GRAPH EIGENVALUES AND WALSH SPECTRUM OF BOOLEAN FUNCTIONS

Pantelimon Stănică
Naval Postgraduate School Department of Applied Mathematics Monterey, CA 93943, USA
pstanica@nps.edu

Received: 12/29/05, Revised: 8/7/06, Accepted: 9/10/06

Abstract

In this paper we consider the Cayley graph G_f associated with a Boolean function f and we use it to investigate some of the cryptographic properties of f. We derive necessary (but not sufficient) conditions for a Boolean function to be bent. We also find a complete characterization of the propagation characteristics of f using the topology of its associated Cayley graph G_f. Finally, some inequalities between the cardinality of the spectrum of G_f and the Hamming weight of f are obtained, and some problems are raised.

1. Introduction and Motivation

In this paper we will concentrate on a new technique for dealing with Boolean functions. The technique has already been used successfully to find a characterization of Boolean bent functions in terms of spectrum of the Cayley graph G_f associated with f. Here, we will completely describe the propagation characteristics of the Boolean function f using the spectrum of the associated Cayley graph, we find some necessary conditions for a function to be bent, and show some inequalities (albeit, far from being tight) connecting the Hamming weight of f, the dimension of the vector space where f is defined, and the cardinality of the spectrum of G_f.

Let $\mathbb{V}_n$ be the vector space of dimension n over the two-element field $\mathbb{F}_2$ $(= \mathbb{V}_1)$. Let us denote the addition operator over $\mathbb{F}_2$ by $\oplus$, and the direct product by "$\cdot$". A Boolean function f on n variables is a mapping from $\mathbb{V}_n$ into $\mathbb{V}_1$, that is, a multivariate polynomial over $\mathbb{F}_2$,

$$f(x_1, \ldots, x_n) = a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{1 \le i < j \le n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n, \tag{1}$$

where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f. We make the convention that for all matrices and vectors the indexing starts from 0.

For a Boolean function on $\mathbb{V}_n$, let $\Omega_f = \{\mathbf{x} \in \mathbb{V}_n \,|\, f(\mathbf{x}) = 1\}$. We denote by $\langle \Omega_f \rangle$ the space of the $0,1$ sequences generated by Ω_f, and by $\dim\langle\Omega_f\rangle$ its dimension. The cardinality of Ω_f is $wt(f)$, called the *Hamming weight* of f. The *Hamming distance* between two functions $f, g : \mathbb{V}_n \to \mathbb{V}_1$ is $d(f,g) = wt(f \oplus g)$. A Boolean function $f(\mathbf{x})$ is called an *affine function* if its algebraic degree is 1. If, in addition, $a_0 = 0$ in (1), then $f(\mathbf{x})$ is a *linear function.* The nonlinearity of a function f, denoted by N_f, is defined as

$$\min_{\phi \in A_n} d(f, \phi),$$

where A_n is the class of all affine functions on $\mathbb{V}_n$. We say that f satisfies the *propagation criterion (PC)* with respect to $\mathbf{c}$ if

$$\sum_{\mathbf{x} \in \mathbb{V}_n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}) = 2^{n-1}. \tag{2}$$

If f satisfies the PC with respect to all vectors of weight 1, f is called an *SAC* (*Strict Avalanche Criterion*) function. If the above relation holds for any $\mathbf{c}$ with $wt(\mathbf{c}) \leq s$, we say that f satisfies $PC(s)$, and if $s = n$, then we say that f is a *bent function.* Recall that the Hamming weight of bent functions is $2^{n-1} \pm 2^{n/2-1}$ (n even), and they attain maximum nonlinearity, namely $2^{n-1} - 2^{n/2-1}$ (cf. [14]). The *correlation value* between g and h (both are defined on $\mathbb{V}_n$) is

$$c(g,h) = 1 - \frac{d(g,h)}{2^{n-1}}.$$

We define the *Walsh transform* of a function f on $\mathbb{V}_n$ to be the map $W(f) : \mathbb{V}_n \to \mathbf{R}$, $W(f)(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{V}_n} f(\mathbf{x})(-1)^{\mathbf{w}\cdot\mathbf{x}}$, which defines the coefficients of f with respect to the orthonormal basis of the group characters $Q_{\mathbf{w}}(\mathbf{x}) = (-1)^{\mathbf{w}\cdot\mathbf{x}}$. In turn,

$$f(\mathbf{x}) = 2^{-n} \sum_{\mathbf{w}} W(f)(\mathbf{w})(-1)^{\mathbf{w}\cdot\mathbf{x}}.$$

A graph is *regular of degree* r (or r-regular) if every vertex has degree r (number of edges incident to it). We say that an r-regular graph G with parameters (v, r, d, e) is a *strongly regular graph* (srg) if there exist nonnegative integers e, d such that for all vertices $\mathbf{u}, \mathbf{v}$ the number of vertices adjacent to both $\mathbf{u}, \mathbf{v}$ is e, d, if $\mathbf{u}, \mathbf{v}$ are adjacent, respectively, nonadjacent.

