G. Pareschi

ALGEBRE DI BOOLE

1. Algebre di Boole

Nel file precedente abbiamo incontrato la definizione di algebra di Boole come reticolo: un'algebra di Boole e' un reticolo limitato, complementato e distributivo. Ora vedremo la definizione più usuale e mostreremo l'equivalenza tra le due definizioni. In conformità alla letteratura sull'argomento, useremo la terminologia seguente:

- dato un insieme B, per *operazione binaria su* B intenderemo quello che di solito si chiama semplicemente un'operazione su B, cioè una funzione $B \times B \to B$. Ad esempio, la somma di numeri reali è la funzione $\mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $(x, y) \mapsto x + y$.

- per *operazione unaria* su B intederemo semplicemente una funzione $B \to B$. Ad esempio, se X è un'insieme e $B = \mathcal{P}(X)$, il complemento di un sottoinsieme $A \subseteq X$, denotato $\mathcal{C}_X(A) = \{x \in X \mid x \notin A\}$, definisce l'operazione unaria $\mathcal{C}_X : \mathcal{P}(X) \to \mathcal{P}(X)$, $A \mapsto \mathcal{C}_X(A)$.

Definizione 1.1. *(Algebra di Boole)* Un'algebra di Boole è un'insieme B dotato di due operazioni binarie, $\vee$ e $\wedge$, e di un'operazione unaria $'$ tali che valgono le seguenti proprietà:
(1) *Commutatività:* $a \vee b = b \vee a$, $a \wedge b = b \wedge a$, per ogni $a, b \in B$.
(2) *Distributività:* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ e $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ per ogni $a, b, c \in B$.
(3) *Elementi neutri, o "leggi di identità":* esistono due elementi distinti $0, 1 \in B$ tali che $x \vee 0 = x$ e $x \wedge 1 = x$ per ogni $x \in B$.
(4) *Complemento:* $x \vee x' = 1$ e $x \wedge x' = 0$ per ogni $x \in B$.

In breve, si denota l'insieme di tutti questi dati con $(B, \vee, \wedge, ', 0, 1)$.

Esempio 1.2. *(Insieme delle parti)* Sia X un insieme. Consideriamo il suo insieme delle parti $\mathcal{P}(X)$. Allora $(\mathcal{P}(X), \cup, \cap, \mathcal{C}_X, \emptyset, X)$ è un'algebra di Boole (esercizio)

Esempio 1.3. *($\{0,1\}$)* Sia $\mathbb{B} = \{0, 1\}$ dotato delle operazioni binarie $\vee, \wedge$ e dell'operazione unaria $'$, dove:
- $\vee$ è definita da $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$.
- $\wedge$ è definita da $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$.
- $'$ è definita da $0' = 1$, $1' = 0$.
Si ha che $(\mathbb{B}, \vee, \wedge, 0, 1)$ è un'algebra di Boole.

Esempio 1.4. *($\{0,1\}^n$)* Consideriamo il prodotto cartesiano $\{0, 1\}^n = \{0, 1\} \times \cdots \times \{0, 1\}$ (n volte), dotato delle operazioni $\vee$, $\wedge$, $'$ definite componente a componente come nell'esempio precedente: $(x_1, .., x_n) \vee (y_1, .., y_n) = (x_1 \vee y_1, ..., x_n \vee y_n)$, , $(x_1, .., x_n) \wedge (y_1, .., y_n) = (x_1 \wedge y_1, ..., x_n \wedge y_n)$, $(x_1, ..., x_n)' = (x_1', ..., x_n')$. Ad esempio: $(001010) \vee (010111) = (011111)$, $(001010) \wedge (010111) = (000010)$, $(001010)' = (110101)$. Denotiamo $O = (0, ..., 0)$ e $\mathbf{1} = (1, ..., 1)$.
Si ha che $(\{0, 1\}^n, \vee, \wedge, ', O, \mathbf{1})$ è un'algebra di Boole (esercizio).

