Durata della prova: 1h 30'

Esame di Logica e Algebra

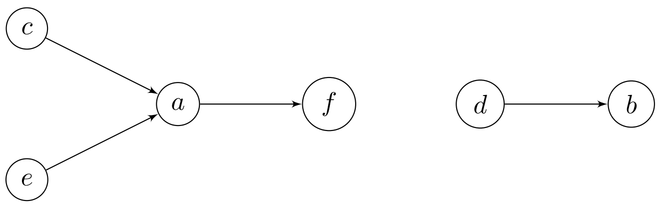
Politecnico di Milano – Ingegneria Informatica – 12 Luglio 2022

Docente e ultimo voto laboratorio:	**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: a) 3 b) 3 c) 2 d) 3)

   Sia $X = \{a, b, c, d, e, f\}$ e sia R la relazione su X rappresentata dal seguente grafo di adiacenza:



   (a) Determinare, se possibile, la minima relazione d'ordine S contenente R e, se esistono, gli elementi massimali e minimali, massimo e minimo di X rispetto a S.

   (b) Determinare la relazione d'equivalenza ρ generata da R e l'insieme quoziente X/ρ.

   (c) Dire quante sono le funzioni da X ad X contenenti R e quante tra queste ammettono inversa sinistra.

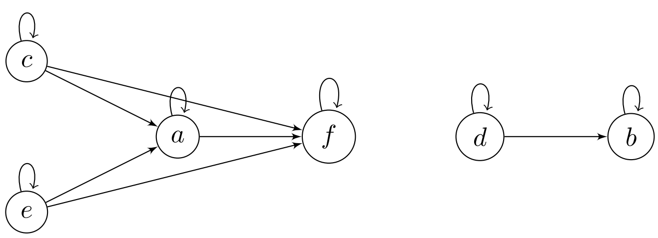
   (d) Data la seguente formula della logica del primo ordine

$$\forall x \forall z (A(x, y) \wedge A(z, y) \Longrightarrow \exists t A(y, t) \vee A(x, z))$$

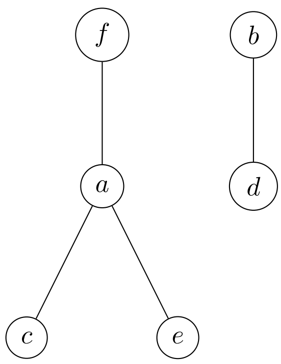
   stabilire se essa è vera, falsa o soddisfacibile ma non vera nell'interpretazione avente come dominio X e in cui A sia da interpretare come la relazione R.

Soluzioni:

   (a) La minima relazione d'ordine S contenente R è la chiusura riflessiva e transitiva di R e quindi ha il seguente grafo di adiacenza:

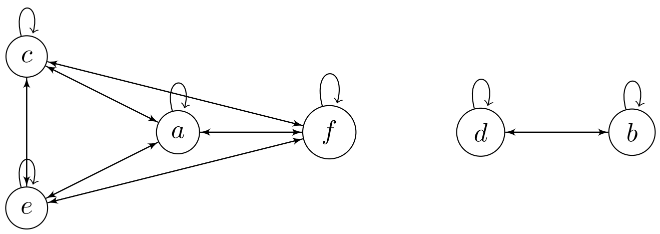


   Il diagramma di Hasse di S è il seguente:



   da cui si evince che l'insieme dei massimali è $\{b, f\}$, l'insieme dei minimali è $\{c, e, d\}$ e quindi non esistono massimo e minimo di X rispetto ad S.

(b) La relazione d'equivalenza ρ generata da R è la chiusura riflessiva, simmetrica e transitiva di R e quindi ha il seguente grafo di adiacenza:



L'insieme quoziente è $X/\rho = \{[a]_\rho, [b]_\rho\}$, dove $[a]_\rho = \{a, c, e, f\}$, $[b]_\rho = \{b, d\}$.

(c) Le funzioni $g : X \to X$ contenenti R devono essere tali che $g(a) = f$, $g(c) = g(e) = a$, $g(d) = b$ mentre per $g(f)$ e $g(b)$ si hanno rispettivamente 6 possibili scelte. Segue che il numero totale di funzioni contenenti R è 36. Di queste nessuna ammette inversa sinistra poiché nessuna di esse è suriettiva. Infatti, essendo X un insieme finito, una funzione $g : X \to X$ è suriettiva se e solo se è iniettiva e nessuna funzione g contenente R può essere iniettiva dal momento che deve verificare la condizione $g(c) = g(e) = a$.