An easy counting argument shows that $r(r-d-1) = e(v-r-1)$. The *complementary* graph $\bar{G}$ of the strongly regular graph G is also strongly regular with parameters $(v, v-r-1, v-2r+e-2, v-2r+d)$.

Let f be a Boolean function on $\mathbb{V}_n$. We define the *Cayley graph* of f to be the graph $G_f = (\mathbb{V}_n, E_f)$ whose vertex set is $\mathbb{V}_n$ and the set of edges is defined by

$$E_f = \{(\mathbf{w}, \mathbf{u}) \in \mathbb{V}_n \mid f(\mathbf{w} \oplus \mathbf{u}) = 1\}.$$

The adjacency matrix A_f is the matrix whose entries are $A_{i,j} = f(\mathbf{b}(i) \oplus \mathbf{b}(j))$, where $\mathbf{b}(\cdot)$ is the binary representation of the argument. It is simple to prove that A_f has the dyadic property: $A_{i,j} = A_{i+2^{k-1},j+2^{k-1}}$. Also, from its definition we derive that G_f is a *regular graph of degree* $wt(f) = |\Omega_f|$ (see [12, Chapter 3] for further definitions).

Given a graph f and its adjacency matrix A, the *spectrum* $Spec(G_f)$ is the set of eigenvalues of A (called also the eigenvalues of G_f). All of our theorems will assume that G_f is connected. One can show easily that all connected components of G_f are isomorphic (we shall point out from time to time what changes in our arguments in case G_f is not connected).

We observe that a strongly regular graph is essentially the same as an association scheme of class 2 (see [11, 18] and the references therein). In spite of their (apparently) strict arithmetic nature, strongly regular graphs are difficult to investigate. P.J. Cameron [7] mentions that "*Strongly regular graphs lie on the cusp between highly structured and unstructured. For example, there is a unique strongly regular graph with parameters* $(36; 10; 4; 2)$*, but there are* 32548 *non-isomorphic graphs with parameters* $(36; 15; 6; 6)$*. (The first assertion is a special case of a theorem of Shrikhande* (our note [*23*])*, while the second is the result of a computer search by McKay and Spence* (our note [*19*])*.) In the light of this, it will be difficult to develop a theory of random strongly regular graphs!*"

The complete determination for the class of bent functions is still an open problem. This type of function is relevant to cryptography, cf. [21] (although balancedness is often required, and bent functions are not balanced, if $n > 20$, the difference $2^{n/2-1}$ between bent functions' weights and the weight 2^{n-1} of balanced functions is negligible and cannot be used in attacks [10]); algebraic coding theory (Kerdock codes are constructed from quadratic bent functions [20]); sequences [22]; design theory (any difference set will render a symmetric design, cf. [2, pp. 274–278]).

As bent Boolean functions are as elusive as the strongly regular graphs, perhaps it is then not surprising that there should be some connections between graph theory and Boolean functions. In fact, they are more related than one might initially guess, as we shall see next. The attempt in the present paper (and in a few other works, see [3, 4, 5]) is to push further the connection between two very intriguing topics, bent functions and strongly regular graphs, with the hope that the investigation will shed more light into the constructions of both. We would like to invite researchers in these two areas to collaborate for the benefit of all parties.

2. Known Results

Here and throughout we assume that $n \geq 4$. The following theorem is a compilation of various results in [3] (we slightly changed the notation).

Theorem 2.1. *The following statements hold:*

(i) *Let $f : \mathbb{V}_n \to \mathbb{F}_2$, and let $\lambda_i, 0 \leq i \leq 2^n - 1$ be the eigenvalues of its associated Cayley graph G_f. Then $\lambda_i = W(f)(\mathbf{b}(i))$, for any i.*

(ii) *The multiplicity of the largest spectral coefficient of f, $W(f)(\mathbf{b}(0))$, is equal to $2^{n-dim\langle\Omega_f\rangle}$.*

(iii) *If G_f is connected, then f has a spectral coefficient equal to $-wt(f)$ if and only if its Walsh spectrum is symmetric with respect to zero.*

(iv) *The number of nonzero spectral coefficients is equal to $rk(A_f)$, the rank of A_f, which satisfies $2^{d_2} \leq rk(A_f) \leq \sum_{i=1}^{d} \binom{n}{i}$ (d_2, respectively, d is the degree of f over $\mathbb{F}_2$, respectively $\mathbf{R}$).*

It is known (see [12, pp. 194–195]) that a connected r-regular graph is strongly regular iff it has exactly three distinct eigenvalues $\lambda_0 = r, \lambda_1, \lambda_2$ (so $e = r+\lambda_1\lambda_2+\lambda_1+\lambda_2$, $d = r+\lambda_1\lambda_2$). The following result is known [12, Th. 3.32, p. 103].

