Association schemes arising from bent functions

Pott, Alexander; Tan, Yin; Feng, Tao; Ling, San

2011

Pott, A., Tan, Y., Feng, T., & Ling, S. (2011). Association schemes arising from bent functions. *Designs, Codes and Cryptography*, 59, 319-331.

<https://hdl.handle.net/10356/94475>

<https://doi.org/10.1007/s10623-010-9463-z>

© 2011 Springer. This is the author created version of a work that has been peer reviewed and accepted for publication by *Designs, Codes and Cryptography*, Springer. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: <http://dx.doi.org/10.1007/s10623-010-9463-z>

Downloaded on 26 Apr 2023 19:45:29 SGT

Association Schemes Arising from Bent Functions

Alexander Pott · Yin Tan · Tao Feng · San Ling

the date of receipt and acceptance should be inserted later

Abstract We give a construction of 3-class and 4-class association schemes from s -nonlinear and differentially 2^s -uniform functions, and a construction of p -class association schemes from weakly regular p -ary bent functions, where p is an odd prime.

1 Introduction

Association schemes (see the definition in Section 2.2) are a very important topic in combinatorial theory. They have applications in many areas of research, in particular in coding theory, see [Delsarte and Levenshtein(1998)], for instance. Association schemes were first introduced by Bose and Nair in [Bose and Nair(1939)]. After that, Bose and Shimamoto studied association schemes in statistical combinatorial designs, see [Bose and Shimamoto(1952)]. There are many methods to construct association schemes, see, for instance, [Bannai and Ito(1984), Delsarte(1973), Delsarte and Levenshtein(1998), Ma(1989)] and the references cited there. Recently, there are some constructions for association schemes using nonlinear functions [Budaghyan and Pott(2009), van Dam and Fon-Der-Flaass(2000)]. In this paper, we give some

The research of the second author has been partially supported by China Scholarship Council. The third and fourth author have been supported by NTU Grant No. 58110003, and the fourth author has been also supported by research grant NRF-CRP2-2007-03.

Alexander Pott
Department of Mathematics, Otto-von-Guericke-University
Magdeburg, D-39016 Magdeburg, Germany
E-mail: alexander.pott@ovgu.de

Yin Tan
School of Mathematical Sciences, Peking University,
100087 Peking, China
E-mail: tanyin@ntu.edu.sg

Tao Feng
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371

San Ling
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371

other constructions of association schemes from nonlinear and p -ary bent functions.

Functions which are s -nonlinear or differentially 2^s -uniform (see definitions in Section 2.3) are important research objects. In particular, we know that 1-nonlinear functions are the well known almost bent (AB) functions, and differentially 2-uniform functions are almost perfect nonlinear (APN) functions. In Section 3, we will use s -nonlinear and differentially 2^s -uniform functions to construct association schemes of class 3 and 4.

Boolean bent functions, first introduced by Rothaus [Rothaus(1976)] in 1976, 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 [Kumar et al(1985)Kumar, Scholtz, and Welch], the authors generalized Boolean bent functions to the case of finite fields of arbitrary characteristic (see Section 2.4). Bent functions $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ 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 $\zeta_p = e^{2\pi i/p}$ is a complex p -th root of unity and μ is a fixed complex number of absolute value 1. For the precise definition of weak regularity, see Section 2.4. In Section 4, a family of association schemes is constructed by using weakly regular p -ary bent functions, where p is an odd prime.

We organize the paper as follows. In Section 2, necessary definitions and results are given. Several families of 3-class and 4-class association schemes are discussed in Section 3. In Section 4, we use weakly regular p -ary bent functions to construct a family of association schemes of class p , where p is an odd prime.

2 Preliminaries

2.1 Group rings and character theory

The association schemes which we are going to construct can be best described using group rings $\mathbb{F}[G]$ where $\mathbb{F}$ is a field (in most cases the field $\mathbb{C}$ of complex numbers) and G a group (in our cases G will always be an elementary abelian group). We refer the reader to [Passman(1977)] or any good textbook on algebra for basic facts and notations.

We identify a subset S of G with the group ring element $\sum_{s \in S} s$ in $\mathbb{F}[G]$, 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 $\mathbb{C}^*$. A character χ is called *principal* if $\chi(c) = 1$ for all $c \in G$, otherwise it is called *non-principal*. We usually denote the principal character by χ_0 . All characters form a group denoted by $\hat{G}$. This *character group* is isomorphic to G . For a group ring element $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$

and a character $\chi \in \hat{G}$, we denote $\sum_{g \in G} a_g \chi(g)$ by $\chi(A)$. The following two equations are the *orthogonal relations* of characters:

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ |G| & \text{if } \chi = \chi_0; \end{cases}$$

and

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

By linearity, we extend each character $\chi \in \widehat{G}$ to a ring homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we denote this homomorphism by χ , again. Let $\mathbb{F}_{p^m}$ be the Galois field with p^m elements and $\text{Tr} : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ be the absolute trace function. Define $\chi_1 : \mathbb{F}_{p^m} \rightarrow \mathbb{C}$ as $\chi_1(x) := \zeta_p^{\text{Tr}(x)}$ 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_b ($b \in \mathbb{F}_{p^m}$), where χ_b is defined by $\chi_b(x) = \chi_1(bx)$ for all $x \in \mathbb{F}_{p^m}$. In particular, if $G = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, an isomorphism $\sigma : G \rightarrow \widehat{G}$ between the character group $\widehat{G}$ and G can be defined by $\sigma(u, v) = \chi_{u,v}$, where $\chi_{u,v}(a, b) = \zeta_p^{\text{Tr}(au+bv)}$ for any $(a, b) \in G$.

For a group ring element $M \in \mathbb{C}[G]$, the *Fourier transform* of M is the element $\widetilde{M} = \sum_{\chi \in \widehat{G}} \chi(M) \chi$ in $\mathbb{C}[\widehat{G}]$. It is easy to verify that $\widetilde{\widetilde{M}} = |G|M^{(-1)}$ by noting that $\widehat{\widehat{G}} \cong G$ and $g(\chi) := \chi(g)$ for any $g \in G$ defines a character of $\widehat{G}$, where $M^{(-1)} = \sum_{m \in M} m^{-1}$, as defined above.

2.2 Association schemes and Schur rings

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

- (1) $V \times V = R_0 \cup R_1 \cup \dots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$;
- (2) ${}^t R_i = R_{i'}$ for some $i' \in \{0, 1, \dots, d\}$, where ${}^t R_i := \{(x, y) : (y, x) \in R_i\}$. If $i' = i$, we call R_i symmetric.
- (3) for $i, j, k \in \{0, 1, \dots, d\}$ and $x, y \in V$ with $(x, y) \in R_k$, the number $\#\{z \in V : (x, z) \in R_i, (z, y) \in R_j\}$ is a constant, which is denoted by p_{ij}^k .

Furthermore, an association scheme is said to be *symmetric* if every R_i is symmetric.

