
Durata della prova: 1 h 30’

Esame di Logica e Algebra Politecnico di Milano – Ingegneria Informatica – 15 giugno 2019		
Cognome:	Nome:	Matricola:

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.

Esercizio 1

Si consideri la seguente tavola di verità:

A	B	C	f (A,B,C)
0	0	0	1
0	0	1	x
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	y
1	1	1	z

con x, y, z $\in\{0; 1\}$.

1. Si attribuiscano ad x, y, z dei valori in modo tale che valgano contemporaneamente le due seguenti condizioni:
   $A \wedge B \mid\!-_L f(A,B,C)$ $\qquad\qquad$ $f(A,B,C) \not\models C \Rightarrow (B \vee A)$.
2. Si scriva una formula in cui compaiano solo i connettivi $\neg$ e $\Rightarrow$ e che abbia come tavola di verità quella che si ottiene sostituendo nella tavola data i valori di x, y, z trovati al punto precedente.
3. Si verifichi che $f(A,B,C) \not\models C \Rightarrow (B \vee A)$ usando la risoluzione.

<u>Svolgimento</u>

1. Poiché i modelli della formula $A \wedge B$ sono gli ultimi due che compaiono nella tavola di verità assegnata, allora, affinchè valga la deduzione $A \wedge B \mid\!-_L f(A,B,C)$ è necessario che y = z = 1. Per soddisfare la condizione $f(A,B,C) \not\models C \Rightarrow (B \vee A)$ è necessario che f (A,B,C) abbia un modello in corrispondenza del quale la f.b.f. $C \Rightarrow (B \vee A)$ sia falsa e ciò può accadere solo se x = 1.
2. Risulta:
   $$f(A,B,C) \equiv (\sim A \wedge \sim B \wedge \sim C) \vee (\sim A \wedge \sim B \wedge C) \vee (A \wedge B \wedge \sim C) \vee (A \wedge B \wedge C)$$
   $$\equiv ((\sim A \wedge \sim B) \wedge (\sim C \vee C)) \vee ((A \wedge B) \wedge (\sim C \vee C)) \equiv (\sim A \wedge \sim B) \vee (A \wedge B)$$
   $$\equiv \sim(\sim A \wedge \sim B) \Rightarrow (A \wedge B) \equiv A \vee B \Rightarrow \sim(A \Rightarrow \sim B) \equiv (\sim A \Rightarrow B) \Rightarrow \sim(A \Rightarrow \sim B)$$
3. Trasformiamo le formule f (A,B,C) e $\sim(C \Rightarrow (B \vee A))$ in forma a clausole:
   $f(A,B,C) \equiv (\sim A \wedge \sim B) \vee (A \wedge B) \equiv (\sim A \vee (A \wedge B)) \wedge (\sim B \vee (A \wedge B)) \equiv (\sim A \vee B) \wedge (\sim B \vee A)$
   $\sim(C \Rightarrow (B \vee A)) \equiv \sim(\sim C \vee B \vee A) \equiv C \wedge \sim B \wedge \sim A$
   Si ottiene allora il seguente insieme di clausole di input:

S = {{~A, B}, {~B, A}, {C}, {~B}, {~A}}
Risulta Ris(S) = S $\cup$ {{~A, A}, {~B, B }} e $Ris^2(S)$ = Ris(S). Poiché □ $\notin$ Ris(S) segue che f (A,B,C) $|\neq$ C$\Rightarrow$(B$\vee$A).

Esercizio 2
Si consideri la relazione binaria R sull'insieme X = {a,b,c,d,e,f} definita dalla seguente matrice di incidenza:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

1) Si costruisca la relazione di equivalenza S generata da R e si determini l'insieme quoziente X / S.
2) Si dimostri che esiste la minima relazione d'ordine T contenente R e si determinino, se esistono, gli elementi massimali, minimali, massimo e minimo di X rispetto a T.
3) Si consideri la seguente formula della logica del primo ordine:
$$\forall x \exists y A_1^2(x,y) \wedge \exists x \forall y \left(A_1^2(y,x) \Rightarrow A_2^2(x,y) \right)$$
e si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio l'insieme X e in cui la lettera predicativa A_1^2 è interpretata dalla relazione d'ordine T trovata al punto precedente mentre A_2^2 è interpretata dalla relazione di uguaglianza. Portare infine la formula data in forma di Skolem.