Proposition 2.2. *The following identity holds for a strongly r-regular graph:*

$$A^2 = (d - e)A + (r - e)I + eJ,$$

where J is the "all ones" matrix.

3. Odd Cycles and Bent Functions

One can infer the following result from [3], [4], and Proposition 2.2.

Theorem 3.1. *Bent functions (on $\mathbb{V}_n$, with n even) are the only functions whose associated Cayley graphs are strongly regular graphs with the additional property $e = d$. The eigenvalues of G are $\lambda_1 = |\Omega_f| = wt(f)$, $\lambda_3 = -\lambda_2 = -\sqrt{|\Omega_f| - e}$, of multiplicities $m_1 = 1$, $m_2 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)-|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$, $m_3 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)+|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$. Moreover, the adjacency matrix satisfies*

$$A^2 = \left(2^{n-1} \pm 2^{n/2-1} - e\right) I + eJ,$$

for some choice of the $\pm$ sign.

It is assumed above that G_f is connected. If it is not connected, then the multiplicities must be multiplied by $2^{n-\dim\langle\Omega_f\rangle}$ (since the connected components of G are isomorphic).

A graph $G = (V(G), E(G))$ is *bipartite* if the vertex set $V(G)$ can be partitioned into two sets V_1, V_2 in such a way that no two vertices from the same set are adjacent. The following result is well-known (see [1]).

Theorem 3.2. *The following statements are equivalent for a graph G:*

(i) G is bipartite.

(ii) G has no cycles of odd length.

(iii) Every subgraph H of G has at least $|V(H)|/2$ mutually non-adjacent vertices.

(iv) The spectrum of G is symmetric with respect to 0, that is, if λ is an eigenvalue, then $-\lambda$ is also an eigenvalue.

We can now prove

Theorem 3.3. *The Cayley graph associated with a bent function is not bipartite.*

Proof. Theorem 3.2 implies that the graph G_f associated with a Boolean function f is bipartite if and only if its spectrum is symmetric with respect to the origin. But according to Theorem 3.1, that is impossible since $-\lambda_1 = -wt(f)$ is not an eigenvalue of G. The theorem is proved. $\square$

As stated in Theorem 3.2, a graph is bipartite if and only if it contains no cycles of odd length. Thus, if f is bent then the associated Cayley graph contains a cycle of odd length. One can get more precise results.

Theorem 3.4. *Let $n > 4$. If G_f is triangle-free, then f is not bent.*

Proof. For a contradiction, assume that f is bent. Erdös and Sós proved in 1974 (cf. [1]), that a triangle-free graph G on p vertices with minimum degree $\delta(G) > 2p/5$ is bipartite. Recall that G_f is a regular graph of degree $|\Omega_f|$ of order $p = 2^n$. Since $n > 4$, then $2^{n/2} > 5$ is equivalent to $5(2^{n-1} - 2^{n/2-1}) > 2^{n+1}$, which implies $|\Omega_f| = wt(f) > 2^{n+1}/5$. Thus, G is bipartite. That is certainly false by Theorem 3.3, contradicting our assumption that f is bent. $\square$

In the previous proof it is sufficient to assume that G_f is regular of degree greater than $2^{n+1}/5$ (if the degree is $< 2^{n+1}/5$, then the function is certainly not bent).

A more constructive argument that proves Theorem 3.4 is the following. Assume that f is bent. One may replace f by its complement, also bent (cf. [14]), so we assume that the constant term, a_0, in Equation (1), equals 0. Next, we prove that there exist triangles in G_f. By Theorem 3.1, G_f is strongly regular. Lemma 8 of [3] shows that $e = |(\mathbf{x} \oplus \Omega_f) \cap (\mathbf{y} \oplus \Omega_f)| \geq 1$. Applying this for $\mathbf{x} = \mathbf{0}$ and an arbitrary vector $\mathbf{y} \in \Omega_f$, implies that $e = |\Omega_f \cap (\mathbf{y} \oplus \Omega_f)| \geq 1$. That is, there exists $\mathbf{z} \in \Omega_f$ such that $\mathbf{y} \oplus \mathbf{z} \in \Omega_f$. Thus, $f(\mathbf{y} \oplus \mathbf{z}) = f(\mathbf{z}) = f(\mathbf{y}) = 1$. It follows that $\mathbf{0}, \mathbf{y}, \mathbf{z}$ is a triangle in G_f.

The converse of Theorem 3.4 is not true, as it can be seen by considering on $\mathbb{V}_6$ the function $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_1 \oplus x_6x_1x_2$ and the associated Cayley graph which has plenty of triangles, but f is not bent.

