#A35 INTEGERS 16 (2016)

# EDGE-WEIGHTED CAYLEY GRAPHS AND $p$-ARY BENT FUNCTIONS

**Charles Celerier**
*Department of Mathematics, U.S. Naval Academy, Annapolis, Maryland*

**David Joyner**
*Department of Mathematics, U.S. Naval Academy, Annapolis, Maryland*
wdj@usna.edu

**Caroline Melles**
*Department of Mathematics, U.S. Naval Academy, Annapolis, Maryland*
cgg@usna.edu

**David Phillips**
*Department of Mathematics, U.S. Naval Academy, Annapolis, Maryland*
dphillip@usna.edu

**Steven Walsh**
*Department of Mathematics, U.S. Naval Academy, Annapolis, Maryland*

*Received: 9/24/14, Revised: 10/23/15, Accepted: 5/15/16, Published: 6/10/16*

## Abstract

Let $f\colon GF(p)^n \to GF(p)$. When $p = 2$, Bernasconi and Codenotti discovered a correspondence between certain properties of $f$ (e.g., if it is bent) and properties of its associated Cayley graph. Analogously, but much earlier, Dillon showed that $f$ is bent if and only if the "level curves" of $f$ have certain combinatorial properties (again, only when $p = 2$). We investigate an analogous theory when $p > 2$. We formulate some problems concerning natural generalizations of the Bernasconi correspondence and Dillon correspondence. We give a partial classification, in a combinatorial way, of even bent functions $f\colon GF(p)^n \to GF(p)$ with $f(0) = 0$ for $(p, n) = (3, 2)$, $(3, 3)$, and $(5, 2)$, where "even" means $f(x) = f(-x)$. We will show that for any prime $p > 2$, there are $(p+1)!/2$ amorphic bent functions $f\colon GF(p)^2 \to GF(p)$ of signature $(p-1, p-1, \ldots, p-1)$ with algebraic normal form that is homogeneous of degree $p-1$. They are all weakly regular. (Briefly, an amorphic bent function is one whose edge-weighted Cayley graph corresponds to an amorphic association scheme.) Our main conjecture is Conjecture 2, but a number of other open questions are scattered throughout the paper.

## 1. Introduction

Roughly speaking, in this paper we try to investigate which graph-theoretical properties of the Cayley graph of a $p$-ary function can be characterized in terms of function-theoretic properties of the function itself.

In Section 2, we present the combinatorial background needed: difference sets, partial difference sets, weighted partial difference sets, association schemes, adjacency rings and Schur rings. We also discuss how these notions relate in our case. Moreover, we recall the Dillon correspondence and give several examples.

In Section 3, we present the graph-theoretical background needed: Cayley graphs associated with Boolean functions, edge-weighted Cayley graphs associated with $p$-ary functions, amorphic Cayley graphs, strongly regular graphs, and edge-weighted strongly regular graphs. In brief, an amorphic edge-weighted graph is a graph whose corresponding association scheme is amorphic (i.e., one for which all fusions of it are also association schemes). Results on the graph spectrum of edge-weighted Cayley graphs are recalled. We also recall the Bernasconi correspondence in that section and formulate several analogues in the $p$-ary case. More precisely, we try to investigate which graph-theoretical properties of the Cayley graph $\Gamma_f$ of a $p$-ary function $f\colon GF(p)^n \to GF(p)$ can be characterized in terms of function-theoretic properties of $f$, and which function-theoretic properties of $f$ correspond to combinatorial properties of the set of "level curves" $f^{-1}(a)$ (where $a \in GF(p)$). Our main conjecture, Conjecture 2, can be found there.

In Section 4, we give a general formula for algebraic normal forms. For any prime $p > 2$, we show there are $(p+1)!/2$ amorphic bent functions $f\colon GF(p)^2 \to GF(p)$ of signature $(p-1, p-1, \dots, p-1)$ with algebraic normal form that is homogeneous of degree $p-1$. Additionally, we summarize Sagemath computations of a large number of examples (for $p = 3, 5$), which support Conjecture 2 of Section 3.

Finally, in Section 5, we present some suggestions for further study.

More computational details and more (standard) proofs can be found in the expanded paper [10].

Fix $n \geq 1$ and let $V = GF(p)^n$, where $p$ is a prime. Let $f\colon V \to GF(p)$ be given. Our main interest is in how to classify properties of *bent* functions, an important class of functions used in encryption algorithms (e.g., see [16, 21, 28, 36]). For the case when $p = 2$, i.e., $f$ is a binary function, there is a one-to-one correspondence between $f$ being bent and $f^{-1}(1)$ giving rise to a difference set [15] (see Theorem 11 below). In addition, when $p = 2$, $f$ is bent if and only if the Cayley graph of $f$ is strongly regular [1, 2, 3] (see Theorem 25 below). We investigate how these theorems generalize when $p > 2$. We require the following definitions.

**Definition 1.** The *Walsh(-Hadamard) transform* of a function $f\colon GF(p)^n \to GF(p)$ is a complex-valued function on $V$ that can be defined as

$$W_f(u) = \sum_{x \in V} \zeta^{f(x) - \langle u, x \rangle}, \tag{1}$$

where $\zeta = e^{2\pi i/p}$ and $\langle \ , \ \rangle$ is the usual inner product.

We call $f$ *bent* if

$$|W_f(u)| = p^{n/2}, \tag{2}$$

for all $u \in V$. The $p$-ary bent functions are "maximally non-linear" in some sense, and can be used to generate pseudo-random sequences rather easily.

Next, we recall some properties of the Walsh transform.

1. The Walsh coefficients satisfy *Parseval's equation*

$$\sum_{u \in V} |W_f(u)|^2 = p^{2n}.$$

2. If $\sigma$ denotes the map $\sigma_k \colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ defined by sending $\zeta$ to $\zeta^k$, then $W_f(u)^\sigma = W_{kf}(ku)$, where $W_f(u)^\sigma$ is the image of $W_f(u) \in \mathbb{Q}(\zeta)$ under $\sigma$.

If $f \colon V \to GF(p)$, then we let $f_{\mathbb{C}} \colon V \to \mathbb{C}$ be the function whose values are those of $f$ but regarded as integers (i.e., we select the congruence class residue representative in the interval $\{0, 1, \ldots, p-1\}$). We abuse notation and often write $f$ in place of $f_{\mathbb{C}}$.

**Definition 2.** When $g$ is a complex-valued function on $V$, we define the *Fourier transform* $g^\wedge \colon V \to \mathbb{Q}(\zeta)$ of $g$ as

$$g^\wedge(y) = \sum_{x \in V} g(x) \zeta^{-\langle x, y \rangle}. \tag{3}$$

If $f \colon V \to GF(p)$, we define the Fourier transform of $f$ to be the Fourier transform of $f_{\mathbb{C}}$.

Note that

$$f^\wedge(0) = \sum_{x \in V} f_{\mathbb{C}}(x)$$

and

$$W_f(y) = (\zeta^f)^\wedge(y).$$

We say $f$ is *even* if $f(x) = f(-x)$ for all $x \in GF(p)^n$. It is not hard to see that if $f$ is even then the Fourier transform of $f$ is real-valued. (However, this is not necessarily true of the Walsh transform.)

**Example 3.** It turns out that there are $3^4 = 81$ even functions $f \colon GF(3)^2 \to GF(3)$ such that $f(0) = 0$, of which exactly 18 are bent. Section 4.3 discusses this in more detail.

**Example 4.** It turns out that there are a total of $3^{13} = 1594323$ even functions $f\colon GF(3)^3 \to GF(3)$ such that $f(0) = 0$, of which exactly 2340 are bent. Section 4.4 discusses this in more detail.

**Example 5.** It turns out that there are a total of $5^{12} = 244140625$ even functions $f\colon GF(5)^2 \to GF(5)$ such that $f(0) = 0$, of which exactly 1420 are bent. Section 4.5 discusses this in more detail.

In the Boolean case, there is a nice simple relationship between the Fourier transform and the Walsh-Hadamard transform. In Equation (26) below, we shall try to connect these two transforms, (1) and (3), in the $GF(p)$ case, as well. In this context, it is worth noting that it is possible (see Proposition 7) to characterize a bent function in terms of the Fourier transform of its derivative.

**Definition 6.** Suppose $f\colon GF(p)^n \to GF(p)$ is bent. We say $f$ is *regular* if and only if $W_f(u)/p^{n/2}$ is a $p$th root of unity for all $u \in V = GF(p)^n$.

If $f$ is regular, then there is a function $f^*\colon GF(p)^n \to GF(p)$, called the *dual* (or *regular dual*) of $f$, such that $W_f(u) = \zeta^{f^*(u)}p^{n/2}$, for all $u \in V$. We call $f$ *weakly regular*[1], if there is a function $f^*\colon GF(p)^n \to GF(p)$, called the *dual* (or *$\mu$-regular dual*) of $f$, such that $W_f(u) = \mu\zeta^{f^*(u)}p^{n/2}$, for some constant $\mu \in \mathbb{C}$ with absolute value 1. These duals $f^*$ are described in more detail in Proposition 1 below.

Let $V = GF(p)^n$ and suppose $f\colon V \to GF(p)$ is bent. In this case, for each $u \in V$, the quotient $W_f(u)/p^{n/2}$ is, by definition, an element of the cyclotomic field $\mathbb{Q}(\zeta)$ having absolute value 1.

**Proposition 1.** *(Kumar, Scholtz, Welch) If $f$ is bent, then there are functions $f_*\colon GF(p)^n \to \mathbb{Z}$ and $f^*\colon GF(p)^n \to GF(p)$ such that*

$$W_f(u)p^{-n/2} = \begin{cases} (-1)^{f_*(u)}\zeta^{f^*(u)}, & \text{if } n \text{ is even, or } n \text{ is odd and } p \equiv 1 \bmod 4; \\ i^{f_*(u)}\zeta^{f^*(u)}, & \text{if } n \text{ is odd and } p \equiv 3 \bmod 4. \end{cases}$$

The above result is known (thanks to Kumar, Scholtz, and Welch [27]), but the form above is due to Helleseth and Kholosha [24] (although we made a minor correction to their statement). Also, note that [27, Property 8] established a more general fact than the statement above.

**Corollary 1.** *If $f$ is bent and $W_f(0)$ is rational (i.e., belongs to $\mathbb{Q}$), then $n$ must be even.*

The condition $W_f(0) \in \mathbb{Q}$ arises in Lemma 10 below, so this corollary will be useful later.

Below we give a necessary and sufficient condition to determine if $f$ is regular. The next lemmas are well-known but included for the reader's convenience.

[1] If $\mu$ is fixed and we want to be more precise, we call this *$\mu$-regular*.

**Lemma 1.** *If $f\colon V \to GF(p)$ is bent, then the following conditions are equivalent:*

*(a) The function $f$ is weakly regular.*

*(b) The quotient $W_f(u)/W_f(0)$ is a $p$-th root of unity for all $u \in V$.*

**Lemma 2.** *If $f\colon V \to GF(p)$ is bent and weakly regular, then the following conditions are equivalent:*

*(a) The function $f$ is regular.*

*(b) The quotient $W_f(0)/p^{n/2}$ is a $p$-th root of unity.*

**Lemma 3.** *Suppose that $f$ is bent and weakly regular, with $\mu$-regular dual $f^*$. Then $f^*$ is bent and weakly regular, with $\mu^{-1}$-regular dual $f^{**}$ given by $f^{**}(x) = f(-x)$. If $f$ is also even, then $f^*$ is even and $f^{**} = f$.*

## 2. Combinatorial Background

In this section, we introduce the notion of a partial difference set and its weighted analogue, and the related notion of an association scheme and algebraic variants: the Schur ring and the Bose-Mesner algebra. Amorphic association schemes are defined. Also, we recall the relationship between partial difference sets and bent functions in the Boolean case.

Dillon's thesis [15] was one of the first publications to discuss the relationship between bent functions and combinatorial structures, such as difference sets. His work concentrated on the Boolean case. In Dillon's work, it was proven that the "level curve" $f^{-1}(1)$ gives rise to a difference set in $GF(2)^n$. A more precise statement is given below (Theorem 11).

In this paper, we consider $p$-ary functions $f\colon GF(p)^n \to GF(p)$ (where $p$ is a prime), and try to obtain analogues of Dillon's Theorem for the "level curves" $f^{-1}(a)$ in $GF(p)^n$ (where $a \in GF(p)$, $a \neq 0$).

### 2.1. Partial Difference Sets

We recall some well-known definitions and some generalizations.

**Definition 7.** Let $G$ be a finite abelian multiplicative group of order $v$, and let $D$ be a subset of $G$ of order $k$. The set $D$ is a $(v, k, \lambda)$-*difference set* (DS) if the list of differences $d_1 d_2^{-1}$, where $d_1, d_2 \in D$, represents every non-identity element in $G$ exactly $\lambda$ times. The set $D$ is a $(v, k, \lambda, \mu)$-*partial difference set* (PDS) if the list of differences $d_1 d_2^{-1}$, where $d_1, d_2 \in D$, represents every non-identity element in $D$ exactly $\lambda$ times and every non-identity element in $G \setminus D$ exactly $\mu$ times.

We sometimes refer to the pair $(G, D)$ as a DS or PDS.

**Definition 8.** A PDS $(G, D)$ is of *Latin square type* (respectively, *negative Latin square type*) if there exist $N > 0$ and $R > 0$ (respectively, $N < 0$ and $R < 0$) such that

$$(v, k, \lambda, \mu) = (N^2, R(N-1), N + R^2 - 3R, R^2 - R).$$

**Example 9.** Consider the finite field $GF(9)$, represented as

$$GF(3)[x]/(x^2+1) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

The set of non-zero quadratic residues is given by $D = \{1, 2, x, 2x\}$. One can show that $D$ is a PDS with parameters $v = 9$, $k = 4$, $\lambda = 1$, $\mu = 2$. This example is of Latin square type ($N = 3$ and $R = 2$) and of negative Latin square type ($N = -3$ and $R = -1$).

We shall return to this example with more details below (see Example 14).

**Definition 10.** A *Hadamard difference set* is one whose parameters are of the form $(4m^2, 2m^2 - m, m^2 - m)$, for some $m \in \mathbb{Z}$. It is, in addition, *elementary* if $G$ is an elementary abelian 2-group (i.e., isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $k$).

The following result is well-known.

**Theorem 11.** *(Dillon Correspondence. [15, Theorem 6.2.10, p. 78]) The function $f\colon GF(2)^n \to GF(2)$ is bent if and only if $f^{-1}(1)$ is an elementary Hadamard difference set of $GF(2)^n$.*

Two (naive) analogues of this are formalized below (see Analogue 45 and Analogue 46).

Let $D^{-1} = \{d^{-1} \mid d \in D\}$.

**Lemma 4.** *Let $G$ be a finite abelian multiplicative group of order $v$, and let $D$ be a subset of $G$ of order $k$ such that $(G, D)$ is a partial difference set.*

*(a) If $\lambda = \mu$, then $(G, D)$ is also a $(v, k, \lambda)$-difference set.*

*(b) If $\lambda \neq \mu$, then $D = D^{-1}$.*

*Proof.* Part (a) follows directly from the definitions. Part (b) is Proposition 1 in Polhill's article [29]. □

**Definition 12.** Let $G$ be a finite abelian multiplicative group of order $v$, and let $D$ be a subset of $G$ such that $1 \notin D$. Let

$$D = D_1 \cup \cdots \cup D_r, \tag{4}$$

be a decomposition of $D$ into a union of disjoint subsets, let $k_i = |D_i|$, and let $k = (k_1, \ldots, k_r)$. We say $D$ is a *weighted $(v, k, \lambda, \mu)$-PDS* if there exist constants $\lambda \in \mathbb{Z}^{3r}$ and $\mu \in \mathbb{Z}^{2r}$ such that the following conditions hold:

(a) The list of "differences"

$$D_iD_j^{-1} = \{d_1d_2^{-1} \mid d_1 \in D_i, d_2 \in D_j\}$$

represents every non-identity element of $D_\ell$ exactly $\lambda_{i,j,\ell}$ times and every non-identity element of $G \setminus D$ exactly $\mu_{i,j}$ times (where $1 \le i, j, \ell \le r$).

(b) For each $i$ there is a $j$ such that $D_i^{-1} = D_j$ (and if $D_i^{-1} = D_i$ for all $i$, then we say the weighted PDS is *symmetric*).

We sometimes refer to the pair $(G, D)$ or the tuple $(G, D_1, D_2, \dots, D_r)$ as a weighted PDS. In addition, we sometimes define $D_0 = \{1\}$ and $D_{r+1} = G\backslash(D \cup D_0)$.

**Remark 13.** If $D = D_1 \cup \cdots \cup D_r$ is a symmetric weighted PDS, then $\mu_{i,j} = \mu_{j,i}$ and $\lambda_{i,j,\ell} = \lambda_{j,i,\ell}$.

How does the above notion of a weighted PDS relate to the usual notion of a PDS?

**Lemma 5.** *Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$. Let $(G, D)$, where $D = D_1 \cup \cdots \cup D_r$ (disjoint union) is as in Equation (4), be a symmetric weighted PDS with parameters $(v, (k_i), (\lambda_{i,j,\ell}), (\mu_{i,j}))$.*

*(a) If*

$$\sum_{i,j} \lambda_{i,j,\ell}$$

*does not depend on $\ell$, for $1 \le \ell \le r$, then $D$ is also an unweighted PDS with parameters $(v, k, \lambda, \mu)$, where*

$$k = \sum_i k_i, \qquad \lambda = \sum_{i,j} \lambda_{i,j,\ell}, \qquad \mu = \sum_{i,j} \mu_{i,j}.$$

*(b) If*

$$\lambda_{i,i,\ell} = \mu_{i,i}$$

*for all $\ell \neq i$, then $D_i$ is an unweighted PDS with parameters $(v, k, \lambda, \mu)$, where*

$$k = k_i, \quad \lambda = \lambda_{i,i,i}, \quad \mu = \mu_{i,i}.$$

The proof follows directly from the definitions.

In Proposition 13 we give an example in which level curves $D_1 = f^{-1}(1)$ and $D_2 = f^{-1}(2)$ of a bent function $f\colon GF(3)^3 \to GF(3)$ give a weighted PDS but $D = D_1 \cup D_2$ is not an unweighted PDS (see Example 60 and Theorem 22).

**Example 14.** Consider the finite field of Example 9,

$$GF(9) = GF(3)[x]/(x^2+1).$$

Recall that the set of non-zero quadratic residues is given by $D = \{1, 2, x, 2x\}$ and that $D$ is a PDS. Note that, by our convention of writing multiplicative operations additively,

$$D^{-1} = \{1^{-1}, 2^{-1}, x^{-1}, (2x)^{-1}\} = \{-1, -2, -x, -2x\} = \{2, 1, 2x, x\} = D.$$

Let $D_1 = \{1, 2\}$ and $D_2 = \{x, 2x\}$. These define a symmetric weighted PDS. Indeed, in the additive notation,

$$D_1D_1^{-1} = \{d_1 - d_2 \mid d_1 \in D_1, d_2 \in D_1\} = \{0, 1, 2\},$$

$$D_1D_2^{-1} = \{d_1 - d_2 \mid d_1 \in D_1, d_2 \in D_2\} = \{x+1, x+2, 2x+1, 2x+2\} = D_2D_1^{-1},$$
$$D_2D_2^{-1} = \{d_1 - d_2 \mid d_1 \in D_2, d_2 \in D_2\} = \{0, x, 2x\}.$$

Therefore, the symmetric weighted PDS has the following parameters:

$$k_1 = 2,\ k_2 = 2,$$

$$\lambda_{1,1,1} = 1,\ \lambda_{1,1,2} = 0,\ \lambda_{1,2,1} = 0,\ \lambda_{1,2,2} = 0,$$

$$\lambda_{2,1,1} = 0,\ \lambda_{2,1,2} = 0,\ \lambda_{2,2,1} = 0,\ \lambda_{2,2,2} = 1,$$

$$\mu_{1,1} = 0,\ \mu_{1,2} = 1,\ \mu_{2,1} = 1,\ \mu_{2,2} = 0.$$

### 2.2. Association Schemes

The following definition is standard, but we give [30] as a reference.

