Informatica — 2025-06-23

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

Esercizio 1. *Si enunci e dimostri il teorema di Knaster-Tarski.*

Esercizio 2. *Le seguenti regole definiscono induttivamente una relazione* $R \in \mathcal{P}(\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N})$ *(regole* $[R0], [R1], [R2], [R3]$*). Sotto,* x, a, b, k *indicano naturali.*

$$\frac{}{R(x, 0, a, a)}[R0] \quad \frac{R(x, b, a, k) \quad b < a}{R(x, a, b, k)}[R1]$$

$$\frac{R(x, a, b - a, k) \quad b \geq a}{R(x, a, b, k)}[R2] \quad \frac{R(0, a, b - 2a, k) \quad b \geq 2a}{R(0, a, b, k)}[R3]$$

1. *[20%] Si trovi un* $k \in \mathbb{N}$ *per cui valga* $R(7, 15, 9, k)$*. 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:*

$$\forall x, a, b, k \in \mathbb{N}.\ R(x, a, b, k) \land x = 0 \implies R(1, a, b, k).$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall x, a, b, k \in \mathbb{N}.\ R(x, a, b, k) \implies p(x, a, b, k)$$

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. Una possibile derivazione è:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{R(7,0,3,3)}[R0]}{R(7,3,0,3)}[R1]}{R(7,3,3,3)}[R2]}{R(7,3,6,3)}[R2]}{R(7,6,3,3)}[R1]}{R(7,6,9,3)}[R2]}{R(7,9,6,3)}[R1]}{R(7,9,15,3)}[R2]}{R(7,15,9,3)}[R1]$$

Parte 2.
Affinché valga $\forall x, a, b, k. R(x, a, b, k) \implies p(x, a, b, k)$ è sufficiente che

$$\begin{aligned}
&R0)\ \forall x, a.\ p(x, 0, a, a)\\
&R1)\ \forall x, a, b, k.\ p(x, b, a, k) \land b < a \implies p(x, a, b, k)\\
&R2)\ \forall x, a, b, k.\ p(x, a, b - a, k) \land b \geq a \implies p(x, a, b, k)\\
&R3)\ \forall x, a, b, k.\ p(0, a, b - 2a, k) \implies p(0, a, b, k)
\end{aligned}$$

Parte 3.
Basta prendere $p(x, a, b, k) :\ x = 0 \implies R(1, a, b, k)$.
Parte 4.
Caso $[R0]$.

Dobbiamo dimostrare $p(x, 0, a, a)$ e cioè $0 = 0 \implies R(1, 0, a, a)$, il che è equivalente a $R(1, 0, a, a)$. La tesi segue direttamente da $[R0]$ prendendo $x = 1$ e $a = a$.

Caso $[R1]$.

Assumendo l'ipotesi induttiva $IP1 : p(x, b, a, k)$ e $IP2 : b < a$ dobbiamo dimostrare $p(x, a, b, k)$. L'ipotesi e la tesi sono:

$$\begin{aligned} &IP1: \ x = 0 \implies R(1, b, a, k) \\ &IP2: \ b < a \\ &tesi: \ x = 0 \implies R(1, a, b, k) \end{aligned}$$

Assumiamo quindi $IP3 : x = 0$ e dimostriamo la nuova tesi $R(1, a, b, k)$.

Da $IP1$ e $IP3$ si ha $R(1, b, a, k)$. Da qui, usando $IP2$ e la regola $[R1]$ (con $x = 1$) ricaviamo $R(1, a, b, k)$ che è la tesi.

Caso $[R2]$. Assumendo l'ipotesi induttiva $IP1 : p(x, a, b - a, k)$ e $IP2 : b \geq a$ dobbiamo dimostrare $p(x, a, b, k)$. L'ipotesi e la tesi sono:

$$\begin{aligned} &IP1: \ x = 0 \implies R(1, a, b - a, k) \\ &IP2: \ b \geq a \\ &tesi: \ x = 0 \implies R(1, a, b, k) \end{aligned}$$

Assumiamo quindi $IP3 : x = 0$ e dimostriamo la nuova tesi $R(1, a, b, k)$.

Da $IP1$ e $IP3$ si ha $R(1, a, b - a, k)$. Da qui, usando $IP2$ e la regola $[R2]$ (con $x = 1$) ricaviamo $R(1, a, b, k)$ che è la tesi.

Caso $[R3]$. Assumendo l'ipotesi induttiva $IP1 : p(0, a, b - 2a, k)$ e $IP2 : b \geq 2a$ dobbiamo dimostrare $p(0, a, b, k)$. L'ipotesi e la tesi sono:

$$\begin{aligned} &IP1: \ 0 = 0 \implies R(1, a, b - 2a, k) \\ &IP2: \ b \geq 2a \\ &tesi: \ 0 = 0 \implies R(1, a, b, k) \end{aligned}$$

Semplificando opportunamente:

$$\begin{aligned} &IP1: \ R(1, a, b - 2a, k) \\ &IP2: \ b \geq 2a \\ &tesi: \ R(1, a, b, k) \end{aligned}$$

(Nota a margine: qui non possiamo applicare la regola $[R3]$ visto che $1 \neq 0$.)