The number of triangles sitting on any two (fixed) adjacent vertices is equal to e. We know that $e = |(\Omega_f \oplus \mathbf{v}_i) \cap (\Omega_f \oplus \mathbf{v}_j)|$ (Lemma 8 of [3]) for any pair of vertices $\mathbf{v}_i \neq \mathbf{v}_j$. We note that $e \neq |\Omega_f|$, since the equality prompts two eigenvalues to become 0. That is not possible since in that case (see [12]) the graph G_f cannot be strongly connected. Thus $e < |\Omega_f|$. There are other restrictions on e. A simple corollary of Theorem 3.1 is that e must differ from $|\Omega_f|$ by a perfect square.

4. Coloring the Boolean Cayley Graph

Assume that the eigenvalues of G_f are ordered as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_v$.

Theorem 4.1. *Let f be a Boolean function, and let G_f be the associated Cayley graph with g being the multiplicity of its lowest eigenvalue $\lambda_v(G_f)$. Then,* $\min\left\{g+1, 1-\frac{\lambda_v(G_f)}{\lambda_2(G_f)}\right\} \leq \chi(G_f) \leq |\Omega_f|$ *(provided $\lambda_2(G_f) \neq 0$).*

Proof. The first inequality $\min\left\{g+1, 1-\frac{\lambda_v(G)}{\lambda_2(G)}\right\} \leq \chi(G)$ can be found in [16], being true for arbitrary graphs G. Cao proved in [8] that the chromatic number satisfies $\chi(G) \leq \sqrt{T(G)}+1$, for any graph G, where $T(G)$ is the maximum sum of degrees of vertices adjacent to any vertex v (that is, the maximum number of 2-walks in G). When $G = G_f$, since G_f is Ω_f-regular, then $T(G_f) = |\Omega_f|^2$, so we get $\chi(G_f) \leq |\Omega_f| + 1$. By Wilf's theorem [26], the equality $\chi(G_f) = |\Omega_f| + 1$ holds if and only if G_f is a complete graph or an odd cycle. Since G_f is neither, we obtain $\chi(G_f) \leq |\Omega_f|$. □

Corollary 4.2. *With the notations of the previous theorem, assuming that G_f is a strongly regular (connected) graph, with $e = d$, then* $\max\left\{2, 1+\frac{|\Omega_f|}{\sqrt{|\Omega_f|-e}}\right\} \leq \chi(G_f) \leq |\Omega_f|$.

Proof. The corollary follows easily observing that under the imposed conditions $v = 3$, $\lambda_3 = -\lambda_2$. Using Theorem 4.1 (with $g \geq 1$), Hoffman's famous bound on the chromatic number $\chi(G_f) \geq 1 - \frac{\lambda_1(G_f)}{\lambda_v(G_f)}$ (cf. [17]), and Theorem 3.1, we get the result. □

One cannot get better bounds by using the fact that G_f (for f a bent function) is always a Ramanujan graph. Recall that a graph is Ramanujan if it is r-regular and all eigenvalues $\neq r$ are $\leq 2\sqrt{r-1}$. That certainly is the case here since $r = |\Omega_f|$ and the eigenvalues in absolute value are $\sqrt{|\Omega_f| - e} \leq 2\sqrt{|\Omega_f| - 1}$. If G_f is connected, non-bipartite, and r-regular, then $\chi(G_f) \geq \frac{r}{2\sqrt{r-1}} \sim \frac{\sqrt{r}}{2}$ (see [13]). However, this bound is not better than the one obtained by Corollary 4.2.

5. Avalanche Features of the Cayley graphs

In [24, 25] it was proved that a Boolean function f depends on the variable x_i linearly if and only if the Walsh transform of $\hat{f}(\mathbf{u}) = (-1)^{f(\mathbf{u})}$ is 0, that is, $W(\hat{f})(\mathbf{u}) = 0$ for all $\mathbf{u}$ with the ith component $u_i = 0$. Using the known relationship between the Walsh transform of f and $\hat{f}$,

$$W(\hat{f})(\mathbf{u}) = -2W(f)(\mathbf{u}) + 2^n\delta(\mathbf{u}), \text{ on } \mathbb{V}_n \tag{3}$$

where $\delta(\mathbf{u}) = 1$ if $\mathbf{u} = \mathbf{0}$ and 0 otherwise, it is rather easy to deduce the following result.

Proposition 5.1. *A Boolean function f depends on a variable x_i linearly if and only if the eigenvalues for the Cayley graph G_f satisfy $\lambda_0 = 2^{n-1}$, and $\lambda_{j\neq 0} = 0$ whenever $\mathbf{b}(j)$ has its i-th component equal to 0.*

We call a function f on $\mathbb{V}_n$ *ℓ-order correlation-immune* ($\ell - CI$) if its Walsh transform satisfies $W(\hat{f})(\mathbf{v}) = 0$ for all $1 \leq wt(\mathbf{v}) \leq \ell$. If, in addition, $W(\hat{f})(\mathbf{0}) = 0$, then f is called *ℓ-resilient*. We derive the following characterization of these properties in terms of graph spectra.