1.1. Conseguenze degli assiomi di Algebra di Boole.

Le operazioni di un'algebra di Boole soddisfano anche altre proprietà notevoli, che possono essere dedotte dagli assiomi $1, 2, 3, 4$. Per fare queste deduzioni, è utile osservare che, essendo gli assiomi $1, 2, 3, 4$ "simmetrici" rispetto alle operazioni $\vee$ e $\wedge$, se un certo enunciato, riguardante le operazioni in un'algebra di Boole,

è vero, anche il suo *enunciato duale* – ossia l'enunciato ottenuto scambiando le $\vee$ con le $\wedge$ – è vero. Questo fatto va sotto il nome di *Principio di Dualità*.

Proposizione 1.5. Sia B un'algebra di Boole e siano $x, y, z \in B$. Allora:
(5) *Idempotenza:* $x \vee x = x$ e $x \wedge x = x$
(6) *Limitatezza:* $x \vee 1 = 1$ e $x \wedge 0 = 0$
(7) *Assorbimento:* $x \vee (x \wedge y) = x$ e $x \wedge (x \vee y) = x$
(8) *Associatività:* $x \vee (y \vee z) = (x \vee y) \vee z$, e $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
(9) *Unicità del complemento:* se $x \vee y = 1$ e $x \wedge y = 0$ allora $y = x'$
(10) *Involutività:* $(x')' = x$
(11) $0' = 1$, $1' = 0$
(12) *Leggi di De Morgan:* $(x \vee y)' = x' \wedge y'$ e $(x \wedge y)' = x' \vee y'$.

Proof. È conveniente dimostrare le varie proprietà nell'ordine in cui sono enunciate. Alcune le dimostrerò e altre le lascerò per esercizio.
Ad esempio, (5) si dimostra così:
$x \overset{(3)}{=} x \wedge 1 \overset{(4)}{=} x \wedge (x \vee x') \overset{(2)}{=} (x \wedge x) \vee (x \wedge x') \overset{(4)}{=} (x \wedge x) \vee 0 = x \wedge x$ (l'altro enunciato segue per dualità).

Dimostriamo ora la (8), assumendo (1)....(7). Si comincia col dimostrare che

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

Infatti
$x \vee (x \wedge (y \wedge z) \overset{(2)}{=} (x \vee x) \wedge (x \vee (y \wedge z)) \overset{(5)}{=} x \wedge (x \vee (y \wedge z)) \overset{(7)}{=} x$ e
$x \vee ((x \wedge y) \wedge z) \overset{(2)}{=} (x \vee (x \wedge y)) \wedge (x \vee z) \overset{(7)}{=} x \wedge (x \vee z) \overset{(7)}{=} x$.
Poi si dimostra che

$$x' \vee (x \wedge (y \wedge z) = x' \vee ((x \wedge y) \wedge z)$$

Infatti
$x' \vee (x \wedge (y \wedge z) \overset{(2)}{=} (x' \vee x) \wedge (x' \wedge (y \wedge z) \overset{(4)}{=} 1 \wedge (x' \wedge (y \wedge z) \overset{(3)}{=} x' \wedge (y \wedge z)$.
Inoltre
$x' \vee ((x \wedge y) \wedge z) \overset{(2)}{=} (x' \vee (x \wedge y) \wedge (x' \vee z) \overset{(2)}{=} ((x' \vee x) \wedge (x' \vee y)) \wedge (x' \vee z) \overset{(4)}{=} (1 \wedge (x' \vee y)) \wedge (x' \vee z) \overset{(3)}{=}$
$(x' \vee y) \wedge (x' \vee z) \overset{(2)}{=} x' \vee (y \wedge z)$.

