Generalized bent Boolean functions and strongly regular Cayley graphs

Constanza Riera\textsuperscript{1}, Pantelimon Stănică\textsuperscript{2}, Sugata Gangopadhyay\textsuperscript{3},

\textsuperscript{1}Department of Computing, Mathematics, and Physics, Western Norway University of Applied Sciences, 5020 Bergen, Norway; \texttt{csr@hvl.no}
\textsuperscript{2}Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943, USA; \texttt{pstanica@nps.edu}
\textsuperscript{3}Department of Computer Science and Engineering Indian Institute of Technology Roorkee, Roorkee 247667, INDIA; \texttt{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, "." A Boolean function $f$ on $n$ variables is a mapping from $\mathbb{V}_n$ into $\mathbb{F}_2$, that is, a multivariate polynomial over $\mathbb{F}_2$,

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

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 $f$.

For a Boolean function on $\mathbb{V}_n$, the Hamming weight of $f$, $wt(f)$, is the cardinality of $\Omega_f = \{x \in \mathbb{V}_n : f(x) = 1\}$ (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 \( f, g : \mathbb{V}_n \to \mathbb{F}_2 \) is \( d(f, g) = wt(f \oplus g) \). A Boolean function \( f(x) \) is called an affine function if its algebraic degree is 1. If, in addition, \( a_0 = 0 \) in \([1]\), then \( f(x) \) is a linear function (see \[9\] 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 \( u \cdot x \) as an inner product.

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

\[
H_f^{(q)}(u) = \sum_{x \in V_n} \zeta_q^{f(x)}(-1)^{u \cdot x},
\]

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

\[
W_f(u) = \sum_{x \in V_n} (-1)^{f(x)}(-1)^{u \cdot x},
\]

which defines the coefficients of character form of \( f \) with respect to the orthonormal basis of the group characters \( \chi_w(x) = (-1)^{w \cdot x} \). In turn, \( f(x) = 2^{-n} \sum_w W_f(w)(-1)^{u \cdot x} \).

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 \( f : \mathbb{V}_n \to \mathbb{Z}_q \) is called generalized bent (gbent) if \( |\mathcal{H}_f(u)| = 2^{n/2} \) for all \( u \in \mathbb{V}_n \). We recall that a function \( f \) for which \( |W_f(u)| = 2^{n/2} \) for all \( u \in \mathbb{V}_n \) is called a bent function, which only exist for even \( n \) since \( W_f(u) \) 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

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

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 \( u, v \) the number of vertices adjacent to both \( u, v \) is \( d \), \( e \), if \( u, v \) are adjacent, respectively, nonadjacent (see for instance \([9]\)). The complementary graph \( \overline{G} \) 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 \textit{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 \textit{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 \textit{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

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

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

The adjacency matrix \( A_f \) is the matrix whose entries are \( A_{i,j} = f(i \oplus j) \) (here \( \iota \) 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 \textit{regular graph of degree} \( \text{wt}(f) = |\Omega_f| \) (see \([9, \text{Chapter 3}]\) for further definitions).

Given a graph \( f \) and its adjacency matrix \( A \), the \textit{spectrum}, with notation \( \text{Spec}(G_f) \), 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 \([9, \text{pp. 194–195}]\)) that a connected \( r \)-regular graph is strongly regular iff it has exactly three distinct eigenvalues \( \lambda_0 = r, \lambda_1, \lambda_2 \) (so \( e = r + \lambda_1 \lambda_2 + \lambda_1 + \lambda_2, \quad d = r + \lambda_1 \lambda_2 \)).

The following result is known \([9, \text{Th. 3.32, p. 103}]\) (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 \( f : \mathbb{V}_n \to \mathbb{Z}_q \) be a generalized Boolean function. We define the \textit{(generalized) Cayley graph} \( G_f \) to be the graph where vertices are the elements of \( \mathbb{V}_n \) and two vertices \( u, v \) are connected by a weighted edge of (multiplicative) weight \( \zeta_f(u \oplus v) \) (respectively, additive weight \( f(u \oplus v) \)). Certainly, the underlying unweighted graph is a complete pseudograph (every vertex also has a loop). We sketch in Figure 1 such an example.
Certainly, one can define a modified (generalized) Cayley graph $G'_f$ where two vertices are connected if and only if $f(u \oplus v) \neq 0$ with weights given by $\zeta^{f(u \oplus v)}$. 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 $f : \mathbb{V}_n \to \mathbb{Z}_4$ 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 $\chi_1(x) = (-1)^0$, $\vec{v}_2 = (1 \ -1 \ 1 \ -1)^T$ with $\chi_2(x) = (-1)^{x_2}$, $\vec{v}_3 = (1 \ 1 \ -1 \ -1)^T$ with $\chi_3(x) = (-1)^{x_1}$, $\vec{v}_4 = (1 \ -1 \ -1 \ 1)^T$ with $\chi_4(x) = (-1)^{x_1 + x_2}$, having respective eigenvalues $\lambda_0 =$
Figure 2: Modified Cayley graph associated to gbent $f(x) = x_1 + 2(x_1x_2 \oplus x_3x_4)$

