



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2017-11

Generalized bent Boolean functions and strongly regular Cayley graphs

Riera, Constanza; Stnic, Pantelimon; Gangopadhyay, Sugata

ArXiv

Riera, Constanza, Pantelimon Stnic, and Sugata Gangopadhyay. "Generalized bent Boolean functions and strongly regular Cayley graphs." Discrete Applied Mathematics (2020).

<https://hdl.handle.net/10945/65304>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

Generalized bent Boolean functions and strongly regular Cayley graphs

Constanza Riera¹, Pantelimon Stănică², Sugata Gangopadhyay³,

¹Department of Computing, Mathematics, and Physics,
Western Norway University of Applied Sciences,
5020 Bergen, Norway; csr@hvl.no

²Department of Applied Mathematics,
Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

³Department of Computer Science and Engineering
Indian Institute of Technology Roorkee,
Roorkee 247667, INDIA; gsugata@gmail.com

November 21, 2017

Abstract

In this paper we define the (edge-weighted) Cayley graph associated to a generalized Boolean function, introduce a notion of strong regularity and give several of its properties. We show some connections between this concept and generalized bent functions (gbent), that is, functions with flat Walsh-Hadamard spectrum. In particular, we find a complete characterization of quartic gbent functions in terms of the strong regularity of their associated Cayley graph.

1 (Generalized) Boolean functions background

Let \mathbb{V}_n be the vector space of dimension n over the two element field \mathbb{F}_2 , and for a positive integer q , let \mathbb{Z}_q be the ring of integers modulo q . Let us denote the addition, respectively, product operators over \mathbb{F}_2 by “ \oplus ”, respectively, “ \cdot ”. A Boolean function f on n variables is a mapping from \mathbb{V}_n into \mathbb{F}_2 , that is, a multivariate polynomial over \mathbb{F}_2 ,

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

where the coefficients $a_0, a_i, a_{ij}, \dots, a_{12\dots n} \in \mathbb{F}_2$. 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 .

For a Boolean function on \mathbb{V}_n , the *Hamming weight* of f , $wt(f)$, is the cardinality of $\Omega_f = \{\mathbf{x} \in \mathbb{V}_n : f(\mathbf{x}) = 1\}$ (this is extended to any vector, by taking its weight to

be the number of nonzero components of that vector). The *Hamming distance* between two functions $f, g : \mathbb{V}_n \rightarrow \mathbb{F}_2$ 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* (see [8] for more on Boolean functions). In $\mathbb{V}_n = \mathbb{F}_2^n$, the vector space of the n -tuples over \mathbb{F}_2 , we use the conventional dot product $\mathbf{u} \cdot \mathbf{x}$ as an inner product.

For a *generalized Boolean function* $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$ we define the *generalized Walsh-Hadamard transform* to be the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_q^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}},$$

where $\zeta_q = e^{\frac{2\pi i}{q}}$ (we often use ζ, \mathcal{H}_f , instead of ζ_q , respectively, $\mathcal{H}_f^{(q)}$, when q is fixed). The inverse is given by $\zeta^{f(\mathbf{x})} = 2^{-n} \sum_{\mathbf{u}} \mathcal{H}_f(\mathbf{u}) (-1)^{\mathbf{u} \cdot \mathbf{x}}$. For $q = 2$, we obtain the usual *Walsh-Hadamard transform*

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}},$$

which defines the coefficients of character form of f with respect to the orthonormal basis of the group characters $\chi_{\mathbf{w}}(\mathbf{x}) = (-1)^{\mathbf{w} \cdot \mathbf{x}}$. In turn, $f(\mathbf{x}) = 2^{-n} \sum_{\mathbf{w}} \mathcal{W}_f(\mathbf{w}) (-1)^{\mathbf{u} \cdot \mathbf{x}}$.

We use the notation as in [10, 11, 12, 15, 16] (see also [14, 17]) and denote the set of all generalized Boolean functions by \mathcal{GB}_n^q and when $q = 2$, by \mathcal{B}_n . A function $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$. We recall that a function f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is called a *bent function*, which only exist for even n since $\mathcal{W}_f(\mathbf{u})$ is an integer. Let $f \in \mathcal{GB}_n^q$, where $2^{k-1} < q \leq 2^k$, then we can represent f uniquely as

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x})$$

for some Boolean functions a_i , $0 \leq i \leq k-1$ (this representation comes from the binary representation of the elements in the image set \mathbb{Z}_{2^k}). For results on classical bent functions and related topics, the reader can consult [5, 8, 13, 18].

2 Unweighted strongly regular graphs

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 is a *strongly regular graph* (srg) with parameters (v, r, e, d) 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 d, e , if \mathbf{u}, \mathbf{v} are adjacent, respectively, nonadjacent (see for instance [9]). The *complementary* graph \bar{G} of the strongly regular graph G is also strongly regular with parameters $(v, v-r-1, v-2r+e-2, v-2r+d)$ (see [9]).

Since the objects of this paper are edge-weighted graphs $G = (V, E, w)$ (with vertices V , edges E and weight function w defined on E with values in some set, which in our case it will be either the set of integers modulo q , \mathbb{Z}_q with $q = 2^k$, or the complex

numbers set \mathbb{C}), we define the *weighted degree* $d(v)$ of a vertex v to be the sum of the weights of its incident edges, that is, $d(v) = \sum_{u, (u,v) \in E} w(u, v)$ (later, we will introduce yet another degree or strength concept). Certainly, one can also define the *combinatorial degree* $r(v)$ of a vertex to be the number of such incident edges. For more on graph theory the reader can consult [4, 9] or one's favorite graph theory book.

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

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

For some fixed (but understood from the context) positive integer s , let the canonical injection $\iota : \mathbb{V}_s \rightarrow \mathbb{Z}_{2^s}$ be defined by $\iota(\mathbf{c}) = \mathbf{c} \cdot (1, 2, \dots, 2^{s-1}) = \sum_{j=0}^{s-1} c_j 2^j$, where $\mathbf{c} = (c_0, c_1, \dots, c_{s-1})$. For easy writing, we denote by $\mathbf{j} := \iota^{-1}(j)$.

The adjacency matrix A_f is the matrix whose entries are $A_{i,j} = f(\mathbf{i} \oplus \mathbf{j})$ (here ι is defined on \mathbb{V}_n). 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 [9, Chapter 3] for further definitions).

