

Partial Difference Sets from Quadratic Forms and p -ary Weakly Regular Bent Functions

Tao Feng^{*}, Bin Wen[†], Qing Xiang[‡], Jianxing Yin[§]

Abstract

We generalize the construction of affine polar graphs in two different ways to obtain new partial difference sets and amorphic association schemes. The first generalization uses a combination of quadratic forms and uniform cyclotomy. In the second generalization we replace the quadratic form in the affine polar graph construction by higher degree homogeneous functions that are p -ary weakly regular bent. The negative Latin square type partial difference sets arising from the first generalization are new.

2000 Mathematics Subject Classification: 05E30, 05B10.


Keywords and Phrases: Amorphic association scheme, Association scheme, Bent function, Difference set, p -ary bent function, Partial difference set, Quadratic form, Strongly regular graph, Uniform cyclotomy.


1 Introduction

Let G be a finite (multiplicative) group of order v . A k -element subset D of G is called a (v, k, λ) *difference set* if the list of “differences” xy^{-1} , $x, y \in D$, $x \neq y$, represents each nonidentity element in G exactly λ times. Thus, D is a (v, k, λ) difference set in G if and only if it satisfies the following equation in the group ring $\mathbb{Z}[G]$:


$$DD^{(-1)} = (k - \lambda)1_G + \lambda G, \quad (1.1)$$

where $D = \sum_{d \in D} d$, $D^{(-1)} = \sum_{d \in D} d^{-1}$, $G = \sum_{g \in G} g$, and 1_G is the identity element of

^{*}Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA. 

[†]Department of Mathematics, Suzhou University, Suzhou 215006, China.  Department of Mathematics, Changshu Institute of Technology, Changshu 215500, China.

[‡]Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA. Research supported in part by NSF Grant DMS 1001557, and by the Overseas Cooperation Fund of China (grant 10928101). Email: xiang@math.udel.edu.

[§]Department of Mathematics, Suzhou University, Suzhou 215006, China.  Research supported in part by Natural Science Foundation of China (grant 10831002).

G . As an example of difference sets, we mention the classical Paley difference set (in the additive group of \mathbb{F}_q) consisting of the nonzero squares of \mathbb{F}_q , where $q \equiv 3 \pmod{4}$. Difference sets are the same objects as regular (i.e., sharply transitive) symmetric designs. They are the subject of much study in the past 50 years. For a recent survey, see [27].

Again let G be a finite (multiplicative) group of order v . A k -element subset D of G is called a (v, k, λ, μ) *partial difference set* (PDS, in short) provided that the list of “differences” xy^{-1} , $x, y \in D$, $x \neq y$, contains each nonidentity element of D exactly λ times and each nonidentity element of $G \setminus D$ exactly μ times. Using the group ring notation, we have that D is a (v, k, λ, μ) partial difference set in G if and only if

$$DD^{(-1)} = \gamma 1_G + (\lambda - \mu)D + \mu G, \quad (1.2)$$

where $\gamma = k - \mu$ if $1_G \notin D$ and $\gamma = k - \lambda$ if $1_G \in D$. A PDS with $\lambda = \mu$ is just a difference set. If D is a (v, k, λ, μ) PDS with $\lambda \neq \mu$, then $D^{(-1)} = D$; in which case, (1.2) becomes

$$D^2 = \gamma 1_G + (\lambda - \mu)D + \mu G. \quad (1.3)$$

A well-known example of PDS is the Paley PDS. Let \mathbb{F}_q be a finite field of size q with $q \equiv 1 \pmod{4}$. Then the set of nonzero squares in \mathbb{F}_q forms a $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right)$ PDS in the additive group of \mathbb{F}_q , which is called the *Paley PDS*.

Given a (v, k, λ, μ) partial difference set D in G with $1_G \notin D$ and $D^{(-1)} = D$, one can construct a strongly regular Cayley graph, $\text{Cay}(G, D)$, whose vertex set is G , and two vertices x, y are adjacent if and only if $xy^{-1} \in D$. Such a strongly regular graph $\text{Cay}(G, D)$ has G as a regular automorphism group. For example, the strongly regular Cayley graph constructed from the Paley PDS is the *Paley graph*. On the other hand, if a strongly regular graph has a regular automorphism group G , one can obtain a partial difference set in G . Therefore partial difference sets are equivalent to strongly regular graphs with a regular automorphism group. For a survey on partial difference sets, we refer the reader to [21]. For connections among partial difference sets, two-weight codes, projective two-intersection sets, we refer the reader to [6]. The following is a well-known construction of PDS. See for example [6].

Construction 1.1. Let $Q : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form, where n is even and q is a power of an odd prime p , and let

$$D = \{x \in \mathbb{F}_q^n : Q(x) \text{ is a nonzero square}\}.$$

Then D is a PDS in $(\mathbb{F}_q^n, +)$. The corresponding strongly regular graph $\text{Cay}(\mathbb{F}_q^n, D)$ is the so-called *affine polar graph*.

In this paper, we generalize Construction 1.1 in two different directions. First, we will replace the condition “ $Q(x)$ is a nonzero square” in the above definition of D by “ $Q(x)$ is a nonzero e th power in \mathbb{F}_q , where $e \geq 2$, $e|(q-1)$, and $p^j \equiv -1 \pmod{e}$ for some positive integer j ”. In doing so, we obtain new PDS in $(\mathbb{F}_q^n, +)$

and new amorphic association schemes on \mathbb{F}_q^n . We give the detailed statement of the our first generalization of Construction 1.1 below.

Theorem 1.2. *Let p be a prime, $e \geq 2$, $q = p^{2j\gamma}$, where $\gamma \geq 1$, $e|(p^j + 1)$ and j is the smallest such positive integer. Let C_i , $0 \leq i \leq e - 1$, be the cyclotomic classes of \mathbb{F}_q of order e , $n = 2m$ be an even positive integer, and $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form. Then each of the sets*

$$D_{C_i} := \{x \in V : Q(x) \in C_i\}, \quad 0 \leq i \leq e - 1$$

is a PDS in $(V, +)$ with parameters $(N^2, (N - \epsilon)R, \epsilon N + R^2 - 3\epsilon R, R^2 - \epsilon R)$, where $N = q^m$, $R = fq^{m-1}$, and $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic.

Second, we will replace the quadratic form in Construction 1.1 by higher degree homogeneous functions that are p -ary weakly regular bent (we will define the terms used here in the sequel). In doing so we also generalize a recent construction of PDS in [25] from the characteristic 3 case to the case of arbitrary odd characteristic p . The detailed statement of this generalization of Construction 1.1 is postponed to Section 3 since it involves too many technical terms.