Concludendo:
$x \wedge (y \wedge z) \overset{(4),(3)}{=} (x \wedge x') \vee (x \wedge (y \wedge z)) \overset{(2)}{=} (x \vee (x \wedge (y \wedge z))) \wedge (x' \vee (x \wedge (y \wedge z))) = (x \vee ((x \wedge$
$y) \wedge z) \wedge (x' \vee ((x \wedge y) \wedge z) \overset{(2)}{=} (x \wedge x') \vee (x \wedge (y \wedge z)) \overset{(3),(4)}{=} (x \wedge y) \wedge z$.
L'altra associatività segue per dualità.

Assumendo (1)....(8), la (9) si dimostra così: $x' \overset{(3)}{=} x' \vee 0 = x' \vee (x \wedge y) \overset{(2)}{=} (x' \vee x) \wedge (x' \vee y) \overset{(1),(4)}{=} 1 \wedge (x' \vee y) \overset{(3)}{=} x' \vee y$. Quindi

$$x' = x' \vee y.$$

Allo stesso modo si dimostra che

$$y = x' \vee y$$

(esercizio) Dunque

$$x' = y$$

Assumendo (1).....(11), la (12) si dimostra così:
A causa della (9), è sufficiente dimostrare che $(x \vee y) \vee (x' \wedge y') = 1$ e che $(x \vee y) \wedge (x' \wedge y') = 0$

(l'altro enunciato segue per dualità). Dimostriamo la prima:
$(x\vee y)\vee(x'\wedge y') \overset{(2)}{=} ((x\vee y)\vee x')\wedge((x\vee y)\vee y') \overset{(7),(1)}{=} (y\vee x\vee x')\wedge(x\vee y\vee y') \overset{(4)}{=} (x\vee 1)\wedge(y\vee 1) \overset{(3)}{=} 1\wedge 1 \overset{(3)}{=} 1$. Dimostriamo la seconda:
$(x\vee y)\wedge(x'\wedge y') \overset{(1),(2)}{=} (x\wedge(x'\wedge y'))\vee(y\wedge(x'\wedge y')) \overset{7}{=} (x\wedge x'\wedge y')\vee(x'\wedge y\wedge y') \overset{(3)}{=} (0\wedge y')\vee(x'\wedge 0) \overset{(3)}{=} 0\vee 0 \overset{(3)}{=} 0$. □

Esercizio 1.6. Dimostrare tutte le altre proprietà, cioè: $(6), (7), (10), (11)$.

Anche nel contesto delle algebre di Boole si ha la nozione di *isomorfismo*.

Definizione 1.7. *(Morfismi e isomorfismi di algebre di Boole)* Siano B e C due algebre di Boole. Una funzione $f : B \to C$ è detta un morfismo di algebre di Boole se, per ogni $x, y \in B$,
(a) $f(x) \vee f(y) = f(x \vee y)$,
(b) $f(x) \wedge f(y) = f(x \wedge y)$,
(c) $f(x)' = f(x')$.

Un omomorfismo di algebre di Boole biettivo è detto un isomorfismo di algebre di Boole. In tal caso le algebre di Boole B e C sono dette isomorfe.

Esercizio 1.8. Dimostrare che se $f : B \to C$ è un isomorfismo di algebre di Boole, anche f^{-1} è un isomorfismo di algebre di Boole.

Esercizio 1.9. (a) Dimostrare che $\mathcal{P}(\{a, b, c\})$ e $\{0, 1\}^3$ sono algebre di Boole isomorfe.
(b) Generalizzare l'esercizio precedente dimostrando che, se $|A| = n$, le algebre di Boole $\mathcal{P}(A)$ e $\{0, 1\}^n$ sono isomorfe.

Analogamente, anche nel contesto delle algebre di Boole si ha la nozione di "sotto-oggetto":

Definizione 1.10. *(Sottoalgebra di Boole)* Sia $(B, \vee, \wedge, ', 1, 0)$ un'algebra di Boole. Un sottoinsieme $C \subset B$ è detto una sottoalgebra di Boole se, per ogni $x, y \in C$:
(a) $x \vee y \in C$,
(b) $x \wedge y \in C$,
(c) $x' \in C$.