Proposition 5.2. *A function f on $\mathbb{V}_n$ is $\ell - CI$ if and only if the eigenvalues of the associated Cayley graph G_f satisfy $\lambda_i = 0$ for all i with $1 \leq wt(\mathbf{b}(i)) \leq \ell$. Further, f is ℓ-resilient if and only if $\lambda_i = 0$ for all $1 \leq wt(\mathbf{b}(i)) \leq \ell$ and $\lambda_0 = 2^{n-1}$.*

Proof. We know that $\lambda_i = W(f)(\mathbf{b}(i))$, for any $0 \leq i \leq 2^n - 1$. Using the definition of the $\ell - CI$ functions and Equation (3) we derive the result. □

Corollary 5.3. *For an unbalanced ℓ-CI function f, there are $\sum_{s=1}^{\ell} \binom{n}{s}$ zero eigenvalues of G_f.*

One can compute the Walsh spectrum by using $f = H_n W(f)$ and $W(f) = 2^{-n} H_n f$. Recall that the Sylvester-Hadamard matrix H_n is defined as $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$, that is, H_n is the Kronecker product $H_n = H_1 \otimes H_{n-1}$. We show the following result (this was also proved by McFarland, cf. [14]).

Theorem 5.4. *If $H = H_n$ is the Sylvester-Hadamard matrix with entries $(-1)^{\mathbf{v}_i\cdot\mathbf{v}_j}$, where $\mathbf{v}_i, \mathbf{v}_j$ are the vectors of $\mathbb{V}_n$, then*

$$HA_fH^t = 2^nD,$$

where D is the diagonal matrix formed by the eigenvalues of A_f.

Proof. Since $HH^t = 2^nI_{2^n}$, it suffices to show that

$$HA_f = DH. \tag{4}$$

Now, for $H = (h_{i,j})$ and $A_f = (a_{i,j})$, the left-hand side is

$$\begin{aligned}(HA_f)_{i,j} &= \sum_{l=1}^{2^n} h_{i,l}a_{l,j} = \sum_{l=1}^{2^n}(-1)^{\mathbf{v}_i\cdot\mathbf{v}_l}f(\mathbf{v}_l\oplus\mathbf{v}_j)\\ &= \sum_{l=1}^{2^n}(-1)^{\mathbf{v}_i\cdot(\mathbf{v}_l\oplus\mathbf{v}_j)+\mathbf{v}_i\cdot\mathbf{v}_j}f(\mathbf{v}_l\oplus\mathbf{v}_j)\\ &= (-1)^{\mathbf{v}_i\cdot\mathbf{v}_j}\sum_{\mathbf{x}\in\mathbb{V}_n}(-1)^{\mathbf{v}_i\cdot\mathbf{x}}f(\mathbf{x})\\ &= (-1)^{\mathbf{v}_i\cdot\mathbf{v}_j}W(f)(\mathbf{v}_i) = (-1)^{\mathbf{v}_i\cdot\mathbf{v}_j}\,\lambda_i.\end{aligned}$$

□

Let f be a Boolean function on $\mathbb{V}_n$ and assume that $f(\mathbf{0}) = 0$. Moreover, assume that G_f is connected. Bernasconi and Codenotti [5] proved

Theorem 5.5. *The graph G_f is bipartite if and only if $\mathbb{V}_n \setminus \Omega_f$ contains a subspace of dimension $n-1$.*

Now let S_0 be a subspace of dimension $n-1$ with basis $\{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n-1)}\}$. Complete the previous basis with $\alpha^{(n)}$ to get a basis for $\mathbb{V}_n$. Let $\mathbf{b}$ be the unique solution in $\mathbb{V}_n$ of the system:

$$\begin{pmatrix}\alpha_1^{(1)} & \alpha_2^{(1)} & \ldots & \alpha_n^{(1)}\\ \alpha_1^{(2)} & \alpha_2^{(2)} & \ldots & \alpha_n^{(2)}\\ \vdots & \vdots & \ldots & \vdots\\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)}\end{pmatrix}\begin{pmatrix}b_1\\ b_2\\ \vdots\\ b_n\end{pmatrix} = \begin{pmatrix}0\\ 0\\ \vdots\\ 1\end{pmatrix} \tag{5}$$

Let $\mathbf{w} \in \mathbb{V}_n$. Since f is 0 on S_0, we have

$$W(f)(\mathbf{w}\oplus\mathbf{b}) = \sum_{\mathbf{x}\in\mathbb{V}_n}(-1)^{\mathbf{x}\cdot(\mathbf{w}\oplus\mathbf{b})}f(\mathbf{x}) = \sum_{\mathbf{x}\in\mathbb{V}_n\setminus S_0}(-1)^{\mathbf{x}\cdot\mathbf{w}}(-1)^{\mathbf{x}\cdot\mathbf{b}}f(\mathbf{x}).$$

Furthermore, since $\mathbf{b}$ is the solution to (5) and $\mathbf{x} \notin S_0$ is a linear combination of the vectors $\alpha^{(1)}, \ldots, \alpha^{(n)}$ (with $\alpha^{(n)}$ always present), we get $(-1)^{\mathbf{x}\cdot\mathbf{b}} = -1$, and the following result is proven [5].

