UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Metodi matematici per l'Informatica

Modulo 10 – Algebre di Boole

Docente: Pietro Cenciarelli

Reticoli

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ *join*

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ *meet*

$(\mathcal{A}, \leq)$

$\forall$ a, b $\in \mathcal{A}$
$\exists$ sup {a, b} e inf {a, b}

$A \vee (B \vee C) = (A \vee B) \vee C$ associativa

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A$ $\quad A \wedge B = B \wedge A$ commutativa

$A \vee (A \wedge B) = A$ $\quad A \wedge (A \vee B) = A$ assorbimento

$A \vee A = A$ $\quad A \wedge A = A$ idempotenza

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A \qquad A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$

$A \vee A = A \qquad A \wedge A = A$

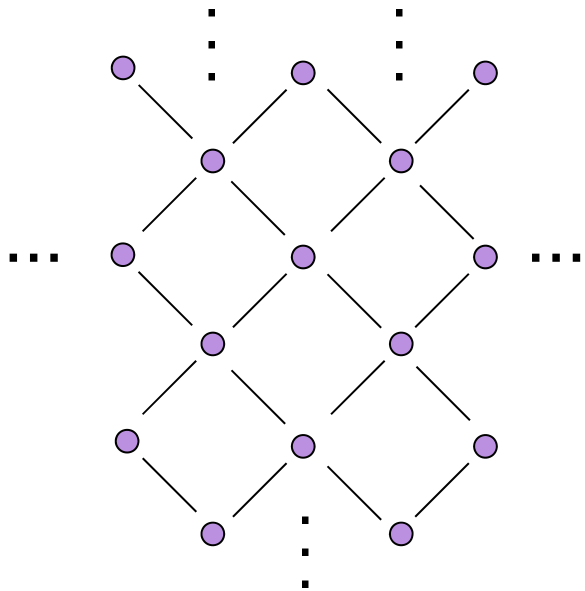
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$(\mathcal{A}, \leq)$

$\forall\, a, b \in \mathcal{A}$

$\exists \sup \{a, b\}$ e $\inf \{a, b\}$



Reticoli distributivi

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A \qquad A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$

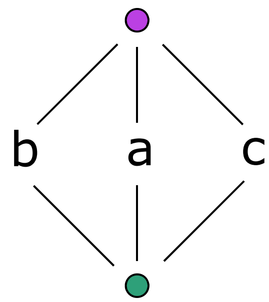
$A \vee A = A \qquad A \wedge A = A$

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$(\mathcal{A}, \leq)$

$\forall\, a, b \in \mathcal{A}$
$\exists \sup \{a, b\}$ e $\inf \{a, b\}$



$a \wedge (b \vee c) = a \wedge \bullet = a$

$(a \wedge b) \vee (a \wedge c) = \bullet \neq a$

non distributivo!

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A$ $\quad$ $A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A$ $\quad$ $A \wedge (A \vee B) = A$

$A \vee A = A$ $\quad$ $A \wedge A = A$

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$(\mathcal{A}, \leq)$

$\forall$ a, b $\in \mathcal{A}$
$\exists$ sup {a, b} e inf {a, b}

☺ $\Uparrow$ $\Downarrow$?

$\forall$ A $\subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

sup $\{a_1, a_2, \dots a_n\}$
= sup (a1, sup (a2, …))

sup {} ?

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A \qquad A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$

$A \vee A = A \qquad A \wedge A = A$

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$(\mathcal{A}, \leq)$

$\forall$ a, b $\in \mathcal{A}$
$\exists$ sup {a, b} e inf {a, b}

☺ $\Uparrow$ $\Downarrow$?

