New Pseudo-Planar Binomials in Characteristic Two and Related Schemes

Sihuang Hu[a], Shuxing Li[a], Tao Zhang[a], Tao Feng[a] and Gennian Ge[b,c,*]

[a] Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China

[b] School of Mathematical Sciences, Capital Normal University, Beijing, 100048, China

[c] Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China.

Abstract

Planar functions in odd characteristic were introduced by Dembowski and Ostrom in order to construct finite projective planes in 1968. They were also used in the constructions of DES-like iterated ciphers, error-correcting codes, and signal sets. Recently, a new notion of pseudo-planar functions in even characteristic was proposed by Zhou. These new pseudo-planar functions, as an analogue of planar functions in odd characteristic, also bring about finite projective planes. There are three known infinite families of pseudo-planar monomial functions constructed by Schmidt and Zhou, and Scherr and Zieve. In this paper, three new classes of pseudo-planar binomials are provided. Moreover, we find that each pseudo-planar function gives an association scheme which is defined on a Galois ring.

Key words and phrases: Pseudo-Planar function, relative difference set, projective plane, association scheme

AMS subject classifications: Primary 05B10, 05E30, 94A60.

1 Introduction

Let $q = p^n$ where p is an odd prime and n is a positive integer. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is *planar* if the mapping

$$x \to f(x + \epsilon) - f(x) \tag{1}$$

is a permutation of $\mathbb{F}_q$ for each $\epsilon \in \mathbb{F}_q^*$. Planar functions were introduced by Dembowski and Ostrom [8] to construct finite projective planes over finite fields with odd characteristic. Apart from this, planar functions emerge from many other applications. In the cryptography literature, they are called *perfect nonlinear functions* [18], and used in the constructions of DES-like iterated ciphers, since they are optimally resistant to differential cryptanalysis. Carlet, Ding, and Yuan [7, 9, 23], among others, utilized planar functions to construct error-correcting codes, which are then employed to design secret sharing

*Corresponding author. Email address: gnge@zju.edu.cn

Table 1: The known pseudo-planar monomials on $\mathbb{F}_{2^n}$

Function	Condition	Reference
ax^{2^k}	$a \in \mathbb{F}_{2^n}^*$	trivial
ax^{2^k+1}	$n = 2k, a \in \mathbb{F}_{2^{n/2}}^*, \mathrm{Tr}_{n/2}(a) = 0$	[20, Theorem 6]
$ax^{4^k(4^k+1)}$	$n = 6k$, $a \in \mathbb{F}_{2^n}^*$, a is a (4^k-1)-th power but not a $3(4^k-1)$-th power	[19, Theorem 1.1]

schemes. Planar functions are also applied to the construction of authentication codes [10], constant composition codes [12] and signal sets [11]. Besides, planar functions induce many combinatorial objects such as skew Hadamard difference sets and Paley type partial difference sets [22].

When $p = 2$, there are no planar functions over $\mathbb{F}_{2^n}$, since if x satisfies $f(x+\epsilon) - f(x) = d$, then so does $x + \epsilon$. As an alternative, a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be *almost perfect nonlinear* if the mapping (1) is 2-to-1 for every $\epsilon \in \mathbb{F}_{2^n}^*$. However, there is no apparent link between almost perfect nonlinear functions and finite projective planes. Recently, Zhou [24] put forward a definition of "planar" functions over finite fields with characteristic two, which give rise to finite projective planes. From now on, we call a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *pseudo-planar* if

$$x \to f(x+\epsilon) + f(x) + \epsilon x$$

is a permutation on $\mathbb{F}_{2^n}$ for each $\epsilon \in \mathbb{F}_{2^n}^*$. Note that Zhou [24] called such functions "planar", and the term "pseudo-planar" was first used by Abdukhalikov [1] to avoid confusion with planar functions in odd characteristic.

The pseudo-planar monomial functions have been investigated by Schmidt and Zhou [20], and Scherr and Zieve [19]. They are listed in Table 1, where $\mathrm{Tr}_{n/2}$ denotes the trace function from $\mathbb{F}_{2^{n/2}}$ to $\mathbb{F}_2$. In this paper, we construct three new classes of pseudo-planar binomial functions, at least two of them are infinite families. Association schemes form a central part of algebraic combinatorics, and play important roles in several branches of mathematics, such as coding theory and graph theory. One interesting result we obtained is that pseudo-planar functions will always give 5-class association schemes which are defined on Galois rings. Our construction can be regarded as an analogue of the one studied by Liebler and Mena [16], and Bonnecaze and Duursma [5]. Similar (but symmetric) 4-class association schemes were constructed by Abdukhalikov, Bannai and Suda [2], and LeCompte, Martin and Owens [14]. Analogous to the case of almost perfect nonlinear functions, we define the Fourier spectrum of pseudo-planar functions. With the information obtained from eigenmatrices of those association schemes, we completely determine the Fourier spectrum.