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

$\lambda_0 = i^0 \chi_1(00) + i^0 \chi_1(01) + i^2 \chi_1(10) + i^3 \chi_1(11) = 1 + 1 + i^2 + i^3 = 1 - i = H_f^{(4)}(0)$,

$\lambda_1 = i^0 \chi_2(00) + i^0 \chi_2(01) + i^2 \chi_2(10) + i^3 \chi_2(11) = 1 - 1 + i^2 - i^3 = -1 + i = H_f^{(4)}(1)$,

$\lambda_2 = i^0 \chi_3(00) + i^0 \chi_3(01) + i^2 \chi_3(10) + i^3 \chi_3(11) = 1 + 1 - i^2 - i^3 = 3 + i = H_f^{(4)}(2)$,

$\lambda_3 = i^0 \chi_4(00) + i^0 \chi_4(01) + i^2 \chi_4(10) + i^3 \chi_4(11) = 1 - 1 - i^2 + i^3 = 1 - i = H_f^{(4)}(3)$.

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

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

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

$$\lambda_i = H_f^{(q)}(i) \text{ (recall that } i = \iota^{-1}(i)).$$

Proof. Let $\chi : \mathbb{V}_n \to \mathbb{C}$ be a character of $\mathbb{V}_n$, and for each such character, let $x_\chi = (x_j)_{0 \leq j \leq 2^n - 1} \in \mathbb{C}^{2^n}$, where $x_j = \chi(j)$. We claim (and show) that $x_\chi$ is an eigenvector
of $A = A_f$ (for simplicity, we use $A$ in lieu of $A_f$ in this proof), with eigenvalue 
$$
\sum_{k=0}^{q-1} \sum_{s_k \in S_k} \zeta^k \chi(s_k),
$$
where $S_k = \{s_k : f(s_k) = k\}$. (Observe that the characters of $\mathbb{V}_n$ are
$$
\chi_w(x) = (-1)^{u \cdot x},
$$
and thus the eigenvalues are exactly the Walsh–Hadamard transform coefficients).

The $i$-th entry of $Ax$ is
$$
(Ax)_i = \sum_j A_{i,j}x_j = \sum_j A_{i,j} \chi(j) = \sum_{k=0}^{q-1} \sum_{i \oplus j \in S_k} \zeta^k \chi(j)
$$
If $i \oplus j \in S_k$, then $i \oplus j = s_k$, for some $s_k \in S_k$, and so, $j = i \oplus s_k$. Since $\chi$ is a character,
$$
\chi(j) = \chi(i \oplus s_k) = \chi(i) \chi(s_k) = x_i \chi(s_k)
$$
Then,
$$
(Ax)_i = \sum_{k=0}^{q-1} \sum_{s_k \in S_k} \zeta^k x_i \chi(s_k) = x_i \sum_{k=0}^{q-1} \sum_{s_k \in S_k} \zeta^k \chi(s_k),
$$
which shows our theorem. \(\square\)

4 Generalized bents and their Cayley graphs

We recall that a $q$-Butson Hadamard matrix \([\mathbf{6}]\) ($q$-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 $\pm 1$). Recall that the crosscorrelation function is defined by
$$
C_{f,g}(z) = \sum_{x \in \mathbb{V}_n} \zeta^{f(x) - g(x \oplus z)},
$$
and the autocorrelation of $f \in GB_n^q$ at $u \in \mathbb{V}_n$ is $C_{f,f}(u)$ above, which we denote by $C_f(u)$.

