Qeios

Bent functions and strongly regular graphs

June 17, 2024

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 paper we list the parameters of such Cayley graphs. Moreover, a condition is given 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.

Keywords:bent functions, strongly regular graphs

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 *ciphertext* 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 information 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 known private key algorithms are *DES* (Data Encryption Standard) and its successor *AES* (Advanced Encryption Standard). The reader can find more information on cryptography in [12]. One of the most important features of cryptographic algorithms is the *confusion*, i.e. the relation between any

https://doi.org/10.32388/A2V6PB.2

bit and all the plaintext appearing at random. After the linear cryptanalysis techniques of H. Matsui [11], one of the research items in cryptography was to find functions as far as possible from the linear functions, that is 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] a characterization of bent functions is given 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 $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ 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 Ω_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 $Nl(f) = \frac{2^n - 2^{\frac{n}{2}}}{2}$.*

Note that by Definition 2.2 n must be even. Bent functions are also called PN (perfectly nonlinear). 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 $Q_w(x) = (-1)^{(w \cdot x)}$, where " $\cdot$ " is the standard inner product and $w \cdot x = \sum_{i=1}^{n} x_i w_i = Tr_1^n(wx)$. Then

$$f^*(w) = \frac{\sum_{x \in \mathbb{Z}_2^n} (-1)^{Tr_1^n(wx)} f(x)}{2^n}.$$

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 Γ 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 Γ with respect to C is the graph whose vertex set is Γ, 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 componentwise 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 $2^{n - dim\langle\Omega_f\rangle}$ 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 $Q_w(x) = (-1)^{Tr_m^n(wx)}$, see [14],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 λ_i of the Cayley graph, which corresponds to the eigenvector $Q_{b(i)}$, is given by*

$$\lambda_i = \sum_{x \in \mathbb{Z}_2^n} (-1)^{Tr_1^n(b(i)x)} f(x) = 2^n f^*(b(i)).$$

Result 3.3. *[1, Proposition 2]*

1. *The largest spectral coefficients is $\lambda_0 = 2^n f^*(b(0)) = |\Omega_f|$, with multiplicity $2^{n-dim\langle\Omega_f\rangle}$.*
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, λ, μ), denoted by $srg(v, k, \lambda, \mu)$, is a graph with v vertices, each vertex lies on k edges, any two adjacent vertices have λ common neighbours and any two non-adjacent vertices have μ 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 determined by its parameters.

Result 4.2. *A strongly regular graph G with parameters (v, k, λ, μ) has exactly three eigenvalues: k, θ_1 and θ_2 of multiplicity, respectively, 1, m_1 and m_2, where:*

$$\theta_1 = \frac{1}{2}\Big[(\lambda - \mu) + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\Big],$$

$$\theta_2 = \frac{1}{2}\Big[(\lambda - \mu) - \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\Big],$$

$$m_1 = \frac{1}{2}\Big[(v - 1) - \frac{2k - (v - 1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}\Big],$$

$$m_2 = \frac{1}{2}\Big[(v-1) + \frac{2k-(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\Big].$$

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* λ *and* μ *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] a characterization of bent functions is given 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:*

- $srg(2^n, \frac{2^n+2^{\frac{n}{2}}}{2}, \frac{2^n+2^{\frac{n}{2}}-2^{n-1}}{2}, \frac{2^n+2^{\frac{n}{2}}-2^{n-1}}{2})$;
- $srg(2^n, \frac{2^n-2^{\frac{n}{2}}}{2}, \frac{2^n-2^{\frac{n}{2}}-2^{n-1}}{2}, \frac{2^n-2^{\frac{n}{2}}-2^{n-1}}{2})$.

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 λ and μ, while 4.1 allows us to compute $v = 2^n = |\mathbb{Z}_2^n|$. □

Example 4.8. *The first strongly regular graph defined by bent functions are*

$n = 2$

- $srg(4, 3, 1, 1)$*, i.e. the complete graph* K_4*.*
- $srg(4, 1, 0, 0)$*, i.e. a trivial strongly regular graph made of 2 disconnected edges.*

$n = 4$

- $srg(16, 10, 6, 6)$*.*
- $srg(16, 10, 2, 2)$*.*

$n = 6$

- $srg(64, 36, 20, 20)$*.*
- $srg(64, 28, 12, 12)$*.*

$n = 8$

- $srg(256, 136, 72, 72)$*.*
- $srg(256, 120, 56, 56)$*.*

$n = 10$

- $srg(1024, 528, 272, 272)$*.*
- $srg(1024, 496, 240, 240)$*.*

Note that in each case graphs have the parameters of the complements of the affine polar graphs $VO^{\mp}(2n, 2)$*, 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 $F : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$, $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$, where for each i, $f_i : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$. 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:

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

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

Definition 5.1. *A (n,m)-bent function, or vectorial bent function, is a function $F=(f_1,\ldots,f_m)$ such that $nl(F)=\frac{2^n-2^{\frac{n}{2}}}{2}$, 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 [9] 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;

$$\triangle\mathcal{M}=\left\{a\in\bigcup\mathcal{M}\middle|\sharp\{A\in M|a\in A\}=2k+1,k\in\mathbb{N}\right\}.$$

Proposition 5.4. *Consider a vectorial Boolean function $F=(f_1,\ldots,f_m)$, with $f_i:\mathbb{Z}_2^n\longrightarrow\mathbb{Z}_2$, 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 $Cay(\mathbb{Z}_2^n,\triangle_{i\in I}\Omega_i)$ are strongly regular with $\lambda=\mu$ for all index subset $I\subseteq[1,\ldots,m]$.*

6 Conclusion

Future works should extend this notions to the case n odd, by taking into account APN (almost perfectly non linear) functions, i.e. functions which are as close as possible to perfect nonlinearity.

References

[1] A. Bernasconi, B. Codenotti, *Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem*, IEEE Transactions on Computers, 1999, 48(3), pp. 345-351.

[2] A. Bernasconi, B. Codenotti, J. M. VanderKam, *A Characterization of Bent Functions in terms of Strongly Regular Graphs*, IEEE Transactions on Computers, 2001, 50(9), pp. 984-985.

[3] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, 1991, 4, pp. 3-72.

[4] A. E. Brouwer, H. Van Maldeghem, *Strongly Regular Graphs*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2022.

[5] A. E. Brouwer, *Parameters of Strongly Regular Graphs*, https://www.win.tue.nl/ aeb/graphs/srg/srgtab.html

[6] C. Carlet, C. Ding, J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes*, IEEE Transactions on Information Theory, 2005, 51(6), pp. 2089-2102.

[7] C. Carlet, S. Mesnager, *Four decades of research on bent functions*, Deisgns, Codes amnd Cryptography, 2016, 78, pp. 5-50.

[8] D. Dong, X. Zhang, L. Qu, S. Fu, *A note on vectorial bent functions*, Information Processing Letters, 2013, 113(22-24), pp. 866-870.

[9] P. Givant, P. Halmos, *Introduction to Boolean Algebras*, Springer, 2009.

[10] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton Universtity Press, 2007.

[11] H. Matsui, *Linear cryptanalysis method for DES cypher*, EUROCRYPT93, LNCS 765, Springer, 1994, pp. 386-397.

[12] A. J. Menezes, P. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.

[13] S. Mesnager, *Bent Functions. Fundamentals and Results*, Springer, 2016.

[14] P. H. Zieschang, *Cayley graphs of finite groups*, Journal of Algebra, 1988, 118(2), pp. 447-454.