The description of our first generalization of Construction 1.1 given above is quite straightforward except that we did not explain why we impose the condition $p^j \equiv -1 \pmod{e}$. We now give the owed explanation.

Let g be a fixed primitive element of \mathbb{F}_q , and let $e \geq 2$ be a divisor of $q - 1$, and $f = (q - 1)/e$. The i th cyclotomic classes C_0, C_1, \dots, C_{e-1} are defined by

$$C_i = \{g^{i+ej} : 0 \leq j \leq f - 1\},$$

where $0 \leq i \leq e - 1$. Let $\psi_\alpha, \alpha \in \mathbb{F}_q$, be the character of $(\mathbb{F}_q, +)$ defined by

$$\psi_\alpha(x) = \omega_p^{\text{Tr}(\alpha x)}, \quad (1.4)$$

for all $x \in \mathbb{F}_q$, where $\text{Tr} : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ is the absolute trace function. The cyclotomic periods η_i of order e are defined by

$$\eta_i = \sum_{z \in C_i} \psi_1(z),$$

where $i = 0, 1, \dots, e - 1$.

It is clear that $\sum_{i=0}^{e-1} \eta_i = -1$. Therefore it is impossible to have $\eta_0 = \eta_1 = \dots = \eta_{e-1}$ since, otherwise we have $\eta_i = -\frac{1}{e}$ for all $0 \leq i \leq e - 1$, implying that $\frac{1}{e}$, $e \geq 2$, is an algebraic integer, a contradiction. This fact motivates the following definition. We say that the cyclotomic periods η_i are *uniform* if all but one are equal. It is well known [2, 3] that $\eta_i, 0 \leq i \leq e - 1$, are uniform if and only if $p^j \equiv -1 \pmod{e}$ for some positive integer j (here p is the characteristic of \mathbb{F}_q). Therefore the essence in our first generalization of Construction 1.1 is to

replace “ $Q(x)$ is a nonzero square” by “ $Q(x)$ is a nonzero e th power in \mathbb{F}_q , and η_i are uniform”.

Next we give the definitions of the terms used in our second generalization of Construction 1.1. Let p be a prime, $n \geq 1$ be an integer, and $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a function. The *Walsh coefficient* of f at $b \in \mathbb{F}_{p^n}$ is defined by

$$\mathcal{W}_f(b) = \sum_{x \in \mathbb{F}_{p^n}} \omega_p^{f(x) + \text{Tr}(bx)},$$

where $\omega_p = e^{\frac{2\pi i}{p}}$ is a primitive complex p th root of unity, and elements of \mathbb{F}_p are considered as integers modulo p . The function f is said to be *p -ary bent* if $|\mathcal{W}_f(b)|^2 = p^n$ for all $b \in \mathbb{F}_{p^n}$. A p -ary bent function f is said to be *regular* if for every $b \in \mathbb{F}_{p^n}$, $p^{-\frac{n}{2}} \mathcal{W}_f(b)$ is equal to a complex p th root of unity. A p -ary bent function f is said to be *weakly regular* if there exists a complex number u with $|u| = 1$ such that $u p^{-\frac{n}{2}} \mathcal{W}_f(b) = \omega_p^{f^*(b)}$ for all $b \in \mathbb{F}_{p^n}$, where $f^* : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ is a function. Clearly, a regular p -ary bent function is weakly regular. Moreover, it is not difficult to see that if f is weakly regular bent, then so is f^* ; we call f^* the *dual* of f . For example, let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a nonsingular quadratic form (here we view \mathbb{F}_{p^n} as an n -dimensional vector space over \mathbb{F}_p), where p is an odd prime. Then f is a weakly regular bent function (cf. [15, 13]).

Binary bent functions are usually called *Boolean bent functions*, or simply *bent functions*. These functions were first introduced by Rothaus [24] in 1976. Later Kumar, Scholtz and Welch [19] generalized the notion of a Boolean bent function to that of a p -ary bent function.

Let $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ be a function. Then it is well known [12] that f is bent if and only if $D_1 := \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$ is a difference set in $(\mathbb{F}_{2^n}, +)$. Thus, given a bent function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, the inverse image of 1 (respectively, 0) is a difference set in $(\mathbb{F}_{2^n}, +)$. We comment that a difference set D in $(\mathbb{F}_{2^n}, +)$ is also a partial difference set since $-D = D$.

Now let p be an odd prime, and $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a p -ary bent function such that $f(-x) = f(x)$ for all $x \in \mathbb{F}_{p^n}$. For each $i \in \mathbb{F}_p$, we define

$$D_i := \{x \in \mathbb{F}_{p^n} : f(x) = i\}.$$

It is then natural to ask whether D_i is a PDS. It turns out that the answer to this question is in general negative. But in a recent paper [25], Tan, Pott and Feng proved that under certain conditions, the answer to the above question is indeed positive. Specifically, let $f : \mathbb{F}_{3^{2m}} \rightarrow \mathbb{F}_3$ be a weakly regular bent function such that $f(-x) = f(x)$ for all $x \in \mathbb{F}_{3^{2m}}$ and $f(0) = 0$. Then it was shown in [25] that $D_0 \setminus \{0\}$, D_1 and D_2 are all partial difference sets in $(\mathbb{F}_{3^{2m}}, +)$.

In this paper, we give a generalization of the aforementioned result of Tan et al. To be precise, let $f : \mathbb{F}_{p^{2m}} \rightarrow \mathbb{F}_p$ be a weakly regular bent function, where p is an odd prime. Define D_i for each $i \in \mathbb{F}_p$ as above. Let \mathcal{R} (respectively, \mathcal{N}) denote the set of nonzero squares (respectively, nonsquares) of \mathbb{F}_p . If there exists a positive integer k satisfying $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^{2m}}$, then $D_0 \setminus \{0\}$, $D_{\mathcal{R}} := \bigcup_{i \in \mathcal{R}} D_i$ and $D_{\mathcal{N}} := \bigcup_{i \in \mathcal{N}} D_i$ are

all partial difference sets in $(\mathbb{F}_{p^{2m}}, +)$. This construction can also be viewed as a generalization of Construction 1.1.

