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 <u>*sintetico*</u> *ma* **esauriente**, *spiegando chiaramente quanto si fa, e scrivendo in* corsivo *con grafia leggibile.*

.... $\mathcal{R}$ ....

[1] Dato l'insieme $\{S\,,P\,,Q\,,R\}$, si consideri il corrispondente insieme delle parti $\mathcal{P}\big(\{S\,,P\,,Q\,,R\}\big)$, 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 $\mathcal{P}\big(\{S\,,P\,,Q\,,R\}\big)$ il sottoinsieme

$$\mathbb{F} := \big\{\,\emptyset\,,\underline{S}\,,\underline{Q}\,,\underline{R}\,,\underline{S\,P}\,,\underline{Q\,R}\,,\underline{S\,P\,Q\,R}\,\big\}$$

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

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

(b) Determinare tutti gli atomi e tutti gli elementi $\vee$–irriducibili del reticolo $\mathbb{F}$.

(c) Esiste una $\vee$–fattorizzazione non ridondante in *fattori* $\vee$*–irriducibili* per l'elemento $\underline{S\,P\,Q\,R}$ nel reticolo $\mathbb{F}$? 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 $\underline{S\,P\,Q\,R}$ nel reticolo $\mathbb{F}$? 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 $\big(\mathbb{F}\,;\subseteq\big)$ sia un'algebra di Boole oppure no.

[2] Dati i due numeri interi 228 e 495, calcolare:

(a) il $\mathrm{M.C.D.}(228,495)$;

(b) una identità di Bézout per $\mathrm{M.C.D.}(228,495)$;

(c) il $\mathrm{m.c.m.}(228,495)$.

(continua...)

[3] Si consideri il polinomio booleano

$$\begin{aligned} q(h,k,\ell\,) \;:=\; & \Big(\big(\big(h' \vee 0 \vee h \big)' \vee \big(k'' \vee \ell \vee k \,\big) \big) \wedge \big(\ell \vee 1' \vee h \,\big)' \Big) \vee \\ & \vee \Big(\big(\ell'' \vee h \vee \ell \,\big) \wedge \big(\ell' \vee k'' \vee 0 \vee h'' \vee k \,\big) \Big)' \end{aligned}$$

(a) Calcolare la *Forma Normale Disgiuntiva* di $q(h,k,\ell\,)$.

(b) Calcolare una *forma minimale* di $q(h,k,\ell\,)$.

[4] *(a)* Calcolare il *minimo* valore di $x \in \mathbb{Z}_{\geq 0}$ tale che $7\,x \equiv 49^{29618} \pmod{77}$.

(b) Nell'anello $\mathbb{Z}_{77}$ degli interi modulo 77, determinare se esista la classe $[7]_{77}^{-1}$ inversa della classe $[7]_{77}$. In caso negativo si spieghi perché la classe inversa non esista; in caso affermativo si calcoli esplicitamente tale classe inversa.

(c) Nell'anello $\mathbb{Z}_{11}$ degli interi modulo 11, determinare se esista la classe $[7]_{11}^{-1}$ inversa della classe $[7]_{11}$. 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 $Y := \{D, N, A\}$. Si consideri poi in $\mathbb{V}_I$ la relazione $\lessdot$ definita da

$$\mathcal{P}_1 \lessdot \mathcal{P}_2 \quad \Longleftrightarrow \quad \begin{array}{c} \text{“}\textit{la parola } \mathcal{P}_1 \textit{ contiene al più tante lettere} \\ \textit{di } Y \textit{ quante ne contiene la parola } \mathcal{P}_2 \text{”} \end{array}$$

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

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

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

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

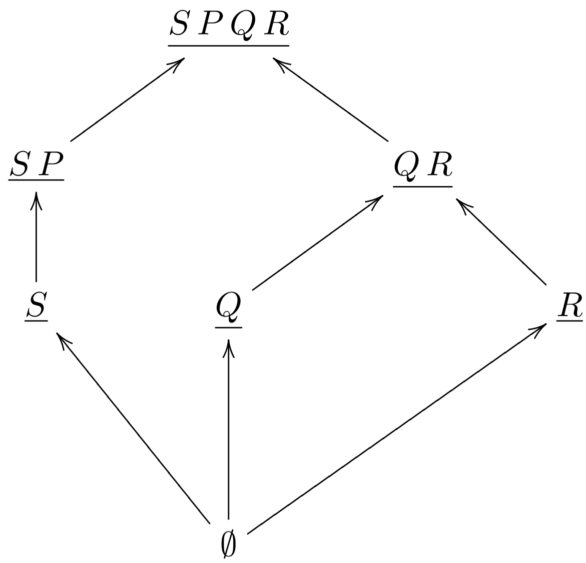
(d) Descrivere esplicitamente le quattro classi di $\lessdot\!\!\gtrdot$ –equivalenza $[DADO]_{\lessdot\!\gtrdot}$, $[TUBO]_{\lessdot\!\gtrdot}$, $[NANO]_{\lessdot\!\gtrdot}$ e $[ORDE]_{\lessdot\!\gtrdot}$.

— ⋆ —

(continua...)

SOLUZIONI

[1] — Per comodità di visualizzazione disegnamo qui di seguito il *diagramma di Hasse* dell'insieme ordinato $\big(\mathbb{F}\,;\subseteq\big)$, che a priori non è necessario (e infatti non è richiesto...). Tale diagramma è



