

ALGEBRA e LOGICA
CdL in Ingegneria Informatica
prof. Fabio GAVARINI

Sessione Estiva Anticipata 2014–2015 / Sessione Invernale 2013–2014 — II appello
Esame scritto del 23 Febbraio 2015 — COMPITO S

.....

*N.B.: compilare il compito in modo sintetico ma **esauriente**, spiegando
chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

..... S

[1] Sia D_{56} l'insieme dei numeri naturali divisori di 56, dotato della relazione d'ordine di *divisibilità*, e sia $\mathcal{P}(\{x, y, z\})$ l'insieme delle parti dell'insieme $\{x, y, z\}$, dotato della relazione d'ordine di *inclusione*; in particolare, entrambi sono insiemi ordinati.

(a) D_{56} è totalmente ordinato? $\mathcal{P}(\{x, y, z\})$ è totalmente ordinato?

(b) D_{56} è limitato? $\mathcal{P}(\{x, y, z\})$ è limitato? In entrambi i casi, se la risposta è negativa se ne spieghi il perché, se è affermativa si precisi chi siano i limiti.

(c) D_{56} è un *reticolo*? $\mathcal{P}(\{x, y, z\})$ è un *reticolo*? Se sono entrambi reticoli, sono isomorfi l'uno all'altro?

(d) D_{56} è un'algebra di Boole? $\mathcal{P}(\{x, y, z\})$ è un'algebra di Boole?

(e) Quali sono — se esistono — gli *atomi* di D_{56} e gli atomi di $\mathcal{P}(\{x, y, z\})$?

[2] (a) Scrivere in base $b' := \text{DIECI}$ il numero N che in base $b := \text{CINQUE}$ è espresso dalla scrittura posizionale $N := (4203)_b$.

(b) Scrivere in base $b := \text{CINQUE}$ il numero T che in base $b' := \text{DIECI}$ è espresso dalla scrittura posizionale $T := (276)_{b'}$.

(c) Scrivere in base $b' := \text{DIECI}$ il numero K che in base $b'' = \text{DODICI}$, tramite le dodici cifre (ordinate!) dell'insieme $\{0, 1, 2, 3, \dots, 8, 9, \perp, \wedge\}$, è espresso dalla scrittura posizionale $K := (3\perp 7)_{b''}$.

[3] Sia $q \in \mathbb{Q}$. Determinare — se esistono — tutte le successioni $\underline{a}^{(q)} := \{a_n^{(q)}\}_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ (dipendenti dal parametro q), tali che

$$a_0^{(q)} = q + 3 \quad , \quad a_1^{(q)} = 3q + 5 \quad , \quad a_n^{(q)} = 5a_{n-1}^{(q)} - 6a_{n-2}^{(q)} \quad \forall n \geq 2 \quad .$$

[4] Determinare l'insieme di tutte le soluzioni del sistema di equazioni congruenziali

$$\circledast : \begin{cases} 146x \equiv -78 & (\text{mod } 10) \\ -59x \equiv 130 & (\text{mod } 7) \end{cases}$$

[5] Dati i due numeri interi $a := 30$ e $b := 78$, calcolare $\delta := \text{M.C.D.}(a, b)$, calcolare $\mu := \text{m.c.m.}(a, b)$, e determinare una identità di Bézout per $\text{M.C.D.}(a, b)$.

[6] Si consideri il polinomio booleano $S(x, y, z)$, nelle variabili x, y e z , dato da

$$S(x, y, z) := (y' \vee 0 \vee x \vee z')' \vee (z' \wedge y \wedge 1 \wedge z) \vee \\ \vee \left(\left((y'' \vee z' \vee y) \wedge (z' \wedge 1 \wedge x)' \right) \vee y'' \right)' \vee \left(1 \wedge \left(z' \vee (x \wedge 0' \wedge y')' \right) \right)'$$

(a) Determinare la *forma normale disgiuntiva* di $S(x, y, z)$.

(b) Determinare la *somma di tutti gli implicant primari* di $S(x, y, z)$.

(c) Determinare una *forma minimale* di $S(x, y, z)$.

