Journal of Combinatorial Theory, Series A 117 (2010) 668–682

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Journal of Combinatorial Theory

Strongly regular graphs associated with ternary bent functions

Yin Tan [a,1], Alexander Pott [b], Tao Feng [c,2]

[a] School of Mathematical Sciences, Peking University, 100871 Beijing, China
[b] Department of Mathematics, Otto-von-Guericke-University, 39106 Magdeburg, Germany
[c] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 637371 Singapore

ARTICLE INFO

Article history:
Received 31 July 2008
Available online 16 June 2009

Keywords:
Bent functions
Partial difference sets
Strongly regular graphs
Association schemes

ABSTRACT

We prove a new characterization of weakly regular ternary bent functions via partial difference sets. Partial difference sets are combinatorial objects corresponding to strongly regular graphs. Using known families of bent functions, we obtain in this way new families of strongly regular graphs, some of which were previously unknown. One of the families includes an example in [N. Hamada, T. Helleseth, A characterization of some $\{3v_2+v_3, 3v_1+v_2, 3, 3\}$-minihypers and some $[15, 4, 9; 3]$-codes with $B_2 = 0$, J. Statist. Plann. Inference 56 (1996) 129–146], which was considered to be sporadic; using our results, this strongly regular graph is now a member of an infinite family. Moreover, this paper contains a new proof that the Coulter–Matthews and ternary quadratic bent functions are weakly regular.

1. Introduction

In this paper we describe a new connection between partial difference sets and ternary weakly regular bent functions.

Partial difference sets (see the definition in Section 2.2) have been studied extensively because of their connections with other combinatorial objects such as two-weight codes and strongly regular graphs. We refer the reader to [3,18] for details.

There are many constructions of partial difference sets in elementary abelian groups, and recently some have also been constructed in non-elementary abelian groups, see [18,9] for details. It is well

E-mail addresses: tanyin@math.pku.edu.cn (Y. Tan), Alexander.Pott@ovgu.de (A. Pott), FengTao@ntu.edu.sg (T. Feng).

[1] Supported partially by China Scholarship Council.

[2] Supported by NTU Grant No. 58110003.

0097-3165/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2009.05.003

known that partial difference sets can be used to construct strongly regular graphs (see the definition in Section 2.2). In this paper, we are going to construct partial difference sets whose strongly regular graphs (SRG) are of Latin square type and of negative Latin square type. For the precise definitions, see Section 2.2.

Boolean bent functions, first introduced by Rothaus [23], have been extensively studied because of their importance in cryptography. Such functions have the maximum Hamming distance to the set of all affine functions. In [15], the authors generalized Boolean bent functions to the case of finite fields of arbitrary characteristic (see Section 2.3). Bent functions $f:\mathbb{F}_p^n \to \mathbb{F}_p$ are those functions whose Walsh coefficients have absolute value $p^{n/2}$ (see Section 2.3 for the definition of Walsh coefficients). In this paper we are interested in weakly regular bent functions. These are functions where the Walsh coefficients take just the values $\mu p^{n/2}\zeta_p^i$, where $\zeta_p = e^{2\pi \mathrm{i}/p}$ is a complex p-th root of unity and μ is a complex number of absolute value 1. For the precise definition of weakly regularity, see Section 2.3.

We will show (Theorem 1) that a bent function $f:\mathbb{F}_3^{2m} \to \mathbb{F}_3$ which satisfies $f(-x) = f(x)$ and $f(0) = 0$ is weakly regular if and only if the sets $D_1 := \{x \in \mathbb{F}_3^n \mid f(x) = 1\}$ and $D_2 := \{x \in \mathbb{F} \mid f(x) = 2\}$ are partial difference sets with the same parameters. Therefore, ternary bent functions can be used to construct partial difference sets, hence strongly regular graphs.

The partial difference sets constructed from ternary bent functions also correspond to projective two-weight codes. We will not discuss this connection further, but refer to [3].

There are two very interesting classes of ternary bent functions: One class is derived from the Coulter–Matthews planar functions, see [7], and the other one is constructed in [12], see the table in Section 2.3. It seems that the strongly regular graphs of negative Latin square type corresponding to these families are new. We can check this (by computer) only for small graphs, but we are quite sure that the SRGs of negative Latin square type are new in general. One of our families contains a sporadic example due to Hamada and Helleseth [11], therefore we generalize the Hamada–Helleseth strongly regular graph to an infinite family.

It seems not to be easy to check whether a p-ary bent function is weakly regular or not. In [12], Helleseth and Kholosha proved that all quadratic p-ary bent functions are weakly regular, and all known monomial p-ary bent functions are weakly regular, except possibly the Coulter–Matthews bent functions and a newly found family in [12]. It was conjectured that these two families are weakly regular, too. Finally, this has been proven in [13]. Our characterization of ternary bent functions (Theorem 1) through partial difference sets gives an alternative proof for the weak regularity of the Coulter–Matthews bent functions (Theorem 2).

The paper is organized as follows. In Section 2, we give the definitions and results used in this paper. Section 3 contains the main theorems and proofs. We discuss the “newness” of the strongly regular graphs constructed from ternary bent functions in Section 4.

2. Preliminaries

2.1. Group rings and characters

Group rings are a very useful tool to study difference set problems, the reader may refer to any good textbook on algebra for basic facts and notations, see [20] for instance. Let $\mathbb{F}$ be an arbitrary field, and let G be a multiplicatively written abelian group with identity element 1_G. We restrict ourselves to abelian groups since these are the only groups which will appear throughout this paper.

We identify a subset S of G with the group ring element $\sum_{s\in S} s$, which will also be denoted by S (by abuse of notation). For $A = \sum_{g\in G} a_g g \in \mathbb{F}[G]$ and t an integer, we define $A^{(t)} := \sum_{g\in G} a_g g^t$.

A *character* χ of a finite abelian group G is a homomorphism from G to $\mathbb{C}^*$, the multiplicative group of $\mathbb{C}$. A character χ is called *principal* if $\chi(g) = 1$ for all $g \in G$, otherwise it is called *non-principal*. All characters form a group which is denoted by $\widehat{G}$ and called the *character group* $\widehat{G}$ which is isomorphic to G.

By linearity, we extend each character $\chi \in \widehat{G}$ to a homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we still denote this homomorphism by χ. The following are the well-known orthogonality relations for characters.

Result 1 *(Orthogonality relations).* Let G be a finite abelian group and $\widehat{G}$ be its character group. Then the following hold:

$$\sum_{g\in G}\chi(g)=\begin{cases}0 & \text{if } \chi \text{ is non-principal,}\\ |G| & \text{if } \chi \text{ is principal;}\end{cases}$$

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}0 & \text{if } g\neq 1_G,\\ |G| & \text{if } g=1_G.\end{cases}$$

Corollary 1 *(Inversion formula). If $A=\sum_{g\in G}a_g g$ in $\mathbb{C}[G]$, then*

$$a_g=\sum_{\chi\in\widehat{G}}\chi(A)\chi\left(g^{-1}\right).$$

If $G=\mathbb{F}_p^m$ is elementary abelian, there are two possibilities to describe characters. We may identify $\mathbb{F}_p^m$ with the additive group of the finite field $\mathbb{F}_{p^m}$. Let $\mathrm{Tr}:\mathbb{F}_{p^m}\to\mathbb{F}_p$ be the absolute trace function, i.e. $\mathrm{Tr}(x):=\sum_{i=0}^{m-1}x^{p^i}$. Define $\chi_1:\mathbb{F}_{p^m}\to\mathbb{C}$ as $\chi_1(x):=\zeta_p^{\mathrm{Tr}(x)}$ for all $x\in\mathbb{F}_{p^m}$. Then χ_1 is an additive character of $\mathbb{F}_{p^m}$. Moreover, every additive character χ is of the form χ_β ($\beta\in\mathbb{F}_{p^m}$), where χ_β is defined by $\chi_\beta(x)=\chi_1(\beta x)$ for all $x\in\mathbb{F}_{p^m}$.

If we do not want to identify $\mathbb{F}_p^m$ with the additive group of a field, characters are simply the mappings $x\mapsto\zeta_p^{\langle b,x\rangle}$ ($b\in\mathbb{F}_p^m$) where $\langle\,,\rangle$ denotes the standard inner product. Using any of these descriptions of the characters, it is easy to see that $G\cong\widehat{G}$.

If $G=H_1\times H_2$, then $\widehat{G}\cong\widehat{H_1}\times\widehat{H_2}$. If $\mu_1\in\widehat{H_1}$ and $\mu_2\in\widehat{H_2}$, then the mapping $(\mu_1,\mu_2):H_1\times H_2\to\mathbb{C}$ with $(\mu_1,\mu_2)(h_1,h_2):=\mu_1(h_1)\cdot\mu_2(h_2)$ is a character of G, and all characters can be written in this form.

