

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 P

.....

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

..... P

[1] Sia D_{135} l'insieme dei numeri naturali divisori di 135, dotato della relazione d'ordine di *divisibilità*, e sia $\mathcal{P}(\{a, b, c\})$ l'insieme delle parti dell'insieme $\{a, b, c\}$, dotato della relazione d'ordine di *inclusione*; in particolare, entrambi sono insiemi ordinati.

(a) D_{135} è totalmente ordinato? $\mathcal{P}(\{a, b, c\})$ è totalmente ordinato?

(b) D_{135} è limitato? $\mathcal{P}(\{a, b, c\})$ è limitato? In entrambi i casi, se la risposta è negativa se ne spieghi il perché, se è affermativa si precisino i limiti.

(c) D_{135} è un *reticolo*? $\mathcal{P}(\{a, b, c\})$ è un *reticolo*? Se sono entrambi reticoli, sono isomorfi l'uno all'altro?

(d) D_{135} è un'algebra di Boole? $\mathcal{P}(\{a, b, c\})$ è un'algebra di Boole?

(e) Quali sono — se esistono — gli *atomi* di D_{135} e gli *atomi* di $\mathcal{P}(\{a, b, c\})$?

[2] (a) Scrivere in base $b' := \text{DIECI}$ il numero N che in base $b := \text{CINQUE}$ è espresso dalla scrittura posizionale $N := (3124)_b$.

(b) Scrivere in base $b := \text{CINQUE}$ il numero T che in base $b' := \text{DIECI}$ è espresso dalla scrittura posizionale $T := (495)_{b'}$.

(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 $K := (2\perp 9)_{b''}$.

[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

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

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

$$⊗ : \begin{cases} -61x \equiv 125 \pmod{7} \\ 136x \equiv -82 \pmod{10} \end{cases}$$

[5] Dati i due numeri interi $a := 32$ e $b := 56$, 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 $P(a, b, c)$, nelle variabili a, b e c , dato da

$$P(a, b, c) := (c' \vee 0 \vee a' \vee b')' \vee (c' \wedge 1 \wedge a \wedge c) \vee \\ \vee \left(\left((a'' \vee c' \vee a) \wedge (c' \wedge 1 \wedge b')' \right) \vee a'' \right)' \vee \left(0' \wedge \left((b' \wedge 1 \wedge a')' \vee c' \right) \right)'$$

(a) Determinare la *forma normale disgiuntiva* di $P(a, b, c)$.

(b) Determinare la *somma di tutti gli implicant primari* di $P(a, b, c)$.

(c) Determinare una *forma minimale* di $P(a, b, c)$.

— ★ —

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 $(D_{135}; |)$ non è totalmente ordinato, perché ad esempio si ha che per $3, 5 \in D_{135}$ si verifica che $3 \nmid 5$ (cioè “3 non divide 5”) e $5 \nmid 3$ (cioè “5 non divide 3”). Analogamente, $(\mathcal{P}(\{a, b, c\}); \subseteq)$ non è totalmente ordinato, perché ad esempio si ha che per $\{a\}, \{b\} \in \mathcal{P}(\{a, b, c\})$ si verifica che $\{a\} \not\subseteq \{b\}$ e $\{b\} \not\subseteq \{a\}$.

(b) D_{135} è limitato, con minimo $\min(D_{135}) = 1$ e massimo $\max(D_{135}) = 135$. Analogamente anche $\mathcal{P}(\{a, b, c\})$ è limitato, con minimo $\min(\mathcal{P}(\{a, b, c\})) = \emptyset$ e massimo $\max(\mathcal{P}(\{a, b, c\})) = \{a, b, c\}$.

(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 $(D_{135}; |)$ e $(\mathcal{P}(\{a, b, c\}); \subseteq)$ 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 $d', d'' \in D_{135}$ mentre $\inf(S', S'') = S' \cap S''$ e $\sup(S', S'') = S' \cup S''$ per ogni $S', S'' \in \mathcal{P}(\{a, b, c\})$.

Infine, i due reticoli $(D_{135}; |)$ e $(\mathcal{P}(\{a, b, c\}); \subseteq)$ non sono isomorfi. Una possibile spiegazione è la seguente. Se i due reticoli fossero isomorfi, un qualunque isomorfismo da

D_{135} a $\mathcal{P}(\{a, b, c\})$ darebbe per restrizione una biiezione tra l'insieme degli atomi di D_{135} e l'insieme degli atomi di $\mathcal{P}(\{a, b, c\})$; ma D_{135} ha esattamente *due* atomi — che sono 3 e 5 — mentre $\mathcal{P}(\{a, b, c\})$ ha esattamente *tre* atomi — che sono i tre singoletti $\{a\}$, $\{b\}$ e $\{c\}$: 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 $|D_{135}| = 8 = |\mathcal{P}(\{a, b, c\})|$.