A well-known approach to construct association schemes is to use Schur rings: Let G be a finite Abelian group and $D_0, \dots, D_d$ be nonempty subsets of G with the following properties:

- (1) $D_0 = \{1_G\}$, where 1_G is the identity element of G ;
- (2) $G = D_0 \cup D_1 \cup \dots \cup D_d$ and $D_i \cap D_j = \emptyset$ for $i \neq j$;
- (3) $D_i^{(-1)} = D_{i'}$ for some $i' \in \{0, \dots, d\}$, where $D_i^{(-1)} = \{g^{-1} : g \in D_i\}$;
- (4) $D_i D_j = \sum_{k=0}^d p_{ij}^k D_k$ for all $i, j \in \{0, \dots, d\}$, where p_{ij}^k are integers.

The subalgebra $\langle D_0, \dots, D_d \rangle$ of $\mathbb{C}[G]$ generated by $D_0, \dots, D_d$ is a so called *Schur ring* over G . The configuration $(G; R_0, \dots, R_d)$ forms an association scheme of class d on G , where $R_i := \{(g, h) : gh^{-1} \in D_i\}$ for $i \in \{0, \dots, d\}$. Note that if $D_i^{(-1)} = D_i$ for each i , the scheme is symmetric.

Assume $D_0, D_1, \dots, D_d$ span a Schur ring $\mathcal{L}$ over G . There are exactly $d+1$ equivalence classes $E_0 = \{\chi_0\}, E_1, \dots, E_d$, where for any two characters χ_1, χ_2 , $\chi_1 \sim \chi_2$ if and only if $\chi_1(D_i) = \chi_2(D_i)$ for all $i \in \{0, \dots, d\}$. Moreover, $E_0, E_1, \dots, E_d$ span a Schur ring

$\mathcal{L}^*$ over $\widehat{G}$ which is called the *dual* of $\mathcal{L}$ (see [Bannai and Ito(1984), Chapter II]).

It is well known that a 2-class symmetric association scheme is equivalent to a strongly regular graph, see [Bose and Shimamoto(1963)]. Strongly regular graphs can be constructed from partial difference sets, see [Ma(1994)] for a survey on partial difference sets. Let D be a k -subset of a group G of order v . Then D is called a (v, k, λ, μ) *partial difference set* (PDS) if the list of “differences” gh^{-1} , $g, h \in D$ ($g \neq h$) represent every non-identity element in D exactly λ times, and every non-identity element in $G \setminus D$ exactly μ times. The subset D is called *regular* if $D^{(-1)} = D$ and $1_G \notin D$. If χ is a non-principal character of G , then $\chi(D) \in \{a, b\}$, where $a, b = \frac{\lambda - \mu}{2} \pm \frac{1}{2} \sqrt{(\mu - \lambda)^2 + 4(k - \mu)}$, see [Ma(1994), Corollary 3.3]. Define the sets $D_a := \{\chi \in \widehat{G} | \chi(D) = a\}$, $D_b := \{\chi \in \widehat{G} | \chi(D) = b\}$, we call either of D_a, D_b the *dual* of D . The following result implies that both D_a and D_b are partial difference sets.

Proposition 1 [Delsarte(1973)] *Let G be an Abelian group of order v and D ($\neq \emptyset$ and $\neq G$) be a regular (v, k, λ, μ) -PDS in G . Then the dual D_a of D is a regular PDS in $\widehat{G}$ (the parameters are given in [Ma(1989)]).*

If D is a regular PDS, then $G \setminus (D \cup \{1_G\})$ is another regular PDS. It is called the *complement* of D . Therefore, the two PDS's D_a and D_b corresponding to the two different character values are complements of each other: For any non-principal character $\chi \in \widehat{G}$, we have $\chi(D) \in \{a, b\}$. Now $D_a = \{\chi : \chi(D) = a\}$ and $D_b = \{\chi : \chi(D) = b\}$, then clearly $D_a + D_b + \chi_0 = \widehat{G}$ which implies that D_a and D_b are complements of each other.

2.3 Walsh spectrum and differential spectrum

Next we introduce some basic concepts about nonlinear functions. Suppose f is a function from $\mathbb{F} := \mathbb{F}_{p^m}$ to $\mathbb{F}$ with p prime. Let ζ_p be a primitive complex p -th root of unity $\zeta_p := e^{\frac{2\pi i}{p}}$. We usually define the nonlinearity of functions in two different ways. Let $G := \mathbb{F} \times \mathbb{F}$ be the direct product of the additive group of $\mathbb{F}$. We define the *Walsh transform* $\lambda_f : G \rightarrow \mathbb{C}$ of f as follows:

$$\lambda_f(a, b) := \sum_{x \in \mathbb{F}} \zeta_p^{\text{Tr}(ax + bf(x))}, \quad a, b \in \mathbb{F},$$

where ζ_p is a primitive p -th root of unity, and Tr denotes the usual trace function. The set $\Lambda_f := \{\lambda_f(a, b) : a \in \mathbb{F}, b \in \mathbb{F}^*\}$ is called the *Walsh spectrum* of f , and each $\lambda_f(a, b)$ is called *Walsh coefficient*. In the case $p = 2$, we call f an *s-nonlinear function* if $\Lambda_f(a, b) = \{0, \pm 2^{\frac{m+s}{2}}\}$. Functions which are 1-nonlinear are also called *almost bent* (AB). Moreover, for the function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$, the Walsh transformation of f is defined as $\mathcal{W}_f : \mathbb{F}_{p^n} \rightarrow \mathbb{C}$, where $\mathcal{W}_f(a) := \sum_{x \in \mathbb{F}} \zeta_p^{f(x) + \text{Tr}(ax)}$.

Another concept of nonlinearity is the following: Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a function. We define

$$\delta_f(a, b) := \#\{x \in \mathbb{F} : f(x + a) - f(x) = b\},$$

and the set $\Delta_f := \{\delta_f(a, b) : a \in \mathbb{F}^*, b \in \mathbb{F}\}$ is called the *differential spectrum* of f . In the case $p = 2$, the function f is said to be a *differentially 2^s -uniform* function if $\Delta_f = \{0, 2^s\}$. Differentially 2-uniform functions are called *almost perfect nonlinear* (APN). If p is odd and $\Delta_f = \{1\}$, then f is called *perfect nonlinear* or *planar*. It is well known that f is planar if and only if $|\lambda_f(a, b)| = p^{m/2}$ for all $a \in \mathbb{F}, b \neq 0$, see [Pott(2004)], for instance.

2.4 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.

Let f be a function $\mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$. The function f is called *p-ary bent* if every Walsh coefficient $\mathcal{W}_f(b)$ has magnitude $p^{m/2}$, i.e. $|\mathcal{W}_f(b)| = p^{m/2}$ for all $b \in \mathbb{F}_{p^m}$. The classical examples of p -ary bent functions are the *quadratic* ones. For background about quadratic functions on finite fields, we refer to [Lidl and Niederreiter(1997)].

