

ALGEBRA e LOGICA
CdL in Ingegneria Informatica
prof. Fabio GAVARINI

a.a. 2016–2017 — Sessione Estiva Anticipata, I appello
Esame scritto del 2 Febbraio 2017

.....

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

..... \mathcal{B}

[1] Dato l'insieme $\{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}$, si consideri il corrispondente insieme delle parti $\mathcal{P}(\{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\})$, dotato della relazione (d'ordine) di inclusione; per semplificare la notazione indicheremo un sottoinsieme $\{x_1, x_2, \dots, x_n\}$ con $\underline{x_1 x_2 \dots x_n} := \{x_1, x_2, \dots, x_n\}$. Si consideri poi in $\mathcal{P}(\{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\})$ il sottoinsieme

$$\mathbb{H} := \{ \emptyset, \underline{\heartsuit}, \underline{\clubsuit}, \underline{\diamondsuit}, \underline{\heartsuit \clubsuit}, \underline{\clubsuit \diamondsuit}, \underline{\heartsuit \spadesuit \clubsuit \diamondsuit} \}$$

dotato a sua volta della relazione (d'ordine) di inclusione.

(a) Verificare che l'insieme ordinato $(\mathbb{H}; \subseteq)$ è un reticolo, scrivendo esplicitamente tutti i valori $\sup(x, y)$ e $\inf(x, y)$ per ogni $x, y \in \mathbb{H}$.

(b) Determinare tutti gli atomi e tutti gli elementi \vee -irriducibili del reticolo \mathbb{H} .

(c) Esiste una \vee -fattorizzazione non ridondante in *fattori* \vee -irriducibili per l'elemento $\underline{\heartsuit \spadesuit \clubsuit \diamondsuit}$ nel reticolo \mathbb{H} ? In caso affermativo, si determini esplicitamente una tale \vee -fattorizzazione; in caso negativo, si spieghi perché essa non esista.

(d) Esiste una \vee -fattorizzazione non ridondante in *atomi* per l'elemento $\underline{\heartsuit \spadesuit \clubsuit \diamondsuit}$ nel reticolo \mathbb{H} ? In caso affermativo, si determini esplicitamente una tale \vee -fattorizzazione; in caso negativo, si spieghi perché essa non esista.

(e) Stabilire, motivando la risposta, se l'insieme ordinato $(\mathbb{H}; \subseteq)$ sia un'algebra di Boole oppure no.

[2] Dati i due numeri interi 225 e 489, calcolare:

(a) il M.C.D.(225, 489);

(b) una identità di Bézout per M.C.D.(225, 489);

(c) il m.c.m.(225, 489).

(continua...)

[3] Si consideri il polinomio booleano

$$d(u, v, w) := \left((u' \vee v'' \vee u') \wedge (w'' \vee u \vee w \vee 1' \vee v'') \right)' \vee \\ \vee \left((u' \vee 0 \vee v)' \wedge ((w'' \vee u' \vee w) \vee (v \vee 0 \vee v')') \right)$$

(a) Calcolare la *Forma Normale Disgiuntiva* di $d(u, v, w)$.

(b) Calcolare una *forma minimale* di $d(u, v, w)$.

[4] (a) Calcolare il *minimo* valore di $x \in \mathbb{Z}_{\geq 0}$ tale che $4x \equiv 16^{191} \pmod{76}$.

(b) Nell'anello \mathbb{Z}_{76} degli interi modulo 76, determinare se esista la classe $[4]_{76}^{-1}$ inversa della classe $[4]_{76}$. In caso negativo si spieghi perché la classe inversa non esista; in caso affermativo si calcoli esplicitamente tale classe inversa.

(c) Nell'anello \mathbb{Z}_{19} degli interi modulo 19, determinare se esista la classe $[4]_{19}^{-1}$ inversa della classe $[4]_{19}$. In caso negativo si spieghi perché la classe inversa non esista; in caso affermativo si determini esplicitamente tale classe inversa.

[5] Si considerino l'insieme $\mathbb{V}_I := \{\text{parole della lingua italiana}\}$ e l'insieme di lettere $X := \{B, I, T\}$. Si consideri poi in \mathbb{V}_I la relazione \triangleleft definita da

$$\mathcal{P}_1 \triangleleft \mathcal{P}_2 \iff \begin{array}{l} \text{“la parola } \mathcal{P}_1 \text{ contiene al più tante lettere} \\ \text{di } X \text{ quante ne contiene la parola } \mathcal{P}_2 \text{”} \end{array}$$

dove le lettere, se compaiono più di una volta, vanno contate una volta sola (dunque *senza molteplicità*).

(a) Si dimostri che la relazione \triangleleft è una relazione di preordine in \mathbb{V}_I , ma *non* di ordine.

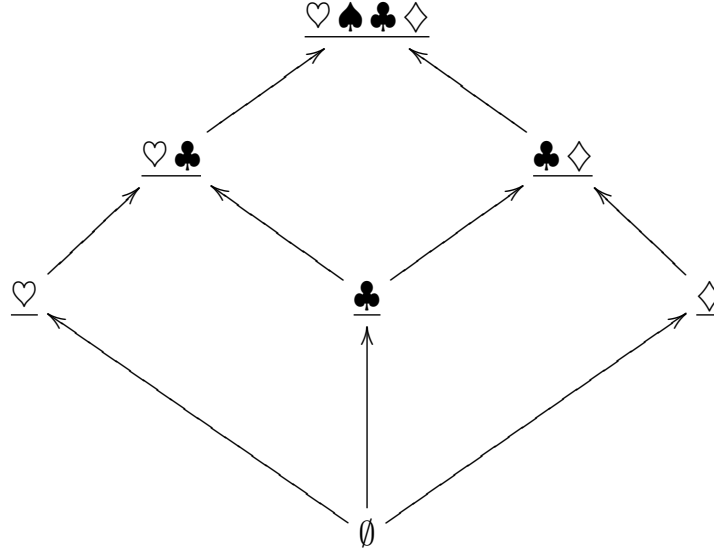
(b) Si dimostri che la relazione $\trianglelefteq := \triangleleft \cap \triangleright = \triangleleft \cap \triangleleft^{-1}$ è una relazione di equivalenza in \mathbb{V}_I .

(c) Determinare la cardinalità dell'insieme quoziente $\left| \mathbb{V}_I / \trianglelefteq \right|$.

(d) Descrivere esplicitamente le quattro classi di \trianglelefteq -equivalenza $[BARO]_{\trianglelefteq}$, $[FARO]_{\trianglelefteq}$, $[ALTO]_{\trianglelefteq}$ e $[TORI]_{\trianglelefteq}$.