Given a graph f and its adjacency matrix A , the *spectrum*, with notation $Spec(G_f)$, is the set of eigenvalues of A (called also the eigenvalues of G_f). We assume throughout that G_f is connected (in fact, one can show that all connected components of G_f are isomorphic).

It is known (see [9, 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 [9, Th. 3.32, p. 103] (the second part follows from a counting argument and is also well known).

Proposition 1. *The following identity holds for a strongly r -regular graph:*

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

where J is the all 1 matrix. Moreover, $r(r - d - 1) = e(v - r - 1)$.

In [1, 2] it was shown that a Boolean function f is bent if and only if the Cayley graph G_f is strongly regular with $e = d$. We shall refer to this as the Bernasconi-Codenotti correspondence.

3 The Cayley graph of a generalized Boolean function

We now let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$ be a generalized Boolean function. We define the (*generalized*) *Cayley graph* G_f to be the graph where vertices are the elements of \mathbb{V}_n and two vertices \mathbf{u}, \mathbf{v} are connected by a weighted edge of (multiplicative) weight $\zeta^{f(\mathbf{u} \oplus \mathbf{v})}$ (respectively, additive weight $f(\mathbf{u} \oplus \mathbf{v})$). Certainly, the underlying unweighted graph is a complete pseudograph (every vertex also has a loop). We sketch in Figure 1 such an example.

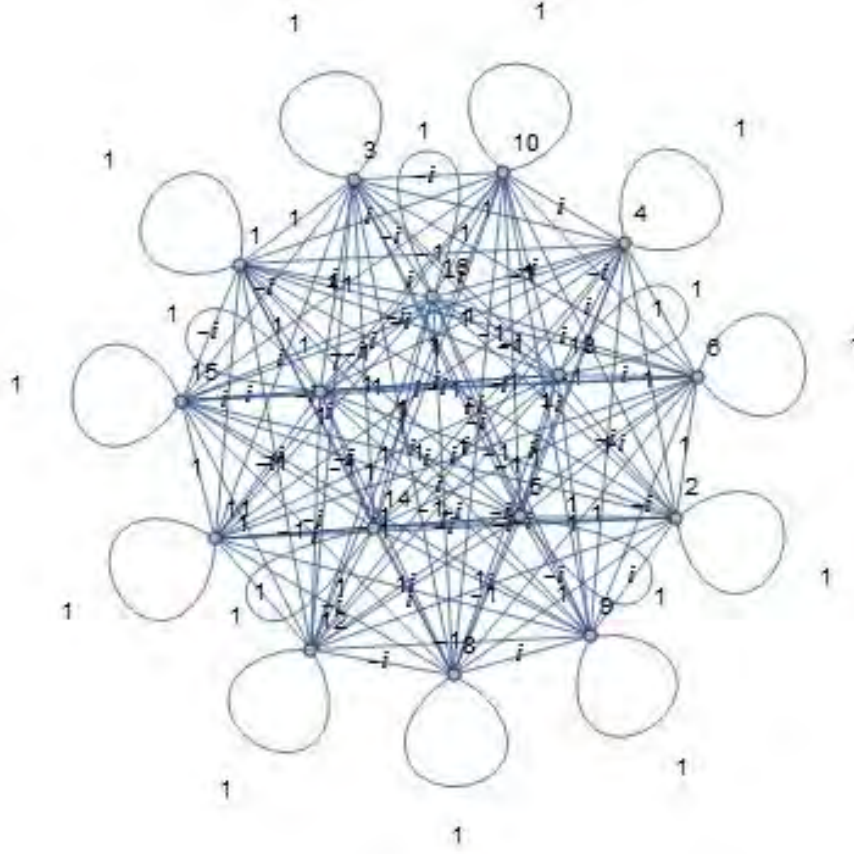


Figure 1: Cayley graph associated to the gbent $f(\mathbf{x}) = x_1 + 2(x_1x_2 \oplus x_3x_4)$

Certainly, one can define a modified (generalized) Cayley graph G'_f where two vertices are connected if and only if $f(\mathbf{u} \oplus \mathbf{v}) \neq 0$ with weights given by $\zeta^{f(\mathbf{u} \oplus \mathbf{v})}$. We sketch in Figure 2 such a graph (it is ultimately the above graph with all weight 1 edges removed).

In Example 2, we give an example of a generalized Cayley graph, and its spectrum.

Example 2. Let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_4$ defined by $f(x_1, x_2) = x_1x_2 + 2x_1$. The truth table is $(0 \ 0 \ 2 \ 3)^T$ (using the lexicographical order x_1, x_2). Then, the adjacency matrix (with multiplicative weights) is

$$A_f = \begin{pmatrix} 1 & 1 & -1 & -i \\ 1 & 1 & -i & -1 \\ -1 & -i & 1 & 1 \\ -i & -1 & 1 & 1 \end{pmatrix}.$$

A basis for its eigenspace is $\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4\}$, where $\vec{v}_1 = (1 \ 1 \ 1 \ 1)^T$ with $\chi_1(\mathbf{x}) = (-1)^0$, $\vec{v}_2 = (1 \ -1 \ 1 \ -1)^T$ with $\chi_2(\mathbf{x}) = (-1)^{x_2}$, $\vec{v}_3 = (1 \ 1 \ -1 \ -1)^T$ with $\chi_3(\mathbf{x}) = (-1)^{x_1}$, $\vec{v}_4 = (1 \ -1 \ -1 \ 1)^T$ with $\chi_4(\mathbf{x}) = (-1)^{x_1+x_2}$, having respective eigenvalues $\lambda_0 =$