Proposition 2 *Any non-degenerate quadratic form Q on $\mathbb{F}_p^m$ is bent.*

Planar functions can be also used to construct bent functions:

Proposition 3 (see [Pott(2004)], for instance) *If $f : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ is planar, then the mappings $f_a(x) = \text{Tr}(\alpha f(x))$ are bent for all $a \in \mathbb{F}_{p^m}^*$.*

We call a bent function f *regular* if there exists some function $f^* : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ such that $\mathcal{W}_f(b) = p^{m/2} \zeta_p^{f^*(b)}$, and f is called to be *weakly regular* if $\mathcal{W}_f(b) = \mu p^{m/2} \zeta_p^{f^*(b)}$ for some constant $\mu \in \mathbb{C}$ with $|\mu| = 1$. We call f^* the *dual* function of f . Obviously, every regular function is also weakly regular. There are severe restrictions on the existence of regular bent functions: They can only exist when m is even, or m is odd and $p \equiv 1 \pmod{4}$, see [Kumar et al(1985)Kumar, Scholtz, and Welch]. All quadratic bent functions are (weakly) regular, see [Helleseht and Kholosha(2006)].

Since bent functions exist for **all** p and m , there are many bent functions which are not regular since they do not satisfy the aforementioned necessary conditions. The existence status of weakly regular bent functions is different from the existence of regular bent functions: 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 [Helleseht and Kholosha(2006)]: We say that a p -ary function $f : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ is *monomial* if there is an integer d and an element $\alpha \in \mathbb{F}_{p^m}$ such that $f(x) = \text{Tr}(\alpha x^d)$. A well-rounded treatment of the regularity properties of the known monomial p -ary bent functions is [Helleseht and Kholosha(2006)].

In [Helleseht and Kholosha(2006)], the authors gave a table of the known monomial p -ary bent functions of the form $\text{Tr}(\alpha x^d)$ ($\alpha \in \mathbb{F}_{p^n}^*$) over $\mathbb{F}_{p^n}$. We record the table here (Table 1) for the convenience of the reader. In the table, 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 $\mathbb{F}_{p^n}$. The HHKWX example has been conjectured in [Helleseht and Kholosha(2006)], and finally it was shown in [Helleseht et al(2008)Helleseht, Hollmann, Kholosha, Wang, and Xiang] that it is bent. Moreover, the weak regularity of this example as well as the weak regularity of the Coulter-Matthews example has been proven in [Helleseht et al(2008)Helleseht, Hollmann, Kholosha, Wang, and Xiang]. We note that the Sidelnikov and the Coulter Matthews examples correspond to planar functions as described in Proposition 3.

For the proof of the result in Section 4, we state some basic facts on the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ which can be found in [Ireland and Rosen(1990)]. The first statement in the following result means that every element in $\mathcal{O}_{\mathbb{K}}$ (which are the elements in $\mathbb{K}$ which are roots of integral monic polynomials in $\mathbb{Z}[x]$) can be expressed uniquely in the form $\sum_{i=0}^{p-2} a_i \zeta_p^i$, $a_i \in \mathbb{Z}$. The second part means that $\mathbb{K}$ has a unique quadratic subfield (which follows easily from the Galois correspondence between subfields and subgroups of the Galois group). The nontrivial part of the result is that we can explicitly describe this subfield as $\mathbb{Q}(\sqrt{p^*})$.

Table 1 Monomial bent functions

Bent Functions	m	d	α
Sidelnikov(wr)	arbitrary	2	$\alpha \neq 0$
p -ary Kasami (wr)	$2k$	$p^k + 1$	$\alpha + \alpha^{p^k} \neq 0$
Kumar-Moreno(wr)	arbitrary	$p^j + 1, \frac{m}{(m,j)} \text{ is odd}$	$\alpha \neq 0$
Coulter-Matthews(wr)	arbitrary	$\frac{3^k+1}{2}, (k, 2m) = 1$	$\alpha \neq 0$
p -ary Gold(wr)	arbitrary	$p^j + 1$	$p^{(2j,m)} - 1 \nmid (\frac{p^m-1}{2} - i_0(p^j - 1))$
p -ary Dillon(r)	$2k$	$t(3^k - 1), (t, 3^k + 1) = 1$	$\sum_{c \in \mathbb{F}_p^*} \xi_3^{Tr(c + \alpha^{3^k+1} c^{-1})} = -1$
HHKWX (wr)	$2k, k \text{ odd}$	$\frac{3^m-1}{4} + 3^k + 1$	$\alpha = \xi^{\frac{3^k+1}{4}}$

Result 1 (1) The ring of integers in $\mathbb{K} = \mathbb{Q}(\zeta_p)$ is $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ and $\{\zeta_p^i : 0 \leq i \leq p-2\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$. The group of roots of unity in $\mathcal{O}_{\mathbb{K}}$ is $W_{\mathbb{K}} = \{\pm \zeta_p^i : 0 \leq i \leq p-1\}$.

(2) The field $\mathbb{K}$ has a unique quadratic subfield $\mathbb{L} = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (\frac{-1}{p})p = (-1)^{\frac{p-1}{2}}p$ and for $1 \leq a \leq p-1$, $(\frac{a}{p})$ is the Legendre symbol. For $1 \leq a \leq p-1$, $\sigma_a(\sqrt{p^*}) = (\frac{a}{p})\sqrt{p^*}$. Therefore, $\text{Gal}(\mathbb{L}/\mathbb{Q}) = \{1, \sigma_\gamma\}$, where γ is any quadratic non-residue in $\mathbb{F}_p$.

3 The construction of 3-class and 4-class association schemes

In this section, let $\mathbb{F} = \mathbb{F}_{2^m}$ and $G = \mathbb{F} \times \mathbb{F}$. Let $f : \mathbb{F} \rightarrow \mathbb{F}$ be an s -nonlinear and differentially 2^s -uniform function with $f(0) = 0$, and let $R = \{(x, f(x)) : x \in \mathbb{F}\}$ be the graph of the function f . We define the sets $D_0 := \{\chi \in \widehat{G} : \chi(R) = 0\}$, $D_+ := \{\chi \in \widehat{G} : \chi(R) = \eta\}$, $D_- := \{\chi \in \widehat{G} : \chi(R) = -\eta\}$, where $\eta = 2^{\frac{m+s}{2}}$ and $\widehat{G}$ is the character group of G . Here we choose the notation D_0, D_+, D_- since for an s -nonlinear function f , the character value $\chi(R) \in \{0, 2^{\frac{m+s}{2}}, -2^{\frac{m+s}{2}}\}$. Note that we are working in the additive group of $\mathbb{F}$ with characteristic 2, thus $-x = x$ and $M^{(-1)} = M$ for any $x \in \mathbb{F}$ and $M \in \mathbb{C}[G]$.

