ALGEBRA e LOGICA

CdL in Ingegneria Informatica

prof. Fabio GAVARINI

a.a. 2016–2017 — Sessione Autunnale, I appello

Esame scritto del 5 Settembre 2017 — *Testo e Soluzioni*

. . . .

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

. . . . ∗ . . . .

[1] Si consideri il polinomio booleano (nelle quattro variabili a, c, e, s) dato da

$$P(a,c,e,s) \; := \; \Big(\big(e'' \vee 0 \vee s\,\big) \wedge \big(\,c \wedge a\,\big)\Big) \vee \big(\big(\,s \vee c\,\big)' \wedge a\,\big)'' \vee \\ \vee \Big(\big(\,e' \vee s\,\big)' \wedge \big(\,c \vee 1' \vee c''\,\big)\Big)$$

(a) Determinare la *forma normale disgiuntiva* di P.

(b) Determinare la *somma di tutti gli implicanti primi* di P.

(c) Determinare una *forma minimale* di P.

[2] *(a)* Determinare se esistano le classi inverse $\overline{9}^{\,-1}$, $\overline{5}^{\,-1}$, $\overline{7}^{\,-1}$, $\big(\overline{9}\cdot\overline{7}\big)^{-1}$ e $\big(\overline{5}\cdot\overline{7}\big)^{-1}$ nell'anello $\mathbb{Z}_{20}$ degli interi modulo 20. In caso negativo, si spieghi perché tale classe inversa non esista; in caso affermativo, si calcoli esplicitamente la suddetta classe inversa.

(b) Calcolare tutte le soluzioni dell'equazione modulare $\overline{647}\,\overline{x} = \overline{-516}$ nell'anello $\mathbb{Z}_{20}$ delle classi resto modulo 20;

(c) Calcolare tutte le soluzioni dell'equazione congruenziale $436\,x \equiv 92 \pmod{20}$ nell'anello $\mathbb{Z}$ dei numeri interi.

[3] *(a)* Scrivere in base $b' :=$ DUE il numero L che in base $b :=$ OTTO è espresso dalla scrittura posizionale $L := \big(5034\big)_b$.

(b) Scrivere in base $b'' :=$ QUATTRO il numero M che in base $b' :=$ DUE è espresso dalla scrittura posizionale $M := \big(110001101\big)_{b'}$.

(c) Utilizzando la notazione posizionale in base $\beta :=$ CINQUE, calcolare la somma $A + B$ dove A e B sono i due numeri naturali espressi in base β da

$$A := \big(31042\big)_\beta \qquad \text{e} \qquad B := \big(24304\big)_\beta$$

esprimendo a sua volta la suddetta somma con la scrittura posizionale in base $\beta :=$ CINQUE.

(continua...)

[**4**] Dimostrare che per ogni $n \in \mathbb{N}$ con $n \geq 2$ si ha $\sum_{s=2}^{n} \dfrac{1}{s\,(s-1)} = \dfrac{n-1}{n}$.

[**5**] Si considerino gli insiemi delle parti $\mathcal{P}\big(\{\heartsuit, \spadesuit, \clubsuit\}\big)$ e $\mathcal{P}\big(\{\spadesuit, \clubsuit, \diamondsuit\}\big)$ rispettivamente dell'insieme $\{\heartsuit, \spadesuit, \clubsuit\}$ e dell'insieme $\{\spadesuit, \clubsuit, \diamondsuit\}$. Si considerino poi la funzione

$$f : \mathcal{P}\big(\{\heartsuit, \spadesuit, \clubsuit\}\big) \longrightarrow \mathcal{P}\big(\{\spadesuit, \clubsuit, \diamondsuit\}\big) \quad , \qquad X \mapsto f(X) := X \cap \{\spadesuit, \clubsuit, \diamondsuit\}$$

— per ogni $X \in \mathcal{P}\big(\{\heartsuit, \spadesuit, \clubsuit\}\big)$ — e la relazione ρ_f in $\mathcal{P}\big(\{\heartsuit, \spadesuit, \clubsuit\}\big)$ definita da

$$X' \rho_f X'' \iff f(X') = f(X'') \qquad \forall \; X', X'' \in \mathcal{P}\big(\{\heartsuit, \spadesuit, \clubsuit\}\big)$$

(a) Verificare se la funzione f è *iniettiva* oppure no.