2.2. Partial difference sets and strongly regular graphs

Let G be a multiplicative group of order v. A k-subset D of G is a (v,k,λ,μ) *partial difference set* (PDS) if each non-identity element in D can be represented as gh^{-1} ($g,h\in D$, $g\neq h$) in exactly λ ways, and each non-identity element in $G\setminus D$ can be represented as gh^{-1} ($g,h\in D$, $g\neq h$) in exactly μ ways. We shall always assume that the identity element 1_G of G is not contained in D. The terminology "partial difference set" is quite common, even if the groups are written multiplicatively.

In group ring notation, a k-subset D of G is a (v,k,λ,μ)-partial difference set if and only if the following group ring equation holds in $\mathbb{C}[G]$ (see [18]):

$$DD^{(-1)}=(k-\mu)1_G+(\lambda-\mu)D+\mu G \quad\text{and}\quad D^{(-1)}=D.$$

Using a simple counting argument, we have the following necessary condition for the parameter set (v,k,λ,μ):

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

We may apply characters to the equation above and obtain the following character theoretic characterization of partial difference sets:

Result 2. (See [18].) Let G be an abelian group of order v. Suppose D is a k-subset such that $D^{(-1)}=D$, $1\notin D$. Then D is a (v,k,λ,μ)-PDS if and only if for every non-principal character χ of G,

$$\chi(D)=\frac{\beta\pm\sqrt{\Delta}}{2},$$

where $\beta=\lambda-\mu$, $\gamma=k-\mu$ and $\Delta=\beta^2+4\gamma$.

Combinatorial objects associated with partial difference sets are strongly regular graphs: A graph Γ with v vertices is called a (v,k,λ,μ) *strongly regular graph* (SRG) if each vertex is adjacent to exactly k other vertices, and if any two adjacent vertices have exactly λ common neighbors, and two non-adjacent vertices have exactly μ common neighbors.

Given a group G of order v and a k-subset D of G with $1_G \notin D$ and $D^{(-1)} = D$, the graph $\Gamma = (V,E)$ defined as follows is called the *Cayley graph* generated by D:

(1) The vertex set V is G;
(2) Two vertices g,h are joined by an edge if and only if $gh^{-1} \in D$.

A Cayley graph generated by D is strongly regular if and only if D is a PDS with $D^{(-1)} = D$:

Result 3. (See [18].) Let Γ be the Cayley graph generated by a k-subset D of a finite multiplicative group G. Then Γ is a (v,k,λ,μ) strongly regular graph if and only if D is a (v,k,λ,μ)-PDS with $1 \notin D$ and $\{d^{-1} \mid d \in D\} = D$.

The parameters of SRGs have to satisfy some necessary conditions. In this paper, we consider only SRGs which are of Latin square or negative Latin square type. Strongly regular graphs (or partial difference sets) with parameters $(n^2, r(n+\varepsilon), -\varepsilon n + r^2 + 3\varepsilon r, r^2 + \varepsilon r)$ are called of *Latin square type* if $\varepsilon = -1$, and *negative Latin square type* if $\varepsilon = 1$. There are many constructions of SRGs of Latin square type (any collection of $r-1$ mutually orthogonal Latin squares gives rise to such a graph, see [18], for instance), but only a few constructions of negative Latin square type seem to be known. We will show that weakly regular ternary bent functions can be used to construct PDSs of Latin square and of negative Latin square type.

2.3. Bent functions

In this section and throughout the rest of the paper, we identify the group $\mathbb{F}_p^m$ with the additive group of the finite field $\mathbb{F}_{p^m}$. This has the advantage that we may use the multiplicative structure of $\mathbb{F}_{p^m}$ to define functions on $\mathbb{F}_p^m$, as we will see below.

For a prime p, we define a primitive complex p-th root of unity $\zeta_p := e^{\frac{2\pi \mathrm{i}}{p}}$. Let f be a function $\mathbb{F}_{p^m} \to \mathbb{F}_p$. The *Walsh transform* of f is the complex-valued function $\mathcal{W}_f : \mathbb{F}_{p^m} \to \mathbb{C}$ defined by

$$\mathcal{W}_f(\beta) := \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x)+\mathrm{Tr}(\beta x)}, \quad \beta \in \mathbb{F}_{p^m}.$$

The function f is called *p-ary bent* if every Walsh coefficient $\mathcal{W}_f(\beta)$ has magnitude $p^{m/2}$, i.e. $|\mathcal{W}_f(\beta)| = p^{m/2}$ for all $\beta \in \mathbb{F}_{p^m}$. The classical examples of p-ary bent functions are the *quadratic* ones. For background about quadratic functions on finite fields, we refer to [16].

We call a bent function f *regular* if there exists some function $f^* : \mathbb{F}_{p^m} \to \mathbb{F}_p$ such that $\mathcal{W}_f(\beta) = p^{m/2}\zeta_p^{f^*(b)}$, and f is called to be *weakly regular* if $\mathcal{W}_f(\beta) = \mu p^{m/2}\zeta^{f^*(b)}$ for some constant $\mu \in \mathbb{C}$ with $|\mu| = 1$. There are restrictions on the existence of regular bent functions: They can only exist when m is even, or m is odd and $p \equiv 1 \bmod 4$, see [15]. All quadratic bent functions are (weakly) regular, see [12].

Since bent functions exist for all p and m, there are many bent functions which are not regular. The situation is different for the weak regularity: Many families of bent functions seem to be weakly regular. In particular, all known *monomial* bent functions are weakly regular except one sporadic example in [12]. We say that a p-ary function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is *monomial* if there is an integer d and an element $\alpha \in \mathbb{F}_{p^m}$ such that $f(x) = \mathrm{Tr}(\alpha x^d)$. A well-rounded treatment of the regularity properties of the known monomial p-ary bent functions is [12].

Helleseth and Kholosha gave a table of the known families of monomial p-ary bent functions of the form $\mathrm{Tr}(\alpha x^d)$ $(\alpha \in \mathbb{F}_{p^m}^*)$ over $\mathbb{F}_{p^m}$. We record Table 1 here for the convenience of the reader. In

Table 1

Bent functions	m	d	α
Sidelnikov (wr)	Arbitrary	2	$\alpha \neq 0$
p-ary Kasami (wr)	$2k$	p^k+1	$\alpha + \alpha^{p^k} \neq 0$
K–M (wr)	Arbitrary	p^j+1, $\frac{n}{(n,j)}$-odd	$\alpha \neq 0$
C–M (wr)	Arbitrary	$\frac{3^k+1}{2}$, $(k,2n)=1$	$\alpha \neq 0$
p-ary Gold (wr)	Arbitrary	p^j+1	$\alpha^{\gcd(2j,m)} - 1 \nmid \frac{p^m-1}{2} - i_0(p^j-1)$
Ternary Dillon (r)	$2k$	$t(3^k-1)$, $(t, 3^k+1)=1$	$\sum_{c \in \mathbb{F}^*_{p^{m/2}}} \zeta_3^{\mathrm{Tr}(c+\alpha^{3^k+1}c^{-1})} = -1$
H–K (wr)	$2k$, k odd	$\frac{3^m-1}{4} + 3^k + 1$	$\alpha = \xi^{\frac{3^k+1}{4}}$

Table 1, r (resp. wr) means that the bent function is regular (resp. weakly regular), and $\alpha = \xi^{i_0}$ where ξ is a primitive element in $\mathbb{F}_{p^n}$.

Some remarks are in order: First of all, "C–M" stands for "Coulter–Matthews", "K–M" for Kumar–Moreno, and "H–K" for Helleseth–Kholosha". Please see [12] for references. Moreover, the weak regularity of the C–M family and the H–K family has been proved in [13].

We say that a function $f : \mathbb{F}_p^m \to \mathbb{F}_p^n$ is *quadratic* if for all $a \neq 0$, the mapping $x \mapsto f(x+a) - f(x)$ is nonzero and linear (here n is not necessarily 1). We note that the C–M, the H–K and the Dillon functions are the only non-quadratic bent functions in Table 1.

2.4. Relative difference sets and planar functions

In this section, we briefly describe the connection between p-ary bent functions and relative difference sets.