(a) Ovviamente, in tutti i "casi banali", cioè quelli in cui sia $a \subseteq b$ oppure $a \subseteq b$, abbiamo che esiste $\sup\big(\{a,b\}\big) = a$ e $\inf\big(\{a,b\}\big) = b$ se $b \subseteq a$ mentre invece $\sup\big(\{a,b\}\big) = b$ e $\inf\big(\{a,b\}\big) = a$ se $a \subseteq b$. Per ogni altro caso (non banale) possibile, direttamente dall'analisi del diagramma di Hasse, notiamo che esistono sempre $\sup\big(\{a,b\}\big)$ e $\inf\big(\{a,b\}\big)$, dati esplicitamente da

$$\sup\big(\{\underline{S},\underline{Q}\}\big) = \underline{SPQR}\,, \quad \sup\big(\{\underline{Q},\underline{R}\}\big) = \underline{QR}\,, \quad \sup\big(\{\underline{S},\underline{R}\}\big) = \underline{SPQR}$$
$$\sup\big(\{\underline{S},\underline{QR}\}\big) = \underline{SPQR} \quad , \quad \sup\big(\{\underline{SP},\underline{Q}\}\big) = \underline{SPQR}$$
$$\sup\big(\{\underline{SP},\underline{R}\}\big) = \underline{SPQR} \quad , \quad \sup\big(\{\underline{SP},\underline{QR}\}\big) = \underline{SPQR}$$
$$\inf\big(\{\underline{S},\underline{Q}\}\big) = \emptyset\,, \quad \inf\big(\{\underline{Q},\underline{R}\}\big) = \emptyset\,, \quad \inf\big(\{\underline{S},\underline{R}\}\big) = \emptyset$$
$$\inf\big(\{\underline{S},\underline{QR}\}\big) = \emptyset \quad , \quad \inf\big(\{\underline{SP},\underline{Q}\}\big) = \emptyset$$
$$\inf\big(\{\underline{SP},\underline{R}\}\big) = \emptyset \quad , \quad \inf\big(\{\underline{SP},\underline{QR}\}\big) = \emptyset$$

Così concludiamo che l'insieme ordinato $\big(\mathbb{F}\,;\subseteq\big)$ è effettivamente un reticolo.

NOTA: È opportuno sottolineare che, in generale, a priori *non possiamo sapere se* $\sup\big(\{a,b\}\big) = a \cup b$ né se $\inf\big(\{a,b\}\big) = a \cap b$, bench'e la relazione d'ordine sia l'inclusione! In effetti, dalla tavola qui sopra possiamo osservare che si ha $\inf\big(\{a,b\}\big) = a \cap b$ per ogni $a, b \in \mathbb{F}$ mentre invece $\sup\big(\{a,b\}\big) \neq a \cup b$ in tutti i casi su esposti tranne il primo e l'ultimo. Di fatto, questa (apparente) "anomalia" si verifica proprio perché si tratta di casi di elementi $a, b \in \mathbb{F}$ per i quali $a \cup b \notin \mathbb{F}$.

(b) Il minimo del reticolo $\mathbb{F}$ è $\emptyset$, quindi gli *atomi* — che, per definizione, sono gli elementi che coprono il minimo — sono $\underline{S}$, $\underline{Q}$, $\underline{R}$. Tutti questi sono ovviamente $\vee$*–irriducibili*; in aggiunta, gli unici altri elementi $\vee$–irriducibili sono quello "banale", cioè il minimo $\emptyset$, e anche $\underline{SP}$.

(c) Siccome il reticolo $\mathbb{F}$ è finito, sicuramente esiste (almeno) una $\vee$–fattorizzazione (non ridondante) in $\vee$–irriducibili per ogni suo elemento, quindi anche per $\underline{SPQR}$. Analizzando direttamente il diagramma di Hasse, troviamo che *tutte le possibili* $\vee$*–fattorizzazioni non ridondanti in* $\vee$*–irriducibili per questo elemento sono date da*

$$\underline{SPQR} = \underline{SP} \vee \underline{Q} \vee \underline{R} \quad , \qquad \underline{SPQR} = \underline{S} \vee \underline{Q} \vee \underline{R}$$

$$\underline{SPQR} = \underline{SP} \vee \underline{Q} \quad , \qquad \underline{SPQR} = \underline{SP} \vee \underline{R}$$

$$\underline{SPQR} = \underline{S} \vee \underline{Q} \quad , \qquad \underline{SPQR} = \underline{S} \vee \underline{R}$$

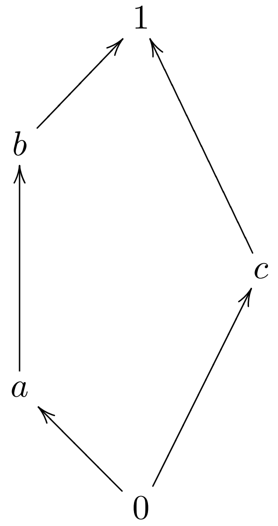
(d) A priori, una $\vee$–fattorizzazione (non ridondante) in *atomi* di $\underline{SPQR}$ potrebbe esistere oppure no, diversamente da quanto possiamo dire per una fattorizzazione in $\vee$–irriducibili; in ogni caso, dato che ogni atomo è sempre $\vee$–irriducibile, un'eventuale $\vee$–fattorizzazione (non ridondante) in atomi sarebbe una particolare $\vee$–fattorizzazione (non ridondante) in $\vee$–irriducibili, che abbiamo trattato nel precedente punto *(c)*. Così analizzando quanto già trovato al punto *(c)* osserviamo che tra le sei $\vee$–fattorizzazioni (non ridondanti) in $\vee$–irriducibili di $\underline{JQKA}$ lì elencate troviamo che *esistono esattamente tre* $\vee$*–fattorizzazioni non ridondanti di* $\underline{SPQR}$ *in atomi, date da*

$$\underline{SPQR} = \underline{S} \vee \underline{Q} \vee \underline{R} \quad , \quad \underline{SPQR} = \underline{S} \vee \underline{Q} \quad , \quad \underline{SPQR} = \underline{S} \vee \underline{R}$$

(e) L'insieme $\mathbb{F}$ è finito, con esattamente 7 elementi. Ora, come conseguenza del *Teorema di Rappresentazione di Stone* è noto 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 $n \in \mathbb{N}$. Siccome $|\mathbb{F}| = 7$ *non è una potenza di 2*, possiamo concludere che $\big(\mathbb{F}\,;\subseteq\big)$ *non è un'algebra di Boole.* In particolare si osservi che con questo metodo non c'è neanche bisogno di analizzare come sia fatta la relazione d'ordine fissata in $\mathbb{F}$: qualunque essa sia, la conclusione sarà sempre la stessa, perché dipende esclusivamente da una proprietà insiemistica di $\mathbb{F}$ stesso.

