Corso di Laurea in Informatica Applicata

Linguaggio e Metodi della Matematica

Prova scritta del 18 Gennaio 2006

[Esercizio 1]
Sia $f : \mathbb{N} \rightarrow \mathbb{Z}$ la funzione definita come $f(n) = n^2 - 3n + 1$. Si dica, giustificando ogni risposta, se f è iniettiva, surgettiva, bigettiva. Inoltre, a cosa corrispondono $f^{-1}(0)$, $f^{-1}(1)$ e $f^{-1}(5)$?

Svolgimento

f non è iniettiva perché esistono due valori che hanno la stessa immagine. Infatti $f(0) = 1 = f(3)$ (o anche $f(1) = -1 = f(2)$).

f non è surgettiva perché ad esempio non esiste $n \in \mathbb{N}$ tale che $f(n) = 0$.

f non è bigettiva perché non è iniettiva (e neppure surgettiva).

$f^{-1}(0) = \emptyset$, $f^{-1}(1) = \{0, 3\}$ e $f^{-1}(5) = \{4\}$

[Esercizio 2]
Si dica, giustificando tutte le risposte, se le seguenti formule predicative sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

1. $\forall x.(Q(x) \land \neg R(x)) \ \rightarrow \ \exists x.\neg P(x)$
2. $\exists x.(P(x) \ \rightarrow \ R(x) \lor \neg Q(x))$

Svolgimento

Verifichiamo prima se le formule sono equivalenti, poi mostriamo che sono soddisfacibili.

$$
\begin{aligned}
\forall x.(Q(x) \land \neg R(x)) \ \rightarrow \ \exists x.\neg P(x) &\equiv \neg(\forall x.(Q(x) \land \neg R(x))) \lor \exists x.\neg P(x) \quad \text{(implic.)} \\
&\equiv \exists x.\neg(Q(x) \land \neg R(x)) \lor \exists x.\neg P(x) \quad \text{(neg. quantif.)} \\
&\equiv \exists x.(\neg Q(x) \lor \neg\neg R(x)) \lor \exists x.\neg P(x) \quad \text{(de morgan)} \\
&\equiv \exists x.(\neg Q(x) \lor R(x)) \lor \exists x.\neg P(x) \quad \text{(doppia neg.)} \\
&\equiv \exists x.((\neg Q(x) \lor R(x)) \lor \neg P(x)) \quad \text{(distrib. quantif.)} \\
&\equiv \exists x.(\neg Q(x) \lor R(x) \lor \neg P(x)) \quad \text{(assoc.)}
\end{aligned}
$$

$$
\begin{aligned}
\exists x.(P(x) \rightarrow R(x) \lor \neg Q(x)) &\equiv \exists x.(\neg P(x) \lor (R(x) \lor \neg Q(x))) \quad \text{(implic.)} \\
&\equiv \exists x.(\neg Q(x) \lor R(x) \lor \neg P(x)) \quad \text{(assoc. + comm.)}
\end{aligned}
$$

Quindi le formule sono equivalenti.

Per mostrare che non sono tautologie si consideri l'interpretazione $\mathcal{I}$ tale che $D_{\mathcal{I}} = \{a\}$, $TS_{\mathcal{I}}(P) = TS_{\mathcal{I}}(Q) = \{a\}$, e $TS_{\mathcal{I}}(R) = \emptyset$. Infatti $\mathcal{I} \models P(a)$ ma $\mathcal{I} \not\models R(a) \lor \neg Q(a)$ e quindi $\mathcal{I} \not\models P(a) \rightarrow R(a) \lor \neg Q(a)$. Dato che a è l'unico valore nel dominio $D_{\mathcal{I}}$, si ha $\mathcal{I} \not\models \exists x.(P(x) \rightarrow R(x) \lor \neg Q(x))$.

Analogamente, per mostrare che non sono contraddizioni si consideri l'interpretazione $\mathcal{I}'$ tale che $D_{\mathcal{I}'} = \{a\}$, $TS_{\mathcal{I}'}(P) = TS_{\mathcal{I}'}(Q) = TS_{\mathcal{I}'}(R) = \emptyset$. Infatti $\mathcal{I}' \not\models P(a)$ e quindi $\mathcal{I}' \models P(a) \rightarrow R(a) \lor \neg Q(a)$ (quando la premessa è falsa, l'implicazione è vera). Dunque $\mathcal{I}' \models \exists x.(P(x) \rightarrow R(x) \lor \neg Q(x))$ (scegliendo $x = a$).

Le interpretazioni $\mathcal{I}$ e $\mathcal{I}'$ mostrano che le formule sono soddisfacibili.

[Esercizio 3 - SOLO PER RECUPERO PRIMO COMPITINO]

P	Q	$P\|Q$
0	0	1
0	1	1
1	0	1
1	1	0

Si dimostri che tutti i connettivi logici (della logica proposizionale) possono essere espressi in termini del solo operatore $P|Q$ (si legge "P *nand* Q") definito dalla tabella di verità a lato. L'operatore di *nand* è commutativo? È associativo?