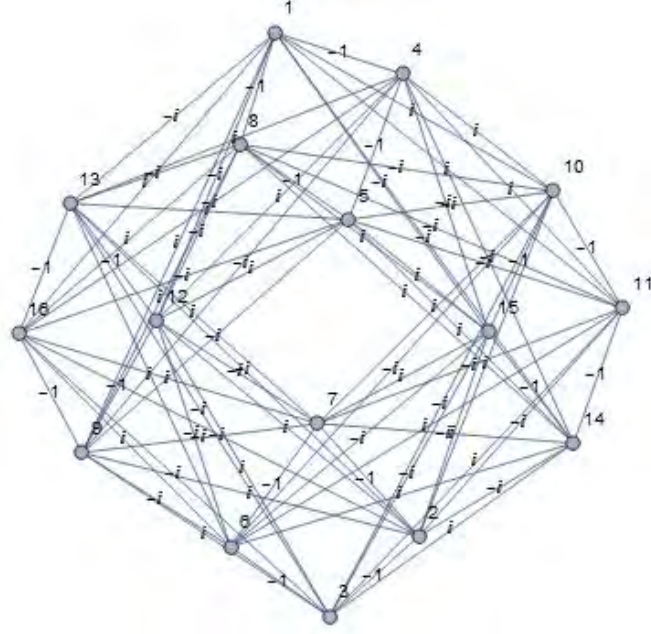


Figure 2: Modified Cayley graph associated to gbent $f(\mathbf{x}) = x_1 + 2(x_1x_2 \oplus x_3x_4)$

$1 - i$, $\lambda_1 = -1 + i$, $\lambda_2 = 3 + i$, $\lambda_3 = 1 - i$. We can see that the eigenvalues A_f are

$$\begin{aligned}\lambda_0 &= i^0\chi_1(00) + i^0\chi_1(01) + i^2\chi_1(10) + i^3\chi_1(11) = 1 + 1 + i^2 + i^3 = 1 - i = \mathcal{H}_f^{(4)}(\mathbf{0}), \\ \lambda_1 &= i^0\chi_2(00) + i^0\chi_2(01) + i^2\chi_2(10) + i^3\chi_2(11) = 1 - 1 + i^2 - i^3 = -1 + i = \mathcal{H}_f^{(4)}(\mathbf{1}), \\ \lambda_2 &= i^0\chi_3(00) + i^0\chi_3(01) + i^2\chi_3(10) + i^3\chi_3(11) = 1 + 1 - i^2 - i^3 = 3 + i = \mathcal{H}_f^{(4)}(\mathbf{2}), \\ \lambda_3 &= i^0\chi_4(00) + i^0\chi_4(01) + i^2\chi_4(10) + i^3\chi_4(11) = 1 - 1 - i^2 + i^3 = 1 - i = \mathcal{H}_f^{(4)}(\mathbf{3}).\end{aligned}$$

Although, we do not use it in this paper, we define the *strength* of the vertex \mathbf{a} in the Cayley graph G_f as the sum of the additive weights of incident edges, that is, $s(\mathbf{a}) = \sum_b f(\mathbf{a} \oplus \mathbf{b})$.

Remark 3. If $f \in \mathcal{GB}_n^q$ and G_f is its Cayley graph, we observe that all vertices are adjacent of multiplicative (respectively, additive) weights in $\mathbb{U}_q = \{1, \zeta, \zeta^2, \dots, \zeta^{q-1}\}$ (respectively, in $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$).

We next show that the eigenvalues of the Cayley graph G_f (with multiplicative weights) are precisely the (generalized) Walsh-Hadamard coefficients.

Theorem 4. Let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$, $q = 2^k$, and let $\lambda_i, 0 \leq i \leq 2^n - 1$ be the eigenvalues of its associated (multiplicative) edge-weighted graph G_f . Then,

$$\lambda_i = \mathcal{H}_f^{(q)}(\mathbf{i}) \text{ (recall that } \mathbf{i} = \iota^{-1}(i)).$$

Proof. Let $\chi : \mathbb{V}_n \rightarrow \mathbb{C}$ be a character of \mathbb{V}_n , and for each such character, let $\mathbf{x}_\chi = (x_j)_{0 \leq j \leq 2^n - 1} \in \mathbb{C}^{2^n}$, where $x_j = \chi(\mathbf{j})$. We claim (and show) that \mathbf{x}_χ is an eigenvector

of $A = A_f$ (for simplicity, we use A in lieu of A_f in this proof), with eigenvalue $\sum_{k=0}^{q-1} \sum_{\mathbf{s}_k \in S_k} \zeta^k \chi(\mathbf{s}_k)$, where $S_k = \{\mathbf{s}_k : f(\mathbf{s}_k) = k\}$. (Observe that the characters of \mathbb{V}_n are $\chi_{\mathbf{w}}(\mathbf{x}) = (-1)^{\mathbf{u} \cdot \mathbf{x}}$, and thus the eigenvalues are exactly the Walsh–Hadamard transform coefficients).

The i -th entry of $A\mathbf{x}$ is

$$(A\mathbf{x})_i = \sum_j A_{i,j} x_j = \sum_j A_{i,j} \chi(\mathbf{j}) = \sum_{k=0}^{q-1} \sum_{\mathbf{i} \oplus \mathbf{j} \in S_k} \zeta^k \chi(\mathbf{j})$$

If $\mathbf{i} \oplus \mathbf{j} \in S_k$, then $\mathbf{i} \oplus \mathbf{j} = \mathbf{s}_k$, for some $\mathbf{s}_k \in S_k$, and so, $\mathbf{j} = \mathbf{i} \oplus \mathbf{s}_k$. Since χ is a character,

$$\chi(\mathbf{j}) = \chi(\mathbf{i} \oplus \mathbf{s}_k) = \chi(\mathbf{i}) \chi(\mathbf{s}_k) = x_i \chi(\mathbf{s}_k)$$

Then,

$$(A\mathbf{x})_i = \sum_{k=0}^{q-1} \sum_{\mathbf{s}_k \in S_k} \zeta^k x_i \chi(\mathbf{s}_k) = x_i \sum_{k=0}^{q-1} \sum_{\mathbf{s}_k \in S_k} \zeta^k \chi(\mathbf{s}_k),$$

which shows our theorem. \square

4 Generalized bents and their Cayley graphs

We recall that a q -Butson Hadamard matrix [6] (q -BH) of dimension d is a $d \times d$ matrix H with all entries q -th roots of unity such that $HH^* = dI_d$, where H^* is the conjugate transpose of H . When $q = 2$, q -BH matrices are called Hadamard matrices (where the entries are ± 1). Recall that the *crosscorrelation* function is defined by

$$\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{z})},$$

and the *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{V}_n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$.

