Apunte - Algoritmos y Estructuras de Datos (ex Algo II)

Sebastian Andrés

September 2023

Contents

1 Especificacion

2 Correctitud

La idea es demostrar que un programa propuesto satisface la especificacion dada. Estas tecnicas de demostracion formal son utiles especialmente para software ligado al funcionamiento de piezas de hardware (chips, componentes, etc).

2.1 Triplas de Hoare

Concepto: Introducido por Charles Hoare en 1969, es un sistema formal que proporciona reglas de inferencia para la correccion de programas imperativas con logica matematica. Se representa a una especificacion y el programa propuesto como la tripla:

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

Donde P es la precondicion, Q la postcondicion y S el programa.

Validez: Esta tripla es valida si se cumple que

- 1. Si el programa S comienza en un estado que cumple P ...
- 2. ... entonces termina luego de un numero finito de pasos
- 3. ... Y ademas en un estado que cumple Q.

2.2 Weakest precondition (WP)

Def: WP(S,Q), la precondicion mas debil de un programa S respecto de una postcondicion Q, es el predicado P mas debil posible tal que $\{P\}S\{Q\}$ es valida.

Su utilidad es que sirve como formula logica para demostrar la correctitud de algunas triplas Hoare. Vale que si la precondicion P implica $WP(S,Q)$ entonces la tripla es valida.

$$\{P \rightarrow WP(S,Q)\} \rightarrow \{P\}S\{Q\} \text{ valida}$$

2.2.1 Axioma 1 - Asignacion

$$WP(x := E, Q) \equiv def(E) \wedge Q_E^X$$

2.2.2 Axioma 2 - Skip

$$WP(skip, Q) \equiv Q$$

2.2.3 Axioma 3 - Secuencia

$$WP(s_1; s_2, Q) \equiv WP(s_1, WP(s_2, Q))$$

2.2.4 Axioma 4 - Condicionales

Sea S = if B then s_1 else s_2 endif, entoces:

$$WP(S,Q) \equiv def(B) \wedge_L ((B \wedge WP(s_1,Q)) \vee (\neg B \wedge WP(s_2,Q)))$$

2.3 Correctitud en ciclos

2.3.1 Axioma 5 - Ciclos

Def: Definimos $H_k(Q)$ como el predicado que define el conjunto de estados a partir de los cuales la ejecucion del ciclo termina en exactamente k iteraciones, satisfaciendo Q.

$$H_0(Q) \equiv def(B) \wedge \neg B \wedge Q$$
$$H_k(Q) \equiv def(B) \wedge B \wedge WP(S, H_k(Q))$$

Propiedad: Sea S = while B do S endwhile, si el ciclo se realiza a lo sumo k veces, entonces.

$$WP(S,Q) \equiv \vee_{i=0}^{\infty} H_i(Q)$$
$$WP(S,Q) \equiv (\exists i \geq 0) H_i(Q)$$

Pero esto es una formula infinitaria! No podemos usar mecanicamente el axioma 5 para demostrar la correctitud de un ciclo con una cantidad de iteraciones no acotada a prori.

Queremos buscar otra forma de armar una formula logica de WP(S,Q), para S ciclo, para capturar todos los estados que tras una cantidad arbitraria finita de pasos, valga Q.

2.3.2 Teorema del invariante

Invariante: Un predicado I es invariante de un ciclo si:

1. I vale antes de comenzar el ciclo
2. Si vale $I \wedge B$ al comenzar una iteracion arbitraria, entonces sigue valiendo I al finalizar la ejecucion del cuerpo del ciclo.

Un invariante describe un estado que se satisface cada vez que comienza la ejecucion del cuerpo de un ciclo y tambirn se cumple cuando la ejecucion del ciclo concluye.

Observaciones: Refleja la hipotesis inductiva de un ciclo. Un buen invariante debe incluir el rango de las variables de control del ciclo. Debe afirmar sobre el acumulador del ciclo.

Teorema del invariante: Si existe un predicado I tal que:

1. $P_C \to I$
2. $\{I \wedge B\}S\{I\}$
3. $I \wedge \neg B \to Q_C$

Entonces while B do S endwhile es parcialmente correcto respecto a la especificacion (P_C, Q_C).

Esto significa que, si el programa siempre termina, entonces la tripla de hoare es valida.

2.3.3 Teorema de la terminacion de un ciclo

Teorema: Sea V el producto cartesiano de los dominios de las variables del programa y sea I un invariante del ciclo "while B do S endwhile". Si existe una funcion $f_v : V \to Z$ tal que:

1. $\{I \wedge B \wedge v_0 = f_v\}S\{f_v < v_0\}$
2. $I \wedge f_v \leq 0 \to \neg B$

Entonces la ejecucion del ciclo "while B do S endwhile" siempre termina.

Funcion variante del ciclo (f_v): Es una funcion que representa una cantidad que se va reduciendo a lo largo de las iteraciones del ciclo.

2.3.4 Teorema de correctitud de un ciclo

Teorema: Sean un predicado I y una funcion $f_V : V \to \mathbf{Z}$, donde V es el producto cartesiano de las variables del programa, y supongamos que $I \to def(B)$. Si valen las 5 condiciones para que se cumpla:

1. El teorema del invariante.
2. El teorema de terminacion.

Entonces la tripla de Hoare $\{P_C\}$while B do S endwhile$\{Q_C\}$ es valida.

Observaciones: Probar esto equivale a probar $P_C \to WP(\text{while B do S endwhile}, Q_C)$, pero no implica haber obtenido el predicado $WP(\text{while b do S endwhile}, Q_C)$

2.3.5 Guia para demostrar correctitud de programas con ciclos

Si quiero probar la validez de:

$$\{Pre\}S_1; \text{while B do } S_2 \text{ endwhile}; S_3\{Post\}$$

Tengo que probar:

1 . $Pre \rightarrow_L WP(S_1, P_C)$

2 . $P_C \rightarrow_L WP(\text{while B do } S_2 \text{ endwhile}, Q_C)$

3 . $Q_C \rightarrow_L WP(S_3, Post)$