

**ALGEBRA e LOGICA**  
**CdL in Ingegneria Informatica**  
*prof. Fabio GAVARINI*

*a.a. 2020–2021 — Sessione Estiva, I appello*

Esame scritto del 16 Giugno 2021

*Testo & Svolgimento*

.....  $\otimes$  .....

[1] Nell'insieme  $\mathbb{Z}$  dei numeri interi si consideri la relazione  $\omega$  definita da

$$a \omega b \iff a^2 \equiv b^2 \pmod{11} \quad \forall \quad a, b \in \mathbb{Z}$$

- (a) Dimostrare che  $\omega$  è una equivalenza.
- (b) Determinare il numero di  $\omega$ -classi di equivalenza distinte in  $\mathbb{Z}$ .
- (c) Descrivere esplicitamente l'insieme quoziente  $\mathbb{Z}/\omega$ .
- (d) Descrivere esplicitamente tutte le  $\omega$ -classi di equivalenza in  $\mathbb{Z}$ .

[2] Determinare tutte le soluzioni in  $\mathbb{Z}$  dell'equazione congruenziale

$$99^{36056} x \equiv -51^{5473} \pmod{19}$$

[3] Dimostrare che per ogni  $n \in \mathbb{N}$  si ha  $\sum_{s=0}^{2n} \frac{s(s+1)}{8} = \sum_{c=0}^n c^2$ .

[4] Si consideri il polinomio booleano — nelle tre variabili  $x, y$  e  $z$  — dato da

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

- (a) Determinare la *forma normale disgiuntiva* di  $P$ .
- (b) Determinare, giustificando opportunamente la risposta, se la suddetta forma normale disgiuntiva sia (anche) una *forma minimale* di  $P$  oppure no.

(continua...)

[5] Dato l'insieme  $\{S, P, Q, R\}$ , si consideri il corrispondente insieme delle parti  $\mathcal{P}(\{S, P, Q, R\})$ , dotato della relazione (d'ordine) di inclusione.

Si consideri poi in  $\mathcal{P}(\{S, P, Q, R\})$  il sottoinsieme  $\mathbb{E}$  definito da

$$\begin{aligned}\mathbb{E} &:= \mathcal{P}(\{S, P, Q, R\}) \setminus \{\{Q\}, \{S, R\}, \{P, Q\}, \{P, R\}, \{S, Q, R\}, \{P, Q, R\}\} = \\ &= \{\emptyset, \{S\}, \{P\}, \{R\}, \{S, P\}, \{S, Q\}, \{Q, R\}, \\ &\quad \{S, P, Q\}, \{S, P, R\}, \{S, P, Q, R\}\}\end{aligned}$$

dotato a sua volta della relazione (d'ordine) di inclusione, per la quale è un reticolo.

(a) Disegnare il diagramma di Hasse dell'insieme ordinato  $(\mathbb{E}; \subseteq)$ .

(b) Verificare che  $(\mathbb{E}; \subseteq)$  non è un sottoreticolo di  $(\mathcal{P}(\{S, P, Q, R\}); \subseteq)$ .

(c) Esiste una  $\vee$ -fattorizzazione non ridondante in *fattori*  $\vee$ -irriducibili per l'elemento  $\{S, P, Q, R\}$  nel reticolo  $\mathbb{E}$ ? In caso negativo, si spieghi perché essa non esista; in caso affermativo, si determini esplicitamente una tale  $\vee$ -fattorizzazione, e se possibile se ne determini più di una.

(d) Determinare — giustificando adeguatamente la risposta — se il reticolo  $\mathbb{E}$  sia un'algebra di Boole oppure no.

— ★ —

### SVOLGIMENTO

*N.B.: lo svolgimento qui presentato è molto lungo... Questo non significa che lo sviluppo ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si approfitta per spiegare — in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con molti particolari tutti gli aspetti della teoria toccati più o meno a fondo dal testo in questione.*

[1] — (a) Indicando con  $\mathbb{Z}_{11} := \mathbb{Z} / \equiv_{11}$  l'anello degli interi modulo 11, consideriamo la funzione

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}_{11} \quad , \quad z \mapsto f(z) := \overline{z^2} = \overline{z}^2 \quad \forall z \in \mathbb{Z} \quad (1)$$

Allora, rileggendo la definizione della relazione  $\omega$  in  $\mathbb{Z}$  troviamo che

$$a \omega b \iff f(a) = f(b) \iff a \rho_f b \quad \forall a, b \in \mathbb{Z} \quad (2)$$

dove  $\rho_f$  indica la relazione canonicamente associata alla funzione  $f$ . Siccome sappiamo che una tale  $\rho_f$  è *sempre* una relazione di equivalenza, e la (2) significa proprio che  $\omega = \rho_f$ , possiamo concludere che  $\omega$  è una relazione di equivalenza, q.e.d.

(b)–(c)–(d) Ricordiamo che per una relazione di equivalenza della forma  $\rho_f$  — per una qualsiasi funzione  $f : A \longrightarrow B$  — le classi di equivalenza sono tutti e soli i sottoinsiemi della forma

$$[a]_{\rho_f} := \{ \alpha \in A \mid \alpha \rho_f a \} = \{ \alpha \in A \mid f(\alpha) = f(a) \} = f^{-1}(f(a)) \quad \forall a \in A$$

Applicando questo fatto generale al caso in esame otteniamo

$$[z]_{\eta} := [z]_{\rho_f} = f^{-1}(f(z)) \quad \forall z \in \mathbb{Z}$$

quindi le varie  $\eta$ -classi sono tutti e soli i sottoinsiemi  $f^{-1}(\bar{b})$  al variare del valore  $\bar{b} \in \text{Im}(f) := \{ f(z) \mid z \in \mathbb{Z} \}$ . Ora, il calcolo diretto ci dà

$$\begin{aligned} \bar{0}^2 &= \bar{0} \ , & \bar{1}^2 &= \bar{1} \ , & \bar{2}^2 &= \bar{4} \ , & \bar{3}^2 &= \bar{9} \ , & \bar{4}^2 &= \bar{5} \\ \bar{5}^2 &= \bar{3} \ , & \bar{6}^2 &= \overline{-5}^2 = \bar{5}^2 = \bar{3} \ , & \bar{7}^2 &= \overline{-4}^2 = \bar{4}^2 = \bar{5} \\ \bar{8}^2 &= \overline{-3}^2 = \bar{3}^2 = \bar{9} \ , & \bar{9}^2 &= \overline{-2}^2 = \bar{2}^2 = \bar{4} \ , & \bar{10}^2 &= \overline{-1}^2 = \bar{1}^2 = \bar{1} \end{aligned}$$