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

Ricordiamo che, per definizione, un reticolo è detto *algebra di Boole* se e soltanto se è limitato, distributivo e complementato. Ora, il reticolo $\mathbb{F}$ è limitato, con minimo $\emptyset$ e massimo $\underline{SPQR}$. D'altronde, dall'analisi del diagramma di Hasse deduciamo che *il reticolo* $\big(\mathbb{F}\,;\subseteq\big)$ *non è distributivo.* Infatti, ricordiamo che *un reticolo è distributivo se e soltanto se non contiene nessun sottoreticolo che sia isomorfo al* *reticolo* $\mathfrak{N}_5$, dove il reticolo indicato con $\mathfrak{N}_5$ è quello rappresentato dal diagramma di Hasse



Ora, il reticolo $\big(\mathbb{F}\,;\subseteq\big)$ contiene ben *sette* sottoreticoli isomorfi al reticolo $\mathfrak{N}_5$, precisamente

$$\begin{array}{l}
\textit{quattro} \text{ di tipo } \ \mathbb{E}'_{X,Y} := \big\{\emptyset\,,\underline{X}\,,\underline{Q\,R}\,,\underline{Y}\,,\underline{S\,P\,Q\,R}\,\big\} \quad \forall\ \underline{X}\in\big\{\underline{Q}\,,\underline{R}\,\big\},\ \underline{Y}\in\big\{\underline{S}\,,\underline{S\,P}\big\} \\
\text{ e isomorfismo } \quad \mathbb{E}'_{X,Y} \hookrightarrow\!\!\!\!\rightarrow \mathfrak{N}_5 \ , \quad \emptyset\mapsto 0\,,\ \underline{X}\mapsto a\,,\ \underline{Q\,R}\mapsto b\,,\ \underline{Y}\mapsto c\,,\ \underline{S\,P\,Q\,R}\mapsto 1 \\
\textit{tre} \text{ di tipo } \ \mathbb{E}''_Z := \big\{\emptyset\,,\underline{Z}\,,\underline{S}\,,\underline{S\,P}\,,\underline{S\,P\,Q\,R}\,\big\} \qquad \forall\ \ \underline{Z}\in\big\{\underline{Q}\,,\underline{R}\,,\underline{Q\,R}\big\} \\
\quad \text{ e isomorfismo } \quad \mathbb{E}''_Z \hookrightarrow\!\!\!\!\rightarrow \mathfrak{N}_5 \ , \quad \emptyset\mapsto 0\,,\ \underline{S}\mapsto a\,,\ \underline{S\,P}\mapsto b\,,\ \underline{Z}\mapsto c\,,\ \underline{S\,P\,Q\,R}\mapsto 1
\end{array}$$

per cui possiamo concludere che il reticolo $\big(\mathbb{F}\,;\subseteq\big)$ non è distributivo.

Da un altro punto di vista, osserviamo che $\big(\mathbb{F}\,;\subseteq\big)$ è *complementato*, poiché ogni elemento ha un complemento. D'altra parte, ci sono casi in cui tale complemento non è unico; precisamente, la situazione è la seguente:

$$\begin{array}{c}
\emptyset \ \text{ ha come complemento (unico) } \ \underline{S\,P\,Q\,R} \\
\underline{S} \ \text{ ha come complementi } \ \underline{Q}\ , \ \ \underline{R} \ \text{ e } \ \underline{Q\,R} \\
\underline{Q} \ \text{ ha come complementi } \ \underline{S} \ \text{ e } \ \underline{S\,P} \\
\underline{R} \ \text{ ha come complementi } \ \underline{S} \ \text{ e } \ \underline{S\,P} \\
\underline{S\,P} \ \text{ ha come complementi } \ \underline{Q}\ , \ \ \underline{R} \ \text{ e } \ \underline{Q\,R} \\
\underline{Q\,R} \ \text{ ha come complementi } \ \underline{S} \ \text{ e } \ \underline{S\,P} \\
\underline{S\,P\,Q\,R} \ \text{ ha come complemento (unico) } \ \emptyset
\end{array}$$

Ma da questo ricaviamo di nuovo che il reticolo non è distributivo, perché in qualsiasi reticolo distributivo il complemento di un elemento, se esiste, è sempre unico.

[2] — *(a)* Calcoliamo $\text{M.C.D.}(228, 495)$ tramite l'algoritmo euclideo delle divisioni successive. I calcoli diretti ci danno

$$\begin{aligned} 228 &= 495 \cdot 0 + 228 \\ 495 &= 228 \cdot 2 + 39 \\ 228 &= 39 \cdot 5 + 33 \\ 39 &= 33 \cdot 1 + 6 \\ 33 &= 6 \cdot 5 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned} \tag{1}$$

da cui ricaviamo che il M.C.D.(228,495) richiesto è l'ultimo resto non nullo in questa successione di divizioni con resto, cioè $\text{M.C.D.(228,495)} = 3$.

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

$$\begin{aligned} 228 + 495 \cdot (-0) &= 228 \\ 495 + 228 \cdot (-2) &= 39 \\ 228 + 39 \cdot (-5) &= 33 \\ 39 + 33 \cdot (-1) &= 6 \\ 33 + 6 \cdot (-5) &= 3 \end{aligned} \qquad \text{o anche} \qquad \begin{aligned} 228 &= 228 + 495 \cdot (-0) \\ 39 &= 495 + 228 \cdot (-2) \\ 33 &= 228 + 39 \cdot (-5) \\ 6 &= 39 + 33 \cdot (-1) \\ 3 &= 33 + 6 \cdot (-5) \end{aligned}$$

A questo punto sostituiamo nell'ultima identità l'espressione di 6 data dalla penultima identità, poi sostituiamo nel risultato l'espressione di 33 data dalla terzultima identità, e così via, così da ottenere — per sostituzioni successive — la seguente catena di identità:

$$\begin{aligned} 3 &= 33 + 6 \cdot (-5) = 33 + \big(39 + 33 \cdot (-1)\big) \cdot (-5) = 39 \cdot (-5) + 33 \cdot 6 = \\ &= 39 \cdot (-5) + \big(228 + 39 \cdot (-5)\big) \cdot 6 = 228 \cdot 6 + 39 \cdot (-35) = \\ &= 228 \cdot 6 + \big(495 + 228 \cdot (-2)\big) \cdot (-35) = 495 \cdot (-35) + 228 \cdot 76 = \\ &= 495 \cdot (-35) + \big(228 + 495 \cdot (-0)\big) \cdot 76 = 228 \cdot 76 + 495 \cdot (-35) \end{aligned}$$

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

$$\text{M.C.D.}(228, 495) = 3 = 228 \cdot 76 + 495 \cdot (-35)$$

che è una identità di Bézout per $\text{M.C.D.}(228, 495)$, come richiesto.

