Algoritmos y Estructuras de Datos I

Segundo cuatrimestre de 2019

Departamento de Computación - FCEyN - UBA

Correctitud y Teorema del Invariante

Transformación de estados

- Llamamos estado de un programa a los valores de todas sus variables en un punto de su ejecución:
  1. Antes de ejecutar la primera instrucción,
  2. entre dos instrucciones, y
  3. después de ejecutar la última instrucción.
- Podemos considerar la ejecución de un programa como una sucesión de estados.
- La asignación es la instrucción que permite pasar de un estado al siguiente en esta sucesión de estados.
- Las estructuras de control se limitan a especificar el flujo de ejecución (es decir, el orden de ejecución de las asignaciones).

Afirmaciones sobre estados

- Sea el siguiente programa que se ejecuta con estado inicial $\{True\}$.
- $\{True\}$
  ```
  int x = 0;
  ```
  $\{x = 0\}$
  ```
  x = x + 3;
  ```
  $\{x = 3\}$
  ```
  x = 2 * x;
  ```
  $\{x = 6\}$
- ¿Finaliza siempre el programa? Sí, porque no hay ciclos
- ¿Cuál es el estado final al finalizar su ejecución? $\{x = 6\}$

Afirmaciones sobre estados

- Sea el siguiente programa que se ejecuta con estado inicial con una variable a ya definida ($\{a = A_0\}$).
- $\{a = A_0\}$
  ```
  int b = a + 2;
  ```
  $\{a = A_0 \wedge b = A_0 + 2\}$
  ```
  int result = b - 1;
  ```
  $\{a = A_0 \wedge b = A_0 + 2 \wedge result = (A_0 + 2) - 1 = A_0 + 1\}$
- ¿Finaliza siempre el programa? Sí, porque no hay ciclos
- ¿Cuál es el estado final al finalizar su ejecución?
  $\{a = A_0 \wedge b = A_0 + 2 \wedge result = A_0 + 1\}$
  de lo que se deduce $\{result = a + 1\}$

Corrección de un programa

- **Definición.** *Decimos que un programa S es correcto respecto de una especificación dada por una precondición P y una postcondición Q, si siempre que el programa comienza en un estado que cumple P, el programa* **termina su ejecución**, *y en el estado final* **se cumple** Q.
- **Notación.** Cuando S es correcto respecto de la especificación (P, Q), lo denotamos con la siguiente tripla de Hoare:

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

Afirmaciones sobre estados

- Sea la siguiente especificación para incrementar en una unidad el valor de un entero.
- proc *incrementar*(inout $a : \mathbb{Z}$){
  Pre $\{a = A_0\}$
  Post $\{a = A_0 + 1\}$
  }
- ¿Es el siguiente programa S **correcto** con respecto a su especificación?

```
int incrementar(int& a) {
  int b = a + 2;
  int result = b - 1;
  a = result;
}
```


Ejemplo

- proc *incrementar*(inout $a : \mathbb{Z}$){
  Pre $\{a = A_0\}$
  Post $\{a = A_0 + 1\}$
  }
- Sea el siguiente programa que se ejecuta con estado inicial con una variable $a = A_0$.
- $\{a = A_0\}$
  `int b = a + 2;`
  $\{a = A_0 \land b = A_0 + 2\}$
  `int result = b - 1;`
  $\{a = A_0 \land b = A_0 + 2 \land result = (A_0 + 2) - 1 = A_0 + 1\}$
  `a = result;`
  $\{a = A_0 + 1 \land b = A_0 + 2 \land result = A_0 + 1\}$
  Por lo tanto, se deduce que:
  $\{a = A_0 + 1\}$