— dove i calcoli sono stati ottimizzati ricordando che  $\overline{-a}^2 = (-\bar{a})^2 = \bar{a}^2$  — quindi abbiamo  $\text{Im}(f) = \{ \bar{0}, \bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9} \}$  con

$$\begin{aligned} f(z) = \bar{0} &\iff \bar{z}^2 = \bar{0} \iff \bar{z} = \bar{0} \iff z \in 11\mathbb{Z} = [0]_{\equiv_{11}} \\ f(z) = \bar{1} &\iff \bar{z}^2 = \bar{1} \iff \bar{z} \in \{ \bar{1}, \bar{10} \} \iff z \in [1]_{\equiv_{11}} \cup [10]_{\equiv_{11}} \\ f(z) = \bar{3} &\iff \bar{z}^2 = \bar{3} \iff \bar{z} \in \{ \bar{5}, \bar{6} \} \iff z \in [5]_{\equiv_{11}} \cup [6]_{\equiv_{11}} \\ f(z) = \bar{4} &\iff \bar{z}^2 = \bar{4} \iff \bar{z} \in \{ \bar{2}, \bar{9} \} \iff z \in [2]_{\equiv_{11}} \cup [9]_{\equiv_{11}} \\ f(z) = \bar{5} &\iff \bar{z}^2 = \bar{5} \iff \bar{z} \in \{ \bar{4}, \bar{7} \} \iff z \in [4]_{\equiv_{11}} \cup [7]_{\equiv_{11}} \\ f(z) = \bar{9} &\iff \bar{z}^2 = \bar{9} \iff \bar{z} \in \{ \bar{3}, \bar{8} \} \iff z \in [3]_{\equiv_{11}} \cup [8]_{\equiv_{11}} \end{aligned}$$

da cui otteniamo che

$$\begin{aligned} f^{-1}(\bar{0}) &= [0]_{\equiv_{11}} \ , & f^{-1}(\bar{1}) &= [1]_{\equiv_{11}} \cup [10]_{\equiv_{11}} \ , & f^{-1}(\bar{3}) &= [5]_{\equiv_{11}} \cup [6]_{\equiv_{11}} \\ f^{-1}(\bar{4}) &= [2]_{\equiv_{11}} \cup [9]_{\equiv_{11}} \ , & f^{-1}(\bar{5}) &= [4]_{\equiv_{11}} \cup [7]_{\equiv_{11}} \ , & f^{-1}(\bar{9}) &= [3]_{\equiv_{11}} \cup [8]_{\equiv_{11}} \end{aligned}$$

sono tutte le  $\omega$ -classi di equivalenza (distinte) in  $\mathbb{Z}$ . In particolare, il loro numero è 6 (pari al numero dei valori distinti assunti dalla funzione  $f$ , a cui tali classi corrispondono biunivocamente), e complessivamente esse formano l'insieme quoziente

$$\mathbb{Z}/\eta = \{ f^{-1}(\bar{0}), f^{-1}(\bar{1}), f^{-1}(\bar{3}), f^{-1}(\bar{4}), f^{-1}(\bar{5}), f^{-1}(\bar{9}) \}$$

[2] — Partendo dall'equazione congruenziale assegnata

$$99^{36056} x \equiv -51^{5473} \pmod{19} \quad (3)$$

riduciamo modulo 19 le due basi delle potenze che appaiono in tale equazione: abbiamo

$$99 = 19 \cdot 5 + 4 \equiv_{19} 4, \quad 51 = 19 \cdot 2 + 13 \equiv_{19} 13$$

da cui deduciamo che la (3) è equivalente alla

$$4^{36056} x \equiv -13^{5473} \pmod{19} \quad (4)$$

Adesso, visto che 19 è numero primo e sia 4 che 13 non sono multipli di 19, abbiamo che  $\text{M.C.D.}(4, 19) = 1$  e  $\text{M.C.D.}(13, 19) = 1$ ; allora possiamo applicare il Teorema di Eulero, che ci dà

$$4^{\phi(19)} \equiv_{19} 1 \quad \text{e} \quad 13^{\phi(19)} \equiv_{19} 1 \quad (5)$$

dove  $\phi$  è la funzione di Eulero. Visto che 19 è primo, si ha  $\phi(19) = 19 - 1 = 18$ . Dividendo ora gli esponenti per  $\phi(19) = 18$  otteniamo

$$36056 = 18 \cdot 2003 + 2 \equiv_{18} 2 \quad \text{e} \quad 5473 = 18 \cdot 304 + 1 \equiv_{18} 1 \quad (6)$$

Mettendo insieme (5) e (6) otteniamo

$$\begin{aligned} 4^{36056} &\equiv_{19} (4^{18})^{2003} \cdot 4^2 \equiv_{19} 1^{2003} \cdot 4^2 \equiv_{19} 4^2 \equiv_{19} 16 \equiv_{19} -3 \\ 13^{5473} &\equiv_{19} (13^{18})^{304} \cdot 13^1 \equiv_{19} 1^{304} \cdot 13^1 \equiv_{19} 13^1 \equiv_{19} 13 \end{aligned}$$

e quindi sostituendo nella (4) otteniamo l'equazione equivalente

$$3x \equiv_{19} -13 \equiv 6 \pmod{19}$$

Per quest'ultima, una soluzione particolare ovvia è  $x_0 = 2$ , e siccome il coefficiente della  $x$  (che è 3) è coprimo con il modulo (che è 19), concludiamo che l'insieme di tutte le soluzioni della equazione congruenziale di partenza (4) in definitiva è

$$\mathcal{S} = x_0 + 19\mathbb{Z} = 2 + 19\mathbb{Z} = \{z = 2 + 19k \mid k \in \mathbb{Z}\}$$

[3] — La nostra tesi è che valgono le (infinite) uguaglianze

$$A(n) = B(n) \quad \forall n \in \mathbb{N}_+ \quad (7)$$

dove abbiamo posto

$$A(n) := \sum_{s=0}^{2n} \frac{s(s+1)}{8}, \quad B(n) := \sum_{c=0}^n c^2$$

Procediamo a dimostrare la (7) per induzione, utilizzando l'*induzione debole* (o *semplice*), che si sviluppa in due passi: *Base dell'Induzione* e *Passo Induttivo*.