$\forall A \subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

sup {} = min $(\mathcal{A})$

- $\forall$ a $\in$ {}, a $\leq$ sup {}
- $\forall$ b $\in \mathcal{A}$, se a $\leq$ b $\forall$ a $\in$ {} allora sup {} $\leq$ b

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A \qquad A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$

$A \vee A = A \qquad A \wedge A = A$

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$(\mathcal{A}, \leq)$

$\forall\, a, b \in \mathcal{A}$

$\exists$ sup $\{a, b\}$ e inf $\{a, b\}$

☺ $\Uparrow$ $\Downarrow$ ☹

$\forall\, A \subseteq \mathcal{A}$, A *finito*,

$\exists$ sup (A) e inf (A)

sup $\{\} =$ min $(\mathcal{A})$

$\ldots \leq a_2 \leq a_1 \leq a_0$

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge, \bot, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

$A \vee B = B \vee A \qquad A \wedge B = B \wedge A$

$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$

$A \vee A = A \qquad A \wedge A = A$

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

$A \vee \bot = A \qquad A \wedge \top = A$

$(\mathcal{A}, \leq)$

$\forall\, a, b \in \mathcal{A}$
$\exists$ sup $\{a, b\}$ e inf $\{a, b\}$

$\forall\, A \subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

sup {} = min ($\mathcal{A}$)
inf {} = max ($\mathcal{A}$)

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge, \perp, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$

$(\mathcal{A}, \leq)$

$\forall A \subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

Lemma: in un reticolo *distributivo*, $\forall$ a, b e c
se $a \vee b = a \vee c$ e $a \wedge b = a \wedge c$, allora $b = c$.

$$
\begin{aligned}
b = b \vee (b \wedge a) &= b \vee (c \wedge a) && \textit{distributiva} \\
&= (b \vee c) \wedge (b \vee a) \\
&= (b \vee c) \wedge (a \vee c) && \textit{distributiva} \\
&= (b \wedge a) \vee c = (a \wedge c) \vee c = c
\end{aligned}
$$

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge, \perp, \top)$

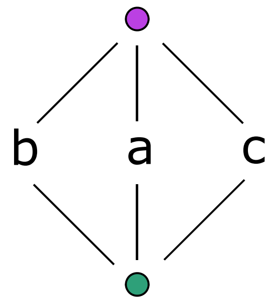
$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$(\mathcal{A}, \leq)$

$\forall$ A $\subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

Lemma: in un reticolo *distributivo*, $\forall$ a, b e c
se $a \vee b = a \vee c$ e $a \wedge b = a \wedge c$, allora $b = c$.



non distributivo!

☹

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge, \bot, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$(\mathcal{A}, \leq)$

$\forall A \subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

Lemma: in un reticolo *distributivo*, $\forall$ a, b e c
se $a \vee b = a \vee c$ e $a \wedge b = a \wedge c$, allora $b = c$.

Definizione: un elemento b un reticolo $\mathcal{A}$ si dice
complemento di $a \in \mathcal{A}$ se $a \vee b = \top$ e $a \wedge b = \bot$.

Teorema: in un reticolo *distributivo*, ogni elemento
ha *al più* un complemento.

(consegue banalmente dal lemma)

…e il vice-versa?

Reticoli distributivi

$(\mathcal{A}, \vee, \wedge, \perp, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$(\mathcal{A}, \leq)$

$\forall$ A $\subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

Esistono reticoli *non* distributivi a complemento unico!
(Dilwhort)

Algebre di Boole

$(\mathcal{A}, \vee, \wedge, \overline{}, \perp, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$(\mathcal{A}, \leq)$

$\forall A \subseteq \mathcal{A}$, A *finito*,
$\exists$ sup (A) e inf (A)

Definizione: un'*algebra di Boole* è un reticolo distributivo, dove ogni elemento ha un complemento.