Esercizio 1.11. Sia $(B, \vee, \wedge, ', 1, 0)$ un'algebra di Boole, e sia C una sua sottoalgebra di Boole. Dimostrare che $0 \in C$, $1 \in C$ e che $(C, \vee, \wedge, ', 1, 0)$ è a sua volta un'algebra di Boole.

Esercizio 1.12. (a) Sia X un'insieme e sia $Y \subset X$ un suo sottoinsieme proprio. Si consideri quindi il sottoinsieme $\mathcal{P}(Y) \subset \mathcal{P}(X)$. È vero che $\mathcal{P}(Y)$ è una sottoalgebra di Boole di $\mathcal{P}(X)$?
(b) Si consideri l'algebra di Boole $\mathcal{P}(\{a, b, c\})$. Determinare tutte le sue sottoalgebre di Boole. (Suggerimento: ad esempio, cominciare col verificare che $\{\emptyset, \{a\}, \{b, c\}, \{a, b, c\}\}$ è una sottoalgebra di Boole.)

2. Equivalenza delle due definizioni

Nella sezione precedente abbiamo visto la definizione di Algebra di Boole come reticolo. Come è facile immaginare, le due definizioni sono equivalenti

Proposizione 2.1. (a) Sia $(B, \vee, \wedge)$ un reticolo limitato, complementato, distributivo. Denotiamo rispettivamente 0 e I il minimo e il massimo di B. Dato $x \in B$ denotiamo x' il suo complemento. Allora $(B, \vee, \wedge, ', 0, I)$ è un'algebra di Boole.
(b) Viceversa, sia $(B, \vee, \wedge, ', 0, 1)$ un'algebra di Boole. Allora essa è un reticolo limitato, complementato e distributivo rispetto alla stesse operazioni.

La dimostrazione consiste nel verificare che gli assiomi della prima nozione implicano quelli della seconda e viceversa. Tutto per esercizio.

È bene ricordare che, a sua volta, la nozione di reticolo è equivalente alla nozione di insieme parzialmente ordinato con certe proprietà (il sup e l'inf esistono sempre). Quindi, in virtù della precedente Proposizione, su un'algebra di Boole esiste sempre una relazione d'ordine, definita da:
$x\,R\,y$ se $x = x \wedge y$,
o, equivalentemente, $x\,R\,y$ se e solo se $y = x \vee y$.

Esercizio 2.2. Sia B un'algebra di Boole, e siano $x, y \in B$.
(a) Dimostrare che $x\,R\,y$ se e solo se $y'\,R\,x'$.
(b) Dimostrare che $x\,R\,y$ se e solo se $x \wedge y' = 0$, e che ciò avviene se e solo se $x' \vee y = 1$.

Osservazione/Esercizio 2.3. Sia B un'algebra di Boole e sia C un sottoinsieme di B. Dinostrare che se C è una sottoalgebra di Boole di B, allora C è un sottoreticolo di B. Si noti che il viceversa non è vero: ad esempio, se $Y \subset X$, $\mathcal{P}(Y)$ è un sottoreticolo di $\mathcal{P}(X)$, ma non è una sottoalgebra di Boole di $\mathcal{P}(X)$ (suggerimento: il punto è che il massimo e il minimo del sottoreticolo Y non coincidono necessariamente con il massimo e il minimo dell'algebra di Boole X. Dunque, dato un sottoinsieme A di Y, il complementare di A in Y non coincide con il complementare di A in X. Infatti, il complementare di A in X può non appartenere a $\mathcal{P}(Y)$.

Esercizio 2.4. Siano B e C due algebre di Boole. Mostrare che un morfismo di reticoli $f : A \to B$ non è necessariamente un morfismo di algebre di Boole (suggerimento: trovare un morfismo di reticoli $f : \mathcal{P}(\{a, b\}) \to \mathcal{P}(\{1, 2, 3\})$ che non è un morfismo di algebre di Boole).