**Definition 15.** Let $S$ be a finite set, and let $R_0, R_1, \ldots, R_s$ denote binary relations on $S$ (subsets of $S \times S$). The *dual* of a relation $R$ is the set

$$R^* = \{(x, y) \in S \times S \mid (y, x) \in R\}.$$

Assume $R_0 = \Delta_S$, where $\Delta_S = \{(x, x) \in S \times S \mid x \in S\}$. We say $(S, R_0, R_1, \ldots, R_s)$ is an *$s$-class association scheme on $S$* if the following conditions hold:

(a) We have a disjoint union, i.e.,

$$S \times S = R_0 \cup R_1 \cup \cdots \cup R_s, \text{ with } R_i \cap R_j = \emptyset \text{ for all } i \neq j. \tag{5}$$

(b) For each $i$ there is a $j$ such that $R_i^* = R_j$ (and if $R_i^* = R_i$ for all $i$, then we say the association scheme is *symmetric*).

(c) For each $i, j, k$ and for all $(x, y) \in R_k$, define

$$p_{ij}^k(x, y) = |\{z \in S \mid (x, z) \in R_i, (z, y) \in R_j\}|.$$

For each $i, j, k$, the integer $p_{ij}^k(x, y)$ is a constant (independent of $x$ and $y$), denoted $p_{ij}^k$.

These constants $p_{ij}^k$ are called the *intersection numbers* or *parameters* or *structure constants* of the association scheme.

Next, we recall (see Herman [25]) the matrix-theoretic version of this definition. Let $M_{m\times n}(\mathbb{Z})$ denote the set of $m \times n$ matrices with integer entries.

**Definition 16.** Let $(S, R_0, \dots, R_s)$ denote a tuple consisting of a finite abelian multiplicative group $S$ of order $N$, with relations $R_i$ for which we have a disjoint union as in Equation (5). Let $A_i \in M_{N\times N}(\mathbb{Z})$ denote the adjacency matrix of $R_i$, for $i = 0, 1, \dots, s$. We say that the subring of $\mathbb{Z}[M_{N\times N}(\mathbb{Z})]$ generated by the the set of matrices $\{A_i\}_{i=0,1,\dots,s}$ is an *adjacency ring* (also called the *Bose-Mesner algebra*) provided the set of adjacency matrices satisfies the following conditions:

(a) For each integer $i \in \{0, 1, 2, \dots, s\}$, $A_i$ is a $(0, 1)$-matrix.

(b) The identity $\sum_{i=0}^{s} A_i = J$ (where $J$ is the all 1's matrix) holds.

(c) For each integer $i \in \{0, 1, 2, \dots, s\}$, ${}^tA_i = A_j$ holds true, for some integer $j \in \{0, 1, 2, \dots, s\}$ (where ${}^tA_i$ denotes the transpose of the matrix $A_i$).

(d) There is a subset $K \subset \{0, 1, 2, \dots, s\}$ such that $\sum_{k\in K} A_k = I$.

(e) There is a set of non-negative integers $\{p_{ij}^k \mid i, j, k \in \{0, 1, 2, \dots, s\}\}$ (structure constants) such that

$$A_iA_j = \sum_{k=0}^{s} p_{ij}^k A_k, \tag{6}$$

for all $i, j \in \{0, 1, 2, \dots, s\}$.

In our examples, the subset $K$ will simply be $K = \{0\}$.

We will see (see Corollary 2) that the weight-specific adjacency matrices of an edge-weighted Cayley graph corresponding to a symmetric weighted PDS form a Bose-Mesner algebra.

Let us consider the "Schur ring," which naturally gives rise to an association scheme.

For the following definition, we identify any subset $S$ of a finite group $G$ with the formal sum of its elements in the group ring

$$\mathbb{C}[G] = \{\sum_{g\in G} c_g \cdot g \mid c_g \in \mathbb{C}\},$$

where addition is "componentwise" and multiplication is that induced by the multiplicative[2] structure of $G$. Whenever convenient, we identify a subset $S \subset G$ with the corresponding formal sum in $\mathbb{C}[G]$:

$$S \mapsto \sum_{g \in S} g \in \mathbb{C}[G]. \tag{7}$$

For instance, from Example 14, we compute, using the "multiplicative convention," that

$$\begin{aligned} D^{-1} &= \{1^{-1}, 2^{-1}, x^{-1}, (2x)^{-1}\} \\ &\mapsto 1^{-1} + 2^{-1} + x^{-1} + (2x)^{-1} \\ &= 2 + 1 + 2x + x \\ &\mapsto \{1, 2, x, 2x\} = D. \end{aligned}$$

**Definition 17.** Let $G$ be a finite abelian group, and let $C_0, C_1, \ldots, C_s$ denote finite subsets of G. Assume that $C_0 = \{1\}$ is the singleton containing the identity. The subalgebra $\mathcal{A}$ of $\mathbb{C}[G]$ generated by $C_0, C_1, \ldots, C_s$ is called a *Schur ring* over $G$ if the following conditions hold:

(a) We have a disjoint union, i.e.,

$$G = C_0 \cup C_1 \cup \cdots \cup C_s, \text{ with } C_i \cap C_j = \emptyset \text{ for all } i \neq j.$$

(b) For each $i$ there is a $j$ such that $C_i^{-1} = C_j$.

(c) For all $i, j$, we have

$$C_i \cdot C_j = \sum_{k=0}^{s} \rho_{ij}^k C_k,$$

for some nonnegative integers $\rho_{ij}^k$ (the structure constants of the Schur ring).

We will sometimes denote the Schur ring $\mathcal{A}$ as $(G, C_0, \ldots, C_s)$ for convenience.

If $C_i^{-1} = C_i$ for all $i$, then we say the Schur ring is *symmetric.*

Note that, in the cases we are dealing with, the Schur ring is commutative, so $\rho_{ij}^k = \rho_{ji}^k$, for all $i, j, k$. Moreover, observe that if $(G, C_0, \ldots, C_s)$ is a Schur ring, then the binary relations

$$R_i = \{(g, h) \in G \times G \mid gh^{-1} \in C_i\},$$

for $0 \leq i, j \leq s$, give rise to an $s$-class association scheme.

[2] Note: even if $G$ is an additive group, for the purpose of computations in this group ring, we re-express it multiplicatively to avoid confusing it with the additive structure of $\mathbb{C}$.

**Remark 18.** Suppose that $G$ is a finite abelian multiplicative group of order $v$ and $D$ is a subset of order $k$ such that $1 \notin D$. Then $(G, D)$ is a $(v, k, \lambda, \mu)$-PDS if and only if the following identity holds in $\mathbb{C}[G]$ (see, e.g., [29]):

$$D \cdot D^{-1} = (k - \mu) \cdot 1 + (\lambda - \mu) \cdot D + \mu \cdot G, \tag{8}$$

where we have used correspondence (7) to identify $D$ and $D^{-1}$ as elements of $\mathbb{C}[G]$.

If $(G, D)$ is a $(v, k, \lambda, \mu)$-PDS with $1 \notin D$ and $D^{-1} = D$, and such that $D' = G \setminus (D \cup \{1\})$ is non-empty, we obtain from Equation (8) the well-known identity

$$k^2 - k = k\lambda + (v - k - 1)\mu. \tag{9}$$

The following result is well-known. A proof is given for the convenience of the reader.

**Lemma 6.** *Suppose that $G$ is a finite abelian multiplicative group of order $v$ and $D$ is a subset of order $k$ such that $1 \notin D$ and $D^{-1} = D$. Suppose also that $D' = G \setminus (D \cup \{1\})$ is not empty. Let*

$$R_0 = \Delta_G, \textit{ where } \Delta_G = \{(g, g) |\ g \in G\},$$

$$R_1 = \{(g, h) \in G \times G |\ gh^{-1} \in D\}, \textit{ and}$$

$$R_2 = \{(g, h) \in G \times G |\ gh^{-1} \notin D,\ g \neq h\}.$$

*Then $(G, D)$ is a PDS if and only if $(G, R_0, R_1, R_2)$ is a symmetric 2-class association scheme.*

*Proof.* Suppose that $(G, R_0, R_1, R_2)$ is a symmetric association scheme with intersection numbers $p_{ij}^{\ell}$. Regarding $D$ and $D^{-1}$ as elements of $\mathbb{C}[G]$, we have

$$D \cdot D^{-1} = D \cdot D = p_{11}^0 \cdot 1 + p_{11}^1 \cdot D + p_{11}^2 \cdot D'.$$

It follows that $(G, D)$ is a $(v, k, \lambda, \mu)$-PDS with $k = p_{11}^0$, $\lambda = p_{11}^1$, and $\mu = p_{11}^2$.

Conversely, suppose that $(G, D)$ is a $(v, k, \lambda, \mu)$-PDS. We first construct a Schur ring from the PDS.

Note that, by Equation (8) and the fact that $D = D^{-1}$, we have

$$D \cdot D = (k - \mu) \cdot 1 + (\lambda - \mu) \cdot D + \mu \cdot G.$$

By expanding out expressions for $D \cdot G$ in $\mathbb{C}[G]$, we obtain

$$D \cdot D' = (-k + \mu) \cdot 1 + (-1 - \lambda + \mu) \cdot D + (k - \mu) \cdot G,$$

or equivalently,

$$D \cdot D' = (k - 1 - \lambda) \cdot D + (k - \mu) D'.$$

Similarly, by expanding out expressions for $G \cdot D'$ in $\mathbb{C}[G]$, we obtain

$$D' \cdot D' = (k - \lambda - 1) \cdot 1 + (\mu - \lambda - 2) \cdot D' + (v - 2k + \lambda) \cdot G.$$

From this identity and Remark 18, we see that $D'$ is $(v, k', \lambda', \mu')$-PDS, where

$$\begin{aligned} k' &= v - k - 1, \\ \lambda' &= v - 2k - 2 + \mu, \text{ and} \\ \mu' &= v - 2k + \lambda. \end{aligned} \tag{10}$$

Furthermore, $(D')^{-1} = D'$ and $1 \notin D'$.

It follows that the PDS $(G, D)$ naturally yields an associated Schur ring, generated by $D$, $D'$, and $D_0 = \{1\}$ in $\mathbb{C}[G]$, and a corresponding 2-class association scheme with intersection numbers given by the following tables:

| $p^0_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | $k$ | 0 |
| 2 | 0 | 0 | $k'$ |

| $p^1_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 0 |
| 1 | 1 | $\lambda$ | $k-1-\lambda$ |
| 2 | 0 | $k-1-\lambda$ | $\mu'$ |

| $p^2_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 1 | 0 | $\mu$ | $k-\mu$ |
| 2 | 1 | $k-\mu$ | $\lambda'$ |

□

There is a weighted version of this result, i.e., a weighted symmetric PDS $(G, D)$ with $D = D_1 \cup \cdots \cup D_r$ (disjoint union) and $1 \notin D$ determines an $(r+1)$-class association scheme.

**Lemma 7.** *Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$. Suppose that $D$ is a disjoint union $D = D_1 \cup \cdots \cup D_r$, with $D_i^{-1} = D_i$ for all $i$. Let $D_0 = \{1\}$ and let $D_{r+1} = G \setminus (D \cup \{1\})$. Suppose that $D_{r+1}$ is not empty. For each $i$ with $0 \le i \le r+1$, let*

$$R_i = \{(g, h) \in G \times G |\ gh^{-1} \in D_i\}.$$

*Then $(G, D)$ is a symmetric weighted PDS if and only if $(G, R_0, R_1, \ldots, R_{r+1})$ is a symmetric association scheme of class $s = r + 1$.*

*Proof.* Suppose that $(G, D)$ is a symmetric weighted PDS. To show that it determines a Schur ring, we must show that structure constants exist, i.e., we must show that there are nonnegative integers $\rho^\ell_{ij}$ such that

$$D_i \cdot D_j = \sum_{\ell=0}^{r+1} \rho^\ell_{ij} D_\ell, \tag{11}$$

for $0 \le i, j \le r+1$. Symmetry of the Schur ring follows from symmetry of the weighted PDS.

Let $k_i = |D_i|$ for $0 \le i \le r+1$. Note that $(G, D)$ is a symmetric weighted PDS if and only if $D_i^{-1} = D_i$ for $1 \le i \le r$ and the following identity holds in $\mathbb{C}[G]$, for $1 \le i, j \le r$:

$$D_i \cdot D_j = \delta_{ij} k_i \cdot D_0 + \sum_{\ell=1}^{r} \lambda_{i,j,\ell} D_\ell + \mu_{i,j} D_{r+1} \tag{12}$$

(where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise). Note that identity (12) implies identity (11), provided that, for $0 \le i, j \le r+1$, we put $\rho_{ij}^0 = \delta_{ij} k_i$, for $1 \le i, j, \ell \le r$, we put $\rho_{ij}^\ell = \lambda_{i,j,\ell}$ and $\rho_{ij}^{r+1} = \mu_{i,j}$. Furthermore, since $D_0 \cdot D_j = D_j \cdot D_0 = D_j$, for all $j$, identity (11) holds if we put $\rho_{0j}^\ell = \rho_{j0}^\ell = \delta_{j\ell}$ for $0 \le j, \ell \le r+1$.

By expanding out expressions for $D_i \cdot G$ and $D_{r+1} \cdot G$, it can be shown that

$$\rho_{i,r+1}^\ell = k_i - \delta_{i\ell} - \sum_{j=1}^{r} \lambda_{i,j,\ell}, \qquad \text{for } 1 \le i, \ell \le r,$$

$$\rho_{i,r+1}^{r+1} = k_i - \sum_{j=1}^{r} \mu_{i,j}, \qquad \text{for } 1 \le i \le r, \text{ and}$$

$$\rho_{r+1,r+1}^{r+1} = k_{r+1} - 1 - \sum_{i=1}^{r} k_i + \sum_{i=1}^{r} \sum_{j=1}^{r} \mu_{i,j}.$$

Also, $\rho_{ij}^\ell = \rho_{ji}^\ell$ for all $i$ and $j$, because $G$ is abelian.

In the converse direction, if $(G, R_0, R_1, \ldots, R_{r+1})$ is a symmetric association scheme, it follows immediately that $(G, D)$ is a symmetric weighted PDS whose parameters are related to the intersection numbers of the association scheme by the same relations as above. □

Consequently, if $f\colon GF(p)^n \to GF(p)$ is an even function with $f(0) = 0$, then saying that the level curves of $f$ give rise to a symmetric weighted PDS is equivalent to saying that the level curves determine a symmetric $p$-class association scheme. (See, e.g., Theorem 30 and Propositions 11, 13, and 14.) When we refer to the intersection numbers $p_{ij}^k$ of a symmetric weighted PDS, we mean the intersection numbers of the corresponding symmetric association scheme.

**Definition 19.** Suppose that $S$ is a finite set and $\{R_0, R_1, \ldots R_s\}$ is a collection of binary relations on $S$. A collection of binary relations $\{T_0, T_1, \ldots, T_u\}$ is called a *fusion* of $\{R_0, R_1, \ldots R_s\}$ if each $T_i$ is a union of elements of $\{R_0, R_1, \ldots R_s\}$.

An association scheme $(S, R_0, R_1, \ldots, R_s)$ is called *amorphic* if, for every fusion $\{T_0, T_1, \ldots, T_u\}$ of $\{R_0, R_1, \ldots, R_s\}$, $(S, T_0, T_1, \ldots, T_u)$ is also an association scheme.

A symmetric weighted PDS is called *amorphic* if the symmetric association scheme it determines is amorphic.

## 3. Cayley Graphs

In this section, we discuss edge-weighted Cayley graphs and their relationship with weighted PDSs. We recall results on graph decompositions and amorphic Cayley graphs. We also discuss possible generalizations of the Dillon and BCV correspondences, posing several open questions.

Let $G$ be a finite abelian multiplicative group, and let $D$ be a non-empty subset of $G$ such that $1 \notin D$.

**Definition 20.** The *Cayley graph* $\Gamma = \Gamma(G, D)$ *associated with* $(G, D)$ is a graph constructed as follows. Let the vertices of the graph be the elements of the group $G$. Two vertices $g_1$ and $g_2$ are connected by a directed edge if $g_2 = dg_1$ for some $d \in D$.

If there exist $d_1$ and $d_2$ in $D$ such $g_1 = d_1g_2$ and $g_2 = d_2g_1$, we say that the vertices $g_1$ and $g_2$ are connected by an undirected edge. (We must have $d_2 = d_1^{-1}$ in this case.) Suppose that $D = D^{-1}$. If $g_2 = dg_1$, then $g_1 = d^{-1}g_2$, so the Cayley graph $\Gamma(G, D)$ can naturally be regarded as an undirected graph in this case.

**Definition 21.** A connected (undirected) graph $\Gamma = (V, E)$ with vertex set $V$ and edge set $E$ is a $(v, k, \lambda, \mu)$-*strongly regular graph* (SRG) provided it has the following properties:

(a) The graph $\Gamma$ has $v$ vertices, and each vertex $g \in V$ is adjacent to $k$ other vertices, i.e., the degree of $g$ is $k$.

(b) Distinct vertices $g_1$ and $g_2$ have $\lambda$ common neighbors if $g_1$ and $g_2$ are neighbors, and $\mu$ common neighbors if $g_1$ and $g_2$ are not neighbors.

In the usual terminology/notation, such a graph is called an $SRG(v, k, \lambda, \mu)$.

The *neighborhood* of a vertex $g$ in a graph $\Gamma = (V, E)$ is the set

$$N(g) = \{g' \in V \mid (g, g') \text{ is an edge in } \Gamma\}.$$

The following result is well-known (see, e.g., [12]). The proof is included for convenience.

**Theorem 22.** *Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$. Then $D$ is a $(v, k, \lambda, \mu)$-PDS such that $D^{-1} = D$ if and only if the associated Cayley graph $\Gamma(G, D)$ is a $(v, k, \lambda, \mu)$-strongly regular undirected graph.*

*Proof.* Suppose $D$ is a $(v, k, \lambda, \mu)$-PDS such that $D = D^{-1}$. Then $\Gamma(G, D)$ has $v$ vertices. The set $D$ has $k$ elements, and each vertex $g$ of $\Gamma(G, D)$ has neighbors $dg$, where $d \in D$. Therefore, $\Gamma(G, D)$ is regular of degree $k$. Let $g_1$ and $g_2$ be distinct vertices in $\Gamma(G, D)$. Let $x$ be a vertex that is a common neighbor of $g_1$ and $g_2$, i.e., $x \in N(g_1) \cap N(g_2)$. Then $x = d_1g_1 = d_2g_2$ for some $d_1, d_2 \in D$, which implies that $d_1d_2^{-1} = g_1^{-1}g_2$. If $g_1^{-1}g_2 \in D$, then there are exactly $\lambda$ ordered pairs $(d_1, d_2)$ that satisfy the previous equation (by Definition 7). If $g_1^{-1}g_2 \notin D$, then $g_1^{-1}g_2 \in G \setminus (D \cup \{1\})$, so there are exactly $\mu$ ordered pairs $(d_1, d_2)$ that satisfy the equation. If $g_1^{-1}g_2 \in D$, then $g_2 = dg_1$ for some $d \in D$, so $g_1$ and $g_2$ are adjacent. By a similar argument, if $g_1^{-1}g_2 \in G \setminus (D \cup \{1\})$, then $g_1$ and $g_2$ are not adjacent. So $\Gamma(G, D)$ is a $(v, k, \lambda, \mu)$-strongly regular graph.

Conversely, suppose $\Gamma(G, D)$ is a $(v, k, \lambda, \mu)$-strongly regular undirected graph. Since $\Gamma(G, D)$ is undirected, for distinct vertices $g_1$ and $g_2$ there is an edge from $g_1$ to $g_2$ if and only if there is an edge from $g_2$ to $g_1$. By definition, $g_1$ and $g_2$ are connected by an edge if and only if $g_1 = dg_2$, for some $d \in D$. This means that $g_1 = d_1g_2$ if and only if $g_2 = d_2g_1$, for some $d_1, d_2 \in D$. This implies that $d_2 = d_1^{-1}$, so $D = D^{-1}$. Since $\Gamma(G, D)$ is $(v, k, \lambda, \mu)$-strongly regular, it is $k$-regular, so the order of $D$ is $k$. Let $x$ be a vertex in $\Gamma(G, D)$ such that $x \in N(g_1) \cap N(g_2)$. Then $x = d_1g_1 = d_2g_2$ for some $d_1, d_2 \in D$, which implies that $d_1d_2^{-1} = g_1^{-1}g_2$. If $g_1$ and $g_2$ are adjacent, then $g_1^{-1}g_2 \in D$, and there are exactly $\lambda$ ordered pairs $(d_1, d_2)$ that satisfy the previous equation. If $g_1$ and $g_2$ are not adjacent, then $g_1^{-1}g_2 \in G \setminus (D \cup \{1\})$, and there are exactly $\mu$ ordered pairs $(d_1, d_2)$ that satisfy the equation. Therefore, $D$ is a $(v, k, \lambda, \mu)$-PDS and $D = D^{-1}$. □

**Remark 23.** It is well-known that the complement of a $(v, k, \lambda, \mu)$-strongly regular graph is a $(v, v-k-1, v-2k-2+\mu, v-2k+\lambda)$-strongly regular graph. Combining this result with Theorem 22 gives another way to see that if $D$ is a symmetric PDS with $1 \notin D$, then $D' = G \setminus (D \cup \{1\})$ is also a symmetric PDS which does not contain 1.