It is clear that $\tilde{R} = \sum_{\chi \in \widehat{G}} \chi(R) \chi = 2^m \chi_0 + \eta(D_+ - D_-)$. Since $\tilde{R} = |G|R^{(-1)}$, we know that $|G|R^{(-1)} = 2^m G + \eta(\tilde{D}_+ - \tilde{D}_-) = 2^m G + \eta \sum_{g \in G} (g(D_+) - g(D_-))g$, where, as before, $R^{(-1)} = \sum_{r \in R} r^{-1}$. Now $|G|R = \sum_{g \in G} (2^m + \eta(g(D_+) - g(D_-)))g$. By comparing the coefficients of the elements in G on both sides, we get the following equations:

$$\begin{aligned} 2^m + \eta(g(D_+) - g(D_-)) &= |G| = 2^{2m} & \text{if } g \in R \\ 2^m + \eta(g(D_+) - g(D_-)) &= 0 & \text{if } g \notin R. \end{aligned} \quad (1)$$

Let $f : \mathbb{F} \rightarrow \mathbb{F}$ be a differentially 2^s -uniform and s -nonlinear function, and assume $D = \{(a, b) \in G : \delta_f(a, b) = 2^s\}$, where $\delta_f(a, b) := \#\{x \in \mathbb{F} : f(x+a) + f(x) = b\}$. It is shown in [Budaghyan and Pott(2009)] that D is a $(2^{2m}, 2^{m-s}(2^m - 1), 2^{m-s}(2^{m-s} - 3 + 2^s), 2^{m-s}(2^{m-s} - 1))$ partial difference set, hence it gives rise to a 2-class association scheme.

Now we consider the group ring element $\sum_{\chi \in \widehat{G}} \chi(R)^2 \chi$ in $\mathbb{C}[\widehat{G}]$. It is clear that $\sum_{\chi \in \widehat{G}} \chi(R)^2 \chi = 2^{2m} \chi_0 + \eta^2(D_+ + D_-)$. For any $g = (u, v)$ in G , on the one hand side we get $g(2^{2m} \chi_0 +$

$\eta^2(D_+ + D_-) = 2^{2m} + \eta^2(g(D_+) + g(D_-))$. On the other side,

$$\begin{aligned}
g(\sum_{\chi \in \widehat{G}} \chi(R)^2 \chi) &= \sum_{\chi \in \widehat{G}} \chi(R)^2 \chi(g) \\
&= \sum_{(a,b) \in G} \left(\sum_{x,y \in \mathbb{F}} (-1)^{\text{Tr}(ax+bf(x))} (-1)^{\text{Tr}(ay+bf(y))} (-1)^{\text{Tr}(au+bv)} \right) \\
&= \sum_{b,x,y \in \mathbb{F}} (-1)^{\text{Tr}(b(f(x)+f(y)+v))} \sum_{a \in \mathbb{F}} (-1)^{\text{Tr}(a(x+y+u))} \\
&= 2^m \sum_{b \in \mathbb{F}} \sum_{x \in \mathbb{F}} (-1)^{\text{Tr}(b(f(x)+f(x+u)+v))} \\
&= 2^{2m} \sum_{b \in \mathbb{F}} \# \{x \in \mathbb{F} : f(x) + f(x+u) = v\} \\
&= \begin{cases} 2^{2m} \cdot 2^m & \text{if } (u,v) = (0,0), \\ 0 & \text{if } g \notin D, \\ 2^{2m} \cdot 2^s & \text{if } g \in D. \end{cases}
\end{aligned}$$

Hence, $2^{2m} + \eta^2(g(D_+) + g(D_-)) = 0$ or 2^{2m+s} for any $g \neq (0,0)$, which implies

$$\begin{aligned}
g(D_+) + g(D_-) &= -2^{m-s} & \text{if } g \notin D, \\
g(D_+) + g(D_-) &= 2^m - 2^{m-s} & \text{if } g \in D.
\end{aligned} \tag{2}$$

For any $g \in G \setminus \{(0,0)\}$, we define $x = g(D_+)$ and $y = g(D_-)$. By Eq. (1) and (2), we can determine the values of x, y which depend on whether g is in one of $R \cap D, \overline{R} \cap D, R \cap \overline{D}, \overline{R} \cap \overline{D}$; here $\overline{R}, \overline{D}$ is the complement of R, D in G . For instance, if $g \in R \cap D$, we have the equations

$$\begin{aligned}
x - y &= 2^{\frac{3m-s}{2}} - 2^{\frac{m-s}{2}}, \\
x + y &= 2^m - 2^{m-s}.
\end{aligned}$$

Through simple calculation, we get $(g(D_+), g(D_-)) = (2^{m-1} - 2^{m-s-1} + 2^{\frac{3m-s}{2}-1} - 2^{\frac{m-s}{2}-1}, 2^{m-1} - 2^{m-s-1} - 2^{\frac{3m-s}{2}-1} + 2^{\frac{m-s}{2}-1})$. Using the same argument, we obtain

Lemma 1 *Let $g \in G \setminus \{(0,0)\}$. The character values $(g(D_+), g(D_-))$ satisfy*

$$\begin{aligned}
&(2^{m-1} - 2^{m-s-1} + 2^{\frac{3m-s-2}{2}} - 2^{\frac{m-s-2}{2}}, 2^{m-1} - 2^{m-s-1} - 2^{\frac{3m-s-2}{2}} + 2^{\frac{m-s-2}{2}}) \\
&\quad \text{if } g \in R \cap D, \\
&(2^{m-1} - 2^{m-s-1} - 2^{\frac{m-s-2}{2}}, 2^{m-1} - 2^{m-s-1} + 2^{\frac{m-s-2}{2}}) \\
&\quad \text{if } g \in \overline{R} \cap D, \\
&(-2^{m-s-1} + 2^{\frac{3m-s-2}{2}} - 2^{\frac{m-s-2}{2}}, -2^{m-s-1} - 2^{\frac{3m-s-2}{2}} + 2^{\frac{m-s-2}{2}}) \\
&\quad \text{if } g \in R \cap \overline{D}, \\
&(-2^{m-s-1} - 2^{\frac{m-s-2}{2}}, -2^{m-s-1} + 2^{\frac{m-s-2}{2}}) \\
&\quad \text{if } g \in \overline{R} \cap \overline{D}.
\end{aligned}$$

Define $X_0 = \{\chi_0\}$, $X_1 = D_0$, $X_2 = D_+$, $X_3 = D_-$. We will show that X_0, X_1, X_2, X_3 span a Schur ring. To prove this, we need to show that there exist integers p_{ij}^k such that $X_i X_j = \sum_{k=0}^3 p_{ij}^k X_k$ for any $i, j \in \{0, 1, 2, 3\}$.