The PDS constructed in this paper naturally lead to amorphic association schemes, which we define below. Let V be a finite set. A d -class *symmetric association scheme* on V is a partition of $V \times V$ into sets R_0, R_1, \dots, R_d (called *relations, or associate classes*) such that

1. $R_0 = \{(x, x) : x \in V\}$ (the diagonal relation);
2. R_ℓ is symmetric for $\ell = 1, 2, \dots, d$;
3. for all i, j, k in $\{0, 1, 2, \dots, d\}$ there is an integer p_{ij}^k such that, for all $(x, y) \in R_k$,

$$|\{z \in V : (x, z) \in R_i \text{ and } (z, y) \in R_j\}| = p_{ij}^k.$$

Since each symmetric relation R_ℓ , $1 \leq \ell \leq d$, corresponds to an undirected graph $G_\ell = (X, R_\ell)$, $1 \leq \ell \leq d$, with vertex set V and edge set R_ℓ , we can think of an association scheme $(V, \{R_\ell\}_{0 \leq \ell \leq d})$ as an edge-decomposition of the complete graph on the vertex set V into graphs G_ℓ on the same vertex set with the property that for all i, j, k in $\{1, 2, \dots, d\}$ and for all $xy \in E(G_k)$,

$$|\{z \in V : xz \in E(G_i) \text{ and } zy \in E(G_j)\}| = p_{ij}^k,$$

where $E(G_k)$, $E(G_i)$ and $E(G_j)$ are the edge sets of G_k , G_i and G_j respectively. The graphs G_ℓ , $1 \leq \ell \leq d$, will be called *the graphs* of the association scheme $(V, \{R_\ell\}_{0 \leq \ell \leq d})$. A strongly regular graph (SRG) and its complement form a symmetric 2-class association scheme. For more background on association schemes and strongly regular graphs, see [5]. Given an association scheme $(V, \{R_\ell\}_{0 \leq \ell \leq d})$, we can take the union of classes to form graphs with larger edge sets (this process is called a *fusion*), but it is not necessarily guaranteed that the fused collection of graphs will form an association scheme on V . If an association scheme has the property that any of its fusions is also an association scheme, then we call the association scheme *amorphic*. A well known and important example of amorphic association schemes is given by the cyclotomic association scheme on \mathbb{F}_q where the cyclotomic periods are uniform [2, 1].

A (v, k, λ, μ) strongly regular graph is said to be of *Latin square type* (respectively, *negative Latin square type*) if $(v, k, \lambda, \mu) = (N^2, R(N - \epsilon), \epsilon N + R^2 - 3\epsilon R, R^2 - \epsilon R)$ and $\epsilon = 1$ (respectively, $\epsilon = -1$). If an association scheme is amorphic, then each of its graphs is clearly strongly regular. Moreover, A. V. Ivanov [18] showed that in an amorphic association scheme with at least three classes, all graphs of the scheme are of Latin square type, or all graphs are of negative Latin square type. The converse of Ivanov's result is proved to be true in [17]. In fact even more is true because Van Dam [9] could prove the following result.

Theorem 1.3. *Let V be a set of size v , let $\{G_1, G_2, \dots, G_d\}$ be an edge-decomposition of the complete graph on V , where each G_i is a strongly regular graph on V . If $G_i, 1 \leq i \leq d$, are all of Latin square type or all of negative Latin square type, then the decomposition is a d -class amorphic association scheme on V .*

Theorem 1.3 will be used in Section 2 to show that the PDS constructed there actually lead to amorphic association schemes. For a recent survey of results on amorphic association schemes, we refer the reader to [10].

The rest of the paper is organized as follows. In Sections 2 and 3 we give the two generalizations of Construction 1.1. In each of those two sections, we show that the PDS obtained actually lead to amorphic association schemes. As far as we know, the PDS with negative Latin square type parameters constructed in Section 2 are new.

2 Partial difference sets from quadratic forms and uniform cyclotomy

We start with some background on characters of abelian groups. Let G be a finite abelian group. A (complex) character χ of G is a homomorphism from G to \mathbb{C}^* , the multiplicative group of \mathbb{C} . A character χ of G is called *principal* if $\chi(g) = 1$ for all $g \in G$; otherwise it is called *nonprincipal*. The set of all characters of G forms a group (under point-wise multiplication), which is isomorphic to G . Let χ be a character of G , and $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. We define

$$\chi(A) = \sum_{g \in G} a_g \chi(g).$$

Starting with the important work of Turyn [26], character sums have been a powerful tool in the study of difference sets of all types. The following lemma states how character sums can be used to verify that a subset of an abelian group is a PDS.

Lemma 2.1. *Let G be a multiplicatively written abelian group of order v and D be a subset of G such that $D = \{d^{-1} : d \in D\}$, and $1_G \notin D$. Let k, λ, μ be positive integers such that $k^2 = \mu v + (\lambda - \mu)k + (k - \mu)$. Then D is a (v, k, λ, μ) PDS in G if and only if*

$$\chi(D) = \begin{cases} k, & \text{if } \chi \text{ is principal on } G, \\ \frac{(\lambda - \mu) \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}{2}, & \text{if } \chi \text{ is nonprincipal on } G. \end{cases}$$

Let q be a power of a prime p , and $e \geq 2$ be a divisor of $q - 1$. Let g be a fixed primitive element of \mathbb{F}_q , $C_0 = \langle g^e \rangle$, $C_i = g^i C_0$, $1 \leq i \leq e - 1$, be the cyclotomic classes of \mathbb{F}_q of order e , and $\eta_i = \sum_{x \in C_i} \psi_1(x)$ be the cyclotomic periods of order e ,

where ψ_1 is defined in (1.4). The cyclotomic periods η_i are in general very difficult to determine when e is large. But in a special case, one can compute η_i explicitly.

Theorem 2.2. *Let p be a prime, $e \geq 2$, $q = p^{2j\gamma}$, where $\gamma \geq 1$, $e | (p^j + 1)$ and j is the smallest such positive integer. Then the cyclotomic periods are given by*

Case A. *If $\gamma, p, \frac{p^j + 1}{e}$ are all odd, then*

$$\eta_{e/2} = \sqrt{q} - \frac{\sqrt{q} + 1}{e}, \quad \eta_i = -\frac{1 + \sqrt{q}}{e}, \quad \text{for all } i \neq \frac{e}{2}.$$

Case B. *In all the other cases,*

$$\eta_0 = -(-1)^\gamma \sqrt{q} + \frac{(-1)^\gamma \sqrt{q} - 1}{e}, \quad \eta_i = \frac{(-1)^\gamma \sqrt{q} - 1}{e}, \quad \text{for all } i \neq 0.$$

For a proof of Theorem 2.2, we refer the reader to [2, 22].

Next we define what we mean by nonsingular quadratic forms. Let V be an n -dimensional vector space over \mathbb{F}_q . A function $Q : V \rightarrow \mathbb{F}_q$ is called a *quadratic form* if

1. $Q(\alpha v) = \alpha^2 Q(v)$ for all $\alpha \in \mathbb{F}_q$ and $v \in V$,
2. the function $B : V \times V \rightarrow \mathbb{F}_q$ defined by $B(v_1, v_2) = Q(v_1 + v_2) - Q(v_1) - Q(v_2)$ is bilinear.