Da $IP2$ si ricava $b - a \geq a$ e $b \geq a$ visto che sono naturali. Sfruttando questo e $IP1$, possiamo applicare due volte la regola $[R2]$ in questo modo:

$$\dfrac{\dfrac{R(1, a, b - 2a, k) \quad b - a \geq a}{R(1, a, b - a, k) \quad b \geq a}[R2]}{R(1, a, b, k)}[R2]$$

Ricaviamo quindi così la tesi.

(Nota a conclusione: l'ipotesi $x = 0$ non ci è mai servita davvero se non per dimostrare se stessa nelle ipotesi induttive. Avremmo potuto dimostrare per induzione $R(x, a, b, k) \implies R(1, a, b, k)$ direttamente.)

□

Esercizio 3. *Si consideri il seguente comando di IMP con le guardie estese a espressioni booleane arbitrarie:*

$$c = (\mathsf{while}\ \phi_1\ \mathsf{do}\ c_1); (\mathsf{while}\ \phi_2\ \mathsf{do}\ c_2); x := 0; y := 0; z := 0$$

dove le variabili x, y, z non appaiono in ϕ_1, c_1, ϕ_2, c_2.

1. *[60%] Si fornisca un comando c' nello stesso linguaggio, in modo che c' sia equivalente al comando c e che c' abbia al suo interno al massimo un singolo ciclo* while *(oltre a quelli eventualmente presenti all'interno di c_1 e c_2).*

2. *[40%] Si giustifichi informalmente la risposta.*

Soluzione (bozza).
Parte 1.
Basta prendere c' uguale a:

$x := 1;$
while $x \neq 0$ do
    if $x = 1$ then
        if ϕ_1 then c_1 else $x := 2$
    else if $x = 2$ then
        if ϕ_2 then c_2 else $x := 0$
    else skip
$y := 0; z := 0$

Parte 2. Eseguire c a partire da uno stato iniziale può avere esattamente uno dei seguenti effetti:

1. Il primo while esegue c_1 infinite volte e quindi c non termina.

2. Il primo while esegue c_1 un numero finito di volte (n_1), e subito dopo il secondo while esegue c_2 infinite volte. Anche qui c non termina.

3. Il primo while esegue c_1 un numero finito di volte (n_1), e subito dopo il secondo while esegue c_2 un numero finito di volte (n_2). Qui c termina.

Si noti che i casi sopra sono disgiunti ed esaustivi.

In tutti i casi, è facile convincersi che c' ha lo stesso comportamento.

Nel caso 1, x viene impostato a 1, causando il controllo della guardia ϕ_1 (vera), e l'esecuzione di c_1 che non altera x. Questo si ripete all'infinito, visto che la guardia ϕ_1 rimane sempre vera.

Nel caso 2, il procedimento sopra si arresta dopo n_1 esecuzioni di c_1, rendendo falsa la guardia ϕ_1 e impostando x a 2. Questo causa il controllo della guardia ϕ_2 (vera), e l'esecuzione di c_2 che non altera x. Questa ultima parte si ripete all'infinito, visto che la guardia ϕ_2 rimane sempre vera.

Nel caso 3, il procedimento sopra si arresta dopo n_1 esecuzioni di c_1 seguite da n_2 esecuzioni di c_2, rendendo falsa la guardia ϕ_2 e impostando x a 0. Questo fa terminare il ciclo while dentro c'. Lo stato finale è lo stesso di quello dell'esecuzione di c, visto che la variabile x non viene usata nelle guardie e nei comandi c_1 e c_2, e quindi le altre variabili vengono modificate esattamente come accade eseguendo c. Infine, entrambi c e c' impostano x, y, z a 0 alla fine.

(Nota: la parte else skip è ridondante, non viene mai davvero eseguita e si sarebbe potuto semplificare l'if subito sopra, ma è stata lasciata per chiarezza.)

□

Nome _____ Matricola _____

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

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

$x := 0;$

$y := 0;$

---

while $y < n$ do

$y := y + 1;$

$x := x + 1 + 3 * y$

$\{2x = 3N^2 + 5N\}$

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

Soluzione (bozza).

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

Per le PrePost:

1) Banale aritmetica.

2) La parte della tesi $y + 1 \leq n = N$ deriva dalle ipotesi $y < n$ e INV, visto che sono valori interi. Per la parte della tesi $2(x+1+3(y+1)) = 3(y+1)^2+5(y+1)$, semplificando ambo i membri ricaviamo $2x + 6y + 8 = 3y^2 + 3 + 6y + 5y + 5$ e quindi $2x = 3y^2 + 5y$ che vale per INV.

3) Da INV si ha $y \leq n = N$ che con l'ipotesi $\neg(y < n)$ implica $y = n = N$. Usando il resto di INV, si ha $2 * x = 3y^2 + 5y = 3N^2 + 5N$ ovvero la tesi.

□