There is a weighted analogue of the correspondence between PDSs and SRGs in Theorem 22. After defining edge-weighted strongly regular graphs and edge-weighted Cayley graphs, we will give a generalization of that theorem in Theorem 29 below.

**Definition 24.** Let $f$ be a $GF(p)$-valued function on $GF(p)^n$. The *Cayley graph of $f$* is defined to be the edge-weighted digraph $\Gamma_f = (V, E)$ whose vertex set is $V = GF(p)^n$ and whose set of edges is defined by

$$E = \{(u, v) \mid u, v \in GF(p)^n,\ f(u - v) \neq 0\},$$

where the edge $(u, v) \in E$ has weight $f(u - v)$. We routinely identify $GF(p)$ with $\{0, 1, \ldots, p-1\}$ when referring to the edge-weights of $\Gamma_f$.

If $f$ is even, then we can (and do) regard $\Gamma_f$ as a weighted undirected graph.

The support of a function $f\colon GF(p)^n \to GF(p)$ is defined to be the set

$$\mathrm{supp}(f) = \{v \in GF(p)^n \mid f(v) \neq 0\}.$$

**Theorem 25.** *(BCV correspondence, [1], [2], [3]) Suppose $f\colon GF(2)^n \to GF(2)$. The function $f$ is bent if and only if the Cayley graph of $f$ is a strongly regular graph having parameters $(2^n, k, \lambda, \lambda)$ for some $\lambda$, where $k = |\mathrm{supp}(f)|$.*

The (naive) analogue of this for $p > 2$ is formalized in Analogue 43.

**Example 26.** Let $f\colon GF(2)^4 \to GF(2)$ be given by

$$f(x_0, x_1, x_2, x_3) = x_0x_1 + x_2x_3.$$

The function $f$ is bent and $|\mathrm{supp}(f)| = 6$. Therefore, the Cayley graph is a strongly regular graph with parameters $v = 16$ and $k = 6$. By the classification of strongly regular graphs of small size (see Spence [31]), it must be the Shrikhande graph, which is $(16, 6, 2, 2)$-strongly regular.

Suppose that $\Gamma = (V, E)$ is any edge-weighted graph (without loops or multiple edges) whose edge weights are positive integers. We fix a labeling of the set of vertices $V(\Gamma)$, which we often identify with the set $\{0, 1, \ldots, N-1\}$, where $N = |V(\Gamma)|$. If $u$ and $v$ are vertices of $\Gamma$, then a *walk $P$ from $u$ to $v$ with weight sequence* $(w_0, w_1, \ldots, w_{k-1})$ is a sequence of edges $e_0 = (v_0, v_1) \in E$, $e_1 = (v_1, v_2) \in E$, $\ldots$, $e_{k-1} = (v_{k-1}, v_k) \in E$, where $v_0 = u$ and $v_k = v$, connecting $u$ to $v$, where edge $e_i$ has weight $w_i$. Let $A = (a_{ij})$ denote the $N \times N$ weighted adjacency matrix of $\Gamma$, where $i, j \in \{0, 1, \ldots, N-1\}$ and where

$$a_{ij} = \begin{cases} w, & \text{if } (i,j) \text{ is an edge of weight } w; \\ 0, & \text{if } (i,j) \text{ is not an edge of } \Gamma. \end{cases} \tag{13}$$

From the adjacency matrix $A$, we can derive weight-specific adjacency matrices as follows. For each weight $w$ of $\Gamma$, let $A_w = (a(w)_{ij})$ denote the $N \times N$ $(1,0)$-matrix defined by

$$a(w)_{ij} = \begin{cases} 1, & \text{if } (i,j) \text{ is an edge of weight } w; \\ 0, & \text{if } (i,j) \text{ is not an edge of weight } w. \end{cases} \tag{14}$$

When $\Gamma$ is the Cayley graph of a $GF(p)$-valued function, we identify the edge-weights with the integers $\{1, \ldots, p-1\}$. We extend the weight set by imposing the following conventions:

(a) If $u$ and $v$ are distinct vertices of $\Gamma$ but $(u, v)$ is not an edge of $\Gamma$, then we say the *weight* of $(u, v)$ is $w = p$.

(b) If $u = v$ is a vertex of $\Gamma$ (so $(u, v)$ is not an edge, since $\Gamma$ has no loops), then we say the *weight* of $(u, v)$ is $w = 0$.

This allows us to define the weight-specific adjacency matrices $A_p$ and $A_0$ as well, and we can (and do) extend the weight set of $\Gamma$ by appending $p$ and $0$. Clearly, these weight-specific adjacency matrices have disjoint supports: if $a(w)_{ij} \neq 0$, then $a(w')_{ij} = 0$ for all weights $w' \neq w$.

Note that an alternative convention, which can be used for more general edge-weighted graphs, is to extend the weight set by appending 0 (for case (a) above) and $-1$ (for case (b) above).

In Corollary 2, we will give conditions under which these weight-specific adjacency matrices form a Bose-Mesner algebra.

For the reader's convenience, the well-known matrix-walk theorem is formulated as in the result below (see, e.g., [19] for a proof in the unweighted case).

**Proposition 2.** *For any vertices $u$ and $v$ of $\Gamma$ and any sequence of non-zero edge weights $w_1, w_2, \ldots, w_k$, the $(u, v)$th entry of $A_{w_1} A_{w_2} \ldots A_{w_k}$ is equal to the number of walks of weight sequence $(w_1, w_2, \ldots, w_k)$ from $u$ to $v$. Moreover, the total number of closed walks of weight sequence $(w_1, w_2, \ldots, w_k)$ is equal to $\mathrm{tr}\,(A_{w_1} A_{w_2} \ldots A_{w_k})$.*

Let us return to describing the Cayley graph of Definition 24 above. We identify $\mathbb{Z}/p^n\mathbb{Z}$ with $\{0, 1, \ldots, p^n - 1\}$, and let

$$\eta \colon \mathbb{Z}/p^n\mathbb{Z} \to GF(p)^n \tag{15}$$

be the $p$-ary representation map. In other words, if we regard $x \in \mathbb{Z}/p^n\mathbb{Z}$ as a polynomial in $p$ of degree $\leq n - 1$, then $\eta(x)$ is the list of coefficients, arranged in order of decreasing degree. This is a bijection. (Actually, for our purposes, any bijection will do, but the $p$-ary representation is the most natural one.)

As the following lemma illustrates, it is very easy to characterize the Cayley graph of an even $p$-ary function in terms of its adjacency matrix.

**Lemma 8.** *Let $\Gamma$ be an undirected edge-weighted graph with weights in $GF(p)$ and with vertex set $V = GF(p)^n$ (and vertices labeled using the bijection given by the $p$-ary representation map of Equation 15). Let $A = (a_{ij})$ be the (symmetric) weighted adjacency matrix of $\Gamma$, where $i, j \in \{0, 1, \ldots, p^n - 1\}$. Let $f$ be an even $GF(p)$-valued function on $V$ with $f(0) = 0$. Then $\Gamma$ is the Cayley graph of $f$ if and only if $\Gamma$ is regular and the following conditions hold:*

*(a) For each $i \in \{0, 1, \ldots, p^n - 1\}$, $a_{i,0} = f(\eta(i))$.*

*(b) For each $i, j \in \{0, 1, \ldots, p^n - 1\}$, $a_{i,j} = a_{k,0}$, where $\eta(k) = \eta(i) - \eta(j)$.*

*Proof.* Let $w$ be an element of $GF(p)$. We know that $a_{i,j} = w$ if and only if there is an edge of weight $w$ from $\eta(i)$ to $\eta(j)$ if and only if $f(\eta(i) - \eta(j)) = w$. The lemma follows. □

Let $\Gamma$ be an edge-weighted graph with vertices $V$, edges $E$, and weight set $W$. Usually our weight set will be $GF(p)^\times = GF(p) \setminus \{0\}$, which we identify with

$\{1, \ldots, p-1\}$. Recall that we define

$$N(u) = \text{ the set of all neighbors } v \text{ of } u \text{ in } \Gamma.$$

For each $u \in V$ and $a \in W \cup \{0\}$, we define the weighted $a$-neighborhood of $u$, $N(u,a)$, as follows:

- $N(u,a) =$ the set of all neighbors $v$ of $u$ in $\Gamma$ for which the edge $(u,v) \in E$ has weight $a$ (for each $a \in W$).
- $N(u,0) =$ the set of all non-neighbors $v$ of $u$ in $\Gamma$ (i.e., the set of $v$ such that $(u,v) \notin E$). In particular, $u \in N(u,0)$.

Now suppose that $V = GF(p)^n$ and $f\colon V \to GF(p)$ is an even function with $f(0) = 0$. Let $\Gamma = \Gamma_f$ be the Cayley graph of $f$. Recall that the support of $f$ is defined to be

$$\text{supp}(f) = \{v \in V \mid f(v) \neq 0\}.$$

It is clear that $\text{supp}(f) = N(0)$ is the set of neighbors of the zero vector in $\Gamma$. More generally, for any $u \in V$,

$$N(u) = u + \text{supp}(f), \tag{16}$$

where the last set is the collection of all vectors $u + v$, for some $v \in \text{supp}(f)$.

Let $S_a = \{v \in V \mid f(v) = a\}$, for $a \in GF(p)$. We can extend Equation (16) to the following more precise statement describing the $a$-neighborhood of $u$:

$$N(u,a) = u + S_a. \tag{17}$$

We can restate the definition of a strongly regular graph, using neighborhood notation, as follows. A connected simple graph $\Gamma$ (without edge weights) is strongly regular if there are constants $(v, k, \lambda, \mu)$ such that $\Gamma$ has $v$ vertices, and for vertices $u_1$ and $u_2$ we have

$$|N(u_1) \cap N(u_2)| = \begin{cases} k, & \text{if } u_1 = u_2; \\ \lambda, & \text{if } u_1 \in N(u_2); \\ \mu, & \text{if } u_1 \notin N(u_2) \text{ and } u_1 \neq u_2. \end{cases}$$

The concept of strongly regular simple graphs generalizes to that of edge-weighted graphs.

**Definition 27.** 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 *edge-weighted strongly regular* 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 $\Gamma$ 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

$$|N(u,a)| = k_a \quad \text{for all vertices } u,$$

and for vertices $u_1 \neq u_2$ we have

$$|N(u_1, a_1) \cap N(u_2, a_2)| = \begin{cases} \lambda_{a_1,a_2,a_3}, & \text{if } u_1 \in N(u_2, a_3); \\ \mu_{a_1,a_2}, & \text{if } u_1 \notin N(u_2) \text{ and } u_1 \neq u_2. \end{cases} \tag{18}$$

In our examples, the weights will usually be in $GF(p)$, but will be routinely identified with integers. Thus we will treat the set of edge weights $W$ as a subset of $\mathbb{Z}$, and note that $k \in \mathbb{Z}^{|W|}$, $\lambda \in \mathbb{Z}^{|W^3|}$, and $\mu \in \mathbb{Z}^{|W^2|}$.

How does the above notion of an edge-weighted strongly regular graph relate to the usual notion of a strongly regular graph?

**Lemma 9.** *Let $\Gamma$ be an edge-weighted strongly regular graph as in Definition 27, with edge-weights $W$ and parameters $(v, (k_a), (\lambda_{a_1,a_2,a_3}), (\mu_{a_1,a_2}))$.*

*(a) If*

$$\sum_{(a_1,a_2)\in W^2} \lambda_{a_1,a_2,a_3}$$

*does not depend on $a_3$, for $a_3 \in W$, then $\Gamma$ is strongly regular (as an unweighted graph) with parameters $(v, k, \lambda, \mu)$, where*

$$k = \sum_{a\in W} k_a, \quad \lambda = \sum_{(a_1,a_2)\in W^2} \lambda_{a_1,a_2,a_3}, \quad \mu = \sum_{(a_1,a_2)\in W^2} \mu_{a_1,a_2}.$$

*(b) For each weight $a$, let $\Gamma_a$ be the graph with the same vertices as $\Gamma$, whose edges are the edges of weight $a$. If*

$$\lambda_{a,a,a_3} = \mu_{a,a}$$

*for all weights $a_3 \neq a$, then $\Gamma_a$ is strongly regular (as an unweighted graph) with parameters $(v, k, \lambda, \mu)$, where*

$$k = k_a, \quad \lambda = \lambda_{a,a,a}, \quad \mu = \mu_{a,a}.$$

The proof follows directly from the definitions.

**Definition 28.** Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$ and such that $D$ has a disjoint decomposition $D = D_1 \cup D_2 \cup \cdots \cup D_r$. The *edge-weighted Cayley graph $\Gamma = \Gamma(G, D)$ associated with* $(G, D)$ is the edge-weighted graph constructed as follows. Let the vertices of the graph be the elements of the group $G$. Two vertices $g_1$ and $g_2$ are connected by an edge of weight $i$ if $g_2 = dg_1$ for some $d \in D_i$. If $D_i^{-1} = D_i$ for all $i$, the graph $\Gamma$ is undirected.

We have the following generalization of Theorem 22.

**Theorem 29.** *Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$ and such that $D$ has a disjoint decomposition $D = D_1 \cup D_2 \cup \cdots \cup D_r$. Let $D_0 = \{1\}$, let $D_{r+1} = G \setminus (D \cup D_0)$, and let*

$$R_i = \{(g,h) \in G \times G| \; gh^{-1} \in D_i\}, \qquad 0 \le i \le r+1.$$

*The following statements are equivalent:*

*(a) The set $D$ is a symmetric weighted partial difference set.*

*(b) The graph $\Gamma(G,D)$ is an edge-weighted strongly regular graph with edge weights $\{1,2,\ldots,r\}$.*

*(c) The tuple $(G, R_0, R_1, \ldots, R_{r+1})$ is a symmetric association scheme of class $r+1$.*

*Proof.* The equivalence of $(a)$ and $(c)$ is just Lemma 7.

($(a) \implies (b)$) Suppose $(G,D)$ is a weighted partial difference set satisfying $D_i^{-1} = D_i$ for all $i$, and having parameters $(v,k,\lambda,\mu)$, where $v = |G|$, $k = \{k_i\}$ with $k_i = |D_i|$, $\lambda = \{\lambda_{i,j,\ell}\}$, and $\mu = \{\mu_{i,j}\}$. The graph $\Gamma = \Gamma(G,D)$ has $v = |G|$ vertices, by definition. Each vertex $g$ of $\Gamma$ has $k_i$ neighbors of weight $i$, namely, $dg$ where $d \in D_i$. Let $g_1$ and $g_2$ be distinct vertices in $\Gamma$. Let $x$ be a vertex which is a neighbor of each: $x \in N(g_1,i) \cap N(g_2,j)$. By definition, $x = d_1 g_1 = d_2 g_2$, for some $d_1 \in D_i$, $d_2 \in D_j$. Therefore, $d_1^{-1} d_2 = g_1 g_2^{-1}$. If $g_1 g_2^{-1} \in D_\ell$, for some $\ell \neq 0, r+1$, then there are $\lambda_{i,j,\ell}$ solutions, by definition of a weighted PDS. If $g_1 g_2^{-1} \in D_{r+1}$, then there are $\mu_{i,j}$ solutions, by definition of a weighted PDS.

($(b) \implies (a)$) For the remainder of the proof, note that the reasoning above is reversible. Details are left to the reader. □

We sometimes extend the weight set of $\Gamma = \Gamma(G,D)$ by imposing the following conventions:

(a) If $u$ and $v$ are distinct vertices of $\Gamma$ but $(u,v)$ is not an edge of $\Gamma$, then we say the *weight* of $(u,v)$ is $w = r+1$.

(b) If $u = v$ is a vertex of $\Gamma$ (so $(u,v)$ is not an edge, since $\Gamma$ has no loops), then we say the *weight* of $(u,v)$ is $w = 0$.

This allows us to extend the set of weight-specific adjacency matrices given by Equation (14) to the set $A_0, A_1, \ldots, A_r, A_{r+1}$.

**Corollary 2.** *The graph $\Gamma(G,D)$ is an edge-weighted strongly regular graph if and only if the (extended) set of weight-specific adjacency matrices given by Equation (14) form a Bose-Mesner algebra with $K = \{0\}$.*

*Proof.* The corollary is immediate from the definition of Bose-Mesner algebra (see Definition 16), since the weight-specific adjacency matrices of $\Gamma(G, D)$ coincide with the adjacency matrices of the binary relations $R_i$. □

Note that if a function $f\colon GF(p)^n \to GF(p)$ is even (i.e., $f(x) = f(-x)$), then its level curves $D_i = f^{-1}(i)$ satisfy $D_i^{-1} = D_i$ (as sets).

**Theorem 30.** *Let $f\colon GF(p)^n \to GF(p)$ be an even function such that $f(0) = 0$. Let $G = GF(p)^n$, and let $D_i = f^{-1}(i)$, for $i = 1, 2, \dots, p-1$ If $(G, D_1, D_2, \dots, D_{p-1})$ is a symmetric weighted partial difference set, then the associated edge-weighted strongly regular graph is the edge-weighted Cayley graph of $f$.*

The proof is straightforward and left to the reader.

**Remark 31.** Roughly speaking, this theorem says that "if the level curves of $f$ form a symmetric weighted PDS, then the edge-weighted Cayley graph corresponding to $f$ agrees with the edge-weighted strongly regular graph associated with the symmetric weighted PDS."

**Definition 32.** A *graph decomposition* of an edge-weighted graph $\Gamma$, for this paper, means the graph decomposition determined by the collection $\{\Gamma_a\}$, where for each weight $a$, we define $\Gamma_a$ to be the graph with the same vertices as $\Gamma$, whose edges are the edges of weight $a$. There is a corresponding graph decomposition of the complete graph on the vertex set of $\Gamma$, consisting of the graphs $\Gamma_a$ and the complement of $\Gamma$. A graph decomposition is said to be a *strongly regular graph decomposition* (see [34]) if the individual graphs of the decomposition are all strongly regular.

**Definition 33.** Let $\Gamma = \Gamma(G, D)$ be the edge-weighted Cayley graph associated with a symmetric weighted PDS. We say that $\Gamma$ is *amorphic* if $(G, D)$ is amorphic, i.e., if the association scheme determined by $(G, D)$ is amorphic. If $f\colon GF(p)^n \to GF(p)$ is an even function with $f(0) = 0$, then we call $f$ *amorphic* if its associated Cayley graph is edge-weighted strongly regular and amorphic.

Note that if $\Gamma(G, D)$ is amorphic, then it determines a strongly regular graph decomposition (see [34]).

The following proposition is a consequence of a theorem from [20] on amorphic association schemes (which we quote from van Dam and Muzychuk [35]).

**Proposition 3.** *(Gol'fand, Ivanov, Klin) Let $\Gamma = \Gamma(G, D)$ be the edge-weighted Cayley graph associated with a symmetric weighted PDS. Suppose that the corresponding graph decomposition of the complete graph on the vertices of $\Gamma$ consists of at least 3 (nonempty) graphs. If $\Gamma$ is amorphic, then either all the graphs of the decomposition are of Latin square type, or all the graphs of the decomposition are of negative Latin square type.*

The following result is a consequence of a theorem of van Dam [34, Theorem 3].

**Proposition 4.** *(van Dam) Let $f\colon GF(p)^n \to GF(p)$ be an even bent function with $f(0) = 0$. If the decomposition of the edge-weighted Cayley graph of $f$ and its complement form a strongly regular graph decomposition of the complete graph, such that the individual graphs are all of Latin square type or all of negative Latin square type, then $f$ is an amorphic bent function.*

We will use this result in Proposition 11 and Example 65, where we give examples of even bent functions with $f(0) = 0$ whose Cayley graphs are amorphic. In Section 4.2, we see how these examples fit into a more general framework. We use van Dam's result in Corollary 7 in the construction of a family of amorphic bent functions $f\colon GF(p)^2 \to GF(p)$ that are homogeneous of degree $p - 1$ and weakly regular.