SOLUZIONI

[1] — Per comodità di visualizzazione disegniamo qui di seguito il *diagramma di Hasse* dell'insieme ordinato $(\mathbb{H}; \subseteq)$, ma a rigore non è necessario (in particolare, non è richiesto...). Tale diagramma è



(a) Ovviamente, in tutti i “casi banali”, cioè quando sia $a \subseteq b$ oppure $a \supseteq b$, abbiamo che esiste $\sup(\{a, b\}) = a$ e $\inf(\{a, b\}) = b$ se $b \subseteq a$ mentre invece $\sup(\{a, b\}) = b$ e $\inf(\{a, b\}) = a$ se $a \subseteq b$. Per tutti gli altri casi (non banali), direttamente dall’analisi del diagramma di Hasse, osserviamo che esistono sempre $\sup(\{a, b\})$ e $\inf(\{a, b\})$, dati esplicitamente da

$$\begin{aligned} \sup(\{\underline{\heartsuit}, \underline{\clubsuit}\}) &= \underline{\heartsuit\clubsuit}, & \sup(\{\underline{\clubsuit}, \underline{\diamondsuit}\}) &= \underline{\clubsuit\diamondsuit}, & \sup(\{\underline{\heartsuit}, \underline{\diamondsuit}\}) &= \underline{\heartsuit\spadesuit\clubsuit\diamondsuit} \\ \sup(\{\underline{\heartsuit}, \underline{\clubsuit\diamondsuit}\}) &= \underline{\heartsuit\spadesuit\clubsuit\diamondsuit}, & \sup(\{\underline{\heartsuit\clubsuit}, \underline{\diamondsuit}\}) &= \underline{\heartsuit\spadesuit\clubsuit\diamondsuit} \\ \sup(\{\underline{\heartsuit\clubsuit}, \underline{\clubsuit\diamondsuit}\}) &= \underline{\heartsuit\spadesuit\clubsuit\diamondsuit} \\ \inf(\{\underline{\heartsuit}, \underline{\clubsuit}\}) &= \emptyset, & \inf(\{\underline{\clubsuit}, \underline{\diamondsuit}\}) &= \emptyset, & \inf(\{\underline{\heartsuit}, \underline{\diamondsuit}\}) &= \emptyset \\ \inf(\{\underline{\heartsuit}, \underline{\clubsuit\diamondsuit}\}) &= \emptyset, & \inf(\{\underline{\heartsuit\clubsuit}, \underline{\diamondsuit}\}) &= \emptyset \\ \inf(\{\underline{\heartsuit\clubsuit}, \underline{\clubsuit\diamondsuit}\}) &= \underline{\clubsuit} \end{aligned}$$

In conclusione dunque, l’insieme ordinato $(\mathbb{H}; \subseteq)$ è effettivamente un reticolo.

NOTA: Vale la pena sottolineare che, in generale, a priori *non possiamo sapere* se $\sup(\{a, b\}) = a \cup b$ né se $\inf(\{a, b\}) = a \cap b$, sebbene la relazione d’ordine sia l’inclusione! Di fatto, dalla tavola qui sopra possiamo osservare che si ha $\inf(\{a, b\}) = a \cap b$ per ogni $a, b \in \mathbb{H}$ mentre invece $\sup(\{a, b\}) \neq a \cup b$ in tutti i casi su esposti tranne i primi due. In effetti, questa (apparente) “anomalia” si verifica proprio perché si tratta di casi di elementi $a, b \in \mathbb{H}$ per i quali $a \cup b \notin \mathbb{H}$.

(b) Il minimo del reticolo \mathbb{H} è \emptyset , quindi gli *atomi* — cioè, per definizione, gli elementi che coprono il minimo — sono \heartsuit , \clubsuit , \diamondsuit . Tutti questi sono ovviamente \vee -irriducibili, e in aggiunta l'unico altro elemento \vee -irriducibile è quello “banale”, cioè il minimo \emptyset .

(c) Dato che il reticolo \mathbb{H} è finito, certamente esiste (almeno) una fattorizzazione (non ridondante) in \vee -irriducibili di qualunque suo elemento, dunque anche di $\heartsuit \spadesuit \clubsuit \diamondsuit$. Esplicitamente, per tale elemento *esiste un'unica fattorizzazione non ridondante* in \vee -irriducibili, data da $\heartsuit \spadesuit \clubsuit \diamondsuit = \heartsuit \vee \clubsuit \vee \diamondsuit$.

(d) A priori una \vee -fattorizzazione (non ridondante) in *atomi* di $\heartsuit \spadesuit \clubsuit \diamondsuit$ potrebbe esistere oppure no, diversamente da quanto si può dire per una fattorizzazione in \vee -irriducibili; in ogni caso, poiché ogni atomo è sempre \vee -irriducibile ogni \vee -fattorizzazione (non ridondante) in atomi sarebbe una particolare \vee -fattorizzazione (non ridondante) in \vee -irriducibili, che abbiamo trattato nel precedente punto (c). Ora, dall'analisi esplicita di quanto già trovato osserviamo che la \vee -fattorizzazione (non ridondante) in \vee -irriducibili di $\heartsuit \spadesuit \clubsuit \diamondsuit$ già trovata è anche una \vee -fattorizzazione in *atomi*, come richiesto. Dunque, in conclusione, *esiste un'unica \vee -fattorizzazione non ridondante* di $\heartsuit \spadesuit \clubsuit \diamondsuit$ in *atomi*, data da $\heartsuit \spadesuit \clubsuit \diamondsuit = \heartsuit \vee \clubsuit \vee \diamondsuit$.

(e) L'insieme \mathbb{H} è finito, con esattamente 7 elementi. Ora, come conseguenza del *Teorema di Rappresentazione di Stone* sappiamo che ogni algebra di Boole *finita* ha un numero di elementi che è una potenza di 2, cioè è del tipo 2^n per un certo esponente $n \in \mathbb{N}$. Visto che $|\mathbb{H}| = 7$ *non è una potenza di 2*, possiamo concludere che $(\mathbb{H}; \subseteq)$ *non è un'algebra di Boole*. Osserviamo in particolare che con questo metodo non c'è nemmeno bisogno di analizzare come sia fatta la relazione d'ordine fissata in \mathbb{H} : qualunque essa sia, la conclusione sarà sempre la stessa, perché dipende soltanto da una proprietà insiemistica di \mathbb{H} stesso.

In alternativa, possiamo procedere tramite un'analisi diretta delle proprietà di reticolo di $(\mathbb{H}; \subseteq)$, come segue.

