# I RETICOLI E IL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Sia P un insieme non vuoto. Una relazione d'ordine $\leq$ su P è una relazione riflessiva, antisimmetrica e transitiva. La coppia $(P,\leq)$ si dice *insieme parzialmente ordinato (p.o.).* Il *duale* di $(P,\leq)$ è l'insieme p.o. $(P,\geq)$, dove $\geq$ è la relazione duale di $\leq$ che è anch'essa una relazione d'ordine. Due elementi x,y di P si dicono *confrontabili* se risulta $x \leq y$ oppure $y \leq x$, in particolare $x \leq y$ e $x \neq y$ sarà indicato $x< y$. Un insieme parzialmente ordinato tale che ogni coppia di suoi elementi sia confrontabile si dice *totalmente ordinato* o *catena,* la *lunghezza di una catena* è il numero dei suoi elementi diminuito di una unità.

L'insieme $[a,b] = \{x\in P : a \leq x \leq b\}$ si dice *intervallo di estremi* a,b; se l'intervallo [a,b] ($a\neq b$) è costituito solo da a e b si dice che b *copre* a (o che a *è coperto da* b), in simboli $a <\bullet\, b$. Dati $x, y\in P$, si definisce *estremo inferiore di* x e y l'elemento inf(x,y) di P tale che

(I1) $\inf(x,y) \leq x$ e $\inf(x,y) \leq y$,

(I2) se $z\in P$, $z \leq x$ e $z \leq y$ allora $z \leq \inf(x,y)$.

Si definisce *estremo superiore di* x e y l'elemento sup(x,y) di P tale che

(S1) $x \leq \sup(x,y)$ e $y \leq \sup(x,y)$,

(S2) se $z\in P$, $x \leq z$ e $y \leq z$ allora $\sup(x,y) \leq z$.

Ovviamente l'estremo inferiore di x e y, se esiste, è unico, come pure è unico l'estremo superiore.

Siano $(P_1,\leq_1)$ e $(P_2,\leq_2)$ insiemi p.o., un *morfismo di insiemi p.o.* (o *funzione monotona*) è una applicazione $f$: $P_1 \rightarrow P_2$ tale che se $x \leq_1 y$ allora $f(x) \leq_2 f(y)$, quando il morfismo è biiettivo, ossia è un *isomorfismo,* i due insiemi p.o. si dicono *isomorfi.*

Un insieme parzialmente ordinato $(P,\leq)$ con 0 può essere rappresentato graficamente attraverso un diagramma (*diagramma di Hasse*) i cui punti corrispondono biunivocamente agli elementi di P in modo che per ogni coppia (x,y) di elementi distinti si abbia:

i) se $x \leq y$ allora il punto x è più in basso del punto y ,

ii) se y copre x allora i punti x ed y sono uniti da un segmento.

Il *prodotto* di due insiemi parzialmente ordinati $(P_1,\leq_1)$ e $(P_2,\leq_2)$ è l'insieme p.o $(P_1xP_2,\leq)$ dove la relazione d'ordine è definita da:

$$(x_1,x_2) \leq (y_1,y_2) : \text{se e solo se } x_1 \leq y_1 \text{ e } x_2 \leq y_2.$$

In generale data una famiglia di insiemi p.o $\{(P_i,\leq)\}_{i\in I}$, l' *insieme p.o. prodotto* $(\Pi_{i\in I} P_i,\leq)$ è definito da:

$$\{x_i\}_{i\in I}, \{y_i\}_{i\in I} \in \Pi_{i\in I} P_i,\ \{x_i\}_{i\in I} \leq \{y_i\}_{i\in I}: \text{ se e solo se } x_i \leq y_i \text{ per ogni } i \in I.$$

Si osservi che, se $(P, \leq)$ è un insieme p.o. e $X =\{x_1,\ldots,x_n\}$ un insieme con n elementi, è possibile definire una relazione d'ordine sull'insieme $P^X$ delle funzioni da X in P ponendo:

$$f \leq g : \text{se e solo se } (f(x_1),\ldots,f(x_n)) \leq (g(x_1),\ldots,g(x_n)) \text{ nell'insieme prodotto } (P^n, \leq).$$

In particolare se $P = \{0,1\}$, la funzione $F : (2^P,\subseteq) \rightarrow (\{0,1\}^X,\leq)$ che ad ogni sottoinsieme A di X associa la sua funzione caratteristica $\phi_A$ ( per ogni $i = 1,\ldots,r$ ,$\phi_A(x_i) = 0$ se $x_i \notin A$, $\phi_A(x_i) = 1$ se $x_i\in A$) è un isomorfismo di insiemi p.o.

