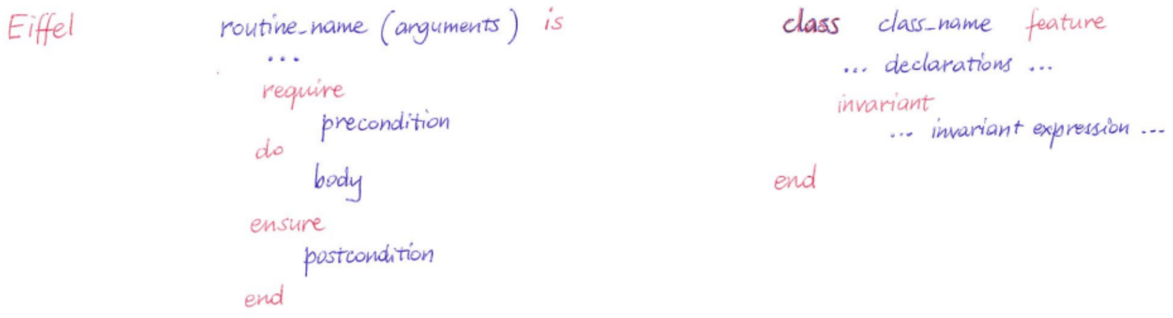
Lezione 17 04/12/2023

Design by contract

Propone di considerare una tripla come un contratto tra “cliente” e “fornitore”, il fornitore è il programmatore. In questa interpretazione la precondizione consiste negli obblighi che il cliente deve rispettare. Il programmatore garantisce che il programma fornirà il risultato atteso, purché il cliente rispetti il contratto.



```
routine_name (arguments) is
   ...
   require
       precondition
   do
       body
   ensure
       postcondition
   end
```

```
class class_name feature
   ... declarations ...
invariant
       ... invariant expression ...
end
```

Eiffel è un linguaggio di programmazione ad oggetti. Nell’esempio vediamo una funzione. Il linguaggio consente di dichiarare una precondizione (require) e postcondizione (ensure).

Posso anche specificare una classe che contiene un’invariante.

JML Java Modeling Language

```
//@ requires x >= 0.0
/*@ ensures JMLDouble.approximatelyEqualTo
  @              (x, \result * \result, eps);
  @*/
public static double sqrt(double x) {
        ...
}
```

```
public class P {
    ...
   /*@ public invariant
     @     w >= 0;
     @*/
   ...
}
```

```
$> jmlc P.java
```

il bytecode contiene istruzioni per verificare le asserzioni

è un’estensione di java che permette di specificare precondizioni, postcondizioni e invarianti.

A questo linguaggio è associato un compilatore. Nel bytecode ci saranno anche istruzioni che permettono di verificare le pre e post condizioni.

Esercizi

La logica di Hoare e la sintesi di programmi iterativi

PROBLEMA Calcolare la radice quadrata intera di un numero K

a. Stabiliamo il criterio di correttezza (i "termini del contratto")

$$\{ K \geq 0 \}\ \ P\ \ \{ 0 \leq x^2 \leq K < (x+1)^2 \}$$

b. Ipotesi di soluzione: calcoliamo il valore richiesto per approssimazioni successive ⟶ iterazione fino a quando il valore calcolato soddisfa la postcondizione

Struttura del programma

```
x := E(K);        // preparazione di x
while  B(x,K)  do           ]
    x := F(x,K)             ] W
endwhile                    ]
```

c. Spezziamo la postcondizione per cercare un invariante di ciclo

$$0 \leq x^2 \qquad x^2 \leq K \qquad (x+1)^2 > K$$

Supponiamo di calcolare il risultato partendo da un'approssimazione per difetto, e incrementando

