Durata della prova: 1h 30'

Esame di Logica e Algebra

Politecnico di Milano – Ingegneria Informatica – 03 Febbraio 2022

Docente:	**Cognome:**	**Nome:**	**Codice persona:**

Tutte le risposte devono essere motivate. Gli esercizi vanno svolti su questi fogli, nello spazio sotto il testo e sul retro. I fogli di brutta non devono essere consegnati. I compiti privi di indicazione leggibile di nome e cognome non verranno corretti.

1. (Punteggio:2.5+3.5, 3)

   (a) Verificare sia per via semantica sia usando la risoluzione che il seguente insieme di f.b.f.:
   $$\Gamma = \{\neg A, B \wedge C \Rightarrow (A \iff B), B \Rightarrow A, C \vee (B \Rightarrow \neg C)\}$$
   è soddisfacibile.

   (b) Verificare se $\Gamma \cup \{\neg(\neg A \wedge (B \Rightarrow A) \wedge \neg C)\}$ è un insieme insoddisfacibile.

Soluzione:

(a) E' immediato verificare che $C \vee (B \Rightarrow \neg C)$ è una tautologia, quindi i modelli di Γ e quelli di
$$\Gamma' = \{\neg A, B \wedge C \Rightarrow (A \iff B), B \Rightarrow A\}$$
coincidono. Dalle tavole di verità delle formule di Γ' otteniamo i modelli di Γ' che sono solo due: $\nu_1(A) = \nu_1(B) = \nu_1(C) = 0$ e $\nu_2(A) = \nu_1(B) = 0$, $\nu_2(C) = 1$. Pertanto Γ è chiaramente un insieme soddisfacibile poichè ammette almeno un modello.
Con la risoluzione dobbiamo mostrare che dalle clausole di Γ' non ricaviamo quella vuota. Le clausole di Γ' sono le seguenti:

- dalla prima formula si ricava $\{\neg A\}$;
- dalla seconda si ricava $\{\neg B, A, \neg C\}$ (dato che la formula è semanticamente equivalente a $\neg B \vee A \vee \neg C$);
- dalla terza formula si ricava $\{\neg B, A\}$.

Ora dalle tre clausole $\{\neg A\}$, $\{\neg B, A, \neg C\}$, $\{\neg B, A\}$ vediamo subito che possiamo eliminare (pruning) le ultime due clausole che contengono $\neg B$ (dato che non compare un B e quindi non potrò mai "eliminarlo") e quindi rimaniamo con la sola clausola $\{\neg A\}$ da cui non potrò mai ottenre la clausola vuota, quindi Γ' è soddisfacibile, e quindi anche Γ. Alternativamente bastava verificare che $Ris(\Gamma') = \Gamma' \cup \{\{\neg B, \neg C\}, \{\neg B\}\} = Ris^2(\Gamma')$ e, poichè la clausola vuota non appartiene a $Ris(\Gamma')$, segue che l'insieme Γ' è soddisfacibile e quindi lo è anche Γ.

(b) Il problema è equivalente a verificare
$$\Gamma \models (\neg A \wedge (B \Rightarrow A) \wedge \neg C)$$
dato che l'interpretazione ν_2 tale che $\nu_2(A) = \nu_1(B) = 0$, $\nu_2(C) = 1$ è modello di Γ ma non di $(\neg A \wedge (B \Rightarrow A) \wedge \neg C)$, ne deduciamo che l'insieme $\Gamma \cup \{\neg(\neg A \wedge (B \Rightarrow A) \wedge \neg C)\}$ è soddisfacibile.

2. (Punteggio:2+1+1,1,2, 2+2)
Sia R la relazione binaria sull'insieme $X = \{a, b, c, d, e, f\}$ definita nel seguente modo:

$$R = \{(a, b), (a, d), (c, d), (c, e), (c, f), (d, b), (d, e), (f, b)\}$$

(a) Verificare che può esistere una relazione d'ordine contenente R e indicare con S la più piccola relazione d'ordine contenente R. Costruire il diagramma di Hasse di S e determinare se X ammette massimo e/o minimo, elementi massimali e/o elementi minimali rispetto ad S.