— ★ —

SOLUZIONI

[1] — (a) Un insieme ordinato $(E; \preceq)$ è *totalmente* ordinato se per ogni $e', e'' \in E$ si ha $e' \preceq e''$ oppure $e'' \preceq e'$ (in breve, “ e' ed e'' sono comparabili”). Nel caso in esame $(D_{56}; |)$ non è totalmente ordinato, perché ad esempio si ha che per $2, 7 \in D_{56}$ si verifica che $2 \nmid 7$ (cioè “2 non divide 7”) e $7 \nmid 2$ (cioè “7 non divide 2”). Analogamente, $(\mathcal{P}(\{x, y, z\}); \subseteq)$ non è totalmente ordinato, perché ad esempio si ha che per $\{x\}, \{y\} \in \mathcal{P}(\{x, y, z\})$ si verifica che $\{x\} \not\subseteq \{y\}$ e $\{y\} \not\subseteq \{x\}$.

(b) D_{56} è limitato, con minimo $\min(D_{56}) = 1$ e massimo $\max(D_{56}) = 56$. Analogamente anche $\mathcal{P}(\{x, y, z\})$ è limitato, con minimo $\min(\mathcal{P}(\{x, y, z\})) = \emptyset$ e massimo $\max(\mathcal{P}(\{x, y, z\})) = \{x, y, z\}$.

(c) Un insieme ordinato $(E; \preceq)$ è un reticolo se per ogni $e', e'' \in E$ esiste $\inf(e', e'') \in E$ e $\sup(e', e'') \in E$. Nei casi in esame si ha che entrambi $(D_{56}; |)$ e $(\mathcal{P}(\{x, y, z\}); \subseteq)$ sono reticoli, in cui $\inf(d', d'') = \text{M.C.D.}(d', d'')$ e $\sup(d', d'') = \text{m.c.m.}(d', d'')$ per ogni $d', d'' \in D_{56}$ mentre $\inf(S', S'') = S' \cap S''$ e $\sup(S', S'') = S' \cup S''$ per ogni $S', S'' \in \mathcal{P}(\{x, y, z\})$.

Infine, i due reticoli $(D_{56}; |)$ e $(\mathcal{P}(\{x, y, z\}); \subseteq)$ non sono isomorfi. Una possibile spiegazione è la seguente. Se i due reticoli fossero isomorfi, un qualunque isomorfismo da

D_{56} a $\mathcal{P}(\{x, y, z\})$ darebbe per restrizione una biiezione tra l'insieme degli atomi di D_{56} e l'insieme degli atomi di $\mathcal{P}(\{x, y, z\})$; ma D_{56} ha esattamente *due* atomi — che sono 2 e 7 — mentre $\mathcal{P}(\{x, y, z\})$ ha esattamente *tre* atomi — che sono i tre singoletti $\{x\}$, $\{y\}$ e $\{z\}$: quindi non ci può essere una biiezione tra i due insiemi di atomi (hanno cardinalità diverse...), e dunque i due reticoli considerati non sono isomorfi — sebbene abbiano la stessa cardinalità, precisamente $|D_{56}| = 8 = |\mathcal{P}(\{x, y, z\})|$.

(d) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, i reticoli D_{56} e $\mathcal{P}(\{x, y, z\})$ sono entrambi limitati — vedasi (b) — e distributivi; però D_{56} *non* è complementato (perché, ad esempio, non esiste un complemento per 2) e quindi *non* è un'algebra di Boole, mentre invece $\mathcal{P}(\{x, y, z\})$ è complementato (per ogni $S \in \mathcal{P}(\{x, y, z\})$ come complemento in $\mathcal{P}(\{x, y, z\})$ c'è il suo complementare $\{x, y, z\} \setminus S$) e quindi è un'algebra di Boole.

N.B.: questo è anche un altro modo per provare che i due reticoli D_{56} e $\mathcal{P}(\{x, y, z\})$ *non* sono isomorfi l'uno all'altro: infatti, se lo fossero allora sarebbero *entrambi* algebre di Boole oppure *entrambi* non lo sarebbero, e invece non è così (hanno proprietà opposte).

(e) Ricordiamo che in un insieme ordinato si dicono *atomi* gli elementi (se esistono...) che coprono il minimo. Nei casi in esame, gli atomi di D_{56} sono 2 e 7 — cioè gli unici fattori primi di 56 — mentre gli atomi di $\mathcal{P}(\{x, y, z\})$ sono i tre singoletti $\{x\}$, $\{y\}$ e $\{z\}$.