We say that Q is *nonsingular* if the subspace W of V with the property that Q vanishes on W and $B(w, v) = 0$ for all $v \in V$ and $w \in W$ is the zero subspace. If the field \mathbb{F}_q has odd characteristic, then Q is nonsingular if and only if B is nondegenerate; but this may not be true when \mathbb{F}_q has characteristic 2, because in that case Q may not be zero on the radical $\text{Rad}(V) = \{w \in V : B(w, v) = 0 \text{ for all } v \in V\}$. However, if V is an even-dimensional vector space over an even-characteristic field \mathbb{F}_q , then Q is nonsingular if and only if B is nondegenerate (cf. [7, p. 14]).

Now assume that $n = 2m$ is an even positive integer, and $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ is a nonsingular quadratic form. Therefore the polar form $B(x, y) := Q(x + y) - Q(x) - Q(y)$ of Q is nondegenerate. We write $\chi_b, b \in V$, for the additive character of V defined by

$$\chi_b(x) = \psi_1(B(b, x)), \quad x \in V.$$

Since B is nondegenerate, we see that $\{\chi_b : b \in V\}$ is the set of all additive characters of V .

For each $u \in \mathbb{F}_q$, we define $D_u = \{x \in V : Q(x) = u\}$, and $\mathcal{L}_\alpha = \sum_{u \in \mathbb{F}_q} D_u \psi_\alpha(u)$ for each $\alpha \in \mathbb{F}_q$, where ψ_α is defined in (1.4). (Here \mathcal{L}_α is viewed as an element of the group ring $\mathbb{C}[V, +]$.) For a subset X of \mathbb{F}_q , we write

$$D_X = \sum_{x \in X} D_x, \quad \mathcal{L}_X = \sum_{x \in X} \mathcal{L}_x.$$

Our main result in this section is Theorem 1.2, as stated in Section 1. Below we give the proof of that theorem.

Proof of Theorem 1.2. We will compute the character sums $\chi_b(D_{C_i}), b \in V$, explicitly, and then use Lemma 2.1 to finish the proof. To simplify notation, we write C for C_0 .

First, we have

$$\begin{aligned}\mathcal{L}_C &= \sum_{\alpha \in C} \sum_{u \in \mathbb{F}_q} D_u \psi_\alpha(u) = fD_0 + \sum_{\alpha \in C} \sum_{i=0}^{e-1} \sum_{u \in C_i} D_u \psi_\alpha(u) \\ &= fD_0 + \sum_{i=0}^{e-1} D_{C_i} \psi_1(C_i).\end{aligned}$$

Corresponding to the two cases of Theorem 2.2, we have

$$\mathcal{L}_C = \begin{cases} (f - \eta_0)D_0 + D_{C_{e/2}}(\eta_{e/2} - \eta_0) + \eta_0V, & \text{in Case A,} \\ (f - \eta_1)D_0 + D_C(\eta_0 - \eta_1) + \eta_1V, & \text{in Case B.} \end{cases} \quad (2.1)$$

Given any $b \in V$, we now compute $\chi_b(\mathcal{L}_C)$.

$$\begin{aligned}\chi_b(\mathcal{L}_C) &= \sum_{\alpha \in C} \sum_{u \in \mathbb{F}_q} \chi_b(D_u) \psi_\alpha(u) = \sum_{\alpha \in C} \sum_{x \in V} \chi_b(x) \psi_\alpha(Q(x)) \\ &= \sum_{\alpha \in C} \sum_{x \in V} \psi_1(\alpha Q(x) + B(b, x)) = \sum_{\alpha \in C} \sum_{x \in V} \psi_1(\alpha Q(x + \alpha^{-1}b) - \alpha^{-1}Q(b)) \\ &= \sum_{\alpha \in C} \psi_1(-\alpha^{-1}Q(b)) \sum_{x \in V} \psi_1(\alpha Q(x)).\end{aligned}$$

For each $\alpha \in \mathbb{F}_q^*$, $\alpha Q(x)$ is a quadratic form which is nonsingular and of the same type as $Q(x)$. By [20, Theorem 3.2], we have for each $\alpha \in \mathbb{F}_q^*$, $\sum_{x \in V} \psi_1(\alpha Q(x)) = \epsilon q^m$, where $\epsilon = 1$ if Q is hyperbolic and $\epsilon = -1$ if Q is elliptic. Therefore, in Case A we have

$$\chi_b(\mathcal{L}_C) = \epsilon q^m \sum_{\alpha \in C} \psi_1(-\alpha^{-1}Q(b)) = \begin{cases} \epsilon q^m f, & \text{if } Q(b) = 0, \\ \epsilon q^m \eta_{e/2}, & \text{if } -Q(b) \in C_{e/2}, \\ \epsilon q^m \eta_0, & \text{otherwise,} \end{cases}$$

and, in Case B we have

$$\chi_b(\mathcal{L}_C) = \begin{cases} \epsilon q^m f, & \text{if } Q(b) = 0, \\ \epsilon q^m \eta_0, & \text{if } -Q(b) \in C, \\ \epsilon q^m \eta_1, & \text{otherwise.} \end{cases}$$

Next we compute $\chi_b(D_0)$. We have

$$\begin{aligned}q\chi_b(D_0) &= \sum_{x \in V} \sum_{u \in \mathbb{F}_q} \chi_b(x) \psi_u(Q(x)) = \sum_{x \in V} \sum_{u \in \mathbb{F}_q} \psi_1(B(b, x) + uQ(x)) \\ &= \sum_{x \in V} \psi_1(B(b, x)) + \sum_{x \in V} \sum_{u \in \mathbb{F}_q^*} \psi_1(B(b, x) + uQ(x)).\end{aligned}$$

We now restrict our attention to the case where $b \neq 0$; in that case, we have $\sum_{x \in V} \psi_1(B(b, x)) = 0$. It follows that

$$\begin{aligned} q\chi_b(D_0) &= \sum_{x \in V} \sum_{u \in \mathbb{F}_q^*} \psi_1(-u^{-1}Q(b) + uQ(x + u^{-1}b)) \\ &= \sum_{u \in \mathbb{F}_q^*} \psi_1(-u^{-1}Q(b)) \sum_{x \in V} \psi_1(uQ(x)) = \epsilon q^m \sum_{u \in \mathbb{F}_q^*} \psi_1(-u^{-1}Q(b)) \\ &= \begin{cases} \epsilon q^m (q-1), & \text{if } Q(b) = 0, \\ -\epsilon q^m, & \text{otherwise.} \end{cases} \end{aligned}$$

From (2.1), in Case A, we have

$$\chi_b(D_{C_{e/2}}) = \frac{\chi_b(\mathcal{L}_C) - (f - \eta_0)\chi_b(D_0)}{\eta_{e/2} - \eta_0}.$$

