Informatica — 2018-09-05

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

Esercizio 1. *Si forniscano gli enunciati, senza dismostrarli, del teorema di Knaster-Tarski e del lemma del minimo punto fisso.*

Esercizio 2. *Sia* $f : \mathbb{N} \to \mathbb{N}$ *una funzione data. Le seguenti regole definiscono induttivamente l'insieme* S *delle sequenze di numeri naturali (regole* $[S0], [S1]$*), una relazione* $R \in \mathcal{P}(S \times S)$ *(regole* $[R0], [R1]$*), e una una relazione* $M \in \mathcal{P}(S \times S)$ *(regole* $[M0], [M1]$*). Sotto, si usano le variabili* $s, z \in S$*,* $n \in \mathbb{N}$*.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{n : s}(n \in \mathbb{N})[S1] \qquad \frac{}{R(\epsilon, \epsilon)}[R0] \quad \frac{R(s,z)}{R(n : s, n : n : z)}[R1]$$

$$\frac{}{M(\epsilon, \epsilon)}[M0] \qquad \frac{M(s,z)}{M(n : s, f(n) : z)}[M1]$$

1. *[20%] Si forniscano un* $s_1, s_2 \in S$*, tale per cui* $R(1 : 2 : \epsilon,\ s_1)$ *e* $M(1 : 2 : \epsilon,\ s_2)$ *valgano. Si giustifichi la risposta con opportune derivazioni.*

2. *[20%] Si enunci il principio di induzione associato all'insieme delle sequenze* S*.*

3. *[60%] Si dimostri l'enunciato seguente*

   $$\forall s_1, s_2, s_3 \in S.\ R(s_1, s_2) \wedge M(s_2, s_3) \implies \exists s_4 \in S.\ M(s_1, s_4) \wedge R(s_4, s_3)$$

   per induzione su $s_1 \in S$ *(quindi usando il principio di induzione* *<u>associato ad S</u>).*

Soluzione (bozza).
Parte 1.

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

$$\cfrac{\cfrac{\cfrac{}{M(\epsilon, \epsilon)}[M0]}{M(2 : \epsilon, f(2) : \epsilon)}[M1]}{M(1 : 2 : \epsilon, f(1) : f(2) : \epsilon)}[M1]$$

Parte 2.

Sia p un predicato sulle sequenze di naturali. Per dimostrare che vale $\forall s \in S.\ p(s)$ è sufficiente verificare che

$$1) p(\epsilon)$$
$$2) \forall n \in \mathbb{N}, s.\ p(s) \implies p(n : s)$$

Parte 3.

Sia p il predicato sulle sequenze di naturali definito come

$$p(s_1) :\ \forall s_2, s_3 \in S.\ R(s_1, s_2) \wedge M(s_2, s_3) \implies \exists s_4 \in S.\ M(s_1, s_4) \wedge R(s_4, s_3)$$

Procediamo quindi per induzione su S:

Caso $[S0]$**.**

Dobbiamo dimostrare $p(\epsilon)$ e cioè

$$\forall s_2, s_3 \in S.\ R(\epsilon, s_2)\ \wedge\ M(s_2, s_3) \implies \exists s_4 \in S.\ M(\epsilon, s_4)\ \wedge\ R(s_4, s_3)$$

Assumiamo per ipotesi $IP1 : R(\epsilon, s_2)$ e $IP2 : M(s_2, s_3)$ e dimostriamo la tesi $\exists s_4 \in S.\ M(\epsilon, s_4)\ \wedge\ R(s_4, s_3)$.

Invertendo $IP1$, notiamo che può solo essere derivata con $R0$, per cui $s_2 = \epsilon$.

$IP2$ si riscrive come $M(\epsilon, s_3)$. Invertendola, notiamo che può solo essere derivata con $M0$, per cui $s_3 = \epsilon$.

La tesi diventa quindi

$$\exists s_4 \in S.\ M(\epsilon, s_4)\ \wedge\ R(s_4, \epsilon)$$

che si dimostra scegliendo $s_4 = \epsilon$ ed usando le regole $M0$ e $R0$.

Caso $[S1]$**.**

Assumiamo per ipotesi induttiva $p(s)$, cioè:

$$IP1 : \forall \bar{s_2}, \bar{s_3} \in S.\ R(s, \bar{s_2})\ \wedge\ M(\bar{s_2}, \bar{s_3}) \implies \exists \bar{s_4} \in S.\ M(s, \bar{s_4})\ \wedge\ R(\bar{s_4}, \bar{s_3})$$

e dimostriamo la tesi $p(n : s)$, cioè:

$$\forall s_2, s_3 \in S.\ R(n : s, s_2)\ \wedge\ M(s_2, s_3) \implies \exists s_4 \in S.\ M(n : s, s_4)\ \wedge\ R(s_4, s_3)$$

Per farlo, assumiamo $IP2 : R(n : s, s_2)$ e $IP3 : M(s_2, s_3)$ e dimostriamo la nuova tesi

$$\exists s_4 \in S.\ M(n : s, s_4)\ \wedge\ R(s_4, s_3)$$

Invertendo $IP2$, notiamo che può solo essere derivata con $R1$, per cui $s_2 = n : n : z$ e $IP4 : R(s, z)$.