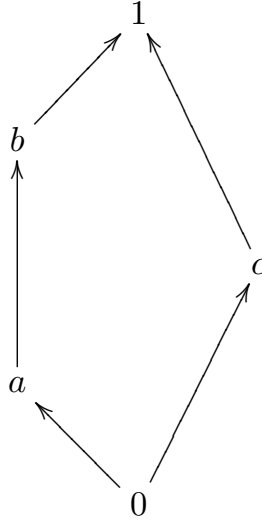
Ricordiamo che, per definizione, un reticolo si dice *algebra di Boole* se e soltanto se è limitato, distributivo e complementato. Ora, il reticolo \mathbb{H} è limitato, con minimo \emptyset e massimo $\heartsuit \spadesuit \clubsuit \diamondsuit$. D'altra parte, dall'analisi del diagramma di Hasse di $(\mathbb{H}; \subseteq)$ possiamo osservare che:

— il reticolo $(\mathbb{H}; \subseteq)$ *non è complementato*, in quanto in esso *non esiste un complemento dell'elemento \clubsuit* , come risulta immediatamente da una semplice verifica diretta (nessun elemento di \mathbb{H} soddisfa le condizioni per essere complemento di \clubsuit).

— il reticolo $(\mathbb{H}; \subseteq)$ *non è distributivo*, in quanto contiene i sottoreticoli

$$\{\emptyset, \heartsuit, \heartsuit \clubsuit, \diamondsuit, \heartsuit \spadesuit \clubsuit \diamondsuit\} \quad \text{e} \quad \{\emptyset, \heartsuit, \diamondsuit, \clubsuit \diamondsuit, \heartsuit \spadesuit \clubsuit \diamondsuit\}$$

che sono entrambi isomorfi al reticolo \mathfrak{N}_5 : ricordiamo infatti che *un reticolo è distributivo se e soltanto se non contiene nessun sottoreticolo che sia isomorfo al reticolo \mathfrak{N}_5* . Ricordiamo anche che il reticolo indicato con \mathfrak{N}_5 è quello rappresentato dal diagramma di Hasse



Un isomorfismo (l'unico possibile!) tra il sottoreticolo $\{\emptyset, \underline{\heartsuit}, \underline{\heartsuit\clubsuit}, \underline{\diamond}, \underline{\heartsuit\spadesuit\clubsuit\heartsuit}\}$ di $(\mathbb{H}; \subseteq)$ e \mathfrak{N}_5 è dato da

$$\emptyset \mapsto 0, \quad \underline{\heartsuit} \mapsto a, \quad \underline{\heartsuit\clubsuit} \mapsto b, \quad \underline{\diamond} \mapsto c, \quad \underline{\heartsuit\spadesuit\clubsuit\heartsuit} \mapsto 1$$

e un isomorfismo (l'unico, di nuovo) tra il sottoreticolo $\{\emptyset, \underline{\heartsuit}, \underline{\diamond}, \underline{\clubsuit\heartsuit}, \underline{\heartsuit\spadesuit\clubsuit\heartsuit}\}$ di $(\mathbb{H}; \subseteq)$ e \mathfrak{N}_5 è dato da

$$\emptyset \mapsto 0, \quad \underline{\heartsuit} \mapsto c, \quad \underline{\diamond} \mapsto a, \quad \underline{\clubsuit\heartsuit} \mapsto b, \quad \underline{\heartsuit\spadesuit\clubsuit\heartsuit} \mapsto 1$$

In alternativa, riconosciamo che \mathbb{H} non è distributivo dal fatto che *gli elementi* $\underline{\heartsuit}$ e $\underline{\diamond}$ *hanno entrambi due complementi*, che sono $\underline{\diamond}$ e $\underline{\clubsuit\heartsuit}$ per $\underline{\heartsuit}$ e $\underline{\heartsuit}$ e $\underline{\heartsuit\clubsuit}$ per $\underline{\diamond}$; siccome in un reticolo distributivo il complementare, se esiste, è unico, da questa osservazione possiamo concludere che \mathbb{H} non è distributivo.

[2] — (a) Calcoliamo M.C.D.(225, 489) tramite l'algoritmo euclideo delle divisioni successive. I calcoli diretti ci danno

$$\begin{aligned}
 225 &= 489 \cdot 0 + 225 \\
 489 &= 225 \cdot 2 + 39 \\
 225 &= 39 \cdot 5 + 30 \\
 39 &= 30 \cdot 1 + 9 \\
 30 &= 9 \cdot 3 + 3 \\
 9 &= 3 \cdot 3 + 0
 \end{aligned} \tag{1}$$

da cui ricaviamo che il M.C.D.(225, 489) richiesto è l'ultimo resto non nullo in questa successione di divisioni con resto, cioè $\text{M.C.D.}(225, 489) = 3$.

(b) Invertendo le identità in (1), tranne l'ultima, le riscriviamo nella forma

$$\begin{array}{ll}
 225 + 489 \cdot (-0) = 225 & 225 = 225 + 489 \cdot (-0) \\
 489 + 225 \cdot (-2) = 39 & 39 = 489 + 225 \cdot (-2) \\
 225 + 39 \cdot (-5) = 30 & \text{o anche} \quad 30 = 225 + 39 \cdot (-5) \\
 39 + 30 \cdot (-1) = 9 & 9 = 39 + 30 \cdot (-1) \\
 30 + 9 \cdot (-3) = 3 & 3 = 30 + 9 \cdot (-3)
 \end{array}$$

A questo punto sostituendo nell'ultima identità l'espressione di 9 data dalla penultima identità, poi sostituendo nel risultato l'espressione di 30 data dalla terzultima identità, e così via, si ottiene — per sostituzioni successive — la seguente catena di identità:

$$\begin{aligned}
 3 &= 30 + 9 \cdot (-3) = 30 + (39 + 30 \cdot (-1)) \cdot (-3) = 39 \cdot (-3) + 30 \cdot 4 = \\
 &= 39 \cdot (-3) + (225 + 39 \cdot (-5)) \cdot 4 = 225 \cdot 4 + 39 \cdot (-23) = \\
 &= 225 \cdot 4 + (489 + 225 \cdot (-2)) \cdot (-23) = 489 \cdot (-23) + 225 \cdot 50 = \\
 &= 489 \cdot (-23) + (225 + 489 \cdot (-0)) \cdot 50 = 225 \cdot 50 + 489 \cdot (-23)
 \end{aligned}$$

(si noti che l'ultimo passaggio qui sopra — così come anche la prima divisione in (1) — di fatto è superfluo, ma l'algoritmo — se applicato rigidamente — prescrive di farlo!), da cui abbiamo

$$\text{M.C.D.}(225, 489) = 3 = 225 \cdot 50 + 489 \cdot (-23)$$

che è una identità di Bézout per $\text{M.C.D.}(225, 489)$, come richiesto.

