

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

**TITOLO
DELLA
TESI**

Relatore:
Chiar.mo Prof.
UGO DAL LAGO

Presentata da:
FEDERICO PECONI

II Sessione
a.a. 2016/2017

*Questa è la DEDICA:
ognuno può scrivere quello che vuole,
anche nulla ...*

Indice

1	Introduzione	2
2	Funzioni Booleane Bilanciate	3
2.1	Funzioni Booleane	3
2.2	Classi di Funzioni Booleane Bilanciate	5
	Bibliografia	9

Capitolo 1

Introduzione

Capitolo 2

Funzioni Booleane Bilanciate

Come già anticipato nell'Introduzione, le funzioni Booleane bilanciate sono una struttura matematica su cui poggia parte del contenuto di questa tesi. È risultato perciò utile, ai fini di una trattazione chiara ed esaustiva, impiegare un capitolo per definirne in maniera rigorosa i concetti di base.

”Per fare un tavolo ci vuole il legno” recita l’inizio di una famosa canzone per bambini, ad indicare la natura celata delle cose che, così nella quotidianità come nella matematica, spesso necessitano di altre conoscenze per essere comprese appieno; seguendo quindi questa impronta fondazionale, andiamo per prima cosa ad introdurre le funzioni Booleane.

2.1 Funzioni Booleane

Le funzioni Booleane apparvero per la prima volta a metà 19esimo secolo durante la formulazione matematica di problemi logici e prendono il loro nome da George Boole, matematico britannico considerato fondatore della logica matematica odierna^{[ref2](#)}_[2].

Una semplice funzione Booleana può essere rappresentata da
 $l : \{0, 1\}^2 \mapsto \{0, 1\}$

$$f(00) = 0$$

$$f(01) = 0$$

$$f(10) = 1$$

$$f(11) = 0$$

oppure da $f' : \{TRUE, FALSE\} \mapsto \{TRUE, FALSE\}$

$$f'(FALSE) = TRUE$$

$$f'(TRUE) = FALSE$$

Notiamo come entrambe abbiano in comune la dimensione del codominio e la capacità di agire su un numero finito di valori appartenenti ad un insieme di 2 elementi. È tuttavia conveniente operare su di un insieme che possa essere visto sia dal punto di vista qualitativo (vero, falso) sia da un punto di vista quantitativo, e quindi numerico, che ci permetta così di compiere anche operazioni algebriche oltre che logiche. Prediligeremo allora da qui in avanti, l'insieme $\{0, 1\}$ come campo vettoriale su cui lavorare.

Definizione 2.1. Una funzione Booleana a n variabili è una funzione da \mathcal{B}^n a \mathcal{B} , dove $\mathcal{B} = \{0, 1\}$, $n > 0$ e \mathcal{B}^n è l' n -esimo prodotto cartesiano di \mathcal{B} con se stesso.^[ref3]

Corollario. $\forall n > 0$, ci sono 2^{2^n} funzioni da \mathcal{B}^n a \mathcal{B} .

Dimostrazione. Sia $\mathcal{F} = \{f | f : \mathcal{B}^n \mapsto \mathcal{B}\}$, ogni f riceve in input n -uple $\vec{x} = (x_1, \dots, x_n)$ che possono essere viste come sequenze di n bit. In n bit possiamo codificare 2^n oggetti differenti, quindi $|\mathcal{B}^n| = 2^n$. Per ogni \vec{x} , $f(\vec{x}) = 0$ oppure $f(\vec{x}) = 1$, quindi ogni possibile f individua un sottoinsieme di \mathcal{B}^n .

Allora \mathcal{F} corrisponde all'insieme delle parti per \mathcal{B}^n , quindi $|\mathcal{F}| = 2^{\mathcal{B}^n} = 2^{2^n}$

□

Un altro modo più tradizionale per descrivere una funzione Booleana è quello di fornire la sua tabella di verità. Ad esempio, per la f precedentemente definita, la tabella di verità relativa sarà:

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	0
1	0	1
1	1	0

In entrambe le rappresentazioni, tuttavia, le funzioni vengono descritte in maniera implicita mostrando solamente input e output, senza mai andare a specificare come questo output venga calcolato.