Lemma 2 (1) $X_1X_2 = a_1X_1 + a_2X_2 + a_3X_3$ where

$$\begin{aligned} a_1 &= -2^{2m-2s-1} + 2^{2m-s-1} - 2^{\frac{3m-3s-2}{2}} + 2^{\frac{3m-s-2}{2}}, \\ a_2 &= 2^{\frac{m-s-2}{2}} + 2^{\frac{3m-s-2}{2}} - 2^{\frac{3m-3s-2}{2}} - 2^{2m-2s-1} + 3 \cdot 2^{m-s-1} + 2^{2m-1-s} - 1 - 2^m, \\ a_3 &= -2^{2m-s-1} + 2^{m-s-1} - 2^{\frac{2m-3s-2}{2}} + 2^{2m-1-s} + 2^{\frac{2m-s-2}{2}} + 2^{\frac{m-s-2}{2}}. \end{aligned}$$

(2) $X_1X_3 = b_1X_1 + b_2X_2 + b_3X_3$ where

$$\begin{aligned} b_1 &= -2^{2m-2s-1} + 2^{2m-1-s} + 2^{\frac{3m-3s-2}{2}} - 2^{\frac{3m-s-2}{2}}, \\ b_2 &= 2^{\frac{3m-3s-2}{2}} - 2^{\frac{m-s-2}{2}} - 2^{\frac{3m-s-2}{2}} - 2^{2m-2s-1} + 2^{2m-1-s} + 2^{m-s-1}, \\ b_3 &= -2^{2m-2s-1} + 2^{\frac{3m-3s-2}{2}} + 2^{2m-1-s} + 3 \cdot 2^{m-s-1} - 1 - 2^m - 2^{\frac{2m-s-2}{2}} - 2^{\frac{m-s-2}{2}}. \end{aligned}$$

(3) $X_2X_3 = c_1X_1 + c_2X_2 + c_3X_3$ where

$$\begin{aligned} c_1 &= 2^{2m-2s-2} - 2^{m-s-2}, \\ c_2 &= 2^{2m-2s-2} - 3 \cdot 2^{m-s-2} + 2^{m-2} + 2^{\frac{m-s}{2}-1} - 2^{\frac{3m-s}{2}-2}, \\ c_3 &= 2^{2m-2s-2} - 3 \cdot 2^{m-s-2} + 2^{m-2} - 2^{\frac{m-s}{2}-1} + 2^{\frac{3m-s}{2}-2}. \end{aligned}$$

Proof We only prove (1), the other cases are similar. Suppose $g \in R \cap D \subseteq G$ and $g \neq (0, 0)$, $(g(X_1), g(X_2), g(X_3)) = (-1 - 2^m + 2^{m-s}, 2^{m-1} - 2^{m-s-1} + 2^{\frac{3m-s-2}{2}} - 2^{\frac{m-s-2}{2}}, 2^{m-1} - 2^{m-s-1} - 2^{\frac{3m-s-2}{2}} + 2^{\frac{m-s-2}{2}})$ by Lemma 1 and $g(X_1) + g(X_2) + g(X_3) = -1$. On the one hand, $g(X_1X_2) = g(X_1)g(X_2)$. On the other hand, $g(a_1X_1 + a_2X_2 + a_3X_3) = a_1g(X_1) + a_2g(X_2) + a_3g(X_3)$. We can see $g(X_1X_2) = g(a_1X_1 + a_2X_2 + a_3X_3)$ through simple computation. The cases for $g \in \overline{R} \cap D, R \cap \overline{D}, \overline{R} \cap \overline{D}$ are similar.

Theorem 1 Let $f : \mathbb{F} \rightarrow \mathbb{F}$ be an s -nonlinear and differentially 2^s -uniform function. Define the subsets $X_0 = \{\chi_0\}, X_1 := \{\chi \in \widehat{G} : \chi(R) = 0\}, X_2 = \{\chi \in \widehat{G} : \chi(R) = \eta\}, X_3 := \{\chi \in \widehat{G} : \chi(R) = -\eta\}$ of $\widehat{G}$, where $\eta = 2^{\frac{m+s}{2}}$ and $\widehat{G}$ is the character group of $G = \mathbb{F} \times \mathbb{F}$. Then X_0, X_1, X_2, X_3 span a Schur Ring.

Proof It is clear that X_0, X_1, X_2, X_3 are disjoint subsets which form a partition of $\widehat{G}$. Note that we can compute X_iX_j from the knowledge of $X_iX_j, i \neq j$: $X_iX_i = X_i(G - \sum_{j \neq i} X_j)$. The result follows from the above lemmas.

Corollary 1 Let $V = \mathbb{F} \times \mathbb{F}$, and define the binary relation $R_i := \{(\chi, \phi) : \chi\phi^{-1} \in X_i\}$ for $i \in \{0, 1, 2, 3\}$. Then $(\widehat{G}; R_0, R_1, R_2, R_3)$ is a 3-class association scheme.

We give an example of the above construction.

Example 1 Let $\mathbb{F} = \mathbb{F}_{2^5}$ and $f(x) = x^3$. Define $X_0 = \{\chi_0\}, X_1 := \{\chi \in \widehat{G} : \chi(R) = 0\}, X_2 = \{\chi \in \widehat{G} : \chi(R) = 8\}, X_3 = \{\chi \in \widehat{G} : \chi(R) = -8\}$. Then X_0, X_1, X_2, X_3 span a Schur ring. We have $\#X_0 = 1, \#X_1 = 527, \#X_2 = 310, \#X_3 = 186$ and

$$\begin{aligned} X_1X_1 &= 527X_0 + 270X_1 + 272X_2 + 272X_3 \\ X_1X_2 &= 160X_1 + 153X_2 + 170X_3 \\ X_1X_3 &= 96X_1 + 102X_2 + 85X_3 \\ X_2X_2 &= 310X_0 + 90X_1 + 126X_2 + 50X_3 \\ X_2X_3 &= 60X_1 + 30X_2 + 90X_3 \\ X_3X_3 &= 186X_0 + 30X_1 + 54X_2 + 10X_3. \end{aligned}$$

With a small modification, we can construct a 4-class association scheme. Note that in Theorem 1, we have $\{\chi_{a,0} : a \in \mathbb{F}^*\} \subseteq X_1$. The following lemma is proved by using the same arguments as before.

Lemma 3 *Let $f : \mathbb{F} \rightarrow \mathbb{F}$ be an s -nonlinear and differentially 2^s -uniform function. Define the subsets $Y_0 = \{\chi_0\}$, $Y_1 = \{\chi_{a,0} : a \in \mathbb{F}^*\}$, $Y_2 := \{\chi_{u,v} \in \widehat{G} : \chi_{u,v}(R) = 0, v \neq 0\}$, $Y_3 = \{\chi \in \widehat{G} : \chi(R) = \eta\}$, $Y_4 := \{\chi \in \widehat{G} : \chi(R) = -\eta\}$ of $\widehat{G}$, where $\eta = 2^{\frac{m+s}{2}}$ and $\widehat{G}$ is the character group of $G = \mathbb{F} \times \mathbb{F}$. We have:*

$$\begin{aligned} (Y_0 + Y_1)Y_2 &= (2^m - 2^{m-s})(Y_2 + Y_3 + Y_4) \\ (Y_0 + Y_1)Y_3 &= (2^{m-s-1} + 2^{\frac{m-s-2}{2}})(Y_2 + Y_3 + Y_4) \\ (Y_0 + Y_1)Y_4 &= (2^{m-s-1} - 2^{\frac{m-s-2}{2}})(Y_2 + Y_3 + Y_4). \end{aligned}$$

Now we will prove that Y_0, Y_1, Y_2, Y_3, Y_4 span a Schur ring.