Theorem 5. Let $f \in GB_n^q$. Then $f$ is bent 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 $A_f = (\zeta^{f(a \oplus b)})_{a,b}$. Then, the $(a,b)$-entry of $A_f \cdot A_f$ is
$$
(A_f \cdot A_f)_{a,b} = \sum_{c \in \mathbb{V}_n} \zeta^{f(a \oplus c)} \zeta^{f(c \oplus b)} = \sum_{c \in \mathbb{V}_n} \zeta^{f(a \oplus c) - f(a \oplus b)} = C_f(a \oplus b). \quad (2)
$$
Now, recall from \([\mathbf{15}]\) that if $f, g \in GB_n^q$, then
$$
\sum_{u \in \mathbb{V}_n} C_{f,g}(u)(-1)^{u \cdot x} = 2^{-n}H_f(x)\overline{H_g(x)},
$$
$$
C_{f,g}(u) = 2^{-n} \sum_{x \in \mathbb{V}_n} H_f(x)\overline{H_g(x)}(-1)^{u \cdot x}.
$$
Thus, equation (2) becomes

\[(A_f \cdot \tilde{A}_f)_{a,b} = 2^{-n} \sum_{x \in V_n} \mathcal{H}_f(x)\mathcal{H}_f(x)(-1)^{(a \oplus b) \cdot x} = 2^{-n} \sum_{x \in V_n} \|\mathcal{H}_f(x)\|^2(-1)^{(a \oplus b) \cdot x}.\]

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

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

**Proposition 6.** Given a generalized Boolean function \(f \in \mathcal{GB}_q\), 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 \(x_0\), and consider the equation \(f(x_0 \oplus y) = j\) with solutions \(y_1,y_2,\ldots,y_t\), say. For any other vertex \(x_1\), the equation \(f(x_1 \oplus y) = j\) will have solutions \(y_1 \oplus x_1 \oplus x_0,y_2 \oplus x_1 \oplus x_0,\ldots,y_t \oplus x_1 \oplus x_0\). The proof of the lemma is done.

We will define our first concept of strong regularity here. Let \(X,\bar{X}\) be a fixed bisection of the weights \(\mathbb{Z}_q = X \cup \bar{X}, X \cap \bar{X} = \emptyset, |X| = |ar{X}| = 2^{k-1}\), and let \(Y \subseteq \mathbb{Z}_q\). We say that a weighted regular (of parameters \((v;r_0,r_1,\ldots,r_{q-1})\)) graph \(G = (V,E,w)\), \(V \subseteq V_n\), \(w : E \rightarrow \mathbb{Z}_q\), \(q = 2^k\), is a (generalized) \((X;Y)\)-strongly regular (srg) of parameters \((v;r_0,r_1,\ldots,r_{q-1};e_X,d_X)\) if and only if the number of vertices \(c\) adjacent to both \(a,b\), with \(w(a,c) \in Y,w(b,c) \in Y\), is exactly \(e_X\) if \(w(a,b) \in X\), respectively, \(d_X\) if \(w(a,b) \in \bar{X}\). 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 \(c\) adjacent to both \(a,b\), with \(w(a,c) \in Y,w(b,c) \in Y\), to be exactly \(e_X\) if \(w(a,b) \in X_1\), respectively, \(d_X\) if \(w(a,b) \in X_2\); 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 \((v; r_0, r_1, \ldots, r_{q-1}; e_X, d_X)\), 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 \( u \in V \) and let \( A \) be the set of vertices adjacent to \( u \) with connecting edges of weight in \( X \), and \( B = V \setminus \{A, u\} \). 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 \( G = (V, E, w) \) \((w : E \to \mathbb{Z}_q)\) 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, \( c^{q-1-f(\mathbf{a} \oplus \mathbf{b})} \)). This is a natural definition, since if \( G \) is the Cayley graph associated to \( f = a_0 + 2a_1, a_0, a_i \in B_n \), then we observe that \( \bar{G} \) is the Cayley graph associated to \( \bar{f} = a_0 + 2a_1 + \cdots + 2^{k-1}a_{k-1} \), where \( a_i \) is the binary complement of \( a_i \) (that follows from \( 2^k - 1 - f = (1 - a_0) + 2(1 - a_1) + \cdots + 2^{k-1}(1 - a_{k-1}) = \bar{a}_0 + 2\bar{a}_1 + \cdots + 2^{k-1}\bar{a}_{k-1} \)).

Lemma 8. Let \( G = (V, E, w) \) \((w : E \to \mathbb{Z}_q)\) be a weighted regular graph of parameters \((v; r_0, r_1, \ldots, r_{q-1})\). Then the complement \( \bar{G} \) is a weighted regular graph of parameters \((v; \bar{r}_0, \ldots, \bar{r}_{q-1})\), 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 \( A \subseteq B \) and \( x \in B \). As it is customary, we will denote by \( x + A \) the set \( \{x + a : a \in A\} \).