Theorem 5.6. *If* $\mathbf{b}$ *is given by* (5), *then* $W(f)(\mathbf{w}) = -W(f)(\mathbf{w} \oplus \mathbf{b})$, *for any* $\mathbf{w} \in \mathbb{V}_n$.

Further, Bernasconi and Codenotti proved the following theorem [5] that describes the propagation features of f for all vectors with a specific property.

Theorem 5.7. *Let* $f : \mathbb{V}_n \to \mathbb{F}_2$ *be a Boolean function whose associated graph is bipartite, and let* $\mathbf{b} \in \mathbb{V}_n$ *given by (5). If* $|\Omega_f| = 2^{n-2}$, *then* f *satisfies the PC with respect to all strings* $\mathbf{w}$ *such that* $\mathbf{w} \cdot \mathbf{b}$ *is an odd integer. If* $|\mathbf{b}| = n$, *then* f *satisfies the SAC.*

The previous theorem seems to be quite restrictive. We prove a new result next that connects the *PC* property with the symmetric difference in counting vertices of G_f.

Denote by $\mathcal{N}(\mathbf{x})$ the set of vertices adjacent to a vertex $\mathbf{x}$ in the graph G_f. For easy writing, we write $\lambda_i = \lambda_{\mathbf{b}(i)}$. The next result is our main theorem of this section.

Theorem 5.8. *Let* $f : \mathbb{V}_n \to \mathbb{F}_2$ *be a Boolean function. Then the following statements are equivalent:*

1. f *satisfies the PC with respect to* $\mathbf{w}$*;*
2. $|\mathcal{N}(\mathbf{0}) \setminus \mathcal{N}(\mathbf{w})| + |\mathcal{N}(\mathbf{w}) \setminus \mathcal{N}(\mathbf{0})| = 2^{n-1}$*;*
3. $\sum_{\mathbf{u}\in\mathbb{V}_n} (-1)^{\mathbf{u}\cdot\mathbf{w}} \lambda_{\mathbf{u}}^2 = 2^n \lambda_{\mathbf{0}} - 2^{2n-2} = 2^n wt(f) - 2^{2n-2}$.

Proof. It is easy to see that f satisfies the PC with respect to $\mathbf{w}$ if and only if the autocorrelation function

$$\begin{aligned}
\hat{r}_f(\mathbf{w}) &= \sum_{v} (-1)^{f(\mathbf{v})+f(\mathbf{v}\oplus\mathbf{w})} \\
&= \sum_{\mathbf{v}\in\Omega_f} (-1)^{f(\mathbf{v})+f(\mathbf{v}\oplus\mathbf{w})} + \sum_{\mathbf{v}\notin\Omega_f} (-1)^{f(\mathbf{v})+f(\mathbf{v}\oplus\mathbf{w})} \\
&= \sum_{\mathbf{v}\in\Omega_f} (-1)^{1+f(\mathbf{v}\oplus\mathbf{w})} + \sum_{\mathbf{v}\notin\Omega_f} (-1)^{f(\mathbf{v}\oplus\mathbf{w})} \\
&= \sum_{\mathbf{v}\in\Omega_f\cap\mathcal{N}(\mathbf{w})} 1 + \sum_{\mathbf{v}\in\Omega_f\cap\overline{\mathcal{N}(\mathbf{w})}} (-1) \\
&\quad + \sum_{\mathbf{v}\in\overline{\Omega_f}\cap\mathcal{N}(\mathbf{w})} (-1) + \sum_{\mathbf{v}\in\overline{\Omega_f}\cap\overline{\mathcal{N}(\mathbf{w})}} 1 = 0.
\end{aligned}$$

Thus, $|(\mathcal{N}(\mathbf{0}) \cap \mathcal{N}(\mathbf{w})) \cup (\overline{\mathcal{N}(\mathbf{0})} \cap \overline{\mathcal{N}(\mathbf{w})})| = |(\mathcal{N}(\mathbf{0}) \cap \overline{\mathcal{N}(\mathbf{w})}) \cup (\overline{\mathcal{N}(\mathbf{0})} \cap \mathcal{N}(\mathbf{w}))|$. Further, using the inclusion-exclusion principle, the previous identity is equivalent to