**Reticoli come insieme parzialmente ordinati.** Un reticolo $(L,\leq)$ è un insieme p.o. tale che ogni coppia di elementi ha un estremo inferiore ed un estremo superiore.

Un morfismo di reticoli è una funzione monotona $f : (L,\leq) \rightarrow (L', \leq)$ tale che :

$$f(\inf(x,y)) = \inf (f(x),f(y)) \text{ e } f(\sup(x,y)) = \sup (f(x), f(y)), \text{ per ogni } x,y \in L$$

Due reticoli si dicono isomorfi se è possibile definire tra di essi un morfismo di reticoli biiettivo (*isomorfismo di reticoli*).

Si osservi che l'insieme p.o. $(L, \geq )$, duale di un reticolo, è anch'esso un reticolo in quanto, ponendo per ogni x,y in L : $\inf^*(x,y) = \sup(x,y)$ e $\sup^*(x,y) = \inf(x,y)$, si ha :

(I1) $\inf^*(x,y) \geq x$ e $\inf^*(x,y) \geq y$,

(I2) se $z\in P$, $z \geq x$ e $z \geq y$ allora $z \geq \inf^*(x,y)$.

(S1) $x \geq \sup^*(x,y)$ e $y \geq \sup^*(x,y)$,
(S2) se $z \in P$, $x \geq z$ e $y \geq z$ allora $\sup^*(x,y) \geq z$..
In un reticolo $(L,\leq)$ è possibile definire due operazioni: l'operazione $\wedge$ *di inf* definita da: $x \wedge y = \inf(x,y)$ e l'operazione $\vee$ *di sup* definita da: $x \vee y = \sup(x,y)$. Tali operazioni hanno le seguenti proprietà fondamentali:

(L1) idempotenza : $x \wedge x = x$ $\quad$ $x \vee x = x$
(L2) commutativa : $x \wedge y = y \wedge x$ $\quad$ $x \vee y = y \vee x$
(L3) associativa : $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ $\quad$ $x \vee (y \vee z) = (x \vee y) \vee z$
(L4) assorbimento $x \wedge (x \vee y) = x = x \vee (x \wedge y)$

Inoltre le operazioni di inf e sup risultano isotone, ossia :

se $x, y, z \in L$ e $y \leq z$ allora: $x \wedge y \leq x \wedge z$ e $x \vee y \leq x \vee z$

Si osservi che ogni proprietà (Li) è espressa da uguaglianze di stringhe $E(\wedge,\vee)$ nelle quali compaiono solo elementi del reticolo e i simboli: $\wedge$, $\vee$, (, ). La stringa $E^*(\vee, \wedge)$ duale di $E(\wedge,\vee)$ è quella ottenuta da $E(\wedge,\vee)$ scambiando $\wedge$ con $\vee$ e $\vee$ con $\wedge$. Pertanto se nella proprietà (Li) si sostituisce ad ogni stringa la sua duale si ottiene ancora la proprietà stessa. Questo fatto si esprime affermando che le proprietà fondamentali sono auto-duali, quindi se $I(\wedge,\vee)$ è una identità che consegue dalle proprietà fondamentali allora è necessariamente vera anche l'identità $I^*(\vee, \wedge)$ sua duale. Nei reticoli vale più in generale il

**Principio di dualità.** Se in un reticolo $(L, \leq)$ è vero un enunciato $\mathscr{E}$ su stringhe composte solo da elementi del reticolo e dai simboli $\wedge$ , $\vee$, (, ), allora è vero anche l'enunciato duale $\mathscr{E}^*$ che si ottiene sostituendo ad ogni stringa $E(\wedge, \vee)$ di $\mathscr{E}$ la sua duale $E^*(\vee, \wedge)$ e ad ogni relazione $E_i \leq E_j$ la relazione $E_j{}^* \leq E_i{}^*$ .

