Informatica — 2023-01-23

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

Esercizio 1. *Si forniscano le regole della semantica big step per i comandi di IMP* $(\to_b)$*. Si fornisca anche la segnatura della relazione semantica* $(\to_b) \in \mathcal{P}(\ldots)$*, descrivendo brevemente gli insiemi che appaiono in essa.*

Esercizio 2. *Sia* $f : \mathbb{N} \to (\mathbb{N} \times \mathbb{N})$ *un funzione arbitraria. Le seguenti regole definiscono induttivamente l'insieme* S *delle sequenze di naturali (regole* $[S0], [S1]$*) e una relazione* $U \in \mathcal{P}(\mathbb{N} \times S)$ *(regole* $[U0], [U1]$*). Sotto,* n, k, l, a, b *indicano naturali, mentre* s *indica una sequenza in* S*.*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{n : s}(n \in \mathbb{N})[S1] \qquad \frac{}{U(0, \epsilon)}[U0] \qquad \frac{U(b,\ s)}{U(n+1,\ a : s)}(f(n) = (a, b))[U1]$$

1. *[20%] Si trovi una funzione* f *tale per cui la relazione* U *definita sopra soddisfi* $U(1,\ 1 : 2 : 3 : \epsilon)$*. Si giustifichi la risposta esibendo una derivazione, includendo anche il risultato di* f *negli usi della regola* $[U1]$*.*

   Nota bene*: i punti seguenti sono da risolversi con* f *funzione arbitraria.*

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

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

$$\forall n \in \mathbb{N}, s \in S.\ U(n, s) \wedge n \neq 0 \implies \exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall n \in \mathbb{N}, s \in S.\ U(n, s) \implies p(n, s)$$

   per un qualche predicato p*.*

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

Soluzione (bozza).
Parte 1

Un possibile esempio è prendere $f(2) = (3, 0)$ e $f(n) = (n + 1, n + 2)$ per $n \neq 2$.

$$\dfrac{\dfrac{\dfrac{\overline{U(0, \epsilon)}}{U(3, 3 : \epsilon)}(f(2) = (3, 0))}{U(2, 2 : 3 : \epsilon)}(f(1) = (2, 3))}{U(1, 1 : 2 : 3 : \epsilon)}(f(0) = (1, 2))$$

Parte 2
Per dimostrare che per ogni n, s tali che $U(n, s)$ vale $p(n, s)$ basta che:

$U0)$ $p(0, \epsilon)$
$U1)$ $\forall n, a, b \in \mathbb{N}, s \in S.\ p(b, s) \wedge f(n) = (a, b) \implies p(n + 1, a : s)$

Parte 3

Basta prendere $p(n, s) : n \neq 0 \implies \exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$.

Parte 4
Caso $U0$

Bisogna dimostrare $p(0, \epsilon)$ e cioè $0 \neq 0 \implies \exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$. Assumendo l'ipotesi $0 \neq 0$ ricaviamo un assurdo.

Caso $U1$

Assumiamo come ipotesi induttiva $IP1 : p(b, s)$ e la condizione a lato $IP2 : f(n) = (a, b)$. La prima si riscrive come

$$IP1 : b \neq 0 \implies \exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$$

Procediamo a dimostrare la tesi $p(n + 1, a : s)$, cioè:

$$n + 1 \neq 0 \implies \exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$$

Assumiamo l'ipotesi (inutile) $n + 1 \neq 0$ e dimostriamo

$$\exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$$

Ora, procediamo per casi su b: si ha $b = 0$ oppure $b \neq 0$. Se fosse $b = 0$, allora per $IP2$ si ha $f(n) = (a, 0)$ da cui la tesi scegliendo $k = n, l = a$. Se invece fosse $b \neq 0$, possiamo applicate $IP1$ che fornisce $\exists k, l \in \mathbb{N}.\ f(k) = (l, 0)$ che è la tesi. □

Esercizio 3. *Nel linguaggio IMP, si supponga* $Var = VarP \cup VarD$ *per due insiemi infiniti disgiunti* $VarP$ *e* $VarD$*. Si supponga che gli operatori aritmetici usati nella definizione di Exp siano solo* $+, -, *$*. Si definisca inoltre* $State^* \subseteq State$ *come segue:*

$$State^* = \{\sigma : Var \to \mathbb{Z} \mid \forall x \in VarP.\ \sigma(x)\ pari \wedge \forall y \in VarD.\ \sigma(y)\ dispari\}$$

1. *[70%] Si definisca induttivamente, tramite regole di inferenza, una relazione* $R \in \mathcal{P}(Exp \times \{0, 1\})$ *tale che:*
   (a) R *è una funzione* $Exp \to \{0, 1\}$*;*
   (b) *Per ogni* $e \in Exp, n \in \{0, 1\}, v \in \mathbb{Z}, \sigma \in State^*$ *se vale* $R(e, n) \wedge \langle e, \sigma\rangle \to_e v$ *allora* $\exists k \in \mathbb{Z}.\ v = 2k + n$*.*
2. *[30%] Si dia una giustificazione informale ma precisa per le due proprietà sopra, relativamente alle tre regole che ritenete più significative. Non vi si chiede di esaminare gli altri casi.*

Soluzione (bozza).

Parte 1.