The rest of this paper is organized as follows. Section 2 contains the background of the mathematical objectives involved. Section 3 presents the construction of three classes of pseudo-planar binomial functions. Section 4 investigates the association schemes arising from pseudo-planar functions. Section 5 concludes this paper.

2 Preliminaries

2.1 Relative difference sets and the inversion formula

Let G be a finite abelian group and let N be a subgroup of G. A subset D of G is a *relative difference set (RDS)* with parameters $(|G|/|N|, |N|, |D|, \lambda)$ and *forbidden subgroup* N if the list of nonzero differences of D comprises every element in $G \setminus N$ exactly λ times, and no element of $N \setminus \{0\}$. The *group ring* $\mathbb{Z}[G]$ is a free abelian group with a basis $\{g \mid g \in G\}$. For any set A whose elements belong to G (A may be a multiset), we identify A and the group ring element $\sum_{g\in A} d_g g$ throughout the rest of the paper, where d_g is the multiplicity of g appears in A. Given any $A = \sum d_g g \in \mathbb{Z}[G]$, we define $A^{(-1)} = \sum d_g g^{-1}$, in which g^{-1} is the inverse of g with respect to the operation of group G. Using the language of group ring, a relative difference set D in G with forbidden group N can be expressed in a succinct way:

$$DD^{(-1)} = |D|1_G + \lambda(G - N),$$

where 1_G is the identity of group G.

For a finite abelian group G, denote its character group by $\widehat{G}$. For any $A = \sum d_g g$ and $\chi \in \widehat{G}$, define $\chi(A) = \sum d_g \chi(g)$. The following *inversion formula* shows that A is completely determined by its character value $\chi(A)$, where χ ranges over $\widehat{G}$. For convenience, we will denote d_{1_G} by $[A]_0$ throughout this paper.

Lemma 2.1. *Let G be an abelian group. If $A = \sum_{g\in G} d_g g \in \mathbb{Z}[G]$, then*

$$d_h = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\chi(h^{-1}),$$

for all $h \in G$. In particular, we have

$$[A]_0 = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A).$$

2.2 Galois rings

We give a brief introduction to the *Galois ring* $GR(4, n)$. Let $R = GR(4, n)$, then the additive group of R can be identified with the abelian group $(\mathbb{Z}_4^n, +)$. Let $Z = \{2x \mid x \in R\}$, then Z consists of 0 and the zero divisors of R, where 0 is the identity with respect to the addition. The unit group $R \setminus Z$ contains a cyclic subgroup of order $2^n - 1$ generated by an element ξ. The set $T = \{\xi^i \mid 0 \le i \le 2^n - 2\} \cup \{0\}$ is called *Teichmüller system*. For any $x \in R$, there exists a unique representation

$$x = a + 2b, \tag{2}$$

where $a, b \in T$. For any $x \in R$, write $\sqrt{x}$ for $x^{2^{n-1}}$. If we define the addition on T by

$$x \oplus y = x + y + 2\sqrt{xy},$$

then $(T, \oplus, \cdot)$ is a finite field with 2^n elements. Hence, a pseudo-planar function over $\mathbb{F}_{2^n}$ can also be identified with a function from T into itself. For any $x \in R$, we have $x = a + 2b$ for some $a, b \in T$. The map

$$\sigma : a + 2b \mapsto a^2 + 2b^2$$

is the Frobenius map of R, which is a ring automorphism. For any $a \in R$, the trace function of R is the map $\mathrm{Tr} : R \to \mathbb{Z}_4$ defined by

$$\mathrm{Tr}(a) = \sum_{i=0}^{n-1} \sigma^i(a).$$

Let $\mathbf{i} = \sqrt{-1}$. For any $a \in R$, define the map $\chi_a : R \to \mathbb{C}$ by

$$\chi_a(x) = \mathbf{i}^{\mathrm{Tr}(ax)}, \quad \forall\, x \in R.$$

Then the character group $\widehat{R} = \{\chi_a \mid a \in R\}$. For more information on Galois rings, please refer to [13, 16, 21].

2.3 Association schemes

Let X be a nonempty finite set. Let $R_0, R_1, \cdots, R_d$ be a partition of $X \times X$ satisfying that

(i) $R_0 = \{(x, x) \mid x \in X\}$;

(ii) for any $0 \le i \le d$, there exists $0 \le i' \le d$ such that $R_{i'} = \{(y, x) \mid (x, y) \in R_i\}$.

For each R_i, its adjacency matrix is denoted by A_i, whose (x, y)-th entry is 1 if $(x, y) \in R_i$ and 0 otherwise. We call $(X, \{R_i\}_{i=0}^d)$ a *d-class association scheme* if there exist nonnegative integers $p_{i,j}^k$ such that

$$A_i A_j = \sum_{k=0}^{d} p_{i,j}^k A_k,$$

where $0 \le i, j, k \le d$. The $\mathbb{C}$-linear span of $A_0, A_1, \cdots, A_d$ forms a semisimple algebra of dimension $d+1$. Hence, there exists another basis $\{E_0, E_1, \cdots, E_d\}$ consisting of pairwise orthogonal idempotents. So we have

$$A_i = \sum_{j=0}^{d} P_{ji} E_j$$

and

$$E_i = \frac{1}{|X|} \sum_{j=0}^{d} Q_{ji} A_j$$

for certain complex numbers P_{ji}, Q_{ji}. The matrix $P = (P_{ji})$ (resp. $Q = (Q_{ji})$) is called the first (resp. second) eigenmatrix. Clearly, we have $PQ = |X|I$, where I denotes the identity matrix of order $|X|$.