Theorem 9. Let \( G = (V, E, w) \) \((V \subseteq \mathbb{F}_2^n, w : E \to \mathbb{Z}_q)\) be an \((X; Y)\)-strongly regular, for some \( X, Y \subseteq \mathbb{Z}_q \) with \(|X| = 2^k-1, q = 2^k \), of parameters \((v; r_0, r_1, \ldots, r_{q-1}; e_X, d_X)\) 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 \((v; \bar{r}_0, \ldots, \bar{r}_{q-1}; \bar{e}_{q-1-X}, \bar{d}_{q-1-X})\), 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 $X$, separately. As before, for any two vertices $a, b$ we denote by $N_Y(a, b)$ the set of all vertices $c$ adjacent to both $a, b$ such that $w(a, c) \in Y, w(b, c) \in Y$.

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

Similarly, for two vertices $a, b$ with $w(a, b) \in \bar{X}$, then $|N_Y(a, b)| = d_X$.

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

Similarly, for two vertices $a, b$ with $w(a, b) \in \bar{X}$, then $|N_Y(a, b)| = e_X$. 

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 $a, b$ of the associated Cayley graph, for $i, j \in \{0, 1, 2, 3\}$, let $N_{\{i,j\}}(a, b)$ be the set of all “neighbor” vertices $w$ to both $a, b$ such that the edges have additive weights $f(w \oplus a) \in \{i, j\}, f(w \oplus b) \in \{i, j\}$.

**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 $\{a, b\}, \{c, d\}$, then $|N_{\{2,3\}}(a, b)| = |N_{\{2,3\}}(c, d)|$.

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

**Proof.** We know that $f = a_0 + 2a_1$, where $a_0, a_1 \in B_n$, is gbent if and only if $a_1, a_1 \oplus a_0$ are both bent (see [13][15]). Let $u \in \mathbb{V}_n$. We have that:

1. $f(u) = 0 \iff a_0(u) = 0, (a_1 \oplus a_0)(u) = 0$
2. $f(u) = 1 \iff a_0(u) = 1, (a_1 \oplus a_0)(u) = 1$
3. $f(u) = 2 \iff a_0(u) = 0, (a_1 \oplus a_0)(u) = 1$
4. $f(u) = 3 \iff a_0(u) = 1, (a_1 \oplus a_0)(u) = 1$

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

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


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

Similarly, \( |N_{(1,2)}(a, b)| = \{\{c : (a_1 \oplus a_0)(a \oplus c) = 1 = (a_1 \oplus a_0)(b \oplus c)\}\} \). This number is a constant, regardless of the value of \( (a_1 \oplus a_0)(a \oplus b) \). This implies that the Cayley graph corresponding to \( a_1 \oplus a_0 \) is srg with \( e' = d' \), where \( e' = |N_{(1,2)}(a, b)| \). 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 \((X; \tilde{X})\)-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 semibent 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 \( GB_{n}^{q} \), \( q = 2^k \), we can follow a similar approach as in Theorem [10] to find a necessary condition on the Cayley graph of a generalized bent in \( GB_{n}^{q} \). As in the previous result, for \( X \subseteq \mathbb{Z}_q \) and two vertices \( u, v \), let \( N_{X}(u, v) \) be the set of vertices \( w \) such that \( f(u \oplus w) \in X \) and \( f(v \oplus w) \in X \). As usual, \( \tilde{c} \) is the complement of the vector \( c \), and for two vectors \( a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t), \) the notation \( a \preceq b \) means that \( a_i \leq b_i \), for all \( 1 \leq i \leq t \). Recall that the canonical injection \( \iota : W_s \rightarrow \mathbb{Z}_q^t \), \( \iota(c) = c \cdot (1, 2, \ldots, 2^{s-1}) = \sum_{j=0}^{s-1} c_j 2^j \), where \( c = (c_0, c_1, \ldots, c_{s-1}) \).