Let G be a group of order mn, and let N be a subgroup of order n. A k-subset R of G is called an (m,n,k,λ)-*relative difference set* (RDS) in G relative to N if every element $g \in G \setminus N$ can be represented in exactly λ ways in the form $r_1 r_2^{-1}$ ($r_1, r_2 \in R$, $r_1 \neq r_2$), and no non-identity element in N has such a representation. In the language of group rings, a k-subset R of G is an (m,n,k,λ)-RDS in G relative to N if and only if

$$RR^{(-1)} = k + \lambda(G - N) \quad \text{in } \mathbb{C}[G]. \tag{2}$$

If χ is a complex-valued character of an abelian group, then $\chi(R^{(-1)}) = \overline{\chi(R)}$, i.e. $\chi(R^{(-1)})$ is the complex conjugate of $\chi(R)$. If we apply complex characters to (2), we get

$$\left|\chi(R)\right|^2 = \begin{cases} k^2 & \text{if } \chi \text{ is principal,} \\ k - n\lambda & \text{if } \chi \text{ is non-principal, but } \chi \text{ is principal on } N, \\ k & \text{if } \chi \text{ is non-principal on } N. \end{cases} \tag{3}$$

Similar to Result 2, we have a characterization of relative difference sets using characters

Result 4. (See [22].) Let G be a group of order mn and $N < G$ a subgroup of order n. A subset of R is a relative (m,n,k,λ)-difference set in G relative to N if and only if (3) holds for all characters.

If R is a relative (m,n,m,λ)-difference set in $H \times N$, then R defines a function $f : H \to N$: For $h \in H$, there is precisely one element $n_h \in N$ such that $(h, n_h) \in R$, hence we may define $f(h) := n_h$. Conversely, any function $f : H \to N$ defines an m-set $R_f := \{(h, f(h)) \mid h \in H\}$. Note that in the case $m = k$ we have $\lambda = m/n$, which can be seen by an easy counting argument. The following proposition is easy to prove and well known, see [22], for instance.

Proposition 1. *A set R is an (m,n,m,λ)-difference set in $H \times N$ if and only if the corresponding function f has the following property: the equation $f(x+a) - f(x) = b$ has precisely λ solutions x for all non-identity $a \in H$ and all $b \in N$.*

If $f:\mathbb{F}_p^m \to \mathbb{F}_p$, then the character values of $R_f \in \mathbb{C}[\mathbb{F}_p^m \times \mathbb{F}_p]$ are

$$\sum_{x\in\mathbb{F}_p^m} \zeta_p^{\alpha f(x)+\mathrm{Tr}(\beta x)}$$

for $\alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_{p^m}$, where $\zeta = e^{\frac{2\pi \mathrm{i}}{p}}$. If $\alpha \neq 0$, then the character χ is non-principal on $\{0\} \times \mathbb{F}_p$. The character values of R_f (with $\alpha = 1$) are precisely the Walsh coefficients of f. This implies, using Result 4, the following well-known proposition:

Proposition 2. *The set R is a relative (p^m, p, p^m, p^{m-1})-difference set in an elementary abelian group if and only if the corresponding function is p-ary bent.*

The functions corresponding to $(n, n, n, 1)$-relative difference sets in $H \times N$ are called *planar*. Planar functions have the property that all the mappings $x \mapsto f(x+a) - f(x)$ are bijective. All *known* planar functions are between elementary abelian groups. If $f:\mathbb{F}_p^m \to \mathbb{F}_p^m$ is planar, then $x \mapsto \mathrm{Tr}(\alpha f(x))$ is p-ary bent for all $\alpha \neq 0$, hence planar functions give rise to many bent functions. With the exception of the Coulter–Matthews planar function, all known planar functions are quadratic.

We need the following highly nontrivial result on the Walsh coefficients of planar functions:

Result 5. (See [10].) Let p be an odd prime. Define

$$W_K^+ := \{\zeta_p^i \mid 0 \leqslant i \leqslant p-1\}, \qquad W_K^- := \{-\zeta_p^i \mid 0 \leqslant i \leqslant p-1\}$$

where $\zeta_p = e^{\frac{2\pi \mathrm{i}}{p}}$. Suppose f is a planar function which is quadratic or of Coulter–Matthews type. Then for all $\alpha \in \mathbb{F}^*$ and $\beta \in \mathbb{F}$, we have

$$\mathcal{W}_{\mathrm{Tr}(\alpha f)}(\beta) = \varepsilon_{\alpha,\beta}(\sqrt{p^*})^m, \quad \varepsilon_{\alpha,\beta} \in W_K^+ \cup W_K^-,$$

where $\varepsilon_{\alpha,0} \in \{\pm 1\}$, $p^* = (-1)^{\frac{p-1}{2}} p$ and $\varepsilon_{\alpha,\beta} \cdot \varepsilon_{\alpha,0} \in W_K^+$.

2.5. Amorphic association schemes

Let V be a finite set of vertices, and let $\{R_0, R_1, \ldots, R_d\}$ be binary relations on V with $R_0 := \{(x,x)\colon x \in V\}$. The configuration $(V; R_0, R_1, \ldots, R_d)$ is called an *association scheme* of class d on V if the following hold:

(1) $V \times V = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$.
(2) ${}^tR_i = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where ${}^tR_i := \{(x,y)\colon (y,x) \in R_i\}$. If $i' = i$, we call R_i is symmetric.
(3) For $i, j, k \in \{0, 1, \ldots, d\}$, the number $\sharp\{z \in V \mid (x,z) \in R_i,\ (z,y) \in R_j\}$ is a constant, which is denoted by p_{ij}^k.

An association scheme is said to be *symmetric* if every R_i is symmetric.

Given an association scheme $(V, \{R_l\}_{0\leqslant l\leqslant d})$, we can take the union of classes to form schemes with larger sets (this is called *fusion*), but it is not necessarily guaranteed that the fused collection of relations 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*. Van Dam [8] could prove the following result:

Result 6. Let V be a set of size v, and let $\{G_1, G_2, \ldots, G_d\}$ be an edge-decomposition of the complete graph on V, where each G_i is a strongly regular graph on V. If G_i, $1 \leqslant i \leqslant d$, 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.

Using Result 6, we will construct a family of amorphic association schemes on the additive group of the finite field $\mathbb{F}_3^{2m}$ (Theorem 3).

3. Main results

We first introduce some notations. Let $\mathbb{F}$ be the Galois field $\mathbb{F}_{3^{2m}}$ with $m \geqslant 2$, and let ξ be a primitive element in $\mathbb{F}$. Moreover, $\zeta_3 = e^{2\pi \mathrm{i}/3}$ is a complex third root of unity. Denote by G and H the additive group of $\mathbb{F}_{3^{2m}}$ and $\mathbb{F}_3$ respectively. Let $f : \mathbb{F} \to \mathbb{F}_3$ be a ternary bent function satisfying $f(-x) = f(x)$. We define

$$D_i := \{x \in \mathbb{F} \mid f(x) = i\}, \quad 0 \leqslant i \leqslant 2.$$

Clearly, $D_0 + D_1 + D_2 = G$. We may assume $f(0) = 0$ without loss of generality, since otherwise we may replace $f(x)$ by $f(x) - f(0)$. For $\beta \in \mathbb{F}^*$, we have $\chi_\beta(D_0) + \chi_\beta(D_1) + \chi_\beta(D_2) = 0$, see Result 1. From $f(-x) = f(x)$ we get $D_i = D_i^{(-1)}$ for each i, hence $\chi_\beta(D_i) = \overline{\chi_\beta(D_i)}$. Since $\chi_\beta(D_i) \in \mathbb{Z}[\zeta_3]$, we have $\chi_\beta(D_i) \in \mathbb{Z}$. Since f is a bent function from G to H, the set $R := \{(x, f(x)) \mid x \in G\}$ is a $(3^{2m}, 3, 3^{2m}, 3^{2m-1})$-RDS in $G \times H$ relative to H, see Proposition 2. By the definition of D_i, we have $R = (D_0, 0) + (D_1, 1) + (D_2, 2)$. Let η be the character of H which maps 1 to ζ_3, and define $(\chi_\beta, \eta) : G \times H \to \mathbb{C}$ by $(\chi_\beta, \eta)(x, y) = \chi_\beta(x)\eta(y)$. Then (χ_β, η) is a character of $G \times H$, and we have

$$(\chi_\beta, \eta)(R) = \chi_\beta(D_0) + \chi_\beta(D_1)\zeta_3 + \chi_\beta(D_2)\zeta_3^2. \tag{4}$$

Using (4) and $1 + \zeta_3 + \zeta_3^2 = 0$, we have

$$(\chi_\beta, \eta)(R) = \bigl(-\chi_\beta(D_1) - 2\chi_\beta(D_2)\bigr) + \bigl(\chi_\beta(D_1) - \chi_\beta(D_2)\bigr)\zeta_3. \tag{5}$$

On the other hand,

$$\begin{aligned} \mathcal{W}_f(\beta) &= \sum_{x \in D_0} \chi_\beta(x) + \sum_{x \in D_1} \chi_\beta(x)\xi_3 + \sum_{x \in D_2} \chi_\beta(x)\xi_3^2 \\ &= \chi_\beta(D_0) + \chi_\beta(D_1)\xi_3 + \chi_\beta(D_2)\xi_3^2 \\ &= (\chi_\beta, \eta)(R). \end{aligned} \tag{6}$$