Let $\{S_i \mid 0 \le i \le d\}$ be a partition of X. It induces a partition $\{R_i \mid 0 \le i \le d\}$ on $X \times X$ with

$$R_i = \{(x, y) \mid x - y \in S_i\}.$$

If $(X, \{R_i\}_{i=0}^d)$ forms an association scheme, then we call $(X, \{S_i\}_{i=0}^d)$ a *Schur ring.*

Assume that $(X, \{S_i\}_{i=0}^d)$ is a Schur ring. There is an equivalence relation defined on the character group $\widehat{X}$ of X as follows: $\chi \sim \chi'$ if and only if $\chi(S_i) = \chi'(S_i)$ for each $0 \le i \le d$. Denote by $T_0, T_1, \cdots, T_d$ the equivalence classes, with T_0 consisting of only the principal character. Then $(\widehat{X}, \{T_i\}_{i=0}^d)$ also forms a Schur ring, called the *dual* of $(X, \{S_i\}_{i=0}^d)$. The first eigenmatrix of the dual scheme is equal to the second eigenmatrix of the original scheme. Please refer to [4] or [6] for more details.

We shall need the following well-known criterion due to Bannai [3] and Muzychuk [17].

Theorem 2.2 (Bannai-Muzychuk criterion)**.** *Let P be the first eigenmatrix of an association scheme $(X, \{R_i\}_{0\le i\le d})$, and $\Lambda_0 := \{0\}, \Lambda_1, \ldots, \Lambda_{d'}$ be a partition of $\{0, 1, \ldots, d\}$. Then $(X, \{R_{\Lambda_i}\}_{0\le i\le d'})$ forms an association scheme if and only if there exists a partition $\{\Delta_i\}_{0\le i\le d'}$ of $\{0, 1, 2, \ldots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j)-block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i, Λ_j)-block is the (i, j)-th entry of the first eigenmatrix of the fusion scheme.*

3 Pseudo-planar binomials

It is well-known that every function from $\mathbb{F}_{2^n}$ to itself can be uniquely written as a polynomial function of degree at most $2^n - 1$. The monomial functions $x \mapsto cx^t$ for some $c \in \mathbb{F}_{2^n}$ and some integer t are the simplest nontrivial polynomial functions. An integer t satisfying that $1 \le t \le 2^n - 1$ is a *pseudo-planar exponent* of $\mathbb{F}_{2^n}$ if the function $x \mapsto cx^t$ is pseudo-planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$. The pseudo-planar monomials were first investigated by Schmidt and Zhou [20], and subsequently by Scherr and Zieve [19]. Moreover, in [20, Conjecture 8], it is conjectured that the only exponents that give pseudo-planar monomials are those listed in Table 1.

Besides pseudo-planar monomial functions, the next simplest cases are pseudo-planar binomials. In this section, we construct three classes of pseudo-planar binomials on the field $\mathbb{F}_{2^{3m}}$. The following result will be useful.

Lemma 3.1 ([15, p. 362])**.** *Let q be a prime power and $\mathbb{F}_{q^r}$ be an extension of $\mathbb{F}_q$. Then the linearized polynomial*

$$L(x) = \sum_{i=0}^{r-1} c_i x^{q^i} \in \mathbb{F}_{q^r}[x]$$

is a permutation of $\mathbb{F}_{q^r}$ if and only if

$$\det \begin{pmatrix} c_0 & c_{r-1}^q & c_{r-2}^{q^2} & \cdots & c_1^{q^{r-1}} \\ c_1 & c_0^q & c_{r-1}^{q^2} & \cdots & c_2^{q^{r-1}} \\ c_2 & c_1^q & c_0^{q^2} & \cdots & c_3^{q^{r-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{r-1} & c_{r-2}^q & c_{r-3}^{q^2} & \cdots & c_0^{q^{r-1}} \end{pmatrix} \ne 0.$$

Let m be a positive integer. The relative trace (resp. norm) from $\mathbb{F}_{2^{3m}}$ to $\mathbb{F}_{2^m}$ is denoted by Tr_3 (resp. N_3) from now on.

