Durata della prova: 1h 30'

Esame di Logica e Algebra

Politecnico di Milano – Ingegneria Informatica – 31 Agosto 2018

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.

1. Sia $X = \{a, b, c, d, e\}$ $Y = \{x, y, z\}$ e sia $R \subseteq X \times Y$ la relazione definita da:

$$R = \{(a, x), (b, y), (b, z), (c, x), (d, z), (e, x), (e, y), (e, z)\}$$

(a) Quante funzioni sono contenute in R? Quante di queste sono iniettive?

(b) Indicare una funzione $f : X \to Y$ che sia contenuta in R. Determinare $\ker f$, e costruire $X/_{kerf}$.

(c) Dire se esiste una funzione $g : X \to Y$ che sia suriettiva e contenuta in R. In caso affermativo costruire una sua inversa sinistra e dire quante sono le possibili inverse sinistre di g.

Soluzione:

(a) Dato che l'unico elemento in relazione con a e c è x e con d è z, allora se $f \subseteq R$ necessariamente $f(a) = f(c) = x$, mentre $f(d) = z$, $f(b)$ può essere o z o y, mentre $f(e)$ può essere x, y, z. Quindi $2 \cdot 3 = 6$ scelte. Non ci sono funzioni iniettive dato che se esistesse una funzione iniettiva g avremmo $5 = |g(X)| \leq |Y| = 3$, assurdo.

(b) Una possibile funzione è $f(a) = f(c) = x$, $f(d) = f(b) = f(e) = z$. Le $\ker f$-classi di f sono $[a]_{\ker f} = \{a, c\}$, $[b]_{\ker f} = \{d, b, e\}$ da cui $X/_{\ker f} = \{[a]_{\ker f}, [b]_{\ker f}\}$.

(c) Una possibile funzione suriettiva è $g(a) = g(c) = x$, $g(d) = g(b) = z$, $g(e) = y$. Un'inversa sinistra è data scegliendo $h(x) \in \{a, c\}$, $h(z) \in \{b, d\}$, $h(e) = y$, quindi 4 possibili inverse sinistre, una possibile è data da $h(x) = a$, $h(z) = b$, $h(e) = y$. È facile verificare che $h \cdot f$ è l'identità su Y.

2. (a) Dire se nella teoria $\mathcal{L}$ la formula $(A \wedge B) \Rightarrow (A \Rightarrow \neg B)$ può essere dedotta da $A \vee \neg B$.

   (b) Provare lo stesso risultato utilizzando la teoria della risoluzione.

Soluzione:

(a) Per il teorema di correttezza e completezza nella teoria $\mathcal{L}$ abbiamo $A \vee \neg B \vdash_{\mathcal{L}} (A \wedge B) \Rightarrow (A \Rightarrow \neg B)$ se e solo se $A \vee \neg B \vDash (A \wedge B) \Rightarrow (A \Rightarrow \neg B)$ dato che $(A \wedge B) \Rightarrow (A \Rightarrow \neg B)$ è falso solo quando A e B sono entrambe vere, abbiamo che $(A \wedge B) \Rightarrow (A \Rightarrow \neg B)$ è equivalente a $\neg(A \wedge B) = \neg A \vee \neg B$. Quindi il modello $A = 1, B = 1$ di $A \vee \neg B$ non è modello di $(A \wedge B) \Rightarrow (A \Rightarrow \neg B)$, da cui possiamo dedurre $A \vee \neg B \nvdash_{\mathcal{L}} (A \wedge B) \Rightarrow (A \Rightarrow \neg B)$.

(b) Dal teorema di correttezza e completezza per refutazione dobbiamo mostrare che $\{\neg((A \wedge B) \Rightarrow (A \Rightarrow \neg B)), (A \vee \neg B)\}^c \vdash_R \Box$. Dato che $\neg((A \wedge B) \Rightarrow (A \Rightarrow \neg B))$ è equivalente a $(A \wedge B)$, abbiamo $\{\neg((A \wedge B) \Rightarrow (A \Rightarrow \neg B)), (A \vee \neg B)\}^c = \{\{A\}, \{B\}, \{A, \neg B\}\}$. Si nota subito che l'unica risolvente significativa che si può ottenere è quella tra $\{A, \neg B\}$ e $\{B\}$ che da ancora $\{A\}$, quindi non si può ottenere la clausola vuota e quindi $A \vee \neg B \nvdash_{\mathcal{L}} (A \wedge B) \Rightarrow (A \Rightarrow \neg B)$.

