Durata della prova: 1h 30'

Esame di Logica e Algebra

Politecnico di Milano – Ingegneria Informatica – Appello telematico Luglio 2020

Tutte le risposte devono essere motivate. Gli esercizi vanno svolti in bella copia su fogli numerati e poi scannerizzati con lo stesso ordine di svolgimento dell'esame. Il primo foglio deve contenere nome cognome e matricola. Il numero massimo di fogli ammessi è di 6 pagine. Il file da caricare deve essere in formato pdf e quando lo salvate sul vostro OneDrive va nominato come "vostro-codice-persona".

1. (a) Scrivere una formula $f(A, B, C)$ che ammetta la tavola di verità qui a fianco.

   (b) Argomentando bene la risposta, dire se $\neg A \wedge C \vdash_L f(A, B, C)$ usando la risoluzione.

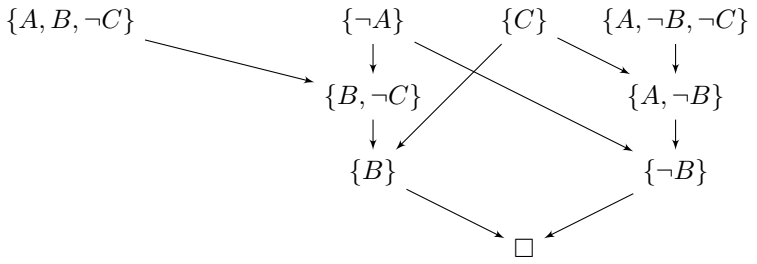
   (c) Scrivere una formula $g(A, B, C)$ non equivalente a $f(A, B, C)$ che non sia una tautologia tale che $\{f(A, B, C), \neg g(A, B, C)\}$ sia un insieme di formule insoddisfacibile.

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

Soluzione:

a) Dato che il numero di "1" presenti nella tabella è minore del numero di "0", possiamo costruire una formula f(A,B,C) in forma normale disgiuntiva: $f(A, B, C) \equiv (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C)$.

b) Dal teorema di correttezza e completezza della teoria L, abbiamo che $\neg A \wedge C \vdash_L f(A, B, C)$ se e solo se $\neg A \wedge C \vDash f(A, B, C)$ e questo è equivalente a dire che l'insieme di formule $\{\neg A \wedge C, \neg f(A, B, C)\}$ è insoddisfacibile. Dal teorema di correttezza e completezza per refutazione abbiamo che $\{\neg A \wedge C, \neg f(A, B, C)\}$ è insoddisfacibile se e solo se dall'insieme di clausole $\{\neg A \wedge C, \neg f(A, B, C)\}^c$ che si ottengono da questo insieme di formule si ottiene la clausola vuota per risoluzione. Calcoliamo $\{\neg A \wedge C, \neg f(A, B, C)\}^c$, da $\neg f(A, B, C)$ ricaviamo le clausole $\{A, B, \neg C\}, \{A, \neg B, \neg C\}, \{\neg A, B, \neg C\}$, e dalla prima formula ricaviamo le clausole $\{\neg A\}, \{C\}$. Un possibile modo per ottenere la clausola vuota è dato dalla seguente derivazione per risoluzione:



c) Dobbiamo cercare una formula $g(A, B, C)$ tale che per ogni modello v di $f(A, B, C)$ non sia modello di $\neg g(A, B, C)$, cioè sia un modello di $g(A, B, C)$. Quindi $g(A, B, C)$ deve avere gli stessi modelli di $f(A, B, C)$, corrispondenti alle righe in cui $f(A, B, C)$ è vera. Dato che $g(A, B, C)$ non deve essere equivalente a $f(A, B, C)$ basta che la tavola di verità di g differisca da quella di f per esempio sulla prima riga, cioè facciamo in modo che nell'interpretazione $w(A) = w(B) = w(C) = 0$ la f.b.f. $g(A, B, C)$ valga "1". Quindi abbiamo $g(A, B, C) \equiv f(A, B, C) \vee (\neg A \wedge \neg B \wedge \neg C)$. Notiamo che $g(A, B, C)$ non è una tautologia.