Theorem 2 *Let $f : \mathbb{F} \rightarrow \mathbb{F}$ be an s -nonlinear and differentially 2^s -uniform function. Define the subsets $Y_0 = \{\chi_0\}$, $Y_1 = \{\chi_{a,0} \in \widehat{G} : a \in \mathbb{F}^*\}$, $Y_2 := \{\chi_{u,v} \in \widehat{G} : \chi_{u,v}(R) = 0, v \neq 0\}$, $Y_3 = \{\chi \in \widehat{G} : \chi(R) = \eta\}$, $Y_4 := \{\chi \in \widehat{G} : \chi(R) = -\eta\}$ of $\widehat{G}$, where $\eta = 2^{\frac{m+s}{2}}$ and $\widehat{G}$ is the character group of $G = \mathbb{F} \times \mathbb{F}$. Then Y_0, Y_1, Y_2, Y_3, Y_4 span a Schur ring.*

Proof Note that $Y_0 \cup Y_1$ is a subgroup of $\widehat{G}$. It is clear that the Y_i 's are disjoint subsets which form a partition of $\widehat{G}$. We need to show that for each $i, j \in \{0, 1, 2, 3, 4\}$, there exist integers p_{ij}^k such that $Y_i Y_j = \sum_{k=0}^4 p_{ij}^k Y_k$. Note that $Y_2 = X_1 - Y_1$, $Y_3 = X_2$, $Y_4 = X_3$, where X_i is defined in Theorem 1. By Lemma 3, we know $Y_1 Y_i = \sum_{k=0}^4 p_{1i}^k Y_k$ for some integers p_{1i}^k , since $Y_0 Y_i = Y_i$ for $i \in \{0, 1, 2, 3, 4\}$. For the remaining cases, the results hold by Lemma 3 and Theorem 1. For example, $Y_2 Y_3 = (X_1 - Y_1)X_2 = X_1 X_2 - Y_1 X_2 = \sum_{k=0}^4 p_{23}^k Y_k$.

Corollary 2 *Let $V = \mathbb{F} \times \mathbb{F}$, and define the binary relation $R_i := \{(\chi, \phi) : \chi\phi^{-1} \in Y_i\}$ for $i \in \{0, 1, 2, 3\}$. Then $(\widehat{G}; R_0, R_1, R_2, R_3, R_4)$ is a 4-class association scheme.*

4 The construction of a family of p -class association schemes

In this section, let $\mathbb{F} := \mathbb{F}_{p^n}$ with p an odd prime always denote a finite field of odd characteristic. The element ζ_p denotes, as before, a complex primitive p -th root of unity, say $\zeta_p = e^{\frac{2\pi i}{p}}$. Suppose $f : \mathbb{F} \rightarrow \mathbb{F}_p$ is a weakly regular p -ary bent function with $f(0) = 0$. For later use, we note that the field extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois of degree $p-1$, and the Galois group $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{\sigma_a : a \in \mathbb{Z}_p^*\}$ where the automorphism σ_a of K is defined by $\sigma_a(\zeta_p) = \zeta_p^a$.

By [Feng and Luo(2007), Hellesest and Kholosha(2006)], we know that for all known weakly regular functions f , the Walsh coefficient $\mathcal{W}_f(b) = u(\sqrt{p}^*)^n \zeta_p^{f^*(b)}$ with $u = \pm 1$, where $p^* = (-1)^{\frac{p-1}{2}} p$. Also, for each known weakly regular bent function f , we have $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p, x \in \mathbb{F}$; here k is a constant with $(k-1, p-1) = 1$. For the bent functions in the table in Section 2.4, we may just take $k = d$.

Lemma 4 *Assume there exists a constant k with $(k-1, p-1) = 1$ such that $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p$. Then there always exists a constant l with $(l-1, p-1) = 1$ such that $f^*(tx) = t^l f^*(x)$, where f^* is the dual function of f , see Section 2.4 for the definition of the dual function.*

Proof We have

$$\begin{aligned}\mathcal{W}_f(tb) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\text{Tr}(bt\alpha x) + f(x)} = \sum_x \zeta_p^{\text{Tr}(bt\alpha x) + f(\alpha x)} \\ &= \sum_x \zeta_p^{t\alpha \text{Tr}(bx) + \alpha^k f(x)} \\ &= \sigma_{\alpha t}(\mathcal{W}_f(b))\end{aligned}$$

where $\alpha^{k-1} = t$ and $\alpha \in \mathbb{F}_p$; the existence of α is guaranteed by $(k-1, p-1) = 1$. Now we have $u(\sqrt{p^*})^n \zeta_p^{f^*(tb)} = \sigma_{\alpha t}(u(\sqrt{p^*})^n \zeta_p^{f^*(b)}) = u(\sqrt{p^*})^n (\frac{\alpha t}{p})^n \zeta_p^{\alpha t f^*(b)}$ (Result 1), which implies $f^*(tb) = \alpha t f^*(b) = t^{\frac{k}{k-1}} f^*(b)$ since $(\frac{\alpha t}{p})^n = (\frac{t^{\frac{k}{k-1}}}{p})^n = (\frac{t}{p})^{k(k-1)^{-1}n} = 1$, which follows since k is even. Finally, define $l = k(k-1)^{-1}$, then $k(k-1)^{-1} - 1 = (k-1)^{-1}$ is relative prime to $p-1$ since $(k-1, p-1) = 1$.

One can show that f^* is also a weakly regular bent function and $f^{**}(x) = f(-x)$, see [Helleseth and Kholosha(2006)].

Now we suppose that f is a weakly regular bent function s.t. $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p, x \in \mathbb{F}$; here k is a constant with $(k-1, p-1) = 1$. By Lemma 4, we know there exists a constant l with $(l-1, p-1) = 1$ such that $f^*(tx) = t^l f^*(x)$ for all $t \in \mathbb{F}_p, x \in \mathbb{F}$. Assume that the Walsh coefficient $\mathcal{W}_f(b) = u(\sqrt{p^*})^n \zeta_p^{f^*(b)}$ with $u = \pm 1$, where p^* is defined in Result 1. We define the subsets

$$D_i := \{x \in \mathbb{F} : f(x) = i\}, \quad 0 \leq i \leq p-1; \quad L_t := \sum_{i=0}^{p-1} D_i \zeta_p^{it}, \quad 0 \leq t \leq p-1,$$

in particular $L_0 = \mathbb{F}$. The main goal in this section is to prove that $\{0\}, D_0 - \{0\}, D_1, D_2, \dots, D_{p-1}$ span a Schur ring. First, we give some properties of the L_i 's.

Lemma 5 (1) If $s, t, s+t \neq 0$, then $L_t L_s = u(\frac{tsv}{p})^n (\sqrt{p^*})^n L_v$ with $u = \pm 1$ and $s^{1-l} + t^{1-l} = v^{1-l}$;

(2) $L_t L_{-t} = p^n$ for $t \in \{1, \dots, p-1\}$;

(3) $\sum_{t=1}^{p-1} L_t L_0 \zeta_p^{-at} = (p|D_a| - p^n)\mathbb{F}$.