(c) In conseguenza del *Teorema di Fattorizzazione Unica* per i numeri interi sappiamo che $\text{M.C.D.}(225, 489)$ e $\text{m.c.m.}(225, 489)$ sono legati dall'identità

$$\text{M.C.D.}(225, 489) \cdot \text{m.c.m.}(225, 489) = 225 \cdot 489$$

da cui ricaviamo $\text{m.c.m.}(225, 489)$ con la formula

$$\begin{aligned}
 \text{m.c.m.}(225, 489) &= \frac{225 \cdot 489}{\text{M.C.D.}(225, 489)} = \frac{225 \cdot 489}{3} = \\
 &= 225 \cdot 163 = 75 \cdot 489 = 36675
 \end{aligned}$$

così che, in conclusione, abbiamo $\text{m.c.m.}(225, 489) = 36675$.

[3] — Per un qualsiasi polinomio booleano, sia la *Forma Normale Disgiuntiva* — indicata qui di seguito con *F.N.D.* — sia una *forma minimale* — indicata con *f.m.* — sono particolari *somme di prodotti equivalenti al polinomio assegnato*. Pertanto, in prima battuta operiamo per “trasformare” il polinomio assegnato $d(u, v, w)$ in un altro ad esso equivalente che si presenti però come somma di prodotti.

A partire dall'espressione iniziale di $d(u, v, w)$ otteniamo

$$\begin{aligned} d(u, v, w) &:= \left((u' \vee v'' \vee u') \wedge (w'' \vee u \vee w \vee 1' \vee v'') \right)' \vee \\ &\quad \vee \left((u' \vee 0 \vee v)' \wedge ((w'' \vee u' \vee w) \vee (v \vee 0 \vee v'))' \right) \sim \\ &\sim \left((u' \vee u' \vee v) \wedge (u \vee v \vee 0 \vee w \vee w) \right)' \vee \\ &\quad \vee \left((u' \vee 0 \vee v)' \wedge ((u' \vee w \vee w) \vee (v \vee v'))' \right) \sim \\ &\sim \left((u' \vee v) \wedge (u \vee w \vee v) \right)' \vee \left((u' \vee v)' \wedge (u' \vee w) \right) \end{aligned}$$

dove abbiamo sfruttato la commutatività e l'idempotenza di \vee , il fatto che $1' \sim 0$, il fatto che $P'' \sim P$, che $0 \vee P \sim P$, e che $P \vee P' \sim 1$ per ogni possibile polinomio booleano P . Inoltre, sfruttando la legge di De Morgan $(P \wedge Q)' \sim P' \vee Q'$ si ha

$$\begin{aligned} d(u, v, w) &\sim \left((u' \vee v) \wedge (u \vee w \vee v) \right)' \vee \left((u' \vee v)' \wedge (u' \vee w) \right) \sim \\ &\sim (u' \vee v)' \vee (u \vee w \vee v)' \vee \left((u' \vee v)' \wedge (u' \vee w) \right) \sim \\ &\sim (u \vee w \vee v)' \vee (u' \vee v)' \vee \left((u' \vee v)' \wedge (u' \vee w) \right) \end{aligned}$$

dove nell'ultimo passaggio abbiamo sfruttato la commutatività di \vee . Ora, applicando la legge di assorbimento $A \vee (A \wedge B) \sim A$ al caso $A := (u' \vee v)'$ e $B := (u' \vee w)$ otteniamo

$$\begin{aligned} d(u, v, w) &\sim (u \vee w \vee v)' \vee (u' \vee v)' \vee \left((u' \vee v)' \wedge (u' \vee w) \right) \sim \\ &\sim (u \vee w \vee v)' \vee (u' \vee v)' \end{aligned}$$

Adesso applichiamo l'altra legge di De Morgan, nelle due forme $(P \vee Q \vee R)' \sim P' \wedge Q' \wedge R'$ e $(A \vee B)' \sim A' \wedge B'$ e otteniamo

$$\begin{aligned} d(u, v, w) &\sim (u \vee w \vee v)' \vee (u' \vee v)' \sim \\ &\sim (u' \wedge w' \wedge v') \vee (u'' \wedge v') \sim (u' \wedge w' \wedge v') \vee (u \wedge v') \end{aligned}$$

cioè in definitiva

$$d(u, v, w) \sim (u' \wedge w' \wedge v') \vee (u \wedge v') \quad (2)$$

che è proprio un'espressione del tipo cercato: il membro di destra infatti è un polinomio booleano equivalente a $d(u, v, w)$ e espresso come somma di prodotti.

(a) Per calcolare la F.N.D. di $d(u, v, w)$ partiamo dalla sua espressione equivalente data in (2), che è una somma di prodotti fondamentali non ridondante, e “completiamo” in essa tutti i prodotti che non siano completi, per poi eliminare eventuali “ridondanze”. Dei due addendi coinvolti nella somma, soltanto il secondo non è completo — perché manca in esso la variabile w — e il suo “completamento” chiaramente è

$$u \wedge v' \sim (u \wedge v' \wedge w) \vee (u \wedge v' \wedge w')$$

sostituendo dunque l'espressione di destra nella (2) troviamo

$$d(u, v, w) \sim (u' \wedge w' \wedge v') \vee (u \wedge v') \sim (u' \wedge v' \wedge w') \vee (u \wedge v' \wedge w) \vee (u \wedge v' \wedge w')$$

e quindi in conclusione la F.N.D. di $d(u, v, w)$ è

$$d(u, v, w) \sim (u' \wedge v' \wedge w') \vee (u \wedge v' \wedge w) \vee (u \wedge v' \wedge w') \quad (3)$$

(b) Per calcolare una f.m. di $d(u, v, w)$ partiamo dalla sua espressione equivalente come somma di prodotti data in (2) e applichiamo il *metodo del consenso*. Per cominciare, i due addendi della somma in (2) sono in consenso — in quanto differiscono unicamente per la variabile u — e quindi dalla (2) stessa otteniamo

$$\begin{aligned} d(u, v, w) &\sim (u' \wedge w' \wedge v') \vee (u \wedge v') \sim \\ &\sim (u' \wedge w' \wedge v') \vee (u \wedge v') \vee (w' \wedge v' \wedge v') \sim \\ &\sim (u' \wedge w' \wedge v') \vee (u \wedge v') \vee (w' \wedge v') \sim \\ &\sim (u \wedge v') \vee (u' \wedge w' \wedge v') \vee (w' \wedge v') \sim \\ &\sim (u \wedge v') \vee (w' \wedge v') \sim (u \wedge v') \vee (v' \wedge w') \end{aligned}$$

dove nel penultimo passaggio abbiamo applicato la legge di assorbimento

$$(A \wedge B) \vee B \sim B \quad \text{per } A := u' \quad \text{e} \quad B := w' \wedge v'$$

e nell'ultimo passaggio la commutatività di \wedge . Pertanto abbiamo

$$d(u, v, w) \sim (u \wedge v') \vee (v' \wedge w') \quad (4)$$

dove l'ultima espressione è una somma di prodotti tra i quali non c'è consenso: allora l'algoritmo fondato sul metodo del consenso si arresta qui, e *questa somma di prodotti che abbiamo trovato è la somma di tutti gli implicanti primi di $d(u, v, w)$.*

Osserviamo ora che nella (4) non si può eliminare nessuno dei due prodotti presenti nella somma di destra: infatti, confrontando la (4) con la (3) vediamo che

— il prodotto completo $(u' \wedge v' \wedge w')$ in (3) viene dal completamento del prodotto $(v' \wedge w')$, ma non da quello di $(u \wedge v')$;

— il prodotto completo $(u \wedge v' \wedge w)$ in (3) viene dal completamento del prodotto $(u \wedge v')$, ma non da quello di $(v' \wedge w')$.