Base dell'Induzione: La tesi è vera per il più piccolo valore utile di  $n$  (per il quale l'enunciato abbia senso) — quindi, nel caso in esame, per  $n = 0$ .

Dimostrazione: L'uguaglianza da dimostrare è  $A(0) = B(0)$ . Ora, il calcolo diretto ci dà

$$A(0) = \sum_{s=0}^{2 \cdot 0} \frac{s(s+1)}{8} = \frac{0(0+1)}{8} = \frac{0 \cdot 1}{8} + \frac{0}{8} = 0$$

$$B(0) = \sum_{c=0}^0 c^2 = 0^2 = 0$$

quindi in particolare  $A(0) = B(0)$ , q.e.d.

Passo Induttivo (in forma debole): Per ogni valore utile di  $n$ , SE è vero l'enunciato per  $n$  ALLORA è vero anche l'enunciato per  $n+1$ .

Nel caso in esame, tale passo induttivo assume questa forma:

Sia  $n \in \mathbb{N}_+$ . SE (Ipotesi Induttiva)  $A(n) = B(n)$ ,

ALLORA (Tesi Induttiva)  $A(n+1) = B(n+1)$ .

Dimostrazione: Calcoliamo separatamente  $A(n+1)$  e  $B(n+1)$ : otteniamo

$$\begin{aligned} A(n+1) &:= \sum_{s=0}^{2(n+1)} \frac{s(s+1)}{8} = \\ &= \sum_{s=0}^{2n} \frac{s(s+1)}{8} + \frac{(2n+1)((2n+1)+1)}{2} + \frac{(2n+2)((2n+2)+1)}{8} = \\ &= A(n) + \frac{((2n+1)+1)(2n+1)}{2} + \frac{((2n+2)+1)(2n+2)}{2} = \\ &= A(n) + \frac{(2n+1)(2n+2) + (2n+3)(2n+2)}{8} = \\ &= A(n) + \frac{(4n+4)2(n+1)}{8} = A(n) + \frac{(n+1)4 \cdot 2(n+1)}{8} = \\ &= A(n) + (n+1)^2 \end{aligned}$$

dunque in sintesi

$$A(n+1) = A(n) + (n+1)^2 \quad (8)$$

e analogamente troviamo

$$B(n+1) := \sum_{c=0}^{n+1} c^2 := \sum_{c=0}^n c^2 + (n+1)^2 = B(n) + (n+1)^2$$

dunque in breve

$$B(n+1) = B(n) + (n+1)^2 \quad (9)$$

Ora aggiungendo a (8) e (9) l'ipotesi induttiva che  $A(n) = B(n)$  deduciamo infine che  $A(n+1) = B(n+1)$ , q.e.d.

[4] — (a) Partendo dal polinomio booleano assegnato lo riscriviamo in forme (diverse ma) equivalenti, con l'obiettivo di trovarne un'espressione come *somma di prodotti*, dalla quale poi cercheremo di ottenere la *Forma Normale Disgiuntiva* (= *F.N.D.*), che è la somma non ridondante di prodotti (unica, a meno di commutazione dei prodotti tra loro e dei fattori in ciascun prodotto) fondamentali e completi che è equivalente al polinomio assegnato. Dunque procediamo:

$$\begin{aligned}
P(x, y, z) &:= \left( (x' \wedge 0' \wedge z' \wedge x' \wedge y)' \wedge (z' \vee y' \vee z) \right)' \vee \\
&\quad \vee \left( (y' \vee (x' \wedge (z \vee x') \wedge x) \vee x \vee z') \wedge (x \vee z' \vee x \vee 1' \vee x') \right)' \sim \\
&\sim \left( (\underline{x' \wedge 0'} \wedge \underline{z' \wedge x'} \wedge y)' \wedge (z' \vee \underline{y' \vee z}) \right)' \vee \\
&\quad \vee \left( (y' \vee (x' \wedge (z \vee x') \wedge x) \vee x \vee z') \wedge (x \vee z' \vee x \vee \underline{1' \vee x'}) \right)' \sim \\
&\sim \left( (\underline{0'} \wedge \underline{x' \wedge x'} \wedge \underline{z' \wedge y})' \wedge (\underline{z' \vee z} \vee y') \right)' \vee \\
&\quad \vee \left( (\underline{y' \vee x} \vee z') \wedge (x \vee z' \vee \underline{x \vee x'} \vee \underline{1'}) \right)' \sim \\
&\sim \left( (\underline{1 \wedge x'} \wedge y \wedge z')' \wedge (\underline{1 \vee y'}) \right)' \vee \left( (x \vee y' \vee z') \wedge (x \vee z' \vee \underline{1 \vee 0}) \right)' \sim \\
&\sim \left( (x' \wedge y \wedge z')' \underline{\wedge 1} \right)' \vee \left( (x \vee y' \vee z') \underline{\wedge 1} \right)' \sim \\
&\sim \left( (\underline{(x' \wedge y \wedge z')'})' \vee (x \vee y' \vee z') \right)' \sim \\
&\quad \sim (x' \wedge y \wedge z') \vee (x' \wedge \underline{y''} \wedge \underline{z''}) \sim \\
&\quad \sim (x' \wedge y \wedge z') \vee (x' \wedge y \wedge z)
\end{aligned}$$

(dove abbiamo sottolineato i punti delle espressioni in cui al passaggio successivo operiamo qualche trasformazione). In conclusione, abbiamo trovato

$$P(x, y, z) \sim (x' \wedge y \wedge z') \vee (x' \wedge y \wedge z) =: F(x, y, z) \quad (10)$$

dove l'elemento di destra è proprio una *somma di prodotti* fondamentali e completi, che è non ridondante e equivalente al polinomio originale  $P(x, y, z)$ : pertanto, il polinomio booleano  $F(x, y, z)$  in (10) è esattamente la forma normale disgiuntiva di  $P(x, y, z)$ , come richiesto.

Metodo alternativo (tramite le "Tavole di Verità"): In generale, la *F.N.D.* di un polinomio è la somma di tutti e soli i prodotti fondamentali e completi che corrispondono alle stringhe di valori 0 e 1 su cui il polinomio assegnato vale 1.

