Logica e Algebra (30 Gennaio 2018)

Esercizio 1

Sia f(A,B,C) una f.b.f. avente la seguente tavola di verità:

A	B	C	f (A,B,C)
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

1. Scrivere una f.b.f. equivalente avente la tavola di verità di f(A,B,C) usando solo i connettivi $\{\sim, \Rightarrow\}$.
2. Mostrare che vale la deduzione $(\sim A \wedge B \wedge \sim C) \vdash_L f(A,B,C)$.
3. Provare lo stesso risultato utilizzando la risoluzione.
4. Trovare una formula g(A,B,C) tale che $\sim f(A,B,C)\ ) \vdash_L g(A,B,C)$ ma tale che g(A,B,C) non sia deducibile in L dalla formula A.

Esercizio 2

Sia X = {a, b, c, d, e, f} e sia $R \subseteq X \times X$ la relazione con la seguente matrice di incidenza:

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

1. R è una funzione? Calcolare una eventuale (se esiste) inversa destra e/o sinistra.
2. Sia $S \subseteq X \times X$ la relazione $S = R \cup \{(a,e),(d,c)\}$. Dire se esiste la minima relazione d'ordine T contenente S e in caso affermativo disegnarne il diagramma di Hasse. Trovare, se esistono, Sup{b,c,d}, Sup{b,c,e}, gli elementi massimali, minimali, massimi e minimi di X rispetto a T.
3. Sia U la chiusura transitiva di R. Verificare se la formula:
$$F = \forall x \exists y (A_1^2(x,y) \wedge \forall z (A_1^2(z,x) \Rightarrow A_1^2(z,y)\ ))$$
è vera, o meno, nell'interpretazione che ha come dominio l'insieme X e la lettera predicativa $A_1^2(x,y)$ è interpretata dalla relazione U. In generale, quali proprietà (di quelle che conoscete) sono richieste da U affinché soddisfi la precedente formula?
4. La formula F è soddisfacibile? È logicamente valida?

Esercizio 3

Sia $G = Z_n \times Z$ un insieme dotato della seguente operazione interna $*$ definita da

$$([a]_n, b) * ([c]_n, d) = ([a+c]_n, b+d)$$

1. Provare che (G,*) è un gruppo.
2. Provare che la funzione $f: (G,*) \rightarrow (Z_n, +)$ definita da $f([a]_n, b) = [a-b]_n$ è un omomorfismo di gruppi. Descrivere la ker-f classe dell'elemento neutro di G.

GIUSTIFICARE OGNI RISPOSTA

Soluzione

Esercizio 1

1. Una f.b.f. avente la tavola di verità di f(A,B,C) e contenente solo i connettivi $\{\sim, \Rightarrow\}$ è

$$f(A,B,C) \equiv (\sim A \wedge B \wedge \sim C) \vee (A \wedge \sim B \wedge \sim C) \equiv$$

$$\equiv \sim C \wedge \big((\sim A \wedge B) \vee (A \wedge \sim B)\big) \equiv$$

$$\equiv \sim C \wedge ((\sim A \vee A) \wedge (\sim A \vee \sim B) \wedge (B \vee A) \wedge (B \vee \sim B)) \equiv$$

$$\equiv \sim C \wedge ((\sim A \vee \sim B) \wedge (B \vee A)) \equiv$$

$$\equiv \sim C \wedge ((A \Rightarrow \sim B) \wedge (\sim B \Rightarrow A)) \equiv$$

$$\equiv \sim C \wedge \sim ((A \Rightarrow \sim B) \Rightarrow \sim (\sim B \Rightarrow A)) \equiv$$

$$\equiv \sim (\sim C \Rightarrow (A \Rightarrow \sim B) \Rightarrow \sim (\sim B \Rightarrow A))$$

2. Per il teorema di correttezza e completezza forte, dimostrare che vale la deduzione sintattica $(\sim A \wedge B \wedge \sim C) |-_L f(A,B,C)$ equivale a mostrare che vale la deduzione semantica $(\sim A \wedge B \wedge \sim C) \models f(A,B,C)$, cioè che tutti i modelli di $(\sim A \wedge B \wedge \sim C)$ sono modelli di f(A,B,C).
Osservando che la f.b.f. $(\sim A \wedge B \wedge \sim C)$ ha un solo modello che è v(A) = v(C) = 0 e v(B) = 1 che è anche modello di f(A,B,C), si ottiene il risultato.