Proposition 3.2. *Suppose m is an even positive integer, then the function*

$$f(x) = a^{2^{2m}+1}x^{2^{2m}+1} + a^{-(2^m+1)}x^{2^m+1}$$

is pseudo-planar on $\mathbb{F}_{2^{3m}}$ if and only if

$$\mathrm{Tr}_3((a^{2^{2m}+2^m} + a^{-2^{2m}-2^m-2})(a^{2^m+1} + \epsilon^{2^m-1})\epsilon^{2^m+2} + a^{2^m-2^{2m}}\epsilon^3 + \epsilon) \neq 0$$

for all $\epsilon \in \mathbb{F}_{2^{3m}}^*$.

Proof. Set $t = 2^m$. For each $\epsilon \in \mathbb{F}_{2^{3m}}^*$,

$$f(x+\epsilon) + f(x) + \epsilon x = a^{t^2+1}\epsilon x^{t^2} + a^{-(t+1)}\epsilon x^t + (a^{t^2+1}\epsilon^{t^2} + a^{-(t+1)}\epsilon^t + \epsilon)x + (a\epsilon)^{t^2+1} + (a^{-1}\epsilon)^{t+1}.$$

Then it suffices to show that the polynomial

$$G_\epsilon(x) := a^{t^2+1}\epsilon x^{t^2} + a^{-(t+1)}\epsilon x^t + (a^{t^2+1}\epsilon^{t^2} + a^{-(t+1)}\epsilon^t + \epsilon)x$$

is a permutation on $\mathbb{F}_{2^{3m}}$ for any $\epsilon \in \mathbb{F}_{2^{3m}}^*$. By Lemma 3.1, we see that $G_\epsilon(x)$ is a permutation if and only if

$$\begin{aligned}
&\det\begin{pmatrix} a^{t^2+1}\epsilon^{t^2} + a^{-(t+1)}\epsilon^t + \epsilon & a^{t+1}\epsilon^t & a^{-(t^2+1)}\epsilon^{t^2} \\ a^{-(t+1)}\epsilon & a^{t+1}\epsilon + a^{-(t^2+t)}\epsilon^{t^2} + \epsilon^t & a^{t^2+t}\epsilon^{t^2} \\ a^{t^2+1}\epsilon & a^{-(t^2+t)}\epsilon^t & a^{t^2+t}\epsilon^t + a^{-(t^2+1)}\epsilon + \epsilon^{t^2} \end{pmatrix} \\
=&\mathrm{Tr}_3((a^{t^2+t} + a^{-t^2-t-2})(a^{t+1} + \epsilon^{t-1})\epsilon^{t+2} + a^{t-t^2}\epsilon^3 + \epsilon) \\
=&\mathrm{Tr}_3((a^{2^{2m}+2^m} + a^{-2^{2m}-2^m-2})(a^{2^m+1} + \epsilon^{2^m-1})\epsilon^{2^m+2} + a^{2^m-2^{2m}}\epsilon^3 + \epsilon) \\
\neq&0.
\end{aligned}$$

This finishes the proof. □

Remark 3.3. *We are unable to simplify the necessary and sufficient conditions in Proposition 3.2 to provide a more concise criterion. We also cannot decide whether this construction will give infinite families of pseudo-planar binomials or not.*

Here we give two examples. For any $a \in \mathbb{F}_{2^n}^*$, denote the multiplicative order of a by $\mathrm{ord}\,(a)$.

Example 3.4. *When $m = 2$, direct computation via computer program shows that*

$$f(x) = a^{17}x^{17} + a^{-5}x^5$$

is pseudo-planar on $\mathbb{F}_{2^{3m}}$ if and only if $\mathrm{ord}\,(a) \in \{9, 63\}$, which coincides with the condition in Proposition 3.2.

Example 3.5. *When $m = 4$, direct computation via computer program shows that*

$$f(x) = a^{257}x^{257} + a^{-17}x^{17}$$

is pseudo-planar on $\mathbb{F}_{2^{3m}}$ if and only if ord$(a) \in \{9, 63, 117, 819\}$, which coincides with the condition in Proposition 3.2.

In the following of this section, we give two infinite families of pseudo-planar binomials.

Let m be a positive integer. Suppose $\epsilon \in \mathbb{F}_{2^{3m}}^* \backslash \mathbb{F}_{2^m}$ and its minimal polynomial over $\mathbb{F}_{2^m}$ is

$$C_\epsilon(x) = x^3 + B_1x^2 + B_2x + B_3 \in \mathbb{F}_{2^m}[x] \quad (B_3 \neq 0).$$

Denote the three roots of $C_\epsilon(x)$ by $x_1(= \epsilon)$, $x_2(= \epsilon^{2^m})$, and $x_3(= \epsilon^{2^{2m}})$. It follows that

$$\begin{aligned} B_1 =& x_1 + x_2 + x_3 = \mathrm{Tr}_3(\epsilon), \\ B_2 =& x_1x_2 + x_1x_3 + x_2x_3, \\ B_3 =& x_1x_2x_3 = \mathrm{N}_3(\epsilon). \end{aligned}$$