**Theorem 13.** Let \( n \) be even, and \( f = a_0 + 2a_1 + \cdots + 2^{k-1}a_{k-1}, k \geq 2, a_i \in B_n, \) be a generalized Boolean function. If \( f \) is gbent then the associated edge-weighted Cayley graph is \((X_0^q; X_1^q)\)-strongly regular with \( e_{X_0^q} = d_{X_0^q} \), where \( X_0^q = \{\iota(\tilde{c}) + \iota(d) : \tilde{c} \preceq (c, 1), \text{wt}(\tilde{c}) \equiv i \pmod{2}, d \preceq \tilde{c}\}, i = 0, 1, \) for all \( c \in V_{k-1} \); that is, for all \( c \in V_{k-1} \), and for any two pairs of vertices \( (u, v), (x, y) \),

\[ |N_{X_1^q}(u, v)| = |N_{X_2^q}(x, y)|. \]

**Proof.** The weighted regularity of \( f \) follows from Proposition [6]. If \( f \) is gbent then by [10] Theorem 8, we know that for each \( c \in V_{k-1} \), the Boolean function \( f_c \) defined as

\[ f_c(x) = c_0a_0(x) \oplus c_1a_1(x) \oplus \cdots \oplus c_{k-2}a_{k-2}(x) \oplus a_{k-1}(x) \]

is a bent function with \( W_{f_c}(a) = (-1)^{c_{k-1}(g(a) + s(a))2^{k-1}} \), for some \( g : V_n \rightarrow \mathbb{Z}_{2^{k-1}}, s : V_n \rightarrow \mathbb{F}_2 \).
While we cannot control in a simple manner the Walsh-Hadamard spectra conditions of \( f_c \) on the Cayley graph of a gbent \( f \), we can derive some necessary conditions for \( f \) to be gbent. Let \( c \in \mathbb{V}_{k-1} \) and \( f_c \) bent. Consider \( u \in \mathbb{V}_n \). Certainly, the condition that \( f_c(u) = 1 \) means that an odd number of functions \( a_j \), occurring (that is, the corresponding coefficient is nonzero) in \( f_c \) will output 1 at \( u \). The \( a_j \)'s corresponding to entries that are 0 in \( c \) can be taken either 0 or 1 (hence the condition in the definition of \( X^i_c \) that \( d \preceq \bar{c} \)). We see that the set of values of \( f \) when \( f_c(u) = 1 \) is exactly \( X^i_c = \{ \iota(c) + \iota(d) : \bar{c} \preceq (c, 1), \text{wt}(\bar{c}) \equiv 1 \mod 2, d \preceq \bar{c} \} \). Similarly, the set of values for \( f \) when \( f_c(u) = 0 \) is \( X^0_c = \{ \iota(c) + \iota(d) : \bar{c} \preceq (c, 1), \text{wt}(\bar{c}) \equiv 0 \mod 2, d \preceq \bar{c} \} \).

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

5 Further comments

We follow the notation of [7] and define yet another strong regularity concept here. Let \( \Gamma \) be an edge-weighted graph (with no loops) with vertices \( V \), edges \( E \), and weight set \( W \) (in [7], \( W \) was taken to be \( \mathbb{Z}_2^q \), although it could be arbitrary). As before, for each \( u \in V \) and \( a \in W \cup \{0\} \), the weighted \( a \)-neighborhood of \( u \), \( N_a(u) \), is defined as follows:

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

In [7], the following definition of weighted strongly regular graph is given. Let \( \Gamma \) be a connected edge-weighted graph which is regular as a simple (unweighted) graph. Let \( W \) be the set of edge-weights of \( \Gamma \). The graph \( \Gamma \) 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 \( \text{SRG}_W(v, k, \lambda, \mu) \), if \( \Gamma \) has \( v \) vertices, and there are constants \( k_a, \lambda_{a_1,a_2,a_3}, \) and \( \mu_{a_1,a_2} \), for \( a, a_1, a_2, a_3 \in W \), such that

\[
|N_a(u)| = k_a \text{ for all vertices } u,
\]

and for vertices \( u_1 \neq u_2 \) we have

\[
|N_{a_1}(u_1) \cap N_{a_2}(u_2)| = \begin{cases} 
\lambda_{a_1,a_2,a_3} & \text{if } \exists a_3 \in W \text{ with } u_1 \in N_{a_3}(u_2); \\
\mu_{a_1,a_2} & \text{if } u_1 \notin N_{a_3}(u_2) \text{ for all } a_3.
\end{cases}
\]

As was observed in [7] for functions \( f : \mathbb{F}_p^n \to \mathbb{F}_p \), 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–Codenotti 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. Stănićă, 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. Stănićă, *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. Stănićă, *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. Stănićă, *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. Stănićă, 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.