3. Poichè mostrare che $(\sim A \wedge B \wedge \sim C) \models f(A,B,C)$ equivale a mostrare che $\{(\sim A \wedge B \wedge \sim C), \sim f(A,B,C)\}$ è insoddisfacibile, si può, utilizzando la risoluzione, mostrare che dall'insieme $\{(\sim A \wedge B \wedge \sim C), \sim f(A,B,C)\}$ si deduce la clausola vuota.

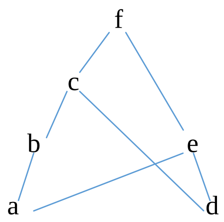
   Osservando che $\sim f(A,B,C) \equiv (A \vee \sim B \vee C) \wedge (\sim A \vee B \vee C)$ e scrivendo le formule in forma a clausole si ha che l'insieme $\{(\sim A \wedge B \wedge \sim C), \sim f(A,B,C)\}$ è formato dalle clausole $C_1=\{\sim A\}$, $C_2=\{B\}$, $C_3=\{\sim C\}$, $C_4=\{A, \sim B, C\}$, $C_5=\{\sim A, B, C\}$.

   Da C_3 e C_4 si ha $C_6=\{A, \sim B\}$, da C_6 e C_1 si ha $C_7=\{\sim B\}$, da C_7 e C_2 si ottiene la clausola vuota.

4. Una possibile formula g(A,B,C) tale che $\sim f(A,B,C)$)$|-_L$ g(A,B,C) ma tale che g(A,B,C) non sia deducibile in L dalla formula A è $\sim A \vee B \vee C$.

Esercizio 2

1. Come si evince dalla matrice d'incidenza della relazione R, tale relazione è una funzione in quanto presenta uno ed un solo uno su ogni riga. Ricordando che una funzione ammette inversa destra se e solo se è iniettiva ed inversa sinistra se e solo se è suriettiva e osservando che la funzione R non è iniettiva in quanto l'ultima colonna della matrice d'incidenza presenta più di un 1 e che non è suriettiva perché la prima colonna non presenta alcun 1, possiamo affermare che la funzione R non ammette né inverse destre né sinistre.
2. Considerata la relazione $S \subseteq X \times X$ con $S = R \cup \{(a,e),(d,c)\}$, si può osservare che S è antisimmetrica quindi può esistere la minima relazione d'ordine T contenente S. Precisamente se la chiusura riflessiva e transitiva di S è antisimmetrica essa è la minima relazione d'ordine contenente S, diversamente tale chiusura non esiste.
Essendo la chiusura riflessiva e transitiva di S uguale a $S \cup \{(a,a),(b,b),(c,c),(d,d),(e,e), (a,c),(a,f),(b,f),(d,f)\}$, si osserva che è antisimmetrica e perciò coincide con la relazione T cercata.
Il diagramma di Hasse di T è



Da esso si evince che Sup{b,c,d} = c, e che Sup{b,c,e} = f, l'unico elemento massimale è f che è anche massimo mentre gli elementi minimali sono a, d ma non esiste minimo.