$$\begin{aligned}
&|\mathcal{N}(\mathbf{0})\cap\mathcal{N}(\mathbf{w})|+|\overline{\mathcal{N}(\mathbf{0})\cup\mathcal{N}(\mathbf{w})}|=|\mathcal{N}(\mathbf{0})\cap\overline{\mathcal{N}(\mathbf{w})}|+|\overline{\mathcal{N}(\mathbf{0})\cup\overline{\mathcal{N}(\mathbf{w})}}| &&\iff\\
&|\mathcal{N}(\mathbf{0})\cap\mathcal{N}(\mathbf{w})|+2^n-|\mathcal{N}(\mathbf{0})\cup\mathcal{N}(\mathbf{w})|=|\mathcal{N}(\mathbf{0})\cap\overline{\mathcal{N}(\mathbf{w})}|+2^n\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad-|\mathcal{N}(\mathbf{0})\cup\overline{\mathcal{N}(\mathbf{w})}| &&\iff\\
&|\mathcal{N}(\mathbf{0})\cup\mathcal{N}(\mathbf{w})|-|\mathcal{N}(\mathbf{0})\cap\mathcal{N}(\mathbf{w})|=|\mathcal{N}(\mathbf{0})\cup\overline{\mathcal{N}(\mathbf{w})}|-|\mathcal{N}(\mathbf{0})\cap\overline{\mathcal{N}(\mathbf{w})}| &&\iff\\
&|\mathcal{N}(\mathbf{0})\setminus\mathcal{N}(\mathbf{w})|+|\mathcal{N}(\mathbf{w})\setminus\mathcal{N}(\mathbf{0})|=2^n-|\mathcal{N}(\mathbf{0})\setminus\mathcal{N}(\mathbf{w})|-|\mathcal{N}(\mathbf{w})\setminus\mathcal{N}(\mathbf{0})|,
\end{aligned}$$

which proves the first claim. Now, using the Wiener-Khintchine's Theorem (see [9]) $W(\hat{r})(w)=W(\hat{f})^2(w)$, the equation (3), and the autocorrelation definition, one can deduce (see also [15]) that f satisfies the PC with respect to $\mathbf{w}$ if and only if

$$\begin{aligned}
&\sum_{\mathbf{u}\in\mathbb{V}_n}(-1)^{\mathbf{u}\cdot\mathbf{w}}W(\hat{f})^2(\mathbf{u})=0 \iff\\
&\sum_{\mathbf{u}\in\mathbb{V}_n}(-1)^{\mathbf{u}\cdot\mathbf{w}}W(f)^2(\mathbf{u})=2^nW(f)(0,0,\ldots,0)-2^{2n-2}.
\end{aligned}$$

Since $W(f)(0,0,\ldots,0)$ is equal to the number of ones in the truth table of f, that is, the weight of f, which is the eigenvalue corresponding to $(0,0,\ldots,0)$, we get the last claim. □

6. Sensitivity of Hamming Weight of f to $Spec(G_f)$

We know that a strongly regular Cayley graph G_f with the extra condition $e=d$ corresponds to a Boolean bent function f. Is there any influence of arbitrary Cayley graph spectra on the weight (or nonlinearity) of f? We can only prove the following theorem and its corollary in this direction.

Theorem 6.1. *Let f be a Boolean function defined on $\mathbb{V}_n$. If G_f is connected and its spectrum $Spec(G_f)$ contains exactly $m+1$ distinct eigenvalues ($m\le n/2$), then*

$$n\le\log_2\left(r+\binom{r}{m}\right),$$

where $r=wt(f)$.

Proof. We know that if $|Spec(G_f)|=m+1$, then the diameter of G_f is $\le m$ (cf. [12, Th. 3.13, p. 88]). Thus, for any $\mathbf{w}\in\mathbb{V}_n\setminus\Omega_f$, there is a constant number of strings $\mathbf{w}^{(i)}\in\Omega_f$ such that $\mathbf{w}=\sum_i\mathbf{w}^{(i)}$. The number of such strings is less than or equal to m, say p. It follows that writing $\mathbf{w}=\sum_{j=1}^r c_j\mathbf{w}^{(j)}$, $c_j\in\mathbb{F}_2$, exactly p coefficients are nonzero. Thus, the number of elements of $\mathbb{V}_n\setminus\Omega_f$ is less than or equal to the number of ways of choosing p nonzero coefficients out of r. Thus, $2^n-r\le\binom{r}{p}\le\binom{r}{m}$ (since $m\le n/2$). The result follows easily. □

Corollary 6.2. *If the Cayley graph associated with a Boolean function f is connected and strongly regular, then* $wt(f) \geq \dfrac{-1+\sqrt{2^{n+3}+1}}{2}$.