Theorem 5. *Let $f \in \mathcal{GB}_n^q$. Then f is gbent if and only if the adjacency matrix A_f of the (multiplicative) edge-weighted Cayley graph associated to f is a q -Butson Hadamard matrix.*

Proof. Let $A_f = (\zeta^{f(\mathbf{a} \oplus \mathbf{b})})_{\mathbf{a}, \mathbf{b}}$. Then, the (\mathbf{a}, \mathbf{b}) -entry of $A_f \cdot \bar{A}_f$ is

$$(A_f \cdot \bar{A}_f)_{\mathbf{a}, \mathbf{b}} = \sum_{\mathbf{c} \in \mathbb{V}_n} \zeta^{f(\mathbf{a} \oplus \mathbf{c})} \zeta^{\bar{f}(\mathbf{c} \oplus \mathbf{b})} = \sum_{\mathbf{c} \in \mathbb{V}_n} \zeta^{f(\mathbf{a} \oplus \mathbf{c}) - f(\mathbf{c} \oplus \mathbf{b})} = \mathcal{C}_f(\mathbf{a} \oplus \mathbf{b}). \quad (2)$$

Now, recall from [15] that if $f, g \in \mathcal{GB}_n^q$, then

$$\begin{aligned} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{C}_{f,g}(\mathbf{u}) (-1)^{\mathbf{u} \cdot \mathbf{x}} &= 2^{-n} \mathcal{H}_f(\mathbf{x}) \overline{\mathcal{H}_g(\mathbf{x})}, \\ \mathcal{C}_{f,g}(\mathbf{u}) &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{x}) \overline{\mathcal{H}_g(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}. \end{aligned}$$

Thus, equation (2) becomes

$$(A_f \cdot \bar{A}_f)_{\mathbf{a}, \mathbf{b}} = 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{x}) \overline{\mathcal{H}_f(\mathbf{x})} (-1)^{(\mathbf{a} \oplus \mathbf{b}) \cdot \mathbf{x}} = 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \|\mathcal{H}_f(\mathbf{x})\|^2 (-1)^{(\mathbf{a} \oplus \mathbf{b}) \cdot \mathbf{x}}.$$

By Parseval's identity, if $\mathbf{a} = \mathbf{b}$, then $(A_f \cdot \bar{A}_f)_{\mathbf{a}, \mathbf{a}} = 2^n$. Assume now that $\mathbf{a} \neq \mathbf{b}$ and we shall show that $(A_f \cdot \bar{A}_f)_{\mathbf{a}, \mathbf{b}} = 0$ for some $\mathbf{a} \neq \mathbf{b}$ if and only if f is gbent. Certainly, if f is gbent then $\|\mathcal{H}_f(\mathbf{x})\|^2 = 2^n$, and since $\sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{(\mathbf{a} \oplus \mathbf{b}) \cdot \mathbf{x}} = 0$, for $\mathbf{a} \oplus \mathbf{b} \neq 0$, we have that implication. We can certainly show it directly, but the converse follows from [15, Theorem 1 (iv)]. \square

For the remaining of the paper, for simplicity, we shall only consider additive weights, namely, our edge-weighted graphs (V, E, w) will have the weight function $w : E \rightarrow \mathbb{Z}_q$, $q = 2^k$.

Next, we say that a weighted graph $G = (V, E, w)$, $V \subseteq \mathbb{V}_n$, $w : E \rightarrow \mathbb{Z}_q$, $q = 2^k$, is a *weighted regular graph* (wrg) of parameters $(v; r_0, r_1, \dots, r_{q-1})$ if every vertex will have exactly r_j neighbors of edge weight j . We denote by $N_j(\mathbf{a})$ the set of all neighbors of a vertex \mathbf{a} of corresponding edge weight j .

Proposition 6. *Given a generalized Boolean function $f \in \mathcal{GB}_n^q$, the associated Cayley graph is weighted regular (of some parameters), that is, every vertex will have the same number of incident edges with a fixed weight.*

Proof. Fix a weight j and a vertex \mathbf{x}_0 , and consider the equation $f(\mathbf{x}_0 \oplus \mathbf{y}) = j$ with solutions $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_t$, say. For any other vertex \mathbf{x}_1 , the equation $f(\mathbf{x}_1 \oplus \mathbf{y}) = j$ will have solutions $\mathbf{y}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_0, \mathbf{y}_2 \oplus \mathbf{x}_1 \oplus \mathbf{x}_0, \dots, \mathbf{y}_t \oplus \mathbf{x}_1 \oplus \mathbf{x}_0$. The proof of the lemma is done. \square

We will define our first concept of strong regularity here. Let X, \bar{X} be a fixed bisection of the weights $\mathbb{Z}_q = X \cup \bar{X}$, $X \cap \bar{X} = \emptyset$, $|X| = |\bar{X}| = 2^{k-1}$, and let $Y \subseteq \mathbb{Z}_q$. We say that a weighted regular (of parameters $(v; r_0, r_1, \dots, r_{q-1})$) graph $G = (V, E, w)$, $V \subseteq \mathbb{V}_n$, $w : E \rightarrow \mathbb{Z}_q$, $q = 2^k$, is a (generalized) $(X; Y)$ -strongly regular (srg) of parameters $(v; r_0, r_1, \dots, r_{q-1}; e_X, d_X)$ if and only if the number of vertices \mathbf{c} adjacent to both \mathbf{a}, \mathbf{b} , with $w(\mathbf{a}, \mathbf{c}) \in Y, w(\mathbf{b}, \mathbf{c}) \in Y$, is exactly e_X if $w(\mathbf{a}, \mathbf{b}) \in X$, respectively, d_X if $w(\mathbf{a}, \mathbf{b}) \in \bar{X}$. One can weaken the condition and define a $(X_1, X_2; Y)$ -srg notion, where $X_1 \cap X_2 = \emptyset$, not necessarily a bisection, and require the number of vertices \mathbf{c} adjacent to both \mathbf{a}, \mathbf{b} , with $w(\mathbf{a}, \mathbf{c}) \in Y, w(\mathbf{b}, \mathbf{c}) \in Y$, to be exactly e_X if $w(\mathbf{a}, \mathbf{b}) \in X_1$, respectively, d_X if $w(\mathbf{a}, \mathbf{b}) \in X_2$; or even allowing a multi-section, and all of these variations can be fresh areas of research for graph theory experts.

Note that our definition (see also [7] for an alternative concept, which we mention in the last section) is a natural extension of the classical definition: Let $q = 2$, and $X = \{1\}$. A classical strongly regular graph is then equivalent to an $(X; X)$ -strongly regular graph.

We first show that (part of) Proposition 1 can be adapted to this notion, as well, in some cases, and we deal below with one such instance.

