Precondición más débil de ciclos

Algoritmos y Estructuras de Datos

Repaso: Triplas de Hoare

- Consideremos la siguiente tripla de Hoare:

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

- Esta tripla es válida si se cumple que:
  1. Si el programa S comienza en un estado que cumple P ...
  2. ... entonces termina luego de un número finito de pasos ...
  3. ... Y además en un estado que cumple Q.

Repaso: Lenguaje SmallLang

- Definimos un lenguaje imperativo basado en variables y las siguientes instrucciones:
  1. Nada: Instrucción **skip** que no hace nada.
  2. Asignación: Instrucción **x := E**.
- Además, tenemos las siguientes estructuras de control:
  1. Secuencia: **S1; S2** es un programa, si **S1** y **S2** son dos programas.
  2. Condicional: **if B then S1 else S2 endif** es un programa, si **B** es una expresión lógica y **S1** y **S2** son dos programas.
  3. Ciclo: **while B do S endwhile** es un programa, si **B** es una expresión lógica y **S** es un programa.

Repaso: Precondición más débil

- **Definición.** La precondición más débil de un programa **S** respecto de una postcondición Q es el predicado P más débil posible tal que $\{P\}\mathbf{S}\{Q\}$.
- **Notación.** $wp(\texttt{S}, Q)$.
- **Teorema:** Decimos que $\{P\}$ **S** $\{Q\}$ es válida sii $P \Rightarrow_L wp(\texttt{S}, Q)$

Repaso: Axiomas wp

- **Axioma 1.** $wp(\texttt{x := E}, Q) \equiv \text{def}(E) \wedge_L Q^x_E$.
- **Axioma 2.** $wp(\texttt{skip}, Q) \equiv Q$.
- **Axioma 3.** $wp(\texttt{S1; S2}, Q) \equiv wp(\texttt{S1}, wp(\texttt{S2}, Q))$.
- **Axioma 4.** $wp(\texttt{if B then S1 else S2 endif}, Q) \equiv$

$$def(B) \wedge_L \Big((B \wedge wp(\texttt{S1}, Q)) \vee (\neg B \wedge wp(\texttt{S2}, Q))\Big)$$

- **Observación:** $wp(\texttt{b[i]:=E}, Q) \equiv wp(\texttt{b:=setAt(b,i,E)}, Q)$

Ciclos (repaso)

- 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.
- Si/cuando el ciclo termina, el estado resultante es el estado posterior a la última instrucción del cuerpo del ciclo.

¿Cuál es la precondición más débil?

```
{???}

while (x>0) do
  x := x -1
endwhile
```

$\{x = 0\}$

$$wp(\texttt{while ...}, x = 0) \equiv x \geq 0$$

¿Cuál es la precondición más débil?

```
{???}

i := 0;
while (x<5) do
  x := x + 1;
  i := i + 1
endwhile
```

$\{x = 5 \wedge i = 5\}$

$$wp(\texttt{i:=0; while ...}, x = 5 \wedge i = 5) \equiv x = 0$$

¿Cuál es la precondición más débil?

$\{???\}$

```
while (x==5) do
  x := 5
endwhile
```

$\{x \neq 5\}$

$$wp(\texttt{while } \ldots, x \neq 5) \equiv x \neq 5$$

¿Es válida la siguiente tripla de Hoare?

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

```
while (i <= n) do
  s := s + i;
  i := i + 1
endwhile
```

$\{s = \sum_{k=1}^{n} k\}$

Precondición más débil de un ciclo

- Supongamos que tenemos el ciclo **while B do S endwhile**.
- **Definición.** Definimos $H_k(Q)$ como el predicado que define el conjunto de estados a partir de los cuales la ejecución del ciclo termina en exactamente k iteraciones, satisfaciendo Q:

$$\begin{aligned} H_0(Q) &\equiv \text{def}(B) \wedge \neg B \wedge Q, \\ H_{k+1}(Q) &\equiv \text{def}(B) \wedge B \wedge wp(\texttt{S}, H_k(Q)) \qquad \text{para } k \geq 0. \end{aligned}$$

- **Propiedad:** Si el ciclo realiza a lo sumo k iteraciones, entonces

$$wp(\texttt{while B do S endwhile}, Q) \equiv \vee_{i=0}^{k} H_i(Q)$$

Ejemplo

$\{???\}$

```
while (0<i && i<3) do
  i := i +1
endwhile
```

$\{i = 3\}$

- A lo sumo, se va a ejecutar 2 veces el cuerpo del ciclo
- ¿Cuál es la precondición más débil?

$$\begin{aligned} & wp(\texttt{while } 0 < i < 3 \texttt{ do i:=i+1 endwhile}, i = 3) \\ \equiv\ & \vee_{i=0}^{2} H_i(i = 3) \\ \equiv\ & H_0(i = 3) \vee H_1(i = 3) \vee H_2(i = 3) \\ \equiv\ & i = 1 \vee i = 2 \vee i = 3 \end{aligned}$$

Otro ejemplo

$\{???\}$

```
while (0<i && i<n) do
  i := i +1
endwhile
```

$\{i \geq 0\}$

- ¿Cuántas veces se va a ejecutar el cuerpo del ciclo?
- ¿Podemos usar la propiedad anterior para conocer la precondición más débil?
- ¡No! Porque no podemos fijar a priori una cota superior a la cantidad de iteraciones que va a realizar el ciclo.