If $\beta = 0$, we get

$$\begin{aligned} \mathcal{W}_f(0) &= (\chi_0, \eta)(R) \\ &= |D_0| + |D_1|\zeta_3 + |D_2|\zeta_3^2 \\ &= \bigl(3^{2m} - |D_1| - 2|D_2|\bigr) + \bigl(|D_1| - |D_2|\bigr)\zeta_3. \end{aligned}$$

The last step uses $|D_0| + |D_1| + |D_2| = 3^{2m}$ and $1 + \zeta_3 + \zeta_3^2 = 0$. Since f is a bent function, $|\mathcal{W}_f(0)|^2 = 3^{2m}$, i.e.

$$\bigl(\bigl(3^{2m} - |D_1| - 2|D_2|\bigr) + \bigl(|D_1| - |D_2|\bigr)\xi\bigr)\bigl(\overline{\bigl(3^{2m} - |D_1| - 2|D_2|\bigr) + \bigl(|D_1| - |D_2|\bigr)\xi}\bigr) = 3^{2m}.$$

Simplifying the above equation and denoting $|D_1|$, $|D_2|$ by x, y, respectively, we get

$$x^2 + xy - 3^{2m}x + y^2 - 3^{2m}y = 3^{2m-1} - 3^{4m-1}. \tag{7}$$

Next we give a lemma to determine the cardinalities of D_1 and D_2.

Lemma 1. *The integer solutions (x, y) of the equation $x^2 + xy - 3^{2m}x + y^2 - 3^{2m}y = 3^{2m-1} - 3^{4m-1}$ are given by*

$$\begin{aligned} &\bigl(3^{2m-1} + 3^{m-1}, 3^{2m-1} + 3^{m-1}\bigr), && \bigl(3^{2m-1} + 3^{m-1}, 3^{2m-1} - 2 \cdot 3^{m-1}\bigr), \\ &\bigl(3^{2m-1} - 3^{m-1}, 3^{2m-1} - 3^{m-1}\bigr), && \bigl(3^{2m-1} + 3^{m-1}, 3^{2m-1} + 2 \cdot 3^{m-1}\bigr), \\ &\bigl(3^{2m-1} + 2 \cdot 3^{m-1}, 3^{2m-1} - 3^{m-1}\bigr), && \bigl(3^{2m-1} - 2 \cdot 3^{m-1}, 3^{2m-1} + 3^{m-1}\bigr). \end{aligned}$$

Proof. Suppose $3^i \parallel x$, i.e. $3^i \mid x$ but $3^{i+1} \nmid x$. We may assume $i \leqslant m-1$. Assume otherwise $3^m \mid x$. Then $3^{2m-1} \mid x^2+xy-3^{2m}x+y^2-3^{2m}y$ implies $3^{2m-1} \mid y(x+y)$, hence $3^m \mid y$, which contradicts to $x^2+xy-3^{2m}x+y^2-3^{2m}y=3^{2m-1}-3^{4m-1}$.

If $3^i \parallel x$ with $i \leqslant m-1$, then $x^2+xy-3^{2m}x+y^2-3^{2m}y \equiv 0 \bmod 3^{2i}$ and hence $y(x+y) \equiv 0 \bmod 3^{2i}$. This shows $3^i \mid y$. If $3^{i+1} \mid y$, then the same arguments show that $3^{i+1} \mid x$ which is false. Hence $3^i \parallel y$. Write $x=3^ix'$, $y=3^iy'$, with x', y' not divisible by 3. Then (7) becomes

$$x'^2+x'y'-3^{2m-i}x'+y'^2-3^{2m-i}y'=3^{2m-2i-1}-3^{4m-2i-1}, \tag{8}$$

which is a quadratic equation in x':

$$x'^2+x'\bigl(y'-3^{2m-i}\bigr)+y'^2-3^{2m-i}y'-3^{2m-2i-1}+3^{4m-2i-1}=0. \tag{9}$$

The discriminant of (9) is

$$\Delta=3\bigl(4\cdot 3^{2m-2i-2}-\bigl(y'-3^{2m-i-1}\bigr)^2\bigr).$$

Since x is an integer, the discriminant Δ must be a positive square. If $i<m-1$, $3 \nmid -(y'-3^{2m-i-1})^2+4\cdot 3^{2m-2i-2}$ since $3 \nmid y'$. Therefore, i must be $m-1$. In this case, (7) can be expressed as:

$$x'^2+x'\bigl(y'-3^{m+1}\bigr)+y'^2-3^{m+1}y'-3+3^{2m+1}=0. \tag{10}$$

Its discriminant is now equal to $\Delta=-3(y'-3^m)^2+12$. If (7) has an integer solution, then $\Delta \geqslant 0$ which implies $y'=3^m \pm 1$ or $3^m \pm 2$.

Since $x'=\frac{-(y'-3^{m+1})\pm\sqrt{\Delta}}{2}$, we know that if $y'=3^m+1$, then

$$x'=\frac{-(3^m+1-3^{m+1})\pm 3}{2}=3^m+1 \text{ or } 3^m-2.$$

The same argument shows if $y'=3^m-1$, we have $x'=3^m-1$ or 3^m+2. If $y'=3^m+2$, note now $\Delta=0$, and $x'=\frac{-(3^m+2-3^{m+1})}{2}=3^m-1$. Similarly, when $y'=3^m-2$, we have $x'=3^m+1$. □

Now we return to the determination of $|D_1|$ and $|D_2|$. We assume $f(0)=0$ and $f(-x)=f(x)$. Then it is clear that $D_1^{(-1)}=D_1$, $D_2^{(-1)}=D_2$ and $0 \notin D_1, D_2$, hence $|D_1|$, $|D_2|$ should be even integers. This shows that the only possible solution pairs are $(3^{2m-1}+3^{m-1}, 3^{2m-1}+3^{m-1})$ and $(3^{2m-1}-3^{m-1}, 3^{2m-1}-3^{m-1})$. Thus we have proved:

Corollary 2. *Let $f:\mathbb{F}\to\mathbb{F}_3$ be a ternary bent function satisfying $f(-x)=f(x)$ and $f(0)=0$. Define $D_i:=\{x\in\mathbb{F} \mid f(x)=i\}$ for each $0\leqslant i\leqslant 2$. Then $|D_1|=|D_2|=3^{2m-1}+3^{m-1}$ or $|D_1|=|D_2|=3^{2m-1}-3^{m-1}$.*

Since f is a ternary bent function over $\mathbb{F}_{3^{2m}}$, and by (4), we have

$$3^{2m}=(\chi_\beta,\eta)(R)\overline{(\chi_\beta,\eta)(R)}=3\bigl(\chi_\beta(D_1)^2+\chi_\beta(D_2)^2+\chi_\beta(D_1)\chi_\beta(D_2)\bigr).$$

We obtain

$$\chi_\beta(D_1)^2+\chi_\beta(D_2)^2+\chi_\beta(D_1)\chi_\beta(D_2)=3^{2m-1}. \tag{11}$$

Using similar arguments as in Lemma 1, we have the following lemma:

Lemma 2. *The integer solutions (x,y) of the equation $x^2+y^2+xy=3^{2m-1}$ are given by ($\delta:=3^{m-1}$)*

$$(\delta,\delta),\quad (\delta,-2\delta),\quad (-2\delta,\delta),\quad (-\delta,-\delta),\quad (-\delta,2\delta),\quad (2\delta,-\delta).$$

This lemma shows that $\chi(D_1), \chi(D_2)\in\{\pm\delta,\pm 2\delta\}$ for any non-principal character χ of G. We are now ready to prove our first main theorem:

Theorem 1. *Let $\mathbb{F}$ be the Galois field $\mathbb{F}_{3^{2m}}$ with $m\geqslant 2$. Let $f:\mathbb{F}\to\mathbb{F}_3$ be a ternary bent function satisfying $f(-x)=f(x)$ and $f(0)=0$. Define $D_i:=\{x\in\mathbb{F} \mid f(x)=i\}$ for each $0\leqslant i\leqslant 2$. Then the following hold:*

(1) *f is weakly regular if and only if D_1 and D_2 are both*

$$\left(3^{2m}, 3^{2m-1} + \varepsilon 3^{m-1}, 3^{2m-2}, 3^{2m-2} + \varepsilon 3^{m-1}\right)\text{-}PDSs, \tag{12}$$

where $\varepsilon = \pm 1$ (the choice of ε for D_1 and D_2 should be the same).

