UNIVERSITÀ DEGLI STUDI "LA SAPIENZA"
CORSO DI STUDI IN INFORMATICA
ESERCITAZIONI AL CORSO DI LOGICA MATEMATICA

ALGEBRE DI BOOLE

(1) Un *reticolo* $(X, \leq, \cap, \cup)$ è un insieme parzialmente ordinato nel quale per ogni coppia di elementi (a, b) esistono un massimo comune minorante $a \cap b$ e un minimo comune maggiorante $a \cup b$.
(2) Un reticolo si dice *distributivo* se per ogni $a, b, \in X$:
   (a) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
   (b) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$
(3) Un reticolo si dice *complementato* se possiede un minimo, indicato con 0, e un massimo, indicato con 1 e se per ogni $a \in X$ esiste $\overline{a} \in X$ (detto *complemento di* a) tale che: $a \cup \overline{a} = 1$ e $a \cap \overline{a} = 0$.
(4) Una *algebra di Boole* è un reticolo distributivo e complementato.

Esercizio 1 (Esempio reticolo non distributivo)**.** *Sia* $X = \{0, a, b, c, 1\}$, $\leq$ *la chiusura transitiva e riflessiva della seguente relazione:*

$$\{(0, a), (0, b), (0, c), (a, 1), (b, 1), (c, 1)\}$$

Disegna il diagramma di $\leq$ *e mostra che* $\leq$ *è un ordine su* X. *Definisci* $\cap$ *e* $\cup$ *rispetto a tale ordine.* $(X, \leq, \cap, \cup)$ *così definito è un reticolo distributivo?*

Soluzione. $\leq$ è ovviamente riflessiva e transitiva, mostriamo che sia antisimmetrica. Per ogni $x \in X - \{0\}$, $0 \leq x$, ma non $x \leq 0$. Similmente per ogni $x \in X - \{1\}$, $x \leq 1$, ma non $1 \leq x$. Infine per ogni $x, y \in X - \{0, 1\}$, se $x \neq y$, allora x, y non sono confrontabili. Quindi $\leq$ è un ordine.

0 è il minimo, 1 è il massimo di $\leq$, inoltre possiamo definire per ogni $x, y \in X - \{0, 1\}$, $x \cap y = 0$, $x \cup y = 1$. $(X, \leq, \cap, \cup)$ così definito è un reticolo con minimo e massimo, ma non è distributivo, ad esempio:

$$a \cup (b \cap c) = a \cup 0 = a$$

mentre:

$$(a \cup b) \cap (a \cup c) = 1 \cap 1 = 1$$

□

Esercizio 2 (Esempio reticolo distributivo non complementato)**.** *Nel prodotto cartesiano* Z^n *si definisca:*

(1) $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ *se e solo se per ogni* $i \leq n$, $a_i \leq b_i$;
(2) $(a_1, \ldots, a_n) \cap (b_1, \ldots, b_n) = (min(a_1, b_1), \ldots, min(a_n, b_n))$;
(3) $(a_1, \ldots, a_n) \cup (b_1, \ldots, b_n) = (max(a_1, b_1), \ldots, max(a_n, b_n))$;

Dimostra che $(Z^n, \leq, \cap, \cup)$ *è un reticolo distributivo, ma non un'algebra di Boole.*

Date: 30 – 11 – 2006.

Soluzione. In primo luogo verifica che $\leq$ definisce una relazione d'ordine. Poi verifichiamo che $\cap$ e $\cup$ sono rispettivamente massimo comune minorante e minimo comune maggiorante. Ad esempio, considero $\cap$:

$(a_1, \ldots, a_n) \cap (b_1, \ldots, b_n) = (min(a_1, b_1), \ldots, min(a_n, b_n))$. Per definizione di min, ottengo per ogni $i \leq n$, $min(a_i, b_i) \leq a_i, b_i$, quindi $(a_1, \ldots, a_n) \cap (b_1, \ldots, b_n) \leq (a_1, \ldots, a_n), (b_1, \ldots, b_n)$. Cioè $\cap$ definisce un minorante, dobbiamo dimostrare che è il massimo tra i minoranti: supponiamo $(z_1, \ldots, z_n) \leq (a_1, \ldots, a_n), (b_1, \ldots, b_n)$, dimostriamo che $(z_1, \ldots, z_n) \leq (a_1, \ldots, a_n) \cap (b_1, \ldots, b_n)$. Per ipotesi abbiamo per ogni $i \leq n$, $z_i \leq a_i, b_i$, quindi per definizione di min, $z_i \leq min(a_i, b_i)$, il che dimostra $(z_1, \ldots, z_n) \leq (a_1, \ldots, a_n) \cap (b_1, \ldots, b_n)$.

In modo simmetrico si ottiene la dimostrazione che $\cup$ definisce il minimo comun maggiorante. Quindi $(Z^n, \leq, \cap, \cup)$ è un reticolo.