Intercambiando los valores de dos variables enteras

- proc *swap*(inout $a : \mathbb{Z}$, inout $b : \mathbb{Z}$){
  Pre $\{a = A_0 \land b = B_0\}$
  Post $\{a = B_0 \land b = A_0\}$
  }
- **Ejemplo:** Intercambiamos los valores de dos variables, pero sin una variable auxiliar!
- $\{a = A_0 \land b = B_0\}$
  `a = a + b;`
  $\{a = A_0 + B_0 \land b = B_0\}$
  `b = a - b;`
  $\{a = A_0 + B_0 \land b = (A_0 + B_0) - B_0\}$
  $\equiv \{a = A_0 + B_0 \land b = A_0\}$
  `a = a - b;`
  $\{a = A_0 + B_0 - A_0 \land b = A_0\}$
  $\equiv \{a = B_0 \land b = A_0\}$

Alternativas

- Sea el siguiente programa con una variable a de entrada cuyo valor no se modifica (i.e. podemos asumir $a = A_0$ como constante)
- Cuando tenemos una alternativa, debemos considerar las dos ramas por separado.
- Por ejemplo:

  $\{a = A_0 \wedge b = B_0\}$

  ```
  if( a > 0 ) {
    b = a;
  } else {
    b = -a;
  }
  ```

  ¿$\{b = |a|\}$?
- Verifiquemos ahora que $b = |a|$ después de la alternativa.

Alternativas

```
if( a > 0 ) {
  b = a;
} else {
  b = -a;
}
```

- Rama positiva:
  - Se cumple la condición B (i.e. $a > 0$)
  - $\{a = A_0 \wedge b = 0 \wedge B\} \equiv \{a = A_0 \wedge b = 0 \wedge A_0 > 0\}$
  - `b = a;`
  - $\{a = A_0 \wedge b = A_0 \wedge A_0 > 0\}$
  - $\Rightarrow \{b = |a|\}$
- Rama negativa:
  - No se cumple la condición B (i.e. $a <= 0$)
  - $\{a = A_0 \wedge b = 0 \wedge \neg B\} \equiv \{a = A_0 \wedge b = 0 \wedge A_0 \leq 0\}$
  - `b = -a;`
  - $\{a = A_0 \wedge b = -A_0 \wedge A_0 \leq 0\}$
  - $\Rightarrow \{b = |a|\}$
- En ambos casos vale $b = |a|$
- Por lo tanto, esta condición vale al salir de la instrucción alternativa.

Ciclos

- Recordemos la sintaxis de un ciclo:

  ```
  while (guarda B) {
        cuerpo del ciclo S
  }
  ```
- Se repite el cuerpo del ciclo S mientras la guarda B se cumpla, cero o más veces. Cada repetición se llama una iteración.
- La ejecución del ciclo termina si no se cumple la guarda al comienzo de su ejecución o bien luego de ejecutar una iteración.
- Cuando el ciclo termina (si lo hace), el estado resultante es el estado posterior a la última instrucción del cuerpo del ciclo.

Ejemplo

$\{n \geq 0 \wedge j = 1 \wedge s = 0\}$

```
while( j ≤ n ) {
  s = s + j;
  j = j + 1;
}
```

¿$\{s = \sum_{k=1}^{n} k\}$?

Ejemplo con n=6

```
while( j ≤ n ) {
  s = s + j;
  j = j + 1;
}
```

- Estados de cada iteración del ciclo:
  Recordar que antes del ciclo j=1 y s=0

Iteración	j	s
0	1	$0 = 0$
1	2	$1 = 0 + 1$
2	3	$3 = 0 + 1 + 2$
3	4	$6 = 0 + 1 + 2 + 3$
4	5	$10 = 0 + 1 + 2 + 3 + 4$
5	6	$15 = 0 + 1 + 2 + 3 + 4 + 5$
6	7	$21 = 0 + 1 + 2 + 3 + 4 + 5 + 6$

- **Observación:** Luego de cada iteración vale que:

$$s = \sum_{k=1}^{j-1} k$$

- A este tipo de afirmación se denomina un invariante del ciclo.