⇒ $0 \leq x^2 \wedge x^2 \leq K$ è un possibile invariante

⇒ x := E(K) deve stabilire l'invariante

Poiché $K \geq 0$, scegliamo 0 come valore iniziale di x

d. Se inv $\equiv 0 \leq x^2 \leq K$ è un invariante per W, al termine dell'esecuzione varrà

$$\text{inv} \wedge \neg B(x,K)$$

⇒ dobbiamo scegliere $B(x,K)$ in modo che

$$(\text{inv} \wedge \neg B(x,K)) \rightarrow (\text{inv} \wedge K < (x+1)^2)$$

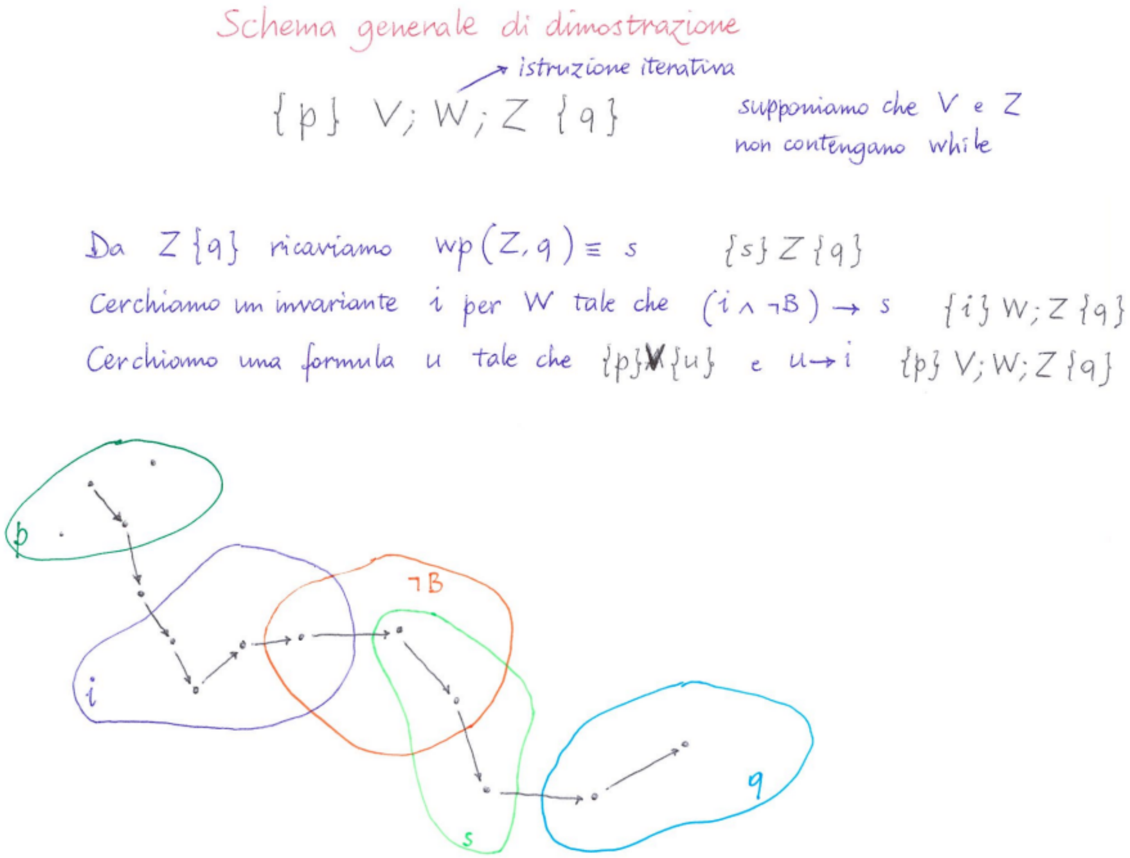
⇒ Poniamo $B(x,K) \equiv \boxed{(x+1)^2 \leq K}$

e. Se nel corpo dell'iterazione incrementiamo x, prima o poi $(x+1)^2$ diventerà maggiore di K

⇒

```
x := 0;
while  (x+1)*(x+1) <= K  do
    x := x + 1
endwhile
```

Esercizio: dimostrare che inv è un invariante
dimostrare la correttezza totale



Schema generale di dimostrazione

$\{p\}\ V;\ \overset{\text{istruzione iterativa}}{W};\ Z\ \{q\}$

supponiamo che V e Z non contengano while

Da $Z\{q\}$ ricaviamo $wp(Z,q) \equiv s$ $\{s\}\,Z\,\{q\}$

Cerchiamo un invariante i per W tale che $(i \wedge \neg B) \rightarrow s$ $\{i\}\,W;Z\,\{q\}$

Cerchiomo una formula u tale che $\{p\}\,V\,\{u\}$ e $u \rightarrow i$ $\{p\}\,V;W;Z\,\{q\}$

non penso che abbiamo fatto questa slide e potrebbe essere sbagliata