We can verify that

$$\begin{aligned} \mathrm{Tr}_3(\epsilon^3) =& x_1^3 + x_2^3 + x_3^3 \\ =& (x_1 + x_2 + x_3)^3 + x_1x_2x_3 + (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) \\ =& B_1^3 + B_3 + B_1B_2, \\ \mathrm{Tr}_3(\epsilon^{1+2^{m+1}}) =& \mathrm{Tr}_3(x_1x_2^2) = x_1x_2^2 + x_2x_3^2 + x_3x_1^2. \end{aligned}$$

Set $u_1 = \mathrm{Tr}_3(x_1x_3^2)$ and $u_2 = \mathrm{Tr}_3(x_1x_2^2)$. Then we have

$$u_1 + u_2 = B_3 + B_1B_2, \tag{3}$$

$$u_1u_2 = B_1^3B_3 + B_2^3 + B_3^2. \tag{4}$$

We would like to point out that part of the following proof for Proposition 3.6 with $m \equiv 1 \pmod 3$ is provided by one of the anonymous referee and communicated with the Associate Editor.

Proposition 3.6. *Let m be a positive integer and $m \not\equiv 2 \pmod 3$. Then*

$$f(x) = x^{2^m+1} + x^{2^{2m}+2^m}$$

is pseudo-planar on $\mathbb{F}_{2^{3m}}$.

Proof. A similar analysis as the proof of Proposition 3.2 shows that f is pseudo-planar if and only if

$$\mathrm{N}_3(\epsilon) + \mathrm{Tr}_3(\epsilon^3 + \epsilon^{1+2^{m+1}}) \neq 0$$

for every $\epsilon \in \mathbb{F}_{2^{3m}}^*$. For convenience, we write $M_\epsilon = \mathrm{N}_3(\epsilon) + \mathrm{Tr}_3(\epsilon^3 + \epsilon^{1+2^{m+1}})$.

First suppose $\epsilon \in \mathbb{F}_{2^m}^*$. Then $M_\epsilon = \mathrm{N}_3(\epsilon) + \mathrm{Tr}_3(\epsilon^3 + \epsilon^3) = \mathrm{N}_3(\epsilon) \neq 0$.

Now let $\epsilon \in \mathbb{F}_{2^{3m}}^* \backslash \mathbb{F}_{2^m}$. It can be verified that

$$M_\epsilon = B_1^3 + B_1 B_2 + u_2.$$

We will split our consideration into two parts according to whether $B_1 = 0$ or not.

Suppose $B_1 = 0$. Then $M_\epsilon = u_2$. Now if $M_\epsilon = 0$, from (4), we get $B_3 = B_2^{3/2}$. Therefore $B_2 \neq 0$, since otherwise $B_1 = B_2 = B_3 = 0$, which is impossible. Replace $B_3 = B_2^{3/2}$ into $C_\epsilon(x)$, we obtain

$$\left(\frac{\epsilon}{B_2^{1/2}}\right)^3 + \frac{\epsilon}{B_2^{1/2}} + 1 = 0,$$

which implies that

$$\frac{\epsilon}{B_2^{1/2}} \in \mathbb{F}_{2^3}.$$

That is to say that $\epsilon = b\beta$ with $\beta := B_2^{1/2} \in \mathbb{F}_{2^m}^*$ and $b := \epsilon / B_2^{1/2} \in \mathbb{F}_{2^3}^*$. If $m \equiv 0 \pmod 3$, then $b \in \mathbb{F}_{2^3}^* \subseteq \mathbb{F}_{2^m}$, so $\epsilon \in \mathbb{F}_{2^m}$, which is a contradiction. If $m \equiv 1 \pmod 3$, we see that $2^m \equiv 2 \pmod 7$ and $2^{m+1} \equiv 2^{2m} \equiv 4 \pmod 7$. Then

$$\begin{aligned}
\mathrm{Tr}_3(\epsilon^3) =& \mathrm{Tr}_3((b\beta)^3) = \beta^3 \mathrm{Tr}_3(b^3), \\
\mathrm{Tr}_3(\epsilon^{1+2^{m+1}}) =& \mathrm{Tr}_3(b^{1+2^{m+1}} \beta^{1+2^{m+1}}) = \beta^3 \mathrm{Tr}_3(b^5) = \beta^3 \mathrm{Tr}_3(b^3).
\end{aligned}$$

Hence

$$M_\epsilon = \mathrm{N}_3(\epsilon) + \mathrm{Tr}_3((b\beta)^3 + (b\beta)^{1+2^{m+1}}) = \mathrm{N}_3(\epsilon) \neq 0$$

which is a contradiction.