(d) Osserviamo innanzitutto che la formula data non è chiusa poiché tutte le occorrenze della variabile y sono libere. La formula data è soddisfacibile ma non vera nell'interpretazione assegnata. Infatti, ad esempio, se consideriamo un assegnamento s' tale che $s'(y) = c$ allora l'antecedente della formula sarà sempre non soddisfatto da s' e pertanto s' soddisferà l'intera formula. Se invece consideriamo un assegnamento s tale che $s(y) = f$ allora l'antecedente $A(x, y) \wedge A(z, y)$ è soddisfatto da s se $s(x) = s(z) = a$. Non esiste però alcun elemento $\bar{t} \in X$ tale che $(f, \bar{t}) \in R$ quindi la sottoformula $\exists t A(y, t)$ del conseguente non è soddisfatta da s e non lo è neppure la sottoformula $A(x, z)$ poiché $(a, a) \notin R$. Pertanto s non soddisferà l'intera formula che quindi risulterà soddisfacibile ma non vera nell'interpretazione assegnata.

2. (Punteggio: a) 3 b) 3 c) 3)

Si consideri la seguente tavola di verità:

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

(a) Si scriva una formula $f(A,B,C)$ che abbia come tavola di verità quella assegnata e che contenga solo i connettivi $\neg$ e $\Longrightarrow$.

(b) Verificare se $B \Rightarrow A \vdash_L f(A,B,C)$ nella teoria L.

(c) Ridimostrare il risultato trovato al punto precedente usando la risoluzione.

Soluzioni:

(a) Una formula $f(A,B,C)$ che abbia come tavola di verità quella assegnata ha la seguente forma normale congiuntiva:

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

Semplifichiamola e scriviamola in modo tale che contenga solo i connettivi $\neg$ e $\Longrightarrow$:

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

$$\equiv (\neg(B \Longrightarrow A) \vee \neg(A \Longrightarrow B)) \Longrightarrow C \equiv ((B \Longrightarrow A) \Longrightarrow \neg(A \Longrightarrow B)) \Longrightarrow C.$$

(b) Per il teorema di correttezza e completezza forte, vale $B \Rightarrow A \vdash_L f(A,B,C)$ se e solo se $B \Rightarrow A \vDash f(A,B,C)$, cioè se e solo se tutti i modelli di $B \Rightarrow A$ sono modelli di $f(A,B,C)$. La deduzione pertanto non esiste in quanto l'interpreatazione v tale che $v(A) = 1$ e $v(B) = v(C) = 0$ è modello di $B \Rightarrow A$ ma non di $f(A,B,C)$. Segue che $B \Rightarrow A \nvdash_L f(A,B,C)$.

(c) Dobbiamo verificare che $\Gamma = \{B \Rightarrow A, \neg f(A,B,C)\}$ non è insoddisfacibile e quindi che dalle clausole di Γ non possiamo ottenere la clausola vuota. Sappiamo che

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

da cui segue che

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

Si ottengono pertanto le clausole $\{\neg C\}, \{\neg A, \neg B\}, \{A, B\}$, mentre dalla formula $B \Rightarrow A$ otteniamo la clausola $\{\neg B, A\}$. Quindi abbiamo:

$$\Gamma^c = \{\, \{\neg C\}, \{\neg A, \neg B\}, \{A, B\}, \{\neg B, A\} \,\}$$

poiché il letterale C non compare in nessuna altra clausola possiamo fare un pruning e considerare l'insieme di clausole

$$\Lambda = \{\, \{\neg A, \neg B\}, \{A, B\}, \{\neg B, A\} \,\}$$

da cui $Ris(\Lambda) = \Lambda \cup \{\{A\}, \{\neg B\}\}$, e $Ris^2(\Lambda) = \Lambda \cup \{\{A\}, \{\neg B\}\}$. Non potendo ottenere la clausola vuota, deduciamo che Γ non è insoddisfacibile. Segue che non è vero che $B \Rightarrow A \vDash f(A,B,C)$ e quindi nemmeno che $B \Rightarrow A \vdash_L f(A,B,C)$.

3. (Punteggio: a) 4 b) 2 c) 3 d) 2)
Sia $(Z_8, +, \cdot)$ l'anello delle classi di resto modulo 8.

(a) Si consideri il sottoinsieme $X = \{[0]_8, [2]_8, [4]_8, [6]_8\}$ dell'anello $(Z_8, +, \cdot)$. Si stabilisca se X è un sottoanello di $(Z_8, +, \cdot)$ e, in caso affermativo, si verifichi se X è anche un ideale.

(b) Si risolva la seguente equazione congruenziale in Z_8:

$$[5]_8 \cdot x + [2]_8 = [3]_8$$

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

$$\neg\exists y A(f(x,y),a) \Longrightarrow \exists y(\neg A(y,b) \wedge A(f(x,y),b))$$

e si stabilisca se è vera, falsa o soddisfacibile ma non vera nell'interpretazione che ha dominio Z_8, in cui la costante a sia da interpretare come l'unità dell'anello, la costante b come lo zero dell'anello, f sia da interpretare come l'operazione di moltiplicazione tra classi di resto modulo 8 e A come l'uguaglianza.

(d) Si chiuda universalmente la formula data e si verifichi, usando la risoluzione del primo ordine, che tale chiusura non è logicamente valida.

