

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 R

.....

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

..... \mathbb{R}

[1] Sia D_{189} l'insieme dei numeri naturali divisori di 189, dotato della relazione d'ordine di *divisibilità*, e sia $\mathcal{P}(\{h, k, \ell\})$ l'insieme delle parti dell'insieme $\{h, k, \ell\}$, dotato della relazione d'ordine di *inclusione*; in particolare, entrambi sono insiemi ordinati.

(a) D_{189} è totalmente ordinato? $\mathcal{P}(\{h, k, \ell\})$ è totalmente ordinato?

(b) D_{189} è limitato? $\mathcal{P}(\{h, k, \ell\})$ 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_{189} è un *reticolo*? $\mathcal{P}(\{h, k, \ell\})$ è un *reticolo*? Se sono entrambi reticoli, sono isomorfi l'uno all'altro?

(d) D_{189} è un'algebra di Boole? $\mathcal{P}(\{h, k, \ell\})$ è un'algebra di Boole?

(e) Quali sono — se esistono — gli *atomi* di D_{189} e gli *atomi* di $\mathcal{P}(\{h, k, \ell\})$?

[2] (a) Scrivere in base $b' := \text{DIECI}$ il numero N che in base $b := \text{CINQUE}$ è espresso dalla scrittura posizionale $N := (2413)_b$.

(b) Scrivere in base $b := \text{CINQUE}$ il numero T che in base $b' := \text{DIECI}$ è espresso dalla scrittura posizionale $T := (479)_{b'}$.

(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 $K := (4\perp 5)_{b''}$.

[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

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

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

$$\circledast : \begin{cases} -66x \equiv 128 & (\text{mod } 7) \\ 128x \equiv -86 & (\text{mod } 10) \end{cases}$$

[5] Dati i due numeri interi $a := 27$ e $b := 72$, 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 $R(h, k, \ell)$, nelle variabili h, k e ℓ , dato da

$$\begin{aligned} R(h, k, \ell) := & \left(0' \wedge \left(\ell' \vee (h' \wedge 1 \wedge k)' \right) \right)' \vee (h \wedge 1 \wedge \ell \wedge k') \vee \\ & \vee \left(h'' \vee \left((\ell' \wedge 1 \wedge k)' \wedge (h'' \vee \ell' \vee h) \right) \right)' \vee (k \vee h' \vee 0 \vee \ell')' \end{aligned}$$

(a) Determinare la *forma normale disgiuntiva* di $R(h, k, \ell)$.

(b) Determinare la *somma di tutti gli implicant primari* di $R(h, k, \ell)$.

(c) Determinare una *forma minimale* di $R(h, k, \ell)$.

— ★ —

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 $(D_{189}; |)$ non è totalmente ordinato, perché ad esempio si ha che per $3, 7 \in D_{189}$ si verifica che $3 \nmid 7$ (cioè “3 non divide 7”) e $7 \nmid 3$ (cioè “7 non divide 3”). Analogamente, $(\mathcal{P}(\{h, k, \ell\}); \subseteq)$ non è totalmente ordinato, perché ad esempio si ha che per $\{h\}, \{k\} \in \mathcal{P}(\{h, k, \ell\})$ si verifica che $\{h\} \not\subseteq \{k\}$ e $\{k\} \not\subseteq \{h\}$.

(b) D_{189} è limitato, con minimo $\min(D_{189}) = 1$ e massimo $\max(D_{189}) = 189$. Analogamente anche $\mathcal{P}(\{h, k, \ell\})$ è limitato, con minimo $\min(\mathcal{P}(\{h, k, \ell\})) = \emptyset$ e massimo $\max(\mathcal{P}(\{h, k, \ell\})) = \{h, k, \ell\}$.

(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 $(D_{189}; |)$ e $(\mathcal{P}(\{h, k, \ell\}); \subseteq)$ 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 $d', d'' \in D_{189}$ mentre $\inf(S', S'') = S' \cap S''$ e $\sup(S', S'') = S' \cup S''$ per ogni $S', S'' \in \mathcal{P}(\{h, k, \ell\})$.