(b) Determinare il diagramma di Hasse di una relazione d'ordine totale contenente S.

(c) Dimostrare che non esistono funzioni contenute in R né funzioni contenenti R.

(d) Si consideri la seguente formula della logica del primo ordine:

$$\forall x\, (A(x, y) \wedge \neg E(x, y) \Rightarrow \exists z A(y, z))$$

stabilire se essa è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio X e in cui, $A(x, y)$ sia da interpretare come la relazione R e $E(x, y)$ come l'uguaglianza. Rispondere alla medesima richiesta nel caso in cui nell'interpretazione precedente $A(x, y)$ sia da interpretare come la relazione S.

Soluzione:

(a) La matrice d'adiacenza di R è data da:

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

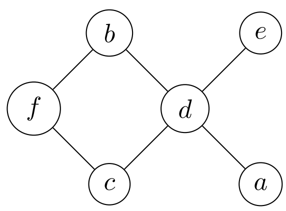
Si nota subito che R è antisimmetrica, per verificare se esiste la relazione d'ordine contente R chiudiamo transitivamente e riflessivamente. Abbiamo

$$M^2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

mentre M^3 è la matrice nulla, quindi la matrice della chiusura transitiva e riflessiva di R è

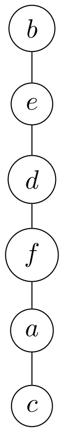
$$N = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

che è chiaramente la matrice di adiacenza di una relazione antisimmetrica e quindi rappresenta la matrice d'adiacenza della chiusura d'ordine S di R. Il diagramma di Hasse di S è il seguente:



da cui deduciamo che non ci sono né massimi né minimi e che l'insieme dei massimali è $\{b, e\}$ mentre l'insieme dei minimali è $\{c, a\}$.

(b) Dobbiamo trovare una relazione d'ordine totale T che contenga S. Per farlo, basta costruire un diagramma di Hasse che sia compatibile con S, cioè se x sta sotto un vertice y nel diagramma di Hasse di S, allora anche nel diagramma di Hasse di T dobbiamo avere che x sta sotto y. Una possibilità è la seguente:



(c) Non esistono funzioni che contengono R poichè per qualunque relazione F con $R \subseteq F$ si avrebbe $(a,d),(a,b) \in F$ e ciò contraddirebbe la definizione di funzione. Inoltre per ogni relazione F tale che $F \subseteq R$ si avrebbe che b non è in relazione con nessun elemento e pertanto F non potrebbe essere una funzione.

(d) Osserviamo innanzitutto che la formula non è chiusa. Dato che il conseguente $\exists z A(y,z)$ è soddisfatto per $y = d$ segue che la formula assegnata è soddisfacibile. La formula però è non vera, infatti per $y = b$ e $x = d$ l'antecedente $A(x,y) \wedge \neg E(x,y)$ è soddisfatto poichè $d \neq b$ e $(d,b) \in R$ ma il conseguente non lo è poichè non esiste alcuno z tale che $(b,z) \in R$. Pertanto la formula assegnata risulta essere soddisfacibile ma non vera nella prima interpretazione. Invece interpretando $A(x,y)$ come la relazione S abbiamo che la formula è vera: infatti, per ogni $y \in X$, abbiamo $(y,y) \in S$ essendo S riflessiva e pertanto il conseguente $\exists z A(y,z)$ è vero rendendo l'intera formula vera in questa seconda interpretazione.

3. (Punteggio: 3,2+1, 2+2)
Si consideri il seguente sottoinsieme S delle matrici quadrate di ordine 2 ad elementi in $\mathbb{Z}_5$

$$S = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}_5 \right\}$$

(a) Si mostri che $(S, \cdot)$ con l'usuale prodotto $\cdot$ righe per colonne è un monoide commutativo.