(c) Come conseguenza del *Teorema di Fattorizzazione Unica* per i numeri interi abbiamo che $\text{M.C.D.}(228, 495)$ e $\text{m.c.m.}(228, 495)$ sono collegati dall'identità

$$\text{M.C.D.}(228, 495) \cdot \text{m.c.m.}(228, 495) = 228 \cdot 495$$

da cui ricaviamo $\mathrm{m.c.m.}(228,495)$ con la formula

$$\begin{aligned} \mathrm{m.c.m.}(228,495) \;&=\; \frac{228\cdot 495}{\mathrm{M.C.D.}(228,495)} \;=\; \frac{228\cdot 495}{3} \;=\\ &=\; 228\cdot 165 \;=\; 76\cdot 495 \;=\; 37620 \end{aligned}$$

così che, in conclusione, abbiamo $\mathrm{m.c.m.}(228,495) = 37620$.

[3] — Per un qualsiasi polinomio booleano, sia la *Forma Normale Disgiuntiva* — che indicheremo nel seguito con *F.N.D.* — sia una *forma minimale* — che indicheremo con *f.m.* — sono particolari *somme di prodotti equivalenti al polinomio assegnato*. Pertanto, per cominciare operiamo sul polinomio assegnato $q(h,k,\ell\,)$ per "trasformarlo" in un altro ad esso equivalente che sia scritto però come somma di prodotti.

A partire dall'espressione iniziale di $q(h,k,\ell\,)$ otteniamo

$$\begin{aligned} q(h,k,\ell\,) \;:=\; &\Big(\big(\big(\,h'\vee 0\vee h\,\big)'\vee\big(\,k''\vee\ell\vee k\,\big)\big)\wedge\big(\,\ell\vee 1'\vee h\,\big)'\Big)\vee\\ &\vee\Big(\big(\,\ell''\vee h\vee\ell\,\big)\wedge\big(\,\ell'\vee k''\vee 0\vee h''\vee k\,\big)\Big)' \;\sim\\ \sim\; &\Big(\big(\big(\,h'\vee h\,\big)'\vee\big(\,k\vee\ell\vee k\,\big)\big)\wedge\big(\,\ell\vee 0\vee h\,\big)'\Big)\vee\\ &\vee\Big(\big(\,\ell\vee h\vee\ell\,\big)\wedge\big(\,\ell'\vee k\vee 0\vee h\vee k\,\big)\Big)' \;\sim\\ \sim\; &\Big(\big(1'\vee\big(\,k\vee\ell\,\big)\big)\wedge\big(\,h\vee\ell\,\big)'\Big)\;\vee\;\Big(\big(\,h\vee\ell\,\big)\wedge\big(\,h\vee k\vee\ell'\,\big)\Big)' \;\sim\\ \sim\; &\Big(\big(\,k\vee\ell\,\big)\wedge\big(\,h\vee\ell\,\big)'\Big)\;\vee\;\Big(\big(\,h\vee\ell\,\big)\wedge\big(\,h\vee k\vee\ell'\,\big)\Big)' \end{aligned}$$

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

$$\begin{aligned} q(h,k,\ell\,) \;\sim\; &\Big(\big(\,k\vee\ell\,\big)\wedge\big(\,h\vee\ell\,\big)'\Big)\;\vee\;\Big(\big(\,h\vee\ell\,\big)\wedge\big(\,h\vee k\vee\ell'\,\big)\Big)' \;\sim\\ \sim\; &\Big(\big(\,k\vee\ell\,\big)\wedge\big(\,h\vee\ell\,\big)'\Big)\;\vee\;\big(\,h\vee\ell\,\big)'\;\vee\;\big(\,h\vee k\vee\ell'\,\big)' \end{aligned}$$

Adesso applichiamo la legge di assorbimento $\big(A\wedge B\,\big)\vee B\;\sim\;B$ al caso $A:=\big(\,k\vee\ell\,\big)$ e $B:=\big(\,h\vee\ell'\,\big)'$, e così otteniamo

$$\begin{aligned} q(h,k,\ell\,) \;\sim\; &\Big(\big(\,k\vee\ell\,\big)\wedge\big(\,h\vee\ell\,\big)'\Big)\;\vee\;\big(\,h\vee\ell\,\big)'\;\vee\;\big(\,h\vee k\vee\ell'\,\big)' \;\sim\\ \sim\; &\big(\,h\vee\ell\,\big)'\;\vee\;\big(\,h\vee k\vee\ell'\,\big)' \end{aligned}$$

Ora applichiamo l'altra legge di De Morgan, nelle due forme $\big(A \vee B\big)' \sim A' \wedge B'$ e $\big(P \vee Q \vee R\big)' \sim P' \wedge Q' \wedge R'$, il che ci dà

$$q(h,k,\ell\,) \;\sim\; \big(\,h \vee \ell\,\big)' \,\vee\, \big(\,h \vee k \vee \ell'\,\big)' \;\sim\; \big(\,h' \wedge \ell'\,\big) \,\vee\, \big(\,h' \wedge k' \wedge \ell''\,\big)$$

cioè in conclusione (tenendo conto che $\ell'' \sim \ell\,$)

$$q(h,k,\ell\,) \;\sim\; \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \tag{2}$$

che è appunto un'espressione del tipo cercato: infatti il membro di destra è un polinomio booleano equivalente a $q(h,k,\ell\,)$ che è espresso da una somma di prodotti.

