Informatica — 2020-01-20

Nota: Scrivete su **tutti** i fogli nome e matricola.

Esercizio 1. *Si fornisca la definizione di validità per una tripla di Hoare, commentandola sinteticamente. Dopo, si enunci il teorema di correttezza per il sistema deduttivo delle triple di Hoare, anche qui commentandolo sinteticamente.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di numeri naturali (regole $[S0], [S1]$), una relazione $\Sigma \in \mathcal{P}(S \times \mathbb{N})$ (regole $[\Sigma 0], [\Sigma 1]$) e una relazione $R \in \mathcal{P}(S \times S \times S)$ (regole $[R0], [R1]$). Sotto, n, k, k_1, k_2 indicano naturali mentre s, s_1, s_2, s_3 indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{n : s}(n \in \mathbb{N})[S1] \qquad \frac{}{\Sigma(\epsilon,\ 0)}[\Sigma 0] \qquad \frac{\Sigma(s,\ k)}{\Sigma(n : s,\ n + k)}[\Sigma 1]$$

$$\frac{}{R(\epsilon,\ s,\ s)}[R0] \qquad \frac{R(s_1,\ n : s_2,\ s_3)}{R(n : s_1,\ s_2,\ s_3)}[R1]$$

1. *[20%] Si fornisca una sequenza s per cui valga $R(1 : 2 : \epsilon, 3 : 4 : \epsilon, s)$ e si giustifichi la risposta esibendo una derivazione.*

2. *[20%] Si enunci il principio di induzione associato alla relazione R.*

3. *[10%] Si consideri l'enunciato seguente:*

   $$\forall s_1, s_2, s_3 \in S.\ \forall k_1, k_2 \in \mathbb{N}.\ R(s_1, s_2, s_3) \land \Sigma(s_1, k_1) \land \Sigma(s_2, k_2) \implies \Sigma(s_3, k_1 + k_2)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s_1, s_2, s_3 \in S.\ R(s_1, s_2, s_3) \implies p(s_1, s_2, s_3)$$

   per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R.*

Soluzione (bozza).
Parte 1.

$$\dfrac{\dfrac{\dfrac{}{R(\epsilon, 2 : 1 : 3 : 4 : \epsilon, 2 : 1 : 3 : 4 : \epsilon)}[R0]}{R(2 : \epsilon, 1 : 3 : 4 : \epsilon, 2 : 1 : 3 : 4 : \epsilon)}[R1]}{R(1 : 2 : \epsilon, 3 : 4 : \epsilon, 2 : 1 : 3 : 4 : \epsilon)}[R1]$$

Parte 2.
Per potere dimostrare che $p(s_1, s_2, s_3)$ vale per ogni s_1, s_s, s_3 che soddisfano $R(s_1, s_2, s_3)$ è sufficiente dimostrare che:

$$1)\forall s.\ p(\epsilon, s, s)$$
$$2)\forall n, s_1, s_2, s_3.\ p(s_1, n : s_2, s_3) \implies p(n : s_1, s_2, s_3)$$

Parte 3.
Basta prendere $p(s_1, s_2, s_3)$ uguale a

$$\forall k_1, k_2 \in \mathbb{N}.\ \Sigma(s_1, k_1) \land \Sigma(s_2, k_2) \implies \Sigma(s_3, k_1 + k_2)$$

Parte 4.
Per induzione su R, procediamo così.

Caso R0. Bisogna dimostrare che per ogni s vale $p(\epsilon, s, s)$, e cioè

$$\forall k_1, k_2 \in \mathbb{N}.\ \Sigma(\epsilon, k_1) \wedge \Sigma(s, k_2) \implies \Sigma(s, k_1 + k_2)$$

Assumiamo quindi $IP1 : \Sigma(\epsilon, k_1)$ e $IP2 : \Sigma(s, k_2)$, andando a dimostrare la nuova tesi $\Sigma(s, k_1 + k_2)$.

