{c = a + b\}$$

b) Para la segunda, también usamos el axioma de asignación:

$$\{c = a + b\} \equiv \left\{ \frac{c}{2} = \frac{a + b}{2} \right\} \equiv \left\{ c = \frac{a + b}{2} \right\}_{c/2}^c \quad c = c/2 \quad \left\{ c = \frac{a + b}{2} \right\}$$

Usando la regla de composición, tenemos demostrado nuestro triple.

**Ejercicio 3.1.11.** ¿Cuáles de los siguientes triples no son demostrables con la Lógica de Programas? (Considerando que  $i, x, a \in \mathbb{Z}$ )

1.  $\{i > 0\} \quad i = i - 1; \quad \{i \geq 0\}$

El siguiente triple sabemos que es cierto:

$$\{i > 0\} \quad i = i - 1 \quad \{i > -1\}$$

$\{i > -1\} \rightarrow \{i \geq 0\}$ , luego es cierto por la primera regla de la consecuencia.

2.  $\{x \geq 7\} \quad x = x + 3; \quad \{x \geq 9\}$

El siguiente triple sabemos que es cierto:

$$\{x \geq 7\} \quad x = x + 3 \quad \{x \geq 10\}$$

$\{x \geq 10\} \rightarrow \{x \geq 9\}$ , luego es cierto por la primera regla de la consecuencia.

3.  $\{i < 9\} \quad i = 2 * i + 1; \quad \{i \leq 20\}$

El siguiente triple sabemos que es cierto:

$$\{i < 9\} \quad i = 2 * i + 1 \quad \{i < 19\}$$

$\{i < 19\} \rightarrow \{i \leq 20\}$ , luego es cierto por la primera regla de la consecuencia.

$$4. \{a > 0\} \quad a = a - 7; \quad \{a > -6\}$$

$$\{a > 0\} \quad a = a - 7 \quad \{a > -7\}$$

Pero  $\{a > -7\} \not\vdash \{a > -6\}$ , luego este triple no es demostrable.

**Ejercicio 3.1.12.** Si el triple  $\{P\}C\{Q\}$  es demostrable, indicar por qué los siguientes triples también lo son (o no se pueden demostrar y por qué):

$$1. \{P\}C\{Q \vee P\}$$

Es demostrable, ya que  $\{Q\} \rightarrow \{Q \vee P\}$  y por la primera regla de la consecuencia, tomando  $R = Q \vee P$ :

$$\frac{\{P\}C\{Q\}, \{Q\} \rightarrow \{R\}}{\{P\}C\{R\}}$$

Tenemos que se debilita la poscondición.

$$2. \{P \wedge D\}C\{Q\}$$

Es demostrable, ya que  $\{P \wedge D\} \rightarrow \{P\}$  y por la segunda regla de la consecuencia, tomando  $R = P \wedge D$ :

$$\frac{\{P\} \rightarrow \{R\}, \{R\}C\{Q\}}{\{P\}C\{Q\}}$$

Tenemos que se fortalece la precondition.

$$3. \{P \vee D\}C\{Q\}$$

No es demostrable, porque se debilita la precondition.

$$4. \{P\}C\{Q \vee D\}$$

Al igual que hemos hecho en el apartado 1, es demostrable ya que  $\{Q\} \rightarrow \{Q \vee D\}$  y usando la primera regla de la consecuencia.

$$5. \{P\}C\{Q \wedge P\}$$

No podemos demostrarlo, ya que se fortalece la poscondición.

**Ejercicio 3.1.13.** Si el triple  $\{P\}C\{Q\}$  es demostrable, ¿cuál de los siguientes triples no se puede demostrar?

$$1. \{P \wedge D\}C\{Q\}$$

Sabemos que  $\{P \wedge D\} \rightarrow \{P\}$ , luego puede demostrarse por la segunda regla de la consecuencia (se fortalece la precondition).

$$2. \{P \vee D\}C\{Q\}$$

No puede demostrarse, porque se debilita la precondition.

$$3. \{P\}C\{Q \vee D\}$$

Puede demostrarse mediante la primera regla de la consecuencia, ya que se tiene que  $\{Q\} \rightarrow \{Q \vee D\}$ .

$$4. \{P\}C\{Q \vee P\}$$

Puede demostrarse mediante la primera regla de la consecuencia, ya que se tiene que  $\{Q\} \rightarrow \{Q \vee P\}$ .

**Ejercicio 3.1.14.** Dado el siguiente programa, obtener:

```

1  int x = 5, y = 2;
   cobegin
       < x = x + y >;
       < y = x * y >;
5  coend

```

1. Valores finales de  $x$  e  $y$ . Tenemos dos posibles trazas de ejecución:
  - a) Primero se ejecuta la primera instrucción, por lo que obtendríamos  $x = 7$  y  $y = 14$ .
  - b) Primero se ejecuta la segunda instrucción, por lo que obtendríamos  $x = 15$  y  $y = 10$ .
2. Valores finales de  $x$  e  $y$  si quitamos los símbolos  $< >$  de instrucción atómica.  
Encontramos cada uno de los dos estados anteriores, además de  $x = 7$  y  $y = 10$ .

**Ejercicio 3.1.15.** Comprobar si la demostración del siguiente triple interfiere con los teoremas siguientes:

$$\{x \geq 2\} \quad < x = x - 2 > \quad \{x \geq 0\}$$

Es decir, queremos comprobar si  $R \equiv < x = x - 2 >$  con  $pre(R) = \{x \geq 2\}$  interfiere con los triples siguientes:

1.  $\{x \geq 0\} \quad < x = x + 3 > \quad \{x \geq 3\}$   
Comprobamos en primer lugar su interferencia con la precondition:

$$\{x \geq 0 \wedge x \geq 2\} \quad < x = x - 2 > \quad \{x \geq 0\}$$

Este triple es correcto por la segunda regla de la consecuencia, luego no interfiere con la precondition.

Comprobemos ahora su interferencia con la poscondición:

$$\{x \geq 3 \wedge x \geq 2\} \quad < x = x - 2 > \quad \{x \geq 1\}$$

En este caso,  $\{x \geq 1\} \not\vdash \{x \geq 3\}$ , luego este triple no es demostrable y  $R$  interfiere con la poscondición del triple en cuestión.

2.  $\{x \geq 0\} \quad < x = x + 3 > \quad \{x \geq 0\}$   
Comprobamos en primer lugar su interferencia con la precondition:

$$\{x \geq 0 \wedge x \geq 2\} \quad < x = x - 2 > \quad \{x \geq 0\}$$

Este triple es correcto por la segunda regla de la consecuencia, luego no interfiere con la precondition. Además, como la precondition y la poscondición son iguales,  $R$  tampoco interfiere con la poscondición, luego no interfiere con este triple.

3.  $\{x \geq 7\} \quad < x = x + 3 > \quad \{x \geq 10\}$

Comprobamos en primer lugar su interferencia con la precondition:

$$\{x \geq 7 \wedge x \geq 2\} \quad < x = x - 2 > \quad \{x \geq 5\}$$

No obstante, como  $\{x \geq 5\} \not\vdash \{x \geq 7\}$ ,  $R$  interfiere con la precondition de este triple.

4.  $\{y \geq 0\} \quad < y = y + 3 > \quad \{y \geq 3\}$

$R$  no interfiere con este triple, ya que son variables disjuntas.

5.  $\{x \text{ es impar}\} \quad < y = x + 1 > \quad \{y \text{ es par}\}$

Comprobamos en primer lugar su interferencia con la precondition:

$$\{x \text{ es impar} \wedge x \geq 2\} \quad < x = x - 2 > \quad \{x \text{ es impar} \wedge x \geq 0\}$$

Por la 2ª regla de la consecuencia, como  $\{x \text{ es impar} \wedge x \geq 0\} \rightarrow \{x \text{ es impar}\}$ , tenemos que es correcto y  $R$  no interfiere con la precondition.

Comprobamos ahora su interferencia con la poscondition:

$$\{y \text{ es par} \wedge x \geq 0\} \quad < x = x - 2 > \quad \{y \text{ es par} \wedge x \geq -2\}$$

Por la 2ª regla de la consecuencia, como  $\{y \text{ es par} \wedge x \geq -2\} \rightarrow \{y \text{ es par}\}$ , tenemos que es correcto y  $R$  no interfiere con la poscondition. Por tanto,  $R$  no interfiere con este triple.

