Istruzioni iterative

while B do C endwhile

Regola di derivazione (correttezza parziale)

invariante di ciclo

$$\frac{\{\ inv \wedge B\ \}\ C\ \{\ inv\ \}}{\{inv\}\ \text{while } B \text{ do } C \text{ endwhile } \{inv \wedge \neg B\}}$$

- Nella precondizione della conclusione non c'è B

Istruzioni iterative

- Data un'istruzione iterativa, non c'è un solo invariante

  Ad esempio, true è un invariante per ogni while ... endwhile

  Può esserci un invariante più utile per la dimostrazione in corso

- Nella pratica, studiamo istruzioni iterative inserite in programmi; la scelta dell'invariante dipende dal contesto e si abbina alla regola dell'implicazione

$$\{ p \}\ C; W; D\ \{ q \}$$

$$\{p\}\ C\ \{r\}\ W\ \{z\}\ D\ \{q\}$$

$$\{ inv \}\ W\ \{ inv \wedge \neg B \}$$

Esercizi

P

```
i := 0; s := 1;
while i < N do
    i := i + 1;
    s := s * x
endwhile
```

? $\{ N \geq 0 \}\ P\ \{ s = x^N \}$

Cerchiamo un invariante

Simuliamo i primi passi di un'esecuzione

i	0	1	2	3	...
s	1	x	x^2	x^3	...

Esercizi

P =
```
i := 0; s := 1;
while i < N do
    i := i + 1;
    s := s * x
endwhile
```
(A = i := 0; s := 1; — W = while i < N do ... endwhile — C = i := i + 1; s := s * x)

? $\{ N \geq 0 \}\ P\ \{ s = x^N \}$

Cerchiamo un invariante

Simuliamo i primi passi di un'esecuzione

i	0	1	2	3	...
s	1	x	x^2	x^3	...

Ipotesi: $s = x^i$ è un invariante

? $\{ s = x^i \wedge i < N \}\ C\ \{ s = x^i \}$

$C\{ s = x^i \} \Rightarrow \vdash_{ASS} \{ sx = x^{i+1} \}\ C\ \{ s = x^i \}$

[ASSEGNAMENTI INDIPENDENTI !]

$sx = x^{i+1} \Rightarrow sx = xx^i \Rightarrow s = x^i$

$\vdash \{ s = x^i \}\ C\ \{ s = x^i \}$

$(s = x^i \wedge i < N) \rightarrow s = x^i$

$\vdash_{IMPL} \{ s = x^i \wedge i < N \}\ C\ \{ s = x^i \}$

$\vdash_{ITER} \{ s = x^i \}\ W\ \{ s = x^i \wedge i \geq N \}$ (1)

La postcondizione di (1) non implica $s = x^N$

Dobbiamo rafforzare l'invariante

Esercizi

Ipotesi: $i \leq N$ è un invariante

? $\{i \leq N \wedge i < N\}\ C\ \{i \leq N\}$

$C\{i \leq N\} \Rightarrow \vdash_{ASS} \{i+1 \leq N\}\ C\ \{i \leq N\}$

$i < N \Rightarrow i+1 \leq N$

$\vdash_{IMPL} \{i < N\}\ C\ \{i \leq N\}$

$\vdash_{ITER} \{i \leq N\}\ W\ \{i \leq N \wedge i \geqslant N\}$

$\Downarrow\Downarrow$

$i = N$

Combinando i due invarianti

$\vdash_{ITER} \{S = X^i \wedge i \leq N\}\ W\ \{S = X^i \wedge i = N\}$

$\Downarrow\Downarrow$

$S = X^N$

Resta da dimostrare che dopo gli assegnamenti iniziali vale l'invariante:

? $\{N \geqslant 0\}\ A\ \{S = X^i \wedge i \leq N\}$

Applichiamo due volte la regola dell'assegnamento, ragionando a ritroso

, $S := 1\ \{S = X^i \wedge i \leq N\} \Rightarrow$

$\vdash_{ASS} \{1 = X^i \wedge i \leq N\}\ S := 1\ \{S = X^i \wedge i \leq N\}$

$i := 0\ \{1 = X^i \wedge i \leq N\} \Rightarrow$

$\vdash_{ASS} \{1 = X^0 \wedge \underline{0 \leq N}\}\ i := 0\ \{1 = X^i \wedge i \leq N\}$

$\Downarrow\Downarrow$

true

↳ precondizione del programma

$\vdash_{SEQ} \{N \geqslant 0\}\ A\ \{S = X^i \wedge i \leq N\}$

Combinando i pezzi con la regola della sequenza ...