Invertiamo $IP1$: siccome può essere derivata solo dalla regola $\Sigma 0$, otteniamo $k_1 = 0$. La tesi si riscrive quindi come $\Sigma(s, k_2)$, che è $IP2$.

Caso R1. Assumendo come ipotesi induttiva $IP1 : p(s_1, n : s_2, s_3)$, dimostriamo $p(n : s_1, s_2, s_3)$. L'ipotesi $IP1$ è

$$\forall \bar{k}_1, \bar{k}_2 \in \mathbb{N}.\ \Sigma(s_1, \bar{k}_1) \wedge \Sigma(n : s_2, \bar{k}_2) \implies \Sigma(s_3, \bar{k}_1 + \bar{k}_2)$$

mentre la tesi è

$$\forall k_1, k_2 \in \mathbb{N}.\ \Sigma(n : s_1, k_1) \wedge \Sigma(s_2, k_2) \implies \Sigma(s_3, k_1 + k_2)$$

Assumiamo quindi $IP2 : \Sigma(n : s_1, k_1)$ e $IP3\Sigma(s_2, k_2)$, andando a dimostrare la nova tesi $\Sigma(s_3, k_1 + k_2)$.

Invertiamo $IP2$: siccome è derivabile solo da $\Sigma 1$, si ottiene $IP4 : R(s_1, k)$ e $k_1 = n + k$ per qualche k.

La tesi diventa quindi $\Sigma(s_3, n + k + k_2)$.

Usiamo ora $IP1$ scegliendo $\bar{k}_1 = k$ e $\bar{k}_2 = n + k_2$, ottenendo

$$\Sigma(s_1, k) \wedge \Sigma(n : s_2, n + k_2) \implies \Sigma(s_3, k + n + k_2)$$

L'antecedente è vera. Infatti $\Sigma(s_1, k)$ è $IP4$, mentre $\Sigma(n : s_2, n + k_2)$ si deriva usando la regola $\Sigma 1$ a partire da $\Sigma(s_2, k_2)$, che è proprio $IP3$.

Da questo, ricaviamo la conseguente $\Sigma(s_3, k + n + k_2)$, che è la tesi.

□

Esercizio 3. *Si considerino i seguenti comandi di IMP, esteso in modo da usare espressioni booleane come guardie per i cicli* while. *Sotto, ϕ e ψ sono espressioni booleane arbitrarie, mentre c è un comando arbitrario.*

$$w_1 = \textsf{while } \phi \textsf{ do } c \qquad\qquad w_2 = (\textsf{while } \phi \wedge \psi \textsf{ do } c); (\textsf{while } \phi \textsf{ do } c)$$
$$w_3 = (\textsf{while } \phi \vee \psi \textsf{ do } c); (\textsf{while } \phi \textsf{ do } c)$$

1. *[50%] Si affermi se, in generale, i comandi w_1 e w_2 sono equivalenti.*
   In caso affermativo, si giustifichi la risposta descrivendo in modo informale ma preciso come una derivazione relativa alla semantica di w_1 si può trasformare in una derivazione per la semantica di w_2, e viceversa.
   In caso negativo, si definiscano ϕ, ψ, c e gli stati iniziale e finale σ, σ' in modo da fornire un controesempio. Si giustifichi in modo informale perché i due comandi non sono equivalenti.

2. *[50%] Si ripeta il punto precedente su w_1 e w_3.*

Soluzione (bozza).

Parte 1.

I comandi w_1 e w_2 sono equivalenti.

Una derivazione per w_1, essendo un ciclo while, sarà formata da $n \geq 0$ usi della regola $While - True$ (e $Comp$) con in cima un singolo uso della regola $While - False$. Questo n è il numero di volte che viene eseguito c, e nella derivazione si troveranno gli stati $\sigma_0, \sigma_1, \ldots, \sigma_n$ dove σ_i è lo stato delle variabili subito dopo che il corpo c è stato eseguito i volte.