Nell'ultimo capitolo, per l'implementazione dell'algoritmo di Deutsch-Jozsa, verranno utilizzate funzioni Booleane *bilanciate* che necessitano di essere calcolate esplicitamente. La prossima sezione introduce questa categoria di funzioni Booleane e propone due metodi effettivi e generali per produrne istanze concrete.

2.2 Classi di Funzioni Booleane Bilanciate

Sia f una funzione Booleana, chiamiamo $\vec{x} = (x_1, \dots, x_n)$ *vettore positivo* per f se e solo se $f(\vec{x}) = 1$, *vettore negativo* altrimenti. Sia $|f|^1$ la quantità che indica il numero di vettori positivi per f e $|f|^0$ la quantità che indica il numero di vettori negativi.

Definizione 2.2. Una funzione Booleana f è detta *bilanciata (FBB)* se e solo se $|f|^1 = |f|^0$.

Una valida tabella di verità per una FBB in \mathcal{B}^3 portebbe essere la seguente:

(x_1, x_2, x_3)	$f(x_1, x_2, x_3)$
(0, 0, 0)	0
(0, 0, 1)	1
(0, 1, 0)	1
(0, 1, 1)	0
(1, 0, 0)	1
(1, 0, 1)	0
(1, 1, 0)	0
(1, 1, 1)	1

Ma come è costruita f nello specifico? Qual'è la computazione che mi porta a determinati outputs? Per rispondere a queste domande si può provare a cercare qualche correlazione tra i valori in entrata e i valori in uscita: dopo un pò di riflessione dovrebbe saltare all'occhio che ogni qual volta abbiamo un numero dispari di 1 nell'input la funzione restituisce 1, restituisce invece 0 quando tale numero è pari. La parità di una sequenza è esprimibile con la somma modulo 2 dei singoli componenti, possiamo definire esplicitamente f come

$$\begin{aligned} f(x_1, x_2, x_3) &= x_1 + x_2 + x_3 \mod 2 \\ &= (x_1 \oplus x_2) \oplus x_3 \\ &= x_1 \oplus x_2 \oplus x_3 \end{aligned}$$

dove \oplus è un connettivo binario logico (una funzione Booleana $\in \mathcal{B}^2$) chiamato XOR oppure OR esclusivo, che restituisce 1 se uno ed uno solo dei due elementi vale 1

(x_1, x_2)	$\oplus(x_1, x_2)$
(0, 0)	0
(0, 1)	1
(1, 0)	1
(1, 1)	0

Teorema 1. Per ogni $n > 0$ la funzione Booleana $f^n(x_1, x_2, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ è una FBB.

Dimostrazione. (per induzione su n)

Base induttiva $f^1(x) = x$ è trivialmente bilanciata.

Ipotesi induttiva Ipotizziamo f^n bilanciata, quindi esistono due partizioni

$\mathcal{M} \subset \mathcal{B}^n$ e $\mathcal{N} \subset \mathcal{B}^n$ t.c. $|\mathcal{M}| = |\mathcal{N}|$, $\mathcal{M} \cup \mathcal{N} = \mathcal{B}^n$ e $\forall m, n$ con $m \in \mathcal{M}, n \in \mathcal{N}$ risulta $f^n(m) = 1$ e $f^n(n) = 0$.

Passo induttivo Avremo $f^{n+1} : \mathcal{B}^{n+1} \mapsto \mathcal{B}$ dove $\mathcal{B}^{n+1} = \mathcal{B}^n \cdot 0 \cup \mathcal{B}^n \cdot 1$ e

$|\mathcal{B}^{n+1}| = 2|\mathcal{B}^n|$. Dobbiamo quindi dimostrare che esiste una partizione $(\mathcal{M}', \mathcal{N}')$ t.c.:

- $|\mathcal{M}'| = |\mathcal{B}^n|$ e $\forall m' \in \mathcal{M}' \ f^{n+1}(m') = 1$
- $|\mathcal{N}'| = |\mathcal{B}^n|$ e $\forall n' \in \mathcal{N}' \ f^{n+1}(n') = 1$