Invariante de un ciclo

- **Definición.** Un predicado $\mathbb{I}$ es un invariante de un ciclo si:
  1. $\mathbb{I}$ vale antes de comenzar el ciclo, y
  2. si vale $\mathbb{I} \wedge \mathbb{B}$ al comenzar una iteración arbitraria, entonces sigue valiendo $\mathbb{I}$ al finalizar la ejecución del cuerpo del ciclo.
- Un invariante describe un estado que se satisface cada vez que comienza la ejecución del cuerpo de un ciclo y también se cumple cuando la ejecución del cuerpo del ciclo concluye.
- Por ejemplo, otros invariantes para este ciclo son:
  - $\mathbb{I}' \equiv j \neq 0$
  - $\mathbb{I}'' \equiv s \geq 0$
  - $j \geq 1$
  - ...*etc*

Ejemplo

- ¿La ejecución del cuerpo del ciclo preserva $\mathbb{I} \equiv s = \sum_{k=1}^{j-1} k$?
- Para chequear esto, asumimos que vale $\mathbb{I} \wedge \mathbb{B}$ ya que se cumplió la condición para ejecutar el cuerpo del ciclo. Es decir, vale:

$$(s = \sum_{k=1}^{j-1} k) \wedge (j <= n)$$

- Agregamos metavariables para las variables que cambian.
- $\{j = J_0 \wedge s = S_0 \wedge S_0 = \sum_{k=1}^{J_0-1} k \wedge (J_0 \leq n)\}$

```
s = s + j;
```

$\{j = J_0 \wedge s = S_0 + J_0 \wedge S_0 = \sum_{k=1}^{J_0-1} k \wedge (J_0 \leq n)\}$
$\Rightarrow \ \{s = \sum_{k=1}^{J_0-1} k + J_0\}$
$\not\Rightarrow \ \{s = \sum_{k=1}^{J_0} k\}$
¿Qué pasa si $J_0 = -1, -2, etc..$?
Sólo vale la implicación si $J_0 \geq 0$

```
j = j + 1;
```


Ejemplo

- El predicado $\mathbb{I} \equiv s = \sum_{k=1}^{j-1} k$ (por sí solo) no es un invariante de ciclo ya que la ejecución del ciclo no lo preserva.
-

Iteración	j	s
0	1	$0 = 0$
1	2	$1 = 0 + 1$
2	3	$3 = 0 + 1 + 2$
3	4	$6 = 0 + 1 + 2 + 3$
4	5	$10 = 0 + 1 + 2 + 3 + 4$
5	6	$15 = 0 + 1 + 2 + 3 + 4 + 5$
6	7	$21 = 0 + 1 + 2 + 3 + 4 + 5 + 6$

- ¿Cómo podemos reforzar $\mathbb{I}$ para obtener un auténtico invariante para el ciclo?
- Nueva propuesta de invariante $\mathbb{I}$:

$$j \geq 1 \wedge s = \sum_{k=1}^{j-1} k$$

Ejemplo

- ¿Vale $\mathbb{I} \equiv j \geq 1 \land s = \sum_{k=1}^{j-1} k$ al principio del ciclo (i.e., antes de la instrucción while)?
-

```
while( j ≤ n ) {
  s = s + j;
  j = j + 1;
}
```

- Antes de ejecutar el ciclo el estado de la ejecución el estado inicial es $\{n \geq 0 \land j = 1 \land s = 0\}$.
- Esto implica que $\mathbb{I} \equiv j \geq 1 \land s = \sum_{k=1}^{j-1} k$.
- Por lo tanto, se cumple $\mathbb{I}$ al principio del ciclo.

Ejemplo

- ¿La ejecución del cuerpo del ciclo preserva $\mathbb{I} \equiv j \geq 1 \land s = \sum_{k=1}^{j-1} k$?
- Nuevamente asumimos que vale $\mathbb{I} \land \mathbb{B}$. Es decir, vale:
$$(j \geq 1 \land s = \sum_{k=1}^{j-1} k) \land (j <= n)$$
- Agregamos metavariables para las variables que cambian.
- $\{j = J_0 \land s = S_0 \land J_0 \geq 1 \land S_0 = \sum_{k=1}^{J_0-1} k \land (J_0 \leq n)\}$

```
s = s + j;
```