Da questa, una derivazione per w_2 si costruisce come segue. Sia k il massimo i tale che σ_i rende vera $\phi \wedge \psi$. La derivazione per w_2 sarà un uso di $Comp$, con sopra due derivazioni per i due while in w_2. La prima derivazione è formata da k usi di $While - True$ (e uno di $While - False$), e contiene come stati intermedi $\sigma_0, \ldots, \sigma_k$. Per costruzione, la guardia $\phi \wedge \psi$ è sempre vera per k volte, e diventa falsa subito dopo, quindi $While - True$ viene usata k volte. $k \leq n$ perchè dopo n iterazioni ϕ è falsa e quindi pure $\phi \wedge \psi$. La seconda derivazione contiene $n - k$ usi di $While - True$ (e uno di $While - False$), e contiene come stati intermedi $\sigma_k, \ldots, \sigma_n$.

Per l'altra direzione, da w_2 a w_1, si procede in modo simile. Una derivazione di w_2 deve contenere due derivazioni per i due while, che effettuano rispettivamente (diciamo) k_1 e k_2 iterazioni. La derivazione per w_1 conterrà $k_1 + k_2$ iterazioni, riusando gli stati intermedi delle due derivazioni di cui sopra. In queste, ϕ è sempre vera tranne all'ultima iterazione (perchè viene dalla seconda derivazione), quindi gli usi di $While - True$ sono corretti.

Parte 2.

I comandi non sono equivalenti, in generale. Per esempio,

$$w_1 = \mathsf{while}\ x < 4\ \mathsf{do}\ x := x + 1$$

eseguito in uno stato iniziale tale che $\sigma(x) = 0$, termina in un σ' tale che $\sigma'(x) = 4$. Invece,

$$w_3 = (\mathsf{while}\ x < 4 \vee x < 5\ \mathsf{do}\ x := x + 1); (\mathsf{while}\ x < 4\ \mathsf{do}\ x := x + 1)$$

eseguito nello stesso σ, termina in un σ'' con $\sigma''(x) = 5$. Più precisamente, il primo while dentro w_3 esegue 5 iterazioni e il secondo nessuna.

□

Nome _____ Matricola _____

Esercizio 4. *Si dimostri formalmente la validità della tripla di Hoare seguente riempiendo le linee sottostanti con opportune asserzioni.*

$\{n = N \geq 0\}$

$x := 0;$

$y := 1;$

---

while $n \neq 0$ do

$y := (x + 1) * y;$

$x := x + 2;$

$y := x * y;$

$n := n - 1$

$\{y = (2N)!\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{0 = 2(N-n) \wedge 1 = 0!\}$
$x := 0;$
$\{x = 2(N-n) \wedge 1 = x!\}$
$y := 1;$
$\{INV : x = 2(N-n) \wedge y = x!\}$
while $n \neq 0$ do
    $\{INV \wedge n \neq 0\}$ (2)
    $\{x+2 = 2(N-(n-1)) \wedge (x+2)(x+1)y = (x+2)!\}$
    $y := (x+1) * y;$
    $\{x+2 = 2(N-(n-1)) \wedge (x+2)y = (x+2)!\}$
    $x := x+2;$
    $\{x = 2(N-(n-1)) \wedge xy = x!\}$
    $y := x * y;$
    $\{x = 2(N-(n-1)) \wedge y = x!\}$
    $n := n-1$
$\{INV \wedge \neg(n \neq 0)\}$ (3)
$\{y = (2N)!\}$

Per le PrePost:

1) Banale aritmetica.

2) Per la prima equazione $x+2 = 2(N-(n-1))$ basta usare INV $(x = 2(N-n))$ e si ha $x+2 = 2(N-n)+2 = 2N-2n+2 = 2(N-(n-1))$. Per la seconda, basta usare INV $(y = x!)$ e osservare che $(x+2)(x+1)y = (x+2)(x+1)(x!) = (x+2)!$.

3) Dalle ipotesi si ha $n = 0$, e quindi da INV si ha $x = 2N$, per cui $y = x! = (2N)!$.

□