(2) *The set $D := D_0 \setminus \{0\}$ is a*

$$\left(3^{2m}, 3^{2m-1} - 1 - 2\varepsilon 3^{m-1}, 3^{2m-2} - 2\varepsilon 3^{m-1} - 2, 3^{2m-2} - \varepsilon 3^{m-1}\right)\text{-}PDS, \tag{13}$$

where we have to choose the same ε as in the first part of the theorem.

Proof. For each $\beta \in \mathbb{F}^*$, the Walsh coefficient $\mathcal{W}_f(\beta)$ is

$$\begin{aligned}\mathcal{W}_f(\beta) &= \chi_\beta(D_0) + \chi_\beta(D_1)\zeta_3 + \chi_\beta(D_2)\zeta_3^2 \\ &= -\left(\chi_\beta(D_1) + \chi_\beta(D_2)\right) + \chi_\beta(D_1)\zeta_3 + \chi_\beta(D_2)(-1 - \zeta_3) \\ &= -\left(\chi_\beta(D_1) + 2\chi_\beta(D_2)\right) + \left(\chi_\beta(D_1) - \chi_\beta(D_2)\right)\zeta_3.\end{aligned}$$

Since f is a ternary bent function, we have shown that for each non-principal character χ_β of $G := (\mathbb{F}, +)$, $(\chi_\beta(D_1), \chi_\beta(D_2))$ must be one of the six cases in Lemma 2. For each of these cases, we compute the corresponding $\mathcal{W}_f(\beta)$ below:

$$\begin{array}{lll}
(1) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (\delta, \delta): & \mathcal{W}_f(\beta) = -3\delta = -3^m; \\
(2) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (\delta, -2\delta): & \mathcal{W}_f(\beta) = -3^m\xi_3^2; \\
(3) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (-2\delta, \delta): & \mathcal{W}_f(\beta) = -3^m\xi_3; \\
(4) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (-\delta, -\delta): & \mathcal{W}_f(\beta) = 3^m; \\
(5) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (2\delta, -\delta): & \mathcal{W}_f(\beta) = 3^m\xi_3; \\
(6) & \left(\chi_\beta(D_1), \chi_\beta(D_2)\right) = (-\delta, 2\delta): & \mathcal{W}_f(\beta) = 3^m\xi_3^2.
\end{array}$$

Therefore, the six cases are divided into two classes according to whether $\mathcal{W}_f(\beta)/3^m$ is in W_K^- or W_K^+, where W_K^-, W_K^+ are defined in Result 5. The first class consists of (δ, δ), $(\delta, -2\delta)$, $(-2\delta, \delta)$, and the second class consists of their negatives.

"⇒" By Lemma 1, $|D_1| = |D_2| = 3^{2m-1} + \varepsilon 3^{m-1}$. If f is weakly regular, we see from the above computations that there is some $f^* : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ and $\mu = \pm 1$ such that $\mathcal{W}_f(\beta) = \mu 3^m \zeta_3^{f^*(\beta)}$. Therefore, $(\chi_\beta(D_1), \chi_\beta(D_2))$ must lie in the same class for all β. In the case that $(\chi_\beta(D_1), \chi_\beta(D_2))$ lie in the first class, we see that $\chi_\beta(D_1)$ and $\chi_\beta(D_2)$ can only take the values δ and -2δ, so it is a partial difference set by Result 2. The size of D_1 and D_2 is $k_\pm = 3^{2m-1} \pm 3^{m-1}$. We can compute the parameters of the putative partial difference sets from the character values and the k-value using Result 2. It turns out that in the case $k = 3^{2m-1} - 3^{m-1}$, the parameters do not satisfy the trivial necessary conditions (1), hence $|D_1|$ must be $3^{2m-1} + 3^{m-1}$ and the parameters are of negative Latin square type.

The case that $(\chi_\beta(D_1), \chi_\beta(D_2))$ is in the second class is similar, and the parameters are $(3^{2m}, 3^{2m-1} - 3^{m-1}, 3^{2m-2}, 3^{2m-2} - 3^{m-1})$ of Latin square type.

"⇐" If D_1 and D_2 are both $(3^{2m}, 3^{2m-1} + 3^{m-1}, 3^{2m-2}, 3^{2m-2} + 3^{m-1})$-partial difference sets, then

$$\left(\chi_\beta(D_1), \chi_\beta(D_2)\right) \in \left\{(\delta, \delta), (\delta, -2\delta), (-2\delta, \delta), (-2\delta, -2\delta)\right\}$$

for any non-principal additive character χ_β where $\beta \in \mathbb{F}_{3^{2m}}^*$ and $\delta = 3^{m-1}$ by Result 2. If $(\chi_\beta(D_1), \chi_\beta(D_2)) = (-2\delta, -2\delta)$, we have $\mathcal{W}_f(\beta) = 2 \cdot 3^m$ by a direct computation. Since f is bent and the magnitude of $\mathcal{W}_f(\beta)$ is 3^m, this case is impossible. For each of the three remaining cases, we see that $\mathcal{W}_f(\beta) = -3^m \zeta_3^{f^*(\beta)}$ for some function $f^* : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$. In the case $\beta = 0$, $\mathcal{W}_f(0) = |D_0| + |D_1|\zeta_3 + |D_2|\zeta_3^2 = 3^{2m} - 3|D_1| = -3^m$ since $|D_1| = |D_2|$ and $D_0 + D_1 + D_2 = G$. Thus for any $\beta \in \mathbb{F}_{3^{2m}}$, the Walsh coefficients $\mathcal{W}_f(\beta) = -3^m \zeta_3^{f^*(\beta)}$ for some function $f^* : \mathbb{F} \to \mathbb{F}_3$, which means that f is weakly regular. The case that D_1, D_2 are both $(3^{2m}, 3^{2m-1} - 3^{m-1}, 3^{2m-2}, 3^{2m-2} - 3^{m-1})$-partial difference sets is similar.

Now let us prove the second part for the case $\varepsilon = 1$. The case $\varepsilon = -1$ is similar. We know that D_1 and D_2 are both negative Latin square type PDSs. Since $D = \mathbb{F} - D_1 - D_2 - 0$ in group ring notation, we know $|D| = 3^{2m-1} - 2 \cdot 3^{m-1} - 1$. Moreover, for any non-principal additive character χ_β of $\mathbb{F}$, we have $\chi_\beta(D) = -(\chi_\beta(D_1) + \chi_\beta(D_2) + 1)$. If D_1, D_2 are both $(3^{2m}, 3^{2m-1} + 3^{m-1}, 3^{2m-2}, 3^{2m-2} + 3^{m-1})$-PDSs, then $(\chi_\beta(D_1), \chi_\beta(D_2)) \in \{(\delta, \delta), (\delta, -2\delta), (-2\delta, \delta)\}$, where $\delta = 3^{m-1}$. Therefore, $\chi_\beta(D) = -(\chi_\beta(D_1) + \chi_\beta(D_2) + 1) \in \{2\delta - 1, -\delta - 1\}$. Result 2 finishes the proof. □

Remark 1.

(1) In the case $\varepsilon = 1$, the PDSs D_0, D_1, D_2 are all of negative Latin square type, if $\varepsilon = -1$ they are of Latin square type.
(2) We will show (see Proposition 3) that D_1 and D_2 are equivalent if the function $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ is weakly regular of the form $\mathrm{Tr}(\alpha x^d)$, where $\alpha \in \mathbb{F}_{3^{2n}}$ and $(d, 3^{2n} - 1) = 2$.

The above result characterizes the regularity property of ternary bent functions using partial difference sets. The next result shows that PDSs can be constructed from special types of ternary bent functions. The proof is relatively easy since most of the work has been done in [10]. We emphasize that our proof does not make use of the weak regularity of quadratic or Coulter–Matthews bent functions.

Theorem 2. *Let $g(x)$ be a planar function which is quadratic or of Coulter–Matthews type, and fix an $\alpha \in \mathbb{F}_{3^{2m}}^*$. Define $D_i := \{x \in \mathbb{F}_{3^{2m}} \mid \mathrm{Tr}(\alpha g(x)) = i\}$ for $0 \leqslant i \leqslant 2$. Then D_1, D_2 are both $(3^{2m}, 3^{2m-1} + \varepsilon 3^{m-1}, 3^{2m-2}, 3^{2m-2} + \varepsilon 3^{m-1})$-partial difference sets with $\varepsilon = \pm 1$ (the choice of ε for D_1 and D_2 is the same).*

Proof. The function $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ defined by $f(x) = \mathrm{Tr}(\alpha g(x))$ is a ternary bent function. It follows that $(\chi_\beta(D_1), \chi_\beta(D_2))$ can only be one of the six cases in the proof of Theorem 1. By Result 5, $\mathcal{W}_f(\beta) = \varepsilon_{\alpha,b} 3^m$ where $\varepsilon_{\alpha,0} \in \{\pm 1\}$ and $\varepsilon_{\alpha,b} \cdot \varepsilon_{\alpha,0} \in W_K^+$. Since α is fixed here, we see that $(\chi_\beta(D_1), \chi_\beta(D_2))$ must be in the same class. Now the result follows as in the proof of Theorem 1. □

Using Theorems 1 and 2, we get another proof of the weak regularity of Coulter–Matthews and ternary quadratic bent functions, which is, through Theorem 2, based on the work by Feng and Luo [10].