**Ejercicio 3.1.16.** Dado el siguiente triple:

$$\begin{array}{c} \{x = 0\} \\ \text{cobegin} \\ < x = x + a > \parallel < x = x + b > \parallel < x = x + c > \\ \text{coend} \\ \{x = a + b + c\} \end{array}$$

Demostrarlo utilizando la lógica de asertos para cada una de las tres instrucciones atómicas y después que se llega a la poscondition final  $x = a + b + c$  utilizando para ello la regla *de la composición concurrente* de instrucciones atómicas.

Inicialmente, demostraremos los 3 siguientes triples, uno por cada instrucción atómica. Hemos de notar que, en cada uno de ellos, como no sabemos en qué orden se ejecutan, tenemos que incluir en las precondiciones y las poscondiciones todas las posibilidades.

1. El correspondiente a la primera instrucción atómica:

$$\begin{array}{c} \{x = 0 \vee x = b \vee x = c \vee x = b + c\} \quad < x = x + a > \\ \{x = a \vee x = a + b \vee x = a + c \vee x = a + b + c\} \end{array}$$

Mediante el axioma de asignación, tenemos que:

$$\begin{aligned} & \{x = a \vee x = a + b \vee x = a + c \vee x = a + b + c\}_{x+a}^a < x = x + a > \\ & \{x = a \vee x = a + b \vee x = a + c \vee x = a + b + c\} \end{aligned}$$

No obstante, de la definición de Sustitución Textual, tenemos:

$$\begin{aligned} & \{x = a \vee x = a + b \vee x = a + c \vee x = a + b + c\}_{x+a}^a \equiv \\ & \equiv \{x + a = a \vee x + a = a + b \vee x + a = a + c \vee x + a = a + b + c\} \equiv \\ & \equiv \{x = 0 \vee x = b \vee x = c \vee x = b + c\} \end{aligned}$$

Por tanto, el triple en cuestión es cierto.

2. El correspondiente a la segunda instrucción atómica:

$$\begin{aligned} & \{x = 0 \vee x = a \vee x = c \vee x = a + c\} < x = x + b > \\ & \{x = b \vee x = a + b \vee x = b + c \vee x = a + b + c\} \end{aligned}$$

Es cierto, y su demostración es análoga al primer caso.

3. El correspondiente a la tercera instrucción atómica:

$$\begin{aligned} & \{x = 0 \vee x = b \vee x = a \vee x = a + b\} < x = x + c > \\ & \{x = c \vee x = a + c \vee x = b + c \vee x = a + b + c\} \end{aligned}$$

Es cierto, y su demostración es análoga al primer caso.

Seguidamente, tenemos que ver que dichos 3 triples están libres de interferencias. Para ello, hemos de probar 12 triples, ya que hay 3 instrucciones atómicas, cada una de ellas con 2 asertos, por lo que por cada instrucción hemos de comprobar 4 asertos:

$$\begin{aligned} & NI(x = 0 \vee x = a \vee x = c \vee x = a + c, < x = x + a >) \\ & NI(x = b \vee x = a + b \vee x = b + c \vee x = a + b + c, < x = x + a >) \\ & NI(x = 0 \vee x = b \vee x = a \vee x = a + b, < x = x + a >) \\ & NI(x = c \vee x = a + c \vee x = b + c \vee x = a + b + c, < x = x + a >) \end{aligned}$$

$$\begin{aligned} & NI(x = 0 \vee x = b \vee x = c \vee x = b + c, < x = x + b >) \\ & NI(x = a \vee x = a + b \vee x = a + c \vee x = a + b + c, < x = x + b >) \\ & NI(x = 0 \vee x = b \vee x = a \vee x = a + b, < x = x + b >) \\ & NI(x = c \vee x = a + c \vee x = b + c \vee x = a + b + c, < x = x + b >) \end{aligned}$$

$$\begin{aligned} & NI(x = 0 \vee x = b \vee x = c \vee x = b + c, < x = x + c >) \\ & NI(x = a \vee x = a + b \vee x = a + c \vee x = a + b + c, < x = x + c >) \\ & NI(x = 0 \vee x = a \vee x = c \vee x = a + c, < x = x + c >) \\ & NI(x = b \vee x = a + b \vee x = b + c \vee x = a + b + c, < x = x + c >) \end{aligned}$$

Demostremos ahora el primero, ya que el resto son idénticos.

$$\begin{aligned}
NI(x = 0 \vee x = a \vee x = c \vee x = a + c, < x = x + a >) &\equiv \\
&\equiv \{(x = 0 \vee x = a \vee x = c \vee x = a + c) \wedge (x = 0 \vee x = b \vee x = c \vee x = b + c)\} \\
&\quad < x = x + a > \{x = 0 \vee x = a \vee x = c \vee x = a + c\} \equiv \\
&\equiv \{x = 0 \vee x = c\} < x = x + a > \{x = 0 \vee x = a \vee x = c \vee x = a + c\}
\end{aligned}$$

Este triple efectivamente es cierto, lo cual se puede demostrar empleando en primer lugar el Axioma de Sustitución y, posteriormente, la primera regla de la consecuencia.

Por tanto, y tras aplicar la Regla de la Composición Concurrente, tenemos de forma directa que:

$$\begin{aligned}
&\{x = 0\} \\
&\text{cobegin} \\
&< x = x + a > \parallel < x = x + b > \parallel < x = x + c > \\
&\text{coend} \\
&\{x = a + b + c\}
\end{aligned}$$

**Ejercicio 3.1.17.** El siguiente triple:

$$\begin{aligned}
&\{x = 0 \wedge y = 0 \wedge z = 0\} \\
&< x = z + a > \parallel < y = x + b > \\
&\{(x = a) \wedge (y = b \vee y = a + b) \wedge z = 0\}
\end{aligned}$$

- (a) Es indemostrable salvo que se cumpla siempre que  $a = 0$ .
- (b) El triple anterior es demostrable para cualquier valor de las variables  $a$  o  $b$ .
- (c) Es indemostrable salvo que se cumpla siempre que  $b = 0$ .
- (d) Es indemostrable salvo que se cumpla siempre que  $a = 0 \wedge b = 0$ .

Veamos si podemos demostrarlo. Para ello, notamos cada instrucción atómica de la siguiente forma:

$$\begin{aligned}
S_1 &= < x = z + a > \\
S_2 &= < y = x + b >
\end{aligned}$$

Veamos cuál ha de ser la precondition de cada instrucción atómica:

$$\begin{aligned}
P_1 &= x = 0 \wedge (y = 0 \vee y = b) \wedge z = 0 \\
P_2 &= (x = 0 \vee x = a) \wedge y = 0 \wedge z = 0
\end{aligned}$$

Veamos cuál ha de ser la poscondición de cada instrucción atómica:

$$\begin{aligned}
Q_1 &= x = a \wedge (y = 0 \vee y = b) \wedge z = 0 \\
Q_2 &= [(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0
\end{aligned}$$

Vemos por tanto que ambos triples son ciertos:

1.  $\{P_1\}S_1\{Q_1\}$ 

De la definición de Sustitución Textual, tenemos que:

$$\begin{aligned} \{x = a \wedge (y = 0 \vee y = b) \wedge z = 0\}_{z+a}^x &\equiv \{z + a = a \wedge (y = 0 \vee y = b) \wedge z = 0\} \equiv \\ &\equiv \{(y = 0 \vee y = b) \wedge z = 0\} \end{aligned}$$

Por tanto, del Axioma de Asignación, tenemos que:

$$\{(y = 0 \vee y = b) \wedge z = 0\} < x = z + a > \{x = a \wedge (y = 0 \vee y = b) \wedge z = 0\}$$

Finalmente, usando la segunda regla de la consecuencia, como se tiene que  $\{P_1\} \rightarrow \{(y = 0 \vee y = b) \wedge z = 0\}$ , tenemos que el triple es cierto.

2.  $\{P_2\}S_2\{Q_2\}$ 

De la definición de Sustitución Textual, tenemos que:

$$\begin{aligned} \{[(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0\}_{x+b}^y &\equiv \\ \equiv \{[(x = 0 \wedge x + b = b) \vee (x = a \wedge x + b = a + b)] \wedge z = 0\} &\equiv \\ \equiv \{(x = 0 \vee x = a) \wedge z = 0\} \end{aligned}$$

Por tanto, del Axioma de Asignación, tenemos que:

$$\begin{aligned} \{(x = 0 \vee x = a) \wedge z = 0\} < y = x + b > \\ \{[(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0\} \end{aligned}$$

Por tanto, usando la segunda regla de la consecuencia, como se tiene que  $\{P_2\} \rightarrow \{(x = 0 \vee x = a) \wedge z = 0\}$ , tenemos que el triple es cierto.