2. In $\mathbb{Z}_6$ sia D l'insieme dei divisori dello zero. Si consideri la relazione $R \subseteq \mathbb{Z}_6 \times \mathbb{Z}_6$ cosi definita: aRb se e solo se $a, b \in D \cup \{[0]_6\}$.

   (a) Disegnare il grafo d'adiacenza di R. Di quali proprietà gode R?

   (b) Esiste la chiusura d'ordine di R?

   (c) Si disegni il grafo d'adiacenza della chiusura d'equivalenza T di R e si costruisca l'insieme quoziente $\mathbb{Z}_6/T$.

   (d) Si consideri la funzione $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ coì definita:

$$f([a]_6) = \begin{cases} [0]_6 & \text{se } M.C.D(a,6) \neq 1 \\ [a]_6 & \text{altrimenti} \end{cases}$$

   e si dica se è un morfismo del monoide $(\mathbb{Z}_6, \cdot)$ (rispetto al prodotto di classi).

   (e) Si dica se $Ker\, f = T$.

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

$$\mathcal{F} = \forall x \exists y \, (\, A(x,y) \Rightarrow \exists z \, ((A(x,z) \wedge \neg E(x,z)) \Rightarrow A(z,x)) \,)$$

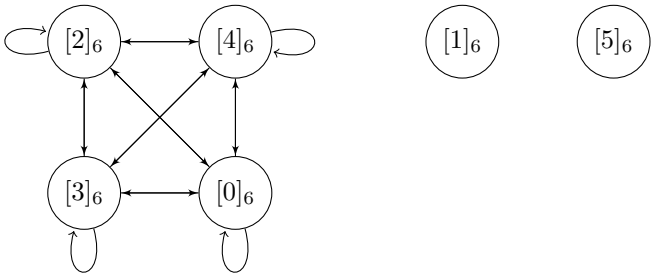
   e si dica se è vera, falsa, soddisfacibile ma non vera nelle seguenti interpretazioni:

   - dominio $\mathbb{Z}_6$, $A(x,y)$ sia R e $E(x,z)$ l'uguaglianza;
   - dominio $\mathbb{Z}_6$, $A(x,y)$ sia T e $E(x,z)$ l'uguaglianza;

   La precedente formula è logicamente valida?

Soluzione:

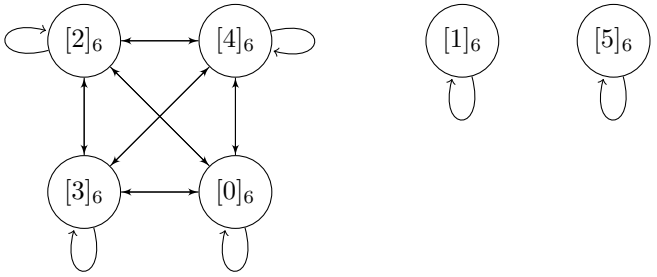
a) I divisori dello zero di $\mathbb{Z}_6$ sono $D = \{[2]_6, [3]_6, [4]_6\}$, quindi il grafo di adiacenza di R è il seguente:



Le proprietà di cui gode R sono la simmetria (tutti gli archi hanno la doppia freccia) e la transitività (tutti gli elementi da cui parte almeno un arco sono collegati fra di loro con archi bidirezionali).

b) Non può esistere la chiusura d'ordine di R perchè qualunque relazione che contiene R contiene anche le coppie $([2]_6, [4]_6)$ e $([4]_6, [2]_6)$ quindi non può essere antisimmetrica.

c) La chiusura d'equivalenza T di R si ottiene chiudendo riflessivamente, quindi $T = R \cup \{([1]_6, [1]_6), ([5]_6, [5]_6)\}$. Il suo grafo d'adiacenza é il seguente:



L'insieme quoziente $\mathbb{Z}_6/T = \{\{[0]_2, [2]_6, [3]_6, [4]_6\}, \{[1]_6\}, \{[5]_6\}\}$

d) Ricordiamo la seguente tavola moltiplicativa di $(\mathbb{Z}_6, \cdot)$:

$\cdot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Dalla tavola di composizione della moltiplicazione fra classi in $\mathbb{Z}_6$ si può notare che:

- se $x, y \in \{[1]_6, [5]_6\}$ allora $f(x) = x, f(y) = y$ e $x \cdot y \in \{[1]_6, [5]_6\}$; quindi $f(x \cdot y) = x \cdot y$ e così $f(x \cdot y) = f(x) \cdot f(y)$;

- se $x, y \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$, abbiamo che $x \cdot y \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$ quindi $f(x \cdot y) = [0]_6 = f(x) = f(y)$, quindi anche in questo caso $f(x \cdot y) = f(x) \cdot f(y)$;
- se $x \in \{[1]_6, [5]_6\}$ e $y \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$ allora $f(x) = x, f(y) = [0]_6$ e quindi $f(x) \cdot f(y) = [0]_6$; inoltre $x \cdot y \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$ e quindi $f(x \cdot y) = [0]_2$ da cui segue che $f(x \cdot y) = f(x) \cdot f(y)$.

Pertanto f è un morfismo ed in particolare si può osservare che è un morfismo di monoidi poichè $f([1]_6) = [1]_6$.

e) Notiamo che $(a, b) \in Ker(f)$ se e solo se $a, b \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$, oppure $a = b$ con $a \in \{[1]_6, [5]_6\}$, quindi $Ker(f)$ è esattamente la chiusura riflessiva di R, cioè T.

f) La formula è chiusa quindi in qualunque interpretazione essa è vera o falsa mentre non può essere soddisfacibile ma non vera.

- Nella prima interpretazione la formula è interpretata nel seguente modo: per ogni x esiste un y tale che se $(x, y) \in R$, allora esiste uno z tale che se $(x, z) \in R$ con $x \neq z$, allora $(z, x) \in R$. La formula è vera. Infatti se $x \in \{[1]_6, [5]_6\}$ allora l'antecedente non è mai soddisfatto dato che non esiste nessun y con $(x, y) \in R$. Se invece $x \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$, basta prendere un qualunque $z \neq x$ con $z \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$ per soddisfare il conseguente della formula $\mathcal{F}$ e quindi soddisfare la formula stessa.
- Nella seconda interpretazione la formula è ancora vera: le motivazioni sono le stesse del caso precedente se $x \in \{[0]_6, [2]_6, [3]_6, [4]_6\}$ mentre nel caso in cui $x \in \{[1]_6, [5]_6\}$ si ha che l'antecedente $A(x, y)$ è ora soddisfatto (basta prendere $y = x$) e però non esiste nessuno $z \neq x$ tale che $(x, z) \in T$, pertanto la sottoformula $A(x, z) \wedge \neg E(x, z)$ non è soddisfatta e quindi il conseguente dell'intera formula $\mathcal{F}$ risulta soddisfatto.

La formula $\mathcal{F}$ è logicamente valida, infatti per ogni relazione R su X che interpreta $A(x, y)$, per ogni $x \in X$, se $(x, x) \notin R$, allora prendendo $y = x$, l'antecedente di $\mathcal{F}$ è non soddisfatto, quindi $\mathcal{F}$ è soddisfatta, invece se $(x, x) \in R$ prendendo $y = x$, l'antecedente di $\mathcal{F}$ è soddisfatto, e prendendo $z = x$, la formula $A(x, z) \wedge \neg E(x, z)$ è non soddisfatta, rendendo il consequente di $\mathcal{F}$ soddisfatto. Quindi in entrambi i casi l'intera formula $\mathcal{F}$ è soddisfatta e pertanto essa risulta essere vera.
E' possibile dimostrare che la formula è logicamente valida anche usando la risoluzione per la logica del primo ordine. Innanzitutto neghiamo la formula data e portiamola in forma normale prenessa:

$$\neg\mathcal{F} \equiv \neg\forall x \exists y \, (\, A(x, y) \Rightarrow \exists z \, ((A(x, z) \wedge \neg E(x, z)) \Rightarrow A(z, x)) \,) \equiv$$