(a) Per calcolare la F.N.D. di $q(h,k,\ell\,)$ cominciamo dalla sua espressione equivalente data in (2), che è già una somma di prodotti fondamentali non ridondante, e in essa "completiamo" tutti quei prodotti che non siano già completi, per poi eliminare eventuali "ridondanze". Nella somma sono presenti due prodotti, di cui soltanto il primo non è completo — perché in esso non figura la variabile k —- e il suo "completamento" è chiaramente

$$h' \wedge \ell' \;\sim\; \big(h' \wedge k \wedge \ell'\,\big) \vee \big(h' \wedge k' \wedge \ell'\,\big)$$

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

$$q(h,k,\ell\,) \sim \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \sim \big(h' \wedge k \wedge \ell'\,\big) \vee \big(h' \wedge k' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big)$$

e così in conclusione *la F.N.D. di* $q(h,k,\ell\,)$ *è*

$$q(h,k,\ell\,) \;\sim\; \big(h' \wedge k \wedge \ell'\,\big) \vee \big(h' \wedge k' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \tag{3}$$

(b) Per trovare una f.m. di $q(h,k,\ell\,)$ partiamo dalla sua espressione equivalente come somma di prodotti data in (2) e applichiamo ad essa il *metodo del consenso*. Come inizio, i due prodotti nella somma in (2) sono in consenso — dato che differiscono solamente per la variabile ℓ — e quindi dalla (2) stessa otteniamo

$$\begin{aligned} q(h,k,\ell\,) &\sim \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \sim \\ &\sim \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \vee \big(\,h' \wedge h' \wedge k'\,\big) \sim \\ &\sim \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k' \wedge \ell\,\big) \vee \big(\,h' \wedge k'\,\big) \sim \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k'\,\big) \end{aligned}$$

dove nell'ultimo passaggio abbiamo sfruttato la legge di assorbimento

$$\big(P \wedge Q\,\big) \vee P \;\sim\; P \qquad \text{per} \quad P := h' \wedge k' \quad \text{e} \quad Q := \ell$$

Dunque per comcludere abbiamo

$$q(h,k,\ell\,) \;\sim\; \big(\,h' \wedge \ell'\,\big) \vee \big(\,h' \wedge k'\,\big) \tag{4}$$

e l'ultima espressione è una somma di prodotti tra i quali non c'è consenso: allora l'algoritmo basato sul metodo del consenso si arresta, e *questa somma di prodotti che abbiamo ottenuto è la somma di tutti gli implicanti primi di* $q(h,k,\ell\,)$.

Adesso osserviamo che nella (4) non possiamo scartare nessuno dei due prodotti presenti nella somma di destra: infatti, confrontando la (4) con la (3) troviamo che

— il prodotto completo $\big(\,h'\wedge k\wedge\ell'\,\big)$ in (3) viene dal completamento del prodotto $\big(\,h'\wedge\ell'\,\big)$, ma non da quello di $\big(\,h'\wedge k'\,\big)$;

— il prodotto completo $\big(h'\wedge k'\wedge\ell\big)$ in (3) viene dal completamento del prodotto $\big(\,h'\wedge k'\,\big)$, ma non da quello di $\big(\,h'\wedge\ell'\,\big)$.

Dunque possiamo concludere che *una f.m. di* $q(h,k,\ell\,)$ *è data dalla (4)*: in aggiunta, poiché quest'ultima è anche la somma di tutti gli implicanti primi di $q(h,k,\ell\,)$, essa è anche *l'unica f.m. possibile di* $q(h,k,\ell\,)$.

[4] — *(a)* Come primo passo, possiamo osservare che l'equazione congruenziale iniziale

$$7\,x \;\equiv\; 49^{29618} \quad \big(\bmod 77\big)$$

ammette soluzioni, perché $7 \;=\; \text{M.C.D.}(7,77)\,\big|\,49^{29618}$, cioè il M.C.D. tra il coefficiente dell'incognita e il modulo divide il termine noto; inoltre, a questo punto possiamo semplificare l'equazione stessa dividendo tutti i suoi termini per $7 = \text{M.C.D.}(7,77)$, così da ottenere l'equazione congruenziale equivalente

$$\frac{7}{7}\,x \;\equiv\; \frac{49^{29618}}{7} \quad \left(\bmod \frac{77}{7}\right)$$

che si riscrive, osservando tra l'altro che $\dfrac{49^{29618}}{7} \;=\; \dfrac{\big(7^2\big)^{29618}}{7} \;=\; \dfrac{7^{2\cdot 29618}}{7} \;=\; \dfrac{7^{59236}}{7} \;=\; 7^{59236-1} \;=\; 7^{59235}$, nella forma

$$x \;\equiv\; 7^{59235} \quad \big(\bmod 11\big)$$

Quest'ultima equazione congruenziale è scritta "in forma già risolta": le sue soluzioni sono tutti e soli i numeri interi che formano la classe di congruenza $\big[7^{59235}\big]_{11}$. Il nostro obiettivo allora sarà semplicemente determinare il *minimo* valore di $x\in\mathbb{Z}_{\geq 0}$ che appartenga a $\big[7^{59235}\big]_{11}$, cioè dobbiamo trovare il minimo numero non negativo in questa classe di congruenza: in particolare, questo equivale a trovare l'unico rappresentante — che di sicuro esiste! — di questa classe che sia contenuto nell'intervallo da 0 a $11-1=10$. Facendo uso della notazione $\overline{z} := [z]_{11}$, dobbiamo dunque trovare l'unico valore di x tale che $\overline{x} \;=\; \overline{7^{59235}}$ e $0\leq x\leq 10$.