Veamos ahora que no interfieren entre sí. Como tenemos dos instrucciones atómicas, cada una con dos asertos, hemos de comprobar 4 asertos:

$$\begin{aligned} NI(P_2, S_1) &\equiv \{P_1 \wedge P_2\}S_1\{P_2\} \\ NI(Q_2, S_1) &\equiv \{P_1 \wedge Q_2\}S_1\{Q_2\} \\ NI(P_1, S_2) &\equiv \{P_2 \wedge P_1\}S_2\{P_1\} \\ NI(Q_1, S_2) &\equiv \{P_2 \wedge Q_1\}S_2\{Q_1\} \end{aligned}$$

Veamos por tanto en qué queda cada uno de ellos:

$$\begin{aligned} NI(P_2, S_1) &\equiv \{x = 0 \wedge y = 0 \wedge z = 0\} < x = z + a > \{(x = 0 \vee x = a) \wedge y = 0 \wedge z = 0\} \\ NI(Q_2, S_1) &\equiv \{x = 0 \wedge y = b \wedge z = 0\} < x = z + a > \\ &\quad \{[(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0\} \\ NI(P_1, S_2) &\equiv \{x = 0 \wedge y = 0 \wedge z = 0\} < y = x + b > \{x = 0 \wedge (y = 0 \vee y = b) \wedge z = 0\} \\ NI(Q_1, S_2) &\equiv \{x = a \wedge y = 0 \wedge z = 0\} < y = x + b > \{x = a \wedge (y = 0 \vee y = b) \wedge z = 0\} \end{aligned}$$

Intentemos demostrar el segundo. Usando la definición de Sustitución Textual, tenemos que:



$$\begin{aligned}
\{[(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0\}_{z+a}^x &\equiv \\
&\equiv \{[(z + a = 0 \wedge y = b) \vee (z + a = a \wedge y = a + b)] \wedge z = 0\} \equiv \\
&\equiv \{y = a + b \wedge z = 0\}
\end{aligned}$$

Por tanto, del Axioma de Asignación, tenemos que:

$$\{y = a + b \wedge z = 0\} < x = z + a > \{[(x = 0 \wedge y = b) \vee (x = a \wedge y = a + b)] \wedge z = 0\}$$

No obstante, de forma general, tenemos que  $\{x = 0 \wedge y = b \wedge z = 0\} \not\rightarrow \{y = a + b \wedge z = 0\}$ , por lo que  $NI(Q_2, S_1)$  no es demostrable. No obstante, si  $a = 0$ , entonces sí que sería demostrable. Supongamos por tanto a partir de ahora que  $\underline{a = 0}$ .

Intentemos ahora demostrar el cuarto. Usando la definición de Sustitución Textual, tenemos que:

$$\begin{aligned}
\{x = a \wedge (y = 0 \vee y = b) \wedge z = 0\}_{x+b}^y &\equiv \\
&\equiv \{x = a \wedge (x + b = 0 \vee x + b = b) \wedge z = 0\} \equiv \\
&\equiv \{x = a \wedge (x = -b \vee x = 0) \wedge z = 0\} \equiv \{x = 0 \wedge z = 0\}
\end{aligned}$$

donde en la última igualdad hemos usado que  $\underline{a = 0}$ . Por tanto, del Axioma de Asignación, tenemos que:

$$\{x = 0 \wedge z = 0\} < y = x + b > \{x = a \wedge (y = 0 \vee y = b) \wedge z = 0\}$$

Además, como  $\underline{a = 0}$ , tenemos que  $\{x = 0 \wedge z = 0\} \rightarrow \{x = a \wedge y = 0 \wedge z = 0\}$ , tenemos que es cierto. Por tanto,  $NI(P_1, S_2)$  es demostrable.

Los otros dos triples son análogamente ciertos, por lo que podemos aplicar la regla de la composición concurrente y llegar al siguiente triple:

$$\begin{aligned}
&\{x = 0 \wedge y = 0 \wedge z = 0\} \\
&< x = z + a > || < y = x + b > \\
&\{x = a \wedge y = a + b \wedge z = 0\}
\end{aligned}$$

Este es el triple que queríamos demostrar, suponiendo que  $\underline{a = 0}$ . Por tanto, la respuesta correcta es la **a)**, ya que no es demostrable salvo que se cumpla siempre que  $a = 0$ .

**Ejercicio 3.1.18.** Suponer que  $\{suma > 1\} \text{ suma} = \text{suma} + 4 \{suma > 5\}$  es demostrable, entonces: ¿cuál de los siguientes triples es también demostrable? (indicar por qué)

1.  $\{suma > 2\} \text{ suma} = \text{suma} + 4 \{suma > 5\}$ .  
Es demostrable, ya que  $\{suma > 2\} \rightarrow \{suma > 1\}$  y podemos aplicar la segunda regla de la consecuencia.
2.  $\{suma \geq 1\} \text{ suma} = \text{suma} + 4 \{suma > 5\}$ .  
No es demostrable, ya que debilita la precondition.
3.  $\{suma > 0\} \text{ suma} = \text{suma} + 4 \{suma > 5\}$ .  
No es demostrable, ya que debilita la precondition.

4.  $\{suma > 1\} \text{ suma} = \text{suma} + 4 \{suma > 6\}$ .

No es demostrable, ya que fortalece la poscondición.

**Ejercicio 3.1.19.** Suponer que  $\{x < y\} C_1 \{u < v\}$  es demostrable, entonces: ¿cuáles de los siguientes triples son también demostrables? (indicar por qué)

1.  $\{x \leq y\} C_1 \{u < v\}$ .

No es demostrable, ya que debilita la precondition.

2.  $\{x \leq y - 2\} C_1 \{u < v\}$ .

Es demostrable, ya que  $\{x \leq y - 2\} \rightarrow \{x + 2 \leq y\} \rightarrow \{x < y\}$ , y mediante la segunda regla de la consecuencia se tiene que es cierto.

3.  $\{x \leq y\} C_1 \{u \leq v\}$ .

El triple  $\{x < y\} C_1 \{u \leq v\}$  sí que es demostrable ya que relaja la poscondición, pero el triple que se nos dice no es demostrable, ya que también relaja la precondition. Como además no tenemos relación entre  $x$  y  $u$  ni entre  $y$  y  $v$ , no podemos inferir nada.

4.  $\{x < y\} C_1 \{u < v - 2\}$ .

No es demostrable, ya que fortalecemos la poscondición.

**Ejercicio 3.1.20.** Seleccionar el valor correcto de las 2 variables ( $x$  e  $y$ ) después de ejecutarse el siguiente programa concurrente:

```
1  int x=5, y=2;
    cobegin <x=x+y>; <y=x*y>; <x=x-y>; coend;
```

(a)  $x = 7$  y  $y = 14$ .

(b)  $x = 5$  y  $y = 10$ .

(c)  $x = -7$  y  $y = 14$ .

(d)  $x = -3$  y  $y = 10$ .

Numeramos las instrucciones atómicas de la siguiente forma:

1.  $\langle x=x+y \rangle$

2.  $\langle y=x*y \rangle$

3.  $\langle x=x-y \rangle$

Veamos ahora, en función del orden de ejecución, cuál sería el valor de las variables  $x$  e  $y$ :

■ 1, 2, 3:  $x = -7$  y  $y = 14$ .

■ 1, 3, 2:  $x = 5$  y  $y = 10$ .

■ 3, 1, 2:  $x = 5$  y  $y = 10$ .

- 2, 1, 3:  $x = 5$  y  $y = 10$ .
- 2, 3, 1:  $x = 5$  y  $y = 10$ .
- 3, 2, 1:  $x = 9$  y  $y = 6$ .

Por tanto, las respuestas  $b$  y  $c$  son correctas.

**Ejercicio 3.1.21.** El siguiente código concurrente no puede ser demostrado directamente con la lógica de aserciones (pre y poscondiciones). Elegir la respuesta que explica correctamente la razón de que ocurra esto.

```
1 {x=0} cobegin <x=x+a>; <x=x+a> coend; {x=2*a}
(a es un valor entero positivo)
```

- (a) Porque la poscondición que se propone  $\{x = 2 * a\}$  es falsa.
- (b) Porque falta incluir la posibilidad de que el valor final de  $x$  sea también  $\{x = a\}$ .
- (c) Porque al aplicar directamente la regla de inferencia de la *composición concurrente* utilizo unas condiciones (pre y post-condiciones) demasiado débiles.
- (d) Porque tengo que incluir en los asertos el valor del contador de programa de cada procesador.