**Reticoli come strutture algebriche.** Le proprietà (L1), (L2), (L3), (L4) caratterizzano i reticoli, ossia:

**Teorema 3.1.** Data una struttura algebrica $(L, \wedge, \vee)$ dove le operazioni $\wedge$, $\vee$ hanno le proprietà (L1), (L2), (L3), (L4), è possibile definire su L una relazione d'ordine $\leq$ tale che $(L,\leq)$ sia un reticolo e che per ogni x, y di L si abbia $\inf(x,y) = x \wedge y$ e $\sup(x,y) = x \vee y$. Viceversa dato un reticolo $(L,\leq)$, le operazioni $\wedge$, $\vee$ definite su L rispettivamente da $x \wedge y = \inf(x,y)$ e $x \vee y = \sup(x,y)$ determinano una struttura algebrica $(L, \wedge, \vee)$ verificante le proprietà (L1), (L2), (L3), (L4).

*Dim*. Sia $(L, \wedge, \vee)$ una struttura algebrica verificante le proprietà (L1), (L2), (L3), (L4). La relazione su L $\leq$ definita da :

(3.1.) $x \leq y$ : se e solo se $x \wedge y = x$

è una relazione d'ordine. Infatti è riflessiva per (L1). Inoltre se $x \leq y$ e $y \leq x$, per (L2) si ha:

$$x = x \wedge y = = y \wedge x = y,$$

quindi la relazione è antisimmetrica. Infine se $x \leq y$ e $y \leq z$, per (L3) si ha:

$$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x ,$$

e dunque $x \leq z$. Rimane da dimostrare che per ogni $x,y \in L$ si ha :

$$\inf(x,y) = x \wedge y \text{ e } \sup(x,y) = x \vee y.$$

Infatti:
(I1) : $(x \wedge y) \wedge x = (x \wedge x) \wedge y = x \wedge y \Rightarrow x \wedge y \leq x$ e analogamente $x \wedge y \leq y$
(I2) : sia $z \leq x$ e $z \leq y$ allora $z \wedge x = z = z \wedge y$ e quindi $(x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y \Rightarrow x \wedge y \leq z$ .
Per dualità si ha :

(S1) = (I1)* $x \le x \vee y$ e $y \le x \vee y$
(S2) = (I2)* se $z \in P$, $x \le z$ e $y \le z$ allora $x \vee y \le z$..
e quindi $\sup(x,y) = x \vee y$.

□

Si osservi che un morfismo di reticoli come strutture algebriche $f$: $(L, \wedge, \vee) \to (L', \wedge, \vee)$, ossia un'applicazione $f$ tale che:

$$f(x \wedge y) = f(x) \wedge f(y) \text{ e } f(x \vee y) = f(x) \vee f(y),$$

è anche un morfismo di insiemi p.o., invece un morfismo di insiemi p.o, ossia una funzione monotona da L in L', non necessariamente è un morfismo di reticoli.

**Alcuni reticoli fondamentali.**
Nel seguito una catena di lunghezza n, ossia una catena costituita da (n+1) elementi, sarà indicata con $\mathscr{C}(n)$, poiché catene della stessa lunghezza risultano isomorfe. Ogni catena è ovviamente un reticolo.

**Esempio 1. La catena dei numeri naturali N ordinati dalla relazione naturale.**

**Esempio 2. Il reticolo (N*,|) dei numeri interi positivi ordinati dalla relazione di divisibilità.**
La relazione | è definita da:

$m \mid n \Leftrightarrow$ m divide n : $\Leftrightarrow$ esiste un intero positivo k tale che n = km.

Risulta:

$m \wedge n :=$ massimo comun divisore tra m e n = MCD(m,n),
$m \vee n :=$ minimo comune multiplo tra m ed n = mcm(m,n).