3. La chiusura transitiva U di R è data da R $\cup$ {(a,c),(a,f),(b,f),(d,f)}.
   La formula
   $$\forall x \exists y (A_1^2(x,y) \wedge \forall z (A_1^2(z,x) \Rightarrow A_1^2(z,y)\ ))$$
   è vera nell'interpretazione che ha come dominio l'insieme X e in cui la lettera predicativa $A_1^2(x,y)$ è interpretata dalla relazione U in quanto U è seriale ed è transitiva. Infatti, su ogni riga della matrice di incidenza di R vi è almeno un 1 e quindi ciò si verifica anche per ogni sua chiusura pertanto la sottoformula $A_1^2(x,y)$ è sempre soddisfatta per ogni x.
   Inoltre vale la proprietà transitiva per U quindi anche la seconda sottoformula che segue l'and è sempre soddisfatta dal momento che lo è $A_1^2(x,y)$.
   Pertanto le proprietà delle relazioni binarie che sono richieste da U affinché sia soddisfatta la precedente formula sono la serialità e la transitività.
4. Ovviamente la formula F è soddisfacibile essendo vera nella precedente interpretazione.
   La formula non è logicamente valida, basta infatti considerare l'interpretazione avente come dominio un insieme D costituito da due elementi, D ={a,b}, e in cui la lettera predicativa $A_1^2(x,y)$ è interpretata dalla relazione x≠y.
   L'assegnamento x = a, y = b, z = b non soddisfa la formula.

<u>Esercizio 3</u>

1. Per provare che (G,*) è un gruppo si deve mostrare che l'operazione * è interna, è associativa, ammette elemento neutro in G e che ogni elemento di G ammette inverso rispetto *.
   Osserviamo che l'operazione * è interna in quanto $[a+c]_n \in Z_n$ e $b+d \in Z$, per ogni $[a]_n[c]_n \in Z_n, b, d \ \in Z$.
   L'operazione * è associativa in quanto
   $(([a]_n,b)*([c]_n,d))*([e]_n,f)$=$([a+c]_n,b+d)*([e]_n,f)$=$([(a+c)+e]_n,(b+d)+f)$

   $([a]_n,b)*(([c]_n,d)*([e]_n,f)) = ([a]_n,b)*([c+e]_n,d+f) = ([a+(c+e)]_n,b+(d+f))$

   ed essendo l'operazione + associativa in Z si ha la tesi.

   Cerchiamo l'elemento neutro a sinistra di * in G, cioè cerchiamo un elemento $([x]_n,y)$ tale che, per ogni $([a]_n,b) \in G$, $([x]_n,y)*([a]_n,b) = ([a]_n,b)$.

   Cerchiamo quindi un elemento $([x]_n,y) \in G$ tale che $([x+a]_n,y+b) = ([a]_n,b)$, per ogni $([a]_n,b) \in G$. L'elemento cercato è la coppia $([0]_n,0)$. Da ultimo cerchiamo l'inverso sinistro del generico elemento $([a]_n,b)$, cioè un elemento $([x]_n,y) \in G$ tale che $([x+a]_n,y+b) = ([0]_n,0)$. Ovviamente l'elemento cercato è la coppia $(-[a]_n,-b) \in G$.

   Essendo * associativa ed esistendo l'elemento neutro a sinistra e l'inverso a sinistra del generico elemento di G, per la riduzione dei postulati di un gruppo, abbiamo dimostrato che (G,*) è un gruppo.

2. Mostriamo ora che la funzione $f: G \to Z_n$ definita da $f([a]_n,b) = [a-b]_n$è un omomorfismo di gruppi.
   Si ha infatti che $f(([a]_n,b)*([c]_n,d)) = f(([a+c]_n,b+d)) = [(a+c)-(b+d)]_n$
   e che $f\big(([a]_n,b)\big) + f(([c]_n,d)) = [a-b]_n + [c-d]_n = [(a-b)+(c-d)]_n$ ed essendo
   $[(a+c)-(b+d)]_n = [(a-b)+(c-d)]_n$ si ha la tesi.
   Cerchiamo ora la kerf –classe della coppia $([0]_n,0)$.

   $$[([0]_n,0)]_{\ker f} = \{([a]_n,b) \in G \mid f(([a]_n,b)) = f(([0]_n,0)) = [0]_n\} =$$
   $$= \{([a]_n,b) \in G \mid [a-b]_n = [0]_n\} = \{([a]_n,b) \in G \mid a \equiv b (\mathrm{mod} n)\}.$$