Notamos cada instrucción atómica de la siguiente forma:

$$S_1 = S_2 = \langle x = x + a \rangle$$

Veamos cuál ha de ser la precondition de cada instrucción atómica:

$$P_1 = P_2 = x = 0 \vee x = a$$

Veamos cuál ha de ser la poscondición de cada instrucción atómica:

$$Q_1 = Q_2 = x = a \vee x = 2a$$

Veamos ahora que cada triple es cierto. Como son los mismos, hemos de demostrar:

$$\{x = 0 \vee x = a\} \langle x = x + a \rangle \{x = a \vee x = 2a\}$$

Este se demuestra de forma directa. Además, también hemos de demostrar que no interfieren entre sí. Tenemos que demostrar:

$$\begin{aligned} NI(P_1, S_2) &\equiv \{x = 0 \vee x = a\} \langle x = x + a \rangle \{x = 0 \vee x = a\} \\ NI(Q_1, S_2) &\equiv \{x = a\} \langle x = x + a \rangle \{x = a \vee x = 2a\} \end{aligned}$$

Estos también son ciertos, por lo que podemos aplicar la regla de la composición concurrente y llegar al siguiente triple:

$$\{x = 0 \vee x = a\} \text{cobegin } \langle x = x + a \rangle; \langle x = x + a \rangle \text{coend}; \{x = a \vee x = 2a\}$$

Por la primera regla de la consecuencia, podemos debilitar la precondition, llegando al siguiente triple:

$$\{x = 0\} \text{cobegin } \langle x = x + a \rangle; \langle x = x + a \rangle \text{coend}; \{x = a \vee x = 2a\}$$

No obstante, la poscondición no se puede debilitar, por lo que la respuesta correcta es la **b)**, ya que falta incluir en los asertos el valor final de  $x$  sea también  $\{x = a\}$ .

**Ejercicio 3.1.22.** Estudiar cuáles son los valores finales de las variables  $x$  e  $y$  en el siguiente programa. Insertar los asertos adecuados entre llaves, antes y después de cada sentencia, para poder obtener una traza de demostración del programa, que incluya en su último aserto los valores finales de las variables.

```
1  int x = c1;
   int y = c2;
   x = x + y;
   y = x * y;
5  x = x - y;
```

Tenemos que cada triple, por orden, es:

$$\begin{aligned} & \{x = c_1 \wedge y = c_2\} \\ & \quad x = x + y \\ & \{x = c_1 + c_2 \wedge y = c_2\} \\ & \quad y = x * y \\ & \{x = c_1 + c_2 \wedge y = (c_1 + c_2) \cdot c_2\} \\ & \quad x = x - y \\ & \{x = (c_1 + c_2) - (c_1 + c_2) \cdot c_2 = (c_1 + c_2) \cdot (1 - c_2) \wedge y = (c_1 + c_2) \cdot c_2\} \end{aligned}$$

**Ejercicio 3.1.23.** Demostrar que el siguiente triple es cierto:

$$\begin{aligned} & \{x = 0\} \\ & \text{cobegin} \\ & \quad \langle x = x + 1 \rangle \parallel \langle x = x + 2 \rangle \parallel \langle x = x + 4 \rangle \\ & \text{coend} \\ & \{x = 7\} \end{aligned}$$

Notamos cada instrucción atómica de la siguiente forma:

$$\begin{aligned} S_1 &= \langle x = x + 1 \rangle \\ S_2 &= \langle x = x + 2 \rangle \\ S_3 &= \langle x = x + 4 \rangle \end{aligned}$$

Veamos cuál ha de ser la precondition de cada instrucción atómica:

$$\begin{aligned} P_1 &= x = 0 \vee x = 2 \vee x = 4 \vee x = 6 \\ P_2 &= x = 0 \vee x = 1 \vee x = 4 \vee x = 5 \\ P_3 &= x = 0 \vee x = 1 \vee x = 2 \vee x = 3 \end{aligned}$$

Veamos cuál ha de ser la poscondición de cada instrucción atómica:

$$Q_1 = x = 1 \vee x = 3 \vee x = 5 \vee x = 7$$

$$Q_2 = x = 2 \vee x = 3 \vee x = 6 \vee x = 7$$

$$Q_3 = x = 4 \vee x = 5 \vee x = 6 \vee x = 7$$

Cada triple es directamente cierto por el Axioma de Asignación. Veamos ahora que no interfieren entre sí. Tenemos que demostrar:

$$NI(P_2, S_1) \equiv \{x = 0 \vee x = 4\} < x = x + 1 > \{x = 0 \vee x = 1 \vee x = 4 \vee x = 5\}$$

$$NI(Q_2, S_1) \equiv \{x = 2 \vee x = 6\} < x = x + 1 > \{x = 2 \vee x = 3 \vee x = 6 \vee x = 7\}$$

$$NI(P_3, S_1) \equiv \{x = 0 \vee x = 2\} < x = x + 1 > \{x = 0 \vee x = 1 \vee x = 2 \vee x = 3\}$$

$$NI(Q_3, S_1) \equiv \{x = 4 \vee x = 6\} < x = x + 1 > \{x = 4 \vee x = 5 \vee x = 6 \vee x = 7\}$$

$$NI(P_1, S_2) \equiv \{x = 0 \vee x = 4\} < x = x + 2 > \{x = 0 \vee x = 2 \vee x = 4 \vee x = 6\}$$

$$NI(Q_1, S_2) \equiv \{x = 1 \vee x = 5\} < x = x + 2 > \{x = 1 \vee x = 3 \vee x = 5 \vee x = 7\}$$

$$NI(P_3, S_2) \equiv \{x = 0 \vee x = 1\} < x = x + 2 > \{x = 0 \vee x = 1 \vee x = 2 \vee x = 3\}$$

$$NI(Q_3, S_2) \equiv \{x = 4 \vee x = 5\} < x = x + 2 > \{x = 4 \vee x = 5 \vee x = 6 \vee x = 7\}$$

$$NI(P_1, S_3) \equiv \{x = 0 \vee x = 2\} < x = x + 4 > \{x = 0 \vee x = 2 \vee x = 4 \vee x = 6\}$$

$$NI(Q_1, S_3) \equiv \{x = 1 \vee x = 3\} < x = x + 4 > \{x = 1 \vee x = 3 \vee x = 5 \vee x = 7\}$$

$$NI(P_2, S_3) \equiv \{x = 0 \vee x = 1\} < x = x + 4 > \{x = 0 \vee x = 1 \vee x = 4 \vee x = 5\}$$

$$NI(Q_2, S_3) \equiv \{x = 2 \vee x = 3\} < x = x + 4 > \{x = 2 \vee x = 3 \vee x = 6 \vee x = 7\}$$

Todos estos son ciertos, por lo que podemos aplicar la regla de la composición concurrente y llegar al siguiente triple:

$$\begin{array}{c} \{x = 0\} \\ \text{cobegin} \\ < x = x + 1 > \parallel < x = x + 2 > \parallel < x = x + 4 > \\ \text{coend} \\ \{x = 7\} \end{array}$$

**Ejercicio 3.1.24.** Dada la siguiente construcción de composición concurrente P:

$$\begin{array}{c} \text{cobegin} \\ < x = x - 1 >; < x = x + 1 >; \parallel < y = y - 1 >; < y = y + 1 >; \\ \text{coend} \end{array}$$

demostrar que se cumple la invarianza de  $\{x = y\}$ , es decir, que  $\{x = y\} P \{x = y\}$  es un triple cierto.

Para ello, comenzamos demostrando los siguientes triples (se ha de mantener la invarianza en el código secuencial)

$$\{x = y\} \ x = x - 1; x = x + 1; \{x = y\}$$

$$\{x = y\} \ y = y - 1; y = y + 1; \{x = y\}$$

1. Respecto al primero, tenemos que los siguientes triples son ciertos:

$$\begin{array}{l} \{x = y\} \ x = x - 1 \ \{x + 1 = y\} \\ \{x + 1 = y\} \ x = x + 1 \ \{x = y\} \end{array}$$

Usando la regla de la composición, se tiene.