**Esempio 3. L'algebra booleana $\mathscr{B}$(r) di rango r.**
Sia R un insieme non vuoto, l'insieme $\mathscr{B}(R)$ di tutti i sottoinsiemi finiti di R risulta un sottoreticolo del reticolo $(2^R, \subseteq)$ dei sottoinsiemi di R, dove l'operazione di inf è l'intersezione e quella di sup è l'unione. Se $|R| = r < \infty$, allora $\mathscr{B}(R) \cong \mathscr{C}(1)^r$ dove $\mathscr{C}(1)^r$ denota il reticolo prodotto di r copie delle catena $\mathscr{C}(1)$. Infatti, ordinati gli elementi di $R = \{x_1,\ldots,x_r\}$, l'applicazione $\phi$ che ad ogni sottoinsieme A associa la r-pla $\phi(A) = (\phi_A(x_1),\ldots,\phi_A(x_r))$ determinata dalla $\phi_A$, funzione caratteristica di A, è un isomorfismo di reticoli. L'*algebra booleana di rango* r è il reticolo $\mathscr{B}(r)$ dei sottoinsiemi di un insieme con r elementi.

**Esempio 4. Reticolo delle partizioni di un insieme.**
Sia A un insieme non vuoto. L'insieme delle partizioni di A è ordinato dalla relazione di raffinamento definita come segue. Siano $\pi$, $\sigma$ partizioni di A e $(\pi)$, $(\sigma)$ le relazioni di equivalenza da esse determinate, si ha:
$\pi \le \sigma :\Leftrightarrow$ $a(\pi)b$ implica $a(\sigma)b$, per ogni $a,b \in A \Leftrightarrow$ ogni blocco di $\pi$ è contenuto in un blocco di $\sigma$
$\Leftrightarrow$ ogni blocco di $\sigma$, $\sigma$ è unione di blocchi di $\pi$.
Inoltre la partizione $\pi \wedge \sigma$ è determinata dalla relazione di equivalenza:

$$a(\pi \wedge \sigma)b :\Leftrightarrow a(\pi)b \text{ e } a(\sigma)b,$$

mentre la partizione $\pi \vee \sigma$ è determinata da:
$a(\pi \vee \sigma)b : \Leftrightarrow$ esistono $u_1,\ldots u_k \in A$ tali che $u_1 = a$ e $u_k = b$ e per ogni $i = 1,\ldots,k-1$ risulta
$u_i(\pi)u_{i+1}$ oppure $u_i(\sigma)u_{i+1}$.
Si indichi con $\mathscr{P}(A)$ il *sottoreticolo costituito dalle partizioni di* A *con un numero finito di blocchi*. Dati due insiemi finiti con la stessa cardinalità n, i rispettivi reticoli delle partizioni risultano isomorfi, pertanto è possibile definire il *reticolo delle partizioni* $\mathscr{P}(n)$ *di ordine* n ($< \infty$).

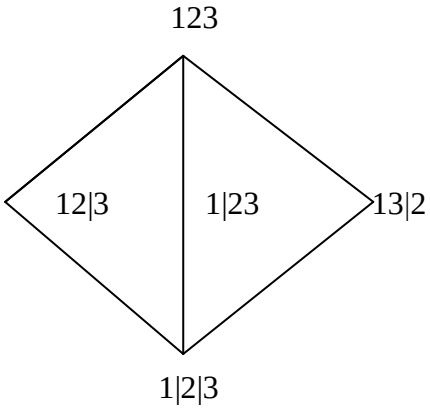


Fig.3.2: Il reticolo $\mathscr{P}(3)$

**Teorema.(Pudlák-Tûma).** Ogni reticolo finito è isomorfo ad un sottoreticolo del reticolo delle partizioni $\mathscr{P}(n)$.

**Lemma.** Si ha: $\sum_{0\le k\le n} (-1)^k \binom{n}{k} = 0$.

*Dim.* Dal teorema binomiale $\sum_{0\le k\le n} x^k \binom{n}{k} = (x+1)^n$ ponendo x = -1

□

**Proposizione. Principio di inclusione-esclusione.** Sia t>1 e siano $A_1,\dots A_t$ sottoinsiemi finiti di un insieme R . Allora si ha:

$$|\cup_{i=1,..t} A_i| = \Sigma_{\varnothing \neq I} (-1)^{|I|-1} |\cap_{i\in I} A_i|$$

dove la somma è estesa a tutti i sottoinsiemi non vuoti I dell'insieme $\{1,\dots,t\}$.
Quindi la funzione rango dell'algebra $\mathscr{B}(R)$ verifica la proprietà di regolarità ($R_t$) per ogni $t>1$.