Possiamo allora concludere che *una f.m. di $d(u, v, w)$ è data dalla (4)*: in aggiunta, dato che quest'ultima è anche la somma di tutti gli implicanti primi di $d(u, v, w)$, essa è anche *l'unica f.m. possibile di $d(u, v, w)$.*

[4] — (a) Per cominciare, osserviamo che l'equazione congruenziale iniziale

$$4x \equiv 16^{191} \pmod{76}$$

ammette soluzioni, perché si ha $4 = \text{M.C.D.}(4, 76) \mid 16^{191}$, cioè il M.C.D. tra il coefficiente dell'incognita e il modulo divide il termine noto; in aggiunta, a questo punto l'equazione stessa può essere semplificata dividendo tutti i suoi termini per $4 = \text{M.C.D.}(4, 76)$, dando luogo all'equazione congruenziale equivalente

$$\frac{4}{4}x \equiv \frac{16^{191}}{4} \pmod{\frac{76}{4}}$$

cioè, notando tra l'altro $\frac{16^{191}}{4} = \frac{(4^2)^{191}}{4} = \frac{4^{2 \cdot 191}}{4} = \frac{4^{382}}{4} = 4^{382-1} = 4^{381}$,

$$x \equiv 4^{381} \pmod{19}$$

Quest'ultima equazione congruenziale si presenta “in forma già risolta”: le sue soluzioni sono tutti e soli i numeri interi nella classe di congruenza $[4^{381}]_{19}$. Il nostro obiettivo allora sarà semplicemente determinare il *minimo* valore di $x \in \mathbb{Z}_{\geq 0}$ che appartenga a $[4^{381}]_{19}$, in altre parole, dobbiamo trovare il minimo numero non negativo in questa classe di congruenza: in particolare, questo equivale a trovare l'unico rappresentante — certamente esistente! — di questa classe che sia contenuto nell'intervallo da 0 a $19-1 = 18$. Usando la notazione $\bar{z} := [z]_{19}$, dobbiamo dunque trovare l'unico valore di x tale che $\bar{x} = \overline{4^{381}}$ e $0 \leq x \leq 18$.

Dovendo calcolare $\overline{4^{381}}$ nell'anello \mathbb{Z}_{19} delle classi resto modulo 19, osserviamo subito che $\overline{4^{381}} = \bar{4}^{381}$ è una potenza di $\bar{4}$. Notiamo poi che $\text{M.C.D.}(4, 19) = 1$, e quindi in forza del *Teorema di Eulero* sappiamo che $\bar{4}^{\varphi(19)} = \bar{1}$, dove φ è la funzione di Eulero. Da questo, scrivendo l'esponente 381 nella forma $381 = \varphi(19) \cdot q + r$ con $0 \leq r < \varphi(19)$ — cioè facendo la *divisione con resto* di 381 per $\varphi(19)$ — otterremo

$$\overline{4^{381}} = \bar{4}^{381} = \bar{4}^{\varphi(19) \cdot q + r} = \left(\bar{4}^{\varphi(19)}\right)^q \cdot \bar{4}^r = \bar{1}^q \cdot \bar{4}^r = \bar{4}^r \quad (5)$$

da cui vediamo che in effetti nella divisione di 381 per $\varphi(19)$ ci interessa soltanto conoscere il resto, mentre il quoziente è irrilevante — in altre parole, *ci interessa conoscere la classe resto di 381 modulo $\varphi(19)$* .

Ora, per esplicitare la (5) osserviamo che $\varphi(19) = 19 - 1 = 18$, e quindi poi andando a dividere 381 per $\varphi(19) = 18$ troviamo $381 = 18 \cdot 21 + 3$, per cui il resto cercato è $r = 3$; pertanto la (5) ci dà

$$\overline{4^{381}} = \bar{4}^r = \bar{4}^3 = \overline{4^3} = \overline{64} = \overline{19 \cdot 3 + 7} = \bar{7}$$

e quindi il valore x richiesto è $x = 7$.

(b) In generale, ricordiamo che nell'anello \mathbb{Z}_n degli interi modulo n per una singola classe $\bar{a} := [a]_n$ esiste la classe inversa $\bar{a}^{-1} := [a]_n^{-1}$ se e soltanto se $\text{M.C.D.}(a, n) = 1$. Infatti, questo segue dal fatto che \bar{a}^{-1} , se esiste, è l'unica soluzione dell'equazione modulare $\bar{a}\bar{x} = \bar{1}$ in \mathbb{Z}_n : quest'ultima è equivalente all'equazione congruenziale (in \mathbb{Z}) $ax \equiv 1 \pmod{n}$, che a sua volta ammette soluzioni se e soltanto se $\text{M.C.D.}(a, n) \mid 1$, dunque se e soltanto se $\text{M.C.D.}(a, n) = 1$.

Applicando quanto appena ricordato al caso $n := 76$ e $a := 4$ abbiamo che $\text{M.C.D.}(4, 76) = 4 \neq 1$, e quindi concludiamo che *non esiste in \mathbb{Z}_{76} la classe $[4]_{76}^{-1}$ inversa della classe $[4]_{76}$* .