$\{j = J_0 \land s = S_0 + J_0 \land J_0 \geq 1 \land S_0 = \sum_{k=1}^{J_0-1} k \land (J_0 \leq n)\}$
$\Rightarrow \ \{s = \sum_{k=1}^{J_0-1} k + J_0\}$
$\Rightarrow \ \{s = \sum_{k=1}^{J_0} k\}$ Este paso se puede aplicar ya que $J_0 \geq 0$

$\{j = J_0 \land s = \sum_{k=1}^{J_0} k \land J_0 \geq 1 \land S_0 = \sum_{k=1}^{J_0-1} k \land (J_0 \leq n)\}$

```
j = j + 1;
```

$\{j = J_0 + 1 \land s = \sum_{k=1}^{J_0} k \land J_0 \geq 1 \land S_0 = \sum_{k=1}^{J_0-1} k \land (J_0 \leq n)\}$
$\Rightarrow \ \{j \geq 1 \land s = \sum_{k=1}^{j-1} k\} \ \equiv \ \{\mathbb{I}\}$

Ejemplo

- Tenemos entonces:
  1. $\mathbb{I}$ vale justo antes de comenzar el ciclo.
  2. Si valía la condición $\mathbb{B}$ y valía $\mathbb{I}$, entonces $\mathbb{I}$ sigue valiendo luego de la ejecución del cuerpo del ciclo.
- Si salió del ciclo fue porque no se cumplió $j \leq n$, y entonces estamos en un estado que satisface:

$$n \geq 0 \land \mathbb{I} \land \neg\mathbb{B} \quad \equiv \quad n \geq 0 \land \underbrace{j \geq 1 \land s = \sum_{k=1}^{j-1} k}_{\mathbb{I}} \ \land \ \underbrace{j > n}_{\neg\mathbb{B}}$$

- Es decir, $\mathbb{I}$ también vale cuando el ciclo termina.

Invariante de un ciclo

- Los invariantes de un ciclo permiten razonar sobre su corrección. Llamamos ...
  1. $\mathbb{P}_\mathbb{C}$: Precondición del ciclo,
  2. $\mathbb{Q}_\mathbb{C}$: Postcondición del ciclo,
  3. $\mathbb{B}$: Guarda del ciclo,
  4. $\mathbb{I}$: Un invariante del ciclo.
- Si se cumplen estas condiciones ...
  1. $\mathbb{P}_\mathbb{C} \Rightarrow \mathbb{I}$,
  2. $\{\mathbb{I} \land \mathbb{B}\}$ `cuerpo del ciclo` $\mathbb{I}$,
  3. $\mathbb{I} \land \neg\mathbb{B} \Rightarrow \mathbb{Q}_\mathbb{C}$,
- ... entonces el ciclo es parcialmente correcto respecto de su especificación (si termina, termina en $\mathbb{Q}_\mathbb{C}$).

Teorema del invariante

- **Teorema del invariante**. Si existe un predicado $\mathbb{I}$ tal que ...

  1. $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$,
  2. $\{\mathbb{I} \wedge \mathbb{B}\}$ S $\{\mathbb{I}\}$,
  3. $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$,

  entonces el ciclo **while(B) S** es parcialmente correcto respecto de la especificación $(\mathbb{P}_{\mathbb{C}}, \mathbb{Q}_{\mathbb{C}})$.
- Este teorema es la herramienta principal para argumentar la corrección de ciclos.
- El teorema del invariante se puede demostrar formalmente (más detalle en las próximas teóricas!).

Ejemplo

1. $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$
2. $\{\mathbb{I} \wedge \mathbb{B}\}$ S $\{\mathbb{I}\}$
3. $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$

- Verifiquemos estas tres condiciones con el ejemplo anterior, y con ...
  1. $\mathbb{P}_{\mathbb{C}} \equiv n \geq 0 \wedge j = 1 \wedge s = 0$
  2. $\mathbb{Q}_{\mathbb{C}} \equiv n \geq 0 \wedge s = \sum_{k=1}^{n} k$
  3. $\mathbb{B} \equiv j \leq n$
  4. $\mathbb{I} \equiv j \geq 1 \wedge s = \sum_{k=1}^{j-1} k$
- En primer lugar, debemos verificar que $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$:
- Ya probamos anteriormente que:

$$\left(n \geq 0 \wedge j = 1 \wedge s = 0\right) \;\Rightarrow\; j \geq 1 \wedge s = \sum_{k=1}^{j-1} k$$

- Por lo tanto, podemos concluir que se cumple la condición $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$

Ejemplo

1. $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$
2. $\{\mathbb{I} \wedge \mathbb{B}\}$ S $\{\mathbb{I}\}$
3. $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$

- ¿Es cierto que $\{\mathbb{I} \wedge \mathbb{B}\} S \{\mathbb{I}\}$?