(b) Verificare se la funzione f è *suriettiva* oppure no.

(c) Dimostrare che la relazione ρ_f *è di equivalenza.*

(d) Dimostrare che la relazione ρ_f *non è d'ordine.*

(e) Descrivere esplicitamente tutte le classi di ρ_f–equivalenza.

— ⋆ —

SOLUZIONI

[**1**] — *(a)* *F.N.D.* $= \big(a \wedge c \wedge e \wedge s\big) \vee \big(a \wedge c \wedge e \wedge s'\big) \vee \big(a \wedge c \wedge e' \wedge s\big) \vee$
$\vee \big(a \wedge c' \wedge e \wedge s'\big) \vee \big(a \wedge c' \wedge e' \wedge s'\big) \vee \big(a' \wedge c \wedge e \wedge s'\big)$

(b) *s.t.i.p.* $= \big(a \wedge c \wedge e\big) \vee \big(a \wedge e \wedge s'\big) \vee \big(a \wedge c \wedge s\big) \vee \big(c \wedge e \wedge s'\big) \vee \big(a \wedge c' \wedge s'\big)$

(c) *f.m.* $= \big(a \wedge c \wedge s\big) \vee \big(a \wedge c' \wedge s'\big) \vee \big(c \wedge e \wedge s'\big)$, e questa in effetti è *l'unica* forma minimale possibile.

[**2**] — *(a)* *Esistono* le classi inverse $\overline{9}^{\,-1}$, $\overline{7}^{\,-1}$ e $\big(\overline{9} \cdot \overline{7}\big)^{-1}$, perché abbiamo M.C.D.$(9,20) = 1$, M.C.D.$(7,20) = 1$ e (in conseguenza) anche M.C.D.$(9 \cdot 7, 20) = 1$: esplicitamente, tali classi inverse sono

$$\overline{9}^{\,-1} = \overline{9} \quad , \qquad \overline{7}^{\,-1} = \overline{3} \quad , \qquad \big(\overline{9} \cdot \overline{7}\big)^{-1} = \overline{7}^{\,-1} \cdot \overline{9}^{\,-1} = \overline{3} \cdot \overline{9} = \overline{27} = \overline{7}$$

Invece *non esistono* le classi inverse $\overline{5}^{\,-1}$ e $\big(\overline{5} \cdot \overline{7}\big)^{-1}$, perché M.C.D.$(5,20) = 5 \neq 1$ e M.C.D.$(5 \cdot 7, 20) = 5 \neq 1$.

(b) Osserviamo che, siccome $\overline{647} = \overline{20 \cdot 32 + 7} = \overline{7}$ e $\overline{-516} = \overline{-26 \cdot 20 + 4} = \overline{4}$, l'equazione modulare $\overline{647}\,\overline{x} = \overline{-516}$ in $\mathbb{Z}_{20}$ si può riscrivere nella forma $\overline{7}\,\overline{x} = \overline{4}$. A questo punto, poiché esiste $\overline{7}^{\,-1} = \overline{3} \in \mathbb{Z}_{20}$, l'equazione $\overline{647}\,\overline{x} = \overline{-516}$ ha esattamente una e una sola soluzione, data da $\overline{x} = \overline{7}^{\,-1} \cdot \overline{4} = \overline{3} \cdot \overline{4} = \overline{12}$.

(c) Osserviamo che, siccome $436 \equiv 440 - 4 \equiv 20 \cdot 22 - 4 \equiv -4 \pmod{7}$ e $92 \equiv 5 \cdot 20 - 8 \equiv -8 \pmod{20}$, l'equazione congruenziale di partenza, cioè a dire $436\,x \equiv 92 \pmod{20}$, è equivalente all'analoga equazione $-4\,x \equiv -8 \pmod{20}$.