Ora, nel nostro caso il calcolo esplicito dà, per ogni terna  $(a, b, c) \in \{0, 1\}^{\times 3}$ ,

$$\begin{aligned}
P(a, b, c) &= (P(x, y, z))(a, b, c) = \\
&= \left( (a' \wedge 0' \wedge c' \wedge a' \wedge b)' \wedge (c' \vee b' \vee c) \right)' \vee \\
&\quad \vee \left( (b' \vee (a' \wedge (c \vee a') \wedge a) \vee a \vee c') \wedge (a \vee c' \vee a \vee 1' \vee a') \right)'
\end{aligned}$$

da cui segue che

$$\begin{aligned}
P(a,b,c) = 1 &\iff \left\{ \begin{array}{l} \left( (a' \wedge 0' \wedge c' \wedge a' \wedge b)' \wedge (c' \vee b' \vee c) \right)' = 1 \\ \text{oppure} \\ \left( (b' \vee (a' \wedge (c \vee a') \wedge a) \vee a \vee c') \wedge (a \vee c' \vee a \vee 1' \vee a') \right)' = 1 \end{array} \right. \iff \\
&\iff \left\{ \begin{array}{l} (a' \wedge 0' \wedge c' \wedge a' \wedge b)' \wedge (c' \vee b' \vee c) = 0 \\ \text{oppure} \\ (b' \vee (a' \wedge (c \vee a') \wedge a) \vee a \vee c') \wedge (a \vee c' \vee a \vee 1' \vee a') = 0 \end{array} \right. \iff \\
&\iff \left\{ \begin{array}{l} (a' \wedge 0' \wedge c' \wedge a' \wedge b)' = 0 \\ \text{oppure} \\ c' \vee b' \vee c = 0 \\ \text{oppure} \\ b' \vee (a' \wedge (c \vee a') \wedge a) \vee a \vee c' = 0 \\ \text{oppure} \\ a \vee c' \vee a \vee 1' \vee a' = 0 \end{array} \right. \iff \\
&\iff \left\{ \begin{array}{l} a' \wedge 0' \wedge c' \wedge a' \wedge b = 1 \\ \text{oppure} \\ c' = b' = c = 0 \quad (\text{non succede mai}) \\ \text{oppure} \\ b' \vee a \vee c' = 0 \\ \text{oppure} \\ a = c' = a = 1' = a' = 0 \quad (\text{non succede mai}) \end{array} \right. \iff \\
&\iff \left\{ \begin{array}{l} c' \wedge a' \wedge b = 1 \\ \text{oppure} \\ b' \vee a \vee c' = 0 \end{array} \right. \iff \left\{ \begin{array}{l} (a', b, c') = (1, 1, 1) \\ \text{oppure} \\ (a, b', c') = (0, 0, 0) \end{array} \right. \iff \\
&\iff \left\{ \begin{array}{l} (a, b, c) = (0, 1, 0) \\ \text{oppure} \\ (a, b, c) = (0, 1, 1) \end{array} \right.
\end{aligned}$$

così che

$$P(a,b,c) = 1 \iff (a,b,c) \in \{(0,1,0), (0,1,1)\}$$

Ora, i due prodotti fondamentali e completi — nelle tre variabili  $x, y, z$ , in quest'ordine — corrispondenti alle due stringhe  $(0, 1, 0)$  e  $(0, 1, 1)$  sono rispettivamente  $x' \wedge y \wedge z'$  e  $x' \wedge y \wedge z$ . Perciò, in conclusione, la F.N.D. di  $P(x, y, z)$  è la somma di questi due prodotti, cioè esattamente il polinomio  $F(x, y, z)$  in (10).

(b) Riprendendo da (10) osserviamo ancora che si ha

$$\begin{aligned} P(x, y, z) &\sim (x' \wedge y \wedge z') \vee (x' \wedge y \wedge z) \sim \\ &\sim (x' \wedge y) \wedge (z' \vee z) \sim (x' \wedge y) \wedge 1 \sim (x' \wedge y) =: M(x, y, z) \end{aligned}$$

dove il polinomio booleano  $M(x, y, z)$  è ancora una somma di prodotti equivalente a  $P(x, y, z)$ . Ora, ricordando che la misura di “grandezza” di una somma di prodotti  $S$  è data da  $G(S) := (E_S, F_S) \in \mathbb{N}^2$  con

$E_S :=$  somma dei gradi di tutti i prodotti in  $S$ ,  $F_S :=$  numero dei prodotti in  $S$

la “grandezza” delle due somme di prodotti  $F$  e  $M$  è data da

$$G(F(x, y, z)) := (6, 2) \quad , \quad G(M(x, y, z)) := (2, 1)$$

pertanto abbiamo  $G(M(x, y, z)) \not\leq_{\times} G(F(x, y, z))$ , dove  $\leq_{\times}$  è la relazione d’ordine prodotto in  $\mathbb{N}^2$ , cioè la somma di prodotti  $M(x, y, z)$  è strettamente più semplice della somma  $F(x, y, z)$ , e pertanto — per definizione! —  $F(x, y, z)$  non è una forma minimale di  $P(x, y, z)$ .

NOTA: Se si applica il *Metodo del Consenso* alla somma di prodotti  $F(x, y, z)$  si trova proprio  $M(x, y, z)$ , perciò quest’ultima è la somma di tutti gli implicanti primi (=s.t.i.p.) di  $P(x, y, z)$ . In aggiunta, visto che questa somma è formata da un solo prodotto, essa è anche una *forma minimale* di  $P(x, y, z)$ , e necessariamente è anche l’unica forma minimale esistente.

