Bent functions and strongly regular graphs

Valentino Smaldore

Abstract

The family of bent functions is a known class of Boolean functions, which have a great importance in cryptography. The Cayley graph defined on \( \mathbb{Z}_2^n \) by the support of a bent function is a strongly regular graph \( srg(v, k, \lambda, \mu) \), with \( \lambda = \mu \). In this note we list the parameters of such Cayley graphs. Moreover, it is given a condition on \((n, m)\)-bent functions \( F = (f_1, \ldots, f_m) \), involving the support of their components \( f_i \), and their \( n \)-ary symmetric differences.

1 Introduction

A cryptosystem is an encryption and decryption algorithm for a message. If Alice wants to send a message \( p \) to Bob, the encryption algorithm \( E \) computes the cyphertext \( z \) starting from a key \( K_A \), i.e. \( z = E(p, K_A) \). Bob uses the decryption algorithm \( D \) to recover \( p \) from a key \( K_B \), i.e. \( p = D(z, K_B) \). Necessarily, for all \( p, K_A, K_B \), \( D(E(p, K_A), K_B) = p \). Cryptosystems are called private key, if the parties know each other and have shared informations about their private keys, or public key if it is not necessary that the two parties know each other, and they have two public keys. The best

\[ \text{https://doi.org/10.32388/A2V6PB} \]
known private key algorithms are DES (Data Encryption System) and its successor AES (Advanced Encryption System). The reader can find more information on cryptography in [11]. One of the most important features for cryptographic algorithms is the confusion, i.e. the relation between any bit and all the plaintext appearing random. After the linear cryptanalysis techniques of A. Matsui [10], one of the research items in cryptography was to find functions as far as possible from the linear functions, i.e. maximizing the Hamming distance, in order to resist to linear attacks, see [3]. Among the family of Boolean functions, such functions are called bent functions. In [1, 2] it is given a characterization of bent functions in terms of strongly regular graphs. Here, we give considerations on parameters of such strongly regular graphs, and a first characterization of $(n, m)$-bent functions.

2 Preliminaries

Let $\mathbb{Z}_2$ be the binary field. A Boolean function is a function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ and to denote $f$ we will use two different notations: the classical notation, where the input string is given by $n$ binary variables, and the $2^n$-tuple vector representation $f = (f_0 f_1 \ldots f_{2^n-1})$ where $f_i = f(b(i))$ and $b(i)$ is the binary expansion of the integer $i$. We will denote by $\Omega_f$ the support of $f$, i.e.

$$\Omega_f = \{w \in \mathbb{Z}_2^n | f(w) \neq 0\} = \{w \in \mathbb{Z}_2^n | f(w) = 1\}.$$

**Definition 2.1.** Let $l$ be a Boolean function.

- We say that $l$ is a linear function if $\forall x, y \in \mathbb{Z}_2^n$, $l(x + y) = l(x) + l(y)$.

- We say that $l$ is an affine function if it is a linear function plus a constant in $\mathbb{Z}_2$.

We denote with $\mathcal{A}$ the set of all affine functions.

The nonlinearity of a Boolean function $f$ is the minimum Hamming distance between $f$ and an affine function, i.e.

$$Nl(f) = \min_{\phi \in \mathcal{A}} |\{x \in \mathbb{Z}_2^n | f(x) \neq \phi(x)\}|.$$
Definition 2.2. A Boolean function $f$ is called bent function if $Nl(f) = \frac{2^n - 2^n}{2}$.

Here we define the Abstract Fourier Transform of a Boolean function $f$ as the rational valued function $f^*$ which defines the coefficients of $f$ with respect to the orthonormal basis of the group characters $Q_w(x) = (-1)^{(w \cdot x)}$, when "·" is the standard inner product and $w \cdot x = \sum_{i=1}^{n} x_i w_i = Tr^n_1(w x)$.

Then $f^*(w) = \frac{\sum_{x \in \mathbb{Z}_2^n} (-1)^{Tr^n_1(w x)} f(x)}{2^n}$.

Note that $f^*(b(0)) = \frac{|\Omega_f|}{2^n}$. The Walsh spectrum is the set of values of $f^*(w)$. Here we investigate the spectrum in terms of a graph eigenvalue problem.

3 The Cayley graph $Cay(\mathbb{Z}_2^n, \Omega_f)$

Definition 3.1. Let $\Gamma$ be a group with identity $e$.

- A Cayley subset, is a subset $C \subseteq \Gamma$ such that $e \notin C$ and whenever $g \in C$, then $g^{-1} \in C$.

- The Cayley graph $G = Cay(\Gamma, C)$ of $\Gamma$ with respect to $C$ is the graph whose vertex set is $\Gamma$, when two vertices $g$ and $h$ are adjacent if and only if $gh^{-1} \in C$.