Proof Applying any additive character of the form χ_b of $\mathbb{F}$ to L_t ($t \neq 0$), we get

$$\begin{aligned}\chi_b(L_t) &= \sum_{i=0}^{p-1} \chi_b(D_i) \zeta_p^{it} = \sum_{x \in \mathbb{F}} \zeta_p^{tf(x) + \text{Tr}(bx)} \\ &= \sigma_t(u(\sqrt{p^*})^n \zeta_p^{f^*(t^{-1}b)}) \\ &= u \left(\frac{t}{p}\right)^n (\sqrt{p^*})^n \zeta_p^{t^{1-l} f^*(b)}.\end{aligned}$$

(1) If $s, t, s+t \neq 0$, then

$$\begin{aligned}\chi_b(L_t L_s) &= \left(\frac{ts}{p}\right)^n (p^*)^n \zeta_p^{(t^{1-l} + s^{1-l})f^*(b)} \\ &= u \left(\frac{v}{p}\right)^n (\sqrt{p^*})^n \zeta_p^{v^{1-l} f^*(b)} \cdot u \left(\frac{tsv^{-1}}{p}\right)^n (\sqrt{p^*})^n\end{aligned}$$

$$\begin{aligned}
&= u \left(\frac{tsv^{-1}}{p} \right)^n (\sqrt{p^*})^n \chi_b(L_v) \\
&= u \left(\frac{tsv}{p} \right)^n (\sqrt{p^*})^n \chi_b(L_v),
\end{aligned}$$

which implies $L_t L_s = u \left(\frac{tsv}{p} \right)^n (\sqrt{p^*})^n L_v$ with $s^{1-l} + t^{1-l} = v^{1-l}$. Note that $\left(\frac{tsv^{-1}}{p} \right) = \left(\frac{tsv}{p} \right)$ for $v \neq 0$. We have $a^{1-l} + b^{1-l} = 0$ if and only if $a + b = 0$ for $a, b \in \mathbb{F}_p$ due to the fact that $(l-1, p-1) = 1$.

- (2) For $t \in \{1, \dots, p-1\}$, we have $\chi_b(L_t L_{-t}) = \left(\frac{-1}{p} \right)^n (p^*)^n = p^n$ since $p^* = \left(\frac{-1}{p} \right)p$.
(3) The result follows from the following computation:

$$\begin{aligned}
\sum_{t=1}^{p-1} L_t L_0 \zeta_p^{-at} &= \sum_{t=1}^{p-1} \sum_{i=0}^{p-1} D_i \zeta_p^{(i-a)t} \mathbb{F} = \sum_{t=1}^{p-1} \sum_{i=0}^{p-1} |D_i| \zeta_p^{(i-a)t} \mathbb{F} \\
&= \sum_{i=0}^{p-1} \left(\sum_{t=1}^{p-1} \zeta_p^{(i-a)t} \right) |D_i| \mathbb{F} = ((p-1)|D_a| - \sum_{i \neq a} |D_i|) \mathbb{F} \\
&= ((p-1)|D_a| - (p^n - |D_a|)) \mathbb{F} = (p|D_a| - p^n) \mathbb{F}.
\end{aligned}$$

We are now ready to prove our main theorem.

Theorem 3 Suppose that $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ is a weakly regular bent function s.t. $f(tx) = t^k f(x)$ for all $t \in \mathbb{F}_p, x \in \mathbb{F}_{p^n}$, where k is a constant with $(k-1, p-1) = 1$. Assume that the Walsh coefficient $\mathcal{W}_f(b) = u(\sqrt{p^*})^n \zeta_p^{f^*(b)}$ with $u = \pm 1$. We define the subsets $A_0 = \{0\}, A_i = \{x \in \mathbb{F}_{p^n} : f(x) = i-1\}$ for $1 \leq i \leq p$. Then $A_0, A_1, \dots, A_p$ span a Schur ring.

Proof Note that we can easily compute the D'_i s from the L'_i s: $D_i = \sum_t L_t \zeta_p^{-it}$. We have $A_i = D_{i-1}$ for $i \in \{2, \dots, p\}$ and $A_1 = D_0 \setminus \{0\}$. By Lemma 4, we know that there exists a constant l with $(l-1, p-1) = 1$ such that $f^*(tx) = t^l f^*(x)$ for all $t \in \mathbb{F}_p, x \in \mathbb{F}$. We compute

$$\begin{aligned}
p^2 D_a D_b &= \sum_{s,t=0}^{p-1} L_t L_s \zeta_p^{-at-bs} \\
&= L_0^2 + \sum_{\substack{s,t \neq 0 \\ s+t \neq 0}} L_t L_s \zeta_p^{-at-bs} + \sum_{s=1}^{p-1} L_s L_{-s} \zeta_p^{s(a-b)} + \sum_{s=1}^{p-1} L_s L_0 \zeta_p^{-bs} + \sum_{t=1}^{p-1} L_t L_0 \zeta_p^{-at} \\
&= p^n \mathbb{F}_{p^n} + \sum_{\substack{s,t,s+t \neq 0 \\ s^{1-l} + t^{1-l} = v^{1-l}}} u \left(\frac{tsv}{p} \right)^n (\sqrt{p^*})^n \zeta_p^{-at-bs} L_v + \sum_{s=1}^{p-1} p^n \zeta_p^{s(a-b)} + (p|D_b| - p^n) \mathbb{F}_{p^n} \\
&\quad + (p(|D_a| - p^n) \mathbb{F}_{p^n} \\
&= \sum_{s=1}^{p-1} p^n \zeta_p^{s(a-b)} + (p(|D_a| + |D_b|) - p^n) \mathbb{F}_{p^n} + \sum_{\substack{s,t,s+t \neq 0 \\ s^{1-l} + t^{1-l} = v^{1-l}}} u \left(\frac{tsv}{p} \right)^n (\sqrt{p^*})^n \zeta_p^{-at-bs} L_v \\
&= c + \sum_{i=0}^{p-1} d_i D_i,
\end{aligned}$$

where $c = p^n(p\delta_{a-b} - 1)$ with δ the Kronecker symbol, and

$$d_i = p(|D_a| + |D_b|) - p^n + (\sqrt{p^*})^n \sum_{\substack{s,t=1, s+t \neq 0 \\ s^{1-l} + t^{1-l} = v^{1-l}}} u \left(\frac{tsv}{p} \right)^n \zeta_p^{vi-at-bs}.$$

Therefore, $A_i A_j$ can be represented as linear combinations of the A_k 's over $\mathbb{C}$. Since $A_i A_j$ has integer coefficients and the A_k 's are disjoint, the result is established.

We determine the dual Schur rings of those in Theorem 3.