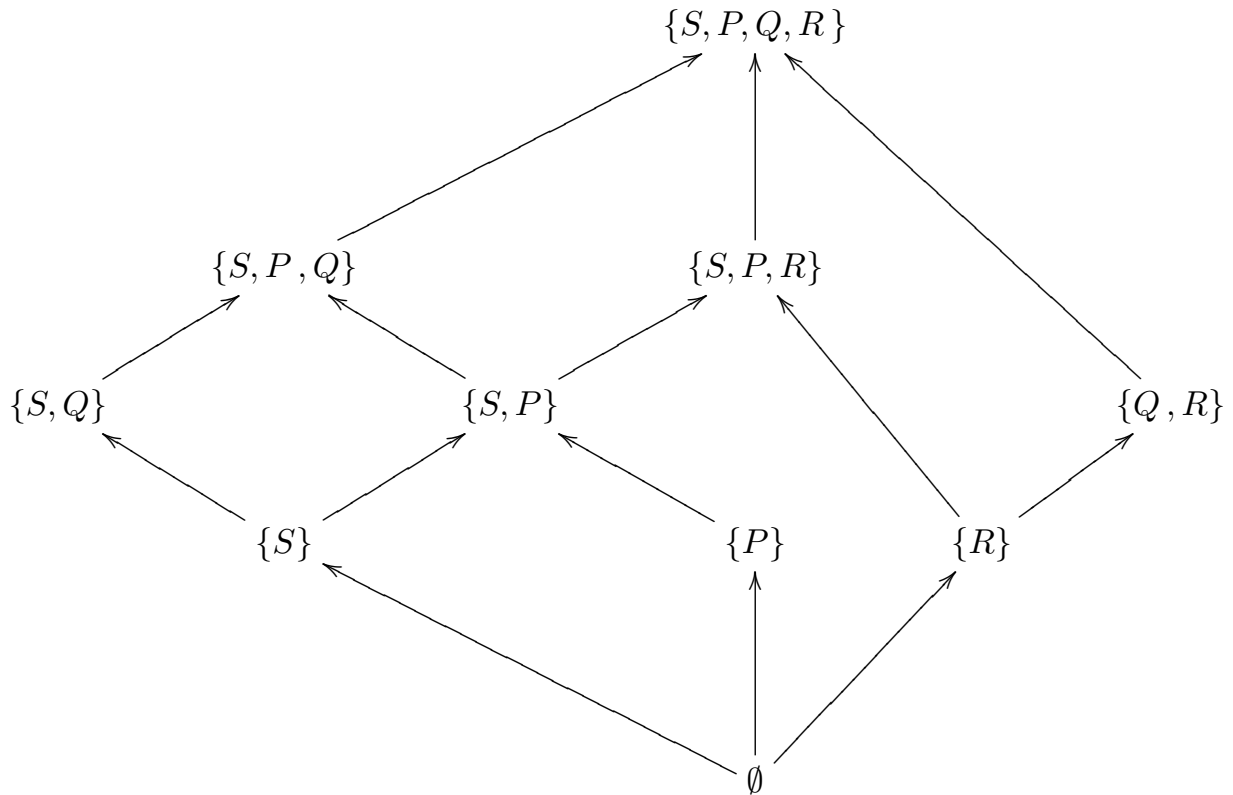
[5] — Nell’insieme delle parti  $\mathcal{P}(\{S, P, Q, R\})$  dell’insieme  $\{S, P, Q, R\}$  consideriamo il sottoinsieme  $\mathbb{E}$  definito da

$$\begin{aligned} \mathbb{E} &:= \mathcal{P}(\{S, P, Q, R\}) \setminus \{\{Q\}, \{S, R\}, \{P, Q\}, \{P, R\}, \{S, Q, R\}, \{P, Q, R\}\} = \\ &= \{\emptyset, \{S\}, \{P\}, \{R\}, \{S, P\}, \{S, Q\}, \{Q, R\}, \\ &\quad \{S, P, Q\}, \{S, P, R\}, \{S, P, Q, R\}\} \end{aligned}$$

L’insieme  $\mathcal{P}(\{S, P, Q, R\})$  è un insieme ordinato rispetto alla relazione di inclusione (per la quale è un reticolo, e anche un’algebra di Boole); restringiamo tale relazione al sottoinsieme  $\mathbb{E}$ , e studiamo l’insieme ordinato  $(\mathbb{E}; \subseteq)$ .



(a) Il diagramma di Hasse dell'insieme ordinato  $(\mathbb{E}; \subseteq)$  è il seguente:



N.B.: ovviamente, lo stesso diagramma può essere disegnato in modi diversi...

Direttamente dall'analisi del diagramma di Hasse otteniamo alcune informazioni, non esplicitamente richieste, ma che saranno utili in seguito (tra l'altro, potremmo verificare che effettivamente l'insieme ordinato  $(\mathbb{E}; \subseteq)$  è davvero un reticolo...):

(a-1)  $\mathbb{E}$  è limitato — cosa nota a priori, perché è un reticolo *finito* — con limiti  $\max(\mathbb{E}) = \{S, P, Q, R\}$  e  $\min(\mathbb{E}) = \emptyset$ ;

(a-2)  $\mathbb{E}$  possiede esattamente tre *atomi* (= gli elementi che coprono il minimo, che in questo caso è  $\emptyset$ ), che sono  $\{S\}$ ,  $\{P\}$ ,  $\{R\}$ ;

(a-3)  $\mathbb{E}$  possiede esattamente sei *elementi*  $\vee$ -irriducibili: quelli ovvî (il minimo e gli atomi) più due non banali, che sono  $\{S, Q\}$  e  $\{Q, R\}$ .

(b) Ricordiamo che un sottoinsieme  $L'$  dentro un reticolo  $L$  si dice *sottoreticolo* di  $L$  se per ogni  $x, y \in L'$  si ha  $x \vee_L y \in L'$  e  $x \wedge_L y \in L'$  dove “ $\vee_L$ ” e “ $\wedge_L$ ” indicano le due operazioni nel reticolo  $L$ . Ora, nel caso del reticolo  $L := \mathcal{P}(\{S, P, Q, R\})$  si ha  $\vee_L = \cup$  e  $\wedge_L = \cap$ , quindi  $L' := \mathbb{E}$  sarebbe un sottoreticolo di  $L := \mathcal{P}(\{S, P, Q, R\})$  se e soltanto se fosse  $X \cup Y \in \mathbb{E}$  e  $X \cap Y \in \mathbb{E}$  per ogni  $X, Y \in \mathbb{E}$ .

Ma questo è falso, in vari casi, precisamente questi:

$$\begin{aligned} \{S\} \cup \{R\} = \{S, R\} &\notin \mathbb{E} \quad , \quad \{S\} \cup \{Q, R\} = \{S, Q, R\} \notin \mathbb{E} \\ \{P\} \cup \{R\} = \{P, R\} &\notin \mathbb{E} \quad , \quad \{P\} \cup \{Q, R\} = \{P, Q, R\} \notin \mathbb{E} \\ \{S, Q\} \cup \{Q, R\} = \{S, Q, R\} &\notin \mathbb{E} \quad , \quad \{S, Q\} \cap \{Q, R\} = \{Q\} \notin \mathbb{E} \\ \{S, P, Q\} \cap \{Q, R\} &= \{Q\} \notin \mathbb{E} \end{aligned}$$

Un altro metodo — indiretto — per dimostrare che  $\mathbb{E}$  non è un sottoreticolo di  $\mathcal{P}(\{S, P, Q, R\})$  può essere questo. Sappiamo che il reticolo  $\mathcal{P}(\{S, P, Q, R\})$  è distributivo, perciò ogni suo sottoreticolo è distributivo anch'esso, automaticamente. Ma si può osservare — come fatto ai punti (d-2/3/4) più avanti — che il reticolo  $\mathbb{E}$  invece non è distributivo, e pertanto esso sicuramente non è sottoreticolo di  $\mathcal{P}(\{S, P, Q, R\})$ , q.e.d.