2. Respecto al segundo, tenemos que los siguientes triples son ciertos:

$$\begin{array}{l} \{y = x\} \ y = y - 1 \ \{y + 1 = x\} \\ \{y + 1 = x\} \ y = y + 1 \ \{y = x\} \end{array}$$

Usando la regla de la composición, se tiene.

Ahora, los triples son libres de interferencia por tener variables disjuntas. Podemos aplicar por tanto la regla de la composición concurrente, llegando a lo que queríamos probar:

$$\begin{array}{c} \{x = y\} \\ \text{cobegin} \\ < x = x - 1 >; < x = x + 1 >; || < y = y - 1 >; < y = y + 1 >; \\ \text{coend} \\ \{x = y\} \end{array}$$

**Ejercicio 3.1.25.** Usando la regla de la conjunción, demostrar que

$$\{i > 2\} \quad i = 2 * i \quad \{i > 4\}$$

**Ejercicio 3.1.26.** Se dan los siguientes triples de Hoare:

$$\begin{array}{l} \{j > 1\} \ i = i + 2; \ j = j + 3; \ \{j > 4\} \\ \{i > 2\} \ i = i + 2; \ j = j + 3; \ \{i > 4\} \end{array}$$

Demostrar que estos triples implican que

$$\{j > 1 \wedge i > 2\} \ i = i + 2; \ j = j + 3 \ \{j > 4 \wedge i > 4\}$$

¿Qué regla se debe utilizar para la demostración?

**Ejercicio 3.1.27.** Sean  $A$  y  $B$  los valores iniciales de  $a$  y  $b$  respectivamente. Escribir un fragmento de código que tenga  $\{a = A + B \wedge b = A - B\}$  como poscondición y demostrar que el código es correcto.

En este caso, nos piden un código  $C$  que cumpla:

$$\{a = A \wedge b = B\} C \{a = A + B \wedge b = A - B\}$$

Sea  $C = \langle a = a + b; b = a - 2b \rangle$ . Buscamos entonces demostrar los siguientes triples:

$$\begin{aligned} & \{a = A \wedge b = B\} a = a + b \{a = A + B \wedge b = B\} \\ & \{a = A + B \wedge b = B\} b = a - 2b \{a = A + B \wedge b = A - B\} \end{aligned}$$

Demostramos cada uno por separado:

1. Usando el axioma de asignación:

$$\begin{aligned} \{a = A + B \wedge b = B\}_{a+b}^a &\equiv \{a + b = A + B \wedge b = B\} \equiv \\ &\equiv \{a = A \wedge b = B\} a = a + b \{a = A + B \wedge b = B\} \end{aligned}$$

2. Usando el axioma de asignación:

$$\begin{aligned} \{a = A + B \wedge b = A - B\}_{a-2b}^b &\equiv \{a = A + B \wedge a - 2b = A - B\} \equiv \\ &\equiv \{a = A + B \wedge A + B - 2b = A - B\} \equiv \\ &\equiv \{a = A + B \wedge b = B\} b = a - 2b \{a = A + B \wedge b = A - B\} \end{aligned}$$

Usando la regla de la composición, tenemos que el código es correcto.

**Ejercicio 3.1.28.** Demostrar que la siguiente sentencia tiene la poscondición  $\{x \geq 0, x^2 \geq a^2\}$ .  
if  $a > 0$  then  $x = a$  else  $x = -a$ . Es decir, probar el triple:

$$\{V\} \text{ if } a > 0 \text{ then } x = a \text{ else } x = -a \{x \geq 0, x^2 \geq a^2\}$$

Para ello, tenemos que usar la regla del if:

$$\frac{\{P \wedge B\} S_1 \{Q\}, \{P \wedge \neg B\} S_2 \{Q\}}{\{P\} \text{ if } B \text{ then } S_1 \text{ else } S_2 \{Q\}}$$

Luego bastará con probar los triples

$$\begin{aligned} \{a > 0\} &\equiv \{V \wedge a > 0\} x = a \{x \geq 0 \wedge x^2 \geq a^2\} \\ \{a \leq 0\} &\equiv \{V \wedge a \leq 0\} x = -a \{x \geq 0 \wedge x^2 \geq a^2\} \end{aligned}$$

1. Usando el axioma de asignación:

$$\{a \geq 0\} \equiv \{a \geq 0 \wedge a^2 \geq a^2\} \equiv \{x \geq 0 \wedge x^2 \geq a^2\}_a^x x = a \{x \geq 0 \wedge x^2 \geq a^2\}$$

Como  $\{a > 0\} \rightarrow \{a \geq 0\}$ , usamos la segunda regla de la consecuencia y tenemos el primer triple demostrado.

2. Usando el axioma de asignación:

$$\{a \leq 0\} \equiv \{-a \geq 0 \wedge a^2 \geq a^2\} \equiv \{x \geq 0 \wedge x^2 \geq a^2\}_{-a}^x x = -a \{x \geq 0 \wedge x^2 \geq a^2\}$$

Y acabamos de probar el triple que nos pedía el ejercicio.

**Ejercicio 3.1.29.** El siguiente fragmento de código tiene  $\{P\} \equiv \left\{sum = \frac{j(j-1)}{2}\right\}$  como precondition y poscondition. Demostrar que es verdadero:

$$\{P\} \quad sum = sum + j; \quad j = j + 1; \quad \{P\}$$

Queremos demostrar el triple:

$$\left\{sum = \frac{j(j-1)}{2}\right\} \quad sum = sum + j; \quad j = j + 1; \quad \left\{sum = \frac{j(j-1)}{2}\right\}$$

Para ello, será suficiente con demostrar los triples

$$\begin{aligned} &\left\{sum = \frac{j(j-1)}{2}\right\} \quad sum = sum + j; \quad \left\{sum = \frac{(j+1)j}{2}\right\} \\ &\left\{sum = \frac{(j+1)j}{2}\right\} \quad j = j + 1; \quad \left\{sum = \frac{j(j-1)}{2}\right\} \end{aligned}$$

y aplicar la regla de composición.

1. Para demostrar el primer triple, usamos el axioma de asignación:

$$\left\{sum = \frac{(j+1)j}{2}\right\} \xrightarrow[sum+j]{sum} sum = sum + j; \quad \left\{sum = \frac{(j+1)j}{2}\right\}$$

Usando la definición de Sustitución Textual, tenemos que:

$$\begin{aligned} &\left\{sum = \frac{(j+1)j}{2}\right\} \xrightarrow[sum+j]{sum} sum = sum + j; \quad \left\{sum = \frac{(j+1)j}{2}\right\} \equiv \\ &\equiv \left\{sum = \frac{(j+1)j}{2} - j\right\} \equiv \left\{sum = \frac{j(j-1)}{2}\right\} \end{aligned}$$

2. Para el segundo, usamos también el axioma de asignación:

$$\left\{sum = \frac{j(j-1)}{2}\right\} \xrightarrow{j+1} j = j + 1; \quad \left\{sum = \frac{j(j-1)}{2}\right\}$$

Usando de nuevo la definición de Sustitución Textual, tenemos que:

$$\left\{sum = \frac{j(j-1)}{2}\right\} \xrightarrow{j+1} j = j + 1; \quad \left\{sum = \frac{j(j-1)}{2}\right\} \equiv \left\{sum = \frac{(j+1)(j+1-1)}{2}\right\} \equiv \left\{sum = \frac{(j+1)j}{2}\right\}$$

Por lo que el triple del enunciado es cierto.

**Ejercicio 3.1.30.** Demostrar que

$$\{i * j + 2 * j + 3 * i = 0\} \quad j = j + 3; \quad i = i + 2; \quad \{i * j = 6\}$$



Vamos buscando aplicar la regla de la composición. Para ello, y como desconocemos el estado intermedio por el que debemos pasar, usamos directamente la Sustitución Textual al final, para así obtener la precondition del segundo triple.

$$\{i * j = 6\}_{i+2}^i \equiv \{(i+2) * j = 6\} \equiv \{i * j + 2 * j = 6\} \equiv \{j * (i+2) = 6\}$$

Usando esa precondition, el segundo libre se demuestra directamente con el axioma de asignación. Demostramos ahora el primer triple:

$$\{i * j + 2 * j + 3 * i = 0\} \quad j = j + 3; \quad \{j * (i+2) = 6\}$$

Usando la sustitución textual, tenemos que:

$$\begin{aligned} \{j * (i+2) = 6\}_{j+3}^j &\equiv \{(j+3) * (i+2) = 6\} \equiv \{j * (i+2) + 3 * (i+2) = 6\} \equiv \\ &\equiv \{i * j + 2 * j + 3 * i = 0\} \end{aligned}$$

Por lo que, tras usar la regla de la composición, vemos que el triple del enunciado es cierto.

