Fondamenti di Informatica

per la Sicurezza

a.a. 2003/04

◇ Algebra booleana ◇

Stefano Ferrari

Università degli Studi di Milano

Dipartimento di Tecnologie dell'Informazione

Algebra Booleana

- E' il modello matematico di supporto per lo sviluppo dei circuiti logici e della logica matematica.
- Sviluppata intorno alla metà del 1800.
- L'algebra booleana è basata su:
  - un insieme di elementi K
  - due operazioni chiuse su K ($+$, $\cdot$)
  - una funzione complemento ($^-$)

Assiomi

1. $\exists\, a,\, b \in K :\, a \neq b$
   almeno due elementi
2. $\forall\, a,\, b \in K :\, a + b \in K,\; a \cdot b \in K$
   chiusura di $+$ e $\cdot$
3. $\forall\, a,\, b \in K :\, a + b = b + a,\; a \cdot b = b \cdot a$
   proprietà commutativa
4. $\forall\, a,\, b,\, c \in K :\, (a + b) + c = a + (b + c) = a + b + c,\; (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$
   proprietà associativa

Assiomi (2)

5. - $\exists\, 0 \in K :\, a + 0 = a, \forall\, a \in K$
     identità rispetto a $+$
   - $\exists\, 1 \in K :\, a \cdot 1 = a, \forall\, a \in K$
     identità rispetto a $\cdot$
6. $\forall\, a,\, b,\, c \in K :\, a + (b \cdot c) = (a + b) \cdot (a + c),\; a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   proprietà distributiva
7. $\forall\, a \in K\; \exists\, \bar{a} \in K :$
   - $a + \bar{a} = 1$
   - $a \cdot \bar{a} = 0$

   complemento

Algebra booleana

- L'insieme $K = \{0, 1\}$
- le operazioni OR e AND
- l'operatore NOT

A	B	A OR B	A AND B	NOT A
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

rispettano gli assiomi dell'algebra booleana.

Altre operazioni

Possono essere definite altre operazioni:

A	B	A XOR B	A NAND B	A NOR B
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

In totale ci sono 16 funzioni binarie a due variabili.

Proprietà

Idempotenza

$$A + A = A \qquad \text{e} \qquad A \cdot A = A$$

Leggi di De Morgan

$$\overline{A + B} = \overline{A} \cdot \overline{B} \qquad \text{e} \qquad \overline{A \cdot B} = \overline{A} + \overline{B}$$

Doppia negazione

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

Tali proprietà possono essere dimostrate per:

- dimostrazione
- analisi esaustiva

Principio di dualità

Le proprietà precedenti (e, in generale, i teoremi dell'algebra booleana) possono essere dimostrate a coppie, scambiando:

- $+ \leftrightarrow \cdot$
- $0 \leftrightarrow 1$

Funzione logica

- Una funzione logica è una funzione $\{0, 1\}^N \rightarrow \{0, 1\}$
- $Z = f(X_1, X_2, \cdots, X_N)$
- è una legge che fa corrispondere ad ogni combinazione di valori binari delle variabili indipendenti $X_1, \cdots, X_N$ uno e un solo valore della variabile Z

Teorema di De Morgan

$$\overline{X_1 + X_2 + \cdots + X_n} = \overline{X_1} \cdot \overline{X_2} \cdot \ldots \overline{X_n}$$

Dimostrazione per induzione:

- caso base:
  $\overline{X_1 + X_2} = \overline{X_1} \cdot \overline{X_2}$ *Legge di De Morgan*
- passo di induzione:
  $\overline{(X_1 + X_2 + \cdots + X_{n-1}) + X_n} = \overline{(X_1 + X_2 + \cdots + X_{n-1})} \cdot \overline{X_n}$
  Dimostrazione per elencazione estensiva (tabella di verità)

  La *dimostrazione per induzione* serve per dimostrare un teorema riferito ad una caratteristica enumerabile. Si dimostra prima la validità nel caso base (l'istanza del teorema che coinvolge il minimo numero di elementi), poi, ipotizzando che il teorema sia valido per il caso $n - 1$, lo si dimostra valido per il caso n.