(c) C'è un risultato generale che dice che in ogni reticolo *finito* (che non significa “limitato”: sono proprietà diverse!) per ogni elemento esiste una  $\vee$ -fattorizzazione non ridondante in elementi  $\vee$ -irriducibili, non necessariamente unica. Visto che il reticolo  $\mathbb{E}$  è finito, ne deduciamo che esiste almeno una  $\vee$ -fattorizzazione non ridondante in elementi  $\vee$ -irriducibili per l'elemento  $\{S, P, Q, R\}$  in  $\mathbb{E}$ .

Vogliamo adesso a trovare *tutte* le  $\vee$ -fattorizzazioni di  $\{S, P, Q, R\}$  di questo tipo; a tal fine, procediamo con metodo. Consideriamo tutte le “somme” — cioè monomi nella sola operazione “ $\vee$ ” — fatte soltanto con elementi  $\vee$ -irriducibili, che sono quelli in (a-3) qui sopra. Tra queste somme dobbiamo scartare tutte quelle ridondanti, che sono tutte e sole quelle in cui ci sia un addendo che è ripetuto più di una volta, oppure compaia  $\emptyset$  (il minimo), oppure compaiano entrambi gli elementi  $\{T\}$  e  $\{T, O\}$ , oppure entrambi  $\{E\}$  e  $\{O, E\}$ . Quindi le possibili somme sono

$$\begin{aligned} 0 \text{ (=somma con zero addendi)} , \quad & \{S, Q\} , \quad \{S\} , \quad \{P\} , \quad \{R\} , \quad \{Q, R\} \\ & \{S, Q\} \vee \{P\} , \quad \{S, Q\} \vee \{R\} , \quad \{S, Q\} \vee \{Q, R\} , \quad \{S\} \vee \{P\} \\ & \{S\} \vee \{R\} , \quad \{S\} \vee \{Q, R\} , \quad \{P\} \vee \{R\} , \quad \{P\} \vee \{Q, R\} \\ & \{S, Q\} \vee \{P\} \vee \{R\} , \quad \{S, Q\} \vee \{P\} \vee \{Q, R\} , \quad \{S\} \vee \{P\} \vee \{Q, R\} \end{aligned}$$

e dobbiamo vedere quali di queste danno  $\{S, P, Q, R\}$ . Dalle definizioni (o dall'analisi del diagramma di Hasse di  $\mathbb{E}$ ) ricaviamo

$$\begin{aligned} 0 , \{S, Q\} , \{S\} , \{P\} , \{R\} , \{Q, R\} &\neq \{S, P, Q, R\} \\ \{S, Q\} \vee \{P\} = \{S, P, Q\} &\neq \{S, P, Q, R\} , \quad \{S, Q\} \vee \{R\} = \{S, P, Q, R\} \\ \{S, Q\} \vee \{Q, R\} = \{S, P, Q, R\} , \quad & \{S\} \vee \{P\} = \{S, P\} \neq \{S, P, Q, R\} \\ \{S\} \vee \{R\} = \{S, P, R\} &\neq \{S, P, Q, R\} , \quad \{S\} \vee \{Q, R\} = \{S, P, Q, R\} \\ \{P\} \vee \{R\} = \{S, P, R\} &\neq \{S, P, Q, R\} , \quad \{P\} \vee \{Q, R\} = \{S, P, Q, R\} \\ \{S, Q\} \vee \{P\} \vee \{R\} &= \{S, P, Q, R\} \\ \{S, Q\} \vee \{P\} \vee \{Q, R\} &= \{S, P, Q, R\} \\ \{S\} \vee \{P\} \vee \{Q, R\} &= \{S, P, Q, R\} \end{aligned}$$

perciò in conclusione esistono per  $\{S, P, Q, R\}$  tutte e sole le seguenti sette  $\vee$ -fattorizzazioni non ridondanti in fattori  $\vee$ -irriducibili (a meno dell'ordine dei fattori), a due a due distinte:

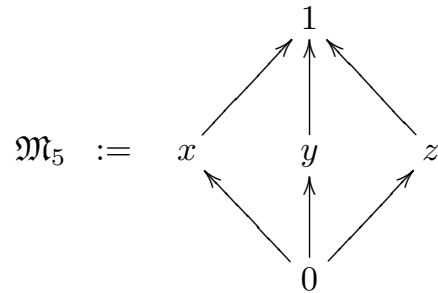
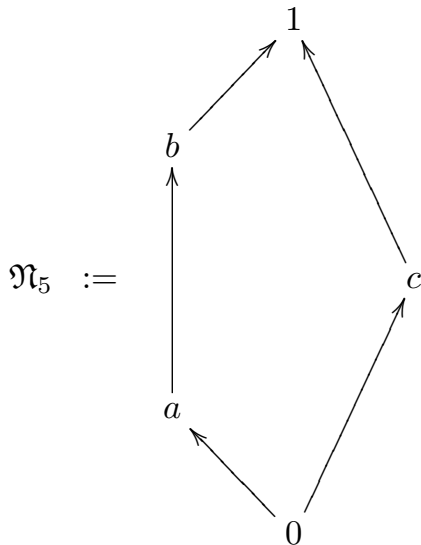
$$\begin{aligned}\{S, P, Q, R\} &= \{S, Q\} \vee \{R\} \quad , \quad \{S, P, Q, R\} = \{S, P\} \vee \{Q, R\} \\ \{S, P, Q, R\} &= \{S\} \vee \{Q, R\} \quad , \quad \{S, P, Q, R\} = \{P\} \vee \{Q, R\} \\ \{S, P, Q, R\} &= \{S, Q\} \vee \{P\} \vee \{R\} \\ \{S, P, Q, R\} &= \{S, Q\} \vee \{P\} \vee \{Q, R\} \\ \{S, P, Q, R\} &= \{S\} \vee \{P\} \vee \{Q, R\}\end{aligned}$$

(d) Sappiamo che un'algebra di Boole (secondo una delle sue varie, possibili definizioni) è un reticolo distributivo, limitato e complementato. Inoltre, un'algebra di Boole — e in particolare una che sia finita — possiede anche altre proprietà, che non sono esplicitate nella definizione ma ne sono conseguenze. Pertanto, per rispondere al quesito (d) dobbiamo dimostrare (direttamente o indirettamente) che  $\mathbb{E}$  è un'algebra di Boole perché soddisfa le condizioni per esserlo, oppure non lo è perché non possiede almeno una delle proprietà espresse nella definizione o che ne sono conseguenza. Osserviamo poi che, come notato in (a-1), il reticolo  $\mathbb{E}$  è limitato, con limiti  $\max(\mathbb{E}) = \{S, P, Q, R\}$  e  $\min(\mathbb{E}) = \emptyset$ . Quindi restano da controllare le altre proprietà di  $\mathbb{E}$ .