Esercizi

P [quo := 0; rem := x;]A
while [rem >= y]B do
rem := rem - y;
quo := quo + 1]C
endwhile]W

$? \{ x \geq 0 \wedge y \geq 0 \}\ P\ \{ q \}$

$q \equiv (x = quo \cdot y + rem \wedge 0 \leq rem < y)$

Cerchiamo un invariante

OSSERVAZIONE $rem < y \equiv \neg B$

Simulazione
Poniamo $x = 26$ $y = 5$

quo	0	1	2	3	4	5
rem	26	21	16	11	6	1

Ipotesi: $x = quo \cdot y + rem$ è invariante
$rem \geq 0$ è invariante

$? \{ \boxed{x = quo \cdot y + rem \wedge rem \geq 0}^{inv} \wedge rem \geq y \}\ C\ \{ inv \}$

$\vdash_{ASS} \{ x = (quo+1)y + (rem - y) \wedge rem - y \geq 0 \}\ C\ \{ inv \}$

$\vdash \{ x = quo \cdot y + rem \wedge \boxed{rem \geq y} \}\ C\ \{ inv \}$
↳ B!
SAPPIAMO CHE $y \geq 0$

$\vdash_{ITER} \{ x = quo \cdot y + rem \wedge rem \geq 0 \}\ W\ \{ x = quo \cdot y + rem \wedge rem \geq 0 \wedge rem < y \}$

Dobbiamo dimostrare che l'invariante vale dopo gli assegnamenti iniziali (e che $y \geq 0$ dopo gli assegnamenti iniziali:

Correttezza totale

$\{p\}$ while B do C endwhile $\{q\}$

$\{p\}\ \underbrace{\text{while B do C endwhile}}_{W}\ \{q\}$

C. parziale "se si esegue W a partire da uno stato in cui vale p e l'esecuzione termina, nello stato finale vale q"

C. totale "se si esegue W a partire da uno stato in cui vale p, l'esecuzione termina e nello stato finale vale q"

$\vdash^{parz} \{p\}\ C\ \{q\}$ $\qquad$ $\vdash^{TOT} \{p\}\ C\ \{q\}$

$\models \{p\}\ C\ \{q\}$

Correttezza totale

while B do C endwhile

W

Tecnica di dimostrazione

Supponiamo che E sia un'espressione aritmetica nella quale compaiono variabili del programma, costanti numeriche e operazioni aritmetiche, e che inv sia un invariante di ciclo per W, scelti in modo che:

1. $inv \rightarrow E \geq 0$
2. $\vdash_{TOT} \{ inv \wedge B \wedge E = k > 0 \}\ C\ \{ inv \wedge E < k \}$

Correttezza totale

while B do C endwhile

W

Tecnica di dimostrazione

Supponiamo che E sia un'espressione aritmetica nella quale compaiono variabili del programma, costanti numeriche e operazioni aritmetiche, e che inv sia un invariante di ciclo per W, scelti in modo che:

1. $inv \rightarrow E \geq 0$
2. $\vdash_{TOT} \{ inv \wedge B \wedge E = k > 0 \}\ C\ \{ inv \wedge E < k \}$

Allora: $\vdash_{TOT} \{ inv \}\ C\ \{ inv \wedge \neg B \}$

- E non è una formula logica $E \geq 0$ è una formula logica
- Lo $\emptyset$ in $E \geq 0$ può essere sostituito da qualsiasi numero

Logica di Hoare – correttezza totale

Cominciamo da un esempio elementare

```
while   x > 5   do
    x := x - 1
endwhile
```

$\{x > 5\} \quad P \quad \{x = 5\}$

Logica di Hoare – correttezza totale

Cominciamo da un esempio elementare

```
while   x > 5   do
    x := x - 1
endwhile
```

$\{x > 5\} \quad P \quad \{x = 5\}$

Dobbiamo cercare un variante E, cioè un'espressione il cui valore decresce a ogni esecuzione del corpo dell'iterazione, e un invariante i che garantisca che l'espressione ha sempre valore maggiore o uguale a 0.