Proposition 7. *Let $G = (V, E, w)$ be a weighted $(X; X)$ -strongly regular graph of parameters $(v; r_0, r_1, \dots, r_{q-1}; e_X, d_X)$, where $X \subseteq \mathbb{Z}_q$, $v = |V|$. Then,*

$$r_X(r_X - e_X - 1) = d_X(v - r_X - 1),$$

where $r_X = \sum_{i \in X} r_i$.

Proof. Without loss of generality we assume that the weights are additive, that is, they belong to \mathbb{Z}_q . Fix a vertex $\mathbf{u} \in V$ and let A be the set of vertices adjacent to \mathbf{u} with connecting edges of weight in X , and $B = V \setminus \{\mathbf{u}, \mathbf{u}\}$. Observe that $|A| = \sum_{i \in X} r_i = r_X$ and $|B| = v - r_X - 1$. We somewhat follow the combinatorial method of the classical case, and we shall count the number of vertices between A and B in two different ways. For any vertex $\mathbf{a} \in A$, there are exactly e_X vertices in A adjacent to both \mathbf{u}, \mathbf{a} of edge weights in X , and so, exactly $r_X - e_X - 1$ neighbors in B whose connecting edges have weight in X . Therefore, the number of edges of weight in X between A and B is $r_X(r_X - e_X - 1)$.

On the other hand, any vertex $\mathbf{b} \in B$ is adjacent to d_X vertices in A of connecting edge with weight in X (since \mathbf{u}, \mathbf{b} must share d_X common vertices of connecting edges of weight in X) and so, the total number of edges of weight in X between A and B is $d_X(v - r_X - 1)$. The proposition follows. \square

Let $G = (V, E, w)$ ($w : E \rightarrow \mathbb{Z}_q$) be a weighted graph, where $w(E) \subseteq \mathbb{Z}_q$ (or $w(E) \subseteq \mathbb{U}_q$). We define the *complement* of G , denoted by \bar{G} the graph of vertex set V with an edge between two vertices \mathbf{a}, \mathbf{b} having weight $q-1-f(\mathbf{a} \oplus \mathbf{b})$ (or, multiplicatively, $\zeta^{q-1-f(\mathbf{a} \oplus \mathbf{b})}$). This is a natural definition, since if G is the Cayley graph associated to $f = a_0 + 2a_1, a_0, a_i \in \mathcal{B}_n$, then we observe that \bar{G} is the Cayley graph associated to $\bar{f} = \bar{a}_0 + 2\bar{a}_1 + \dots + 2^{k-1}\bar{a}_{k-1}$, where \bar{a}_i is the binary complement of a_i (that follows from $2^k - 1 - f = (1 - a_0) + 2(1 - a_1) + \dots + 2^{k-1}(1 - a_{k-1}) = \bar{a}_0 + 2\bar{a}_1 + \dots + 2^{k-1}\bar{a}_{k-1}$).

Lemma 8. *Let $G = (V, E, w)$ ($w : E \rightarrow \mathbb{Z}_q$) be a weighted regular graph of parameters $(v; r_0, r_1, \dots, r_{q-1})$. Then the complement \bar{G} is a weighted regular graph of parameters $(v; \bar{r}_0, \dots, \bar{r}_{q-1})$, where $\bar{r}_{q-1-j} = r_j$.*

Proof. Let \mathbf{a} be an arbitrary vertex. Recall that we denote by $N_j(\mathbf{a})$ the set of all neighbors of a vertex \mathbf{a} of corresponding edge weight j . Since G is weighted regular, then $|N_j(\mathbf{a})| = r_j$. In the graph \bar{G} , the weight j will transform into $q-1-j$, therefore $\bar{r}_{q-1-j} = r_j$ and the lemma is shown. \square

Let $A \subset B$ and $x \in B$. As it is customary, we will denote by $x + A$ the set $\{x + a : a \in A\}$.

Theorem 9. *Let $G = (V, E, w)$ ($V \subseteq \mathbb{F}_2^n$, $w : E \rightarrow \mathbb{Z}_q$) be an $(X; Y)$ -strongly regular, for some $X, Y \subseteq \mathbb{Z}_q$ with $|X| = 2^{k-1}$, $q = 2^k$, of parameters $(v; r_0, r_1, \dots, r_{q-1}; e_X, d_X)$ such that $q-1-X = X$ or \bar{X} , and $q-1-Y = Y$. Then, the complement \bar{G} is a $(q-1-X; Y)$ -strongly regular graph of parameters $(v; \bar{r}_0, \dots, \bar{r}_{q-1}; \bar{e}_{q-1-X}, \bar{d}_{q-1-X})$, where $\bar{r}_{q-1-j} = r_j$, $\bar{e}_{q-1-X} = e_X$ and $\bar{d}_{q-1-X} = d_X$, if $q-1-X = X$, respectively, $\bar{r}_{q-1-j} = r_j$, $\bar{e}_{q-1-X} = d_X$ and $\bar{d}_{q-1-X} = e_X$, if $q-1-X = \bar{X}$.*

Proof. The first claim follows from Lemma 8. We consider the two cases $q-1-X = X$, or \bar{X} , separately. As before, for any two vertices \mathbf{a}, \mathbf{b} we denote by $N_Y(\mathbf{a}, \mathbf{b})$ the set of all vertices \mathbf{c} adjacent to both \mathbf{a}, \mathbf{b} such that $w(\mathbf{a}, \mathbf{c}) \in Y, w(\mathbf{b}, \mathbf{c}) \in Y$.

Case 1. Let $q-1-X = X$. For any two vertices \mathbf{a}, \mathbf{b} with $w(\mathbf{a}, \mathbf{b}) \in X$, then $|N_Y(\mathbf{a}, \mathbf{b})| = e_X$, since the weight of the edge between \mathbf{a}, \mathbf{b} remains in X . Similarly, for two vertices \mathbf{a}, \mathbf{b} with $w(\mathbf{a}, \mathbf{b}) \in \bar{X}$, then $|N_Y(\mathbf{a}, \mathbf{b})| = d_X$.