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

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

Scriviamo, ora, la forma di Skolem della formula ottenuta eliminando il primo quantificatore esistenziale dal prefisso e sostituendo con la costante c ogni occorrenza della variabile x da esso quantificata:

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

Trasformiamo in forma a clausole la matrice della precedente formula:

$$\neg \, (\neg \, A(c, y) \vee (\neg \, (A(c, z) \wedge \neg E(c, z)) \vee A(z, c)) \,) \equiv$$

$$\equiv \; A(c, y) \wedge A(c, z) \wedge \neg E(c, z) \wedge \neg A(z, c)$$

Dopo la separazione delle variabili, si ottengono così le clausole di input $\{A(c, y)\}$, $\{A(c, z)\}$, $\{\neg E(c, z_1)\}$, $\{\neg A(z_2, c)\}$. Applicando la sostituzione $\sigma = \{c/z_2, \, c/y\}$ alla prima e all'ultima clausola si ottengono le clausole $\{A(c, c)\}$, $\{\neg A(c, c)\}$, la cui risolvente è proprio la clausola vuota.

3. Sia $A = \{(a, b) : a, b \in \mathbb{R}, b \neq 0\}$ e sia $\star$ l'operazione interna su A definita da:

$$(a, b) \star (c, d) = (a + bc, bd)$$

(a) Si mostri che $(A, \star)$ è un gruppo;

(b) È commutativo?

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

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

e un'interpretazione avente come dominio l'insieme A e in cui la lettera funzionale E è interpretata dalla relazione di uguaglianza e la lettera funzionale p dall'operazione interna $\star$ vista nei punti precedenti. Dire se la formula è vera, falsa, soddisfacibile ma non vera in questa interpretazione

Soluzione:

a) L'esercizio già afferma che l'operazione $\star$ è interna, quindi verifichiamo che A sia un semigruppo mostrando l'associatività:

$$((a, b) \star (c, d)) \star (e, f) = (a + bc, bd) \star (e, f) = (a + bc + bde, bdf)$$

$$(a, b) \star ((c, d) \star (e, f)) = (a, b) \star (c + de, df) = (a + bc + bde, bdf)$$

che sono uguali. Per mostrare che è un gruppo basta provare che ha identità e inverso destro (teorema sui gruppi presente sulle dispense). Per l'identità imponiamo l'equazione $(a, b) \star (c, d) = (a, b)$ cioè $(a + bc, bd) = (a, b)$, quindi $d = 1, c = 0$. Quindi si verifica poi facilmente che $(a, b) \star (0, 1) = (a, b)$ per ogni $a, b \in \mathbb{R}$. Per l'inverso imponiamo l'equazione $(a, b) \star (x, y) = (0, 1)$ cioè $(a + bx, by) = (0, 1)$ da cui $y = 1/b$, $x = -a/b$ (ricordarsi che $b \neq 0$). Quindi si verifica che $(a, b) \star (-a/b, 1/b) = (0, 1)$.

b) Non è commutativo infatti $(1, 2) \star (3, 1) = (7, 2)$, mentre $(3, 1) \star (1, 2) = (4, 2)$ che sono diversi.

c) La formula è chiusa, quindi è vera o falsa. Nell'interpretazione data si traduce in: per ogni $x, y, z \in A$ se $x \star y = x \star z$, allora $y = z$ che è vera in tutti i gruppi. Infatti basta moltiplicare l'equazione $x \star y = x \star z$ per x^{-1} a sinistra per ottenere che $y = z$ (legge di cancellazione a sinistra per i gruppi).