Da questo, osservando che $\text{M.C.D.}(-4,-8) = 4 \;\Big|\; 4 \cdot 5 = 20$, possiamo dedurre che l'equazione ammette soluzioni, e — in aggiunta — essa è equivalente all'equazione $(-1)\,x \equiv -2 \pmod{5}$ ottenuta dalla precedente dividendo tutto — coefficiente, termine noto e modulo — per $\text{M.C.D.}(-4,-8) = 4$. Quest'ultima equazione congruenziale ovviamente ha una soluzione data da $x = 2$, e allora l'insieme di *tutte* le sue soluzioni — che è anche l'insieme di tutte le soluzioni dell'equazione congruenziale di partenza — è dato da $\big\{\, x = 2 + 5\,z \;\big|\; z \in \mathbb{Z} \,\big\}$.

[3] — *(a)* $L := (5034)_{b\,=\,\text{OTTO}} = (101000011100)_{b'\,=\,\text{DUE}}$.

(b) $M := (110001101)_{b'\,=\,\text{DUE}} = (12031)_{b''\,=\,\text{QUATTRO}}$.

(c) $A + B = (31042)_{\beta\,=\,\text{CINQUE}} + (24304)_{\beta\,=\,\text{CINQUE}} = (110401)_{\beta\,=\,\text{CINQUE}}$.

N.B.: incidentalmente (ma *non è richiesto* per l'esercizio), per $d :=$ DIECI si ha

$$L := (5034)_b = (2588)_d \quad , \qquad M := (110001101)_{b'} = (397)_d$$
$$A := (31042)_\beta = (2022)_d \;\; , \;\; B := (24304)_\beta = (1829)_d \;\; , \;\; A + B = (3851)_d$$

[4] — *(non c'è da dare una soluzione, bisogna dimostrarlo e basta...)*

[5] — *(a)* La funzione f *non è iniettiva*, perché abbiamo — ad esempio — $\{\heartsuit,\clubsuit\} \neq \{\clubsuit\}$ ma $f\big(\{\heartsuit,\clubsuit\}\big) = \{\clubsuit\} = f\big(\{\clubsuit\}\big)$.

(b) La funzione f *non è suriettiva*, perché abbiamo — ad esempio — che per $\{\spadesuit,\diamondsuit\} \in \mathcal{P}\big(\{\spadesuit\,,\clubsuit\,,\diamondsuit\}\big)$ si ha $\{\spadesuit,\diamondsuit\} \not\in Im(f)$.

(c) *(qui non c'è da dare una soluzione, bisogna dimostrarlo e basta...)*

(d) La relazione ρ_f non è d'ordine perché *non è antisimmetrica*: infatti abbiamo — ad esempio — che $\{\heartsuit,\clubsuit\}\;\rho_f\;\{\clubsuit\}$ e anche $\{\heartsuit,\clubsuit\}\;\rho_f\;\{\clubsuit\}$ — perché $f\big(\{\heartsuit,\clubsuit\}\big) = f\big(\{\clubsuit\}\big)$ e quindi anche $f\big(\{\clubsuit\}\big) = f\big(\{\heartsuit,\clubsuit\}\big)$ — ma $\{\heartsuit,\clubsuit\} \neq \{\clubsuit\}$.

(e) Le classi di ρ_f – equivalenza sono tutti e soli i sottoinsiemi di $\mathcal{P}\big(\{\heartsuit,\spadesuit\,,\clubsuit\}\big)$ dati da

$$C_1 := \big\{\,\emptyset\,,\{\heartsuit\}\big\} \qquad , \qquad C_2 := \big\{\{\spadesuit\}\,,\{\heartsuit,\spadesuit\}\big\}$$
$$C_3 := \big\{\{\clubsuit\}\,,\{\heartsuit,\clubsuit\}\big\} \qquad , \qquad C_3 := \big\{\{\spadesuit\,,\clubsuit\}\,,\{\heartsuit,\spadesuit\,,\clubsuit\}\big\}$$