Case 2. Let $q-1-X = \bar{X}$. For any two vertices \mathbf{a}, \mathbf{b} with $w(\mathbf{a}, \mathbf{b}) \in X$, then the weight of the edge between \mathbf{a}, \mathbf{b} in \bar{G} is now in \bar{X} , and we know that in that case $N_Y(\mathbf{a}, \mathbf{b}) = d_X$. Similarly, for two vertices \mathbf{a}, \mathbf{b} with $w(\mathbf{a}, \mathbf{b}) \in \bar{X}$, then $|N_Y(\mathbf{a}, \mathbf{b})| = e_X$. \square

In the next theorem, we shall show a strong regularity theorem (a Bernasconi-Codenotti correspondence) for gbents $f \in \mathcal{GB}_n^4$ when n even and $k = 2$. For two vertices \mathbf{a}, \mathbf{b} of the associated Cayley graph, for $i, j \in \{0, 1, 2, 3\}$, let $N_{\{i,j\}}(\mathbf{a}, \mathbf{b})$ be the set of all “neighbor” vertices \mathbf{w} to both \mathbf{a}, \mathbf{b} such that the edges have additive weights $f(\mathbf{w} \oplus \mathbf{a}) \in \{i, j\}, f(\mathbf{w} \oplus \mathbf{b}) \in \{i, j\}$.

Theorem 10. *Let $f \in \mathcal{GB}_n^4$, n even. Then f is gbent if and only if the associated generalized Cayley graph is $(X; \bar{X})$ -strongly regular with $e_X = d_X$, for both $X = \{0, 1\}$, and $X = \{0, 3\}$, that is, if and only if the following two conditions are satisfied:*

- (i) *For any two pairs of vertices $\{\mathbf{a}, \mathbf{b}\}, \{\mathbf{c}, \mathbf{d}\}$, then $|N_{\{2,3\}}(\mathbf{a}, \mathbf{b})| = |N_{\{2,3\}}(\mathbf{c}, \mathbf{d})|$.*
- (ii) *For any two pairs of vertices $\{\mathbf{a}, \mathbf{b}\}, \{\mathbf{c}, \mathbf{d}\}$, then $|N_{\{1,2\}}(\mathbf{a}, \mathbf{b})| = |N_{\{1,2\}}(\mathbf{c}, \mathbf{d})|$.*

Proof. We know that $f = a_0 + 2a_1$, where $a_0, a_1 \in \mathcal{B}_n$, is gbent if and only if $a_1, a_1 \oplus a_0$ are both bent (see [14, 15]). Let $\mathbf{u} \in \mathbb{V}_n$. We have that:

1. $f(\mathbf{u}) = 0 \Leftrightarrow a_0(\mathbf{u}) = 0, (a_1 \oplus a_0)(\mathbf{u}) = 0$
2. $f(\mathbf{u}) = 1 \Leftrightarrow a_0(\mathbf{u}) = 1, (a_1 \oplus a_0)(\mathbf{u}) = 1$
3. $f(\mathbf{u}) = 2 \Leftrightarrow a_0(\mathbf{u}) = 0, (a_1 \oplus a_0)(\mathbf{u}) = 1$
4. $f(\mathbf{u}) = 3 \Leftrightarrow a_0(\mathbf{u}) = 1, (a_1 \oplus a_0)(\mathbf{u}) = 1$

If f is gbent, then $a_1, a_1 \oplus a_0$ are both bent. Then, by [1], their respective graphs are srg with respective parameters $e = d, e' = d'$. We consider the following cases:

- (a) Let any $\mathbf{a}, \mathbf{b}, \mathbf{c}$ such that $f(\mathbf{a} \oplus \mathbf{c}) \in \{1, 2\}$ and $f(\mathbf{b} \oplus \mathbf{c}) \in \{1, 2\}$, then $(a_1 \oplus a_0)(\mathbf{a} \oplus \mathbf{c}) = 1 = (a_1 \oplus a_0)(\mathbf{b} \oplus \mathbf{c})$. Since the graph corresponding to $a_1 \oplus a_0$ is srg with $e' = d'$, then $|\{\mathbf{c} : (a_1 \oplus a_0)(\mathbf{a} \oplus \mathbf{c}) = 1 = (a_1 \oplus a_0)(\mathbf{b} \oplus \mathbf{c})\}| = e'$. Therefore, $|N_{\{1,2\}}(\mathbf{a}, \mathbf{b})| = e'$.
- (b) Let any $\mathbf{a}, \mathbf{b}, \mathbf{c}$ such that $f(\mathbf{a} \oplus \mathbf{c}) \in \{2, 3\}$ and $f(\mathbf{b} \oplus \mathbf{c}) \in \{2, 3\}$, then $a_1(\mathbf{a} \oplus \mathbf{c}) = 1 = a_1(\mathbf{b} \oplus \mathbf{c})$. Since the graph corresponding to a_1 is srg with $e = d$, then $|\{\mathbf{c} : a_1(\mathbf{a} \oplus \mathbf{c}) = 1 = a_1(\mathbf{b} \oplus \mathbf{c})\}| = e$. Therefore, $|N_{\{2,3\}}(\mathbf{a}, \mathbf{b})| = e'$.

Conversely, let the generalized Cayley graph be such that, for any two pairs of vertices $\{\mathbf{a}, \mathbf{b}\}$, $\{\mathbf{c}, \mathbf{d}\}$, then $|N_{\{2,3\}}(\mathbf{a}, \mathbf{b})| = |N_{\{2,3\}}(\mathbf{c}, \mathbf{d})|$, and $|N_{\{1,2\}}(\mathbf{a}, \mathbf{b})| = |N_{\{1,2\}}(\mathbf{c}, \mathbf{d})|$. As seen in the first part of the proof, $|N_{\{2,3\}}(\mathbf{a}, \mathbf{b})| = |\{\mathbf{c} : a_1(\mathbf{a} \oplus \mathbf{c}) = 1 = a_1(\mathbf{b} \oplus \mathbf{c})\}|$. This number is a constant, regardless of the value of $a_1(\mathbf{a} \oplus \mathbf{b})$. This implies that the Cayley graph corresponding to a_1 is srg with $e = d$, where $e = |N_{\{2,3\}}(\mathbf{a}, \mathbf{b})|$.