Procedendo in questo modo, troviamo che  $\mathbb{E}$  *non* possiede molte delle proprietà di cui sopra (sebbene a noi ne basti una!) e quindi *non è un'algebra di Boole*. Elenchiamo ora queste condizioni “violate” da  $\mathbb{E}$ :

(d-1)  $\mathbb{E}$  *non è complementato*: infatti, l'elemento  $\{S, P, R\}$  *non ha* complemento in  $\mathbb{E}$ , cioè *non esiste un*  $X \in \mathbb{E}$  *tale che*  $\{S, P, R\} \vee X = \max(\mathbb{E}) = \{S, P, Q, R\}$  *e*  $\{S, P, R\} \wedge X = \min(\mathbb{E}) = \emptyset$ .

(d-2)  $\mathbb{E}$  *non è distributivo*: infatti, ricordiamo che un reticolo  $L$  è distributivo se e soltanto se non esiste in  $L$  un sottoreticolo  $L'$  che sia isomorfo a uno dei due reticoli



Questo corrisponde al fatto che gli elementi  $a, b, c$  violano le identità distributive nel reticolo  $\mathfrak{N}_5$ : infatti

$$\left. \begin{array}{l} a \vee (b \wedge c) = a \vee 0 = a \\ (a \vee b) \wedge (a \vee c) = b \wedge 1 = b \end{array} \right\} \implies a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$$

e anche (dualmente)

$$\left. \begin{array}{l} b \wedge (a \vee c) = b \wedge 1 = b \\ (b \wedge a) \vee (b \wedge c) = a \vee 0 = a \end{array} \right\} \implies b \wedge (a \vee c) \neq (b \wedge a) \vee (b \wedge c)$$

perciò, attraverso l'isomorfismo  $\mathfrak{N}_5 \xrightarrow{\cong} L'$ , gli elementi in  $L'(\subseteq L)$  corrispondenti ad  $a, b$  e  $c$  violano le identità distributive nel reticolo  $L'$  e quindi anche in  $L$ , che quindi non è distributivo. Analogamente, gli elementi  $x, y, z$  violano le identità distributive nel reticolo  $\mathfrak{M}_5$ , in quanto

$$\left. \begin{array}{l} x \vee (y \wedge z) = x \vee 0 = x \\ (x \vee y) \wedge (x \vee z) = 1 \wedge 1 = 1 \end{array} \right\} \implies x \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z)$$

come anche (dualmente)

$$\left. \begin{array}{l} x \wedge (y \vee z) = x \wedge 1 = x \\ (x \wedge y) \vee (x \wedge z) = 0 \vee 0 = a \end{array} \right\} \implies x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z)$$

e allora, tramite l'isomorfismo  $\mathfrak{M}_5 \xrightarrow{\cong} L'$ , gli elementi in  $L'(\subseteq L)$  corrispondenti ad  $x, y$  e  $z$  violano le identità distributive nel reticolo  $L'$  e quindi pure in  $L$ .

Ora, dall'analisi del diagramma di Hasse di  $\mathbb{E}$  segue che non ci sono sottoreticoli isomorfi a  $\mathfrak{M}_5$ . Ci sono invece vari sottoreticoli  $L'$  isomorfi a  $\mathfrak{N}_5$ ! Cerchiamo di trovarli tutti, procedendo con metodo: a tal fine, consideriamo le varie possibili coppie di elementi  $A$  e  $B$  in  $L := \mathbb{E}$  che possano corrispondere — all'interno di un sottoreticolo  $L'$  di  $\mathbb{E}$  — agli elementi  $a$  e  $b$  nel reticolo  $\mathfrak{N}_5$ , e poi come si possano “completare” con aggiungendo un terzo elemento  $C$  corrispondente a  $c$ , e quindi poi anche  $Z := \inf_{\mathbb{E}}(\{A, B, C\})$  e  $U := \sup_{\mathbb{E}}(\{A, B, C\})$  in modo che  $L' := \{Z, A, B, C, U\}$  sia un sottoreticolo in  $L := \mathbb{E}$  che sia isomorfo a  $\mathfrak{N}_5 := \{0, a, b, c, 1\}$ , con isomorfismo dato da  $Z \mapsto 0, A \mapsto a, B \mapsto b, C \mapsto c, U \mapsto 1$ .

Dall'analisi diretta del diagramma di Hasse troviamo che le possibili scelte sono tutte e sole le seguenti:

—  $(A, B) = (\{S, P\}, \{S, P, R\})$  oppure  $(A, B) = (\{P\}, \{S, P, Q\})$ : per ciascuno di questi due casi, esiste una sola possibilità per  $C$ , che è  $C = \{Q, R\}$ ; pertanto questo ci dà i due sottoreticoli

$$\begin{aligned} & \{\emptyset, \{S, P\}, \{S, P, R\}, \{Q, R\}, \{S, P, Q, R\}\} \\ & \{\emptyset, \{P\}, \{S, P, Q\}, \{Q, R\}, \{S, P, Q, R\}\} \end{aligned}$$

—  $(A, B)$  è una delle coppie nell'insieme

$$\{ (\{P\}, \{S, P\}), (\{S\}, \{S, P\}), (\{S\}, \{S, Q\}), (\{S, P\}, \{S, P, Q\}), \\ (\{S, Q\}, \{S, P, Q\}), (\{S\}, \{S, P, Q\}), (\{P\}, \{S, P, Q\}) \}$$

per ciascuno di questi sette casi, esistono due possibilità per  $C$ , date da  $C = \{R\}$  oppure  $C = \{Q, R\}$ ; pertanto, combinando tutte le scelte possibili otteniamo i sette sottoreticoli seguenti

$$\begin{aligned} & \{ \emptyset, \{P\}, \{S, P\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, P\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, Q\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S, P\}, \{S, P, Q\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S, Q\}, \{S, P, Q\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, P, Q\}, \{R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{P\}, \{S, P, Q\}, \{R\}, \{S, P, Q, R\} \} \end{aligned}$$

scegliendo  $C = \{R\}$ , e poi invece scegliendo  $C = \{Q, R\}$  otteniamo gli altri sette reticoli seguenti

$$\begin{aligned} & \{ \emptyset, \{P\}, \{S, P\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, P\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, Q\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S, P\}, \{S, P, Q\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S, Q\}, \{S, P, Q\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{S\}, \{S, P, Q\}, \{Q, R\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{P\}, \{S, P, Q\}, \{Q, R\}, \{S, P, Q, R\} \} \end{aligned}$$

ottenuti semplicemente cambiando “ $\{R\}$ ” in “ $\{Q, R\}$ ” nella lista precedente;