**Ejercicio 3.1.31.** ¿Por qué en la regla del **while** B, la condición B debe ser verdadera al comienzo del bucle?

**Ejercicio 3.1.32.** Considerar una función con dos argumentos que se usa en un programa. Explicar por qué el uso de alias puede ser un problema en este caso.

**Ejercicio 3.1.33.** Demostrar la corrección parcial del siguiente fragmento de programa:

```

1  sum := 0; j := 1;
   while j <> c do begin {<> es !=}
       sum := sum + j;
       j := j + 1;
5  end
   {sum = c*(c-1)/2}
```

Para ello, tenemos que hacer uso de la regla de la iteración:

$$\frac{\{I \wedge B\} S \{I\}}{\{I\} \text{ while } B \text{ do } S \text{ end do } \{I \wedge \neg B\}}$$

Identificando términos, sean:

$$\begin{aligned} I &\equiv \text{sum} = \frac{j(j-1)}{2} \\ B &\equiv j \neq c \\ S &\equiv \text{sum} = \text{sum} + j; \quad j = j + 1 \end{aligned}$$

Luego tendremos que probar que se cumple el triple

$$\left\{ \text{sum} = \frac{j(j-1)}{2} \wedge j \neq c \right\} \quad \text{sum} = \text{sum} + j; j = j + 1; \quad \left\{ \text{sum} = \frac{j(j-1)}{2} \right\}$$

Para ello, será suficiente con demostrar los triples

$$\left\{ \text{sum} = \frac{j(j-1)}{2} \wedge j \neq c \right\} \text{sum} = \text{sum} + j; \left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\}$$

$$\left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\} j = j + 1; \left\{ \text{sum} = \frac{j(j-1)}{2} \right\}$$

y aplicar la regla de composición.

1. Para demostrar el primer triple, usamos el axioma de asignación:

$$\left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\}_{\text{sum}+j}^{\text{sum}} \text{sum} = \text{sum} + j; \left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\}$$

$$\left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\}_{\text{sum}+j}^{\text{sum}} \equiv \left\{ \text{sum} + j = \frac{(j+1)j}{2} \wedge j \neq c \right\} \equiv$$

$$\equiv \left\{ \text{sum} = \frac{(j+1)j}{2} - j \wedge j \neq c \right\} \equiv \left\{ \text{sum} = \frac{j(j-1)}{2} \wedge j \neq c \right\}$$

2. Para el segundo, usamos también el axioma de asignación:

$$\left\{ \text{sum} = \frac{j(j-1)}{2} \right\}_{j+1}^j j = j + 1; \left\{ \text{sum} = \frac{j(j-1)}{2} \right\}$$

$$\left\{ \text{sum} = \frac{j(j-1)}{2} \right\}_{j+1}^j \equiv \left\{ \text{sum} = \frac{(j+1)(j+1-1)}{2} \right\} \equiv \left\{ \text{sum} = \frac{(j+1)j}{2} \right\}$$

Además, tenemos que se tiene:

$$\left\{ \text{sum} = \frac{(j+1)j}{2} \wedge j \neq c \right\} \rightarrow \left\{ \text{sum} = \frac{(j+1)j}{2} \right\}$$

Por tanto, usando la segunda regla de la consecuencia, tenemos que el segundo triple es cierto.

Por tanto, mediante la regla de la iteración, tenemos que:

$$\left\{ \text{sum} = \frac{j(j-1)}{2} \right\} \text{ while } j <> c \text{ do begin sum := sum+j; j := j+1 end } \left\{ \text{sum} = \frac{c(c-1)}{2} \right\}$$

Como inicialmente  $j = 1$  y  $\text{sum} = 0$ , tenemos que este triple coincide con el enunciado del ejercicio.

**Ejercicio 3.1.34.** Demostrar la corrección del siguiente triple:

$$\{a[i] \geq 0\} a[i] = a[i] + a[j]; \{a[i] \geq a[j]\}$$

Para ello, basta aplicar el axioma de la asignación:

$$\{a[i] \geq a[j]\}_{a[i]+a[j]}^{a[i]} a[i] = a[i] + a[j]; \{a[i] \geq a[j]\}$$

$$\{a[i] \geq a[j]\}_{a[i]+a[j]}^{a[i]} \equiv \{a[i] + a[j] \geq a[j]\} \equiv \{a[i] \geq 0\}$$

**Ejercicio 3.1.35.** Verificar el siguiente segmento de programa:

$$\begin{aligned}
 &\{n \geq 0\} \\
 &\quad i = 1; \\
 &\textbf{while } i \leq n \textbf{ do begin} \\
 &\quad a[i] = b[i]; \\
 &\quad i = i + 1; \\
 &\quad \textbf{end} \\
 &\left\{ \bigwedge_{i=1}^n (a[i] = b[i]) \right\}
 \end{aligned}$$

Para ello, como tenemos que demostrar la corrección de un bucle, hemos de buscar un invariante global que nos lleve a la poscondición indicada. Queremos demostrar que el programa copia el vector **b** en el **a**, por lo que un invariante que puede servirnos es

$$\{I\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \right\}$$

Primero, comprobamos que el invariante es cierto antes de entrar al bucle, es decir:

$$\{n \geq 0\} \quad i = 1; \quad \{I\}$$

Lo cual es cierto, ya que

$$\begin{aligned}
 &\{n \geq 0\} \quad i = 1; \quad \{n \geq 0 \wedge i = 1\} \\
 &\{n \geq 0 \wedge i = 1\} \rightarrow \{i = 1\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \wedge i = 1 \right\} \rightarrow \{I\}
 \end{aligned}$$

Posteriormente, hemos de demostrar que  $\{I \wedge B\} \quad S \quad \{I\}$  con  $\{B\} \equiv \{i \leq n\}$  y  $S$  el cuerpo del bucle, para poder aplicar la regla de la iteración, que es lo que venimos buscando:

$$\begin{aligned}
 &\{I \wedge B\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \wedge i \leq n \right\} \\
 &\quad a[i] = b[i]; \\
 &\quad \left\{ \bigwedge_{j=1}^i (a[j] = b[j]) \wedge i \leq n \right\} \\
 &\quad i = i + 1; \\
 &\left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \wedge i \leq n + 1 \right\} \rightarrow \{I\}
 \end{aligned}$$

Por lo que podemos aplicar la regla de iteración, llegando a que

$$\begin{aligned} \{I\} &\equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \right\} \\ &\quad \text{while } i \leq n \text{ do begin} \\ &\quad \quad a[i] = b[i]; \\ &\quad \quad i = i + 1; \\ &\quad \text{end} \\ \{I \wedge \neg B\} &\equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \wedge i > n \right\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (a[j] = b[j]) \wedge i - 1 \geq n \right\} \rightarrow \left\{ \bigwedge_{j=1}^n (a[j] = b[j]) \right\} \end{aligned}$$

Y era lo que queríamos probar en este ejercicio.

**Ejercicio 3.1.36.** El siguiente fragmento de programa calcula  $\sum_{i=1}^n i!$ . Demostrar que es correcto.

```

1  i = 1; sum = 0; f = 1;
   while i <> n+1 do begin
       sum = sum + f;
       i = i + 1;
5    f = f * i;
   end

```

Para ello, usaremos la regla de iteración:

$$\frac{\{I \wedge B\} S \{I\}}{\{I\} \text{ while } B \text{ do begin } S \text{ end do } \{I \wedge \neg B\}}$$

Por lo que tenemos que buscar un invariante global  $I$  que nos permita concluir al final que el programa calcula  $\sum_{i=1}^n i!$ .