Next suppose $B_1 \neq 0$. Without loss of generality we let $B_1 = 1$. Assume that $M_\epsilon = 1 + B_2 + u_2 = 0$, then $u_2 = B_2 + 1$. Replace it in (3) and (4), we get $u_1 = B_3 + 1$, and

$$B_2^3 + B_3^2 + B_2 B_3 + B_2 + 1 = 0. \tag{5}$$

If $B_2 = 0$, then $B_3 = 1$, and

$$\epsilon^3 + \epsilon^2 + 1 = 0.$$

Similarly as above, this finally leads to $M_\epsilon = \mathrm{N}_3(\epsilon) \neq 0$, which contradicts the assumption that $M_\epsilon = 0$. If $B_2 \neq 0$, we write $w = (B_3 + 1)/B_2$. Then (5) becomes $B_2 = w^2 + w$. Hence $B_3 = B_2 w + 1 = w^3 + w^2 + 1$. We rewrite $C_\epsilon(x)$ as

$$x^3 + x^2 + (w^2 + w)x + (w^3 + w^2 + 1) = 0. \tag{6}$$

Let the three roots of the polynomial x^3+x+1 in $\mathbb{F}_{2^m}$ be τ_1, $\tau_2(=\tau_1^2)$, and $\tau_3(=\tau_1^4)$. We compute that

$$\begin{aligned}
&(\tau_2+\tau_1 w+1)^3+(\tau_2+\tau_1 w+1)^2+B_2(\tau_2+\tau_1 w+1)+B_3\\
=&(\tau_1^3+\tau_1+1)w^3+(\tau_2\tau_1^2+\tau_2+\tau_1)w^2+(\tau_2^2\tau_1+\tau_2+\tau_1+1)w+\tau_2^3+\tau_2+1\\
=&0.
\end{aligned}$$

Therefore the element $\tau_2+\tau_1 w+1$ is a root of $C_\epsilon(x)$. If $m\equiv 0 \pmod 3$, then $\tau_i\,(1\le i\le 3)\in\mathbb{F}_{2^3}\subseteq\mathbb{F}_{2^m}$ and hence $\tau_2+\tau_1 w+1\in\mathbb{F}_{2^m}$. This contradicts the fact that $C_\epsilon(x)$ is irreducible over $\mathbb{F}_{2^m}$. If $m\equiv 1 \pmod 3$, we see that

$$\begin{aligned}
\mathrm{Tr}_3(\epsilon^3)=&\mathrm{Tr}_3((\tau_2+\tau_1 w+1)^3)\\
=&(\tau_2+\tau_1 w+1)^3+(\tau_2+\tau_1 w+1)^{3\cdot 2^m}+(\tau_2+\tau_1 w+1)^{3\cdot 2^{2m}}\\
=&(\tau_2+\tau_1 w+1)^3+(\tau_3+\tau_2 w+1)^3+(\tau_1+\tau_3 w+1)^3\\
=&(\tau_1^3+\tau_2^3+\tau_3^3)w^3+(\tau_1^2\tau_2+\tau_2^2\tau_3+\tau_3^2\tau_1+\tau_1^2+\tau_2^2+\tau_3^2)w^2\\
&+(\tau_1\tau_2^2+\tau_2\tau_3^2+\tau_3^2\tau_1^2+\tau_1+\tau_2+\tau_3)w+(\tau_1^3+\tau_2^3+\tau_3^3+\tau_1^2+\tau_2^2+\tau_3^2+\tau_1+\tau_2+\tau_3+1)\\
=&w^3+w^2,\\
\mathrm{Tr}_3(\epsilon^{1+2^{m+1}})=&\mathrm{Tr}_3((\tau_2+\tau_1 w+1)^{1+2^{m+1}})\\
=&\mathrm{Tr}_3((\tau_2+\tau_1 w+1)(\tau_1+\tau_3 w^2+1))\\
=&(\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1)w^3+(\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1+\tau_1+\tau_2+\tau_3)w^2\\
&+(\tau_1^2+\tau_2^2+\tau_3^2+\tau_1+\tau_2+\tau_3)w+(\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1+1)\\
=&w^3+w^2.
\end{aligned}$$

Thus

$$M_\epsilon=\mathrm{N}_3(\epsilon)+\mathrm{Tr}_3(\epsilon^3+\epsilon^{1+2^{m+1}})=\mathrm{N}_3(\epsilon)\ne 0,$$

which is also a contradiction. □

Remark 3.7. *Let $m\equiv 2 \pmod 3$. Suppose $\epsilon\in\mathbb{F}_{2^{3m}}$ satisfying $\epsilon^3+\epsilon^2+1=0$. (It is not hard to show that such ϵ exists.) Then we can compute $M_\epsilon=\mathrm{N}_3(\epsilon)+\mathrm{Tr}_3(\epsilon^3+\epsilon^{1+2^{m+1}})=\sum_{i=0}^{6}\epsilon^i=0$. Thus $f(x)=x^{2^m+1}+x^{2^{2m}+2^m}$ is not pseudo-planar on $\mathbb{F}_{2^{3m}}$.*

Proposition 3.8. *Let m be a positive integer and $m\not\equiv 1 \pmod 3$. Then*

$$f(x)=x^{2^{2m}+1}+x^{2^{2m}+2^m}$$

is pseudo-planar on $\mathbb{F}_{2^{3m}}$.