__**Soluzione**__

1) La chiusura riflessiva e simmetrica F di R ha la seguente matrice d'incidenza:
$$M_F = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$
Determiniamo la sua chiusura transitiva:
$$M_F^2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad M_F^3 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = M_F^4$$
Segue che S = F $\cup$ F^2 $\cup$ F^3 = F^3 e quindi l'insieme quoziente è X / S = {$[a]_S$, $[d]_S$, $[e]_S$}, dove $[a]_S$ = {a, b, c, f}, $[d]_S$ = {d}, $[e]_S$ = {e}.
2) La relazione R è antisimmetrica quindi può esistere la sua chiusura d'ordine. Effettuiamo la chiusura riflessiva G di R:

$$M_G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Questa coincide con il suo quadrato e pertanto la relazione G è transitiva. Inoltre G è ancora antisimmetrica quindi essa è la minima relazione d'ordine T contenente R.
Gli elementi massimali di X rispetto a T sono f, e, c, d mentre i minimali sono a, e, d, b mentre non esistono né massimo né minimo.

3) La traduzione della formula nell'interpretazione assegnata è la seguente:
"Per ogni x ∈ X esiste y ∈ X tale che (x, y) ∈ T ed esiste x ∈ X tale che, per ogni y ∈ X, se (y, x) ∈ T allora x = y".
La proposizione "per ogni x ∈ X esiste y ∈ X tale che (x, y) ∈ T" risulta vera poiché la relazione T è seriale. La proposizione "esiste x ∈ X tale che, per ogni y ∈ X, se (y, x) ∈ T allora x = y" risulta anch'essa vera poiché corrisponde alla definizione di elemento minimale e, come visto al punto precedente, esistono elementi minimali di X rispetto a T. Pertanto la formula risulta vera nell'interpretazione assegnata poiché è la congiunzione di due formule vere.
Determiniamo la forma normale prenessa della formula assegnata:
$\forall x \exists y A_1^2(x, y) \wedge \exists x \forall y \left(A_1^2(y, x) \Rightarrow A_2^2(x, y)\right) \equiv \forall x \exists y \exists z \forall t \left(A_1^2(x, y) \wedge \left(A_1^2(t, z) \Rightarrow A_2^2(z, t)\right)\right)$
Considerata la sostituzione $\sigma = \{ f_1^1(x)/y; f_2^1(x)/z\}$, risulta che la forma della formula data è la seguente:
$\forall x \forall t \left(A_1^2(x, f_1^1(x)) \wedge \left(A_1^2(t, f_2^1(x)) \Rightarrow A_2^2(f_2^1(x), t)\right)\right)$.

Esercizio 3
Si consideri il campo (Z_{13}, +, ·) delle classi di resto modulo 13 e la seguente funzione:

$f : (Z_{13}, +) \to (Z_{13}, +) \qquad \forall [a]_{13} \in Z_{13} \quad f([a]_{13}) = 2 \cdot [a]_{13}$.

1) Si dimostri che *f* è un omomorfismo del gruppo (Z_{13}, +) in sé stesso.

2) Si stabilisca se *f* è anche un omomorfismo di (Z_{13}, ·) in sé stesso.

3) Si consideri la seguente f.b.f. della logica del primo ordine:

   $\forall x \forall y \left(A_1^2(f_1^1(f_1^2(x, y)), f_1^2(f_1^1(x), f_1^1(x))) \wedge (\neg A_1^2(x, y) \Rightarrow \neg A_1^2(f_1^1(x), f_1^1(y)))\right)$.