Observando el código, podemos ver que en **sum** va almacenando dicho número, mientras incrementa **i** en cada iteración y va calculando en **f** el factorial de **i**. Planteamos por tanto el siguiente invariante  $I$ :

$$\{I\} \equiv \left\{ sum = \sum_{j=1}^{i-1} j! \wedge f = i! \right\}$$

En primer lugar, demostramos el triple

$$\{V\} i = 1; sum = 0; f = 1; \{I\}$$

para comprobar que el invariante es cierto al inicio del programa. Lo cual tenemos, ya que:

$$\begin{aligned} \{V\} i = 1; sum = 0; f = 1; \{i = 1 \wedge sum = 0 \wedge f = 1\} \\ \{i = 1 \wedge sum = 0 \wedge f = 1\} \equiv \left\{ i = 1 \wedge f = 1! \wedge sum = \sum_{j=1}^0 j! = 0 \right\} \end{aligned}$$

A continuación, trataremos de probar el triple  $\{I \wedge B\} S \{I\}$ , para  $B \equiv \{i \neq n+1\}$  y  $S$  el cuerpo del bucle:

$$\begin{aligned}
\{I \wedge B\} &\equiv \left\{ \begin{aligned} &sum = \sum_{j=1}^{i-1} j! \wedge f = i! \wedge i \neq n+1 \\ &sum = sum + f; \\ &\left\{ sum = \left( \sum_{j=1}^{i-1} j! \right) + i! \wedge f = i! \wedge i \neq n+1 \right\} \equiv \left\{ sum = \sum_{j=1}^i j! \wedge f = i! \wedge i \neq n+1 \right\} \\ &i = i + 1; \\ &\left\{ sum = \sum_{j=1}^{i-1} j! \wedge f = (i-1)! \wedge i \neq n+2 \right\} \\ &f = f * i; \\ &\left\{ sum = \sum_{j=1}^{i-1} j! \wedge f = i \cdot (i-1)! \wedge i \neq n+2 \right\} \equiv \left\{ sum = \sum_{j=1}^{i-1} j! \wedge f = i! \wedge i \neq n+2 \right\} \rightarrow \{I\} \end{aligned} \right\}
\end{aligned}$$

Luego podemos aplicar la regla de iteración, para obtener finalmente que:

$$\begin{aligned}
\{I\} &\equiv \left\{ \begin{aligned} &sum = \sum_{j=1}^{i-1} j! \wedge f = i! \\ &\text{while } i \neq n+1 \text{ do begin} \\ &\quad sum = sum + f; \\ &\quad i = i + 1; \\ &\quad f = f * i; \\ &\text{end} \end{aligned} \right\} \\
\{I \wedge \neg B\} &\equiv \left\{ sum = \sum_{j=1}^{i-1} j! \wedge f = i! \wedge i = n+1 \right\} \rightarrow \left\{ sum = \sum_{j=1}^n j! \wedge f = (n+1)! \right\}
\end{aligned}$$

Si tomamos **sum** como la salida del programa, tenemos probado lo que queríamos.

**Ejercicio 3.1.37.** Hallar la precondition  $\{P\}$  que hace que el siguiente triple sea correcto:

$$\{P\} \ a[i] = 2 * b; \ \{j \leq i \ \wedge \ k < i \ \wedge \ a[i] + a[j-1] + a[k] > b\}$$

Para ello, basta aplicar el axioma de asignación:

$$\begin{aligned}
&\{j \leq i \ \wedge \ k < i \ \wedge \ a[i] + a[j-1] + a[k] > b\} \stackrel{a[i]}{2.b} a[i] = 2 * b; \\
&\{j \leq i \ \wedge \ k < i \ \wedge \ a[i] + a[j-1] + a[k] > b\}
\end{aligned}$$

Usando la definición de Sustitución Textual, tenemos que:

$$\begin{aligned}
&\{j \leq i \ \wedge \ k < i \ \wedge \ a[i] + a[j-1] + a[k] > b\} \stackrel{a[i]}{2.b} \equiv \\
&\equiv \{j \leq i \ \wedge \ k < i \ \wedge \ 2 \cdot b + a[j-1] + a[k] > b\} \equiv \\
&\equiv \{j \leq i \ \wedge \ k < i \ \wedge \ b + a[j-1] + a[k] > 0\}
\end{aligned}$$

Luego estamos buscando la precondition:

$$\{P\} \equiv \{j \leq i \wedge k < i \wedge b + a[j-1] + a[k] > 0\}$$

**Ejercicio 3.1.38.** Demostrar que para  $n > 0$  el siguiente fragmento de programa termina.

```

1  i = 1; f = 1;
   while i <> n do begin
       i = i + 1;
       f = f * r;
5  end

```

**Ejercicio 3.1.39.** Hallar la precondition de la terna:

$$\{P\} \ a[i] = b; \ \{a[j] = 2 * a[i]\}$$

Para ello, simplemente aplicamos el axioma de asignación:

$$\{a[j] = 2 * b\} \equiv \{a[j] = 2 * a[i]\}_b^{a[i]} \ a[i] = b; \ \{a[j] = 2 * a[i]\}$$

**Ejercicio 3.1.40.** Para cada uno de los siguientes fragmentos de código, obtener la poscondición apropiada:

1.  $\{i < 10\} \ i = 2 * i + 1;$ .  
La poscondición es  $\{i < 21\}$ :

$$\{i < 10\} \ i = 2 * i + 1; \ \{i < 21\}$$

que puede demostrarse aplicando el axioma de asignación.

2.  $\{i > 0\} \ i = i - 1;$ .  
La poscondición es  $\{i > -1\}$ :

$$\{i > 0\} \ i = i - 1; \ \{i > -1\}$$

que puede demostrarse aplicando el axioma de asignación.

3.  $\{i > j\} \ i = i + 1; \ j = j + 1;$ .  
La poscondición es  $\{i > j\}$ :

$$\begin{aligned} &\{i > j\} \ i = i + 1; \ \{i > j + 1\} \\ &\{i > j + 1\} \ j = j + 1; \ \{i > j\} \end{aligned}$$

Ambos pueden demostrarse aplicando el axioma de asignación y finalmente tenemos que:

$$\{i > j\} \ i = i + 1; \ j = j + 1; \ \{i > j\}$$

aplicando la regla de composición.

4.  $\{V\} \ i = 3; \ j = 2 * i.$   
La poscondición es  $\{i = 3 \wedge j = 6\}$ :

$$\begin{aligned} &\{V\} \ i = 3; \ \{i = 3\} \\ &\{i = 3\} \ j = 2 * i; \ \{i = 3 \wedge j = 6\} \end{aligned}$$

**Ejercicio 3.1.41.** Para cada uno de los siguientes fragmentos de código, obtener las precondiciones apropiadas.

1.  $i = 3 * k; \{i > 6\}$ .

Aplicando el axioma de asignación:

$$\{k > 2\} \equiv \{3 \cdot k > 6\} \equiv \{i > 6\}_{3 \cdot k}^i i = 3 * k; \{i > 6\}$$

obtenemos que la precondición es  $\{k > 2\}$ .

2.  $a = b * c; \{a = 1\}$ .

Aplicando el axioma de asignación:

$$\{b = c^{-1}\} \equiv \{b \cdot c = 1\} \equiv \{a = 1\}_{b \cdot c}^a a = b * c; \{a = 1\}$$

La precondición es  $\{b = c^{-1}\}$ .

3.  $b = c - 2; a = a/b;$ <sup>1</sup>

**Ejercicio 3.1.42.** Verificar el siguiente código. Indicar todas las reglas usadas.

$$\{y > 0\} \quad xa = x + y; \quad xb = x - y;$$

**Ejercicio 3.1.43.** Verificar el siguiente código, indicando todas las reglas usadas.

$$\{V\} \text{ if } x < 0 \text{ then } x = -x \{x \geq 0\}$$

Para comenzar, probamos que  $\{x < 0\} \quad x = -x; \{x \geq 0\}$  usando el axioma de asignación:

$$\{x < 0\} \equiv \{-x \geq 0\} \equiv \{x \geq 0\}_{-x}^x x = -x; \{x \geq 0\}$$

Posteriormente, como sabemos que  $\{V \wedge (x < 0)\} \equiv \{x < 0\}$  y que  $\{x \geq 0\} \text{ null } \{x \geq 0\}$  por el axioma de la sentencia nula, podemos aplicar la regla del **if**:

$$\frac{\{V \wedge (x < 0)\} \quad x = -x; \{x \geq 0\}, \{V \wedge x \geq 0\} \text{ null } \{x \geq 0\}}{\{V\} \text{ if } x < 0 \text{ then } x = -x \text{ else null } \{x \geq 0\}}$$

**Ejercicio 3.1.44.** Verificar el siguiente segmento de programa:

```

max = a[1]; i = 1;
while i <> n + 1 do begin
  if a[i] ≥ max then max = a[i];
  i = i + 1;
end
{
  ⋀_{i=1}^n (max ≥ a[i])
}
```