Dovendo calcolare $\overline{7^{59235}}$ nell'anello $\mathbb{Z}_{11}$ delle classi resto modulo 131, per prima cosa notiamo che $\overline{7^{59235}} = \overline{7}^{\,59235}$ è una potenza di $\overline{7}$. A seguire osserviamo che $\text{M.C.D.}(7,11) = 1$, perciò grazie al *Teorema di Eulero* sappiamo che $\overline{7}^{\,\varphi(11)} = \overline{1}$, dove φ è la funzione di Eulero. Da questo, scrivendo l'esponente 59235 nella forma $59235 = \varphi(11) \cdot q + r$ con $0 \leq r < \varphi(11)$ — cioè facendo la *divisione con resto* di 59235 per $\varphi(11)$ — troveremo

$$\overline{7^{59235}} = \overline{7}^{\,59235} = \overline{7}^{\,\varphi(11) \cdot q + r} = \left(\overline{7}^{\,\varphi(11)}\right)^q \cdot \overline{7}^{\,r} = \overline{1}^{\,q} \cdot \overline{7}^{\,r} = \overline{7}^{\,r} \tag{5}$$

da cui emerge che in effetti nella divisione di 59235 per $\varphi(11)$ conta soltanto conoscere il resto, mentre il quoziente è irrilevante — in altri termini, *ci interessa soltanto conoscere la classe resto di* 59235 *modulo* $\varphi(11)$.

A questo punto per esplicitare la (5) osserviamo che $\varphi(11) = 11 - 1 = 10$, quindi poi andando a dividere 59235 per $\varphi(11) = 10$ troviamo $59235 = 10 \cdot 5923 + 5$, così che il resto cercato è $r = 5$; dunque la (5) ci dà

$$\overline{7^{59235}} = \overline{7}^{\,r} = \overline{7}^{\,5}$$

Infine, per calcolare $\overline{7}^{\,5}$ notiamo che

$$\overline{7}^{\,2} = \overline{49} = \overline{5} \qquad \Longrightarrow \qquad \overline{7}^{\,3} = \overline{7}^{\,2} \cdot \overline{7} = \overline{5} \cdot \overline{7} = \overline{35} = \overline{2}$$

e quindi

$$\overline{7}^{\,5} = \overline{7}^{\,2} \cdot \overline{7}^{\,3} = \overline{5} \cdot \overline{2} = \overline{10}$$

così che in conclusione otteniamo che *il valore x richiesto è $x = 10$*.

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

Applicando quanto appena ricordato al caso $n := 77$ e $a := 7$ otteniamo che $\text{M.C.D.}(7,77) = 7 \neq 1$, e quindi concludiamo che *non esiste in $\mathbb{Z}_{77}$ la classe $[7]_{77}^{-1}$ inversa della classe $[7]_{77}$*.

(c) Applicando l'analisi fatta per il punto *(b)* al caso $n := 11$ e $a := 7$ abbiamo che $\text{M.C.D.}(7,11) = 1$, e quindi *esiste in $\mathbb{Z}_{11}$ la classe $\overline{7}^{\,-1} := [7]_{11}^{-1}$ inversa della classe $\overline{7} := [7]_{11}$*. Questa inversa $\overline{7}^{\,-1} := [7]_{11}^{-1}$ è l'unica soluzione dell'equazione modulare $\overline{7}\,\overline{x} = \overline{1}$ in $\mathbb{Z}_{11}$, che a sua volta è equivalente all'equazione congruenziale (in $\mathbb{Z}$) $7\,x \equiv 1 \pmod{11}$, che infine è equivalente all'equazione diofantea

$$7\,x + 11\,y = 1$$

e quindi procediamo a risolvere quest'ultima. È da notare che questo equivale a trovare una identità di Bézout per $\text{M.C.D.}(7,11) = 1$, che è un problema del tutto simile a quanto già visto nell'esercizio [**2**]. Utilizzando l'algoritmo delle divisioni successive otteniamo

$$\begin{aligned} 7 &= 11 \cdot 0 + 7 \\ 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

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

$$\begin{aligned} 7 &= 7 + 11 \cdot (-0) \\ 4 &= 11 + 7 \cdot (-1) \\ 3 &= 7 + 4 \cdot (-1) \\ 1 &= 4 + 3 \cdot (-1) \end{aligned}$$

e infine per sostituzioni successive troviamo

$$\begin{aligned} 1 \;&=\; 4 + 3 \cdot (-1) \;=\; 4 + \big(7 + 4 \cdot (-1)\big) \cdot (-1) \;=\; 7 \cdot (-1) + 4 \cdot 2 \;= \\ &= 7 \cdot (-1) + \big(11 + 7 \cdot (-1)\big) \cdot 2 \;=\; 11 \cdot 2 + 7 \cdot (-3) \;= \\ &= 11 \cdot 2 + \big(7 + 11 \cdot (-0)\big) \cdot (-3) \;=\; 7 \cdot (-3) + 11 \cdot 2 \end{aligned}$$

da cui in conclusione $1 = 7 \cdot (-3) + 11 \cdot 2$ è un'identità di Bézout come richiesto, che ci dice che la coppia di interi $(-3, 2)$ è una soluzione dell'equazione diofantea $7 \cdot x + 11 \cdot y = 1$. Da quest'ultima si ottiene $1 \equiv 7 \cdot (-3) \;\big(\mathrm{mod}\ 11\big)$ — così che $x = -3$ è una soluzione dell'equazione congruenziale $7 \cdot x \equiv 1 \;\big(\mathrm{mod}\ 11\big)$ — e quindi $\overline{1} = \overline{7} \cdot \overline{(-3)}$ — così che $\overline{x} = \overline{-3} = -\overline{3} = \overline{8}$ è una soluzione (unica!) dell'equazione modulare $\overline{7} \cdot \overline{x} \equiv 1$ in $\mathbb{Z}_{11}$ — e quindi in definitiva *possiamo concludere che la classe inversa richiesta è* $\overline{7}^{\,-1} = \overline{8}$.

