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

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. É 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[2].

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

$$f(00) = 0$$
$$f(01) = 0$$
$$f(10) = 1$$
$$f(11) = 0$$

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'inisieme $\{0,1\}$ 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] *[3]*

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 $\vec{x} = (x_1, .., x_n)$ che possono essere viste come sequenze di n bit. In n bit possiamo codificare, trattandosi di una distribuzione con ripetizione di classe n, 2^n oggetti differenti, quindi $\mathbb{D}_{2,n} = |\mathcal{B}^n| = 2^n$. 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

Dove a destra viene posto il risultato della funzione calcolata sui valori delle colonne precedenti.

In entrambe le rappresentazioni, tuttavia, le funzioni vengono descritte in maniera implicita mostrando solamente input ed 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 $\vec{x} = (x_1, .., x_n)$ *vettore positivo* per f se e solo se $f(\vec{x}) = 1$, *vettore negativo* altrimenti. Sia $(|f|^1,|f|^0)$ la partizione dove $|f|^1$ è 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 $|f|^1 = |f|^0$.*

Corollario. $\forall\ n > 0$, *ci sono* $\frac{2^n!}{(2^{n-1}!)^2}$ *FBB da* $\mathcal{B}^n$ *a* $\mathcal{B}$.

Dimostrazione. Per definizione, una FBB $fbb : \mathcal{B}^n \mapsto \mathcal{B}$ è individuata da una partizione $(\mathcal{M}, \mathcal{N})$ con $\mathcal{M} \subset \mathcal{B}^n$ e $\mathcal{N} \subset \mathcal{B}^n$ tale che $|\mathcal{M}| = |\mathcal{N}| = 2^{n-1}$ e $fbb(m) = 0 \wedge fbb(n) = 1$ $\forall m, n$ con $m \in \mathcal{M}, n \in \mathcal{N}$. Quindi, il numero delle possibili funzioni corrisponde a tutti i possibili modi di partizionare a metà un insieme di 2^n elementi e, a sua volta, ogni partizione può essere rappresentata da un sottoinsieme $\mathcal{S} \subset \mathcal{B}^n$ dove $\mathcal{M} = \mathcal{S}$ e $\mathcal{N} = \mathcal{B}^n \setminus \mathcal{S}$. Non resta quindi che trovare tutti i possibili $\mathcal{S}$:

$$\mathbb{C}_{2^n,2^{n-1}} = \binom{2^n}{2^{n-1}} = \frac{2^n!}{2^{n-1}!2^{n-1}!} = \frac{2^n!}{(2^{n-1}!)^2}$$

□

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

(x_1, x_2, x_3)	$g(x_1, x_2, x_3)$
$(0, 0, 0)$	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

Dove, giustamente, si noti come il numero dei vettori positivi equivale al numero dei vettori negativi.

Ma come è costruita g 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, allora possiamo definire esplicitamente g come:

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

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

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

Dimostrazione. (per induzione su n)

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

Ipotesi induttiva: Ipotizziamo f^n bilanciata, quindi esiste la partizione $(\mathcal{M}, \mathcal{N})$ con $\mathcal{M} \subset \mathcal{B}^n$ e $\mathcal{N} \subset \mathcal{B}^n$ tale 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 $f^n(m) = 0$ e $f^n(n) = 1$.

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 $\forall m' \in \mathcal{M}'$ $f^{n+1}(m') = 0$
- $|\mathcal{N}'| = |\mathcal{B}^n|$ 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
$x_{n+1} = 0 \Rightarrow f^{n+1}(m \cdot 0) = 0 \wedge f^{n+1}(n \cdot 0) = 1$
$x_{n+1} = 1 \Rightarrow f^{n+1}(m \cdot 1) = 1 \wedge f^{n+1}(n \cdot 1) = 0$
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 $b(\vec{x}) = M\vec{x} = c_1x_1 + c_2x_2 +, ..., +c_nx_n = (c_1 \wedge x_1) \oplus (c_2 \wedge x_2) \oplus, ..., \oplus (c_n \wedge x_n)$. 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 $M = \overbrace{(1, 1, ..., 1)}^{n-volte}$. □

2.2.1 La Classe delle Funzioni Booleane Lineari

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

Teorema 1. *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.
Esisterà quindi la partizione $(\mathcal{M}, \mathcal{N})$ con $\mathcal{M} \subset \mathcal{B}^n$ e $\mathcal{N} \subset \mathcal{B}^n$ tale 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 $l^n(m) = 0$ e $l^n(n) = 1$.