Proof. A similar analysis to the proof of Proposition 3.2 shows that f is pseudo-planar if and only if

$$\mathrm{N}_3(\epsilon)+\mathrm{Tr}_3(\epsilon^3+\epsilon^{2+2^m})\ne 0$$

for every $\epsilon\in\mathbb{F}_{2^{3m}}^*$. The remaining discussion is analogous to Proposition 3.6. □

4 Association schemes arising from pseudo-planar functions

Let $R = GR(4,n)$ be a Galois ring. For any set A whose elements belong to R (A may be a multiset), we identify A and the group ring element $\sum_{g\in A} d_g g \in \mathbb{Z}[R]$ throughout this section, where d_g is the multiplicity of $g \in A$. It is well known that the Teichmüller system T is a $(2^n, 2^n, 2^n, 1)$-RDS in R with respect to Z, where

$$Z = \{2x \mid x \in R\}.$$

Bonnecaze and Duursma in [5] showed that T gives rise to an association scheme. More specifically, when $n \geq 3$, we have four disjoint subsets

$$\Omega_0 = \{0\},\ \Omega_1 = T^*,\ \Omega_2 = \{-x \mid x \in \Omega_1\},\ \Omega_3 = Z \setminus \{0\},$$

where $T^* := T \setminus \{0\}$. The rest elements of R are divided into two classes. Let Ω_4 contain the remaining ones which appear in the multiset T^2 and let Ω_5 contain the remaining ones which do not. The partition $\{\Omega_i \mid 0 \leq i \leq 5\}$ forms a Schur ring over R, which leads to a 5-class association scheme. For a pseudo-planar function f, the set

$$D_f = \{x + 2\sqrt{f(x)} \mid x \in T\}$$

is also a $(2^n, 2^n, 2^n, 1)$-RDS in R with respect to Z (see [20]). Consequently, it is natural to ask whether an association scheme can also be obtained from D_f or not. In this section, we prove that any relative difference set D_f, which necessarily arises from a pseudo-planar function f, will produce an association scheme. In fact, the partition of R is obtained in a similar way. At first, we have four subsets

$$\mathcal{S}_0 = \{0\},\ \mathcal{S}_1 = D_f \setminus \{0\},\ \mathcal{S}_2 = \{-x \mid x \in \mathcal{S}_1\} = \mathcal{S}_1^{(-1)},\ \mathcal{S}_3 = Z \setminus \{0\}.$$

Furthermore, the remaining elements of R are divided into two classes. Let $\mathcal{S}_4$ contain the remaining ones which appear in the multiset D_f^2 and let $\mathcal{S}_5$ contain the remaining ones which do not.

Using the following lemma, it is straightforward to verify that $\{\mathcal{S}_i \mid 0 \leq i \leq 5\}$ indeed forms a partition of R.

Lemma 4.1 ([5, Theorem 1]). *Let $R = GR(4,n)$ and T be the Teichmüller system.*

1. *The multiset $TT^{(-1)}$ contains 0 with multiplicity 2^n, no other elements of Z, and the elements outside Z with multiplicity one.*

2. *The multiset T^2 contains the elements of Z with multiplicity one, and half of the elements outside Z with multiplicity two.*

Now we consider the dual partition of $\{\mathcal{S}_i \mid 0 \leq i \leq 5\}$ on the character group $\widehat{R}$. According to [20, Theorem 3], if f is pseudo-planar then $\chi(D_f)$ takes six values when χ ranges over $\widehat{R}$. More precisely,

$$\chi_a(D_f) = \begin{cases} 2^n & \text{for } a = 0\ , \\ 0 & \text{for } a \in Z \setminus \{0\}, \\ \pm 2^{(n-1)/2} \pm 2^{(n-1)/2}\mathbf{i} & \text{for } a \in R \setminus Z, \end{cases}$$

when n is odd and

$$\chi_a(D_f) = \begin{cases} 2^n & \text{for } a = 0\ , \\ 0 & \text{for } a \in Z \setminus \{0\}, \\ \pm 2^{n/2} \text{ or } \pm 2^{n/2}\mathbf{i} & \text{for } a \in R \setminus Z, \end{cases}$$

when n is even. Furthermore, it is natural to investigate the frequencies of these six values when χ ranges over $\widehat{R}$. Similar to the case of almost perfect nonlinear functions, we introduce the definition of Fourier spectrum of a pseudo-planar function f as follows.

Definition 4.1. *The Fourier spectrum of a pseudo-planar function f is defined to be the multiset*

$$\{\chi(D_f) \mid \chi \in \widehat{R}\}.$$

As a consequence of Theorem 4.4 below, we can show that the Fourier spectrum is the same for every pseudo-planar function.