Algebre di Boole

$(\mathcal{A}, \vee, \wedge, \overline{}, \bot, \top)$

$\vee : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\wedge : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$

$\overline{} : \mathcal{A} \rightarrow \mathcal{A}$

$\vdots$

$a \vee \overline{a} = \top$

$a \wedge \overline{a} = \bot$

$(2^A, \cup, \cap, \overline{}, \{\}, A)$

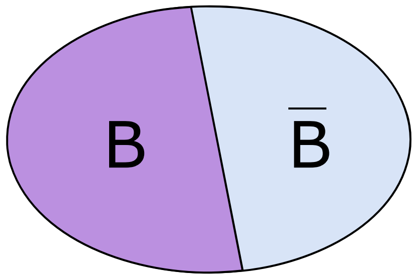
$\cup : 2^A \times 2^A \rightarrow 2^A$

$\cap : 2^A \times 2^A \rightarrow 2^A$

$\overline{} : 2^A \rightarrow 2^A$

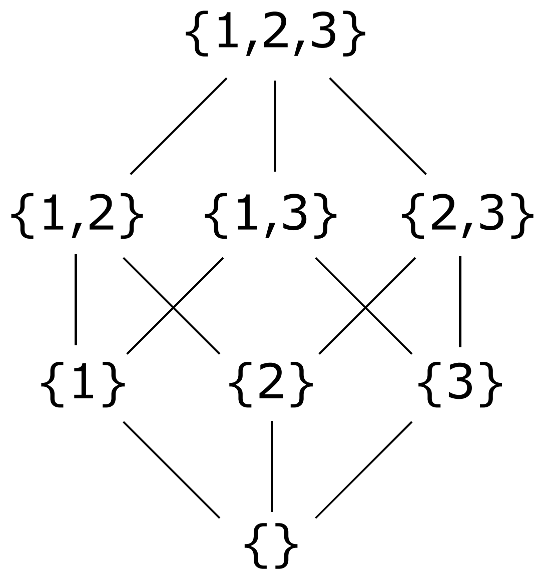
$B \cup \overline{B} = A$

$B \cap \overline{B} = \{\}$



A

Algebre di Boole

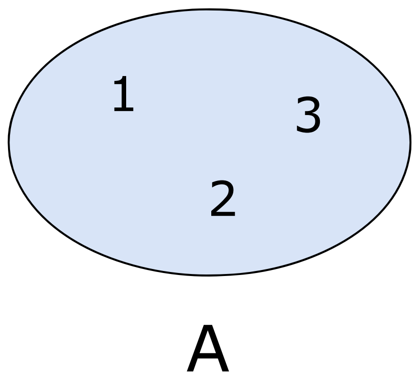


$(2^A, \cup, \cap, \overline{}, \{\}, A)$

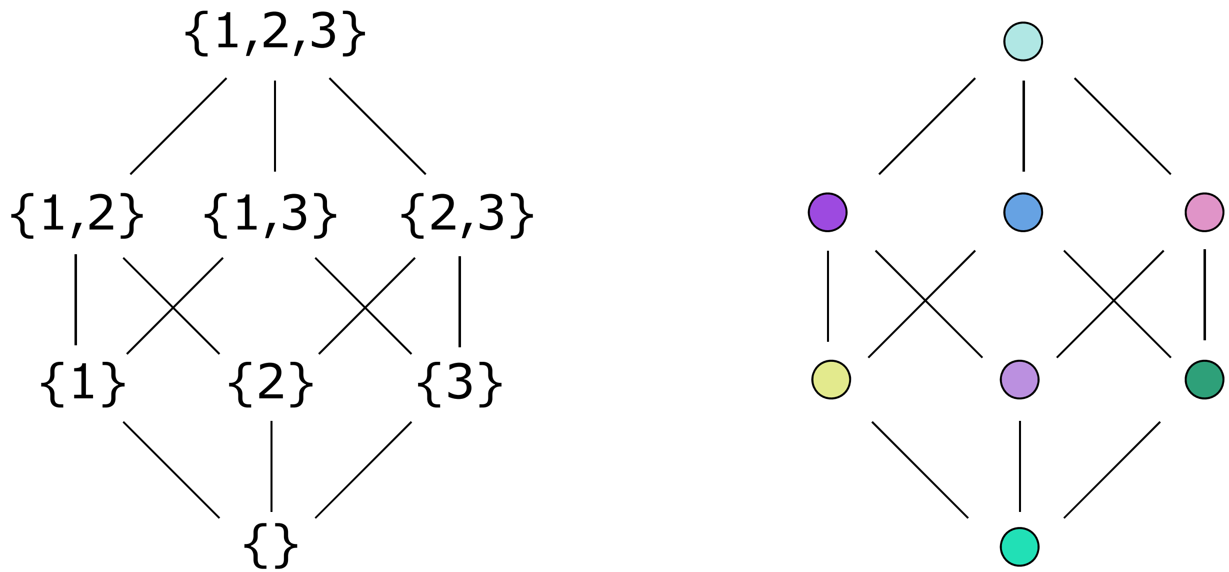
$\cup : 2^A \times 2^A \rightarrow 2^A$

$\cap : 2^A \times 2^A \rightarrow 2^A$

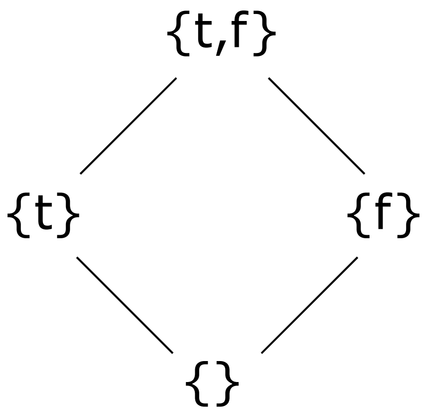
$\overline{} : 2^A \rightarrow 2^A$

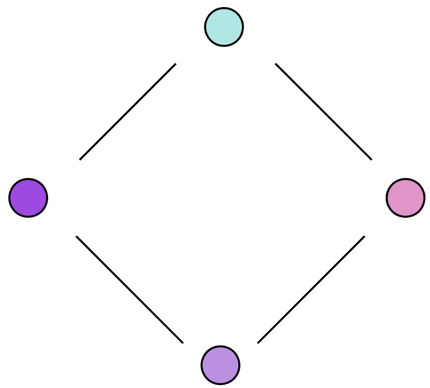


Algebre di Boole



Algebre di Boole





Ogni algebra di Boole è isomorfa a un algebra di insiemi.

Marshall H. Stone (1936)

Algebre di Boole

$A \vee (B \vee C) = (A \vee B) \vee C$		
$A \wedge (B \wedge C) = (A \wedge B) \wedge C$		associativa
$A \vee B = B \vee A$	$A \wedge B = B \wedge A$	commutativa