*Dim.* Ogni elemento di $A_1 \cup \dots \cup A_t$ è contato una volta, infatti sia x appartenente ad $A_{i1}, \dots A_{im}$ allora il contributo di x alla somma è: $\sum_{1\le k\le m} (-1)^{k-1}\binom{m}{k} = -\sum_{1\le k\le m} (-1)^k \binom{m}{k} = \binom{m}{0}$ (per il lemma) = 1.

□

**Applicazioni del Principio di inclusione-esclusione.**

**Esempio 1. Funzione di Eulero.** Due interi *m,n* si dicono *primi tra loro* o *coprimi* se l'unico divisore che hanno in comune è 1. La funzione di Eulero è la funzione :

$\phi : \mathbf{N}^+ \to \mathbf{N}^+$ definita da : $\phi(1) = 1$ e se $n \neq 1$ $\phi(n)$ = numero degli interi minori di *n* e primi con *n*.

Ogni intero maggiore o uguale a 2 si può ottenere in modo unico come prodotto di potenze di numeri primi. Sia $n = p_1^{h_1} \dots p_k^{h_k}$ (scomposizione irriducibile dell'intero *n* ). Si ponga

$$A_p = \{m \in [n]: m \text{ è divisibile per } p\}$$

Allora $|A_p|$ è uguale alla parte intera di $n/p$ in quanto ogni multiplo intero di *p* minore o uguale ad *n* si ottiene moltiplicando *p* per un intero minore o uguale a $n/p$, dunque se *p* un divisore primo di *n*, risulta $|A_p| = n/p$. Si ha:

$$\phi(n) = |[n]| - |\cup_{p \text{ divisore primo di } n} A_p|$$

e quindi per il principio di inclusione esclusione:

$$\phi(n) = n - [n/p_1 + \ldots + n/p_k - n/p_1p_2 - \ldots - n/(p_{k-1}p_k) + n/(p_1p_2p_3) + \ldots + n/(p_{k-2}p_{k-1}p_k) + \\ + \ldots + (-1)^{k-1}(n/(p_1p_2\ldots p_k)\,] = n\,(1 - 1/p_1)\ldots\,(1 - 1/p_k).$$

□

**Esempio 2. Permutazioni senza punti fissi.** Usando il principio di inclusione esclusione è possibile determinare il numero $d_n$ delle permutazioni di $S_n$ senza punti fissi (forma chiusa). Sia $A(i)$ il sottoinsieme di $S_n$ costituito da tutte le permutazioni che fissano $i \in [n]$. Risulta $|A(i_1) \cap \ldots \cap A(i_k)| = (n-k)!$ , pertanto:

$$d_n = n! - |\,A(1) \cup \ldots \cup A(n)| = n! - \left(n(n-1)! - \binom{n}{2}(n-2)! + \ldots + (-1)^{k-1}\binom{n}{k}(n-k)! + \ldots + (-1)^{n-1}\right) = \\ = n!\left(\,1 - 1/1! + 1/2! - 1/3! + \ldots + (-1)^n\,1/n!\right).$$

□

**Esempio 3. Numeri di Stirling.** Il numero delle funzioni suriettive definite su un insieme X con $n$ elementi e a valori in [m] è $m!S(n,m)$, dove $S(n,m)$ è il numero delle partizioni con $m$ blocchi di un insieme con $n$ elementi, tale numero è chiamato *numero di Stirling di II specie*. Sia $[m]^n$ l'insieme delle funzioni da X in [m] e per ogni $i \in [m]$ sia $A(i)$ il sottoinsieme costituito dalle funzioni la cui immagine non contiene $i$. Risulta :

$$|\,A(i)\,| = (m-1)^n\,, \quad |A(i_1) \cap \ldots \cap A(i_k)| = (m-k)^n$$

e quindi, per il principio di inclusione- esclusione, il numero delle funzioni suriettive è:

$$m^n - |\,A(1) \cup \ldots \cup A(m)| = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \binom{m}{3}(m-3)^n + \ldots + (-1)^m$$

da cui l'identità (forma chiusa per la successione dei numeri di Stirling di II specie):

$$m!S(n,m) = \sum_{o \le k \le m} (-1)^k \binom{m}{k}(m-k)^n.$$