Substituting the values of $\chi_b(\mathcal{L}_C)$ and $\chi_b(D_0)$, we obtain the following: for each $b \in V$, $b \neq 0$,

$$\chi_b(D_{C_{e/2}}) = \begin{cases} \epsilon q^{m-1} \frac{q\eta_{e/2} - \eta_0 + f}{\eta_{e/2} - \eta_0} = \epsilon q^{m-1} (q - f), & \text{if } -Q(b) \in C_{e/2}, \\ \epsilon q^{m-1} \frac{(q-1)\eta_0 + f}{\eta_{e/2} - \eta_0} = -\epsilon q^{m-1} f, & \text{otherwise.} \end{cases}$$

Again, from (2.1), in Case B, we have

$$\chi_b(D_C) = \frac{\chi_b(\mathcal{L}_C) - (f - \eta_1)\chi_b(D_0)}{\eta_0 - \eta_1}.$$

Substituting the values of $\chi_b(\mathcal{L}_C)$ and $\chi_b(D_0)$, we obtain the following: for each $b \in V$, $b \neq 0$,

$$\chi_b(D_C) = \begin{cases} \epsilon q^{m-1} \frac{q\eta_0 - \eta_1 + f}{\eta_0 - \eta_1} = \epsilon q^{m-1} (q - f), & \text{if } -Q(b) \in C, \\ \epsilon q^{m-1} \frac{(q-1)\eta_1 + f}{\eta_0 - \eta_1} = -\epsilon q^{m-1} f, & \text{otherwise.} \end{cases}$$

The sizes of $D_{C_{e/2}}$ and D_C can be computed as follows. First we have $|D_0| = \chi_0(D_0) = q^{2m-1} + \epsilon q^{m-1}(q-1)$. By applying the principal character χ_0 to $\mathcal{L}_C = (e - \eta_0)D_0 + D_{C_{e/2}}(\eta_{e/2} - \eta_0) + \eta_0 V$, we solve that $|D_{C_{e/2}}| = (q^m - \epsilon)fq^{m-1}$ in Case A. Similarly, we have $|D_C| = (q^m - \epsilon)fq^{m-1}$ in Case B.

By Lemma 2.1 and the computed character values of $D_{C_{e/2}}$ and D_C , we conclude that $D_{C_{e/2}}$ is a PDS in $(V, +)$ in Case A, D_C is a PDS in Case B. Both of them have parameters $(N^2, (N - \epsilon)R, \epsilon N + R^2 - 3\epsilon R, R^2 - \epsilon R)$, where $N = q^m$, $R = fq^{m-1}$.

Now to prove that each D_{C_i} is a PDS in $(V, +)$, one only needs to replace the quadratic form Q by αQ for an appropriate $\alpha \in \mathbb{F}_q^*$ and note that αQ is also a nonsingular quadratic form on V and of the same type as Q .

The proof is now complete. \square

Remark 2.3. (1) It is well known that $D_0 \setminus \{0\}$ is a PDS with parameters $(q^{2m}, (q^m - \epsilon)r, q^m + r^2 - 3r, r^2 - r)$, where $r = q^{m-1} + \epsilon$, $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic. This PDS is referred to as Example **RT2** in [6].

(2) It is interesting to note that Theorem 1.2 is valid when $p = 2$ while Construction 1.1 only works when p is odd.

(3) When the quadratic form Q in Theorem 1.2 is of elliptic type, the PDS D_{C_i} , $0 \leq i \leq e - 1$, have negative Latin square type parameters. Negative Latin square type PDS are harder to come by than Latin square type PDS. Besides Example **RT2** and the PDS arising from Construction 1.1, there is one more general class of negative Latin square type PDS in elementary abelian p -groups coming from the “difference of two quadrics” construction in [4]. (There exist variations of Brouwer’s construction, see [14, 11].) The negative Latin square type PDS arising from Theorem 1.2 have very different parameters from those in [4, 14, 11] since there is quite a bit of freedom in choosing the parameter $f = (q-1)/e$. As far as we know, the negative Latin square type PDS from Theorem 1.2 are new.

Next we show that the PDS obtained in Theorem 1.2 also lead to amorphic association schemes.

Corollary 2.4. *Let p be a prime, $e \geq 2$, $q = p^{2j\gamma}$, where $\gamma \geq 1$, $e \mid (p^j + 1)$ and j is the smallest such positive integer. Let C_i , $0 \leq i \leq e - 1$, be the cyclotomic classes of \mathbb{F}_q of order e , $n = 2m$ be an even positive integer, and $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form. Then the Cayley graphs $\text{Cay}(G, D_0 \setminus \{0\})$, $\text{Cay}(G, D_{C_i})$, $0 \leq i \leq e - 1$, where $G = (V, +)$, form a $(e + 1)$ -class amorphic association scheme on V .*

Proof. The proof is immediate by combining Theorem 1.2 and Theorem 1.3. \square

Remark 2.5. From Corollary 2.4 one obtains more PDS by choosing an arbitrary subset of $\{D_0 \setminus \{0\}, D_{C_i} : 0 \leq i \leq e - 1\}$, and taking union of the members of the subset.

3 Partial difference sets from weakly regular p -ary bent functions

Throughout this section, p always denotes an **odd** prime, $p^* = (-1)^{\frac{p-1}{2}}p$, and $\omega_p = e^{\frac{2\pi i}{p}}$. Let \mathcal{R} (respectively, \mathcal{N}) denote the set of nonzero squares (respectively, nonsquares) of \mathbb{F}_p . From the values of quadratic Gauss sums [3, p. 22], we have

$$r_0 := \sum_{a \in \mathcal{R}} \omega_p^a = \frac{\sqrt{p^*} - 1}{2},$$

and

$$n_0 := \sum_{a \in \mathcal{N}} \omega_p^a = \frac{-\sqrt{p^*} - 1}{2}.$$

Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a weakly regular bent function. From [13, 15], we have

$$\mathcal{W}_f(b) = u(\sqrt{p^*})^n \omega_p^{f^*(b)}, \quad (3.1)$$

for every $b \in \mathbb{F}_{p^n}$, where $u = \pm 1$ and f^* is a function from \mathbb{F}_{p^n} to \mathbb{F}_p . Furthermore, we define

$$D_i = \{x \in \mathbb{F}_{p^n} : f(x) = i\}, \quad (3.2)$$

for every $i \in \mathbb{F}_p$, and

$$\mathcal{L}_t = \sum_{i=0}^{p-1} D_i \omega_p^{it},$$

for every $t \in \mathbb{F}_p$. (Here \mathcal{L}_t is viewed as an element of the group ring $\mathbb{C}[(\mathbb{F}_{p^n}, +)]$.) Furthermore, we define

$$D_{\mathcal{R}} = \bigcup_{i \in \mathcal{R}} D_i, \quad D_{\mathcal{N}} = \bigcup_{i \in \mathcal{N}} D_i,$$

and

$$\mathcal{L}_{\mathcal{R}} = \sum_{t \in \mathcal{R}} \mathcal{L}_t, \quad \mathcal{L}_{\mathcal{N}} = \sum_{t \in \mathcal{N}} \mathcal{L}_t.$$

We will need a couple of lemmas from [23].