Recall that the weighted adjacency matrix $A$ of the Cayley graph $\Gamma_f$ of an even function $f\colon GF(p)^n \to GF(p)$ is the matrix whose entries are

$$A_{i,j} = f(\eta(i) - \eta(j)),$$

where $\eta(k)$ is the $p$-ary representation as in Equation (15) (and where, as usual, we identify $GF(p)$ with $\{0, 1, \ldots, p-1\}$ when referring to the edge weights of $\Gamma_f$). Note that $\Gamma_f$ is a regular graph (each vertex has the same degree) of degree $wt(f)$, that is, the Hamming weight of $f$ (when $f$ is regarded as a vector of integer values of length $p^n$). Let

$$\omega = \omega_f = wt(f)$$

denote the cardinality of $\mathrm{supp}(f) = \{v \in GF(p)^n \mid f(v) \neq 0\}$. Note that $f^\wedge(0) \geq |\mathrm{supp}(f)|$.

If $A$ is the adjacency matrix of a simple, unweighted, strongly regular graph having parameters $(v, k, \lambda, \mu)$, then

$$A^2 = kI + \lambda A + \mu(J - I - A), \tag{19}$$

where $J$ is the all 1s matrix and $I$ is the identity matrix. This is well-known and relatively easy to verify, by simply computing $(A^2)_{ij}$ in the three separate cases (a) $i = j$, (b) $i \neq j$ and $i, j$ adjacent, (c) $i \neq j$ and $i, j$ non-adjacent[3]. Compare also to Equation (8) for partial difference sets.

Let $G$ be a finite abelian multiplicative group, and let $D$ be a subset of $G$ such that $1 \notin D$ and such that $D$ has a disjoint decomposition $D = D_1 \cup D_2 \cup \cdots \cup D_r$. Let $D_0 = \{1\}$, and let $D_{r+1} = G \setminus (D \cup D_0)$. Suppose that $\Gamma = \Gamma(G, D)$ is an edge-weighted strongly regular graph having weight set $W = \{1, 2, \ldots, r\}$ and parameters $(v, k_i, \lambda_{i,j,\ell}, \mu_{i,j})$ for $i, j, \ell \in W$. For $i \in W \cup \{0, r+1\}$, let $A_i$ be the $i$th weight-specific adjacency matrix of $\Gamma$ (see Equation (14) and the remarks preceding Corollary 2). By Corollary 2, the collection of matrices $\{A_i\}_{i \in W} \cup \{A_0, A_{r+1}\}$

[3] It can also be proven by character-theoretic methods, but this method seems harder to generalize to the edge-weighted case.

forms a Bose-Mesner algebra (with $K = \{0\}$). Note that $A_{r+1} = J - I - \sum_{i \in W} A_i$. For $i, j \in W$, we have the following equation, corresponding to Equation (12) for symmetric weighted partial difference sets:

$$A_i \cdot A_j = \delta_{ij} k_i \cdot I + \sum_{\ell=1}^{r} \lambda_{i,j,\ell} A_\ell + \mu_{i,j} A_{r+1}. \tag{20}$$

In fact the matrices, when appropriately reindexed, satisfy Equation (6) from the definition of a Bose-Mesner algebra, where the constants $p_{ij}^{\ell}$ are related to the parameters of the edge-weighted graph as in the proof of Lemma 7.

**Definition 34.** We call a map $g\colon GF(p)^n \to GF(p)$ *balanced* if the cardinalities $|g^{-1}(x)|$ (for $x \in GF(p)$) do not depend on $x$. We say that $g$ is *balanced on the support of* $g$ if the cardinalities $|g^{-1}(x)|$ $(x \neq 0)$ do not depend on $x$.

**Definition 35.** We call the *signature* of $f\colon GF(p)^n \to GF(p)$ the list

$$|S_1|,\ |S_2|, \ldots, |S_{p-1}|,$$

where, for each $i$ in $GF(p)$,

$$S_i = \{x \mid f(x) = i\}. \tag{21}$$

In the notation of Theorem 30, $S_i = D_i$, for $1 \leq i \leq p-1$, and $S_0 = D_0 \cup D_p$.

Note that

$$W_f(0) = |S_0| + |S_1|\zeta + \cdots + |S_{p-1}|\zeta^{p-1},$$

(where $\zeta = e^{2\pi i/p}$) which we can regard as an identity in the $(p-1)$-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta)$. The relation

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$$

gives

$$W_f(0) - |S_0| + |S_1| = (|S_2| - |S_1|)\zeta^2 + \cdots + (|S_{p-1}| - |S_1|)\zeta^{p-1}.$$

We have proven the following result.

**Lemma 10.** *If $f\colon GF(p)^n \to GF(p)$ has the property that $W_f(0)$ is a rational number, then*

$$|S_1| = |S_2| = \cdots = |S_{p-1}|,$$

*($f$ is balanced on the support of $f$) and*

$$W_f(0) = |S_0| - |S_1|.$$

*In particular,*

$$\begin{aligned} |\mathrm{supp}(f)| &= |S_1| + |S_2| + \cdots + |S_{p-1}| \\ &= (p-1)|S_1| = (p-1)(|S_0| - W_f(0)). \end{aligned}$$

**Remark 36.** See Proposition 1 and its corollary for more information on the condition "$W_f(0)$ is rational." It is also known that if $n$ is even and $f$ is bent, then $f$ is balanced on its support, i.e.,

$$|S_1| = |S_2| = \cdots = |S_{p-1}|.$$

We have more to say about these sets later. See Proposition 11 for $p = 3$ and $n = 2$, and Section 4.5 for $p = 5$ and $n = 2$.

For any graph $\Gamma = (V, E)$, let $\mathrm{dist}\colon V \times V \to \mathbb{Z} \cup \{\infty\}$ denote the distance function. In other words, for any $v_1, v_2 \in V$, $\mathrm{dist}(v_1, v_2)$ is the length (i.e., number of edges) of the shortest path from $v_1$ to $v_2$ (if it exists) and $\infty$ (if it does not). The diameter of $\Gamma$, denoted $\mathrm{diam}(\Gamma)$, is the maximum value (possibly $\infty$) of this distance function.

For any $v \in V$, and any $k \geq 0$, let

$$\Gamma_k(v) = \{u \in V \mid \mathrm{dist}(u, v) = k\}.$$

For example, let $f\colon GF(p)^n \to GF(p)$ be any even function, and let $\Gamma$ be the (unweighted) Cayley graph of $f$. Suppose that $\Gamma$ is connected. It follows from the definitions that, if $v \in GF(p)^n$ is arbitrary, then

$$\Gamma_k(v) = v + \Gamma_k(0).$$

**Lemma 11.** *If $f\colon GF(p)^n \to GF(p)$ is any even function, and if the (unweighted) Cayley graph of $f$ is connected, then*

$$\Gamma_k(0) = \{v \in GF(p)^n \mid v \text{ is the sum of } k \text{ support vectors of } f, \text{ and no fewer}\}.$$

*Proof.* We will prove the lemma by induction on $k$. The statement for $k = 1$ is obvious, since $\Gamma_1(0) = \mathrm{supp}(f)$. Assume the statement is true for $k$. We prove it for $k + 1$. Let $v' \in \Gamma_{k+1}(0)$, so $\mathrm{dist}(0, v') = k + 1$. There is a $v'' \in \Gamma_k(0)$ such that $v' = v'' + v'''$, for some $v''' \in \mathrm{supp}(f)$. By the inductive hypothesis, $v''$ can be written as the sum of $k$ support vectors, so $v'$ is the sum of $k + 1$ vectors. □

**Definition 37.** Let $\Gamma = (V, E)$ be a graph, let $\mathrm{dist}\colon V \times V \to \mathbb{Z}$ denote the distance function, and let $G = \mathrm{Aut}(\Gamma)$ denote the automorphism group of $\Gamma$. We say the graph $\Gamma$ is *distance transitive* if, for any $k \geq 0$, and any $(u_1, v_1) \in V \times V$ and $(u_2, v_2) \in V \times V$ with $\mathrm{dist}(u_i, v_i) = k$ (for $i = 1, 2$), there is a $g \in G$ such that $g(u_2) = v_2$ and $g(u_1) = v_1$.

**Remark 38.** The following "conjecture" is false: If $f\colon GF(p)^n \to GF(p)$ is any even bent function, then the (unweighted) Cayley graph of $f$ is distance transitive. In fact, this fails when $p = 2$ for any bent function of 4 variables having support of size 6. Indeed, in this case the Cayley graph of $f$ is isomorphic to the Shrikhande graph (with strongly regular parameters $(16, 6, 2, 2)$), which is not distance-transitive (see [5, pp. 104-105, 136]).

Let $\Gamma = (V, E)$ be a graph. For any subset $S \subset V$ and any $u \in V$, let $N_u(S)$ denote the subset of all $s \in S$ which are neighbors of $u$, i.e., let

$$N_u(S) = S \cap \Gamma_1(u).$$

**Definition 39.** We say a graph $\Gamma = (V, E)$ is *distance regular* if, for each $k \geq 0$ and any $(v_1, v_2) \in V \times V$ with $\text{dist}(v_1, v_2) = k$, the numbers

$$a_k = |N_{v_1}(\Gamma_k(v_2))|,$$

$$b_k = |N_{v_1}(\Gamma_{k+1}(v_2))|, \text{ and}$$

$$c_k = |N_{v_1}(\Gamma_{k-1}(v_2))|$$

are independent of $v_1$ and $v_2$.

**Remark 40.** The following "conjecture" is false: If $f \colon GF(p)^n \to GF(p)$ is any even bent function then the (unweighted) Cayley graph of $f$ is distance regular. In fact, it can by verified by computer that this fails for every even bent function $f \colon GF(3)^3 \to GF(3)$ with $f(0) = 0$, using the classification of all such functions in 4.4. However, our computer calculations lead us to the following conjecture.

**Conjecture 1.** Suppose that $f$ is an amorphic even bent function with $f(0) = 0$ of the type described in Theorem 56. Then the Cayley graph of $f$ is distance regular.

### 3.1. Cayley Graphs of Bent Functions

**Remark 41.** In Chee, Tan, and Zhang [12], it is shown that if $n$ is even, then the unweighted Cayley graphs of homogeneous[4] weakly regular even bent functions $f \colon GF(p)^n \to GF(p)$, with $f(0) = 0$, are strongly regular.

**Problem 42.** Some natural problems arise. For $f$ even,

1. find necessary and sufficient conditions for $\Gamma_f$ to be strongly regular;

2. find necessary and sufficient conditions for $\Gamma_f$ to be connected (and more generally find a formula for the number of connected components of $\Gamma_f$);

3. classify the spectrum of $\Gamma_f$ in terms of the values of the Fourier transform of $f$; and

4. in general, which graph-theoretic properties of $\Gamma_f$ can be tied to function-theoretic properties of $f$?

[4] When regarded as a function $f \colon GF(p^n) \to GF(p)$.

Parts 2 and 3 of Problem 42 are addressed below (see Lemma 12 and Section 3.3).

Regarding the BCV correspondence (Theorem 25), the following would be a graph-theoretical analogue, but is, unfortunately, not true in general!

**Analogue 43.** We ask under what additional hypotheses the following analogue of the Bernasconi correspondence is true:

Assume $n$ is even. If $f\colon GF(p)^n \to GF(p)$ is even and bent then, for each $a \in GF(p)^\times$, we have

(a) if $u_1, u_2 \in V$ are $a_3$-neighbors in the Cayley graph of $f$, then $|N(u_1, a_1) \cap N(u_2, a_2)|$ does not depend on $u_1, u_2$ (with a given edge-weight), for each $a_1, a_2, a_3 \in GF(p)^\times$; and

(b) if $u_1, u_2 \in V$ are distinct and not neighbors in the Cayley graph of $f$, then $|N(u_1, a_1) \cap N(u_2, a_2)|$ does not depend on $u_1, u_2$, for each $a_1, a_2 \in GF(p)^\times$.

In other words, the associated Cayley graphs is edge-weighted strongly regular as in Definition 27.

**Remark 44.**

1. This analogy fails when $p = 5$. (See Proposition 14.)
2. This analogy fails even if you replace "$f\colon GF(p)^n \to GF(p)$ is even and bent" in the hypothesis by "$f\colon GF(p)^n \to GF(p)$ is even, bent, and regular." (Again, see Proposition 14.) However, when $p = 3$ and $n = 2$, see Lemma 17(a).
3. In general, this analogy fails if you replace "$f\colon GF(p)^n \to GF(p)$ is even and bent" in the hypothesis by "$f\colon GF(p)^n \to GF(p)$ is even, bent, and weakly regular." However, when $p = 3$ and $n = 2$, see Lemma 17(b).
4. This analogy fails if $n$ is odd. (See Section 4.4.)
5. The converse of this analogy fails, if $p > 2$. (See Example 58.)
6. As noted, if $p = 2$ then this analogue is true, by the work of Bernasconi et al. Indeed, if properly formulated, there is a converse (when $p = 2$) which holds as well (see [2], [3]).

Let $f\colon GF(p)^n \to GF(p)$ be a function such that $f(0) = 0$. Let $D_0 = \{0\}$ (the zero vector in $GF(p)^n$), $D_i = f^{-1}(i)$ for $i \in GF(p)\backslash\{0\}$, and $D_p = GF(p)^n \backslash \cup_{i=0}^{p-1} D_i$.

Regarding the Bernasconi correspondence (Theorem 25), the following would be combinatorial analogues. Analogue 45 does not always hold, since we show in Section 4.5 that there are functions $f\colon GF(5)^2 \to GF(5)$ such that $f$ is even and bent and $f(0) = 0$, but the level curves of $f$ do not determine a PDS. Consequently, by Lemma 7, Analogue 46 does not always hold.

**Analogue 45.** We ask under what additional hypotheses the following analogue of the Dillon correspondence is true:

If $f$ is an even bent function, then the tuple $(GF(p)^n, D_1, D_2, \ldots, D_{p-1})$ defines a weighted partial difference set.

**Analogue 46.** Let $f$ be as above, and let $R_0, R_1, \ldots, R_p$ denote binary relations on $GF(p)^n$ given by

$$R_i = \{(x, y) \in GF(p)^n \times GF(p)^n \mid x - y \in D_i\}, \quad 0 \le i \le p.$$

We ask under what additional hypotheses the following analogue of the Dillon correspondence is true:

If $f$ is an even bent function, then $(GF(p)^n, R_0, R_1, \ldots, R_p)$ is a $p$-class association scheme.

**Remark 47.** It is known that for "homogeneous" weakly regular bent functions, the level curves give rise to a weighted PDS. In fact, the weighted PDS corresponds to an association scheme, and the dual association scheme corresponds to the dual bent function (see [30, Corollary 3]). We know that any bent function equivalent to such a bent function also has this property (see Proposition 5).

Our data seems to support the following statement.

**Conjecture 2.** Let $f\colon GF(p)^n \to GF(p)$ be an even bent function with $f(0) = 0$, with $p > 2$. If the level curves of $f$ give rise to a weighted partial difference set[5], then $f$ is weakly regular. If the union of the level curves also determines a corresponding (unweighted) partial difference set[6], this partial difference set is of (positive or negative) Latin square type.

We also pose the following question: is there a "homogeneous"-type condition that $f$ must also satisfy, if the level curves of $f$ give a PDS?

The adjacency matrix $A = A_f$ is the matrix whose entries are

$$A_{i,j} = f_{\mathbb{C}}(\eta(i) - \eta(j)), \tag{22}$$

where $\eta(k)$ is the $p$-ary representation as in Equation (15). Ignoring edge weights, we let

$$A^*_{i,j} = \begin{cases} 1, & f_{\mathbb{C}}(\eta(i) - \eta(j)) \neq 0; \\ 0, & \text{otherwise.} \end{cases} \tag{23}$$

Note that the Cayley graph $\Gamma_f$ is a regular edge-weighted digraph (each vertex has the same in-degree and the same out-degree as each other vertex). The in-degree

[5] In the sense of Remark 31.

[6] In the sense of Lemma 5.

and the out-degree both equal $wt(f)$, where $wt$ denotes the Hamming weight of $f$, when regarded as a vector (of length $p^n$) of integers. Let

$$\omega = \omega_f = wt(f)$$

denote the cardinality of $\mathrm{supp}(f) = \{v \in V \mid f(v) \neq 0\}$, and let

$$\sigma_f = \sum_{v \in V} f_{\mathbb{C}}(v).$$

Note that $f^\wedge(0) = \sigma_f \geq |\mathrm{supp}(f)|$. If $f$ is even, then $\Gamma_f$ is an $\sigma_f$-regular (edge-weighted) graph. If we ignore weights, then it is an $\omega_f$-regular graph.

Recall that, given a Cayley graph $\Gamma$ of a function $f\colon GF(p)^n \to GF(p)$ and its (symmetric) adjacency matrix $A$, the spectrum $\sigma(\Gamma) = \{\lambda_1, \lambda_2, \dots, \lambda_N\}$, where $N = p^n$, is the multi-set of (real) eigenvalues of $A$. Following a standard convention, we index the elements $\lambda_i = \lambda_i(A)$ of the spectrum in such a way that they are monotonically increasing. Because $\Gamma_f$ is regular, the row sums of $A$ are all $\sigma_f$, whence the all-ones vector is an eigenvector of $A$ with eigenvalue $\sigma_f$. We will see later (Corollary 5) that $\lambda_N(A) = \sigma_f$.

Let $D$ denote the identity matrix multiplied by $\sigma_f$. The *Laplacian* of $\Gamma_f$ can be defined as the matrix $L = D - A$.

**Lemma 12.** *Assume $f$ is even. As an edge-weighted graph, $\Gamma_f$ is connected if and only if $\lambda_{N-1}(A) < \lambda_N(A) = \sigma_f$, where $A$ is the adjacency matrix of Equation (22). If we ignore edge weights, then $\Gamma_f$ is connected if and only if $\lambda_{N-1}(A^*) < \lambda_N(A^*) = \omega_f$, where $A^*$ is the unweighted adjacency matrix of Equation (23).*

*Proof.* We only prove the statement for the edge-weighted case. Note that for $i = 1, \dots, N$, $\lambda_i(L) = \sigma_f - \lambda_{N-i+1}(A)$, since $\det(L - \lambda I) = \det(\sigma_f I - A - \lambda I) = (-1)^n \det(A - (\sigma_f - \lambda)I)$. Thus $\lambda_i(L) \geq 0$, for all $i$. By a result on algebraic connectivity of graphs (see [18] or [19] for the unweighted case; the weighted case is a corollary of the unweighted case), $\lambda_2(L) > 0$ if and only if $\Gamma_f$ is connected. But $\lambda_2(L) > 0$ is equivalent to $\sigma_f - \lambda_{N-1}(A) > 0$. □

Clearly, the vertices in $\Gamma_f$ connected to $0 \in V$ are in natural bijection with $\mathrm{supp}(f)$. Let $W_j$ denote the subset of $V$ consisting of those vectors which can be written as the sum of $j$ elements in $\mathrm{supp}(f)$. Clearly,

$$W_1 = \mathrm{supp}(f) \subset W_2 \subset \cdots \subset \mathrm{Span}(\mathrm{supp}(f)),$$

where $\mathrm{Span}(S)$ denotes the vector space of all linear combinations of a set $S \subset V$ of vectors.

For each $v_0 \in W_1 = \mathrm{supp}(f)$, the vertices connected to $v_0$ are the vectors in

$$\mathrm{supp}(f_{v_0}) = \{v \in V \mid f(v - v_0) \neq 0\},$$

where $f_{v_0}(v) = f(v - v_0)$ denotes the translation of $f$ by $-v_0$. Therefore,

$$\mathrm{supp}(f_{v_0}) = v_0 + \mathrm{supp}(f).$$

In particular, all the vectors in $W_2$ are connected to $0 \in V$. For each $v_0 \in W_2$, the vertices connected to $v_0$ are the vectors in $\mathrm{supp}(f_{v_0}) = v_0 + \mathrm{supp}(f)$, so all the vectors in $W_3$ are connected to $0 \in V$. Inductively, we see that $\mathrm{Span}(\mathrm{supp}(f))$ is the connected component of 0 in $\Gamma_f$. Pick any $u \in V$ representing a non-trivial coset in $V/\mathrm{Span}(\mathrm{supp}(f))$, where $V/S$ denotes the vector space quotient of $V$ modulo a subspace $S$. Clearly, 0 is not connected with $u$ in $\Gamma_f$. However, the above reasoning implies $u$ is connected to $v$ if and only if $u$ and $v$ represent the same coset in $V/\mathrm{Span}(\mathrm{supp}(f))$. This proves the following result.

**Lemma 13.** *The connected components of $\Gamma_f$ are in one-to-one correspondence with the elements of the quotient space $V/Span(\mathrm{supp}(f))$.*

### 3.2. Group Actions on Bent Functions

We note here some useful facts about the action of nondegenerate linear transforms on $p$-ary functions. Let $V = GF(p)^n$. Suppose that $f : V \to GF(p)$, and suppose that $\phi : V \to V$ is a nondegenerate linear transformation (isomorphism of $V$). Let $g(x) = f(\phi(x))$. The functions $f$ and $g$ both have the same signature, $(|f^{-1}(i)| \mid i = 1, \dots, p-1)$.