$A \vee (A \wedge B) = A$	$A \wedge (A \vee B) = A$	assorbimento
$A \vee A = A$	$A \wedge A = A$	idempotenza
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$		
$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$		distributiva
$A \vee \bot = A$	$A \wedge \top = A$	identità
$A \vee \overline{A} = \top$	$A \wedge \overline{A} = \bot$	complemento

Convoluzione

$$\overline{\overline{A}} = A$$

perche entrambi complemento di $\overline{A}$

Leggi di De Morgan

$$\overline{A \vee B} = \overline{A} \wedge \overline{B}$$

$$(\overline{A} \wedge \overline{B}) \wedge (A \vee B) = (\overline{A} \wedge \overline{B} \wedge A) \vee (\overline{A} \wedge \overline{B} \wedge B) \quad = \bot \vee \bot = \bot$$

$$(\overline{A} \wedge \overline{B}) \vee (A \vee B) = (\overline{A} \vee A \vee B) \wedge (\overline{B} \vee A \vee B) \quad = \top \wedge \top = \top$$

dunque $\overline{A} \wedge \overline{B}$ è il complemento di $A \vee B$

Leggi di De Morgan

$$\overline{A \vee B} = \overline{A} \wedge \overline{B} \qquad\qquad \overline{A \wedge B} = \overline{A} \vee \overline{B}$$

$$\overline{A \wedge B} = \overline{\overline{\overline{A}} \wedge \overline{\overline{B}}}$$ convoluzione

$$= \overline{\overline{\overline{A} \vee \overline{B}}}$$ De Morgan

$$= \overline{A} \vee \overline{B}$$ convoluzione