Verifichiamo ora che $(Z^n, \leq, \cap, \cup)$ sia distributivo:

$$\begin{aligned}
&(a_1, \ldots, a_n) \cup ((b_1, \ldots, b_n) \cap (c_1, \ldots, c_n)) = \\
&= (max(a_1, min(b_1, c_1)), \ldots max(a_n, min(b_n, c_n)) = \\
&= (min(max(a_1, b_1), max(a_1, c_1)), \ldots, min(max(a_n, b_n), max(a_n, c_n))) = \\
&= ((a_1, \ldots, a_n) \cup (b_1, \ldots, b_n)) \cap ((a_1, \ldots, a_n) \cup (c_1, \ldots, c_n))
\end{aligned}$$

In modo simmetrico si ottiene anche la distributività di $\cap$ su $\cup$. Quindi $(Z^n, \leq, \cap, \cup)$ è un reticolo distributivo.

$(Z^n, \leq, \cap, \cup)$ non è però complementato, perchè non contiene né minimo né massimo. □

Esercizio 3 (esempio algebra di boole)**.** *Sia I un insieme con n elementi. Dimosta che $(\wp(I), \subseteq, \cap, \cup)$ definisce un algebra di Boole di 2^n elementi. Disegna il diagramma di tale algebra per $n = 0, 1, 2, 3$*

Esercizio 4 (Leggi di De Morgan, complemento)**.** *Dimostra che in una algebra di Boole il complemento di un elemento è unico e che valgono le leggi di De Morgan: $\overline{a \cap b} = \overline{a} \cup \overline{b}$, $\overline{a \cup b} = \overline{a} \cap \overline{b}$. Tali leggi valgono anche in un reticolo complementato ma non distributivo?*

Soluzione. Sia a un elemento dell'algebra, dimostriamo che il suo complemento è unico. Supponiamo a_1, a_2 siano due complementi di a, ovvero: $a \cap a_1 = a \cap a_2 = 0$ e $a \cup a_1 = a \cup a_2 = 1$.

$a_1 = a_1 \cap 1 = a_1 \cap (a \cup a_2)$. Per distributività ottengo $a_1 = (a_1 \cap a) \cup (a_1 \cap a_2)$, quindi $a_1 = 0 \cup (a_1 \cap a_2) = a_1 \cap a_2$. In modo simmetrico ottengo da $a_2 = a_2 \cap 1$ che $a_2 = a_1 \cap a_2$, quindi concludo che $a_1 = a_2$.

Osserva che abbiamo dimostrato l'identità dei due complementi utilizzando la distributività. In un reticolo non distributivo il complemento può non essere unico, ad esempio considera il reticolo dell'esercizio 1 e osserva che ogni suo elemento diverso da 1 e 0 ha due complementi.

Per quanto riguarda le leggi di De Morgan. Dimostriamo che $\overline{a \cap b} = \overline{a} \cup \overline{b}$, ovvero dobbiamo dimostrare che:

$$(a \cap b) \cup (\overline{a} \cup \overline{b}) = 1 \quad \text{e} \quad (a \cap b) \cap (\overline{a} \cup \overline{b}) = 0$$

Per distributività ottengo: $(a \cap b) \cup (\overline{a} \cup \overline{b}) = (a \cup (\overline{a} \cup \overline{b})) \cap (b \cup (\overline{a} \cup \overline{b}))$. Per associatività e commutatività di $\cup$ e definizione di complemento, ottengo quindi: $(a \cup (\overline{a} \cup \overline{b})) \cap (b \cup (\overline{a} \cup \overline{b})) = (1 \cup \overline{b}) \cap (1 \cup \overline{a}) = 1$. In modo simmetrico (ovvero utilizzando la associatività e commutatività di $\cap$ invece che quella di $\cup$ si ottiene che $(a \cap b) \cap (\overline{a} \cup \overline{b}) = 0$.

In modo del tutto simile si dimostra $\overline{a \cup b} = \overline{a} \cap \overline{b}$.

Anche in questo caso abbiamo dimostrato le leggi di De Morgan utilizzando la distributività. In un reticolo non distributivo queste leggi infatti possono non essere valide. Come esempio prendi sempre il reticolo dell'esercizio 1: osserva che $\overline{(a \cap b)} = 1$, mentre invece, siccome c può essere considerato il complemento sia di a che di b, ottengo $\overline{a} \cup \overline{b} = c \cup c = c$. □

Esercizio 5 (Ancora induzione ...). *La lunghezza di una stringa è il numero di elementi da cui essa è formata. Ad esempio, la stringa* $\alpha = aabccc$ *su* $I = \{a, b, c\}$, *ha lunghezza* 6, *inoltre in* α *il simbolo* a *occorre* 2 *volte,* b *una volta,* c *tre volte. Indichiamo con* I^n *l'insieme delle stringhe su* I *di lughezza* n. *Dimostra* per induzione *che per ogni* n *il numero di stringhe di* I^n *in cui il simbolo* a *occorre più volte del simbolo* b *è uguale al numero di stringhe in cui il simbolo* b *occorre più volte del simbolo* a.