It is straightforward to check that

$$W_g(u) = W_f({}^t(\phi^{-1})u),$$

where $t$ denotes transpose.

It follows that if $f$ is bent, so is $g$, and if $f$ is bent and regular, so is $g$. If $f$ is bent and weakly regular, with $\mu$-regular dual $f^*$, then $g$ is bent and weakly regular, with $\mu$-regular dual $g^*$, where $g^*(u) = f^*({}^t(\phi^{-1})u)$.

Next, we examine the effect of the group action on bent functions and the corresponding weighted PDSs.

**Proposition 5.** *Let $f : GF(p)^n \to GF(p)$ be an even bent function such that $f(0) = 0$, and define $D_i = f^{-1}(i)$ for $i \in GF(p) - \{0\}$. Suppose $\phi : GF(p)^n \to GF(p)^n$ is a linear map that is invertible (i.e., det $\phi \neq 0 \pmod p$). Define the function $g = f \circ \phi$; $g$ is the composition of a bent function and an affine function, so it is also bent. If the collection of sets $\{D_1, D_2, \dots, D_{p-1}\}$ forms a weighted partial difference set for $GF(p)^n$, then so does its image under the function $\phi$.*

The following result is given in [6, Chapter 17]. We include a different proof.

**Theorem 48.** *Let $f : GF(p)^n \to GF(p)$ be an even function with $f(0) = 0$, and let $\Gamma$ be its Cayley graph. Assume $\Gamma$ is an edge-weighted strongly regular graph. Let*

*$D_k = f^{-1}(k)$ for $k \in GF(p) - \{0\}$. Let $A = (a_{k,l})$ be the adjacency matrix of $\Gamma$. Let $A_i = (a^i_{k,l})$ be the $(0,1)$-matrix where*

$$a^i_{k,l} = \begin{cases} 1, & \textit{if } a_{k,l} = i; \\ 0, & \textit{otherwise}, \end{cases}$$

*for each $i = 1, 2, \ldots, p-1$. Let $A_0$ be the $p^n \times p^n$ identity matrix. Let $A_p$ be the $(0,1)$-matrix such that $A_0 + A_1 + \cdots + A_{p-1} + A_p = J$, where $J$ is the $p^n \times p^n$ matrix with all entries 1. Let $R$ denote the matrix ring generated by $\{A_0, A_1, \ldots, A_p\}$. The structure constants $p^k_{ij}$ defined by Equation (6), with $s = p$, satisfy the formula*

$$p^k_{ij} = \left(\frac{1}{p^n|D_k|}\right) tr(A_i A_j A_k),$$

*for all $i, j, k = 1, 2, \ldots, p$.*

*Proof.* By the matrix-walk theorem, $A_i A_j$ can be considered as counting walks along the Cayley graph of specific edge weights. Supposed $(u, v)$ is an edge of $\Gamma$ with weight $k$. If $k = 0$, then $u = v$ and the edge is a loop. If $k = p$, then $(u, v)$ is technically not an edge in $\Gamma$, but we will label it as an edge of weight $p$.

The $(u, v)$-th entry of $A_i A_j$ is the number of walks of length 2 from $u$ to $v$, where the first edge has weight $i$ and the second edge has weight $j$; the entry is 0 if no such walk exists. If we consider the $(u, v)$-th entry on each side of the equation defining the structure constants, Equation (6) with $s = p$, we can deduce that $p^k_{ij}$ is the number of walks of length 2 from $u$ to $v$, where the first edge has weight $i$ and the second edge has weight $j$ (it equals 0 if no such walk exists) for any edge $(u, v)$ with weight $k$ in $\Gamma$.

Similarly, the matrix-walk theorem implies that $tr(A_i A_j A_k)$ is the total number of closed walks of length 3 having edge weights $i, j, k$. We claim that if $\triangle$ is any triangle with edge weights $i, j, k$, then, by subtracting an element $v \in GF(p)^n$, we will obtain a triangle in $\Gamma$ containing the zero vector as a vertex with the same edge weights. Suppose $\triangle = (u_1, u_2, u_3)$, where $(u_1, u_2)$ has edge weight $i$, $(u_2, u_3)$ has edge weight $j$, and $(u_3, u_1)$ has edge weight $k$. Let $\triangle' = (0, u_2 - u_1, u_3 - u_1)$. We compute the edge weights of $\triangle'$:

$$\text{edge weight of } (0, u_2 - u_1) = f(0 - (u_2 - u_1)) = f(u_1 - u_2) = i;$$
$$\text{edge weight of } (u_2 - u_1, u_3 - u_1) = f((u_2 - u_1) - (u_3 - u_1)) = f(u_2 - u_3) = j;$$
$$\text{edge weight of } (u_3 - u_1, 0) = f((u_3 - u_1) - 0) = f(u_3 - u_1) = k.$$

Thus the claim is proven.

Therefore,

$$\left(\frac{1}{|GF(p)^n|}\right) tr(A_i A_j A_k) = \left(\frac{1}{p^n}\right) tr(A_i A_j A_k)$$

is the number of closed walks of length 3 having edge weights $i, j, k$ and containing the zero vector as a vertex, incident to the edge of weight $i$ and the edge of weight $k$.

There are $|D_k|$ edges of weight $k$ incident to the zero vector, so

$$\left(\frac{1}{p^n}\right)\left(\frac{1}{|D_k|}\right) tr(A_iA_jA_k)$$

is the number of $(i, j)$-weighted walks (of length 2) from the zero vector to any $k$-neighbor of it. This is equivalent to the definition of the number $p_{ij}^k$ in the matrix-walk theorem. □

**Corollary 3.** *Let $f\colon GF(p)^n \to GF(p)$ be an even function such that $f(0) = 0$, and let $\Gamma$ be its edge-weighted Cayley graph. Let $A_i$ be as in the theorem above. If*

$$\left(\frac{1}{p^n|D_k|}\right) tr(A_iA_jA_k)$$

*is not an integer, for some $i, j, k$, then $\Gamma$ is not edge-weighted strongly regular.*

By the intersection numbers of an edge-weighted strongly regular graph, we mean the structure constants of the corresponding adjacency ring. If $f\colon GF(p)^n \to GF(p)$ is an even function such that $f(0) = 0$ whose edge-weighted Cayley graph is edge-weighted strongly regular, then by the intersection numbers of $f$ we mean those of its Cayley graph.

**Remark 49.** Let $f\colon GF(p)^n \to GF(p)$ be an even function with $f(0) = 0$ whose Cayley graph $\Gamma$ is an edge-weighted strongly regular graph. We note that if $g = bf$ for some nonzero $b$ in $GF(p)$, then the intersection numbers $p_{ij}^k(g)$ of $g$ are easily found from the intersection numbers $p_{ij}^k(f)$ of $f$. If we define $\sigma(i) = b^{-1}i$, for $i = 0, \ldots, p-1$, and $\sigma(p) = p$, we have $p_{ij}^k(g) = p_{\sigma(i)\sigma(j)}^{\sigma(k)}(f)$.

### 3.3. Fourier Transforms and the Graph Spectrum

Let $V = GF(p)^n$, and let $f\colon V \to GF(p)$. Let $\zeta = e^{2\pi i/p}$. If we fix an ordering on $GF(p)^n$, then the $p^n \times p^n$ matrix

$$F = (f_{\mathbb{C}}(x-y) \mid x, y \in V) \tag{24}$$

is a $\mathbb{Z}$-valued matrix. Here $x$ indexes the rows, and $y$ indexes the columns.

Recall that a circulant matrix is a square matrix in which each row vector is a cyclic shift one element to the right relative to the preceding row vector. It seems that the matrix $F$ of Equation (24) is not circulant, but is "block circulant." Like circulant matrices, it has the property that $\vec{v}_a = (\zeta^{-\langle a,x\rangle} \mid x \in V)$ is an eigenvector with eigenvalue $\lambda_a = f^\wedge(-a)$ (for $a \in V$), where $f^\wedge$ is the Fourier transform of $f_{\mathbb{C}}$.

This is a property of the Hadamard transform of a Boolean function $f$ (see, e.g., Theorem 2.1 of Stanica's article [32]). Thus the proposition below, whose proof is straightforward and omitted, shows that it "morally" behaves like a circulant matrix in some ways.

**Proposition 6.** *The eigenvalues $\lambda_a = f^\wedge(-a)$ of the matrix $F$ of Equation (24) (for $a \in V$) are values of the Fourier transform $f^\wedge$ of $f$, given by*

$$f^\wedge(y) = \sum_{x \in V} f_{\mathbb{C}}(x)\zeta^{-\langle x,y\rangle},$$

*and the eigenvectors are the vectors of $p$-th roots of unity,*

$$\vec{v}_a = (\zeta^{-\langle a,x\rangle} \mid x \in V).$$

**Corollary 4.** *The matrix $F$ is invertible if and only if none of the values of the Fourier transform of $f_{\mathbb{C}}$ vanish.*

**Corollary 5.** *The spectrum of the graph $\Gamma_f$ is precisely the set of values of the Fourier transform of $f_{\mathbb{C}}$. In particular, if $\{\lambda_1, \lambda_2, \ldots, \lambda_N\}$ is the spectrum, indexed in monotone increasing order, then $\lambda_N = \sum_{v \in V} f_{\mathbb{C}}(v)$.*

Suppose we want to write the function $\zeta^f$ as a linear combination of translates of the function $f_{\mathbb{C}}$:

$$\zeta^{f(x)} = \sum_{a \in V} c_a f_{\mathbb{C}}(x-a), \tag{25}$$

for some $c_a \in \mathbb{C}$. This may be regarded as the convolution of $f_{\mathbb{C}}$ with a function $c$. Note that $c$ is well-defined up to an element of $ker(F)$. One way to solve for the $c_a$'s is to write this as a matrix equation,

$$\zeta^{\vec{f}} = F \cdot \vec{c},$$

where $\vec{c} = \vec{c}_f = (c_a \mid a \in V)$ and $\zeta^{\vec{f}} = (\zeta^{f(x)} \mid x \in V)$. If $F$ is invertible, that is if the Fourier transform of $f$ is always non-zero, then

$$\vec{c} = F^{-1}\zeta^{\vec{f}}.$$

If Equation (25) holds, then we can write the Walsh transform $f$,

$$W_f(u) = \sum_{x \in GF(p)^n} \zeta^{f(x)-\langle u,x\rangle},$$

as a linear combination of values of the Fourier transform,

$$f^\wedge(y) = \sum_{x \in V} f_{\mathbb{C}}(x)\zeta^{-\langle x,y\rangle}.$$

In other words,

$$\begin{aligned} W_f(u) &= \textstyle\sum_{a\in V} c_a \sum_{x\in GF(p)^n} \zeta^{-\langle u,x\rangle} f_{\mathbb{C}}(x-a) \\ &= \textstyle\sum_{a\in V} c_a \sum_{x\in GF(p)^n} \zeta^{-\langle u,x+a\rangle} f(x) \\ &= \textstyle\sum_{a\in V} c_a \zeta^{-\langle u,a\rangle} \sum_{x\in GF(p)^n} \zeta^{-\langle u,x\rangle} f_{\mathbb{C}}(x) \\ &= f^\wedge(u) \textstyle\sum_{a\in V} c_a \zeta^{-\langle u,a\rangle}. \end{aligned} \tag{26}$$

This may be regarded as the product of Fourier transforms (that of the function $f$ and that of the function $c$, which depends on $f$). In other words, there is a relationship between the Fourier transform of a $GF(p)$-valued function and its Walsh-Hadamard transform. However, it is not explicit unless one knows the function $c$ (which depends on $f$ in a complicated way).

**Remark 50.** In the case $p = 2$, the spectrum of $\Gamma_f$ is determined by the set of values of the Walsh-Hadamard transform of $f$ when regarded as a vector of (integer) $0, 1$-values (of length $2^n$). (This nice fact seems to have first appeared in [1].) Does this result have an analogue for $p > 2$?

We include here some results relating bent functions and balanced functions. Recall that a map $g\colon GF(p)^n \to GF(p)$ is *balanced* if the cardinalities $|g^{-1}(x)|$, for $x \in GF(p)$, are all equal.

**Lemma 14.** *Consider a map $g\colon GF(p)^n \to GF(p)$, where we identify $GF(p)$ with $\{0, 1, 2, \dots, p-1\}$. The following statements are equivalent:*

*(a) The map $g$ is balanced.*

*(b) We have $|g^{-1}(x)| = p^{n-1}$, for each $x \in GF(p)$.*

*(c) The Fourier transform of $\zeta^g$ satisfies $(\zeta^g)^\wedge(0) = 0$.*

*Proof.* It is easy to show that $(a)$ and $(b)$ are equivalent. Also, a straightforward and omitted argument shows $(a)$ implies $(c)$.

We show $(c)$ implies $(a)$ by an argument similar to that used for Lemma 10.

Note that

$$(\zeta^g)^\wedge(0) = |\mathrm{supp}(g)_0| + |\mathrm{supp}(g)_1|\zeta + \cdots + |\mathrm{supp}(g)_{p-1}|\zeta^{p-1},$$

which we can regard as an identity in the $(p-1)$-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta)$. If $(\zeta^g)^\wedge(0)$ is rational, the relation

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$$

implies all the $|\mathrm{supp}(g)_j|$ are equal, for $j \neq 0$. It also implies $(\zeta^g)^\wedge(0) = |\mathrm{supp}(g)_0| - |\mathrm{supp}(g)_1|$. Therefore, $(\zeta^g)^\wedge(0) = 0$ implies $g$ is balanced. □

**Definition 51.** We call an $N \times N$ complex matrix $M$ a *Butson matrix* if

$$M \cdot {}^t\overline{M} = NI_N,$$

where $I_N$ is the $N \times N$ identity matrix.

The following equivalences are known (see for example [33] and [8]), but proofs are included for the convenience of the reader.

**Proposition 7.** *Let $f\colon GF(p)^n \to GF(p)$ be any function. The following statements are equivalent:*

*(a) The function $f$ is bent.*

*(b) The matrix $\zeta^F = (\zeta^{f(\eta(i)-\eta(j))})_{0\leq i,j\leq p^n-1}$ is Butson, where $\eta$ is as in Equation (15).*

*(c) The derivative*

$$D_b f(x) = f(x+b) - f(x)$$

*is balanced, for each $b \neq 0$.*

*Proof.* Let

$$h(b) = (\zeta^{D_b f})^\wedge(0) = \sum_{x\in V} \zeta^{f(x+b)-f(x)}.$$

($(a) \implies (c)$) Note that

$$\begin{array}{rl} h^\wedge(y) & = \sum_{b\in V}\sum_{x\in V}\zeta^{f(x+b)-f(x)}\zeta^{-\langle y,b\rangle} \\ & = \sum_{b\in V}\sum_{x\in V}\zeta^{f(x+b)-f(x)-\langle y,b\rangle-\langle y,x\rangle+\langle y,x\rangle} \\ & = \sum_{x\in V}\zeta^{-f(x)+\langle y,x\rangle}\sum_{b\in V}\zeta^{f(x+b)-\langle y,x+b\rangle} \\ & = (\zeta^f)^\wedge(y)\overline{(\zeta^f)^\wedge(y)} \\ & = |(\zeta^f)^\wedge(y)|^2 \\ & = |W_f(y)|^2. \end{array} \tag{27}$$

Therefore, if $f$ is bent then $h^\wedge$ is a constant, which means that $h$ is supported at 0. By Lemma 14, $D_b f(x)$ is balanced.

($(c) \implies (a)$) We reverse the above argument. Suppose $D_b f(x)$ is balanced. By Lemma 14, $h$ is supported at 0, so $h^\wedge$ is a constant. After substituting $y = 0$ into Equation (27) and using the fact $D_b f(x)$ is balanced, it is easy to see that the constant must be $h^\wedge(0) = |V| = p^n$. Thus $|W_f(y)| = p^{n/2}$.

($(c) \implies (b)$) Note that

$$\begin{array}{rl} \sum_{j=0}^{p^n-1}\zeta^{f(\eta(i)-\eta(j))-f(\eta(k)-\eta(j))} & = \sum_{j=0}^{p^n-1}\zeta^{f(\eta(k)-\eta(j)+\eta(i)-\eta(k))-f(\eta(k)-\eta(j))} \\ & = \sum_{x\in V}\zeta^{f(x+b)-f(x)}, \end{array} \tag{28}$$

where $b = \eta(i) - \eta(k)$. If $D_b f(x)$ is balanced, then by Lemma 14, this sum is zero for all $b \neq 0$. These are the off-diagonal terms in the product $\zeta^F\,{}^t\overline{\zeta^F}$. Those terms when $i = k$ are the diagonal terms. They are obviously $|V| = p^n$. This implies $\zeta^F$ is Butson.

($(b) \implies (c)$) This follows by reversing the above argument. The details are omitted. □

## 4. Examples of Bent Functions

In this section, numerous examples illustrating the open questions formulated above are given. We also state and prove a general result on the algebraic normal form of $p$-ary functions (due to the first-named author).

### 4.1. Algebraic Normal Form

If $f\colon GF(p)^n \to GF(p)$ is a $p$-ary function, there is a unique representation of $f$ as a polynomial in $n$ variables, say $x_0, x_1, \ldots, x_{n-1}$ with coefficients in $GF(p)$, such that each variable $x_i$ occurs with exponent at most $p - 1$. This representation is called the *algebraic normal form* (ANF) of $f$ and the highest degree of its terms is called the *degree* of $f$.

In [7], Carlet shows how every Boolean function can be written in algebraic normal form. Similarly, we show how every $GF(p)$-valued function over $GF(p)^n$ can be written in ANF as well.

**Definition 52.** An *atomic p-ary function* is a function $GF(p)^n \to GF(p)$ supported at a single point. For $v \in GF(p)^n$, the atomic function supported at $v$, with value 1 at $v$, is the function $f_v\colon GF(p)^n \to GF(p)$ such that $f_v(v) = 1$, and $f_v(w) = 0$ for every $w \in GF(p)^n$ such that $w \neq v$.

We begin by showing how to write the ANFs of the atomic $p$-ary functions $f_v$.

**Theorem 53.** *Let $v = (v_0, v_1, \ldots, v_{n-1})$ be an element of $GF(p)^n$, and let $f_v$ be the atomic p-ary function defined above. Then*

$$f_v(x) = \prod_{i=0}^{n-1} \left( \frac{1}{(p-1)!} \prod_{j=1}^{p-1} (j + v_i - x_i) \right), \tag{29}$$

*where $x = (x_0, x_1, \ldots, x_{n-1}) \in GF(p)^n$.*

*Proof.* First, we start by showing that $f_v(v) = 1$. We can do this by plugging $v$

directly into Equation (29), to obtain

$$\begin{aligned}
f_v(v) &= \prod_{i=0}^{n-1}\left(\frac{1}{(p-1)!}\prod_{j=1}^{p-1}(j+v_i-v_i)\right)\\
&= \prod_{i=0}^{n-1}\left(\frac{1}{(p-1)!}\prod_{j=1}^{p-1}j\right)\\
&= \prod_{i=0}^{n-1}\left(\frac{(p-1)!}{(p-1)!}\right)\\
&= 1.
\end{aligned}$$

Second, we show that $f_v(w) = 0$ for every $w \neq v$. Let $w \neq v$. Pick $k$ such that $w_k \neq v_k$. So there exists $j \in \{1, \ldots, n-1\} \subset GF(p)$ such that $j + v_k - w_k = 0$ in $GF(p)$. Thus the inside product of Equation (29) is 0 for $i = k$, and the whole equation is 0. So $f_v(w) = 0$. □

It easily follows that every $GF(p)$-valued function over $GF(p)^n$ can be written in ANF.

**Corollary 6.** *Let $g\colon GF(p)^n \to GF(p)$. Then*

$$g(x) = \sum_{v \in GF(p)^n} g(v) f_v(x), \tag{30}$$

*where $f_v$ is as in Equation (29).*

**Example 54.** Sagemath can easily list all the atomic functions over $GF(3)$ having 2 variables:

$$x_0^2x_1^2 - x_0^2 - x_1^2 + 1, x_0^2x_1^2 + x_0x_1^2 - x_0^2 - x_0, x_0^2x_1^2 - x_0x_1^2 - x_0^2 + x_0,$$
$$x_0^2x_1^2 + x_0^2x_1 - x_1^2 - x_1, x_0^2x_1^2 + x_0^2x_1 + x_0x_1^2 + x_0x_1, x_0^2x_1^2 + x_0^2x_1 - x_0x_1^2 - x_0x_1,$$
$$x_0^2x_1^2 - x_0^2x_1 - x_1^2 + x_1, x_0^2x_1^2 - x_0^2x_1 + x_0x_1^2 - x_0x_1, x_0^2x_1^2 - x_0^2x_1 - x_0x_1^2 + x_0x_1.$$

**Remark 55.** The degree of any bent function $f\colon GF(p)^n \to GF(p)$, when represented in ANF, satisfies

$$\deg(f) \leq \frac{n(p-1)}{2} + 1.$$

The degree of any weakly regular bent function $f\colon GF(p)^n \to GF(p)$, when represented in ANF, satisfies

$$\deg(f) \leq \frac{n(p-1)}{2},$$

provided that $(p-1)n \geq 4$. Both of these results are due to Hou [26] (see also [11] for further details).