Infine, i due reticoli $(D_{189}; |)$ e $(\mathcal{P}(\{h, k, \ell\}); \subseteq)$ non sono isomorfi. Una possibile spiegazione è la seguente. Se i due reticoli fossero isomorfi, un qualunque isomorfismo da

D_{189} a $\mathcal{P}(\{h, k, \ell\})$ darebbe per restrizione una biiezione tra l'insieme degli atomi di D_{189} e l'insieme degli atomi di $\mathcal{P}(\{h, k, \ell\})$; ma D_{189} ha esattamente *due* atomi — che sono 3 e 7 — mentre $\mathcal{P}(\{h, k, \ell\})$ ha esattamente *tre* atomi — che sono i tre singoletti $\{h\}$, $\{k\}$ e $\{\ell\}$: 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 $|D_{189}| = 8 = |\mathcal{P}(\{h, k, \ell\})|$.

(d) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, i reticoli D_{189} e $\mathcal{P}(\{h, k, \ell\})$ sono entrambi limitati — vedasi (b) — e distributivi; però D_{189} *non* è complementato (perché, ad esempio, non esiste un complemento per 3) e quindi *non* è un'algebra di Boole, mentre invece $\mathcal{P}(\{h, k, \ell\})$ è complementato (per ogni $S \in \mathcal{P}(\{h, k, \ell\})$ come complemento in $\mathcal{P}(\{h, k, \ell\})$ c'è il suo complementare $\{h, k, \ell\} \setminus S$) e quindi è un'algebra di Boole.

N.B.: questo è anche un altro modo per provare che i due reticoli D_{189} e $\mathcal{P}(\{h, k, \ell\})$ *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_{189} sono 3 e 7 — cioè gli unici fattori primi di 189 — mentre gli atomi di $\mathcal{P}(\{h, k, \ell\})$ sono i tre singoletti $\{h\}$, $\{k\}$ e $\{\ell\}$.

$$[2] \quad (a) \quad N := (2413)_b = (358)_{b'} ;$$

$$(b) \quad T := (479)_{b'} = (3404)_b ;$$

$$(c) \quad K := (4 \perp 5)_{b''} = (701)_{b'} .$$

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

$$\underline{a} = \{a_n = 2(q+1) \cdot 1^n + (-1) \cdot 5^n\}_{n \in \mathbb{N}}$$

$$[4] \quad x \equiv 18 \equiv -17 \pmod{35}, \text{ o in altri termini } x = 18 + 35z, \forall z \in \mathbb{Z}.$$

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

$$a := 27 = 3^3, \quad b := 72 = 2^3 \cdot 3^2$$

Da questo otteniamo

$$\begin{aligned} \delta &:= \text{M.C.D.}(a, b) = \text{M.C.D.}(3^3, 2^3 \cdot 3^2) = 3^2 = 9 \\ \mu &:= \text{m.c.m.}(a, b) = \text{m.c.m.}(3^3, 2^3 \cdot 3^2) = 2^3 \cdot 3^3 = 216 \end{aligned}$$

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:

$$\begin{aligned} 27 &= 72 \cdot 0 + 27 \\ 72 &= 27 \cdot 2 + 18 \\ 27 &= 18 \cdot 1 + \underline{9} \\ 18 &= 9 \cdot 2 + 0 \end{aligned} \tag{2}$$

L'ultimo resto non nullo è il M.C.D. cercato, dunque $\text{M.C.D.}(27, 72) = 9$. Inoltre, una volta che si sia calcolato in tal modo il M.C.D.(32,56) si può poi ottenere il m.c.m(27,72) tramite la formula in (1), per cui si trova

$$\text{m.c.m}(27, 72) = \frac{27 \cdot 72}{\text{M.C.D.}(27, 72)} = \frac{1944}{9} = 216$$

Infine, dobbiamo trovare una identità di Bézout per $\text{M.C.D.}(27, 72)$, cioè un'espressione della forma $\text{M.C.D.}(27, 72) = 27 \cdot r + 72 \cdot s$ 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

$$\begin{aligned} 27 + 72 \cdot (-0) &= 27 \\ 72 + 27 \cdot (-2) &= 18 \\ 27 + 18 \cdot (-1) &= \underline{9} \end{aligned}$$

da cui otteniamo

$$\begin{aligned} \text{M.C.D.}(27, 72) &= 9 = 27 + 18 \cdot (-1) = 27 + (72 + 27 \cdot (-2)) \cdot (-1) = \\ &= 72 \cdot (-1) + 27 \cdot 3 = 72 \cdot (-1) + (27 + 72 \cdot (-0)) \cdot 3 = 27 \cdot 3 + 72 \cdot (-1) \end{aligned}$$

quindi una possibile identità di Bézout è

$$9 = 27 \cdot 3 + 72 \cdot (-1)$$

in cui $r = 3$ e $s = -1$.

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