Similarly, $|N_{\{1,2\}}(\mathbf{a}, \mathbf{b})| = |\{\mathbf{c} : (a_1 \oplus a_0)(\mathbf{a} \oplus \mathbf{c}) = 1 = (a_1 \oplus a_0)(\mathbf{b} \oplus \mathbf{c})\}|$. This number is a constant, regardless of the value of $(a_1 \oplus a_0)(\mathbf{a} \oplus \mathbf{b})$. This implies that the Cayley graph corresponding to $a_1 \oplus a_0$ is srg with $e' = d'$, where $e' = |N_{\{1,2\}}(\mathbf{a}, \mathbf{b})|$. Since both a_1 and $a_1 \oplus a_0$ are therefore bent, we conclude that f is gbent. \square

It is not hard to show that in some instances a “uniform” strong regularity will hold.

Corollary 11. *Let S be a bent set (see [3]), that is, every element of S is a bent function and the sum of any two such is also a bent function. Let $a_0, a_1 \in S$. Then, the generalized edge-weighted Cayley graph of $f = a_0 + 2a_1$ is $(X; \bar{X})$ -strongly regular for any X with $|X| = 2$.*

Remark 12. *One certainly could inquire whether a similar result holds for a gbent for n odd. Since the answer depends on a characterization (not currently known) of classical semibents in terms of their Cayley graphs, we leave that question for a subsequent project of an interested reader.*

While we cannot find a necessary and sufficient condition on a gbent in \mathcal{GB}_n^q , $q = 2^k$, we can follow a similar approach as in Theorem 10 to find a necessary condition on the Cayley graph of a generalized bent in \mathcal{GB}_n^q . As in the previous result, for $X \subseteq \mathbb{Z}_q$ and two vertices \mathbf{u}, \mathbf{v} , let $N_X(\mathbf{u}, \mathbf{v})$ be the set of vertices \mathbf{w} such that $f(\mathbf{u} \oplus \mathbf{w}) \in X$ and $f(\mathbf{v} \oplus \mathbf{w}) \in X$. As usual, $\bar{\mathbf{c}}$ is the complement of the vector \mathbf{c} , and for two vectors $\mathbf{a} = (a_1, \dots, a_t)$, $\mathbf{b} = (b_1, \dots, b_t)$, the notation $\mathbf{a} \preceq \mathbf{b}$ means that $a_i \leq b_i$, for all $1 \leq i \leq t$. Recall that the canonical injection $\iota : \mathbb{V}_s \rightarrow \mathbb{Z}_{2^s}$, $\iota(\mathbf{c}) = \mathbf{c} \cdot (1, 2, \dots, 2^{s-1}) = \sum_{j=0}^{s-1} c_j 2^j$, where $\mathbf{c} = (c_0, c_1, \dots, c_{s-1})$.

Theorem 13. *Let n be even, and $f = a_0 + 2a_1 + \dots + 2^{k-1}a_{k-1}$, $k \geq 2$, $a_i \in \mathcal{B}_n$, be a generalized Boolean function. If f is gbent then the associated edge-weighted Cayley graph is $(X_{\mathbf{c}}^0; X_{\mathbf{c}}^1)$ -strongly regular with $e_{X_{\mathbf{c}}^0} = d_{X_{\mathbf{c}}^0}$, where $X_{\mathbf{c}}^i = \{\iota(\tilde{\mathbf{c}}) + \iota(\mathbf{d}) : \tilde{\mathbf{c}} \preceq (\mathbf{c}, 1), wt(\tilde{\mathbf{c}}) \equiv i \pmod{2}, \mathbf{d} \preceq \tilde{\mathbf{c}}\}$, $i = 0, 1$, for all $\mathbf{c} \in \mathbb{V}_{k-1}$; that is, for all $\mathbf{c} \in \mathbb{V}_{k-1}$, and for any two pairs of vertices $(\mathbf{u}, \mathbf{v}), (\mathbf{x}, \mathbf{y})$,*

$$|N_{X_{\mathbf{c}}^1}(\mathbf{u}, \mathbf{v})| = |N_{X_{\mathbf{c}}^1}(\mathbf{x}, \mathbf{y})|.$$

Proof. The weighted regularity of f follows from Proposition 6. If f is gbent then by [10, Theorem 8], we know that for each $\mathbf{c} \in \mathbb{V}_{k-1}$, the Boolean function $f_{\mathbf{c}}$ defined as

$$f_{\mathbf{c}}(\mathbf{x}) = c_0 a_0(\mathbf{x}) \oplus c_1 a_1(\mathbf{x}) \oplus \dots \oplus c_{k-2} a_{k-2}(\mathbf{x}) \oplus a_{k-1}(\mathbf{x})$$

is a bent function with $\mathcal{W}_{f_{\mathbf{c}}}(\mathbf{a}) = (-1)^{\mathbf{c} \cdot \iota^{-1}(g(\mathbf{a})) + s(\mathbf{a}) 2^{\frac{n}{2}}}$, for some $g : \mathbb{V}_n \rightarrow \mathbb{Z}_{2^{k-1}}$, $s : \mathbb{V}_n \rightarrow \mathbb{F}_2$.

While we cannot control in a simple manner the Walsh-Hadamard spectra conditions of $f_{\mathbf{c}}$ on the Cayley graph of a gbent f , we can derive some necessary conditions for f to be gbent. Let $\mathbf{c} \in \mathbb{V}_{k-1}$ and $f_{\mathbf{c}}$ bent. Consider $\mathbf{u} \in \mathbb{V}_n$. Certainly, the condition that $f_{\mathbf{c}}(\mathbf{u}) = 1$ means that an odd number of functions a_j , occurring (that is, the corresponding coefficient is nonzero) in $f_{\mathbf{c}}$ will output 1 at \mathbf{u} . The a_j 's corresponding to entries that are 0 in \mathbf{c} can be taken either 0 or 1 (hence the condition in the definition of $X_{\mathbf{c}}^i$ that $\mathbf{d} \preceq \bar{\mathbf{c}}$). We see that the set of values of f when $f_{\mathbf{c}}(\mathbf{u}) = 1$ is exactly $X_{\mathbf{c}}^1 = \{\iota(\tilde{\mathbf{c}}) + \iota(\mathbf{d}) : \tilde{\mathbf{c}} \preceq (\mathbf{c}, 1), wt(\tilde{\mathbf{c}}) \equiv 1 \pmod{2}, \mathbf{d} \preceq \bar{\mathbf{c}}\}$. Similarly, the set of values for f when $f_{\mathbf{c}}(\mathbf{u}) = 0$ is $X_{\mathbf{c}}^0 = \{\iota(\tilde{\mathbf{c}}) + \iota(\mathbf{d}) : \tilde{\mathbf{c}} \preceq (\mathbf{c}, 1), wt(\tilde{\mathbf{c}}) \equiv 0 \pmod{2}, \mathbf{d} \preceq \bar{\mathbf{c}}\}$.