Esercizio 2.5. Siano B e C algebre di Boole. Dimostrare che una funzione $f : B \to C$ è un isomorfismo di algebre di Boole se e solo se è un isomorfismo di reticoli.

Dalla proposizione precedente e dal Teorema di rappresentazione per le Algebre di Boole *finite*, segue:

Teorema 1. *Per ogni algebra di Boole B finita esiste un insieme X tale che B è isomorfa all'algebra di Boole $(\mathcal{P}(X), \cup, \cap, \mathcal{C}_X(), \emptyset, X)$. In particolare, la cardinalità di un'algebra di Boole finita è sempre una potenza di 2.*

Esercizio 2.6. Sappiamo che anche $\{0, 1\}^n$ è un'algebra di Boole finita, per ogni $n \in \mathbb{N}$. Quindi è isomorfa a $\mathcal{P}(\{a_1, \ldots, a_n\})$. Descrivere esplicitamente un isomorfismo tra $\{0, 1\}^n$ e $\mathcal{P}(\{a_1, ..., a_n\})$.

Osservazione 2.7. Ne segue che ogni algebra di Boole *finita* B è isomorfa a $\{0, 1\}^n$, dove n è tale che $2^n = |B|$.

Esercizio 2.8. Dimostrare che $\mathbf{D}_n$ è un algebra di Boole se e solo se n è prodotto di primi *distinti*. In questo caso, sappiamo che $\mathbf{D}_n$ è isomorfo a un $\mathcal{P}(X)$. Che cardinalità ha X, e come si possono descrivere gli isomorfismi tra $\mathbf{D}_n$ e $\mathcal{P}(X)$?

Osservazione 2.9. Attenzione: il teorema di rappresentazione vale solo per Algebre di Boole *finite*. Per algebre di Boole infinite non è vero. Ad esempio, consideriamo il sottoinsieme $\mathcal{A}$ di $\mathcal{P}(\mathbb{N})$ formato dai sottoinsiemi finiti di $\mathbb{N}$ e dai sottoinsiemi il cui complementare è finito. Si ha che $(\mathcal{A}, \cup, \cap, \mathcal{C}_{\mathbb{N}}(), \emptyset, \mathbb{N})$ è un'algebra di Boole (esercizio), che non è isomorfa a nessun insieme delle parti. Quello che si può dimostrare in generale è il cosiddetto *Teorema di rappresentazione di Stone:* data un'algebra di Boole B, esiste sempre un insieme A tale che B è una sottoalgebra di Boole di $\mathcal{P}(A)$. Nell'esempio precedente, $\mathcal{A}$ è una sottoalgebra di Boole di $\mathcal{P}(\mathbb{N})$.

Osservazione 2.10. In realtà si potrebbe dimostrare che le due definizioni di algebra di Boole sono a loro volta equivalenti ad una terza nozione: quella di *Anello Booleano*. In breve, un anello Booleano è un anello commutativo $(B, +, \cdot)$ tale che $x^2 = 1$ per ogni $x \in B$. Data un'algebra di Boole $(B, \vee, \wedge, ', 1, 0)$, si possono definire le operazioni su B: $x + y = (x \wedge y') \vee (x' \wedge y)$, e $x \cdot y = x \wedge y$. Risulta che B, munito di tali operazioni, è un anello Booleano. Viceversa, dato un anello Booleano $(B, +, \cdot)$, si definisce: $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, e $x' = x + 1$. Risulta che, con queste definizioni $(B, \vee, \wedge, ', 0, 1)$ è un'algebra di Boole. Si noti che, sull'insieme delle parti $\mathcal{P}(X)$, l'operazione $A + B$ (dove $A, B \subseteq X$) è la *differenza simmetrica* $(A - B) \cup (B - A)$.