Logica di Hoare – correttezza totale

Cominciamo da un esempio elementare

```
while   x > 5   do
    x := x - 1
endwhile
```

$\{x > 5\} \quad P \quad \{x = 5\}$

Dobbiamo cercare un variante E, cioè un'espressione il cui valore decresce a ogni esecuzione del corpo dell'iterazione, e un invariante i che garantisca che l'espressione ha sempre valore maggiore o uguale a 0.

$$i \rightarrow E \geq 0 \qquad \{i \wedge B \wedge E = E_0\} C \{i \wedge E < E_0\}$$

Logica di Hoare – correttezza totale

Cominciamo da un esempio elementare

```
while   x > 5   do
    x := x - 1
endwhile
```

$\{x > 5\} \quad P \quad \{x = 5\}$

Dobbiamo cercare un variante E, cioè un'espressione il cui valore decresce a ogni esecuzione del corpo dell'iterazione, e un invariante i che garantisca che l'espressione ha sempre valore maggiore o uguale a 0.

$$i \rightarrow E \geq 0 \qquad \{i \wedge B \wedge E = E_0\} C \{i \wedge E < E_0\}$$

Soluzione: $E : x - 5 \qquad i : x \geq 5$

Dimostrazione-1

Poniamo

$$i : x \geq 5 \qquad B : x > 5 \qquad E : x - 5$$

Dimostrazione-1

Poniamo

$$i : x \geq 5 \qquad B : x > 5 \qquad E : x - 5$$

Osserviamo che $i \rightarrow E \geq 0$

Dimostrazione-1

Poniamo

$$i : x \geq 5 \qquad B : x > 5 \qquad E : x - 5$$

Osserviamo che $i \rightarrow E \geq 0$

Dobbiamo dimostrare la seguente tripla

$$\{i \wedge B \wedge x - 5 = E_0\} \quad \texttt{x} := \texttt{x} - 1 \quad \{i \wedge x - 5 < E_0\}$$

Dimostrazione-1

Poniamo

$$i : x \geq 5 \qquad B : x > 5 \qquad E : x - 5$$

Osserviamo che $i \rightarrow E \geq 0$

Dobbiamo dimostrare la seguente tripla

$$\{i \wedge B \wedge x - 5 = E_0\} \quad \mathtt{x} := \mathtt{x} - 1 \quad \{i \wedge x - 5 < E_0\}$$

Applichiamo la regola dell'assegnamento e otteniamo la precondizione

$$x - 1 \geq 5 \wedge x - 1 - 5 < E_0$$

Dimostrazione-1

Poniamo

$$i : x \geq 5 \qquad B : x > 5 \qquad E : x - 5$$

Osserviamo che $i \rightarrow E \geq 0$

Dobbiamo dimostrare la seguente tripla

$$\{i \wedge B \wedge x - 5 = E_0\} \quad \mathtt{x} := \mathtt{x} - 1 \quad \{i \wedge x - 5 < E_0\}$$

Applichiamo la regola dell'assegnamento e otteniamo la precondizione

$$x - 1 \geq 5 \wedge x - 1 - 5 < E_0$$

che diventa

$$x \geq 6 \wedge x - 6 < E_0$$

Dimostrazione-2

Poiché $(i \wedge B \wedge x - 5 < E_0) \rightarrow (x \geq 6 \wedge x - 6 < E_0)$, possiamo applicare la regola di derivazione della conseguenza e derivare la tripla richiesta.

Dimostrazione-2

Poiché $(i \wedge B \wedge x - 5 < E_0) \rightarrow (x \geq 6 \wedge x - 6 < E_0)$, possiamo applicare la regola di derivazione della conseguenza e derivare la tripla richiesta.

Come cambia la dimostrazione se B diventa `x != 5`?