Precondición más débil de un ciclo

- **Intituivamente:** $wp(\texttt{while B do S endwhile}, Q)$ tiene que ser una fórmula lógica capaz de capturar todos los estados tales que, luego de ejecutar el ciclo una cantidad arbitraria de veces, vale Q.
- **Axioma 5:**

$$wp(\texttt{while B do S endwhile}, Q) \equiv (\exists_{i\geq 0})(H_i(Q))$$

Precondición más débil de un ciclo

- Ahora tratemos de usar el **Axioma 5**:

$$\begin{aligned} & wp(\texttt{while B do S endwhile}, Q) \\ & \quad \equiv (\exists_{i\geq 0})H_i(Q) \\ & \quad \equiv H_0(Q) \vee H_1(Q) \vee H_2(Q) \vee \ldots \\ & \quad \equiv \vee_{i=0}^{\infty}(H_i(Q)) \end{aligned}$$

¡Es una fórmula infinitaria!

- Por lo tanto, no podemos usar mecánicamente el **Axioma 5** para demostrar la corrección de un ciclo con una cantidad no acotada a priori de iteraciones :(

Invariante de un ciclo

- **Definición.** Un predicado I es un invariante de un ciclo si:
  1. I vale antes de comenzar el ciclo, y
  2. si vale $I \wedge B$ al comenzar una iteración arbitraria, entonces sigue valiendo 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, pensemos invariantes para el ciclo de la diapositiva 10:
  - $I \equiv i \geq 1 \wedge s = \sum_{k=1}^{i-1} k$
  - $I' \equiv i \neq 0$
  - $I'' \equiv s \geq 0$
  - $i \geq 1$
  - *...etc*

Teorema del invariante

- **Teorema del invariante**. Si existe un predicado I tal que ...
  1. $P_C \Rightarrow$ I,
  2. $\{I \wedge B\}$ S $\{I\}$,
  3. $I \wedge \neg B \Rightarrow Q_C$,

  entonces el ciclo **while(B) S** es parcialmente correcto respecto de la especificación (P_C, Q_C).
- Este teorema es la herramienta principal para argumentar la corrección de ciclos.
- El teorema del invariante se puede demostrar formalmente (más detalle luego).

Ejemplo

- Verifiquemos estas tres condiciones con el ejemplo anterior, y con ...
  1. $P_C \equiv n \geq 0 \wedge i = 1 \wedge s = 0$
  2. $Q_C \equiv n \geq 0 \wedge s = \sum_{k=1}^{n} k$
  3. $B_C \equiv i \leq n$
  4. $I \equiv i \geq 1 \wedge s = \sum_{k=1}^{i-1} k$
- En primer lugar, debemos verificar que $P_C \Rightarrow I$:
- Debemos probar que:

$$\big(n \geq 0 \wedge i = 1 \wedge s = 0\big) \;\Rightarrow\; i \geq 1 \wedge s = \sum_{k=1}^{i-1} k.$$

- Lo cual es trivialmente cierto, por lo tanto se cumple la condición $P_C \Rightarrow I$

Ejemplo

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

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

```
s = s + i;
i = i + 1;
```

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

- Esto es decir que I es un invariante para el ciclo.

Ejemplo

- Finalmente, ¿es cierto que $I \wedge \neg B \Rightarrow Q_C$?

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

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

$\Rightarrow$ ¡Reforzamos el invariante!

Ejemplo

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

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

- ¿Vale ahora que tenemos que $I \wedge \neg B \Rightarrow Q_C$?

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

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

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

Ejemplo

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

Para concluir...

- ¿$P_C \Rightarrow I$?

$$P_C \equiv \left(n \geq 0 \wedge i = 1 \wedge s = 0\right) \;\Rightarrow\; 1 \leq i \leq n+1 \wedge s = \sum_{k=1}^{i-1} k$$

- Por lo tanto, se cumple que $P_C \Rightarrow I$

Para concluir...

- ¿La ejecución del cuerpo del ciclo preserva $\mathrm{I} \equiv 1 \leq \mathrm{i} \leq \mathrm{n}+1 \wedge \mathrm{s} = \sum_{k=1}^{i-1} \mathrm{k}$?
- $\{i = I_0 \wedge s = S_0 \wedge 1 \leq I_0 \leq n+1 \wedge S_0 = \sum_{k=1}^{I_0-1} k \wedge \left(I_0 \leq n\right)\}$

```
s = s + i;
```

$\{i = I_0 \wedge s = S_0 + I_0 \wedge 1 \leq I_0 \leq n+1 \wedge S_0 = \sum_{k=1}^{I_0-1} k \wedge (I_0 \leq n)\}$
$\Rightarrow \; \{s = \sum_{k=1}^{I_0-1} k + I_0\}$
$\Rightarrow \; \{s = \sum_{k=1}^{I_0} k\}$Este paso sólo se puede aplicar si $I_0 \geq 0$

$\{i = I_0 \wedge s = \sum_{k=1}^{I_0} k \wedge 1 \leq I_0 \leq n+1 \wedge S_0 = \sum_{k=1}^{I_0-1} k \wedge (I_0 \leq n)\}$

```
i = i + 1;
```

$\{i = I_0 + 1 \wedge s = \sum_{k=1}^{I_0} k \wedge 1 \leq I_0 \leq n+1 \wedge S_0 = \sum_{k=1}^{I_0-1} k \wedge (I_0 \leq n)\}$
$\Rightarrow \; \{1 \leq i \leq n+1 \wedge s = \sum_{k=1}^{i-1} k\} \;\equiv\; \{I\}$Esto lo podemos hacer ya que $I_0 \leq n$

Resultado final

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

Algunas observaciones

- $I \equiv 1 \leq i \leq n+1 \wedge s = \sum_{k=1}^{i-1} k$.
  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 I que permite demostrar la corrección parcial del ciclo, nos referimos a 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 luego).

Para concluir...

- Ojo: Para probar esto:

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

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

  $\{s = \sum_{k=1}^{n} k\}$
- Nos falta demostrar que si vale P_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 Q_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)