Lemma 3.1. ([23]) *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a weakly regular bent function. Assume that the Walsh coefficients of f satisfy (3.1). If there exists a constant k with $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$, then there exists a constant ℓ satisfying $\gcd(\ell-1, p-1) = 1$ and $f^*(tx) = t^\ell f^*(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$.*

Remark 3.2. The condition that there exists some k with $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$ is not a severe one. Almost all known weakly regular bent functions satisfy this condition. From the proof in [23], we see that the constant ℓ can be chosen in such a way that $\ell \equiv k(k-1)^{-1} \pmod{p}$.

Lemma 3.3. ([23]) *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a weakly regular bent function. Assume that the Walsh coefficients of f satisfy (3.1) and there exists a constant k with $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$. Let ℓ be given by Lemma 3.1. Then*

- (1) for $s, t, s+t \in \mathbb{F}_p^*$, $\mathcal{L}_t \mathcal{L}_s = u \left(\frac{tsv}{p} \right)^n (\sqrt{p^*})^n \mathcal{L}_v$, where $v = (s^{1-\ell} + t^{1-\ell})^{\frac{1}{1-\ell}}$;
- (2) for $t \in \mathbb{F}_p^*$, $\mathcal{L}_t \mathcal{L}_{-t} = p^n$;
- (3) for $a \in \mathbb{F}_p$, $\sum_{t=1}^{p-1} \mathcal{L}_t \mathcal{L}_0 \omega_p^{-at} = (p|D_a| - p^n) \mathbb{F}_{p^n}$.

Remark 3.4. The symbol $\left(\frac{\cdot}{p} \right)$ in part (1) of Lemma 3.3 is the **Legendre** symbol.

The equalities in all three parts of the lemma should be viewed as equalities in the group ring $\mathbb{C}[(\mathbb{F}_{p^n}, +)]$. In particular, the right hand side of the equality in part (2) of Lemma 3.3 is really $p^n \cdot 0$, where 0 is the identity of $(\mathbb{F}_{p^n}, +)$.

Now we are able to establish the main result of this section.

Theorem 3.5. *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a weakly regular bent function. Assume that the Walsh coefficients of f satisfy (3.1) and there exists a constant k with $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$. Furthermore, assume that n is even. Then $D_0 \setminus \{0\}$, $D_{\mathcal{R}}$ and $D_{\mathcal{N}}$ are all partial difference sets in $(\mathbb{F}_{p^n}, +)$.*

Proof. By assumption we have $f(-x) = f(x)$ for all $x \in \mathbb{F}_{p^n}$. It follows that $0 \in D_0$, $-D_0 = D_0$, $-D_{\mathcal{R}} = D_{\mathcal{R}}$, and $-D_{\mathcal{N}} = D_{\mathcal{N}}$. We will compute D_0^2 , $D_{\mathcal{R}}^2$ and $D_{\mathcal{N}}^2$ in the group ring $\mathbb{C}[(\mathbb{F}_{p^n}, +)]$. To this end, we first make some preparation.

By definition, we have

$$\begin{aligned} \mathcal{L}_{\mathcal{R}} &= \sum_{t \in \mathcal{R}} \mathcal{L}_t = \sum_{t \in \mathcal{R}} \sum_{i=0}^{p-1} D_i \omega_p^{it} \\ &= \sum_{i=0}^{p-1} D_i \left(\sum_{t \in \mathcal{R}} \omega_p^{it} \right) \\ &= \frac{p-1}{2} D_0 + r_0 D_{\mathcal{R}} + n_0 D_{\mathcal{N}}. \end{aligned}$$

Similarly, $\mathcal{L}_{\mathcal{N}} = \frac{p-1}{2} D_0 + n_0 D_{\mathcal{R}} + r_0 D_{\mathcal{N}}$. Also from definition, we have $\mathcal{L}_0 = \mathbb{F}_{p^n}$.

From the definition of \mathcal{L}_t , where $t \in \mathbb{F}_p$, and orthogonality relations, we have

$$pD_a = \sum_{t=0}^{p-1} \mathcal{L}_t \omega_p^{-at},$$

for any $a \in \mathbb{F}_p$. It follows that in $\mathbb{C}[(\mathbb{F}_{p^n}, +)]$, we have

$$pD_{\mathcal{R}} = \bar{r}_0 \mathcal{L}_{\mathcal{R}} + \bar{n}_0 \mathcal{L}_{\mathcal{N}} + \frac{p-1}{2} \mathbb{F}_{p^n}, \quad (3.3)$$

$$pD_{\mathcal{N}} = \bar{n}_0 \mathcal{L}_{\mathcal{R}} + \bar{r}_0 \mathcal{L}_{\mathcal{N}} + \frac{p-1}{2} \mathbb{F}_{p^n}. \quad (3.4)$$

We now divide the proof into two cases.

Case 1. $p \equiv 1 \pmod{4}$. In this case, \mathcal{R} is a $\left(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4}\right)$ PDS in the additive group of \mathbb{F}_p , we have the following equalities in $\mathbb{Z}[(\mathbb{F}_p, +)]$:

$$\mathcal{R}^2 = \frac{p-5}{4} \mathcal{R} + \frac{p-1}{4} \mathcal{N} + \frac{p-1}{2}, \quad (3.5)$$

$$\mathcal{N}^2 = \frac{p-1}{4} \mathcal{R} + \frac{p-5}{4} \mathcal{N} + \frac{p-1}{2}, \quad (3.6)$$

$$\mathcal{R}\mathcal{N} = \frac{p-1}{4} (\mathbb{F}_p \setminus \{0\}). \quad (3.7)$$

We now compute $\mathcal{L}_{\mathcal{R}}^2$. From definition we have

$$\mathcal{L}_{\mathcal{R}}^2 = \sum_{t,s \in \mathcal{R}} \mathcal{L}_t \mathcal{L}_s = \sum_{t,s \in \mathcal{R}, t+s \neq 0} \mathcal{L}_t \mathcal{L}_s + \sum_{t \in \mathcal{R}} \mathcal{L}_t \mathcal{L}_{-t}.$$