Svolgimento

Abbiamo visto durante il corso che tutti i connettivi logici possono essere espressi usando soltanto negazione e congiunzione. Quindi per mostrare che tutti i connettivi logici possono essere espressi usando il solo nand è sufficiente far vedere che la negazione e la congiunzione possono essere espresse usando solo nand.

Dalle tabelle di verità si nota che $P|Q \equiv \neg(P \wedge Q)$ (come suggerito anche dal nome stesso dell'operatore).

Quindi possiamo esprimere la negazione nel seguente modo:

$$\neg P \equiv P|P$$

Infatti $P|P \equiv \neg(P \wedge P) \equiv \neg(P)$.

Dato che sappiamo come esprimere la negazione, sfruttando il fatto che $P \wedge Q \equiv \neg\neg(P \wedge Q)$ è facile vedere che possiamo esprimere la congiunzione nel seguente modo:

$$P \wedge Q \equiv (P|Q) \mid (P|Q)$$

Infatti $P \wedge Q \equiv \neg\neg(P \wedge Q) \equiv \neg(P|Q) \equiv (P|Q) \mid (P|Q)$.

Confrontando le tabelle di verità si $P|Q$ e $Q|P$ si verifica immediatamente che il nand è commutativo.

Invece non è associativo, dato che, ad esempio $(\top|\top)|\bot \equiv \bot|\bot \equiv \top$, mentre $\top|(\top|\bot) \equiv \top|\top \equiv \bot$.

[Esercizio 4 - SOLO PER RECUPERO PRIMO COMPITINO] Scrivere una formula della logica predicativa che formalizzi la frase "m è il minimo comune multiplo di a e b" sul dominio dei naturali, sfruttando la costante 0, il simbolo di funzione $\times$, e i simboli di predicato $=$ e $\leq$ con l'ovvio significato. (*Consiglio*: definire la formula per esprimere che "x è multiplo di y" e poi riusarla più volte).

Svolgimento

Il minimo comune multiplo è il più piccolo tra i naturali che sono multipli sia di a che di b. La formula per esprimerlo è quindi analoga a quella che definisce il massimo comun divisore.

Definiamo dapprima la formula $\mathrm{mult}(x, y)$ che formalizza la frase "x è multiplo di y". Essendo il dominio quello dei naturali non dobbiamo preoccuparci dei valori negativi.

$$\forall x, y(\ \mathrm{mult}(x, y) \ \leftrightarrow \ \exists p.(y \times p = x \wedge \neg(p = 0))\ )$$

Il controllo $\neg(p = 0)$ serve per evitare che $x = 0$ venga considerato multiplo di un valore y positivo. Alternativamente si potrebbe scrivere:

$$\forall x, y(\ \mathrm{mult}(x, y) \ \leftrightarrow \ \exists p.(y \times p = x \wedge y \leq x)\ )$$

Adesso bisogna formalizzare il fatto che m è un multiplo di a e di b e che preso un qualsiasi altro multiplo k di a e b si ha m minore o uguale a k:

$$\begin{aligned}\forall a, b, m(\ \mathrm{mcm}(a, b, m) \ \leftrightarrow \ & \mathrm{mult}(m, a) \wedge \\ & \mathrm{mult}(m, b) \wedge \\ & \forall k.(\mathrm{mult}(k, a) \wedge \mathrm{mult}(k, b) \ \rightarrow \ m \leq k)\ )\end{aligned}$$

[Esercizio 5]
Si dica se le seguenti proprietà su insiemi sono valide, fornendo una dimostrazione formale in caso positivo oppure un controesempio in caso negativo:

1. $\forall A, B, C. ((A \subseteq B \cup C) \;\rightarrow\; (A - C \subseteq B))$
2. $\forall A, B, C. ((A \subseteq B \cup C) \;\rightarrow\; (A \cap C \subseteq B))$

Svolgimento

La proprietà $\forall A, B, C. ((A \subseteq B \cup C) \;\rightarrow\; (A - C \subseteq B))$ è valida, come dimostrato dalla seguente prova formale:

1.	$A \subseteq B \cup C$	(Ipotesi aggiuntiva)
2.	$\quad x \in A - C$	(Ipotesi aggiuntiva)
3.	$\quad\quad x \in A \cap \overline{C}$	(**EQ**. da 2)
4.	$\quad\quad x \in A$	(**A**.**E**.$_\cap$ da 3)
5.	$\quad\quad x \in B \cup C$	(**M**.**P**.$_\subseteq$ da 1 e 4)
6.	$\quad\quad x \notin C$	(**A**.**E**.$_\cap$ da 3)
7.	$\quad\quad x \in B$	(**D**.**S**.$_\cup$ da 5 e 6)
8.	$\quad x \in A - C \rightarrow x \in B$	(**Imp**. da $\frac{[2]}{7}$)
9.	$\quad A - C \subseteq B$	($\forall$**G**$_\subseteq$ da 8)
10.	$(A \subseteq B \cup C) \;\rightarrow\; (A - C \subseteq B)$	(**Imp**. da $\frac{[1]}{9}$)
11.	$\forall A, B, C. ((A \subseteq B \cup C) \;\rightarrow\; (A - C \subseteq B))$	($\forall$**G** per tre volte da 10)

La proprietà $\forall A, B, C. ((A \subseteq B \cup C) \;\rightarrow\; (A \cap C \subseteq B))$ non è valida, come dimostrato dal seguente semplice controesempio.
Prendiamo $A = \{1, 2\}$, $B = \{1\}$ e $C = \{2\}$.
Ovviamente $B \cup C = \{1, 2\}$ e $A \cap C = \{2\}$, quindi:

- $A \subseteq B \cup C$;
- $A \cap C \not\subseteq B$.