<u>*NOTA*</u>*:* In effetti, ai fini del calcolo della classe inversa sarebbe stato sufficiente anche trovare "a mano" che

$$\overline{7} \cdot \overline{8} \;=\; \overline{7 \cdot 8} \;=\; \overline{56} \;=\; \overline{11 \cdot 5 + 1} \;=\; \overline{11} \cdot \overline{5} + \overline{1} \;=\; \overline{0} \cdot \overline{5} + \overline{1} \;=\; \overline{1}$$

e da questo concludere che $\overline{7}^{\,-1}$ *esiste ed è pari a* $\overline{7}^{\,-1} = \overline{8}$. Tuttavia, questo sarebbe stato un metodo "di forza bruta" (del tipo "faccio dei calcoli, e prima o poi imbrocco 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)* In generale, una relazione si dice *di preordine* se è *riflessiva* e *transitiva*. Nel caso in esame, abbiamo:

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

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

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

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

$$\begin{aligned} \mathcal{P}' \lessdot \mathcal{P}'' &\implies \mathcal{P}' \textit{ contiene al più tante lettere di } Y \textit{ quante ne contiene } \mathcal{P}'' \\ \mathcal{P}'' \lessdot \mathcal{P}''' &\implies \mathcal{P}'' \textit{ contiene al più tante lettere di } Y \textit{ quante ne contiene } \mathcal{P}''' \end{aligned}$$

e allora confrontando le condizioni di destra abbiamo anche

$$\mathcal{P}' \textit{ contiene al più tante lettere di } Y \textit{ quante ne contiene } \mathcal{P}'''$$

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

Infine, una relazione si dice *di ordine* se è *riflessiva, transitiva* — dunque è di preordine — *e antisimmetrica*. Dato che la relazione $\lessdot$ 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 $\lessdot$ è *antisimmetrica* se per ogni $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$, *se* si ha $\mathcal{P}' \lessdot \mathcal{P}''$ e $\mathcal{P}'' \lessdot \mathcal{P}'$ *allora* si ha necessariamente $\mathcal{P}' = \mathcal{P}''$. Pertanto $\lessdot$ *non* sarà antisimmetrica se *non* vale questa proprietà, cioè se la condizione non è soddisfatta da almeno un paio di elementi $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$: dunque in conclusione dobbiamo dimostrare che *esistono* $\mathcal{P}', \mathcal{P}'' \in \mathbb{V}_I$ *tali che* $\mathcal{P}' \lessdot \mathcal{P}''$ *e* $\mathcal{P}'' \lessdot \mathcal{P}'$ *ma* $\mathcal{P}' \neq \mathcal{P}''$.

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

$$\begin{aligned} \mathcal{P}' \lessdot \mathcal{P}'' &\implies \mathcal{P}' \textit{ contiene al più tante lettere di } Y \textit{ quante ne contiene } \mathcal{P}'' \\ \mathcal{P}'' \lessdot \mathcal{P}' &\implies \mathcal{P}'' \textit{ contiene al più tante lettere di } Y \textit{ quante ne contiene } \mathcal{P}' \end{aligned}$$

e quindi confrontando le condizioni di destra abbiamo

$$\mathcal{P}' \text{ contiene tante lettere di } Y \text{ quante ne contiene } \mathcal{P}'' \tag{6}$$

Viceversa, se vale la (6) allora per definizione abbiamo che $\mathcal{P}' \lessdot \mathcal{P}''$ e $\mathcal{P}'' \lessdot \mathcal{P}'$. Pertanto, 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 $Y := \{D, N, A\}$. Ad esempio, scegliendo

$$\mathcal{P}' := \textit{ONDA} \quad , \qquad \mathcal{P}'' := \textit{DANNATO}$$

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

[5] Si considerino l'insieme $\mathbb{V}_I := \{\,\text{parole della lingua italiana}\,\}$ e l'insieme di lettere $Y := \{D, N, A\}$. Si consideri poi in $\mathbb{V}_I$ la relazione $\lessdot$ definita da

$$\mathcal{P}_1 \lessdot \mathcal{P}_2 \quad\Longleftrightarrow\quad \begin{array}{c} \text{“\textit{la parola} } \mathcal{P}_1 \text{ \textit{contiene al più tante lettere}} \\ \text{di } Y \text{ quante ne contiene la parola } \mathcal{P}_2\text{”} \end{array}$$

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

(b) Si dimostri che la relazione $\lessdot\!\gtrdot \; := \; \lessdot \cap \gtrdot \; = \; \lessdot \cap \lessdot^{-1}$ è una relazione di equivalenza in $\mathbb{V}_I$.

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

(d) Descrivere esplicitamente le quattro classi di $\lessdot\!\gtrdot$–equivalenza $[DADO]_{\lessdot\!\gtrdot}$, $[TUBO]_{\lessdot\!\gtrdot}$, $[NANO]_{\lessdot\!\gtrdot}$ e $[ORDE]_{\lessdot\!\gtrdot}$.

[..]

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

$$\nu \,:\, \mathbb{V}_I \longrightarrow \mathbb{N} \quad , \qquad \mathcal{P} \mapsto \nu(\mathcal{P}) := \Big| \big\{ \text{lettere di } \mathcal{P} \big\} \cap \Lambda \Big| \tag{7}$$

che associa ad ogni parola della lingua italiana il numero di lettere (senza ripetizioni) tra quelle di $\Lambda := \{F, C, R\}$ che essa contiene. La definizione della relazione $\rtimes$ può allora essere riscritta così:

$$\mathcal{P}_1 \rtimes \mathcal{P}_2 \quad\Longleftrightarrow\quad \nu(\mathcal{P}_1) \leq \nu(\mathcal{P}_2) \qquad\qquad \forall\; \mathcal{P}_1\,, \mathcal{P}_2 \in \mathbb{V}_I \tag{8}$$

Facendo uso di questa descrizione, i passaggi precedenti per dimostrare riflessività e transitività di $\rtimes$ 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 $\bowtie \,:=\, \rtimes \cap \ltimes \,=\, \rtimes \cap \rtimes^{-1}$ cominciamo osservando che, siccome la relazione $\rtimes$, è riflessiva e transitiva, anche la sua inversa $\ltimes \,:=\, \rtimes^{-1}$, è a sua volta riflessiva e transitiva. Ne segue che *anche* $\bowtie := \rtimes \cap \ltimes$ *è riflessiva e transitiva*: infatti,