Proof. If G_f is connected and strongly regular, then the number of distinct eigenvalues is $m = 3$. Therefore, the diameter of G_f, $diam(G_f)$, is ≤ 2. If $diam(G_f) = 1$, then G_f is complete, but then we would have only two distinct eigenvalues. So $diam(G_f) = 2$. Therefore, any $\mathbf{w} \in \mathbb{V}_n \setminus \Omega_f$ can be written as a sum of two elements in Ω_f. Writing, as before, $\mathbf{w} = \sum_{j=1}^{r} \mathbf{w}^{(j)}$, it follows that exactly two coefficients are nonzero. Therefore,

$$2^n - r \leq \binom{r}{2} \Longleftrightarrow r(r+1) \geq 2^{n+1} \Longleftrightarrow r \geq \frac{-1+\sqrt{2^{n+3}+1}}{2},$$

thus proving the corollary. □

The author challenges the reader to find further indicators of a Boolean function that are more sensitive to $Spec(G_f)$.

Acknowledgements. The author would like to thank the referee for the careful reading of the paper and the very constructive and helpful comments that significantly improved the presentation and quality of this paper. The author was partially supported by the Naval Postgraduate School RIP funding.

References

[1] A.S. Asratian, T.M.J. Denley, R. Häggkvist. Bipartite Graphs and their Applications, Cambridge Univ. Press, 1998.

[2] E.F. Assmus and J.D. Key. Designs and their Codes, Cambridge Univ. Press, 1992.

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

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

[5] A. Bernasconi, B. Codenotti. *On Boolean Functions Associated to Bipartite Cayley Graphs*, Workshop on Boolean Problems (2000), Freiberg - Germany, 167–174.

[6] N. Biggs. Algebraic Graph Theory (2nd ed.), Cambridge Univ. Press, 1993.

[7] P. Cameron. *Random strongly regular graphs?*, Electronic Notes in Discrete Math. **10** (2001) (ed. Jaroslav Nesetril, Marc Noy and Oriol Serra), Elsevier, Amsterdam.

[8] D. Cao. *Bounds On Eigenvalues And Chromatic Numbers*, Linear Algebra and Its Applications **270** (1998), 1–13.

[9] C. Carlet. *Partially-bent functions*, Designs Codes and Cryptography, 3, pp. 135-145 (1993) and proceedings of CRYPTO 92, Advances in Cryptology, LNCS **740** (1993), Springer Verlag, 280–291.

[10] C. Carlet, A. Klapper. *Upper bounds on the number of bent and resilient functions*, to appear in a Special Issue Dedicated to Philippe Delsarte, Spring-Verlag, LNCS.

[11] C.J. Colbourn, J. Dinitz (editors), CRC Handbook of Combinatorial Design, CRC Press, Boca Raton, 1996.

[12] D.M. Cvetkovic, M. Doob, H. Sachs. Spectra of Graphs, Academic Press, 1979.

[13] G. Davidoff, P. Sarnak, A. Valette. Elementary Number Theory, Group Theory and Ramanujan Graphs, Cambridge Univ. Press, 2003.

[14] J.F. Dillon. *A survey of bent functions.* The NSA Technical Journal (unclassified) (1972), 191–215.

[15] R. Forré. *The Strict Avalanche Criterion: Spectral properties of Boolean functions and an extended definition*, Adv. in Cryptology, Crypto'88, LNCS **403** (1989), 450-459.

[16] W.H. Haemers. *Eigenvalue techniques in design and graph theory,* Ph.D. Thesis at Eindhoven Univ. of Technology, 1979 (also found in Math. Centre Tract 121, Mathematical Centre, Amsterdam, 1980).

[17] A. J. Hoffman. *On eigenvalues and colorings of graphs.* Graph Theory and its Applications (B. Harris, ed.) (1970), Academic Press, 78–91.

[18] L.K. Jørgensen, M. Klin. *Switching of edges in strongly regular graphs. I. A family of partial difference sets on* 100 *vertices*, Electronic J. Combin. **10** (2003), # R17.

[19] B.D. McKay, E. Spence, *Classification of regular two-graphs on* 36 *and* 38 *vertices*, Australas. J. Combin. **24** (2001), 293–300.

[20] F. J. Mac Williams, N. J. Sloane. The theory of error-correcting codes, Amsterdam, North Holland, 1977.

[21] W. Meier, O. Staffelbach. *Nonlinearity Criteria for Cryptographic Functions*, Advances in Cryptology, EUROCRYPT 89, LNCS **434** (1990), 549–562.

[22] J. D. Olsen, R. A. Scholtz and L. R. Welch, *Bent function sequences*, IEEE Trans. on Inf. Theory **28** (1982), 858–864.

[23] S.S. Shrikhande, *The uniqueness of the* L_2 *association scheme*, Ann. Math. Statistics **30** (1959), 781-798.

[24] Y. Tarannikov. *Spectral analysis of high order correlation immune functions*, 2000.

[25] Y. Tarannikov, P. Korolev, A. Botev. *Autocorrelation coefficients and correlation immunity of Boolean functions*, Advances in cryptology, ASIACRYPT 2001, LNCS **2248** (2001), 460–479.

[26] H.S. Wilf. *The eigenvalues of a graph and its chromatic number*, J. London Math. Soc. **42** (1967), 330–332.