Corollary 3. *The Coulter–Matthews and ternary quadratic bent functions are weakly regular.*

Remark 2. (1) For an arbitrary p-ary weakly regular bent functions $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ with $p \geqslant 5$, the subsets

$$D_i := \{x \in \mathbb{F}_{p^{2m}} \mid f(x) = i\}, \quad 1 \leqslant i \leqslant p - 1,$$

are not necessarily PDSs. For instance, if we take the bent function $f : \mathbb{F}_{5^4} \to \mathbb{F}_5$ defined by $f(x) = \mathrm{Tr}(x^2)$, then the set $D_i = \{x \mid f(x) = i\}$ is not a partial difference set for each $i \in \{1, 2, 3, 4\}$ (checked by MAGMA [1]). This shows that Theorem 1 cannot be generalized to primes $p \geqslant 5$.

(2) For an arbitrary p-ary bent function $f : \mathbb{F}_{p^{2m+1}} \to \mathbb{F}_p$, the subsets D_i are not necessarily PDSs (we may take $\mathrm{Tr}(x^2) : \mathbb{F}_{p^5} \to \mathbb{F}_p$, where $p = 3, 5$ as examples, and use MAGMA), hence we cannot generalize Theorem 1 to odd exponents.

(3) The ternary bent function $f(x) = \mathrm{Tr}(\xi^7 x^{98})$ in $\mathbb{F}_{3^6}$ is not weakly regular, see [12]. The corresponding sets D_i are not partial difference sets, which can be verified by MAGMA, again. This shows that the assumption of the weak regularity in Theorem 1 is essential.

Finally, we use ternary weakly regular bent functions to construct a family of amorphic association schemes.

Theorem 3. *Let $\mathbb{F}$ be the Galois field $\mathbb{F}_{3^{2m}}$ with $m \geqslant 2$. Let $f : \mathbb{F} \to \mathbb{F}_3$ be a ternary weakly regular bent function satisfying $f(-x) = f(x)$ and $f(0) = 0$. Define $D_i := \{x \in \mathbb{F} \mid f(x) = i\}$ for each $0 \leqslant i \leqslant 2$, and let $D = D_0 \setminus \{0\}$. Then the decomposition $\{D, D_1, D_2\}$ is a 3-class amorphic association scheme on $\mathbb{F}$.*

Proof. This follows from Theorem 1 and Result 6. □

4. Newness

In this section, we discuss the known constructions of the strongly regular graphs of negative Latin square type with parameters

$$\left(3^{2m}, 3^{2m-1} + 3^{m-1}, 3^{2m-2}, 3^{2m-2} + 3^{m-1}\right), \tag{14}$$

and

$$\left(3^{2m}, 3^{2m-1} - 1 - 2 \cdot 3^{m-1}, 3^{2m-2} - 2 \cdot 3^{m-1} - 2, 3^{2m-2} - 3^{m-1}\right). \tag{15}$$

Such graphs can be constructed from Theorem 1. We show that the negative Latin square type SRGs constructed via non-quadratic ternary bent functions over $\mathbb{F}_{3^{2m}}$ using Theorem 1 are, to the best of our knowledge, new for small m. We do not discuss the SRGs of Latin square type constructed via Theorem 1 in detail, since it seems that there are many constructions of such graphs, and it is not that important to know whether our construction produces one more class. The negative Latin square type is more interesting.

4.1. Equivalence of partial difference sets

Two graphs $\mathcal{G}_1 = (V_1, E_1)$, $\mathcal{G}_2 = (V_2, E_2)$ are said to be *isomorphic* if there exists a bijection σ which maps V_1 to V_2, and E_1 to E_2 such that for each pair of $(P, e) \in V_1 \times E_1$, we have $\sigma(P) \in \sigma(e)$ if and only if $P \in e$.

Let D_1, D_2 be two partial difference sets in a group G. The partial difference sets D_1, D_2 are said to be *CI-equivalent* if there exists an automorphism $\phi \in Aut(G)$ such that $\phi(D_1) = D_2 g$ for some $g \in G$. The sets D_1, D_2 are said to be *SRG-equivalent* if the corresponding Cayley graphs are isomorphic, i.e., $\mathrm{Cay}(G, D_1) \cong \mathrm{Cay}(G, D_2)$. It is clear that CI-equivalence implies SRG-equivalence. The converse is not true: there are examples [14] of PDSs which are SRG-equivalent but not CI-equivalent. We first show that the partial difference sets D_1 and D_2 constructed from Theorem 1 are CI-equivalent, at least if they are monomial:

Proposition 3. *Let $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ defined by $f(x) := \mathrm{Tr}(\alpha x^d)$ be a weakly regular ternary bent function, where $(d, 3^{2m} - 1) = 2$. Let ξ be a primitive element of $\mathbb{F}_{3^{2m}}$. Define $D_i := \{x \in \mathbb{F}_{3^{2m}} \mid f(x) = i\}$, $1 \leqslant i \leqslant 2$. Then $D_1 = \xi^{\frac{3^{2m}-1}{4}} D_2$, hence D_1 and D_2 are CI-equivalent.*

Proof. Since $(d, 3^{2m} - 1) = 2$ and $\xi^{\frac{3^{2m}-1}{4}} = -1$, we have $(\xi^{\frac{3^{2m}-1}{4}})^d = -1$. For an arbitrary $x \in D_2$, we have $\mathrm{Tr}((\xi^{\frac{3^{2m}-1}{4}} x)^d) = \mathrm{Tr}(-x^d) = -2 = 1$, which implies $\xi^{\frac{3^{2m}-1}{4}} D_2 \subseteq D_1$. By Theorem 1, we know $|D_1| = |D_2|$, hence $\xi^{\frac{3^{2m}-1}{4}} D_2 = D_1$. □

The above proposition shows that the partial difference sets D_1 and D_2 which can be constructed from weakly ternary monomial bent functions according to Theorem 1 are isomorphic.

The following proposition discusses the equivalent issue for the SRGs constructed from weakly regular ternary bent functions $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ of the form $f(x) = \mathrm{Tr}(\alpha x^d)$, where $(d, p^{2m} - 1) = 2$ and $\alpha \in \mathbb{F}_{p^{2m}}$.

Proposition 4. *Let x^d be a function over $\mathbb{F} := \mathbb{F}_{p^{2m}}$ with $(d, p^{2m} - 1) = 2$, where p is an odd prime. Let $S := \{\alpha \in \mathbb{F}^* \mid \mathrm{Tr}(\alpha x^d)$ is bent$\}$, and define, for each $\alpha \in S$, $f_\alpha(x) := \mathrm{Tr}(\alpha x^d)$. Let $D_{\alpha,i} = \{x \in \mathbb{F} \mid f_\alpha(x) = i\}$*

for $0 \leqslant i \leqslant p-1$. If $\alpha, \beta \in S$ are both nonzero squares or both non-squares in $\mathbb{F}$, then there exists some $\lambda \in \mathbb{F}$ such that $D_{\alpha,i} = \lambda D_{\beta,i}$ for all $0 \leqslant i \leqslant p-1$.