Dimostrazione-2

Poiché $(i \wedge B \wedge x - 5 < E_0) \rightarrow (x \geq 6 \wedge x - 6 < E_0)$, possiamo applicare la regola di derivazione della conseguenza e derivare la tripla richiesta.

Come cambia la dimostrazione se B diventa `x != 5`?

Quali sono i passi della dimostrazione di correttezza parziale?

Dimostrazione-2

Poiché $(i \wedge B \wedge x - 5 < E_0) \rightarrow (x \geq 6 \wedge x - 6 < E_0)$, possiamo applicare la regola di derivazione della conseguenza e derivare la tripla richiesta.

Come cambia la dimostrazione se B diventa `x != 5`?

Quali sono i passi della dimostrazione di correttezza parziale?

Se il programma fosse while x != 5 do x := x-2 endwhile ?

Che cosa fare se nessuna variabile viene decrementata?

```
while   x < 5   do
    x := x + 1
endwhile
```

$\{x < 5\} \quad P \quad \{x = 5\}$

Che cosa fare se nessuna variabile viene decrementata?

```
while   x < 5   do
    x := x + 1
endwhile
```

$\{x < 5\} \quad P \quad \{x = 5\}$

$i : x \leq 5 \qquad E : 5 - x$

ESERCIZIO CPS-1 *prima parte*

①

```
p := 1;  y := b;              ] A
while  y > 0  do
    p := p * x;    c1 ]
    y := y - 1     c2 ] C
endwhile
```

(W = ciclo while; P = intero programma)

② ? $\{ b \geq 0 \}\ P\ \{ p = x^b \}$

③ Cerchiamo un invariante per W:

p	1	x	x^2	x^3	...
y	b	b-1	b-2	b-3	...

Ipotesi: $inv \equiv \boxed{p = x^{b-y} \wedge y \geq 0}$

④ Dimostriamo che inv è un invariante di ciclo per W

? $\{p = x^{b-y} \wedge y \geq 0 \wedge y > 0\}\ C\ \{p = x^{b-y} \wedge y \geq 0\}$

Partendo dalla postcondizione, applichiamo la regola dell'assegnamento (c_1 e c_2 sono indipendenti ⇒ sostituzioni simultanee)

$$C\ \{ p = x^{b-y} \wedge y \geq 0 \}$$

$$\Downarrow$$

$$\vdash^{AS} \{ px = x^{b-(y-1)} \wedge y-1 \geq 0 \}\ C\ \{ inv \}$$

$$\Downarrow$$

$$\vdash \{ px = x^{b-y+1} \wedge y-1 \geq 0 \}\ C\ \{ inv \}$$

$$\vdash \{ p = x^{b-y} \wedge y > 0 \}\ C\ \{ inv \}$$

$$\vdash^{CONS} \{ inv \wedge y > 0 \}\ C\ \{ inv \}$$

ESERCIZIO CPS-1 seconda parte

$$\vdash^{\text{ITER}}_{P} \{p = x^{b-y} \wedge y \geq 0\}\, W\, \{p = x^{b-y} \wedge y \geq 0 \wedge \underbrace{\boxed{y \leq 0}}_{\neg B}\}$$

$$\Downarrow\Uparrow$$

$$\underbrace{y \geq 0 \wedge y \leq 0}_{y = 0}$$

$$\vdash \{p = x^{b-y} \wedge y \geq 0\}\, W\, \{p = x^{b}\}$$

(5) Dobbiamo dimostrare che l'invariante è valido dopo A

$$? \quad \{b \geq 0\}\, A\, \{p = x^{b-y} \wedge y \geq 0\}$$

Regola dell'assegnamento (assegnamenti indipendenti)

$$A\, \{p = x^{b-y} \wedge y \geq 0\}$$

$$\Downarrow\Uparrow$$

$$\vdash^{\text{AS}} \{\underbrace{1 = x^{b-b}}_{\text{true}} \wedge\ b \geq 0\}\, A\, \{inv\}$$

(6) Applicando la regola della sequenza, concludiamo la dimostrazione

$$\{b \geq 0\}\, A\, \{inv\}$$

$$\{inv\}\, W\, \{p = x^{b}\}$$

$$\vdash^{\text{SEQ}}_{P} \{b \geq 0\}\, P\, \{p = x^{b}\}$$

(7) La dimostrazione di correttezza totale è molto semplice ed è lasciata al lettore.

