

Fondamenti di Informatica
per la Sicurezza
a.a. 2004/05

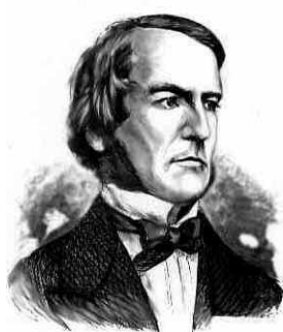
Algebre di Boole

Stefano Ferrari



Università degli Studi di Milano
Dipartimento di Tecnologie
dell'Informazione

George Boole (1815–1864)



Nel 1854, pubblica "An investigation into the Laws of Thought, on Which are founded the Mathematical Theories of Logic and Probabilities".

Boole riduce la logica a semplice algebra, incorporandola nella matematica.

Evidenzia l'analogia tra i simboli algebrici e quelli delle forme logiche.

L'algebra booleana trova applicazioni nella progettazione dei calcolatori.

Algebra booleana

Un'algebra booleana è basata su:

- un insieme di elementi K
- due operazioni chiuse su K ($+$, \cdot)
- una funzione complemento ($\bar{}$)

Assiomi (1)

1. almeno due elementi

$$\exists a, b \in K : a \neq b$$

2. chiusura di $+$ e \cdot

$$\forall a, b \in K :$$

- $a + b \in K$
- $a \cdot b \in K$

Assiomi (2)

3. proprietà commutativa

$\forall a, b \in K :$

- $a + b = b + a$
- $a \cdot b = b \cdot a$

4. proprietà associativa

$\forall a, b, c \in K :$

- $(a + b) + c = a + (b + c) = a + b + c$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$

Assiomi (3)

5. esistenza degli elementi neutri di $+$ e \cdot

- $\exists! 0 \in K : a + 0 = a, \forall a \in K$
- $\exists! 1 \in K : a \cdot 1 = a, \forall a \in K$

6. proprietà distributiva

$\forall a, b, c \in K :$

- $a + (b \cdot c) = (a + b) \cdot (a + c)$
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Assiomi (3)

7. complemento

$$\forall a \in K \exists \bar{a} \in K :$$

- $a + \bar{a} = 1$
- $a \cdot \bar{a} = 0$

Proprietà

Idempotenza $a + a = a$ e $a \cdot a = a$

Leggi di De Morgan $\overline{a + b} = \bar{a} \cdot \bar{b}$ e $\overline{a \cdot b} = \bar{a} + \bar{b}$

Doppio complemento $\overline{\bar{a}} = a$

Elemento nullo $a + 1 = 1$ e $a \cdot 0 = 0$

Tali proprietà possono essere verificate per:

- dimostrazione;
- analisi esaustiva.

Principio di dualità

I teoremi dell'algebra booleana possono essere dimostrati a coppie, scambiando tra loro:

- le operazioni, $+$ \leftrightarrow \cdot ;
- gli elementi neutri, $0 \leftrightarrow 1$.

Teorema di De Morgan (1)

La legge di De Morgan può essere generalizzata a n termini.

$$\overline{X_1 + X_2 + \dots + X_n} = \overline{X_1} \cdot \overline{X_2} \cdot \dots \cdot \overline{X_n}$$

Dimostrazione per induzione:

- caso base:
 - si dimostra vero il caso con il numero minimo di elementi;
- passo di induzione:
 - si ipotizza vero il teorema per $n - 1$ elementi;
 - si utilizza l'ipotesi aggiuntiva per dimostrare il teorema per n elementi.

Teorema di De Morgan (2)

Dimostrazione per induzione:

- caso base:

$$\overline{X_1 + X_2} = \overline{X_1} \cdot \overline{X_2} \quad (\text{Legge di De Morgan})$$

- passo di induzione:

Se per ipotesi, è vero che:

$$\overline{X_1 + \dots + X_{n-1}} = \overline{X_1} \cdot \dots \cdot \overline{X_{n-1}}$$

allora:

$$\begin{aligned} & \overline{(X_1 + \dots + X_{n-1}) + X_n} = \\ & = \overline{(X_1 + \dots + X_{n-1})} \cdot \overline{X_n} = \overline{X_1} \cdot \dots \cdot \overline{X_{n-1}} \cdot \overline{X_n} \end{aligned}$$

Cardinalità

Si può dimostrare che in ogni algebra booleana finita, il numero di elementi di K è una potenza di due.

Esempi

Molte formalizzazioni rispondono agli assiomi dell'algebra di Boole.

Sono algebre di Boole:

- l'algebra binaria;
- l'algebra di insiemi;
- lo spazio degli eventi (calcolo delle probabilità);
- i circuiti logici;
- la logica proposizionale.