Proof. First assume that $\alpha, \beta \in S$ are two nonzero squares. We only show that $D_{\alpha,i} = \lambda D_{\beta,i}$ for $\lambda \in \mathbb{F}^*$. Let $\alpha^{-1}\beta = \eta^2$. From $(d, p^{2m}-1) = 2$, we have $d = 2d'$ for some d' coprime with $p^{2m}-1$. Thus there exists some $\lambda \in \mathbb{F}$ such that $\lambda^{d'} = \eta$ which implies $\lambda^d = \eta^2 = \alpha^{-1}\beta$. Thus, for each $x \in D_{\beta,i}$, $\mathrm{Tr}(\alpha(\lambda x)^d) = \mathrm{Tr}(\beta x^d) = i$ which implies $\lambda x \in D_{\alpha,i}$. It follows that $D_{\alpha,i} \subseteq \lambda D_{\beta,i}$. It is clear that $|D_{\alpha,i}| = |D_{\beta,i}|$ since, using the same argument, there exists some $\lambda' \in \mathbb{F}$ such that $D_{\beta,i} \subseteq \lambda' D_{\alpha,i}$. Therefore we have $D_{\alpha,i} = \lambda D_{\beta,i}$. The case $\alpha, \beta \in S$ are both non-squares can be dealt with similarly. □

Corollary 4. *Let x^d be a function over $\mathbb{F} := \mathbb{F}_{3^{2m}}$ with $(d, 3^{2m}-1) = 2$. Let $S := \{\alpha \in \mathbb{F}^* \mid \mathrm{Tr}(\alpha x^d)$ is weakly regular bent$\}$, and define, for each $\alpha \in S$, $f_\alpha(x) := \mathrm{Tr}(\alpha x^d)$. Let $D_{\alpha,i} = \{x \in \mathbb{F} \mid f_\alpha(x) = i\}$ for $1 \leqslant i \leqslant 2$, and $D_{\alpha,0} = \{x \in \mathbb{F}^* \mid f_\alpha(x) = 0\}$. If $\alpha, \beta \in S$ are both nonzero squares or both non-squares in $\mathbb{F}$, then the PDSs $D_{\alpha,i}$, $D_{\beta,i}$ are CI-equivalent, and thus the SRGs generated by $D_{\alpha,i}$, $D_{\beta,i}$ are isomorphic.*

Note that by [7], we know that $(d, p^{2m}-1) = 2$ if x^d is planar over $\mathbb{F}_{p^{2m}}$, and for the monomial bent functions in Table 1 in Section 2.3.

4.2. Known constructions of SRGs with parameters (14)

One may check the known constructions with the parameters (14) via the online database [2], and two-weight codes via the online database [4]. We note that any projective two-weight code can be used to construct a PDS, hence a strongly regular graph, so we also looked at the known constructions of projective two-weight codes in order to check whether our examples are new.

Result 7. (See [3].) Let $k = 2m$ and $\mathcal{Q}$ be a non-degenerate quadratic form on $\mathbb{F}_q$ with q odd, and let $D = \{v \in \mathbb{F}_q^k \mid \mathrm{Tr}(\mathcal{Q}(v))$ is a nonzero square$\}$. Then the Cayley graph generated by D in $(\mathbb{F}_q^k, +)$ is a $(q^{2m}, q^{m-1}(q^m+\varepsilon), \frac{1}{2}q^{2m-2}(q-1), \frac{1}{2}q^{2m-2}(q-1) - \varepsilon q^{m-1})$-SRG. There are quadratic forms which give graphs with $\varepsilon = 1$ (hence the graphs are of negative Latin square type) and those which give graphs with $\varepsilon = -1$ (Latin square type).

The graphs are called *affine polar graphs*. They can be also constructed using projective two-weight codes. It is easy to check that these affine polar graphs can be constructed from quadratic bent functions. Both Latin square and negative Latin square types occur. To the best of our knowledge, this result and the paper [21] give the only two known infinite families of negative Latin square type SRGs with parameters (14).

When $m = 2$, we found only two non-isomorphic examples of SRGs with parameters (14) and $\varepsilon = 1$ in the literature: These are the affine polar graphs (which includes an example in [17]) as well as a sporadic example in [11]. The latter example due to Helleseth and Hamada was sporadic. As we will show below, it can be also constructed from the Coulter–Matthews bent functions, hence it is now, using Theorem 1, a member of an infinite family. For the two examples, the 3-rank of the adjacency matrices, and the orders of the automorphism groups of the SRGs are $(19, 116640)$ (affine polar graphs) and $(19, 5832)$ (Helleseth–Hamada).

When $m = 3$, we found only three SRGs of negative Latin square type with parameters (14) in the literature: The affine polar graphs, graphs which can be constructed by a projective two weight code due to Chen [5], and graphs constructed by Polhill in [21, Example 2]. The 3-rank of the adjacency matrices, and the orders of the automorphism groups of the SRGs are $(35, 2^{10} \cdot 3^{12} \cdot 5 \cdot 7)$ (affine polar graph), $(106, 2 \cdot 3^6 \cdot 7)$ (Chen) and $(59, 2^4 \cdot 3^9)$ (Polhill). Note that [21, Example 1] can also produce the SRG with these parameter, but it is isomorphic to the affine graph.

When $m \geqslant 4$, to our best knowledge the only known constructions of SRGs with parameters (14) is the quadratic one, i.e. the graphs are affine polar, and Polhill's construction, see [21, Corollary 5.1]. The 3-rank of the adjacency matrices, and the orders of automorphism groups of the Polhill's SRGs are $(54, 2^{12} \cdot 3^{20} \cdot 5 \cdot 7 \cdot 13 \cdot 41)$ and the graph is the affine polar graph, and $(90, 2^6 \cdot 3^{15} \cdot 5)$.

For the Latin square type partial difference sets with parameters $(3^{2m}, 3^{2m-1} - 3^{m-1}, 3^{2m-2}, 3^{2m-2} - 3^{m-1})$, there are many constructions, including the affine polar graphs [6, p. 855]. They can be also constructed from projective two-weight codes, for which there are many different constructions, see [3,18]. Here we do not compare all known Latin square type SRGs with the SRGs of our new construction, since there are so many examples. We think that our construction is much more interesting in the negative Latin square type.

4.3. *Known constructions of SRGs with parameter* (15)

We introduce two families of SRGs with parameter (15).

Result 8. (See [3].) Let $(,)$ be a non-singular Hermitian form on $V := \mathbb{F}_{q^2}^m$, and let $D = \{v \in V,\ v \neq 0 \mid (v, v) = 0\}$. Then the Cayley graph generated by D is a $(q^{2m}, (q^m - \varepsilon)(q^{m-1} + \varepsilon), (q-2) + q(q^{m-1} - \varepsilon)(q^{m-2} + \varepsilon), q^{2m-2} + \varepsilon q^{m-1})$-SRG, where $\varepsilon = (-1)^m$.

One may check that for $q = 3$ and odd l, Result 8 produces SRGs with parameter (15). The graphs constructed in Result 8 are called *RT3* in [3].

Result 9. (See [3].) Let $k = 2m$ and $\mathcal{Q}$ be a non-degenerate quadratic form on $\mathbb{F}_q$ with q odd, and let $D = \{v \in \mathbb{F}_q^k,\ v \neq 0 \mid \mathrm{Tr}(\mathcal{Q}(v)) = 0\}$. Then the Cayley graph generated by D in $(\mathbb{F}_q^k, +)$ is a $(q^{2m}, (q^m - \varepsilon)(q^{m-1} + \varepsilon), (q-2) + q(q^{m-1} - \varepsilon)(q^{m-2} + \varepsilon), q^{2m-2} + \varepsilon q^{m-1})$-SRG, where $\varepsilon = (-1)^{m+1}$.

The graphs constructed using Result 9 are also called, as in Result 9, *affine polar graphs*. One may check that for $q = 3$ and even m in Result 9, SRGs with parameter (15) arise.

By [18, Theorem 8.1], we know that SRGs with parameter (15) can also be constructed by using projective two-weight codes.

When $m = 2$, the parameters are $(81, 20, 1, 6)$, and this SRG is unique, see [6].

When $m = 3$, besides the strongly regular graph RT3 constructed above, $(729, 224, 61, 72)$-SRGs can be also constructed from projective two-weight codes. Since our construction using Theorem 1 does not give rise to new SRGs in this case (checked by MAGMA), we do not list the other constructions here.

When $m = 4$, to our knowledge, the known constructions of $(6561, 2132, 673, 702)$-SRGs are the affine polar graph and Polhill's construction, see [21, Examples 1, 2]. The 3-rank and the order of the automorphism groups of Polhill's constructions are $(6561, 2^{13} \cdot 3^{20} \cdot 5 \cdot 7 \cdot 13 \cdot 41)$ (and the graph is the affine polar graph), and $(6561, 2^7 \cdot 3^{15} \cdot 5)$. Using the Coulter–Matthews bent functions, we obtain another graph.

4.4. *Computational results for the SRGs of our construction*

Proposition 3 and Corollary 4 show that we may construct at most two different families of SRG's with parameters (12) from monomial bent functions. In the case of quadratic functions, this potential is realized: Both Latin square and negative Latin square type SRGs are constructed. In the Coulter–Matthews case, we obtain for small values of m both types of graphs, but we cannot prove this in general. The Dillon examples seem to produce only Latin square type graphs, but, again, we have no proof, yet.