Now using Part (1) and (2) of Lemma 3.3, and noting that n is assumed to be even, we have

$$\mathcal{L}_{\mathcal{R}}^2 = u\sqrt{p}^n \sum_{t,s \in \mathcal{R}, t+s \neq 0} \mathcal{L}_v + \frac{p-1}{2} p^n,$$

where $v = (s^{1-\ell} + t^{1-\ell})^{\frac{1}{1-\ell}}$. Note that as s (respectively, t) runs through \mathcal{R} , so does $s^{1-\ell}$ (respectively, $t^{1-\ell}$). Now using (2.5), we have

$$\mathcal{L}_{\mathcal{R}}^2 = u\sqrt{p}^n \left(\frac{p-5}{4} \mathcal{L}_{\mathcal{R}} + \frac{p-1}{4} \mathcal{L}_{\mathcal{N}} \right) + \frac{p-1}{2} p^n. \quad (3.8)$$

Similarly, we have

$$\mathcal{L}_{\mathcal{N}}^2 = u\sqrt{p}^n \left(\frac{p-1}{4} \mathcal{L}_{\mathcal{R}} + \frac{p-5}{4} \mathcal{L}_{\mathcal{N}} \right) + \frac{p-1}{2} p^n, \quad (3.9)$$

$$\mathcal{L}_{\mathcal{R}} \mathcal{L}_{\mathcal{N}} = u\sqrt{p}^n \left(\frac{p-1}{4} \mathcal{L}_{\mathcal{R}} + \frac{p-1}{4} \mathcal{L}_{\mathcal{N}} \right). \quad (3.10)$$

Since $p \equiv 1 \pmod{4}$, we have $\bar{r}_0 = r_0$ and $\bar{n}_0 = n_0$. Now (2.3) becomes $pD_{\mathcal{R}} = r_0 \mathcal{L}_{\mathcal{R}} + n_0 \mathcal{L}_{\mathcal{N}} + \frac{p-1}{2} \mathbb{F}_{p^n}$. It follows that

$$\begin{aligned} \left(pD_{\mathcal{R}} - \frac{p-1}{2} \mathbb{F}_{p^n} \right)^2 &= (r_0 \mathcal{L}_{\mathcal{R}} + n_0 \mathcal{L}_{\mathcal{N}})^2 \\ &= r_0^2 \mathcal{L}_{\mathcal{R}}^2 + n_0^2 \mathcal{L}_{\mathcal{N}}^2 + 2r_0 n_0 \mathcal{L}_{\mathcal{R}} \mathcal{L}_{\mathcal{N}}. \end{aligned}$$

Using (3.8), (2.9) and (2.10), we have

$$\left(pD_{\mathcal{R}} - \frac{p-1}{2} \mathbb{F}_{p^n} \right)^2 = \frac{p^2-1}{4} p^n + u\sqrt{p}^n \left(pD_{\mathcal{R}} - \frac{p-1}{2} \mathbb{F}_{p^n} \right).$$

By (1.3), we see that $D_{\mathcal{R}}$ is a PDS in $(\mathbb{F}_{p^n}, +)$. Similar computations show that $D_{\mathcal{N}}$ also satisfies the same equation in $\mathbb{Z}[(\mathbb{F}_{p^n}, +)]$, i.e.,

$$\left(pD_{\mathcal{N}} - \frac{p-1}{2} \mathbb{F}_{p^n} \right)^2 = \frac{p^2-1}{4} p^n + u\sqrt{p}^n \left(pD_{\mathcal{N}} - \frac{p-1}{2} \mathbb{F}_{p^n} \right).$$

Therefore $D_{\mathcal{N}}$ is also a PDS in $(\mathbb{F}_{p^n}, +)$.

Now note that $pD_0 = \mathcal{L}_0 + \mathcal{L}_{\mathcal{R}} + \mathcal{L}_{\mathcal{N}}$. So

$$p^2 D_0^2 = \mathcal{L}_0^2 + \mathcal{L}_{\mathcal{R}}^2 + \mathcal{L}_{\mathcal{N}}^2 + 2\mathcal{L}_0 \mathcal{L}_{\mathcal{R}} + 2\mathcal{L}_0 \mathcal{L}_{\mathcal{N}} + 2\mathcal{L}_{\mathcal{R}} \mathcal{L}_{\mathcal{N}}.$$

Using (3.8), (2.9), (2.10) and the fact that $\mathcal{L}_0 = \mathbb{F}_{p^n}$, we have

$$p^2 D_0^2 = (-p^n + 2p|D_0| - u\sqrt{p}^n(p-2))\mathbb{F}_{p^n} + up(p-2)\sqrt{p}^n D_0 + (p-1)p^n.$$

This shows that D_0 is a PDS in $(\mathbb{F}_{p^n}, +)$. Hence $D_0 \setminus \{0\}$ is also a PDS in $(\mathbb{F}_{p^n}, +)$.

Case 2. $p \equiv 3 \pmod{4}$. In this case, \mathcal{R} is a $\left(p, \frac{p-1}{2}, \frac{p-3}{4}\right)$ difference set in $(\mathbb{F}_p, +)$. Hence we have the following equalities in $\mathbb{Z}[(\mathbb{F}_p, +)]$:

$$\begin{aligned}\mathcal{R}^2 &= \frac{p-3}{4}\mathcal{R} + \frac{p+1}{4}\mathcal{N}, \\ \mathcal{N}^2 &= \frac{p+1}{4}\mathcal{R} + \frac{p-3}{4}\mathcal{N}, \\ \mathcal{R}\mathcal{N} &= \frac{p+1}{4} + \frac{p-3}{4}\mathbb{F}_p.\end{aligned}$$

By computations similar to those in Case 1, we now have

$$\begin{aligned}\mathcal{L}_{\mathcal{R}}^2 &= u\sqrt{-p}^n \left(\frac{p-3}{4}\mathcal{L}_{\mathcal{R}} + \frac{p+1}{4}\mathcal{L}_{\mathcal{N}} \right), \\ \mathcal{L}_{\mathcal{N}}^2 &= u\sqrt{-p}^n \left(\frac{p+1}{4}\mathcal{L}_{\mathcal{R}} + \frac{p-3}{4}\mathcal{L}_{\mathcal{N}} \right), \\ \mathcal{L}_{\mathcal{R}}\mathcal{L}_{\mathcal{N}} &= u\sqrt{-p}^n \left(\frac{p-3}{4}\mathcal{L}_{\mathcal{R}} + \frac{p-3}{4}\mathcal{L}_{\mathcal{N}} \right) + \frac{p-1}{2}p^n.\end{aligned}$$