$IP3$ si riscrive come $M(n : n : z, s_3)$. Invertendola, notiamo che può solo essere derivata con $M1$, per cui $s_3 = f(n) : z'$ e $IP5 : M(n : z, z')$. Invertendo anche $IP5$, notiamo che può solo essere derivata con $M1$, per cui $z' = f(n) : z''$ e $IP6 : M(z, z'')$.

Usiamo ora $IP1$, scegliendo $\bar{s_2} = z, \bar{s_3} = z''$. Otteniamo

$$R(s, z)\ \wedge\ M(z, z'') \implies \exists \bar{s_4} \in S.\ M(s, \bar{s_4})\ \wedge\ R(\bar{s_4}, z'')$$

L'antecedente vale per $IP4$ e $IP6$, quindi possiamo concludere che per qualche valore di $\bar{s_4}$ valgono $IP7 : M(s, \bar{s_4})$ e $IP8 : R(\bar{s_4}, z'')$.

Per dimostrare la tesi, scegliamo quindi $s_4 = f(n) : \bar{s_4}$. La tesi diventa

$$M(n : s, f(n) : \bar{s_4})\ \wedge\ R(f(n) : \bar{s_4}, s_3)$$

che, usando le equazioni precedenti per s_3 e z', diventa

$$M(n : s, f(n) : \bar{s_4}) \wedge R(f(n) : \bar{s_4}, f(n) : f(n) : z'')$$

La prima tesi deriva quindi dalla regola $M1$ e da $IP7$.

La seconda tesi deriva invece dalla regola $R1$ e da $IP8$.

$\square$

Esercizio 3. *Sia dato un insieme U e due insiemi di regole di inferenza $\mathcal{R}, \mathcal{R}'$ su U. Si dimostri che*

$$\forall X, Y. \quad X \subseteq Y \subseteq U \wedge \mathcal{R} \subseteq \mathcal{R}' \implies \hat{\mathcal{R}}(X) \subseteq \hat{\mathcal{R}}'(Y)$$

Soluzione (bozza). Sia $x \in \hat{\mathcal{R}}(X)$.

Per definizione di $\hat{\mathcal{R}}$, esiste una regola di $\mathcal{R}$ con conclusione x e premesse $a_1, \ldots, a_n \in X$.

Siccome $\mathcal{R} \subseteq \mathcal{R}'$, la stessa regola appartiene anche a $\mathcal{R}'$. Inoltre, siccome $X \subseteq Y$, le premesse $a_1, \ldots, a_n$ appartengono anche a Y.

Quindi, $x \in \hat{\mathcal{R}}'(Y)$.

Per la generalità di x, otteniamo l'inclusione desiderata $\hat{\mathcal{R}}(X) \subseteq \hat{\mathcal{R}}'(Y)$.

$\square$

Nome ________________________________ Matricola ____________

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

$\{a = A\}$

___

$b := 2 * a * a;$

___

while $b \neq 0$ do

___

___

$a := 2 - a;$

___

$b := b - 1;$

___

$\{a = A\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

___

___

___

___

___

___

___

___

___

Soluzione (bozza).

$\{a = A\}$ (1)
$\{a = (-1)^{2a^2}(A-1)+1\}$
$b := 2 * a * a;$
$\{INV : a = (-1)^b(A-1)+1\}$
while $b \neq 0$ do
$\{INV \wedge b \neq 0\}$ (2)
$\{2-a = (-1)^(b-1)(A-1)+1\}$
$a := 2-a;$
$\{a = (-1)^(b-1)(A-1)+1\}$
$b := b-1;$
$\{INV \wedge \neg(b \neq 0)\}$ (3)
$\{a = A\}$

Per le PrePost:

1) Siccome l'esponente è pari, la tesi si riscrive come $a = A-1+1$ che deriva dall'ipotesi.

2) Siccome $a = (-1)^b(A-1)+1$, si ha $2-a = 2-(-1)^b(A-1)-1 = (-1)^{b-1}(A-1)+1$.

3) Per ipotesi $b = 0$ per cui da INV si ha $a = (-1)^0(A-1)+1 = A-1+1 = A$ che è la tesi.

□