ESERCIZIO CPS-2 prima parte

①

```
z := 1 ;
while  x > 0  do
    z := z * x ;
    x := x - 1
endwhile
```

P = W = C

② $\{ x \geq 0 \}\ P\ \{ ? \}$

Informalmente, P calcola $x!$, ma non possiamo scrivere $\{x \geq 0\}\ P\ \{z = x!\}$, perché nello stato finale x vale 0

Introduciamo una variabile ausiliaria x_0 per "bloccare" il valore iniziale di x

? $\{ x = x_0 \wedge x \geq 0 \}\ P\ \{ z = x_0! \}$

③ Cerchiamo un invariante per W

z	1	x_0	$x_0(x_0-1)$	...
x	x_0	x_0-1	x_0-2	..

Possiamo scrivere $z = \dfrac{x_0(x_0-1)(x_0-2)!}{(x_0-2)!} = \dfrac{x_0!}{(x_0-2)!}$

$\Rightarrow$ candidato invariante: $z = \dfrac{x_0!}{x!}$

aggiungiamo $x \geq 0$

? $\left\{ z = \dfrac{x_0!}{x!} \wedge x \geq 0 \wedge x > 0 \right\}\ C\ \left\{ z = \dfrac{x_0!}{x!} \wedge x \geq 0 \right\}$

Applichiamo la regola dell'assegnamento

$$\vdash_{AS} \left\{ z = \frac{x_0!}{(x-1)!},\ x-1 \geq 0 \right\}\ x := x-1\ \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\}$$

$$\vdash_{AS} \left\{ zx = \frac{x_0!}{(x-1)!},\ x-1 \geq 0 \right\}\ z := z*x\ \left\{ z = \frac{x_0!}{(x-1)!},\ x-1 \geq 0 \right\}$$

ESERCIZIO CPS-2 seconda parte

(3) CONTINUA

Manipoliamo algebricamente l'ultima precondizione. Da $x-1 \geq 0$, ricaviamo $x > 0$; possiamo quindi dividere per x, ottenendo $x = \frac{x_0!}{x!}$.

Applicando la regola della conseguenza e la regola della concatenazione, otteniamo

$$\vdash \left\{ z = \frac{x_0!}{x!} \;,\; x \geq 0,\; x > 0 \right\} C \left\{ z = \frac{x_0!}{x!} \;,\; x \geq 0 \right\}$$

che era il nostro obiettivo: la formula $z = \frac{x_0!}{x!} \wedge x \geq 0$ è un invariante di ciclo per W.

(4) Applicando la regola dell'iterazione, deriviamo

$$\vdash \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\} W \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \wedge x \leq 0 \right\}$$

da cui, usando $(x \geq 0 \wedge x \leq 0) \rightarrow x = 0$ e $0! = 1$,

$$\vdash \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\} W \left\{ x = 0 \wedge z = x_0! \right\}$$

(5) Per completare la dimostrazione di correttezza parziale, dobbiamo mostrare che, dopo l'esecuzione di $z := 1$, l'invariante è verificato.

? $$\left\{ \begin{matrix} x = x_0 \\ \wedge \\ x \geq 0 \end{matrix} \right\} z := 1 \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\}$$

Applichiamo la regola dell'assegnamento:

$$z := 1 \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\}$$

$$\Downarrow$$

$$\vdash \left\{ 1 = \frac{x_0!}{x!} \wedge x \geq 0 \right\} z := 1 \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\}$$

Abbiamo $x = x_0 \rightarrow \frac{x_0!}{x!} = 1$. Per conseguenza,

$$\vdash \left\{ x = x_0 \wedge x \geq 0 \right\} z := 1 \left\{ z = \frac{x_0!}{x!} \wedge x \geq 0 \right\}$$

(6) Incollando i pezzi con la regola di concatenazione, deriviamo la tripla $\left\{ x = x_0 \wedge x \geq 0 \right\} P \left\{ z = \frac{x_0!}{x!} \right\}$

(7) La dimostrazione di correttezza totale in questo esempio è molto semplice, ed è lasciata al lettore.