$\mathbb{I} \wedge \mathbb{B} : \{j \leq n \wedge j \geq 1 \wedge s = \sum_{k=1}^{j-1} k\}$

```
s = s + j;
j = j + 1;
```

$\mathbb{I} : \{j \geq 1 \wedge s = \sum_{k=1}^{j-1} k\}$

- Esto también lo probamos cuando demostramos que $\mathbb{I}$ era un invariante para el ciclo.

Ejemplo

1. $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$
2. $\{\mathbb{I} \wedge \mathbb{B}\}$ S $\{\mathbb{I}\}$
3. $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$

- Finalmente, ¿es cierto que $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$?

$$j \geq 1 \wedge s = \sum_{k=1}^{j-1} k \wedge j > n \;\Rightarrow\; s = \sum_{k=1}^{n} k \; ?$$

- **No!** Contraejemplo: Si $j = n + 2$, entonces la implicación no vale!
- Sin embargo, sabemos que esto no puede pasar, puesto que $j \leq n + 1$ a lo largo del ciclo.
- ¿Qué hacemos?

$\Rightarrow$ Reforzamos el invariante!

Ejemplo

- Proponemos el nuevo invariante de ciclo reforzado (i.e. mas restrictivo):

$$\mathbb{I} \equiv 1 \leq j \leq n+1 \wedge \mathsf{s} = \sum_{k=1}^{j-1} k$$

- ¿Vale ahora que tenemos que $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$?

$$1 \leq j \leq n+1 \wedge \mathsf{s} = \sum_{k=1}^{j-1} k \wedge j > n$$

$$\Rightarrow \quad j = n+1 \wedge \mathsf{s} = \sum_{k=1}^{j-1} k$$

$$\Rightarrow \quad \mathsf{s} = \sum_{k=1}^{n} k \equiv Q_C$$

Ejemplo

- ¿Qué pasa con los dos primeros puntos del teorema del invariante?
  - $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$
  - $\{\mathbb{I} \wedge \mathbb{B}\}$ cuerpo del ciclo $\{\mathbb{I}\}$
- ¿Se siguen verificando estas condiciones con el nuevo invariante?
- Hay que demostrarlo nuevamente! Si $\mathbb{I}' \Rightarrow \mathbb{I}$ no podemos concluir que $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}'$.

¿$\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$?

$$\mathbb{P}_{\mathbb{C}} \equiv \big(n \geq 0 \wedge j = 1 \wedge s = 0\big) \;\Rightarrow\; 1 \leq j \leq n+1 \wedge \mathsf{s} = \sum_{k=1}^{j-1} k$$

- Por lo tanto, se cumple que $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$

¿La ejecución del cuerpo del ciclo preserva el $\mathbb{I}$?

- $\{j = J_0 \wedge \mathsf{s} = \mathsf{S}_0 \wedge \overbrace{1 \leq J_0 \leq n+1 \wedge \mathsf{S}_0 = \sum_{k=1}^{J_0-1} k}^{\mathbb{I}} \wedge \overbrace{(J_0 \leq n)}^{\mathbb{B}}\}$

```
s = s + j;
```

$\{j = J_0 \wedge \mathsf{s} = \mathsf{S}_0 + J_0 \wedge 1 \leq J_0 \leq n+1 \wedge \mathsf{S}_0 = \sum_{k=1}^{J_0-1} k \wedge (J_0 \leq n)\}$
$\Rightarrow \quad \{\mathsf{s} = \sum_{k=1}^{J_0-1} k + J_0\}$
$\Rightarrow \quad \{\mathsf{s} = \sum_{k=1}^{J_0} k\}$ Esto vale porque $J_0 \geq 0$