### 4.2. Bent Functions of Two Variables Construction

Recall that a $p$-ary bent function $f$ is amorphic if its level curves $D_i = f^{-1}(i)$ determine an amorphic association scheme. The signature of a $GF(p)$-valued function is the $(p-1)$-tuple of the sizes of the level curves $D_1, \ldots, D_{p-1}$.

We will show that for any prime $p > 2$, there are $(p+1)!/2$ amorphic bent functions $f\colon GF(p)^2 \to GF(p)$ of signature $(p-1, p-1, \ldots, p-1)$ with ANFs that are homogeneous of degree $p-1$. They are all weakly regular. Furthermore, we show any function from $GF(p)^2$ to $GF(p)$ with signature $(p-1, p-1, \ldots, p-1)$ and ANF that is homogeneous of degree $p-1$ must be one of these $(p+1)!/2$ functions.

These results were suggested by examples computed in Sagemath and Mathematica. We note that for $p = 3$ we obtain $4!/2 = 12$ functions, and for $p = 5$ we obtain $6!/2 = 360$ functions. These agree with our examples.

**Proposition 8.** *Assume $p > 2$ is a prime. Let $v_1, v_2, \ldots, v_{p-1}$ be $p-1$ pairwise linearly independent vectors in $G = GF(p)^2$, and let $D_i$ be the set of all non-zero multiples of $v_i$, for $1 \leq i \leq p-1$. Let $D_0 = \{0\}$, and let $D_p = G \setminus D_0 \cup D_1 \cup \cdots D_{p-1}$. Let $f$ be the function given by $f(x) = i$, for $x \in D_i$ and $1 \leq i \leq p-1$, and $f(x) = 0$ otherwise. Then $f$ is a bent function. There are exactly $(p+1)!/2$ such functions, and each has signature $(p-1, \ldots, p-1)$.*

In fact we will show that these bent functions are all homogeneous, weakly regular, and amorphic.

*Proof.* First we note that there are $(p+1)!/2$ ways to choose the sets $D_i$ in the way described, and each way gives a different function $f$. The signature of each such function is $(p-1, \ldots, p-1)$, by the definition of $f$, since $|D_i| = p-1$ for $1 \leq i \leq p-1$.

Next we will show that each such $f$ is bent. We wish to show that for any non-zero $b$ in $G$, $D_b f$ is balanced, i.e., $D_b f$ takes every value in $GF(p)$ exactly $p$ times. The result follows from the counting argument given below.

In order to keep track of the number of times $D_b f$ takes a value in $GF(p)$, we will work with unordered lists $[\alpha_1, \ldots, \alpha_m]$ of elements of $GF(p)$, where elements may occur more than once, but order does not matter. Let $P$ denote the unordered list $[0, 1, 2, \ldots, p-1]$. For any list $S$, let $P_S$ denote the complement of $S$ in $P$, i.e., the list obtained from $P$ by removing any elements of $S$. Let $P + S$ denote the union of $P$ and $S$ as unordered lists, i.e., with repetitions allowed. For any positive integer $m$, let $mP$ denote a list with each entry of $P$ repeated $m$ times. For example, $P_{[0]} = [1, 2, \ldots, p-1]$, $P + [0] = [0, 0, 1, 2, \ldots, p-1]$, and $2P = [0, 0, 1, 1, 2, 2, \ldots, p-1, p-1]$.

We wish to show that for any non-zero $b$ in $G$, the set of values of $D_b f$ is $pP$.

*Case 1:* Suppose that $b$ is in $D_i$ for some $i$ such that $1 \leq i \leq p-1$.

If $x$ is also in $D_i$, then $x + b$ is either 0 (if $x = -b$) or an element of $D_i$. Therefore $D_b f$ takes the value $-i$ once on $D_i$, and takes the value 0, $p-2$ times on $D_i$. In unordered list notation, $D_b f$ takes the values $[-i] + (p-2)[0]$ on $D_i$.

Next consider $x$ in $D_j$, for some fixed $j \neq i$ such that $1 \leq j \leq p-1$. As $x$ ranges through the $p-1$ elements of $D_j$, the vector $x+b$ takes on $p-1$ pairwise linearly independent values in $G$, none of which is in $D_i$ or $D_j$. Therefore $f(x+b)$ ranges through the values $P_{[i,j]} + [0]$. Consequently, $D_b f(x) = f(x+b) - f(x)$ ranges through the values $P_{[i-j,0]} + [-j]$. Now taking the union of the values of $D_b f$ over the $p-2$ values of $j \neq i$ such that $1 \leq j \leq p-1$, we obtain $\sum_j \left(P_{[i-j,0]} + [-j]\right)$. Let $Q = [i-1, i-2, \ldots, i-(p-1)]_{[i-i]} = P_{[0,i]}$. Let $R = [-1, -2, \ldots, -(p-1)]_{[-i]} = P_{[0,-i]}$. The set of values of $D_b f$ on the union of $D_j$, for $j \neq i$ and $1 \leq j \leq p-1$, is $\left((p-2)P_{[0]}\right)_Q + R = \left((p-2)P_{[0]}\right)_{[-i]} + [i]$.

Similarly, as $x$ ranges through the $2(p-1)$ vectors in $D_p$, $f(x+b)$ takes the values $2P_{[i]}$ and $D_b f(x)$ takes the same values, since $f(x) = 0$ for $x$ in $D_p$.

If $x = 0$, we have $D_b f(x) = f(b) = i$.

Taking the union of the unordered lists from all the cases, we obtain

$$[-i] + (p-2)[0] + \left((p-2)P_{[0]}\right)_{[-i]} + [i] + 2P_{[i]} + [i] = pP.$$

It follows that $D_b f$ is balanced, so $f$ is bent.

*Case 2:* Similarly, suppose that $b$ is in $D_p$.

If $x$ is one of the $p-1$ vectors in $D_p$ which is a multiple of $b$, then $x+b$ is either 0 or is in $D_p$. On these $p-1$ vectors, $D_b f$ takes the values $(p-1)[0]$. As $x$ ranges through the $p-1$ vectors in $D_p$ which are not multiples of $b$, $x+b$ ranges through the sets $D_1, D_2, \ldots, D_{p-1}$, and $D_b f$ takes the values $P_{[0]}$.

As $x$ ranges through the vectors in $D_j$, for each $j$ with $1 \leq j \leq p-1$, then $f(x+b)$ takes values in $P_{[j]}$, and $D_b f(x)$ takes values in $[0-j, 1-j, \ldots, p-1-j]_{[j-j]} = P_{[0]}$. Taking the union over $j$, with $1 \leq j \leq p-1$, gives $(p-1)P_{[0]}$.

If $x = 0$, we have $D_b f(x) = f(b) = 0$.

Thus the values taken by $D_b f$ for $b \in D_p$ are

$$(p-1)[0] + P_{[0]} + (p-1)P_{[0]} + [0] = pP,$$

so once again we see that $D_b f$ is balanced and $f$ is bent. □

**Lemma 15.** *Let $f$ be as in Proposition 8. Then $f$ is weakly regular.*

*Proof.* We will show that $W_f(b)/W_f(0)$ is a $p$th root of unity, for every $b$ in $G = GF(p)^2$.

We first show that $W_f(0) = p$. We let $\zeta = e^{\frac{2\pi i}{p}}$. Noting that $f(x)$ takes the value $i$, $p-1$ times, for $1 \leq i \leq p-1$, and the value 0, $2p-1$ times, we have

$$\begin{aligned} W_f(0) &= \textstyle\sum_{x \in G} \zeta^{f(x)} \\ &= (p-1) \textstyle\sum_{i=1}^{p-1} \zeta^i + 2p - 1 \\ &= -(p-1) + 2p - 1 \\ &= p. \end{aligned}$$

Next suppose that $b \in D_i$ for some $i \neq 0$. Choose a set of representatives $v_j \in D_j$, for $1 \leq j \leq p-1$, and $v_p$ and $v_{p+1}$ linearly independent elements of $D_p$. We note that $G$ is the union of $\{0\}$ and the multiples $\{v_j, 2v_j, \ldots, (p-1)v_j\}$, for all $j$. We note also that $f(v_j) = f(kv_j)$, for all non-zero $k \in GF(p)$. Then

$$\begin{aligned} W_f(b) &= 1 + \textstyle\sum_{j=1}^{p+1} \sum_{k=1}^{p-1} \zeta^{f(v_j) - k<b,v_j>} \\ &= 1 + \textstyle\sum_{j=1}^{p+1} \zeta^{f(v_j)} \sum_{k=1}^{p-1} \left(\zeta^{-<b,v_j>}\right)^k . \end{aligned}$$

There is exactly one index $l$ such that $b$ and $v_l$ are orthogonal. For this $l$ we have

$$\sum_{k=1}^{p-1} \left(\zeta^{-<b,v_l>}\right)^k = p-1.$$

If $j \neq l$, we have

$$\sum_{k=1}^{p-1} \left(\zeta^{-<b,v_j>}\right)^k = \sum_{j=1}^{p-1} \zeta^j = -1.$$

Hence,

$$\begin{aligned} W_f(b) &= 1 + \left(\textstyle\sum_{j=1}^{p+1} \zeta^{f(v_j)}(-1)\right) + \zeta^{f(v_l)} + (p-1)\zeta^{f(v_l)} \\ &= 1 - (\zeta^1 + \zeta^2 + \cdots + \zeta^{p-1} + \zeta^0 + \zeta^0) + p\zeta^{f(v_l)} \\ &= p\zeta^{f(v_l)}. \end{aligned}$$

It follows that $W_f(b)/W_f(0) = \zeta^{f(v_l)}$, which is a $p$th root of unity, so $f$ is weakly regular. □

**Proposition 9.** *Let $f$ be as in Proposition 8. Let $\Gamma_i$ be the subgraph of the Cayley graph of $f$ whose edges are the edges of weight $i$, for $1 \leq i \leq p-1$, i.e., there is an edge between vertices $u$ and $w$ in $\Gamma_i$ if $u - w \in D_i$. Let $\Gamma_p$ be the complement of the Cayley graph of $f$ in the complete graph on the $p^2$ vertices $GF(p)^2$, i.e., there is an edge between vertices $u$ and $w$ if $u - w \in D_p$. Then the graphs $\Gamma_1, \Gamma_2, \ldots, \Gamma_p$ form a strongly regular decomposition of the complete graph on $p^2$ vertices. Furthermore, the graphs $\Gamma_1, \Gamma_2, \ldots, \Gamma_{p-1}$ are all of Latin square type $(p^2, p-1, p-2, 0)$ and the graph $\Gamma_p$ is of Latin square type $(p^2, 2(p-1), p-2, 2)$.*

*Proof.* Recall that a graph $\Gamma$ is $(v, k, \lambda, \mu)$-strongly regular if $\Gamma$ has $v$ vertices, each of degree $k$, and distinct vertices $u$ and $w$ have $\lambda$ common neighbors if $u$ and $w$ are neighbors, and $\mu$ common neighbors if $u$ and $w$ are not neighbors.

We see that $v = p^2$ for each graph $\Gamma_i$. Also, $k = |D_i|$, so $k = p-1$ for $1 \leq i \leq p-1$, and $k = 2(p-1)$ for $i = p$.

*Case 1:* $1 \leq i \leq p-1$. Suppose that $u$ and $w$ are neighbors in $\Gamma_i$. Let $v_i$ be a vector in $D_i$. Then $u = w + \ell v_i$ for some nonzero $\ell \in GF(p)$. If $z$ is a neighbor of both $u$ and $w$, then $z = u + mv_i$ and $z = w + nv_i$, for some nonzero $m, n \in GF(p)$. Then $w + \ell v_i + mv_i = w + nv_i$ or $\ell = n - m$ in $GF(p)$. There are $p-2$ possible pairs $(m, n)$, so $\lambda = p-2$.

If $u$ and $w$ are not equal and not neighbors in $\Gamma_i$, then $z$ cannot be a neighbor of both $u$ and $w$, so $\mu = 0$.

*Case 2:* $i = p$. Suppose that $u$ and $w$ are neighbors in $\Gamma_p$. Then $u = w + v$ for some $v \in D_p$. If $z$ is a neighbor of both $u$ and $w$, then $z = u + v'$ and $z = w + v''$, for some vectors $v'$ and $v''$ in $D_p$. Then $u - w = v'' - v' = v$. This is possible only if $v' = mv$ and $v'' = nv$ for some nonzero $m, n \in GF(p)$ such that $n - m = 1$. As in Case 1, there are $p - 2$ possible pairs $(m, n)$, so $\lambda = p - 2$.

Next suppose that $u$ and $w$ are not equal and not neighbors in $\Gamma_p$. Then $u - w$ is not an element of $D_p$. Let $v_p$ and $v_{p+1}$ be any two linearly independent vectors in $D_p$, so that $D_p$ consists of all nonzero multiples of $v_p$ and $v_{p+1}$. There is exactly one way to express $u - w$ as a linear combination $mv_p + nv_{p+1}$, for nonzero $m, n \in GF(p)$. Therefore, there are exactly two vectors which are neighbors of both $u$ and $w$: $z_1 = u - mv_p = w + nv_{p+1}$ and $z_2 = u - nv_{p+1} = w + mv_p$. Therefore $\mu = 2$. □

**Corollary 7.** *Let the function $f$ and the sets $D_0, D_1, \ldots, D_p$ be as in Proposition 8. Then the sets $D_0, D_1, \ldots, D_p$ determine an amorphic association scheme.*

*Proof.* The corollary is an immediate result of van Dam's theorem (Proposition 4) and Proposition 9. □

**Lemma 16.** *Let $f$ be the function of Proposition 8. Then $f$ has a homogeneous ANF of degree $p - 1$.*

*Proof.* It is easy to see that $f(kx) = k^{p-1}f(x) = f(x)$, for any nonzero $k$ in $GF(p)$. We will show that $f$ has ANF given by $P(x_1, x_2) = a_0x_1^{p-1} + a_1x_1^{p-2}x_2 + \cdots + a_{p-2}x_1x_2^{p-2} + a_{p-1}x_2^{p-1}$ for some $a_0, a_1, \ldots, a_{p-1}$ in $GF(p)$.

Let $\lambda$ be a generator of the cyclic multiplicative group of $GF(p)$. Then the vectors $w_1 = (1, 0), w_2 = (1, \lambda), w_3 = (1, \lambda^2), \ldots, w_p = (1, \lambda^{p-1}) = (1, 1), w_{p+1} = (0, 1)$ are pairwise linearly independent vectors. For some permutation $\sigma$ of $\{1, 2, \ldots, p + 1\}$, we may take $v_i = w_{\sigma(i)}$, where $v_i \in D_i$ for $1 \leq i \leq p - 1$ and $v_p, v_{p+1} \in D_p$. Let $\tau$ be defined by $\tau(i) = \sigma^{-1}(i)$ if $1 \leq \sigma^{-1}(i) \leq p - 1$ and $\tau(i) = 0$ otherwise. Then we want $P(w_i) = \tau(i)$ for all $i$. This gives an equation of the form $Ma = b$, where $a = (a_0, \ldots, a_{p-1})$, $b = (\tau(1), \tau(2), \ldots, \tau(p - 1), \tau(p), \tau(p + 1))$, and $M$ is the $(p + 1) \times p$ matrix shown below:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \lambda^2 & \lambda^3 & \cdots & \lambda^{p-2} & 1 \\ 1 & \lambda^2 & \lambda^4 & \lambda^6 & \cdots & \lambda^{2(p-2)} & 1 \\ 1 & \lambda^3 & \lambda^6 & \lambda^9 & \cdots & \lambda^{3(p-2)} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda^{p-2} & \lambda^{2(p-2)} & \lambda^{3(p-2)} & \cdots & \lambda^{(p-2)^2} & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

We note that the columns of the matrix $M$ all sum to 0. The sum of the entries of $b$ is $1+2+3+\cdots+p-1+0+0=0$, so the system is consistent. We note also that the submatrix of $M$ consisting of the first $p$ rows is a nonsingular Vandermonde matrix, so there is a solution $a$ to the equation $Ma=b$. Thus $f$ has the desired ANF. □

**Theorem 56.** *Suppose that $p>2$ is a prime, and $f$ is a function from $GF(p)^2$ to $GF(p)$ with algebraic normal form that is homogeneous of degree $p-1$ and with signature $(p-1,\ldots,p-1)$. Then $f$ is an amorphic, weakly regular, bent function.*

*Proof.* Such an $f$ must have the form described in Proposition 8. The conclusions follow from Proposition 8, Lemma 15, and Corollary 7. □

### 4.3. Bent Functions $GF(3)^2 \to GF(3)$

We focus on examples of even functions $GF(3)^2 \to GF(3)$ sending 0 to 0. There are exactly $3^4 = 81$ such functions. Sagemath was used to identify and classify the bent functions among them. The Sagemath code for the examples of Section 4.3, Section 4.4, and Section 4.5 is available online on the second author's webpage (see [10]).

**Proposition 10.** *There are 18 even bent functions $f\colon GF(3)^2 \to GF(3)$ such that $f(0)=0$. The group $G=GL(2,GF(3))$ acts on the set $\mathbb{B}$ of all such bent functions and there are two orbits in $\mathbb{B}/G$: $\mathbb{B}/G = B_1 \cup B_2$, where $|B_1|=12$ and $|B_2|=6$.*

*The 18 bent functions $b_1, b_2, \ldots, b_{18}$ are given below in table form and ANF. The orbit $B_1$ consists of the functions $b_2$, $b_3$, $b_4$, $b_5$, $b_6$, $b_7$, $b_8$, $b_9$, $b_{11}$, $b_{14}$, $b_{15}$, and $b_{16}$. These functions are all regular. The orbit $B_2$ consists of the functions $b_1$, $b_{10}$, $b_{12}$, $b_{13}$, $b_{17}$, and $b_{18}$. These functions are weakly regular (but not regular). Each of the bent functions gives rise to a symmetric weighted PDS.*

| $GF(3)^2$ | (0, 0) | (1, 0) | (2, 0) | (0, 1) | (1, 1) | (2, 1) | (0, 2) | (1, 2) | (2, 2) |
|---|---|---|---|---|---|---|---|---|---|
| $b_1$ | 0 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 2 |
| $b_2$ | 0 | 2 | 2 | 1 | 0 | 0 | 1 | 0 | 0 |
| $b_3$ | 0 | 1 | 1 | 2 | 0 | 0 | 2 | 0 | 0 |
| $b_4$ | 0 | 2 | 2 | 0 | 1 | 0 | 0 | 0 | 1 |
| $b_5$ | 0 | 0 | 0 | 2 | 1 | 0 | 2 | 0 | 1 |
| $b_6$ | 0 | 1 | 1 | 0 | 2 | 0 | 0 | 0 | 2 |
| $b_7$ | 0 | 0 | 0 | 1 | 2 | 0 | 1 | 0 | 2 |
| $b_8$ | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 1 | 0 |
| $b_9$ | 0 | 0 | 0 | 2 | 0 | 1 | 2 | 1 | 0 |
| $b_{10}$ | 0 | 2 | 2 | 2 | 1 | 1 | 2 | 1 | 1 |
| $b_{11}$ | 0 | 0 | 0 | 0 | 2 | 1 | 0 | 1 | 2 |
| $b_{12}$ | 0 | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 2 |
| $b_{13}$ | 0 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 2 |
| $b_{14}$ | 0 | 1 | 1 | 0 | 0 | 2 | 0 | 2 | 0 |
| $b_{15}$ | 0 | 0 | 0 | 1 | 0 | 2 | 1 | 2 | 0 |
| $b_{16}$ | 0 | 0 | 0 | 0 | 1 | 2 | 0 | 2 | 1 |
| $b_{17}$ | 0 | 2 | 2 | 1 | 1 | 2 | 1 | 2 | 1 |
| $b_{18}$ | 0 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 1 |

The ANFs of these functions are:

$$b_1 = x_0^2 + x_1^2, \quad b_2 = -x_0^2 + x_1^2, \quad b_3 = x_0^2 - x_1^2, \quad b_4 = -x_0^2 - x_0x_1,$$

$$b_5 = -x_0x_1 - x_1^2, \quad b_6 = x_0^2 + x_0x_1, \quad b_7 = x_0x_1 + x_1^2, \quad b_8 = -x_0^2 + x_0x_1,$$

$$b_9 = x_0x_1 - x_1^2, \quad b_{10} = -x_0^2 - x_1^2, \quad b_{11} = -x_0x_1, \quad b_{12} = -x_0^2 - x_0x_1 + x_1^2,$$

$$b_{13} = x_0^2 - x_0x_1 - x_1^2, \quad b_{14} = x_0^2 - x_0x_1, \quad b_{15} = -x_0x_1 + x_1^2,$$

$$b_{16} = x_0x_1, \quad b_{17} = -x_0^2 + x_0x_1 + x_1^2, \quad b_{18} = x_0^2 + x_0x_1 - x_1^2.$$

For each of these 18 bent functions $GF(3)^2 \to GF(3)$, the corresponding Cayley graph is edge-weighted strongly regular. However, the converse is false, i.e., there exist even functions $f\colon GF(3)^2 \to GF(3)$ with $f(0) = 0$ such that the Cayley graph of $f$ is edge-weighted strongly regular but $f$ is not bent (see Example 58).