Corollary 3 *Let f be as defined in Theorem 3. Let G be the additive group of the field $\mathbb{F}$ and $\widehat{G}$ be its character group. We define the subsets $E_0 = \{\chi_0\}$, $E_i = \{\chi_b \in \widehat{G} : f^*(b) = i - 1\}$ for $1 \leq i \leq p$. Then $E_0, E_1, \dots, E_p$ span a Schur ring which is the dual of the one defined in Theorem 3.*

Proof Recall that $A_i = D_{i-1}$ for $2 \leq i \leq p$ and $A_1 = D_0 \setminus \{0\}$. We fix some i with $2 \leq i \leq p$. By the definition of the dual Schur ring, for any two characters $\chi_b, \chi_{b'}$, we have $\chi_b \sim \chi_{b'} \Leftrightarrow \chi_b(A_i) = \chi_{b'}(A_i) \Leftrightarrow \chi_b(L_i) = \chi_{b'}(L_i)$. Recall that from the beginning of this section we have $\chi_b(L_i) = u(\frac{i}{p})^n (\sqrt{p^*})^n \zeta_p^{t^{1-i} f^*(b)}$, where $u = \pm 1$ (see the proof of Lemma 5). Then this implies $\chi_b \sim \chi_{b'} \Leftrightarrow f^*(b) = f^*(b')$. By Theorem 3, the result is proved.

Example 2 Let $\mathbb{F} = \mathbb{F}_{3^5}$ and f be the Coulter-Matthews bent function $\text{Tr}(x^{14})$. Define $A_0 = \{0\}$, $A_i = \{x \in \mathbb{F}^* : f(x) = i - 1\}$ for $i \in \{1, 2, 3\}$. We have

$$\begin{aligned} A_1 A_1 &= 80A_0 + 25A_1 + 24A_2 + 30A_3 \\ A_1 A_2 &= 27A_1 + 32A_2 + 30A_3 \\ A_1 A_3 &= 27A_1 + 24A_2 + 20A_3 \\ A_2 A_2 &= 90A_0 + 36A_1 + 33A_2 + 30A_3 \\ A_2 A_3 &= 27A_1 + 24A_2 + 20A_3 \\ A_3 A_3 &= 72A_0 + 18A_1 + 24A_2 + 21A_3. \end{aligned}$$

Remark 1 By [Feng and Luo(2007), Helleseth and Kholosha(2006)], the assumption $\mathcal{W}_f(b) = u(\sqrt{p^*})^n \zeta_p^{f^*(b)}$ with $u = \pm 1$ in Theorem 3 is true for all known weakly regular bent functions.

Remark 2 It is important to point out that, for the ternary bent function $f(x) = \text{Tr}(\xi^7 x^{98})$ which is not weakly regular in $\mathbb{F}_{3^6}$, the construction in Theorem 3 does not produce association schemes, which can be easily verified by Magma [Bosma et al(1997)Bosma, Cannon, and Playoust].

Acknowledgment

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

This work was done during the second 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

- [Bannai and Ito(1984)] Bannai E, Ito T (1984) Algebraic combinatorics. I. The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, association schemes
- [Bose and Nair(1939)] Bose R, Nair K (1939) Partially balanced incomplete block designs. Sankhyā
- [Bose and Shimamoto(1952)] Bose R, Shimamoto T (1952) Classification and analysis of partially balanced incomplete block designs with two association schemes. J Amer Statist Assoc

-
- [Bose and Shimamoto(1963)] Bose R, Shimamoto T (1963) Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J Math*
- [Bosma et al(1997)Bosma, Cannon, and Playoust] Bosma W, Cannon J, Playoust C (1997) The Magma algebra system. i. the user language. *J Symbolic Comput* 24(3–4):235–265
- [Budaghyan and Pott(2009)] Budaghyan L, Pott A (2009) On differential uniformity and nonlinearity of functions. *Discrete Math* 309:371–384
- [van Dam and Fon-Der-Flaass(2000)] van Dam ER, Fon-Der-Flaass D (2000) Uniformly packed codes and more distance regular graphs from crooked functions. *J Algebraic Combin* 12(2):115–121, DOI 10.1023/A:1026583725202, URL <http://dx.doi.org/10.1023/A:1026583725202>
- [Delsarte(1973)] Delsarte P (1973) An algebraic approach to the association schemes of coding theory. *Philips Res Rep Suppl* (10):vi+97
- [Delsarte and Levenshtein(1998)] Delsarte P, Levenshtein VI (1998) Association schemes and coding theory. *IEEE Trans Inform Theory* 44(6):2477–2504, DOI 10.1109/18.720545, URL <http://dx.doi.org/10.1109/18.720545>, information theory: 1948–1998
- [Feng and Luo(2007)] Feng K, Luo J (2007) Value distributions of exponential sums from perfect nonlinear functions and their applications. *IEEE Trans Inform Theory* 53(9):3035–3041, DOI 10.1109/TIT.2007.903153, URL <http://dx.doi.org/10.1109/TIT.2007.903153>
- [Helleseth and Kholosha(2006)] Helleseth T, Kholosha A (2006) Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans Inform Theory* 52(5):2018–2032, DOI 10.1109/TIT.2006.872854, URL <http://dx.doi.org/10.1109/TIT.2006.872854>
- [Helleseth et al(2008)Helleseth, Hollmann, Kholosha, Wang, and Xiang] Helleseth T, Hollmann HDL, Kholosha A, Wang Z, Xiang Q (2008) Proofs of two conjectures on ternary weakly regular bent functions. URL <http://www.citebase.org/abstract?id=oai:arXiv.org:0803.2878>
- [Ireland and Rosen(1990)] Ireland K, Rosen M (1990) A classical introduction to modern number theory. Springer-Verlag, New York, graduate Texts in Mathematics, Vol. 84
- [Kumar et al(1985)Kumar, Scholtz, and Welch] Kumar PV, Scholtz RA, Welch LR (1985) Generalized bent functions and their properties. *J Combin Theory Ser A* 40(1):90–107, DOI 10.1016/0097-3165(85)90049-4, URL [http://dx.doi.org/10.1016/0097-3165\(85\)90049-4](http://dx.doi.org/10.1016/0097-3165(85)90049-4)
- [Lidl and Niederreiter(1997)] Lidl R, Niederreiter H (1997) Finite Fields, *Encyclopedia of Mathematics and its Applications*, vol 20, 2nd edn. Cambridge University Press
- [Ma(1989)] Ma SL (1989) Schur rings and cyclic association schemes of class three. *Graphs Combin* 5(4):355–361, DOI 10.1007/BF01788691, URL <http://dx.doi.org/10.1007/BF01788691>
- [Ma(1994)] Ma SL (1994) A survey of partial difference sets. *Des Codes Cryptogr* 4(3):221–261
- [Passman(1977)] Passman D (1977) The Algebraic Structure of Group Rings. Wiley-Interscience
- [Pott(2004)] Pott A (2004) Nonlinear functions in abelian groups and relative difference sets. *Discrete Appl Math* 138:177–193
- [Rothaus(1976)] Rothaus OS (1976) On “bent” functions. *J Combinatorial Theory Ser A* 20(3):300–305