(c) Applicando l'analisi fatta per il punto (b) al caso $n := 19$ e $a := 4$ abbiamo che $\text{M.C.D.}(4, 19) = 1$, e quindi *esiste in \mathbb{Z}_{19} la classe $\bar{4}^{-1} := [4]_{19}^{-1}$ inversa della classe $\bar{4} := [4]_{19}$* . Tale inversa $\bar{4}^{-1} := [4]_{19}^{-1}$ è l'unica soluzione dell'equazione modulare $\bar{4}\bar{x} = \bar{1}$ in \mathbb{Z}_{19} , che a sua volta è equivalente all'equazione congruenziale (in \mathbb{Z}) $4x \equiv 1 \pmod{19}$, che infine è equivalente all'equazione diofantea

$$4x + 19y = 1$$

quindi andiamo a risolvere quest'ultima. Si noti che questo equivale a trovare una identità di Bézout per $\text{M.C.D.}(4, 19) = 1$, dunque un problema del tutto simile a quanto già visto nell'esercizio [2]. Con l'algoritmo delle divisioni successive troviamo

$$\begin{aligned} 4 &= 19 \cdot 0 + 4 \\ 19 &= 4 \cdot 4 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

poi invertiamo queste identità (tranne l'ultima), ottenendo

$$\begin{aligned} 4 &= 4 + 19 \cdot (-0) \\ 3 &= 19 + 4 \cdot (-4) \\ 1 &= 4 + 3 \cdot (-1) \end{aligned}$$

e infine per sostituzioni successive troviamo

$$\begin{aligned} 1 &= 4 + 3 \cdot (-1) = 4 + (19 + 4 \cdot (-4)) \cdot (-1) = 19 \cdot (-1) + 4 \cdot 5 = \\ &= 19 \cdot (-1) + (4 + 19 \cdot (-0)) \cdot 5 = 4 \cdot 5 + 19 \cdot (-1) \end{aligned}$$

da cui in definitiva $1 = 4 \cdot 5 + 19 \cdot (-1)$ è un'identità di Bézout come richiesto, che ci dice che la coppia di interi $(5, -1)$ è una soluzione dell'equazione diofantea $4x + 19y = 1$. Da questa identità di Bézout otteniamo $1 \equiv 4 \cdot 5 \pmod{19}$ — così che $x = 5$ è una soluzione dell'equazione congruenziale $4x \equiv 1 \pmod{19}$ — e quindi $\bar{1} = \bar{4} \cdot \bar{5}$ — così che $\bar{x} = \bar{5}$ è una soluzione (unica!) dell'equazione

modulare $\bar{4} \cdot \bar{x} \equiv 1$ in \mathbb{Z}_{19} — e quindi in definitiva *possiamo concludere che la classe inversa richiesta è $\bar{4}^{-1} = \bar{5}$* .

NOTA: In effetti, ai fini del calcolo della classe inversa sarebbe stato sufficiente anche trovare “a mano” che

$$\bar{4} \cdot \bar{5} = \overline{4 \cdot 5} = \overline{20} = \overline{19+1} = \overline{19} + \bar{1} = \bar{1}$$

e da questo concludere che $\bar{4}^{-1}$ esiste ed è pari a $\bar{4}^{-1} = \bar{5}$. Tuttavia, questo sarebbe stato un metodo “di forza bruta” (del tipo “faccio dei calcoli, e prima o poi imbrotto il risultato, se esiste”...): teoricamente si può sempre applicare, perché \mathbb{Z}_n è un anello finito, però diventa sempre più “costoso” (in termini computazionali) man mano che n diventa più grande. Il metodo presentato qui sopra invece ha un “costo fisso”, indipendente da n .

[5] — (a) Ricordiamo che una relazione si dice *di preordine* se è *riflessiva* e *transitiva*. Nel caso in esame, abbiamo:

— la relazione \triangleleft è *riflessiva*, cioè $\mathcal{P} \triangleleft \mathcal{P}$ per ogni $\mathcal{P} \in \mathbb{V}_I$. Infatti, per definizione abbiamo

$$\mathcal{P} \triangleleft \mathcal{P} \iff \begin{array}{l} \text{“la parola } \mathcal{P} \text{ contiene al più tante lettere} \\ \text{di } X \text{ quante ne contiene la parola } \mathcal{P} \text{”} \end{array}$$

e siccome la condizione di destra è ovviamente soddisfatta, concludiamo che $\mathcal{P} \triangleleft \mathcal{P}$.

— la relazione \triangleleft è *transitiva*, cioè per ogni $\mathcal{P}', \mathcal{P}'', \mathcal{P}''' \in \mathbb{V}_I$, se si ha $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'''$ allora si ha anche $\mathcal{P}' \triangleleft \mathcal{P}'''$. Infatti, dalla definizione abbiamo

$$\begin{array}{ll} \mathcal{P}' \triangleleft \mathcal{P}'' & \implies \mathcal{P}' \text{ contiene al più tante lettere di } X \text{ quante ne contiene } \mathcal{P}'' \\ \mathcal{P}'' \triangleleft \mathcal{P}''' & \implies \mathcal{P}'' \text{ contiene al più tante lettere di } X \text{ quante ne contiene } \mathcal{P}''' \end{array}$$

e quindi confrontando le condizioni di destra abbiamo anche

$$\mathcal{P}' \text{ contiene al più tante lettere di } X \text{ quante ne contiene } \mathcal{P}'''$$

e dunque, ancora per definizione, possiamo concludere che $\mathcal{P}' \triangleleft \mathcal{P}'''$.

Infine, una relazione si dice *di ordine* se è *riflessiva*, *transitiva* — quindi è di preordine — e *antisimmetrica*. Poiché la relazione \triangleleft è riflessiva e transitiva (cioè di preordine), per dimostrare che non è una relazione d’ordine dobbiamo necessariamente dimostrare che non è antisimmetrica.

Ricordiamo che, per definizione, la relazione \triangleleft è *antisimmetrica* se per ogni $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$, se si ha $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'$ allora si ha necessariamente $\mathcal{P}' = \mathcal{P}''$. Pertanto \triangleleft non sarà antisimmetrica se non vale questa proprietà, cioè se la condizione non è soddisfatta da almeno un paio di elementi $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$: perciò in definitiva dobbiamo dimostrare che esistono $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$ tali che $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'$ ma $\mathcal{P}' \neq \mathcal{P}''$.

Osserviamo che se $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$ soddisfano le condizioni $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'$ allora — direttamente dalla definizione — abbiamo che

$$\begin{aligned}\mathcal{P}' \triangleleft \mathcal{P}'' &\implies \mathcal{P}' \text{ contiene al più tante lettere di } X \text{ quante ne contiene } \mathcal{P}'' \\ \mathcal{P}'' \triangleleft \mathcal{P}' &\implies \mathcal{P}'' \text{ contiene al più tante lettere di } X \text{ quante ne contiene } \mathcal{P}'\end{aligned}$$

e quindi dal confronto tra le condizioni di destra ricaviamo

$$\mathcal{P}' \text{ contiene tante lettere di } X \text{ quante ne contiene } \mathcal{P}'' \quad (6)$$

Viceversa, se vale la (6) allora per definizione abbiamo che $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'$. Perciò il nostro obiettivo diventa trovare $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$ per i quali valga la (6) e però $\mathcal{P}' \neq \mathcal{P}''$, cioè trovare due parole diverse che però contengano lo stesso numero di lettere in $X := \{B, I, T\}$. Ad esempio, scegliendo

$$\mathcal{P}' := \text{BATTITO} \quad , \quad \mathcal{P}'' := \text{TUBI}$$

abbiamo appunto che la condizione (6) è soddisfatta mentre $\mathcal{P}' \neq \mathcal{P}''$, q.e.d.