   Si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione in cui il dominio è Z_{13}, A_1^2 è interpretata dalla relazione di uguaglianza, f_1^1 è interpretata dalla funzione f precedentemente assegnata e f_1^2 è interpretata dall'operazione di addizione definita in Z_{13}.

Svolgimento

1) Siano $[a]_{13}, [b]_{13} \in Z_{13}$. Allora
$f([a]_{13} + [b]_{13}) = f([a+b]_{13}) = 2 \cdot [a+b]_{13} = 2 \cdot ([a]_{13} + [b]_{13}) = 2 \cdot [a]_{13} + 2 \cdot [b]_{13} = f([a]_{13}) + f([b]_{13})$
Pertanto *f* è un omomorfismo del gruppo (Z_{13}, +) in sé stesso.

2) Siano $[a]_{13}, [b]_{13} \in Z_{13}$. Risulta:

$$f([a]_{13} \cdot [b]_{13}) = f([a \cdot b]_{13}) = 2 \cdot [a \cdot b]_{13} = 2 \cdot ([a]_{13} \cdot [b]_{13})$$
$$f([a]_{13}) \cdot f([b]_{13}) = 2 \cdot [a]_{13} \cdot 2 \cdot [b]_{13} = 4 \cdot ([a]_{13} \cdot [b]_{13})$$

Pertanto *f* è non è un omomorfismo di (Z_{13}, ·) in sé stesso essendo $f([a]_{13} \cdot [b]_{13}) \neq f([a]_{13}) \cdot f([b]_{13})$.

4) La traduzione della formula nell'interpretazione assegnata è la seguente:
"Per ogni x, y ∈ Z_{13}, $f(x+y) = f(x) + f(y)$ e, se $x \neq y$ allora $f(x) \neq f(y)$".

L'uguaglianza $f(x+y) = f(x) + f(y)$ è sempre verificata essendo *f* un omomorfismo del gruppo (Z_{13}, +) in sé stesso. Inoltre anche la proposizione "se $x \neq y$ allora $f(x) \neq f(y)$" è vera poiché *f* è iniettiva. Infatti siano $x = [a]_{13}, y = [b]_{13} \in Z_{13}$ tali che $x \neq y$ e supponiamo per assurdo che $f(x) = f(y)$. Allora $2 \cdot [a]_{13} = 2 \cdot [b]_{13}$ da cui segue che $[2a]_{13} = [2b]_{13}$. Pertanto 13 divide $2a - 2b$ e quindi 13 divide $2(a - b)$. Ciò implica che 13 divide $a - b$ e che quindi $a \equiv b$ (mod 13). Ma ciò è assurdo in quanto, per ipotesi, $[a]_{13} \neq [b]_{13}$. Segue che se $x \neq y$ allora $f(x) \neq f(y)$ e quindi *f* è iniettiva. In alternativa, per dimostrare l'iniettività di *f* si poteva far vedere che a classi distinte corrispondono immagini distinte per via esaustiva:

$2 \cdot [0]_{13} = [0]_{13}$ $\quad 2 \cdot [1]_{13} = [2]_{13}$ $\quad 2 \cdot [2]_{13} = [4]_{13}$ $\quad 2 \cdot [3]_{13} = [6]_{13}$

$2 \cdot [4]_{13} = [8]_{13}$ $\quad 2 \cdot [5]_{13} = [10]_{13}$ $\quad 2 \cdot [6]_{13} = [12]_{13}$ $\quad 2 \cdot [7]_{13} = [1]_{13}$

$2 \cdot [8]_{13} = [3]_{13}$ $\quad 2 \cdot [9]_{13} = [5]_{13}$ $\quad 2 \cdot [10]_{13} = [7]_{13}$ $\quad 2 \cdot [11]_{13} = [9]_{13}$

$2 \cdot [12]_{13} = [11]_{13}$.

Possiamo concludere quindi che la formula assegnata è vera essendo la chiusura universale della congiunzione di due formule vere.