—  $(A, B) = (\{R\}, \{Q, R\})$ : in tal caso abbiamo due possibilità per  $C$ , che sono  $C = \{S, Q\}$  oppure  $C = \{S, P, Q\}$ ; perciò, combinando tutte le scelte possibili otteniamo i due seguenti sottoreticoli

$$\begin{aligned} & \{ \emptyset, \{R\}, \{Q, R\}, \{S, Q\}, \{S, P, Q, R\} \} \\ & \{ \emptyset, \{R\}, \{Q, R\}, \{S, P, Q\}, \{S, P, Q, R\} \} \end{aligned}$$

Allora in totale esistono esattamente diciotto sottoreticoli in  $\mathbb{E}$  isomorfi a  $\mathfrak{N}_5$ , per cui  $\mathbb{E}$  non è distributivo: precisamente (anche senza conoscere il risultato generale di caratterizzazione dei reticoli *non* distributivi)), ognuno di tali sottoreticoli individua

(almeno) due violazioni della distributività, ad esempio per il sottoreticolo  $L' := \{\emptyset, \{R\}, \{Q, R\}, \{S, P, Q\}, \{S, P, Q, R\}\}$  la violazione

$$\left. \begin{array}{l} a \vee (b \wedge c) = a \vee 0 = a \\ (a \vee b) \wedge (a \vee c) = b \wedge 1 = b \end{array} \right\} \implies a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$$

osservata in precedenza in  $\mathfrak{N}_5$  corrisponde al fatto che in tale  $L'$  — e dunque in  $\mathbb{E}$  — si ha

$$\{R\} \vee (\{Q, R\} \wedge \{S, P, Q\}) = \{R\} \vee \emptyset = \{R\}$$

$$(\{R\} \vee \{Q, R\}) \wedge (\{R\} \vee \{S, P, Q\}) = \{Q, R\} \wedge \{S, P, Q, R\} = \{Q, R\}$$

e quindi

$$\{R\} \vee (\{Q, R\} \wedge \{S, P, Q\}) \neq (\{R\} \vee \{Q, R\}) \wedge (\{R\} \vee \{S, P, Q\})$$

(d-3) (metodo indiretto)  $\mathbb{E}$  non è distributivo, perché in un reticolo distributivo il complemento di un elemento, se esiste, è *unico*, mentre invece nel reticolo  $\mathbb{E}$  esistono elementi che hanno più di un complemento, precisamente questi:

- $\{Q, R\}$  ha complementi  $\{S\}, \{S, Q\}, \{S, P\}, \{S, P, Q\}$ ;
- $\{R\}$  ha complementi  $\{S, Q\}, \{S, P, Q\}$ ;
- $\{S, Q\}$  ha complementi  $\{R\}, \{Q, R\}$ ;
- $\{S, P, Q\}$  ha complementi  $\{R\}, \{Q, R\}$ .

(d-4) (metodo indiretto)  $\mathbb{E}$  non è distributivo, perché in un reticolo distributivo se un elemento ha una  $\vee$ -fattorizzazione non ridondante in  $\vee$ -irriducibili essa è unica (a meno dell'ordine dei fattori). Invece nel reticolo  $\mathbb{E}$  c'è l'elemento  $\{S, P, Q, R\}$  che, come abbiamo già visto al punto (c), ammette diverse  $\vee$ -fattorizzazioni non ridondanti in  $\vee$ -irriducibili a due a due distinte.

(d-5) (metodo indiretto)  $\mathbb{E}$  non è un'algebra di Boole, perché in un'algebra di Boole ogni elemento ha un unico complemento (il che è falso in  $\mathbb{E}$ , come abbiamo già visto; ma adesso immaginiamo di non saperlo): e da questo poi segue — per un risultato generale — che ogni elemento  $\vee$ -irriducibile diverso dal minimo è un atomo. Invece nel reticolo  $\mathbb{E}$ , per quanto visto al punto (a-3), esistono gli elementi  $\{S, Q\}$  e  $\{Q, R\}$  che sono  $\vee$ -irriducibili ma *non sono* atomi; ne segue allora che  $\mathbb{E}$  non è un'algebra di Boole.

(d-6) (metodo indiretto)  $\mathbb{E}$  non è un'algebra di Boole, perché è un reticolo finito e (per il *Teorema di Rappresentazione (Boole)* nel caso finito) ogni algebra di Boole *finita*  $\mathbb{B}$  ha cardinalità del tipo  $|\mathbb{B}| = 2^n$  per un certo  $n \in \mathbb{N}$ . Invece il reticolo  $\mathbb{E}$  ha cardinalità  $|\mathbb{E}| = 10 \neq 2^n$  per ogni  $n \in \mathbb{N}$ . Più precisamente, il Teorema di Rappresentazione garantisce che  $\mathbb{B}$  è isomorfa (come algebra di Boole) all'insieme delle parti  $\mathcal{P}(\mathcal{A}_{\mathbb{B}})$  dell'insieme  $\mathcal{A}_{\mathbb{B}}$  degli atomi di  $\mathbb{B}$ , da cui in particolare segue che

$$|\mathbb{B}| = |\mathcal{P}(\mathcal{A}_{\mathbb{B}})| = 2^{|\mathcal{A}_{\mathbb{B}}|}$$

Nel nostro caso, come già visto in (a-2), gli atomi di  $\mathbb{E}$  sono tre, perciò se  $\mathbb{E}$  fosse algebra di Boole — nel ruolo di  $\mathbb{B}$  — avremmo

$$|\mathbb{E}| = |\mathcal{P}(\mathcal{A}_{\mathbb{E}})| = 2^{|\mathcal{A}_{\mathbb{E}}|} = 2^3 = 8$$

mentre invece risulta  $|\mathbb{E}| = 10 \neq 8$ .

---