NOTA: Quanto appena visto si può formalizzare — e quindi magari rendere più esplicito e chiaro... — come segue. Consideriamo la funzione

$$\nu : \mathbb{V}_I \longrightarrow \mathbb{N} \quad , \quad \mathcal{P} \mapsto \nu(\mathcal{P}) := \left| \{ \text{lettere di } \mathcal{P} \} \cap X \right| \quad (7)$$

che associa ad ogni parola della lingua italiana il numero di lettere (senza ripetizioni) tra quelle di $X := \{B, I, T\}$ che essa contiene. La definizione della relazione \triangleleft può allora essere riscritta così:

$$\mathcal{P}_1 \triangleleft \mathcal{P}_2 \iff \nu(\mathcal{P}_1) \leq \nu(\mathcal{P}_2) \quad \forall \mathcal{P}_1, \mathcal{P}_2 \in \mathbb{V}_I \quad (8)$$

Facendo uso di questa descrizione, i passaggi precedenti per dimostrare riflessività e transitività di \triangleleft dovrebbero essere più chiari. Si noti però che la differenza è puramente formale, in quanto abbiamo sostituito un linguaggio simbolico (indipendente dalla lingua usata per esprimerci...) alle espressioni verbali (in lingua italiana) che avevamo usato in precedenza.

(b) Ricordiamo che una relazione si dice *di equivalenza* se è *riflessiva*, *transitiva* — dunque è un *preordine* — e *simmetrica*. Nel caso in esame, per la relazione $\triangleleft := \triangleleft \cap \triangleright = \triangleleft \cap \triangleleft^{-1}$ cominciamo osservando che, siccome la relazione \triangleleft , è riflessiva e transitiva, anche la sua inversa $\triangleright := \triangleleft^{-1}$ è a sua volta riflessiva e transitiva. In conseguenza, abbiamo che *anche* $\triangleleft := \triangleleft \cap \triangleright$ è *riflessiva e transitiva*: infatti,

— per ogni $\mathcal{P} \in \mathbb{V}_I$ abbiamo $\mathcal{P} \triangleleft \mathcal{P}$ (perché \triangleleft è riflessiva) e $\mathcal{P} \triangleright \mathcal{P}$ (perché \triangleright è riflessiva), e quindi anche $\mathcal{P} \triangleleft \cap \triangleright \mathcal{P}$, cioè $\mathcal{P} \triangleleft \mathcal{P}$, dunque \triangleleft è riflessiva;

— per ogni $\mathcal{P}', \mathcal{P}'', \mathcal{P}''' \in \mathbb{V}_I$, se $\mathcal{P}' \triangleleft \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'''$ significa che $\mathcal{P}' \triangleleft \mathcal{P}''$, $\mathcal{P}' \triangleright \mathcal{P}''$ e $\mathcal{P}'' \triangleleft \mathcal{P}'''$, $\mathcal{P}'' \triangleright \mathcal{P}'''$; ne segue che $\mathcal{P}' \triangleleft \mathcal{P}'''$ (perché \triangleleft è transitiva) e $\mathcal{P}' \triangleright \mathcal{P}'''$ (perché \triangleright è transitiva); ma allora $\mathcal{P}' \triangleleft \cap \triangleright \mathcal{P}'''$, cioè $\mathcal{P}' \triangleleft \mathcal{P}'''$, così che \triangleleft è transitiva.

Infine, la relazione \triangleleft è simmetrica, cioè per ogni $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$ abbiamo che se $\mathcal{P}' \triangleleft \mathcal{P}''$ allora anche $\mathcal{P}'' \triangleleft \mathcal{P}'$. Infatti, dalle definizioni segue che

$$\begin{aligned} \mathcal{P}' \triangleleft \mathcal{P}'' &\implies \mathcal{P}' \triangleleft \cap \triangleright \mathcal{P}'' \implies \mathcal{P}' \triangleleft \mathcal{P}'' \text{ e } \mathcal{P}' \triangleright \mathcal{P}'' \implies \\ &\implies \mathcal{P}' \triangleleft \mathcal{P}'' \text{ e } \mathcal{P}' \triangleleft^{-1} \mathcal{P}'' \implies \mathcal{P}' \triangleleft \mathcal{P}'' \text{ e } \mathcal{P}'' \triangleleft \mathcal{P}' \implies \\ &\implies \mathcal{P}'' \triangleleft \mathcal{P}' \text{ e } \mathcal{P}' \triangleleft \mathcal{P}'' \implies \mathcal{P}'' \triangleleft \mathcal{P}' \text{ e } \mathcal{P}'' \triangleleft^{-1} \mathcal{P}' \implies \\ &\implies \mathcal{P}'' \triangleleft \mathcal{P}' \text{ e } \mathcal{P}'' \triangleright \mathcal{P}' \implies \mathcal{P}'' \triangleleft \cap \triangleright \mathcal{P}' \implies \mathcal{P}'' \triangleleft \mathcal{P}' \end{aligned}$$

cioè in sintesi $\mathcal{P}' \triangleleft \mathcal{P}'' \implies \mathcal{P}'' \triangleleft \mathcal{P}'$, q.e.d.

NOTE — (b.1) Quanto appena visto si può formalizzare — e quindi magari rendere più esplicito e chiaro... — come segue. Consideriamo la funzione

$$\nu : \mathbb{V}_I \longrightarrow \mathbb{N} \quad , \quad \mathcal{P} \mapsto \nu(\mathcal{P}) := \left| \{ \text{lettere di } \mathcal{P} \} \cap X \right|$$

già introdotta in (7). Tramite questa funzione, la relazione \triangleleft è caratterizzata dalla (8), cioè $\mathcal{P}_1 \triangleleft \mathcal{P}_2 \iff \nu(\mathcal{P}_1) \leq \nu(\mathcal{P}_2)$. Ne segue allora che la relazione inversa $\triangleleft^{-1} =: \triangleright$ è caratterizzata da $\mathcal{P}_1 \triangleright \mathcal{P}_2 \iff \nu(\mathcal{P}_1) \geq \nu(\mathcal{P}_2)$, e in conseguenza per la relazione $\triangleleft := \triangleleft \cap \triangleright = \triangleleft \cap \triangleleft^{-1}$ ricaviamo la caratterizzazione

$$\mathcal{P}_1 \triangleleft \mathcal{P}_2 \iff \nu(\mathcal{P}_1) \leq \nu(\mathcal{P}_2) \text{ e } \nu(\mathcal{P}_1) \geq \nu(\mathcal{P}_2) \quad \forall \mathcal{P}_1, \mathcal{P}_2 \in \mathbb{V}_I$$

cioè in breve

$$\mathcal{P}_1 \triangleleft \mathcal{P}_2 \iff \nu(\mathcal{P}_1) = \nu(\mathcal{P}_2) \quad \forall \mathcal{P}_1, \mathcal{P}_2 \in \mathbb{V}_I \quad (9)$$

In particolare, dalla (9) vediamo che la \triangleleft è proprio la relazione ρ_ν associata (in modo canonico) alla funzione ν , e come tale — come tutte le relazioni definite in tal modo — è certamente una equivalenza.