In Tables 2–4, we list some properties of the SRGs constructed from the monomial bent functions listed in Table 1 in Section 2. In the first column, we list the bent function, the second column contains the parameters of the SRG's G, the group $Aut(\mathcal{G})$ is the full automorphism group of the graph $\mathcal{G}$, and M denotes an adjacency matrix of $\mathcal{G}$, to be considered over $\mathbb{F}_3$. The abbreviation n.L. (resp. L.) means that the SRG is of negative Latin square (resp. Latin square) type. As mentioned above, we did not care which isomorphism type of graph we obtain in the Latin square case. In Tables 2–4, the mark $\diamond$ means that the SRG is constructed by $D_0 \setminus \{0\}$ in Theorem 1.

In Table 4, we have two C–M planar functions over $\mathbb{F}_{3^8}$, which are x^{14}, x^{122}. Using MAGMA, we checked that the graphs corresponding to them are isomorphic.

Table 2

Bent functions in $\mathbb{F}_{3^4}$	(v, k, λ, μ)	Type	Rank of M	$\lvert Aut(\mathcal{G})\rvert$	Note
Quadratic	$(81, 30, 9, 12)$	n.L.	19	116 640	Affine polar
Quadratic	$(81, 24, 9, 6)$	L.	19	93 312	
Quadratic ◇	$(81, 20, 1, 6)$	n.L.	81	233 280	Affine polar
Quadratic ◇	$(81, 32, 13, 12)$	L.	81	186 624	
C–M	$(81, 30, 9, 12)$	n.L.	19	5832	≅ Helleseth–Hamada
C–M	$(81, 24, 9, 6)$	L.	19	23 328	
C–M ◇	$(81, 20, 1, 6)$	n.L.	81	233 280	≅ Affine polar
C–M ◇	$(81, 32, 13, 12)$	L.	81	186 624	
Dillon	$(81, 24, 9, 6)$	L.	19	23 328	
Dillon ◇	$(81, 32, 13, 12)$	L.	81	5184	

Table 3

Bent functions in $\mathbb{F}_{3^6}$	(v, k, λ, μ)	Type	Rank of M	$\lvert Aut(\mathcal{G})\rvert$	Note
Quadratic	$(729, 252, 81, 90)$	n.L.	35	$2^{10} \cdot 3^{12} \cdot 5 \cdot 7$	Affine polar
Quadratic	$(729, 234, 81, 72)$	L.	35	$2^{9} \cdot 3^{12} \cdot 5 \cdot 13$	
Quadratic ◇	$(729, 224, 61, 72)$	n.L.	729	$2^{11} \cdot 3^{12} \cdot 5 \cdot 7$	≅ RT3
Quadratic ◇	$(729, 260, 97, 90)$	L.	729	$2^{10} \cdot 3^{12} \cdot 5 \cdot 13$	
C–M	$(729, 252, 81, 90)$	n.L.	92	$2^{2} \cdot 3^{7}$	New
C–M	$(729, 234, 81, 72)$	L.	92	$2^{2} \cdot 3^{7}$	
C–M ◇	$(729, 224, 61, 72)$	n.L.	729	$2^{11} \cdot 3^{12} \cdot 5 \cdot 7$	≅ RT3
C–M ◇	$(729, 260, 97, 90)$	L.	729	$2^{10} \cdot 3^{12} \cdot 5 \cdot 13$	
Dillon	$(729, 234, 81, 72)$	L.	100	$2^{2} \cdot 3^{6} \cdot 13$	
Dillon ◇	$(729, 260, 97, 90)$	L.	729	$2^{3} \cdot 3^{6} \cdot 13$	
H–K	$(729, 252, 81, 90)$	n.L.	98	$2^{2} \cdot 3^{7} \cdot 7$	New
H–K ◇	$(729, 224, 61, 72)$	n.L.	729	$2^{11} \cdot 3^{12} \cdot 5 \cdot 7$	≅ RT3

Table 4

Bent functions in $\mathbb{F}_{3^8}$	(v, k, λ, μ)	Type	Rank of M	$\lvert Aut(\mathcal{G})\rvert$	Note
Quadratic	$(6561, 2214, 729, 756)$	n.L.	54	$2^{12} \cdot 3^{20} \cdot 5 \cdot 7 \cdot 13 \cdot 41$	Affine polar
Quadratic	$(6561, 2160, 729, 702)$	L.	54	$2^{15} \cdot 3^{20} \cdot 5^{2} \cdot 7 \cdot 13$	
Quadratic ◇	$(6561, 2132, 673, 702)$	n.L.	6561	$2^{13} \cdot 3^{20} \cdot 5 \cdot 7 \cdot 13 \cdot 41$	Affine polar
Quadratic ◇	$(6561, 2240, 781, 756)$	L.	6561	$2^{16} \cdot 3^{20} \cdot 5^{2} \cdot 7 \cdot 13$	
C–M	$(6561, 2214, 729, 756)$	n.L.	457	$2^{4} \cdot 3^{8}$	New
C–M	$(6561, 2160, 729, 702)$	L.	457	$2^{4} \cdot 3^{8}$	
C–M ◇	$(6561, 2132, 673, 702)$	n.L.	6561	$2^{5} \cdot 3^{8}$	New
C–M ◇	$(6561, 2240, 781, 756)$	L.	6561	$2^{5} \cdot 3^{8}$	
Dillon	$(6561, 2160, 729, 702)$	L.	498	$2^{5} \cdot 3^{8} \cdot 5$	
Dillon ◇	$(6561, 2240, 781, 756)$	L.	6561	$2^{6} \cdot 3^{8} \cdot 5$	

By Proposition 3, we know that p-ary bent functions are equivalent to the (p^n, p, p^n, p^{n-1})-RDS in $G \times H$ relative to H, where G is elementary abelian group of order p^n. There are many constructions of the RDSs, see [19] for instance. Using MAGMA, we found no RDS constructed from [19, Theorems 2.1, 2.2] which is weakly regular. However, we suggest to look at more non-monomial RDSs to see whether some of them are weakly regular.

Let $\mathcal{G}$ be the strongly regular graph constructed from (*weakly*) regular 3-ary bent function f by Theorem 1. Based on Table 4, we conjecture that the strongly regular graphs are pairwise non-isomorphic when f are quadratic, Coulter–Matthews and H–K bent functions. Moreover, we conjecture that the Coulter–Matthews bent functions can be used to construct two infinite families of SRGs, one of Latin square and one of negative Latin square type.

Acknowledgments

The authors thank the anonymous referees for their reviews containing valuable suggestions which helped to improve the manuscript significantly.

This work was done during the first author's visit at the Otto-von-Guericke-University. He would like to thank the hospitality of the Institute of Algebra and Geometry. He also thanks Prof. Qiu Weisheng for his encouragement.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 39–48.

[2] A.E. Brouwer, Web database of strongly regular graph, http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html (online).

[3] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (2) (1986) 97–122.

[4] E.Z. Chen, Web database of two-weight codes, http://moodle.tec.hkr.se/~chen/research/2-weight-codes/search.php (online).

[5] E.Z. Chen, Construction of two-weight codes, internal reports, 2008.

[6] Charles J. Colbourn, Jeffrey H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC Press, 2006.

[7] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.

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

[9] J.A. Davis, Q. Xiang, Negative Latin square type partial difference sets in nonelementary abelian 2-groups, J. London Math. Soc. (2) 70 (2004) 125–141.

[10] K.Q. Feng, J.Q. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inform. Theory 53 (9) (2007) 3035–3041.

[11] N. Hamada, T. Helleseth, A characterization of some $\{3v_2+v_3, 3v_1+v_2, 3, 3\}$-minihypers and some $[15, 4, 9; 3]$-codes with $B_2=0$, J. Statist. Plann. Inference 56 (1996) 129–146.

[12] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 52 (5) (2006) 2018–2032.

[13] T. Helleseth, H.D.L. Hollmann, A. Kholosha, Z.Y. Wang, Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, 2008, March 19; arXiv:0803.2878v1.

[14] H.A. Heinze, Applications of Schur rings in algebraic combinatorics: Graphs, partial difference sets and cyclotomy scheme, PhD thesis, University of Oldenburg, Germany, 2001.

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

[16] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, 1983.

[17] J.H. van Lint, A. Schrijver, Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields, Combinatorica 1 (1981) 63–73.

[18] S.L. Ma, A survey of partial difference sets, Des. Codes Cryptogr. 4 (1994) 221–261.

[19] S.L. Ma, B. Schmidt, On (p^a, p, p^a, p^{a-1})-relative difference sets, Des. Codes Cryptogr. 6 (1995) 57–71.

[20] Donald S. Passman, The Algebraic Structure of Group Rings, Wiley–Interscience, New York, 1977.

[21] J. Polhill, New negative Latin square type partial difference sets in nonelementary abelian 2-groups and 3-groups, Des. Codes Cryptogr. 46 (2008) 365–377.

[22] Alexander Pott, Finite Geometry and Character Theory, Springer-Verlag, Berlin/New York, 1995.

[23] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20 (1976) 300–305.