We modify this definition by dropping the condition $e \notin C$, allowing loops in the Cayley graph.

Consider now the additive group $(\mathbb{Z}_2^n, \oplus)$, where $\oplus$ is the component-wise sum. For all $w \in \mathbb{Z}_2^n$, $w^{-1} = w$, then each subset of $\mathbb{Z}_2^n$ is a Cayley subset. We can associate each Boolean function $f$ to the Cayley graph $G_f = Cay(\mathbb{Z}_2^n, \Omega_f)$. The vertex-set $V(G_f)$ is the whole $\mathbb{Z}_2^n$, while the edge-set is $E(G_f) = \{(u, v) \in \mathbb{Z}_2^n | u \oplus v \in \Omega_f\} = \{(u, v) \in \mathbb{Z}_2^n | f(u \oplus v) = 1\}$. The graph has $2^n - \dim(\Omega_f)$ vertices which are the cosets of $\langle \Omega_f \rangle$ in $\mathbb{Z}_2^n$. Since eigenvectors of the Cayley graph are exactly the group characters $Q_w(x) = (-1)^{Tr^n_1(w x)}$, ...
see [13], the following two results give a characterization of the spectrum of
$G_f$ from the Walsh spectrum of $f$.

Result 3.2. [1, Theorem 1] The $i$-th eigenvalue $\lambda_i$ of the Cayley graph, which
corresponds to the eigenvector $Q_{b(i)}$, is given by

$$\lambda_i = \sum_{x \in \mathbb{Z}_2^n} (-1)^{Tr^n_i(b(i)x)} f(x) = 2^n f^*(b(i)).$$

Result 3.3. [1, Proposition 2]

1. The largest spectral coefficients is $\lambda_0 = 2^n f^*(b(0)) = |\Omega_f|$, with multi-
plicity $2^{n-\dim(\Omega_f)}$.

2. The number of non zero spectral coefficients is the rank of the adjacency
   matrix of $G_f$.

3. If $G_f$ is connected, $f$ has a spectral coefficient equal to $-\lambda_0$ if and only
   if its Walsh spectrum is symmetric with respect to 0.

4 Strongly regular graphs

A strongly regular graph with parameters $(v, k, \lambda, \mu)$, denoted by $srg(v, k, \lambda, \mu)$,
is a graph with $v$ vertices, each vertex lies on $k$ edges, any two adjacent ver-
tices have $\lambda$ common neighbours and any two non-adjacent vertices have $\mu$
common neighbours. We give now some folklore results on strongly regular
graphs, see [4] for more details.

Result 4.1. $k(k - \lambda - 1) = \mu(v - k - 1)$.

The spectrum of the adjacency matrix of an $srg(v, k, \lambda, \mu)$ is fully deter-
mined by its parameters.

Result 4.2. A strongly regular graph $G$ with parameters $(v, k, \lambda, \mu)$ has ex-
tactly three eigenvalues: $k, \theta_1$ and $\theta_2$ of multiplicity, respectively, 1, $m_1$ and
$m_2$, where:

$$\theta_1 = \frac{1}{2} \left[ (\lambda - \mu) + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)} \right],$$
\[ \theta_2 = \frac{1}{2} \left[ (\lambda - \mu) - \sqrt{(\lambda - \mu)^2 + 4(k - \mu)} \right], \]
\[ m_1 = \frac{1}{2} \left[ (v - 1) - \frac{2k - (v - 1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}} \right], \]
\[ m_2 = \frac{1}{2} \left[ (v - 1) + \frac{2k - (v - 1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}} \right]. \]

We write the spectrum as \( k, \theta_1^{m_1}, \theta_2^{m_2} \). On the other hand, we can express the parameters of a strongly regular graph starting from its spectrum

\[ v = 1 + m_1 \theta_1 + m_2 \theta_2, \]
\[ \lambda = k + \theta_1 \theta_2 + \theta_1 + \theta_2, \]
\[ \mu = k + \theta_1 \theta_2 = \lambda - \theta_1 - \theta_2, \]

Corollary 4.3. Consider a \( srg(v, k, \lambda, \mu) \), with spectrum \( k, \theta_1^{m_1}, \theta_2^{m_2} \). Then \( \lambda = \mu \) if and only if \( \theta_1 = -\theta_2 \).

Result 4.4. The parameters \( \lambda \) and \( \mu \) of a \( srg(v, k, \lambda, \mu) \) may be derived from its spectrum, since:

\[ \begin{cases} 
\lambda = k + \theta_1 \theta_2 + \theta_1 + \theta_2 \\
\mu = k + \theta_1 \theta_2.
\end{cases} \tag{1} \]

In [1, 2] is given a characterization of bent functions in a graph theoretical point of view.

Result 4.5. [1, Lemma 12] If \( f \) is a bent function, the graph \( G_f \) is a strongly regular graph with \( \lambda = \mu \).