(b.2) Esattamente con gli stessi passaggi utilizzati nel caso di $\triangleleft := \triangleleft \cap \triangleleft^{-1}$, si dimostra in generale che se λ è una relazione di preordine — così come nel caso di $\lambda := \triangleleft$ — allora la relazione $\lambda \cap \lambda^{-1}$ è una equivalenza.

(c) Ricordiamo che l'insieme quoziente $\mathbb{V}_I / \triangleleft$ è l'insieme i cui elementi sono le classi di \triangleleft -equivalenza in \mathbb{V}_I . Pertanto determinare $\left| \mathbb{V}_I / \triangleleft \right|$ significa esattamente determinare il numero totale di tali classi di \triangleleft -equivalenza.

Grazie alla caratterizzazione della relazione \triangleleft data in (9), sappiamo che due elementi di \mathbb{V}_I sono \triangleleft -equivalenti se e soltanto se hanno lo stesso valore per la funzione ν : pertanto, abbiamo una e una sola classe di \triangleleft -equivalenza per ogni valore della funzione ν , e viceversa — in altre parole, le classi di \triangleleft -equivalenza sono in corrispondenza biunivoca con i valori assunti dalla funzione ν , cioè con gli elementi dell'insieme $Im(\nu)$. Ora, per costruzione tali valori sono i possibili numeri di lettere scelte in $X := \{B, I, T\}$ contenute in una qualsiasi parola: tali valori quindi sono tutti e soli i quattro numeri $0, 1, 2, 3$, cioè $Im(\nu) = \{0, 1, 2, 3\}$. Quindi

la nostra analisi ci permette di concludere che anche le classi di \triangleleft -equivalenza sono esattamente *quattro*. Pertanto, la soluzione del problema posto è che *la cardinalità dell'insieme quoziente* $\left| \mathbb{V}_I / \triangleleft \right|$ *è precisamente* $\left| \mathbb{V}_I / \triangleleft \right| = 4$.

NOTA: L'analisi appena svolta dipende dal fatto che \triangleleft coincide con la relazione di equivalenza ρ_ν canonicamente associata alla funzione ν : infatti la stessa analisi si può applicare allo stesso modo ogni qual volta si debba calcolare la cardinalità dell'insieme quoziente $A / \eta = A / \rho_f$ relativamente ad una relazione di equivalenza $\eta = \rho_f$ associata ad una funzione $f : A \longrightarrow B$, per la quale in effetti avremo sempre $\left| A / \eta \right| = \left| A / \rho_f \right| = \left| \text{Im}(f) \right|$.

(d) Come già osservato al punto (c), le classi di \triangleleft -equivalenza sono in corrispondenza biunivoca con gli elementi dell'insieme $\text{Im}(\nu) = \{0, 1, 2, 3\}$. In dettaglio, tale corrispondenza biunivoca è data — da $\text{Im}(\nu)$ a $\mathbb{V}_I / \triangleleft$ — da

$$\text{Im}(\nu) \hookrightarrow \mathbb{V}_I / \triangleleft, \quad n \mapsto \nu^{-1}(n) := \{ \mathcal{P} \in \mathbb{V}_I \mid \nu(\mathcal{P}) = n \} \quad \forall n \in \text{Im}(\nu)$$

Pertanto, le quattro classi di \triangleleft -equivalenza in \mathbb{V}_I sono

$$\begin{aligned} C_0 &:= \nu^{-1}(0) = \{ \mathcal{P} \in \mathbb{V}_I \mid \mathcal{P} \text{ non contiene nessuna lettera tra } B, I \text{ e } T \} \\ C_1 &:= \nu^{-1}(1) = \{ \mathcal{P} \in \mathbb{V}_I \mid \mathcal{P} \text{ contiene esattamente una lettera tra } B, I \text{ e } T \} \\ C_2 &:= \nu^{-1}(2) = \{ \mathcal{P} \in \mathbb{V}_I \mid \mathcal{P} \text{ contiene esattamente due lettere tra } B, I \text{ e } T \} \\ C_3 &:= \nu^{-1}(3) = \{ \mathcal{P} \in \mathbb{V}_I \mid \mathcal{P} \text{ contiene tutte e tre le lettere } B, I \text{ e } T \} \end{aligned}$$

Alla luce di questo, abbiamo allora

$$[BARO]_{\triangleleft} = C_1, \quad [FARO]_{\triangleleft} = C_0, \quad [ALTO]_{\triangleleft} = C_1, \quad [TORI]_{\triangleleft} = C_2$$

cioè esplicitamente

$$\begin{aligned} [BARO]_{\triangleleft} &= \{ \text{parole di } \mathbb{V}_I \text{ che contengono esattamente una lettera tra } B, I \text{ e } T \} \\ [FARO]_{\triangleleft} &= \{ \text{parole di } \mathbb{V}_I \text{ che non contengono nessuna lettera tra } B, I \text{ e } T \} \\ [ALTO]_{\triangleleft} &= \{ \text{parole di } \mathbb{V}_I \text{ che contengono esattamente una lettera tra } B, I \text{ e } T \} \\ [TORI]_{\triangleleft} &= \{ \text{parole di } \mathbb{V}_I \text{ che contengono esattamente due lettere tra } B, I \text{ e } T \} \end{aligned}$$

NOTA: Anche in questo caso, l'analisi appena svolta dipende esclusivamente dal fatto che \triangleleft coincide con la relazione di equivalenza ρ_ν canonicamente associata alla funzione ν ; e infatti la stessa analisi si può applicare allo stesso modo ogni qual volta si debbano descrivere le classi di equivalenza di una particolare relazione di equivalenza $\eta = \rho_f$ associata (canonicamente) ad una certa funzione $f : A \longrightarrow B$.

Si avrà così che le classi di ρ_f -equivalenza in A saranno esattamente tutti e soli i sottoinsiemi di A dati da

$$C_v := f^{-1}(v) = \{ a \in A \mid f(a) = v \} \quad \forall v \in \text{Im}(f)$$

cioè tutte (e sole) le *controimmagini dei valori assunti dalla funzione f* .