[Esercizio 6]
Si considerino le stringhe di lunghezza 8 sull'alfabeto $A = \{a, b, c\}$. In quante di esse entrambi i simboli a e b sono usati esattamente una volta (es. *ccacccbc*)? E in quante stringhe a e b sono usati al massimo una volta (es. *ccacccbc*, *ccaccccc*).

Svolgimento

Ogni stringa che contiene esattamente una occorrenza di entrambi a e b è determinata univocamente dalle posizioni occupate dall'unico carattere a e dall'unico carattere b (perché tutti gli altri caratteri sono c).
Quindi il problema si riconduce a scegliere due posizioni tra le otto disponibili: la prima per il carattere a e la seconda per il carattere b.
In questo modo il problema viene formulato in termini delle disposizioni ordinate di due elementi presi da un insieme di otto, e quindi il numero di possibili scelte è

$$P(8, 2) \; = \; 8!/(8-2)! \; = \; 8!/6! \; = \; 8 \cdot 7 \; = \; 56.$$

Le stringhe che contengono al massimo una occorrenza di a e al massimo una occorrenza di b possono essere partizionate in quattro insiemi disgiunti:

- S_0, che comprende le stringhe che non contengono a e b;
- S_{ab}, che comprende le stringhe che contengono esattamente una occorrenza di entrambi a e b;
- S_a, che comprende le stringhe che contengono un solo carattere a e non contengono b;
- S_b, che comprende le stringhe che contengono un solo carattere b e non contengono a.

L'insieme S_0 contiene ovviamente una sola stringa (*cccccccc*): $|S_0| = 1$.
La cardinalità dell'insieme S_{ab} è stata calcolata sopra: $|S_{ab}| = 56$.
La cardinalità dell'insieme S_a può essere calcolata in maniera analoga a quella di S_{ab}: questa volta dobbiamo considerare le disposizioni ordinate di un solo elemento (la posizione dove mettere a, in tutte le altre posizioni dobbiamo mettere c) preso da un insieme di otto. Ovviamente:

$$P(8, 1) \; = \; 8!/(8-1)! \; = \; 8!/7! \; = \; 8.$$

Infatti $S_a = \{acccccccc, caccccccc, ccaccccc, ...\}$ e quindi $|S_a| = 8$.
La cardinalità dell'insieme S_b è ovviamente la stessa di S_a, infatti $S_b = \{bccccccc, cbcccccc, ccbccccc, ...\}$.
Essendo gli insiemi disgiunti, per la regola della somma:

$$|S_0 \cup S_a \cup S_b \cup S_{ab}| \; = \; |S_0| + |S_a| + |S_b| + |S_{ab}| \; = \; 1 + 8 + 8 + 56 = 73$$

[Esercizio 7 - SOLO PER RECUPERO SECONDO COMPITINO] Date due relazioni $R_1 \subseteq \mathbb{Z} \times \mathbb{Z}$ e $R_2 \subseteq \mathbb{Z} \times \mathbb{Z}$, la loro *composizione* è la relazione $R_2 \circ R_1 = \{(n, m) \mid \exists k.(n \; R_1 \; k \; \wedge \; k \; R_2 \; m\} \subseteq \mathbb{Z} \times \mathbb{Z}$. Mostrare con un controesempio che la composizione di relazioni non è commutativa. A cosa corrisponde la relazione $R_{\pm 1} \circ R_{\pm 1}$?

Svolgimento

Prendiamo $R = \{(1, 2)\}$ e $S = \{(2, 1)\}$. Si ha:

- $S \circ R = \{(1, 1)\}$
- $R \circ S = \{(2, 2)\}$

Quindi $S \circ R \neq R \circ S$.

Se $n \; R_{\pm 1} \; k$, allora vuol dire che n e k distano al massimo 1. Analogamente se $k \; R_{\pm 1} \; m$, allora vuol dire che m e k distano al massimo 1. Quindi n e m distano al massimo 2. Quindi:

$$R_{\pm 1} \circ R_{\pm 1} \; = \; \{(n, m) \mid n, m \in \mathbb{Z} \wedge -2 \leq n - m \leq 2\} \; = \; R_{\pm 2}$$

[Esercizio 8 - SOLO PER RECUPERO SECONDO COMPITINO]
Disegnare il diagramma di Hasse della relazione di divisibilità sul dominio $\{4, 5, 6, 20, 24, 30, 600\}$

Svolgimento