Una possibile soluzione è

$$\frac{}{R(2z, 0)}(z \in \mathbb{Z})[LitP] \qquad \frac{}{R(2z + 1, 1)}(z \in \mathbb{Z})[LitD]$$

$$\frac{}{R(x, 0)}(x \in VarP)[VarP] \qquad \frac{}{R(y, 1)}(y \in VarD)[VarD]$$

$$\frac{R(e_1, n) \quad R(e_2, n)}{R(e_1 + e_2, 0)}[PlusP] \qquad \frac{R(e_1, n_1) \quad R(e_2, n_2) \quad n_1 \neq n_2}{R(e_1 + e_2, 1)}[PlusD]$$

$$\frac{R(e_1, n) \quad R(e_2, n)}{R(e_1 - e_2, 0)}[MinusP] \qquad \frac{R(e_1, n_1) \quad R(e_2, n_2) \quad n_1 \neq n_2}{R(e_1 - e_2, 1)}[MinusD]$$

$$\frac{R(e_1, n_1) \quad R(e_2, n_2)}{R(e_1 * e_2, n_1 \cdot n_2)}[Times]$$

Parte 2.

Note: qui sotto si considerano velocemente tutti i casi, ma per l'esame bastava giustificare tre regole.

Per la proprietà (a), R è una funzione perché ogni forma di espressione ha esattamente una regola che la gestisce. Per esempio, $e_1 * e_2$ è gestita solo dalla $[Times]$, mentre un letterale è gestito da $[LitP]$ se è pari, altrimenti da $[LitD]$. Anche un'espressione $e_1 + e_2$ è gestita da una sola regola: per potesi induttiva esistono unici n_1 e n_2 tali che $R(e_1, n_1)$ e $R(e_2, n_2)$. Quindi, se $n_1 = n_2$ si applica solo $[PlusP]$, altrimenti solo $[PlusD]$. I casi $x \in Var$ e $e_1 - e_2$ sono simili.

Per la proprietà (b), esaminiamo i casi.

Le regole $[LitP]$ e $[LitD]$ controllano la parità dei letterali. Ai letterali pari viene associato 0, mentre a quelli dispari 1.

La semantica dei letterali fa sì che il risultato v sia il letterale stesso. Quindi la tesi si riduce a $\exists k \in \mathbb{Z}.\ 2z = 2k + 0$ o a $\exists k \in \mathbb{Z}.\ 2z + 1 = 2k + 1$ che sono banali.

Per le variabili e le regole $[VarP], [VarD]$, il ragionamento è simile, e si sfrutta il fatto che $\sigma(x)$ è pari per $x \in VarP$ e dispari per $x \in VarD$.

Per $[PlusP]$ e $e_1 + e_2$, l'ipotesi induttiva dice che $\exists k_1 \in \mathbb{Z}.\ v_1 = 2k_1 + n$ e $\exists k_2 \in \mathbb{Z}.\ v_2 = 2k_2 + n$, quindi $v_1 + v_2 = 2(k_1 + k_2 + n)$ dà la tesi.

Per $[PlusD]$ e $e_1 + e_2$, l'ipotesi induttiva dice che $\exists k_1 \in \mathbb{Z}.\ v_1 = 2k_1 + n_1$ e $\exists k_2 \in \mathbb{Z}.\ v_2 = 2k_2 + n_2$ con $n_1 \neq n_2$, quindi $v_1 + v_2 = 2(k_1 + k_2) + 1$ dà la tesi.

I casi $[MinusP], [MinusD]$ sono analoghi.

Per $[Times]$ e $e_1 * e_2$, l'ipotesi induttiva dice che $\exists k_1 \in \mathbb{Z}.\ v_1 = 2k_1 + n_1$ e $\exists k_2 \in \mathbb{Z}.\ v_2 = 2k_2 + n_2$, quindi $v_1 \cdot v_2 = 2(k_1k_2 + k_1n_2 + k_2n_1) + n_1n_2$ dà la tesi.

□

Nome _____ Matricola _____

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

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

$y := 0;$

$x := 5;$

---

while $y < n$ do

$x := x - 2;$

$y := y + 1;$

$x := 2 * x$

$\{x = 2^N + 4\}$

Si giustifichino qui sotto gli eventuali usi della regola $PrePost$.

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{5 = 2^0 + 4 \wedge 0 \leq n = N\}$
$y := 0;$
$\{5 = 2^y + 4 \wedge y \leq n = N\}$
$x := 5;$
$\{INV : x = 2^y + 4 \wedge y \leq n = N\}$
while $y < n$ do
    $\{INV \wedge y < n\}$ (2)
    $\{2(x-2) = 2^{y+1} + 4 \wedge y + 1 \leq n = N\}$
    $x := x - 2;$
    $\{2x = 2^{y+1} + 4 \wedge y + 1 \leq n = N\}$
    $y := y + 1;$
    $\{2x = 2^y + 4 \wedge y \leq n = N\}$
    $x := 2 * x$
$\{INV \wedge \neg(y < n)\}$ (3)
$\{x = 2^N + 4\}$

Per le PrePost:

1) Banale aritmetica.

2) La parte della tesi $y + 1 \leq n = N$, visto che lavoriamo con numeri interi, è equivalente a $y < n = N$, che deriva immediatamente dalle ipotesi. La parte della tesi $2(x-2) = 2^{y+1} + 4$, sostituendo x come da INV, si riscrive come $2(2^y + 4 - 2) = 2^{y+1} + 4$ e quindi vale.

3) Per ipotesi $\neg(y < n)$ e $y \leq n = N$, da cui $y = N$. Per ipotesi abbiamo anche $x = 2^y + 4$ da cui la tesi $x = 2^N + 4$.

□