(d) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, i reticoli D_{135} e $\mathcal{P}(\{a, b, c\})$ sono entrambi limitati — vedasi (b) — e distributivi; però D_{135} *non* è complementato (perché, ad esempio, non esiste un complemento per 3) e quindi *non* è un'algebra di Boole, mentre invece $\mathcal{P}(\{a, b, c\})$ è complementato (per ogni $S \in \mathcal{P}(\{a, b, c\})$ come complemento in $\mathcal{P}(\{a, b, c\})$ c'è il suo complementare $\{a, b, c\} \setminus S$) e quindi è un'algebra di Boole.

N.B.: questo è anche un altro modo per provare che i due reticoli D_{135} e $\mathcal{P}(\{a, b, c\})$ *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_{135} sono 3 e 5 — cioè gli unici fattori primi di 135 — mentre gli atomi di $\mathcal{P}(\{a, b, c\})$ sono i tre singoletti $\{a\}$, $\{b\}$ e $\{c\}$.

$$[2] \quad (a) \quad N := (3124)_b = (414)_{b'} ;$$

$$(b) \quad T := (495)_{b'} = (3440)_b ;$$

$$(c) \quad K := (2 \perp 9)_{b''} = (417)_{b'} .$$

[3] — Il polinomio caratteristico associato alle successioni ricorsive cercate è della forma $\Delta(x) = x^2 - x - 6$, 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 $C_+ = 1$, $C_- = q + 1$: perciò esiste una e una sola successione del tipo richiesto, precisamente

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

$$[4] \quad x \equiv 3 \pmod{35}, \text{ o in altri termini } x = 3 + 35z, \forall z \in \mathbb{Z}.$$

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

$$a := 32 = 2^5, \quad b := 56 = 2^3 \cdot 7$$

Da questo otteniamo

$$\begin{aligned} \delta &:= \text{M.C.D.}(a, b) = \text{M.C.D.}(2^5, 2^3 \cdot 7) = 2^3 = 8 \\ \mu &:= \text{m.c.m.}(a, b) = \text{m.c.m.}(2^5, 2^3 \cdot 7) = 2^5 \cdot 7 = 224 \end{aligned}$$

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:

$$\begin{aligned} 32 &= 56 \cdot 0 + 32 \\ 56 &= 32 \cdot 1 + 24 \\ 32 &= 24 \cdot 1 + \underline{8} \\ 24 &= 8 \cdot 3 + 0 \end{aligned} \tag{2}$$

L'ultimo resto non nullo è il M.C.D. cercato, dunque $\text{M.C.D.}(32, 56) = 8$. Inoltre, una volta che si sia calcolato in tal modo il M.C.D.(32,56) si può poi ottenere il m.c.m(32,56) tramite la formula in (1), per cui si trova

$$\text{m.c.m}(32, 56) = \frac{32 \cdot 56}{\text{M.C.D}(32, 56)} = \frac{1792}{8} = 224$$

Infine, dobbiamo trovare una identità di Bézout per $\text{M.C.D.}(32, 56)$, cioè un'espressione della forma $\text{M.C.D.}(32, 56) = 32 \cdot r + 56 \cdot s$ 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

$$\begin{aligned} 32 + 56 \cdot (-0) &= 32 \\ 56 + 32 \cdot (-1) &= 24 \\ 32 + 24 \cdot (-1) &= \underline{8} \end{aligned}$$

da cui otteniamo

$$\begin{aligned} \text{M.C.D.}(32, 56) &= 8 = 32 + 24 \cdot (-1) = 32 + (56 + 32 \cdot (-1)) \cdot (-1) = \\ &= 56 \cdot (-1) + 32 \cdot 2 = 56 \cdot (-1) + (32 + 56 \cdot (-0)) \cdot 2 = 32 \cdot 2 + 56 \cdot (-1) \end{aligned}$$

quindi una possibile identità di Bézout è

$$8 = 32 \cdot 2 + 56 \cdot (-1)$$

in cui $r = 2$ e $s = -1$.

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