(b) Mostrare che la funzione $\varphi : S \to \mathbb{Z}_5$ definita da

$$\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a^2 - b^2$$

è un omomorfismo tra il monoide $(S, \cdot)$ e il monoide $(\mathbb{Z}_5, \cdot)$, φ è anche un monomorfismo?

(c) Si consideri la seguente formula della logica del primo ordine:

$$\forall x \forall y \, (\, E(f(x), f(y)) \Rightarrow \forall z K(p(z, x), p(z, y)) \,)$$

Si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio l'insieme S, in cui f interpreta un omomorfismo $F : (S, \cdot) \to (S, \cdot)$ di monoidi, $p(x, y)$ interpreta il prodotto $x \cdot y$ nel monoide $(S, \cdot)$, $E(x, y)$ interpreta l'uguaglianza, mentre $K(x, y)$ interpreta la relazione $\ker(F)$. La formula è logicamente valida o insoddisfacibile?

Soluzione:

(a) Verifichiamo che l'operazione $\cdot$ sia interna, infatti:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & a\beta + b\alpha \\ \alpha b + \beta a & \beta b + a\alpha \end{pmatrix} \in S$$

dato che $a\alpha + b\beta = \beta b + a\alpha$ e $\alpha b + \beta a = a\beta + b\alpha$. L'associatività è conseguenza dell'associatività del prodotto righe per colonne di matrici su di un campo (in questo caso $\mathbb{Z}_5$), mentre l'identità del monoide è data dalla matrice

$$I = \begin{pmatrix} [1]_5 & [0]_5 \\ [0]_5 & [1]_5 \end{pmatrix}$$

che appartiene chiaramente ad S. Dimostriamo la commutatività dell'operazione:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & a\beta + b\alpha \\ \alpha b + \beta a & \beta b + a\alpha \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Pertanto $(S, \cdot)$ è un monoide commutativo.

(b) Dato che, per ogni $A \in S$, $\varphi(A) = det(A)$, il risultato segue immediatamente dal teorema di Binet, infatti:

$$\varphi(A \cdot B) = det(AB) = det(A)\, det(B) = \varphi(A)\varphi(B)$$

In alternativa si può effettuare una verifica diretta:

$$\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \right) = (a\alpha + b\beta)^2 - (a\beta + b\alpha)^2 = (a^2 - b^2)(\alpha^2 - \beta^2) = \varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} \varphi \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$$

Per essere un omomorfismo di monoidi si verifica anche che $\varphi(I) = [1]_5$ che è l'unità del monoide $(\mathbb{Z}_5, \cdot)$.
L'applicazione assegnata non è un monomorfismo dato che non è iniettiva, infatti:

$$\varphi \begin{pmatrix} [4]_5 & [0]_5 \\ [0]_5 & [4]_5 \end{pmatrix} = [1]_5 = \varphi \begin{pmatrix} [1]_5 & [0]_5 \\ [0]_5 & [1]_5 \end{pmatrix}$$

nonostante le due matrici siano diverse.

(c) Nell'interpretazione data, la formula si traduce nel seguente modo: se $F(x) = F(y)$ allora, per ogni z, $(zx, zy) \in \ker(F)$. Questa è vera dato che F è un omomorfismo e quindi $\ker(F)$ è una congruenza, in particolare $\ker(F)$ è compatibile con la moltiplicazione. Segue che se $(x, y) \in \ker(F)$ (cioè se $F(x) = F(y)$), allora per ogni z abbiamo che anche $(zx, zy) \in \ker(F)$ (ovviamente $(z, z) \in \ker(F)$).
Segue che la formula non è insoddisfacibile ma non è nemmeno logicamente valida. Infatti considerando l'interpretazione in cui $E(x, y)$ è interpretata dalla relazione universale su di un insieme X, $K(x, y)$ dalla relazione vuota e f da una funzione qualunque su X, otteniamo che l'antecedente della formula è sempre vero mentre il conseguente è sempre falso, pertanto la formula è non vera in questa interpretazione.