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

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

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

$$\begin{aligned}
&\mathcal{P}' \bowtie \mathcal{P}'' \implies \mathcal{P}' \rtimes \cap \ltimes \mathcal{P}'' \implies \mathcal{P}' \rtimes \mathcal{P}'' \quad \text{e} \quad \mathcal{P}' \ltimes \mathcal{P}'' \implies \\
&\qquad \implies \mathcal{P}' \rtimes \mathcal{P}'' \quad \text{e} \quad \mathcal{P}' \rtimes^{-1} \mathcal{P}'' \implies \mathcal{P}' \rtimes \mathcal{P}'' \quad \text{e} \quad \mathcal{P}'' \rtimes \mathcal{P}' \implies \\
&\qquad\qquad \implies \mathcal{P}'' \rtimes \mathcal{P}' \quad \text{e} \quad \mathcal{P}' \rtimes \mathcal{P}'' \implies \mathcal{P}'' \rtimes \mathcal{P}' \quad \text{e} \quad \mathcal{P}'' \ltimes^{-1} \mathcal{P}' \implies \\
&\qquad\qquad\qquad \implies \mathcal{P}'' \rtimes \mathcal{P}' \quad \text{e} \quad \mathcal{P}'' \ltimes \mathcal{P}' \implies \mathcal{P}'' \rtimes \cap \ltimes \mathcal{P}' \implies \mathcal{P}'' \bowtie \mathcal{P}'
\end{aligned}$$

cioè in sintesi $\mathcal{P}' \bowtie \mathcal{P}'' \implies \mathcal{P}'' \bowtie \mathcal{P}'$, 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

$$\nu : \mathbb{V}_I \longrightarrow \mathbb{N} \quad , \qquad \mathcal{P} \mapsto \nu(\mathcal{P}) := \Big| \big\{ \text{lettere di } \mathcal{P} \big\} \cap \Lambda \Big|$$

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

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

cioè in breve

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

In particolare, dalla (9) vediamo che la $\bowtie$ 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 sicuramente una equivalenza.

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

(c) Ricordiamo che l'insieme quoziente $\mathbb{V}_I \big/ \bowtie$ è l'insieme i cui elementi sono le classi di $\bowtie$–equivalenza in $\mathbb{V}_I$. Perciò determinare la cardinalità $\Big| \mathbb{V}_I \big/ \bowtie \Big|$ significa determinare il numero totale di tali classi di $\bowtie$–equivalenza.

Grazie alla caratterizzazione della relazione $\bowtie$ data in (9), sappiamo che due elementi di $\mathbb{V}_I$ sono $\bowtie$–equivalenti se e soltanto se hanno lo stesso valore per la funzione ν: perciò abbiamo una e una sola classe di $\bowtie$–equivalenza per ogni valore della funzione ν, e viceversa — in altre parole, le classi di $\bowtie$–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 $\Lambda := \{F, C, R\}$ 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 $\bowtie$–equivalenza sono esattamente *quattro*. Perciò la soluzione del problema posto è che *la cardinalità dell'insieme quoziente* $\left|\, \mathbb{V}_I \big/ \!\bowtie \,\right|$ *è precisamente* $\left|\, \mathbb{V}_I \big/ \!\bowtie \,\right| = 4$.

<u>*NOTA*</u>*:* L'analisi appena svolta dipende dal fatto che $\bowtie$ coincide con la relazione di equivalenza ρ_ν canonicamente associata alla funzione ν: infatti la stessa analisi si può applicare allo stesso modo ogni volta che si debba calcolare l'insieme quoziente $A \big/ \eta = A \big/ \rho_f$ relativamente ad una relazione di equivalenza $\eta = \rho_f$ associata ad una funzione $f : A \longrightarrow B$, per la quale avremo $\left| A \big/ \eta \right| = \left| A \big/ \rho_f \right| = \left| Im(f) \right|$.

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

$$Im(\nu) \lhook\joinrel\twoheadrightarrow \mathbb{V}_I \big/ \!\bowtie \quad , \quad n \mapsto \nu^{-1}(n) := \big\{ \mathcal{P} \in \mathbb{V}_I \,\big|\, \nu(\mathcal{P}) = n \big\} \qquad \forall\; n \in Im(\nu)$$

Pertanto, le quattro classi di $\bowtie$–equivalenza in $\mathbb{V}_I$ sono

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

Alla luce di questo, abbiamo allora

$$[AFTA]_{\bowtie} = C_1 \quad , \quad [CERO]_{\bowtie} = C_2 \quad , \quad [SETA]_{\bowtie} = C_0 \quad , \quad [RIGO]_{\bowtie} = C_1$$

cioè esplicitamente

$$\begin{aligned}
[AFTA]_{\bowtie} &= \big\{ \text{parole di } \mathbb{V}_I \text{ contenenti esattamente una lettera tra } F,\, C \text{ e } R \big\} \\
[CERO]_{\bowtie} &= \big\{ \text{parole di } \mathbb{V}_I \text{ contenenti esattamente due lettere tra } F,\, C \text{ e } R \big\} \\
[SETA]_{\bowtie} &= \big\{ \text{parole di } \mathbb{V}_I \text{ che non contengono nessuna lettera tra } F,\, C \text{ e } R \big\} \\
[RIGO]_{\bowtie} &= \big\{ \text{parole di } \mathbb{V}_I \text{ contenenti esattamente una lettera tra } F,\, C \text{ e } R \big\}
\end{aligned}$$

<u>*NOTA*</u>*:* Anche in questo caso, l'analisi appena svolta dipende esclusivamente dal fatto che $\bowtie$ coincide con la relazione di equivalenza ρ_ν canonicamente associata alla funzione ν; e infatti la stessa analisi può essere applicata allo stesso modo ogni

volta che 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

$$C_v \; := \; f^{-1}(v) \; = \; \big\{\, a \in A \,\big|\, f(a) = v \,\big\} \qquad\qquad \forall \;\, v \in Im(f)$$