**Example 57.** Consider the bent function $b_8$ defined above. It can be shown that the weighted PDS determined by $b_8$ is isomorphic to the weighted PDS of Example 14.

**Example 58.** Consider the even function $f\colon GF(3)^2 \to GF(3)$ with the following values:

| $GF(3)^2$ | (0, 0) | (1, 0) | (2, 0) | (0, 1) | (1, 1) | (2, 1) | (0, 2) | (1, 2) | (2, 2) |
|---|---|---|---|---|---|---|---|---|---|
| $f$ | 0 | 1 | 1 | 2 | 0 | 1 | 2 | 1 | 0 |

This $f$ has ANF

$$2x_0^2x_1^2 + x_0^2 + x_0x_1 + 2x_1^2.$$

Using Sagemath , one can compute the Walsh-Hadamard transform of $f$ and verify that $f$ is not bent. Although $f$ is not bent, its Cayley graph satisfies the statements in the conclusion of Analogue 43. In other words, the associated edge-weighted Cayley graph is edge-weighted strongly regular. The plot of the corresponding Cayley graph is shown in Figure 1.

The *unweighted* Cayley graph of $b_2$ (as well as $b_3$, $b_4$, $b_5$, $b_6$, $b_7$, $b_8$, $b_9$, $b_{11}$, $b_{14}$, $b_{15}$, and $b_{16}$) is a strongly regular graph having parameters $SRG(v, k, \lambda, \mu)$ where $v = 9$, $k = 4$, $\lambda = 1$, and $\mu = 2$. We say that these bent functions are of *type* $(9, 4, 1, 2)$. The other 6 bent functions are of *type* $(9, 8, 7, 0)$. Up to isomorphism, there is only one (unweighted) strongly regular graph having parameters $SRG(9, 4, 1, 2)$ (see [4], [31]). We shall see later that the edge-weighted Cayley graphs arising from these 12 bent functions of type $(9, 4, 1, 2)$ are also isomorphic[7] as edge-weighted graphs. Likewise, the Cayley graphs of these 6 bent functions of type $(9, 8, 7, 0)$ are also isomorphic as edge-weighted graphs.

[7] We say edge-weighted graphs are *isomorphic* if there is a bijection of the vertices which preserves the weight of each edge.

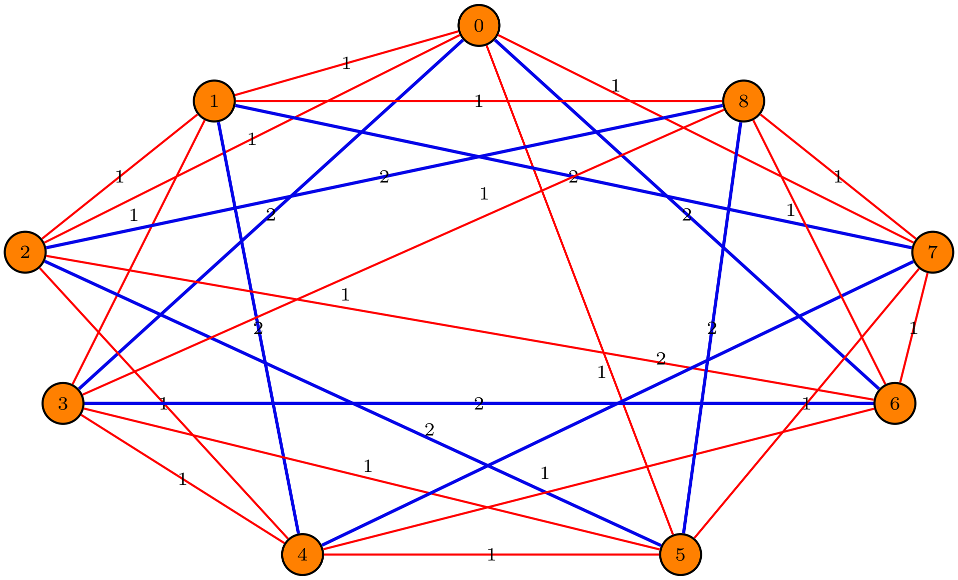

Figure 1: The undirected unweighted Cayley graph of an even $GF(3)$-valued function of two variables from Example 58. (The vertices are ordered as in the example.)

Sagemath computations verify the following relationships:

$$b_1 = -b_{10}, \quad b_2 = -b_3, \quad b_4 = -b_6, \quad b_5 = -b_7, \quad b_8 = -b_{14},$$

$$b_9 = -b_{15}, \quad b_{11} = -b_{16}, \quad b_{12} = -b_{18}, \quad b_{13} = -b_{17},$$

$$b_1 = b_7 + b_{14} = b_6 + b_{15}, \quad b_{10} = b_4 + b_9 = b_5 + b_8, \quad b_{12} = b_2 + b_{11} = b_7 + b_8,$$

$$b_{13} = b_3 + b_{11} = b_6 + b_9, \quad b_{17} = b_2 + b_{16} = b_4 + b_{15}, \quad b_{18} = b_3 + b_{16} = b_5 + b_{14}.$$

According to a Sagemath computation, the following are regular bent:

$$b_2^* = b_3, \quad b_4^* = b_9, \; b_5^* = b_8, \; b_6^* = b_{15}, \quad b_7^* = b_{14}, \; b_{11}^* = b_{16},$$

whereas

$$b_1^* = -b_{10}$$

are weakly regular bent and $(-1)$-dual to each other (but not regular). The others are all $(-1)$-self-dual and weakly regular (but not regular):

$$b_{12}^* = -b_{12}, \; b_{13}^* = -b_{13}, \; b_{17}^* = -b_{17}, \; b_{18}^* = -b_{18}.$$

Define the (left) action of $G = GL(2, GF(3))$ on $V = GF(3)^2$ by linear transformations of the coordinates, i.e., if $\phi$ is an element of $G$ given by

$$\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $ad - bc \neq 0$, and if $\vec{x} = (x_0, x_1)$, then $\phi(\vec{x}) = (ax_0 + bx_1, cx_0 + dx_1)$. This corresponds to the (right) action of $G$ on $GF(3)[x_0, x_1]$ defined for $\phi \in G$ by

$$\phi\colon f(x_0, x_1) \longmapsto f^{\phi}(x_0, x_1) = f(\phi^{-1}\vec{x}).$$

We note the following additional properties of the bent functions $b_i$:

- The 12 functions which are regular, but not $\mu$-regular for some $\mu \neq 1$, can all be obtained from $b_6(x_0, x_1) = x_0^2 + x_0x_1$ by linear transformations of the coordinates, i.e., transformations $(x_0, x_1) \mapsto (ax_0 + bx_1, cx_0 + dx_1)$ where $ad - bc \neq 0$. Each such isomorphism of $GF(3)^2$ induces an isomorphism of the associated edge-weighted Cayley graphs.
- Similarly, the 6 functions which are weakly regular can all be obtained from $b_1(x_0, x_1) = x_0^2 + x_1^2$ by linear transformations of the coordinates.

The following was verified with direct (computer-aided) computations.

**Lemma 17.** *Assume $p = 3$, $n = 2$.*

*(a) The edge-weighted Cayley graph of $b_i$ is edge-weighted strongly regular and not complete as a simple (unweighted) graph if and only if $b_i$ is regular if and only if $i \in \{2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 15, 16\}$, i.e., $b_i$ is in the orbit $B_1$.*

*(b) The edge-weighted Cayley graph of $b_i$ is edge-weighted strongly regular and complete as a simple (unweighted) graph if and only if $b_i$ is weakly regular (but not regular) if and only if $i \notin \{2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 15, 16\}$, i.e., $b_i$ is in the orbit $B_2$.*

**Proposition 11.** *Let $f\colon GF(3)^2 \to GF(3)$ be an even bent function with $f(0) = 0$. Then the level curves of $f$,*

$$D_i = \{v \in GF(3)^2 \mid f(v) = i\},$$

*for $i = 1, 2$, yield a symmetric weighted PDS and consequently a symmetric association scheme.*

1. *If $f$ is one of the twelve functions in orbit $B_1$, we have $|D_1| = |D_2| = 2$. The level curves of $f$ determine a symmetric 3-class association scheme, and the intersection numbers $p_{ij}^k$ are given as follows:*

| $p^0_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 0 |
| 2 | 0 | 0 | 2 | 0 |
| 3 | 0 | 0 | 0 | 4 |

| $p^1_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 |
| 2 | 0 | 0 | 0 | 2 |
| 3 | 0 | 0 | 2 | 2 |

| $p^2_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 2 |
| 2 | 1 | 0 | 1 | 0 |
| 3 | 0 | 2 | 0 | 2 |

| $p^3_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 2 | 0 | 1 | 0 | 1 |
| 3 | 1 | 1 | 1 | 1 |

*Furthermore, $D = D_1 \cup D_2$ is a $(9, 4, 1, 2)$-PDS of Latin square type ($N = 3$ and $R = 2$) and negative Latin square type ($N = -3$ and $R = -1$). Both $D_1$ and $D_2$ are $(9, 2, 1, 0)$-PDSs of Latin square type ($N = 3$ and $R = 1$). The level curve $D_3 = G \setminus (D \cup \{0\})$ is a $(9, 4, 1, 2)$-PDS of Latin square type ($N = 3$ and $R = 2$) and negative Latin square type ($N = -3$ and $R = -1$). Moreover, $f$ is an amorphic bent function.*

2. *If $f$ is one of the six functions in orbit $B_2$, we have $|D_1| = |D_2| = 4$, $D_3 = \emptyset$, and the intersection numbers $p^k_{ij}$ are given as follows:*

| $p^0_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | 4 | 0 |
| 2 | 0 | 0 | 4 |

| $p^1_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 2 |
| 2 | 0 | 2 | 2 |

| $p^2_{ij}$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 1 | 0 | 2 | 2 |
| 2 | 1 | 2 | 1 |

no $p^3_{ij}$

*Proof.* If $f$ is one of the functions in orbit $B_1$, we use Lemma 5, to see that $D_1$ and $D_2$ are both $(9, 2, 1, 0)$-PDSs of Latin square type ($N = 3$ and $R = 1$). It follows from Proposition 4 (and Theorem 22) that $f$ is an amorphic bent function. The rest of the proposition is verified using a case-by-case analysis. The proof is omitted. □

### 4.4. Bent Functions $GF(3)^3 \to GF(3)$

Sagemath and Mathematica were used to find and classify the even bent functions $f : GF(3)^3 \to GF(3)$ such that $f(0) = 0$.

**Proposition 12.** *There are 2340 even bent functions $f : GF(3)^3 \to GF(3)$ such that $f(0) = 0$. The group $G = GL(3, GF(3))$ acts on the set $\mathbb{B}$ of all such bent* *functions, and there are* 4 *orbits in* $\mathbb{B}/G$*:*

$$\mathbb{B}/G = B_1 \cup B_2 \cup B_3 \cup B_4,$$

*where* $|B_1| = 234$*,* $|B_2| = 936$*,* $|B_3| = 234$*, and* $|B_4| = 936$*. Furthermore,* $B_1 = -B_3$ *and* $B_2 = -B_4$*.*

*The bent functions which give rise to a symmetric weighted PDS*[8] *are those in orbits* $B_1$ *and* $B_3$*. The other bent functions do not.*

*The functions in orbits* $B_1$ *and* $B_3$ *are weakly regular, but not regular. The functions in orbits* $B_2$ *and* $B_4$ *are not weakly regular.*

| | |
|---|---|
| $B_1$ | $f_1(x_0, x_1, x_2) = x_0^2 + x_1^2 + x_2^2$ |
| $B_2$ | $f_2(x_0, x_1, x_2) = x_0x_2 + 2x_1^2 + 2x_0^2x_1^2$ |
| $B_3$ | $f_3(x_0, x_1, x_2) = -x_0^2 - x_1^2 - x_2^2$ |
| $B_4$ | $f_4(x_0, x_1, x_2) = -x_0x_2 - 2x_1^2 - 2x_0^2x_1^2$ |

Table 1: Representatives of orbits in $\mathbb{B}/G$ for $GF(3)^3 \to GF(3)$

**Example 59.** Consider the example of the even function $f_2 \colon GF(3)^3 \to GF(3)$ whose ANF is given in Table 1. This function is bent, but not weakly regular. For this example, Analogue 43 is false.

**Example 60.** Consider the example of the even bent function $f_1 \colon GF(3)^3 \to GF(3)$ of Table 1, which is homogeneous but bent. It is weakly regular, but not regular. The unweighted Cayley graph of $f_1$ is regular, but has four distinct eigenvalues, so is not strongly regular. However, a Sagemath computation shows $|W_{f_1}(a)| = 3^{3/2}$ for all $a \in GF(3)^3$, so $f_1$ is bent. Since $W_{f_1}(0)/3^{3/2}$ is not a cube root of 1, $f_1$ is not regular. In this example, Analogue 43 is true.

Let $f \colon GF(3)^3 \to GF(3)$ be an even bent function with $f(0) = 0$. Let

$$D_i = \{v \in GF(3)^3 \mid f(v) = i\}, \quad i = 1, 2,$$

$D_0 = \{0\}$, and $D_3 = GF(3)^3 \setminus (D_0 \cup D_1 \cup D_2)$.

**Proposition 13.** *Let* $f \colon GF(3)^3 \to GF(3)$ *be an even bent function with* $f(0) = 0$*. If the level curves* $D_i$ *of* $f$ *yield a symmetric weighted PDS with intersection numbers* $p_{ij}^k$*, then one of the following two cases occurs:*

1. *The function* $f$ *is in orbit* $B_1$*, we have* $|D_1| = 6$ *and* $|D_2| = 12$*, and the intersection numbers* $p_{ij}^k$ *are given as follows:*

[8] Note, the symmetric weighted PDSs are given in the examples below.

| $p^0_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 6 | 0 | 0 |
| 2 | 0 | 0 | 12 | 0 |
| 3 | 0 | 0 | 0 | 8 |

| $p^1_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 4 | 0 |
| 2 | 0 | 4 | 4 | 4 |
| 3 | 0 | 0 | 4 | 4 |

| $p^2_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 2 | 2 | 2 |
| 2 | 1 | 2 | 5 | 4 |
| 3 | 0 | 2 | 4 | 2 |

| $p^3_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 3 | 3 |
| 2 | 0 | 3 | 6 | 3 |
| 3 | 1 | 3 | 3 | 1 |

2. *The function $f$ is in orbit $B_3$, we have $|D_1| = 12$ and $|D_2| = 6$, and the intersection numbers $p^k_{ij}$ are given as follows:*

| $p^0_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 12 | 0 | 0 |
| 2 | 0 | 0 | 6 | 0 |
| 3 | 0 | 0 | 0 | 8 |

| $p^1_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 5 | 2 | 4 |
| 2 | 0 | 2 | 2 | 2 |
| 3 | 0 | 4 | 2 | 2 |

| $p^2_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 4 | 4 | 4 |
| 2 | 1 | 4 | 1 | 0 |
| 3 | 0 | 4 | 0 | 4 |

| $p^3_{ij}$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 6 | 3 | 3 |
| 2 | 0 | 3 | 0 | 3 |
| 3 | 1 | 3 | 3 | 1 |

**Remark 61.** In the cases of the above proposition where $f$ does give rise to a PDS, $f$ is quadratic.

One way to prove this proposition is to partition the set of even functions into equivalence classes with respect to the group action of $GL(3, GF(3))$, then pick a representative from each class and test for bentness. Once we know which orbits under $GL(3, GF(3))$ are bent, we can test a representative from each orbit. It turns out that there are only 4 orbits whose elements are bent.

By Remark 55 (see [26] and [11]), if $f$ is a bent function $f \colon GF(3)^3 \to GF(3)$, then the algebraic degree of $f$ is at most 4. Furthermore, if $f$ is weakly regular, its degree is at most 3. We note that if $f$ is even, it can have only terms of even degree, and if $f(0) = 0$, then the constant term of $f$ is zero. Thus, if $f \colon GF(3)^3 \to GF(3)$ is even, bent, weakly regular, and satisfies $f(0) = 0$, it must have only terms of degree 2.

Consider the set $\mathbb{E}$ of all functions $f \colon GF(3)^3 \to GF(3)$ such that $f$ is even, $f(0) = 0$, and the degree of the ANF of $f$ is at most 4. The ANF of such a function must be of the form

$$f(x_0, x_1, x_2) = a_1x_0^2 + a_2x_0x_1 + a_3x_0x_2 + a_4x_1^2 + a_5x_1x_2 + a_6x_2^2$$
$$+b_1x_0^2x_1^2 + b_2x_0^2x_1x_2 + b_3x_0^2x_2^2 + b_4x_0x_1^2x_2 + b_5x_0x_1x_2^2 + b_6x_1^2x_2^2$$

where $a_1, \ldots, a_6, b_1, \ldots, b_6$ are in $GF(3)$. Thus there are $3^{12} = 531,441$ such functions. Recall the *signature* of $f$ is the sequence of cardinalities of the level curves

$$D_i = \{x \in GF(3)^3 \mid f(x) = i\}$$

for $i = 1, 2$.

Let $G = GL(3, GF(3))$ be the set of nondegenerate linear transformations

$$\phi\colon GF(3)^3 \to GF(3)^3.$$

This group acts on $\mathbb{E}$ in a natural way, and we say $f \in \mathbb{E}$ is *equivalent* to $g \in \mathbb{E}$ if and only if $f$ is sent to $g$ under some element of $G$. An equivalence class is simply an orbit in $\mathbb{E}$ under this action of $G$. Mathematica was used to calculate that $|G| = 11232$. However, since $f(\phi(x)) = f(-\phi(x))$ for all $\phi$ in $G$ and $x$ in $GF(3)^3$, there are at most 5616 functions in the equivalence class of any nonzero element of $\mathbb{E}$.

If $f$ is bent, then so is $f \circ \phi$, for $\phi$ in $G$. Therefore, one way to find all bent functions in $\mathbb{E}$ is to partition $\mathbb{E}$ into equivalence classes under the action of $G$ and test an element of each equivalence class to see if it is bent. However, the computational time for attacking this problem directly was prohibitive.

We next note that the size of the level curves $f^{-1}(1)$ and $f^{-1}(2)$ is preserved under the action of elements of $G$, i.e., the signature of $f$ is the same for all functions in each equivalence class. Mathematica was used to partition $\mathbb{E}$ into sets with the same signature. There are 35 signatures that occur. The sizes of the signature equivalence classes range from 0 (for the zero function) to 90090 for $|D_1| = |D_2| = 8$. There are 120120 elements of $\mathbb{E}$ of signature $(6, 12)$ or $(12, 6)$.

Mathematica was then used to find all equivalence classes of functions in $\mathbb{E}$ under transformations in $G$ for each of the 35 signature equivalence classes. There are a total of 281 equivalence classes of functions in $\mathbb{E}$ under the action of $GL(3, GF(3))$. Of these, 4 classes consist of bent functions. In other words, if $\mathbb{B}$ denotes the subset of $\mathbb{E}$ consisting of bent functions, then $G$ acts on $\mathbb{B}$ and the number of orbits is 4.