Since $f_{\mathbf{c}}$ is bent, then any two vertices, \mathbf{u}, \mathbf{v} , will have the same number of adjacent \mathbf{w} with $f_{\mathbf{c}}(\mathbf{u} \oplus \mathbf{w}) = f_{\mathbf{c}}(\mathbf{v} \oplus \mathbf{w}) = 1$, regardless of the value of $f_{\mathbf{c}}(\mathbf{u} \oplus \mathbf{v})$. This implies that $|N_{X_{\mathbf{c}}^1}(\mathbf{u}, \mathbf{v})|$ is constant for all \mathbf{u}, \mathbf{v} . \square

5 Further comments

We follow the notation of [7] and define yet another strong regularity concept here. Let Γ be an edge-weighted graph (with no loops) with vertices V , edges E , and weight set W (in [7], W was taken to be \mathbb{Z}_q^* , although it could be arbitrary). As before, for each $\mathbf{u} \in V$ and $a \in W \cup \{0\}$, the weighted a -neighborhood of u , $N_a(\mathbf{u})$, is defined as follows:

- $N_a(\mathbf{u})$ = the set of all neighbors \mathbf{v} of \mathbf{u} in Γ for which the edge $(\mathbf{u}, \mathbf{v}) \in E$ has weight a (for each $a \in W$).
- $N^0(\mathbf{u})$ = the set of all nonadjacent \mathbf{v} of \mathbf{u} in Γ (i.e., the set of \mathbf{v} such that $(\mathbf{u}, \mathbf{v}) \notin E$), that is, $N^0(\mathbf{u}) = V \setminus \cup_{a \in W} N_a(\mathbf{u})$. In particular, $\mathbf{u} \in N^0(\mathbf{u})$.

In [7], the following definition of weighted strongly regular graph is given. Let Γ be a connected edge-weighted graph which is regular as a simple (unweighted) graph. Let W be the set of edge-weights of Γ . The graph Γ is called an *edge-weighted local strongly regular* (to distinguish it from our definition we inserted the adjective “local”) with parameters $v, k = (k_a)_{a \in W}, \lambda = (\lambda_a)_{a \in W^3}$, and $\mu = (\mu_a)_{a \in W^2}$, denoted $SRG_W(v, k, \lambda, \mu)$, if Γ has v vertices, and there are constants $k_a, \lambda_{a_1, a_2, a_3}$, and μ_{a_1, a_2} , for $a, a_1, a_2, a_3 \in W$, such that

$$|N_a(\mathbf{u})| = k_a \text{ for all vertices } \mathbf{u},$$

and for vertices $\mathbf{u}_1 \neq \mathbf{u}_2$ we have

$$|N_{a_1}(\mathbf{u}_1) \cap N_{a_2}(\mathbf{u}_2)| = \begin{cases} \lambda_{a_1, a_2, a_3} & \text{if } \exists a_3 \in W \text{ with } \mathbf{u}_1 \in N_{a_3}(\mathbf{u}_2); \\ \mu_{a_1, a_2} & \text{if } \mathbf{u}_1 \notin N_{a_3}(\mathbf{u}_2) \text{ for all } a_3. \end{cases}$$

As was observed in [7] for functions $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$, where several questions were posed, it is not clear what the connection between this concept and generalized (or p -ary) bentness is. Our strong regularity definition does allow us to show such a connection and in the case $k = 2$, we have a complete Bernasconi–Codonotti correspondence [1, 2].

References

- [1] A. Bernasconi, B. Codenotti, *Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem*, IEEE Trans. on Computers **48:3** (1999), 345–351.
- [2] A. Bernasconi, B. Codenotti, J. M. VanderKam, *A Characterization of Bent Functions in terms of Strongly Regular Graphs*, IEEE Trans. on Computers, **50:9** (2001), 984–985.
- [3] C. Bey, G. M. Kyureghyan, *On Boolean functions with the sum of every two of them being bent*, Des. Codes Cryptogr. **49** (2008), 341–346.
- [4] N. Biggs, *Algebraic Graph Theory* (2nd ed.), Cambridge Univ. Press, 1993.
- [5] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer-Verlag, 2014.
- [6] A. T. Butson, *Generalized Hadamard matrices*, Proc. Amer. Math. Soc. **13** (1962), 894–898.
- [7] C. Celerier, D. Joyner, C. Melles, D. Phillips, S. Walsh, *Edge-weighted Cayley Graphs and p -ary Bent Functions*, Integers **16**, A35, 2016.
- [8] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications*, 2nd Ed. (Academic Press, San Diego, CA, 2017); 1st Ed., 2009.
- [9] D. M. Cvetkovic, M. Doob, H. Sachs, *Spectra of Graphs*, Academic Press, 1979.
- [10] T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, to appear in IEEE Trans. Inform. Th., 2017; DOI: 10.1109/TIT.2017.2754498.
- [11] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, In: Duquesne S., Petkova-Nikova S. (eds), *Arithmetic of Finite Fields. WAIFI 2016*, LNCS 10064. Springer, 160–173.
- [12] T. Martinsen, W. Meidl, P. Stănică, *Partial spread and vectorial generalized bent functions*, Des. Codes Crypt. **85:1** (2017), 1–13.
- [13] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.
- [14] P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, Prikl. Diskr. Mat. **1** (2009), 16–18 (see also, <http://eprint.iacr.org/2009/544.pdf>).
- [15] P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Crypt. **69** (2013), 77–94.
- [16] C. Tang, C. Xiang, Y. Qi, K. Feng, *Complete characterization of generalized bent and 2^k -bent Boolean functions*, IEEE Trans. Inform. Th. **63:7** (2017), 4668–4674.

- [17] N. Tokareva, *Generalizations of bent functions: a survey of publications*, (Russian) Diskretn. Anal. Issled. Oper. 17 (2010), no. 1, 34–64; translation in J. Appl. Ind. Math. 5:1 (2011), 110–129.
- [18] N. Tokareva, *Bent Functions, Results and Applications to Cryptography*, Academic Press, San Diego, CA, 2015.