$\{j = J_0 \wedge \mathsf{s} = \sum_{k=1}^{J_0} k \wedge 1 \leq J_0 \leq n+1 \wedge \mathsf{S}_0 = \sum_{k=1}^{J_0-1} k \wedge (J_0 \leq n)\}$

```
j = j + 1;
```

$\{j = J_0 + 1 \wedge \mathsf{s} = \sum_{k=1}^{J_0} k \wedge 1 \leq J_0 \leq n+1 \wedge \mathsf{S}_0 = \sum_{k=1}^{J_0-1} k \wedge (J_0 \leq n)\}$
$\Rightarrow \quad \{1 \leq j \leq n+1 \wedge \mathsf{s} = \sum_{k=1}^{j-1} k\} \;\equiv\; \{\mathbb{I}\}$ Esto vale ya que $J_0 \leq n$

Resultado final

- Finalmente, Sean:
  1. $\mathbb{P}_{\mathbb{C}} \equiv n \geq 0 \wedge j = 1 \wedge s = 0$
  2. $\mathbb{Q}_{\mathbb{C}} \equiv n \geq 0 \wedge s = \sum_{k=1}^{n} k$
  3. $\mathbb{B} \equiv j \leq n$
  4. $\mathbb{I} \equiv 1 \leq j \leq (n+1) \wedge s = \sum_{k=1}^{j-1} k$
- Ya que demostramos que se cumplen las siguientes condiciones:
  1. $\mathbb{P}_{\mathbb{C}} \Rightarrow \mathbb{I}$
  2. $\{\mathbb{I} \wedge \mathbb{B}\}$ cuerpo del ciclo $\{\mathbb{I}\}$
  3. $\mathbb{I} \wedge \neg\mathbb{B} \Rightarrow \mathbb{Q}_{\mathbb{C}}$
- Entonces, por el Teorema del Invariante podemos concluir que el ciclo `while(B) S` es parcialmente correcto respecto de la especificación $\mathbb{P}_{\mathbb{C}}, \mathbb{Q}_{\mathbb{C}}$.

Algunas observaciones

- $\mathbb{I} \equiv 1 \leq j \leq n+1 \wedge s = \sum_{k=1}^{j-1} k$.
  1. El invariante refleja la hipótesis inductiva del ciclo.
  2. En general, un buen invariante debe incluir el rango de la(s) variable(s) de control del ciclo.
  3. Además, debe incluir alguna afirmación sobre el acumulador del ciclo.
- Cuando tenemos un invariante $\mathbb{I}$ que permite demostrar la corrección parcial del ciclo, nos referimos a $\mathbb{I}$ como el invariante del ciclo.
  1. El invariante de un ciclo caracteriza las acciones del ciclo, y representa al las asunciones y propiedades que hace nuestro algoritmo durante el ciclo.
- En general, es sencillo argumentar informalmente la terminación del ciclo (más detalles en las próximas teóricas).

Para concluir...

- Ojo: Para probar esto:

  $\{n \geq 0 \wedge j = 1 \wedge s = 0\}$

```
while( j ≤ n ) {
  s = s + j;
  j = j + 1;
}
```

  $\{s = \sum_{k=1}^{n} k\}$
- Nos falta demostrar que si vale $\mathbb{P}_{\mathbb{C}}$ el ciclo siempre termina.
- Por ahora, solo probamos que es parcialmente correcto[1]
- Vamos a ver como demostrar terminación en las próximas teóricas.

[1] Cuando termina, cumple $\mathbb{Q}_{\mathbb{C}}$, pero no sabemos si siempre termina

Bibliografía

- David Gries - The Science of Programming
  - Chapter 6 - Using Assertions to Document Programs
    - Chapter 6.1 - Program Specifications
    - Chapter 6.2 - Representing Initial and Final Values of Variables
    - Chapter 6.3 - Proof Outlines (transformación de estados, alternativas)