There were two equivalence classes of bent functions of type $|D_1| = 6$ and $|D_2| = 12$. The other two bent classes were of type $|D_1| = 12$ and $|D_2| = 6$ and consisted of the negatives of the functions in the first two classes. We will call the classes $B_1$, $B_2$, $B_3$, and $B_4$:

$$\mathbb{B}/G = B_1 \cup B_2 \cup B_3 \cup B_4.$$

Note that the $(6, 12)$ classes are negatives of the $(12, 6)$ classes, so after a possible reindexing, we have $B_3 = -B_1$ and $B_4 = -B_2$.

A representative of $B_1$ is

$$x_0^2 + x_1^2 + x_2^2.$$

There are 234 bent functions in its equivalence class under nondegenerate linear transformations. Note that the ANFs of all these functions are quadratic.

A representative of $B_2$ is

$$x_0x_2 + 2x_1^2 + 2x_0^2x_1^2.$$

There are 936 bent functions in its equivalence class under nondegenerate linear transformations.

Thus there are a total of 2340 bent functions in $\mathbb{B}$.

We calculate the intersection numbers $p_{ij}^k$ for representatives of $B_1$ and $B_3$ by the formula

$$p_{ij}^k = \left(\frac{1}{p^n|D_k|}\right) tr(A_iA_jA_k).$$

The right side of this formula yields some fractional values for $k = 3$ for representatives of $B_2$ and $B_4$, showing that the level curves of these functions do not yield weighted PDS's.

We note that the functions in $B_1$ and $B_3$ are weakly regular, but those in $B_2$ and $B_4$ are not.

We know that if $W_f(0)$ is rational, then the level curves $f^{-1}(i)$, where $i \neq 0$, have the same cardinality (see Lemma 10). A Sagemath computation shows that $W_f(0)$ is not a rational number for the representatives of $B_1, B_2$ displayed in Table 1 above.

Since the value of $W_f(0)$ depends only on the signature of $f$, it is easy to check that $W_f(0)/3^{3/2}$ is not a cube root of unity, for any function of class (6,12) or (12,6). It follows from Lemma 2 that $f$ is not regular, for all bent functions $f\colon GF(3)^3 \to GF(3)$.

### 4.5. Bent Functions $GF(5)^2 \to GF(5)$

Using Sagemath , we give examples of bent functions of 2 variables over $GF(5)$ and study their signatures (see Definition 35).

**Proposition 14.** *There are* 1420 *even bent functions* $f\colon GF(5)^2 \to GF(5)$ *such that* $f(0) = 0$. *The group* $G = GL(2, GF(5))$ *acts on the set* $\mathbb{B}$ *of all such bent functions, and there are* 11 *orbits in* $\mathbb{B}/G$*:*

$$\mathbb{B}/G = B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_5 \cup B_6 \cup B_7 \cup B_8 \cup B_9 \cup B_{10} \cup B_{11},$$

*where* $|B_1| = 40$*,* $|B_2| = 60$*,* $|B_3| = \cdots = |B_9| = 120$*, and* $|B_{10}| = |B_{11}| = 240$*.*

*The bent functions which give rise to a symmetric weighted PDS*[9] *are those in the orbits of* $f_1$*,* $f_2$*,* $f_5$*,* $f_6$*, and* $f_9$ *in Table 2. The bent functions in the orbits of the other* $f_i$*'s do not.*

*The function* $f_1$ *is weakly regular, and the functions* $f_2, \ldots, f_{11}$ *are regular.*

| | |
|---|---|
| $B_1$ | $f_1(x_0, x_1) = -x_0^2 + 2x_1^2$ |
| $B_2$ | $f_2(x_0, x_1) = -x_0x_1 + x_1^2$ |
| $B_3$ | $f_3(x_0, x_1) = -2x_0^4 + 2x_0^2 + 2x_0x_1$ |
| $B_4$ | $f_4(x_0, x_1) = -x_1^4 + x_0x_1 - 2x_1^2$ |
| $B_5$ | $f_5(x_0, x_1) = x_0^3x_1 + 2x_1^4$ |
| $B_6$ | $f_6(x_0, x_1) = -x_0x_1^3 + x_1^4$ |
| $B_7$ | $f_7(x_0, x_1) = x_1^4 - x_0x_1$ |
| $B_8$ | $f_8(x_0, x_1) = 2x_1^4 - 2x_0x_1 + 2x_1^2$ |
| $B_9$ | $f_9(x_0, x_1) = -x_0^3x_1 + x_1^4$ |
| $B_{10}$ | $f_{10}(x_0, x_1) = 2x_0x_1^3 + x_1^4 - x_1^2$ |
| $B_{11}$ | $f_{11}(x_0, x_1) = x_0x_1^3 - x_1^4 - 2x_1^2$ |

Table 2: Representatives of orbits in $\mathbb{B}/G$ for $GF(5)^2 \to GF(5)$

**Example 62.** Consider the example of the even function $f\colon GF(5)^2 \to GF(5)$ given by

$$f(x_0, x_1) = x_0^4 + 2x_0x_1.$$

This is non-homogeneous, but bent and regular.

In this example, Analogue 43 is false.

Do the "level curves" of a bent function $GF(5)^2 \to GF(5)$ give rise to a PDS? An association scheme? In specific examples, such questions can be answered using Sagemath .

The number of even (polynomial) functions $f$ of degree less than or equal to 4 is $5^8 = 390625$. The number of such functions having signature $(4, 4, 4, 4)$ is 10740, and the number of such functions having signature $(6, 6, 6, 6)$ is 2920.

If $G = GL(2, GF(5))$, then these 11 bent functions form a complete set of representatives of the $G$-equivalence classes of $\mathbb{B}$. We write $f \sim g$ if and only if $f = g \circ \phi$, for some $\phi \in G$. The group $GF(5)^\times$ also acts on $\mathbb{B}$. The functions $f_i$ satisfy

- for $i \in \{1, 2, 6\}$, $f_i \sim 2f_i \sim 3f_i \sim 4f_i$,
- $f_3 \sim 2f_4 \sim 3f_7 \sim 4f_8$,

[9] Note, the symmetric weighted PDSs are given in the examples below.

- $f_4 \sim 3f_3 \sim 4f_7 \sim 2f_8$,
- $f_5 \sim 4f_5 \sim 2f_9 \sim 3f_9$,
- $f_7 \sim 2f_3 \sim 4f_4 \sim 3f_8$,
- $f_8 \sim 4f_3 \sim 3f_4 \sim 2f_7$,
- $f_9 \sim 2f_5 \sim 3f_5 \sim 4f_9$,
- $f_{10} \sim 4f_{10} \sim 2f_{11} \sim 3f_{11}$,
- $f_{11} \sim 2f_{10} \sim 3f_{10} \sim 4f_{11}$.

It follows that $f_3$, $f_4$, $f_7$ and $f_8$ all must have the same signature. Similarly, $f_5$ and $f_9$ must have the same signature, and $f_{10}$ and $f_{11}$ must have the same signature.

Note that $f_5$ and $f_6$ are not $GL(2, GF(5))$-equivalent, but they both correspond to symmetric weighted PDSs with the same intersection numbers. In particular, the adjacency ring corresponding to $f_5$ is isomorphic to the adjacency ring corresponding to $f_6$.

**Example 63.** The example of $f_1$ above can be used to construct an edge-weighted strongly regular Cayley graph, hence also a symmetric weighted PDS attached to its level curves. Define the level curve $D_i$ (for $i = 1, 2, 3, 4$) as above, and let $D_0 = \{0\}$ and $D_5 = GF(5)^2 \setminus \cup_{i=0}^{4} D_i$. We can interpret $p_{ij}^k$ to be the number of times each element of $D_k$ occurs in $D_j - D_i$. By computing these numbers directly using Sagemath , we obtain the intersection numbers $p_{ij}^k$:

| $p_{ij}^0$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 6 | 0 | 0 | 0 |
| 2 | 0 | 0 | 6 | 0 | 0 |
| 3 | 0 | 0 | 0 | 6 | 0 |
| 4 | 0 | 0 | 0 | 0 | 6 |

| $p_{ij}^1$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 2 | 0 | 2 | 1 |
| 2 | 0 | 0 | 2 | 2 | 2 |
| 3 | 0 | 2 | 2 | 0 | 2 |
| 4 | 0 | 1 | 2 | 2 | 1 |

| $p_{ij}^2$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 2 | 2 | 2 |
| 2 | 1 | 2 | 2 | 1 | 0 |
| 3 | 0 | 2 | 1 | 1 | 2 |
| 4 | 0 | 2 | 0 | 2 | 2 |

| $p_{ij}^3$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 2 | 2 | 0 | 2 |
| 2 | 0 | 2 | 1 | 1 | 2 |
| 3 | 1 | 0 | 1 | 2 | 2 |
| 4 | 0 | 2 | 2 | 2 | 0 |

| $p_{ij}^4$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 2 | 2 | 1 |
| 2 | 0 | 2 | 0 | 2 | 2 |
| 3 | 0 | 2 | 2 | 2 | 0 |
| 4 | 1 | 1 | 2 | 0 | 2 |

no $p_{ij}^5$

**Example 64.** The example of $f_2$ above can be used to construct an edge-weighted strongly regular Cayley graph, hence also a symmetric weighted PDS attached to its level curves. In fact, the union of the level curves determines a $(25, 16, 9, 12)$-PDS of Latin square type ($N = 5$ and $R = 4$).

Define the level curve $D_i$ (for $i = 1, 2, 3, 4$) as above, and let $D_0 = \{0\}$ and $D_5 = GF(5)^2 \setminus \cup_{i=0}^{4} D_i$. We can interpret $p_{ij}^k$ to be the number of times each element of $D_k$ occurs in $D_j - D_i$. By computing these numbers directly using Sagemath , we obtain the intersection numbers $p_{ij}^k$:

| $p_{ij}^0$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 4 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 4 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 4 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 4 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 8 |

| $p_{ij}^1$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 2 | 0 | 1 | 0 |
| 2 | 0 | 2 | 0 | 0 | 0 | 2 |
| 3 | 0 | 0 | 0 | 2 | 0 | 2 |
| 4 | 0 | 1 | 0 | 0 | 1 | 2 |
| 5 | 0 | 0 | 2 | 2 | 2 | 2 |

| $p_{ij}^2$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 0 | 0 | 2 |
| 2 | 1 | 0 | 0 | 1 | 2 | 0 |
| 3 | 0 | 0 | 1 | 1 | 0 | 2 |
| 4 | 0 | 0 | 2 | 0 | 0 | 2 |
| 5 | 0 | 2 | 0 | 2 | 2 | 2 |

| $p_{ij}^3$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 2 | 0 | 2 |
| 2 | 0 | 0 | 1 | 1 | 0 | 2 |
| 3 | 1 | 2 | 1 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 2 | 2 |
| 5 | 0 | 2 | 2 | 0 | 2 | 2 |

| $p_{ij}^4$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 2 |
| 2 | 0 | 0 | 2 | 0 | 0 | 2 |
| 3 | 0 | 0 | 0 | 0 | 2 | 2 |
| 4 | 1 | 1 | 0 | 2 | 0 | 0 |
| 5 | 0 | 2 | 2 | 2 | 0 | 2 |

| $p_{ij}^5$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 1 | 0 | 1 | 1 | 1 |
| 3 | 0 | 1 | 1 | 0 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 0 | 1 |
| 5 | 1 | 1 | 1 | 1 | 1 | 3 |

**Example 65.** The example of $f_5$ above can be used to construct an edge-weighted strongly regular Cayley graph, hence also a symmetric weighted PDS attached to its level curves. In fact, the union of the level curves determines a $(25, 16, 9, 12)$-PDS of Latin square type ($N = 5$ and $R = 4$).

Define the level curve $D_i$ (for $i = 1, 2, 3, 4$) as above, and let $D_0 = \{0\}$ and $D_5 = GF(5)^2 \setminus \cup_{i=0}^{4} D_i$. Using Lemma 5, we can see that each of $D_1$, $D_2$, $D_3$, and $D_4$ is a $(25, 4, 3, 0)$-PDS of Latin square type ($N = 5$ and $R = 1$). Furthermore, since $D_5$ is the complement of $D = \cup_{i=0}^{4} D_i$, it is a $(25, 8, 3, 2)$-PDS (see Remark 23), which is of Latin square type ($N = 5$ and $R = 2$). It follows from Proposition 4 (and Theorem 22) that $f_5$ is an amorphic bent function.

The intersection numbers $p_{ij}^k$ are given by:

| $p_{ij}^0$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 4 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 4 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 4 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 4 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 8 |

| $p_{ij}^1$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 3 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 1 | 1 | 2 |
| 3 | 0 | 0 | 1 | 0 | 1 | 2 |
| 4 | 0 | 0 | 1 | 1 | 0 | 2 |
| 5 | 0 | 0 | 2 | 2 | 2 | 2 |

| $p_{ij}^2$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 2 |
| 2 | 1 | 0 | 3 | 0 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 | 2 |
| 4 | 0 | 1 | 0 | 1 | 0 | 2 |
| 5 | 0 | 2 | 0 | 2 | 2 | 2 |

| $p_{ij}^3$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 2 |
| 2 | 0 | 1 | 0 | 0 | 1 | 2 |
| 3 | 1 | 0 | 0 | 3 | 0 | 0 |
| 4 | 0 | 1 | 1 | 0 | 0 | 2 |
| 5 | 0 | 2 | 2 | 0 | 2 | 2 |

| $p_{ij}^4$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 2 |
| 2 | 0 | 1 | 0 | 1 | 0 | 2 |
| 3 | 0 | 1 | 1 | 0 | 0 | 2 |
| 4 | 1 | 0 | 0 | 0 | 3 | 0 |
| 5 | 0 | 2 | 2 | 2 | 0 | 2 |

| $p_{ij}^5$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 1 | 0 | 1 | 1 | 1 |
| 3 | 0 | 1 | 1 | 0 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 0 | 1 |
| 5 | 1 | 1 | 1 | 1 | 1 | 3 |

The examples of $f_6$ and $f_9$ above have the same $p_{ij}^k$'s.

## 5. Ideas for Further Study

We conclude with some questions touched on in this paper that we hope to explore in more detail in future research:

- Which bent functions give rise to an association scheme or Schur ring?
- Can these functions be distinguished from the spectra of their Cayley graphs?
- Under what additional hypotheses is the analogue of the Bernasconi correspondence true?
- Under what additional hypotheses is the analogue of the Dillon correspondence true?
- Is there a generalization of the construction in Section 4.2 of amorphic bent functions to higher dimensions?

**Acknowledgments**: We are grateful to our colleagues T. S. Michael and Amy Ksir for many stimulating conversations and suggestions on this paper. We also thank the referee for many very detailed comments which greatly helped the exposition.

## References

[1] A. Bernasconi, *Mathematical Techniques for the Analysis of Boolean Functions*, PhD dissertation TD-2/98, Universit di Pisa-Udine, 1998.

[2] A. Bernasconi and B. Codenotti, Spectral analysis of Boolean functions as a graph eigenvalue problem, *IEEE Trans. Comput.*, **48**:3 (1999), 345–351. `http://ilex.iit.cnr.it/codenotti/ps_files/graph_fourier.ps`

[3] A. Bernasconi, B. Codenotti, and J. VanderKam, A characterization of bent functions in terms of strongly regular graphs, *IEEE Trans. Comput.*, **50**:9 (2001), 984–985.

[4] A. Brouwer, Parameters of strongly regular graphs, webpage. `http://www.win.tue.nl/~aeb/graphs/srg/srgtab1-50.html`

[5] A. Brouwer, A. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer, Berlin Heidelberg, 1989.

[6] P. Cameron and J. van Lint, *Designs, Graphs, Codes and Their Links*, London Math. Soc. Lecture Note Series, Vol. **19**, Cambridge University Press, Cambridge, 1991.

[7] C. Carlet, Boolean functions for cryptography and error correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer, eds., Cambridge University Press, Cambridge, 2010, pp. 257–397. `http://www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf`

[8] C. Carlet and C. Ding, Highly non-linear mappings, *J. Complexity*, **20** (2004), 205–244.

[9] C. Celerier, D. Joyner, C. Melles, and D. Phillips, On the Walsh-Hadamard transform of monotone Boolean functions, *Tbilisi Math. J.*, **5** (2012), 19–35.

[10] C. Celerier, D. Joyner, C. Melles, D. Phillips, and S. Walsh, Explorations of edge-weighted Cayley graphs and $p$-ary bent functions, preprint, 2014. `http://www.arxiv.org/abs/1406.1087`
Sagemath code at `http://www.wdjoyner.org/papers/hadamard_transform2b.sage`

[11] A. Cesmelioglu and W. Meidl, Bent functions of maximal degree, *IEEE Trans. Inform. Theory*, **58** (2012), 1186–1190.

[12] Y. Chee, Y. Tan, and X. Zhang, Strongly regular graphs constructed from $p$-ary bent functions, preprint, 2010. `http://arxiv.org/abs/1011.4434`

[13] R. Coulter and R. Matthews, Bent polynomials over finite fields, *Bull. Aust. Math. Soc.*, **56** (1977), 429–437.

[14] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.*, No. **10** (1973).

[15] J. Dillon, *Elementary Hadamard Difference Sets*, PhD thesis, University of Maryland, 1974.

[16] E. Filiol and C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, in *Advances in Cryptology - EUROCRYPT'98*, Springer-Verlag, Berlin Heidelberg, 1998, pp. 475–488.

[17] T. Fen, B. Wen, Q. Xiang, and J. Yin, Partial difference sets from quadratic forms and $p$-ary weakly regular bent functions, in *Number Theory and Related Areas*, ALM **27**, International Press of Boston, 2010, pp. 25–40.

[18] M. Fiedler, Algebraic connectivity of graphs, *Czechoslovak Math. J.*, **23** (1973), 298–305.

[19] C. Godsil and G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, Vol. **207**, Springer-Verlag, New York, 2001.

[20] Ja. Gol'fand, A. Ivanov, and M. Klin, Amorphic cellular rings, in *Investigations in Algebraic Theory of Combinatorial Objects*, I. Faradžev, A. Ivanov, M. Klin, and A. Woldar, eds., Kluwer, Dordrecht, 1994, pp. 167–186.

[21] N. Goots, A. Moldovyan, and N. Moldovyan, Fast encryption algorithm SPECTR-H64, in *Information Assurance in Computer Networks*, Springer-Verlag, Berlin Heidelberg, 2001, pp. 275–286.

[22] T. Helleseth and A. Kholosha, On generalized bent functions, in *Information theory and applications workshop* (ITA), 2010.

[23] T. Helleseth and A. Kholosha, Bent functions and their connections to combinatorics, in *Surveys in Combinatorics 2013*, London Math. Soc. Lecture Note Series, Vol. 409, Cambridge University Press, Cambridge, 2013, pp. 91–126.

[24] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, **52** (2006), 2018–2032.

[25] A. Herman, Algebraic aspects of association schemes and scheme rings, seminar notes, 2011. `http://uregina.ca/~hermana/ASSR-Lecture9.pdf`

[26] X.-D. Hou, p-Ary and q-ary versions of certain results about bent functions and resilient functions, *Finite Fields Appl.*, **10** (2004), 566–582.

[27] P. Kumar, R. Scholtz, and L. Welch, Generalized bent functions and their properties, *J. Combin. Theory Ser. A*, **40** (1985), 90–107.

[28] J. Olsen, R. Scholtz, and L. Welch, Bent-function sequences, *IEEE Trans. Inform. Theory*, **28** (1982), 858–864.

[29] J. Polhill, A brief survey of difference sets, partial difference sets, and relative difference sets, preprint, 2003. `http://www.passhema.org/proceedings/2003/PolhillDifference2003.pdf`

[30] A. Pott, Y. Tan, T. Feng, and S. Ling, Association schemes arising from bent functions, *Des. Codes Cryptogr.*, **59** (2011), 319–331.

[31] E. Spence, Strongly regular graphs on at most 64 vertices, webpage. `http://www.maths.gla.ac.uk/~es/srgraphs.php`

[32] P. Stanica, Graph eigenvalues and Walsh spectrum of Boolean functions, *Integers*, **7**(2) (2007), #A32.

[33] N. Tokareva, Generalizations of bent functions: a survey, preprint, 2010. `http://eprint.iacr.org/2011/111.pdf`

[34] E. van Dam, Strongly regular decompositions of the complete graph, *J. Algebraic Combin.*, **17** (2003), 181–201.

[35] E. van Dam and M. Muzychuk, Some implications on amorphic association schemes, *J. Combin. Theory Ser. A*, **117** (2010), 111–127.

[36] Y. Zheng, J. Pieprzyk, and J. Seberry, HAVAL–a one-way hashing algorithm with variable length of output, in *Advances in Cryptology – AUSCRYPT'92*, Springer-Verlag, Berlin Heidelberg, 1993, pp. 83–104.