$$[2] \quad (a) \quad N := (4203)_b = (553)_{b'} ;$$

$$(b) \quad T := (276)_{b'} = (2101)_b ;$$

$$(c) \quad K := (3 \perp 7)_{b''} = (571)_{b'} .$$

[3] — Il polinomio caratteristico associato alle successioni ricorsive cercate è della forma $\Delta(x) = x^2 - 5x + 6$, che ha radici $r_+ = 3$ e $r_- = 2$; pertanto le successioni cercate sono della forma $\underline{a} = \{a_n = C_+ \cdot 3^n + C_- \cdot 2^n\}_{n \in \mathbb{N}}$. Imponendo le condizioni iniziali si trova che dev'essere necessariamente $C_+ = q - 1$, $C_- = 4$: perciò esiste una e una sola successione del tipo richiesto, precisamente

$$\underline{a} = \{a_n = (q - 1) \cdot 3^n + 4 \cdot 2^n\}_{n \in \mathbb{N}}$$

$$[4] \quad x \equiv 22 \equiv -13 \pmod{35}, \text{ o in altri termini } x = 22 + 35z, \forall z \in \mathbb{Z}.$$

[5] — I numeri assegnati si fattorizzano univocamente in primi come segue:

$$a := 30 = 2 \cdot 3 \cdot 5, \quad b := 78 = 2 \cdot 3 \cdot 13$$

Da questo otteniamo

$$\delta := \text{M.C.D.}(a, b) = \text{M.C.D.}(2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 13) = 2 \cdot 3 = 6$$

$$\mu := \text{m.c.m.}(a, b) = \text{m.c.m.}(2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 13) = 2 \cdot 3 \cdot 5 \cdot 13 = 390$$

Notiamo anche che basta ottenere uno dei due per poi ricavare l'altro tramite la relazione

$$\text{M.C.D.}(a, b) \cdot \text{m.c.m.}(a, b) = a \cdot b \tag{1}$$

Inoltre il M.C.D. (a, b) si può ottenere anche tramite l'algoritmo euclideo delle divisioni successive, che dà quanto segue:

$$\begin{aligned} 30 &= 78 \cdot 0 + 30 \\ 78 &= 30 \cdot 2 + 18 \\ 30 &= 18 \cdot 1 + 12 \\ 18 &= 12 \cdot 1 + \underline{6} \\ 12 &= 6 \cdot 2 + 0 \end{aligned} \tag{2}$$

L'ultimo resto non nullo è il M.C.D. cercato, dunque $\text{M.C.D.}(30, 78) = 6$. Inoltre, una volta che si sia calcolato in tal modo il M.C.D. $(30, 78)$ si può poi ottenere il m.c.m. $(30, 78)$ tramite la formula in (1), per cui si trova

$$\text{m.c.m.}(30, 78) = \frac{30 \cdot 78}{\text{M.C.D.}(30, 78)} = \frac{2340}{6} = 390$$

Infine, dobbiamo trovare una identità di Bézout per $\text{M.C.D.}(30, 78)$, cioè un'espressione della forma $\text{M.C.D.}(30, 78) = 30 \cdot r + 78 \cdot s$ per opportuni valori di $r, s \in \mathbb{Z}$. Una tale espressione si può ottenere invertendo le identità in (2): precisamente, così facendo si trova

$$\begin{aligned} 30 + 78 \cdot (-0) &= 30 \\ 78 + 30 \cdot (-2) &= 18 \\ 30 + 18 \cdot (-1) &= 12 \\ 18 + 12 \cdot (-1) &= \underline{6} \end{aligned}$$

da cui otteniamo

$$\begin{aligned} \text{M.C.D.}(30, 78) &= 6 = 18 + 12 \cdot (-1) = 18 + (30 + 18 \cdot (-1)) \cdot (-1) = \\ &= 30 \cdot (-1) + 18 \cdot 2 = 30 \cdot (-1) + (78 + 30 \cdot (-2)) \cdot 2 = 78 \cdot 2 + 30 \cdot (-5) = \\ &= 78 \cdot 2 + (30 + 78 \cdot (-0)) \cdot (-5) = 30 \cdot (-5) + 78 \cdot 2 \end{aligned}$$

quindi una possibile identità di Bézout è

$$6 = 30 \cdot (-5) + 78 \cdot 2$$

in cui $r = -5$ e $s = 2$.

- [6] — (a) $F.N.D. = (x \wedge y' \wedge z') \vee (x \wedge y' \wedge z) \vee (x' \wedge y \wedge z) \vee (x' \wedge y' \wedge z)$
 (c) $s.t.i.p. = (x \wedge y') \vee (x' \wedge z) \vee (y' \wedge z)$
 (d) $f.m. = (x \wedge y') \vee (x' \wedge z)$, e questa è l'unica forma minimale possibile.