3. Si consideri la seguente formula del primo ordine:

$$((\forall x)(\forall y)A(f(x,y),z)) \Rightarrow (\exists x)\,(A(x,y) \Rightarrow (\forall y)A(x,y))$$

(a) Si indichino le occorrenze libere e vincolate di ogni variabile e si porti la formula data in forma normale prenessa.

(b) Si consideri l'interpretazione avente come dominio i naturali $\mathbb{N}$, in cui la lettera predicativa $A(x,y)$ viene interpretata come $x > y$ e la lettera funzionale $f(x,y)$ viene interpretata come il prodotto $x \cdot y$. Dire se in tale interpretazione la formula è vera, falsa o soddisfacibile ma non vera.

Soluzione:

(a) z è una variabile libera ed inoltre è libera la prima occorrenza di y nel conseguente. Tutte le altre occorrenze di x ed y sono vincolate. Per portare la formula a forma prenessa cominciamo a portare in forma prenessa il suo conseguente:

$$((\forall x)(\forall y)A(f(x,y),z)) \Rightarrow (\exists x)(\forall u)\,(A(x,y) \Rightarrow A(x,u))$$

poi portiamo davanti a tutto i quantificatori dell'antecedente:

$$(\exists x)(\exists v)\,((A(f(x,v),z) \Rightarrow (\exists x)(\forall u)\,(A(x,y) \Rightarrow A(x,u)))$$

e da ultimo portiamo davanti a tutto i quantificatori del conseguente:

$$(\exists x)(\exists v)(\exists w)(\forall u)\,(A(f(x,v),z) \Rightarrow (A(w,y) \Rightarrow A(w,u)))$$

(b) Nell'interpretazione suggerita dal testo la formula data si legge come: "se per ogni x e per ogni y $xy > z$ allora esiste un x tale che se $x > y$ allora per ogni $y, x > y$, dove x,y,z stanno in $\mathbb{N}$. Comunque assegniamo un valore a z, la formula per ogni x e per ogni y $xy > z$ é falsa (basta prendere $x = y = 1$ e $z = 1$), dunque la nostra formula è vera.

4. Sia consideri sull'insieme dei numeri reali $\mathbb{R}$ l'operazione binaria interna $\#$ definita nel seguente modo:

$$a\#b = a + b - (a \cdot b)$$

dove $+$ e $\cdot$ sono le usuali operazioni di addizione e moltiplicazione in $\mathbb{R}$ e l'elemento $-(a \cdot b)$ è l'opposto rispetto all'operazione $+$ dell'elemento $a \cdot b$.

(a) Mostrare che $(R, \#)$ è un monoide commutativo.

(b) $(R, \#)$ è anche un gruppo? In caso contrario, descrivere l'insieme degli elementi che **non** sono invertibili.

Soluzione:

1. Dobbiamo verificare che l'operazione sia associativa. Si ha

$$a\#(b\#c) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc$$

inoltre si ha:

$$(a\#b)\#c = (a + b - ab) + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc$$

che sono chiaramente uguali, quindi l'operazione è associativa. É chiaramente commutativa:

$$a\#b = a + b - ab = b + a - ba = b\#a$$

Cerchiamo l'unità. Questa è un elemento x che deve soddisfare:

$$a\#x = a$$

per ogni a. Quindi $a + x - ax = a$ da cui otteniamo che necessariamente $x(1 - a) = 0$ per ogni a, quindi $x = 0$. Si verifica facilmente che $a\#0 = a$ per ogni a, quindi 0 è l'unità e dunque $(\mathbb{R}, \#)$ è un monoide.

2. Per verificare se è un gruppo, dato che $\#$ è commutativa, basta verificare se, dato un qualunque elemento a, esiste un elemento x tale che:

$$a\#x = 0$$

cioè $a + x - ax = 0$ da cui otteniamo che necessariamente $x = -\frac{a}{1-a}$. Quindi non è un gruppo, dato che l'elemento 1 non è invertibile. Nel caso in cui $a \neq 1$ si verifica subito che $a\# - \frac{a}{1-a} = 0$, da cui deduciamo che l'insieme degli elementi che non sono invertibili è l'insieme $\{1\}$.