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

- **Singoletto** $\Rightarrow l^{n+1}(\vec{x}) = l^{n+1}(x_1, x2, ..., x_{n+1}) = x_{n+1}$
  Che è bilanciata in quanto, sia $(\mathcal{M}, \mathcal{N})$ la partizione dove $\mathcal{M}$ è composto da

tutte le stringhe binarie $\in \mathcal{B}^{n+1}$ che codificano in base due i numeri da 0 a $2^n - 1$ e $\mathcal{N}$ composto da tutte le stringhe binarie $\in \mathcal{B}^{n+1}$ che codificano in base due i numeri da 2^n a $2^{n+1} - 1$ i.e. :
$\mathcal{M} = \{\vec{x} \in \mathcal{B}^{n+1} | \vec{x} = 0 \cdot x_n \cdot x_{n-1} \cdot ... \cdot x_1\}$
$\mathcal{N} = \{\vec{x} \in \mathcal{B}^{n+1} | \vec{x} = 1 \cdot x_n \cdot x_{n-1} \cdot ... \cdot x_1\}$
Allora $\mathcal{M} \subset \mathcal{B}^{n+1}$ e $\mathcal{N} \subset \mathcal{B}^{n+1}$, $|\mathcal{M}| = |\mathcal{N}|$, $\mathcal{M} \cup \mathcal{N} = \mathcal{B}^{n+1}$ e e $\forall m, n.$ $m \in \mathcal{M}$,$n \in \mathcal{N}$ risulta $l^{n+1}(m) = 0$ e $l^{n+1}(n) = 1$.

- **Uguale a** $l^n \Rightarrow$ Bilanciata per ipotesi.
- **Xor di** $l^n \Rightarrow l^{n+1}(\vec{x}) = l^{n+1}(x_1, x2, ..., x_{n+1}) = x_{n+1} \oplus l^n$.
  E quindi se:
  $x_{n+1} = 0 \Rightarrow l^{n+1} = 0 \oplus l^n = l^n$
  $x_{n+1} = 1 \Rightarrow l^{n+1} = 1 \oplus l^n = \neg l^n$
  Individuiamo, concludendo la dimostrazione, la partizione cercata $(\mathcal{M}', \mathcal{N}')$ con:
  $\mathcal{M}' = M \cdot 0 \cup N \cdot 1$ e $\mathcal{N}' = M \cdot 1 \cup N \cdot 0$.

□

Questo significa che, qualsiasi siano i coefficienti della nostra FBL, a patto che questi non siano tutti 0, produrrano anche una funzione bilanciata.

Giunti a questo punto è lecito domandarsi se esistano altre (semanticamente diverse) FBB non lineari e se sì, quante ne si possono ancora trovare? Il numero di FBL per n fissato, equivale al numero di *disposizioni con ripetizione di classe n* (coefficienti) da un insieme di due elementi $\{0, 1\}$ meno la disposizione $M^* = \overbrace{(0, 0, ..., 0)}^{n-volte}$ che identifica la costante 0, cioè $\mathbb{D}_{2,n} - 1 = 2^n - 1$. Tale numero è chiaramente inferiore al numero di FBB : $\mathbb{C}_{2^n, 2^{n-1}}$ ricavato dal Corollario 2.2. E quindi sì, esisteranno sicuramente, per ogni n, $\mathbb{C}_{2^n, 2^{n-1}} - (\mathbb{D}_{2,n} - 1)$ FBB non lineari.

2.2.2 Funzioni Booleane non Lineari Bilanciate

L'approfondimento delle proprietà e della teoria riguardante il vasto campo di studi delle funzioni Booleane, per quanto interessante, esula dai fini della tesi in oggetto. Ri-

manendo in tema, tuttavia, è bene accennare che la ricerca, specie per quanto riguarda l'indagine sulle funzioni booleane bilanciate è molto attiva e di fondamentale importanza in applicazioni come la crittografia a chiave simmetrica.[ref4]
Per rendere più realistica e articolata l'implementazione degli script presentati nel Capitolo 5, si è optato per la ricerca in letteratura di funzioni booleane bilanciate non lineari da utilizzare nell'algoritmo di Deutsch-Jozsa. In particolare, è stata scelta una funzione a 5 variabili, ricavata con il metodo generale esposto da *Logachev*[ref5]:

$$h(x_1, x_2, x_3, x_4, x_5) = (x_1 \wedge x_2) \oplus x_3 \oplus (x_2 \wedge x_3 \wedge x_4) \oplus (x_2 \wedge x_3 \wedge x_5) \oplus (x_3 \wedge x_4) \oplus (x_4 \wedge x_5)$$

a	b	c	d	e	$c \veebar (a \wedge b) \veebar (c \wedge d) \veebar (d \wedge e) \veebar (b \wedge c \wedge d) \veebar (b \wedge c \wedge e)$
T	T	T	T	T	F
T	T	T	T	F	F
T	T	T	F	T	T
T	T	T	F	F	F
T	T	F	T	T	F
T	T	F	T	F	T
T	T	F	F	T	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	T	T	F	F
T	F	T	F	T	T
T	F	T	F	F	T
T	F	F	T	T	T
T	F	F	T	F	F
T	F	F	F	T	F
T	F	F	F	F	F
F	T	T	T	T	T
F	T	T	T	F	T
F	T	T	F	T	F
F	T	T	F	F	T
F	T	F	T	T	T
F	T	F	T	F	F
F	T	F	F	T	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	T	T	F	F
F	F	T	F	T	T
F	F	T	F	F	T
F	F	F	T	T	T
F	F	F	T	F	F
F	F	F	F	T	F
F	F	F	F	F	F

Computed by Wolfram|Alpha

Figura 2.1: Tabella di verità per h

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.

ref4 [4] Dobbertin, Hans. *Construction of bent functions and balanced Boolean functions with high nonlinearity.* International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1994.

ref5 [5] Logachev, O. A. *On Perfectly Balanced Boolean Functions.* IACR Cryptology ePrint Archive 2007 (2007): 22.