Now we can compute $\left(pD_{\mathcal{R}} - \frac{p-1}{2}\mathbb{F}_{p^n}\right)^2$ by using (2.3) and the above three equalities. We have

$$\left(pD_{\mathcal{R}} - \frac{p-1}{2}\mathbb{F}_{p^n}\right)^2 = \frac{p^2-1}{4}p^n + u\sqrt{-p}^n \left(pD_{\mathcal{R}} - \frac{p-1}{2}\mathbb{F}_{p^n}\right).$$

Similarly, we have

$$\left(pD_{\mathcal{N}} - \frac{p-1}{2}\mathbb{F}_{p^n}\right)^2 = \frac{p^2-1}{4}p^n + u\sqrt{-p}^n \left(pD_{\mathcal{N}} - \frac{p-1}{2}\mathbb{F}_{p^n}\right).$$

and

$$p^2D_0^2 = (-p^n + 2p|D_0| - u\sqrt{-p}^n(p-2))\mathbb{F}_{p^n} + up(p-2)\sqrt{-p}^nD_0 + (p-1)p^n.$$

We have shown that D_0 , $D_{\mathcal{R}}$ and $D_{\mathcal{N}}$ are all PDS in $(\mathbb{F}_{p^n}, +)$. The proof is now complete. \square

Most of the known examples of p -ary weakly regular bent functions are either quadratic forms or ternary (i.e., $p = 3$). One can find a table in [25] which summarizes the known examples at that time. After [25] appeared, Helleseth and Kholosha [16] constructed a class of p -ary weakly regular bent functions f from $\mathbb{F}_{p^{4m}}$ to \mathbb{F}_p , where p is an arbitrary odd prime and f is not a quadratic form on $\mathbb{F}_{p^{4m}}$. One can apply Theorem 3.5 to this new class of p -ary weakly regular bent functions to obtain partial difference sets. Here we only want to demonstrate

the applicability of Theorem 3.5 and we are not concerned with the inequivalence issues of the PDS constructed.

Next we prove that the PDS in Theorem 3.5 lead to amorphic association schemes. The quickest way to prove this result is to invoke the following theorem from [9, 10].

Theorem 3.6. ([9, 10]) *Let $\{G_1, G_2, G_3\}$ form a strongly regular decomposition of the complete graph. Then $\{G_1, G_2, G_3\}$ forms an amorphic 3-class association scheme.*

Combining Theorem 3.5 and Theorem 3.6, the following corollary is immediate.

Corollary 3.7. *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be a weakly regular bent function. Assume that the Walsh coefficients of f satisfy (3.1) and there exists a constant k with $\gcd(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$ and all $x \in \mathbb{F}_{p^n}$. Furthermore, assume that n is even. Then the three Cayley graphs $\text{Cay}(G, D_0 \setminus \{0\})$, $\text{Cay}(G, D_{\mathcal{R}})$ and $\text{Cay}(G, D_{\mathcal{N}})$, where $G = (\mathbb{F}_{p^n}, +)$, form a 3-class amorphic association scheme on \mathbb{F}_{p^n} .*

Acknowledgement. After we finished this paper in Jan. 2010, we were informed that Chee, Tan and Zhang [8] also discovered the construction of PDS from weakly regular p -ary bent functions in Section 3 independently.

References

- [1] E. Bannai and A. Munemasa, Davenport-Hasse theorem and cyclotomic association schemes, in: Proc. Algebraic Combinatorics, Hirosaki University, 1990.
- [2] L. D. Baumert, M. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory **14** (1982), 67–82.
- [3] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, A Wiley-Interscience Publication, 1998.
- [4] A. E. Brouwer, Some new two-weight codes and strongly regular graphs, Discrete Appl. Math. **10** (1985), 111–114.
- [5] A. E. Brouwer A. M. Cohen and A. Neumaier, Distance Regular Graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 18. Springer-Verlag, Berlin, 1989.
- [6] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. **18** (2) (1986), 97–122.
- [7] P. J. Cameron, Finite geometry and coding theory, Lecture Notes for Socrates Intensive Programme “Finite Geometries and Their Automorphisms”, Potenza, Italy, 1999.
- [8] Y. M. Chee, Y. Tan and X. D. Zhang, Strongly regular graphs constructed from p -ary bent functions, Journal of Algebraic Combinatorics, to appear.
- [9] E. R. van Dam, Strongly regular decompositions of the complete graph, J. Alg. Comb. **17** (2003), 181–201.

- [10] E. R. van Dam and M. Muzychuk, Some implications on amorphic association schemes, *J. Comb. Theory (A)* **117** (2010), 722–737.
- [11] J. A. Davis and Q. Xiang, Amorphic association schemes with negative Latin square type graphs, *Finite Fields and Appl.* **12** (2006), 595–612.
- [12] J. F. Dillon, Elementary Hadamard Difference Sets, Ph.D. dissertation, University of Maryland, College Park, 1974.
- [13] K. Q. Feng and J. Q. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, *IEEE Transactions on Information Theory* **53** (2007), 3035–3041.
- [14] N. Hamilton, Strongly regular graphs from differences of quadrics, *Discrete Math.* **256** (2002), 465–469.
- [15] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Transactions on Information Theory* **52** (2006), 2018–2032.
- [16] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, [arXiv:0907.3348v1](https://arxiv.org/abs/0907.3348v1).
- [17] T. Ito, A. Munemasa and M. Yamada, Amorphous association schemes over the Galois rings of characteristic 4, *Europ. J. Comb.* **12** (1991), 513–526.
- [18] A. V. Ivanov, Amorphous cellular rings II, in: *Investigations in Algebraic Theory of Combinatorial Objects*, VNIISI, Moscow, Institute for System Studies, 1985, 39–49 (in Russian).
- [19] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *J. Comb. Theory (A)* **40** (1985), 90–107.
- [20] D. B. Leep and L. M. Schuellerb, Zeros of a pair of quadratic forms defined over a finite field, *Finite Fields and Their Applications* **5** (1999), 157–176.
- [21] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.
- [22] G. Myerson, Period polynomials and Gauss sums, *Acta Arithmetica* **39** (1981), 251–264.
- [23] A. Pott, Y. Tan, T. Feng and S. Ling, Association schemes arising from bent functions, preprint.
- [24] O. S. Rothaus, On bent functions, *J. Comb. Theory (A)* **20** (1976), 300–305.
- [25] Y. Tan, A. Pott and T. Feng, Strongly regular graphs associated with ternary bent functions, *J. Comb. Theory (A)* **117** (2010), 668–682.
- [26] R. J. Turyn, Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319–346.
- [27] Q. Xiang, Recent progress in algebraic design theory, *Finite Fields and Appl.* **11** (2005), 622–653.