Es decir, tenemos que probar que el código anterior calcula el máximo del vector **a** de longitud **n** (sin tener en cuenta el valor **a[0]**), que se almacena en **max**. Al tratarse

<sup>1</sup>Esto es lo que pone en la relación, falta la poscondición para poder hacerse.

de un bucle, hemos de buscar un invariante global para poder aplicar la regla de iteración. El invariante global que usamos<sup>2</sup> es el siguiente:

$$\{I\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \right\}$$

Para comenzar, hemos de ver que el invariante es cierto al inicio del programa, es decir, que:

$$\{V\} \quad max = a[1]; \quad i = 1; \quad \{I\}$$

Lo cual es cierto, ya que:

$$\{V\} \quad max = a[1]; \quad i = 1; \quad \{max = a[1] \wedge i = 1\} \\ \{max = a[1] \wedge i = 1\} \rightarrow \{max \geq a[1] \wedge i = 1\} \rightarrow \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i = 1 \right\} \rightarrow \{I\}$$

Posteriormente, pasaremos a demostrar el triple  $\{I \wedge B\} \quad S \quad \{I\}$  con  $\{B\} \equiv \{i \neq n+1\}$  y  $S$  el cuerpo del bucle para poder aplicar la regla de iteración:

$$\{I \wedge B\} \equiv \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i \neq n+1 \right\} \\ \text{if } a[i] \geq max \text{ then } max = a[i]; \\ \left\{ \bigwedge_{j=1}^i (max \geq a[j]) \wedge i \neq n+1 \right\} \\ i = i + 1; \\ \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i \neq n+2 \right\} \rightarrow \{I\}$$

Donde hemos usado que

$$\left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i \neq n+1 \right\} \text{ if } a[i] \geq max \text{ then } max = a[i]; \\ \left\{ \bigwedge_{j=1}^i (max \geq a[j]) \wedge i \neq n+1 \right\}$$

Para comprobar su veracidad, hemos de ver que:

$$\left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i \neq n+1 \wedge a[i] \geq max \right\} \quad max = a[i]; \quad \left\{ \bigwedge_{j=1}^i (max \geq a[j]) \wedge i \neq n+1 \right\} \\ \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i \neq n+1 \wedge max > a[i] \right\} \quad null; \quad \left\{ \bigwedge_{j=1}^i (max \geq a[j]) \wedge i \neq n+1 \right\}$$

---

<sup>2</sup>Para buscarlo, hemos de pensar en una regla que se mantenga iteración tras iteración.



Y ambos se verifican. Podemos ya aplicar la regla de iteración para llegar a que:

$$\begin{aligned} \{I\} &\equiv \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \right\} \\ &\text{while } i <> n+1 \text{ do begin} \\ &\text{if } a[i] \geq max \text{ then } max = a[i]; \\ &\quad i = i + 1; \\ &\text{end} \\ \{I \wedge \neg B\} &\equiv \left\{ \bigwedge_{j=1}^{i-1} (max \geq a[j]) \wedge i = n+1 \right\} \equiv \left\{ \bigwedge_{j=1}^n (max \geq a[j]) \right\} \end{aligned}$$

Que era lo que queríamos probar.

**Ejercicio 3.1.45.** Demostrar la corrección parcial del siguiente código:

$$\begin{aligned} &max = a[1]; i = 1; \\ &\text{while } i < n \text{ do begin} \\ &\quad i = i + 1; \\ &\text{if } a[i] \geq max \text{ then } max = a[i]; \\ &\text{end} \\ &\left\{ \bigwedge_{i=1}^n (max \geq a[i]), \bigvee_{j=1}^n (max = a[j]) \right\} \end{aligned}$$

**Ejercicio 3.1.46.** Demostrar la corrección parcial del siguiente código:

$$\begin{aligned} &i = 0; j = n; \\ &\text{while } i < n \text{ do begin} \\ &\quad i = i + 1; \\ &\quad j = j - 1; \\ &\quad a[i] = b[j] \\ &\text{end} \\ &\left\{ \bigwedge_{i=1}^n (a[i] = b[n-i]) \right\} \end{aligned}$$

Como se trata de un bucle, hemos de usar la regla de iteración, por lo que buscamos un invariante global que nos sirva. Observando el código, vemos que lo que hace es almacenar en el vector **a** el vector simétrico a **b** (es decir, invertir el vector **b**). A partir de esta premisa, pensamos que el invariante que nos sirve puede ser:

$$\{I\} \equiv \left\{ \bigwedge_{k=1}^i (a[k] = b[n-k]) \wedge j = n-i \right\}$$

En primer lugar, hemos de ver que el invariante se verifica al inicio del programa:

$$\{V\} \quad i = 0; \quad j = n; \quad \{I\}$$

Lo cual es cierto, ya que

$$\begin{aligned} \{V\} \quad & i = 0; \quad j = n; \quad \{i = 0 \wedge j = n\} \\ & \{i = 0 \wedge j = n\} \rightarrow \{I\} \end{aligned}$$

Posteriormente, y con vistas a aplicar la regla de iteración, hemos de ver que se cumple el triple  $\{I \wedge B\} \quad S \quad \{I\}$ , con  $\{B\} \equiv \{i < n\}$  y  $S$  el cuerpo del bucle:

$$\begin{aligned} \{I \wedge B\} &\equiv \left\{ \bigwedge_{k=1}^i (a[k] = b[n-k]) \wedge j = n - i \wedge i < n \right\} \\ &\quad i = i + 1; \\ &\left\{ \bigwedge_{k=1}^{i-1} (a[k] = b[n-k]) \wedge j = n - i + 1 \wedge i < n + 1 \right\} \\ &\quad j = j - 1; \\ &\left\{ \bigwedge_{k=1}^{i-1} (a[k] = b[n-k]) \wedge j = n - i \wedge i < n + 1 \right\} \\ &\quad a[i] = b[j]; \\ &\left\{ \bigwedge_{k=1}^{i-1} (a[k] = b[n-k]) \wedge a[i] = b[n-i] \wedge j = n - i \wedge i < n + 1 \right\} \equiv \\ &\equiv \left\{ \bigwedge_{k=1}^i (a[k] = b[n-k]) \wedge j = n - i \wedge i < n + 1 \right\} \rightarrow \{I\} \end{aligned}$$

donde hemos usado que

$$\{j = n - i\} \quad i = i + 1; \quad j = j - 1; \quad \{j = n - i\}$$

que puede probarse mediante composición de los triples

$$\begin{aligned} &\{j = n - i\} \quad i = i + 1; \quad \{j = n - i + 1\} \\ &\{j = n - i + 1\} \quad j = j - 1; \quad \{j = n - i\} \end{aligned}$$

que sabemos que son ciertos por el axioma de asignación.

Podemos finalmente aplicar la regla de iteración, llegando a que:

$$\begin{aligned} \{I\} &\equiv \left\{ \bigwedge_{k=1}^i (a[k] = b[n-k]) \wedge j = n - i \right\} \\ &\quad \textbf{while } i < n \textbf{ do begin} \\ &\quad \quad i = i + 1; \\ &\quad \quad j = j - 1; \\ &\quad \quad a[i] = b[j] \\ &\quad \textbf{end} \\ \{I \wedge \neg B\} &\equiv \left\{ \bigwedge_{k=1}^i (a[k] = b[n-k]) \wedge i \geq n \right\} \rightarrow \left\{ \bigwedge_{k=1}^n (a[k] = b[n-k]) \right\} \end{aligned}$$

Que era lo que queríamos probar.

**Ejercicio 3.1.47.** Demostrar la corrección parcial del siguiente código:

```
1  i = 0;  
   s = 0;  
   while i <= n do begin  
       s = s + a[i];  
5   a[i] = s;  
       i = i + 1;  
   end
```

**Ejercicio 3.1.48.** Dados  $n \geq 0$ ,  $i \leq n$ , demostrar que el siguiente segmento de programa evalúa

$$\frac{n!}{i!(n-i)!}$$

```
1  k = 0; fact = 1;  
   while k <> n do begin  
       k = k + 1;  
       fact = fact * k;  
5   if k <= i then afact = fact;  
       if k <= n-i then bfact = fact;  
   end  
   bcof = fact/(afact*bfact);
```

**Ejercicio 3.1.49.** Demostrar la terminación del fragmento de programa dado en el problema 3.1.44 ¿Qué condición se debe imponer para realizar la demostración?