Soluzioni:

(a) Usiamo il criterio di caratterizzazione dei sottoanelli e verifichiamo che, per ogni $x, y \in X$, si ha che $x - y \in X$ e $xy \in X$. Questo punto può essere affrontato o facendo le tavole delle differenze $x - y$ e dei prodotti xy, oppure notando che X è composto da divisori dello zero e dallo zero stesso. In particolare, i rappresentanti degli elementi di X sono tutti e soli i multipli di 2, cioè $X = \{[2k]_8 : k \in \mathbb{Z}\}$. Quindi se $a, b \in \mathbb{Z}$ sono i rappresentanti di $x = [a]_8, y = [b]_8$, allora $a - b$ e ab sono anch'essi multipli di due e quindi abbiamo che $[a - b]_8, [ab]_8 \in X$ da cui segue che $(X, +, \cdot)$ è sottoanello di $(Z_8, +, \cdot)$. Inoltre $(X, +, \cdot)$ è anche un ideale dato che se $x = [a]_8$ allora moltiplicando x a destra o a sinistra (per commutatività!) per un elemento $z = [c]_8 \in \mathbb{Z}_8$ abbiamo che $xz = [ac]_8$ che appartiene ancora ad X dato che a è multiplo di 2 e quindi anche ac lo è.

(b) L'equazione è equivalente a $[5]_8 \cdot x = [3]_8 - [2]_8$ e quindi a $[5]_8 \cdot x = [1]_8$. Dato che 5 è primo con 8 allora $[5]_8$ ha inverso moltiplicativo che ovviamente non sarà da ricercare fra gli elementi dell'insieme X. Chiaramente $[1]_8$ non è l'inverso di $[5]_8$ e quindi restano da verificare gli elementi $[3]_8, [5]_8, [7]_8$. Poiché $[5]_8 \cdot [5]_8 = [25]_8 = [1]_8$ segue che la soluzione dell'equazione è $x = [5]_8$.

(c) La formula si traduce nel seguente modo: dato un $x \in \mathbb{Z}_8$, se non esiste nessun $y \in \mathbb{Z}_8$ tale che $xy = [1]_8$, allora esiste uno $z \in \mathbb{Z}_8$ (possiamo cambiare nome alla variabile!) diverso da $[0]_8$ tale che $xz = [0]_8$. In pratica la formula dice che se x non ha inverso moltiplicativo, allora x è divisore dello zero. Si può verificare direttamente la formula facendo una casistica su tutti gli $x \in \mathbb{Z}_8$ oppure si può fare riferimento alla teoria in quanto sappiamo che $x \in \mathbb{Z}_n$ ha inverso moltiplicativo se e solo non è divisore dello zero. Pertanto la formula risulta vera nell'interpretazione assegnata.

(d) La chiusura universale della formula data è la seguente:

$$\psi = \forall x\, (\neg\exists y A(f(x,y),a) \Longrightarrow \exists y(\neg A(y,b) \wedge A(f(x,y),b)))$$

Sappiamo che ψ è logicamente valida se e solo se $\neg\psi$ è insoddisfacibile e quindi dal teorema di correttezza e completezza per refutazione $\{\neg\psi\}^c \vdash_R \Box$. Per calcolare le clausole di $\neg\psi$, portiamo prima la formula in FNP:

$$\begin{aligned}\neg\psi \equiv& \exists x \neg\, (\exists y A(f(x,y),a) \vee \exists y(\neg A(y,b) \wedge A(f(x,y),b))) \equiv \\ & \exists x\, (\neg\exists y A(f(x,y),a) \wedge \neg\exists y(\neg A(y,b) \wedge A(f(x,y),b))) \equiv \\ & \exists x \forall y\, (\neg A(f(x,y),a) \wedge \forall y \neg(\neg A(y,b) \wedge A(f(x,y),b))) \equiv \\ & \exists x \forall y \forall z\, (\neg A(f(x,y),a) \wedge \neg(\neg A(z,b) \wedge A(f(x,z),b))) \equiv \\ & \exists x \forall y \forall z\, (\neg A(f(x,y),a) \wedge (A(z,b) \vee \neg A(f(x,z),b)))\end{aligned}$$

e quindi la sua forma di Skolem è

$$\forall y \forall z\, (\neg A(f(d,y),a) \wedge (A(z,b) \vee \neg A(f(d,z),b)))$$

dove d è la nuova costante introdotta nella skolemizzazione al posto della variabile x. Pertanto le clausole che otteniamo sono:

$$\{\neg\psi\}^c = \{\, \{\neg A(f(d,y),a)\}, \{A(z,b), \neg A(f(d,z),b)\}\, \}$$

nessun letterale tra la prima e la seconda clausola è unificabile dato che nella prima clausola la seconda componente è la constante a, mentre nelle altre clausole la seconda componente è b. Pertanto l'insieme delle risolventi di $\{\neg\psi\}^c$ è $\{\neg\psi\}^c$ stesso e quindi non possiamo ottenere la clausola vuota. Ne deduciamo che $\neg\psi$ non è insoddisfacibile da cui segue che ψ non è logicamente valida.