Result 4.6. [2, Theorem 3] Bent functions are the only functions whose associated Cayley graph \( G_f \) is a strongly regular graph with \( \lambda = \mu \).

Proposition 4.7. The Cayley graph \( G_f \) of a bent function is exactly one of the following:

\[ srg(2^n, \frac{2^n+2^n}{2}, \frac{2^n+2^n-2^n}{2}, \frac{2^n+2^n-2^n}{2}). \]
Proof. From [1, Definition 4] we know the three eigenvalues $k, \theta_1, \theta_2 = -\theta_1$ of $G_f$. From 4.4 we get the parameters $\lambda$ and $\mu$, while 4.1 allows us to compute $v = 2^n = |\mathbb{Z}_2^n|$. 

\[ \text{Example 4.8. The first strongly regular graph defined by bent functions are} \]

\begin{itemize}
  \item $n = 2$ \hspace{1cm} $srg(4, 3, 1, 1)$, \textit{i.e.} the complete graph $K_4$.
  \item $n = 2$ \hspace{1cm} $srg(4, 1, 0, 0)$, \textit{i.e.} a trivial strongly regular graph made of 2 disconnected edges.
  \item $n = 4$ \hspace{1cm} $srg(16, 10, 6, 6)$.
  \item $n = 4$ \hspace{1cm} $srg(16, 10, 2, 2)$.
  \item $n = 6$ \hspace{1cm} $srg(64, 36, 20, 20)$.
  \item $n = 6$ \hspace{1cm} $srg(64, 28, 12, 12)$.
  \item $n = 8$ \hspace{1cm} $srg(256, 136, 72, 72)$.
  \item $n = 8$ \hspace{1cm} $srg(256, 120, 56, 56)$.
  \item $n = 10$ \hspace{1cm} $srg(1024, 528, 272, 272)$.
  \item $n = 10$ \hspace{1cm} $srg(1024, 496, 240, 240)$.
\end{itemize}

Note that in each case graphs have the parameters of the complements of the affine polar graphs $VO^\pm(2n, 2)$, which is the graph arising from a quadric $Q$ in the vector space $V = V(2n, 2)$ and two points $u, v \in V$ represent adjacent vertices if and only if $Q(u - v) = 0$. Note that the quadric is elliptic or hyperbolic while we consider the first or the second example, respectively. See the table of strongly regular graphs in [5] for more details.
5 Vectorial bent function

Consider now functions $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$, $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$, where for each $i$, $f_i : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$. The set of affine vectorial functions $\mathcal{A}_{n,m}$ is defined as in the case $m = 1$. We can introduce two different ways to express the nonlinearity of a vectorial Boolean function:

$$nl(F) = \min_{v \in \mathbb{Z}_2^n \setminus \{0\}} Nl(F \cdot v)$$  \hspace{1cm} (2)

$$Nl(F) = \min_{\phi \in \mathcal{A}_{n,m}} \left| \{x \in \mathbb{Z}_2^n | F(x) \neq \phi(x) \} \right|$$  \hspace{1cm} (3)

**Definition 5.1.** A $(n, m)$-bent function, or vectorial bent function, is a function $F = (f_1, \ldots, f_m)$ such that $nl(F) = 2^{n-\frac{2^m}{2}}$ or equivalently each linear combination of $f_1, \ldots, f_m$ is a bent function.

In order to give graph based properties of $(n, m)$-bent functions we need now to define the set operation symmetric difference, which is the equivalent of the logical operation XOR.

**Definition 5.2.** The symmetric difference between two sets $A$ and $B$ is

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

**Proposition 5.3.** The power set of any set $X$ is an elementary abelian 2-group under the operation of symmetric difference.

**Proof.** The symmetric difference is commutative and associative:

- $A \triangle B = B \triangle A$;
- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Moreover the empty set is the identity and each element has order two:

- $A \triangle \emptyset = A$;
- $A \triangle A = \emptyset$.
An elementary abelian 2-group is also called Boolean group, see [8] for more details.

The symmetric difference of a collection of sets is made of elements contained in an odd number of sets. The $n$-ary symmetric difference is defined as follows:

$$\triangle M = \left\{ a \in \bigcup M \big| \sharp\{ A \in M | a \in A \} = 2k + 1 \right\} ,$$

Proposition 5.4. Consider a vectorial Boolean function $F = (f_1, \ldots, f_m)$, with $f_i : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, and let $\Omega_i = \Omega_{f(i)}$ be the support of $f_i$, of $i = 1, \ldots, m$. If the function $F$ is $(n, m)$-bent, then the Cayley graphs $\text{Cay} (\mathbb{Z}_2^n, \triangle_{i \in I} \Omega_i)$ are strongly regular with $\lambda = \mu$ for all index subset $I \subseteq [1, \ldots, m]$.

References