Notiamo come, $\forall m, n$ con $m \in \mathcal{M}, n \in \mathcal{N}$ se

$$x_{n+1} = 0 \Rightarrow f^{n+1}(m \cdot 0) = 1 \wedge f^{n+1}(n \cdot 0) = 0$$

$$x_{n+1} = 1 \Rightarrow f^{n+1}(m \cdot 1) = 0 \wedge f^{n+1}(n \cdot 1) = 1$$

Segue naturalmente che la partizione $\mathcal{M}' = \mathcal{M} \cdot 0 \cup \mathcal{N} \cdot 1$ e $\mathcal{N}' = \mathcal{M} \cdot 1 \cup \mathcal{N} \cdot 0$ rispetta i criteri cercati.

□

Si richiami dall'Algebra Lineare che, $f : \mathcal{V} \mapsto \mathcal{W}$ è un'applicazione lineare se e solo se esiste una matrice $M \in \mathbb{M}^{k \times l}$, dove $k = |\mathcal{V}|$ e $l = |\mathcal{W}|$ sono le dimensioni degli spazi vettoriali su cui agisce, tale che $f(\vec{x}) = M\vec{x}$.

Definizione 2.3. $b : \mathcal{B}^n \mapsto \mathcal{B}$ è una funzione booleana lineare (FBL) se e solo se esiste $M \in \mathbb{B}^{n \times 1}$ tale che $b(\vec{x}) = M\vec{x} = c_1x_1 + c_2x_2 + \dots + c_nx_n = (c_1 \wedge x_1) \oplus (c_2 \wedge x_2) \oplus \dots \oplus (c_n \wedge x_n)$. Dove \oplus è l'operatore di somma per \mathcal{B}^n .

Corollario. Per ogni $n > 0$, f^n è una FBL.

Dimostrazione. Triviale, basta infatti porre $M = \overbrace{(1, 1, \dots, 1)}^{n\text{-volte}}$.

□

Introdotte le FBB e le FLB, possiamo a questo punto procedere con la formulazione del seguente risultato generale:

Teorema 2. Sia $\mathbb{FL} = \{f | f \in FLB \wedge f \neq c : \mathcal{B}^n \mapsto \{0\}, \forall n > 0\}$ la classe di tutte le funzioni Booleane lineari diverse dalle funzioni costanti a 0. Allora, $\forall f \in \mathbb{FL}$ f è bilanciata.

Dimostrazione. (per induzione su n)

Sia l^n una qualsiasi funzione da \mathcal{B}^n appartenente a \mathbb{FL} . Vogliamo dimostrare che l^n è sempre bilanciata.

Base induttiva $l^1(x) = x$ è trivialmente bilanciata.

Ipotesi induttiva Ipotizziamo l^n bilanciata.

Esisteranno quindi due partizioni

$\mathcal{M} \subset \mathcal{B}^n$ e $\mathcal{N} \subset \mathcal{B}^n$ tali che $|\mathcal{M}| = |\mathcal{N}|$, $\mathcal{M} \cup \mathcal{N} = \mathcal{B}^n$ e $\forall m, n$ con $m \in \mathcal{M}, n \in \mathcal{N}$ risulta $l^n(m) = 1$ e $l^n(n) = 0$.

Passo induttivo Il passo chiave sta nel notare che l^{n+1} può assumere esclusivamente una delle seguenti forme:

- **Singoletto** $l^{n+1}(\vec{x}) = l^{n+1}(x_1, x_2, \dots, x_{n+1}) = x_{n+1}$

Che è bilanciata in quanto sia $(\mathcal{M}, \mathcal{N})$ la partizione dove \mathcal{M} è composto da tutt

- **Uguale a l^n**
- **Xor di l^n**

□

Bibliografia

- ref1** [1] Higham, N. (1998). *Handbook of writing for the mathematical sciences*. Philadelphia: SIAM, Soc. for Industrial and Applied Mathematics.
- ref2** [2] Encyclopediaofmath.org. (2017). *Boolean function - Encyclopedia of Mathematics*. [online]
- ref3** [3] Crama, Y. and Hammer, P. (2011). *Boolean Functions Theory, Algorithms and Applications*. 1st ed. Cambridge University Press, p.4.