Note that $\chi(\mathcal{S}_1) = \chi(D_f) - 1$. There is a natural partition $\{\mathcal{E}_i \mid 0 \le i \le 5\}$ on the character group $\widehat{R}$, where χ_a and χ_b are in the same class if and only if $\chi_a(\mathcal{S}_1) = \chi_b(\mathcal{S}_1)$. The partition $\{\mathcal{E}_i \mid 0 \le i \le 5\}$ is given as follows:

$$\begin{array}{rcl} \mathcal{E}_0 &=& \{\chi_0\}, \\ \mathcal{E}_1 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1\} = \{\chi_a \mid a \in Z \setminus \{0\}\}, \\ \mathcal{E}_2 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 + 2^{(n-1)/2} + 2^{(n-1)/2}\mathbf{i}\}, \\ \mathcal{E}_3 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 + 2^{(n-1)/2} - 2^{(n-1)/2}\mathbf{i}\}, \\ \mathcal{E}_4 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 - 2^{(n-1)/2} + 2^{(n-1)/2}\mathbf{i}\}, \\ \mathcal{E}_5 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 - 2^{(n-1)/2} - 2^{(n-1)/2}\mathbf{i}\}, \end{array} \tag{7}$$

when n is odd and

$$\begin{array}{rcl} \mathcal{E}_0 &=& \{\chi_0\}, \\ \mathcal{E}_1 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1\} = \{\chi_a \mid a \in Z \setminus \{0\}\}, \\ \mathcal{E}_2 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 + 2^{n/2}\}, \\ \mathcal{E}_3 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 - 2^{n/2}\}, \\ \mathcal{E}_4 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 + 2^{n/2}\mathbf{i}\}, \\ \mathcal{E}_5 &=& \{\chi \in \widehat{R} \mid \chi(\mathcal{S}_1) = -1 - 2^{n/2}\mathbf{i}\}, \end{array} \tag{8}$$

when n is even.

In the following we show that $(R, \{\mathcal{S}_i\}_{i=0}^5)$ is a Schur ring, whose dual is $(\widehat{R}, \{\mathcal{E}_i\}_{i=0}^5)$. We first use Lemma 4.2 and Lemma 4.3 to prove that $\mathcal{S}_4$ can be expressed as a linear combination of $\mathcal{S}_1^2, \mathcal{S}_2$, and $\mathcal{S}_3$. Then the values of $\chi(\mathcal{S}_4)$ and $\chi(\mathcal{S}_5)$ can be determined where χ ranges over $\widehat{R}$. Combining this with Bannai-Muzychuk criterion, the result follows.

Lemma 4.2. *Let $R = GR(4, n)$, and f be a pseudo-planar function over $\mathbb{F}_{2^n}$ which can be identified with a map from T to T. Let $D_f = \{x + 2\sqrt{f(x)} \mid x \in T\}$ and $\mathcal{S}_1 = D_f \setminus \{0\}$.*

1. *The multiset $\mathcal{S}_1\mathcal{S}_1^{(-1)}$ consists of 0 with multiplicity $2^n - 1$ and the elements of $\mathcal{S}_4 \cup \mathcal{S}_5$ with multiplicity one.*

2. *The multiset $\mathcal{S}_1^2$ contains the elements of $\mathcal{S}_3$ with multiplicity one. In $\mathcal{S}_1^2$, the multiplicity of an element outside $\mathcal{S}_3$ is either zero or two.*

Proof. 1. Since f is pseudo-planar, the set D_f is an RDS with $D_f D_f^{(-1)} = 2^n\mathcal{S}_0 + (R - Z)$. It is easy to verify that $\mathcal{S}_1\mathcal{S}_1^{(-1)} = (2^n - 1)\mathcal{S}_0 + (R - Z - \mathcal{S}_1 - \mathcal{S}_2) = (2^n - 1)\mathcal{S}_0 + \mathcal{S}_4 + \mathcal{S}_5$.

2. For any $x, y, z \in T^*$, suppose $x + 2\sqrt{f(x)} + y + 2\sqrt{f(y)} = 2z$. Then $x + 2\sqrt{f(x)} = y + 2(\sqrt{f(y)} \oplus z \oplus y)$. By the unique representation (2), we must have $x = y = z$. Hence $\mathcal{S}_1^2$ contains the elements of $\mathcal{S}_3$ with multiplicity one. Suppose $\mathcal{S}_1^2 = \mathcal{S}_3 + 2U_f$, where $U_f = \sum_{g\in R\setminus\mathcal{S}_3} d_g g$, it suffices to show that $d_g = 0$ or 1. Since $\mathcal{S}_1^2 = \mathcal{S}_3 + 2U_f$, applying the principal character, we have

$$\sum_{g\in R\setminus\mathcal{S}_3} d_g = (2^n - 1)(2^{n-1} - 1). \tag{9}$$

Now, we consider the coefficient of 0 in $\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2$. On one hand, $\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2 = (\mathcal{S}_1\mathcal{S}_1^{(-1)})^2 = ((2^n-1)\mathcal{S}_0+\mathcal{S}_4+\mathcal{S}_5)^2 = (2^n-1)^2\mathcal{S}_0+2(2^n-1)(\mathcal{S}_4+\mathcal{S}_5)+(\mathcal{S}_4+\mathcal{S}_5)^2$. Since $\mathcal{S}_4+\mathcal{S}_5 = \mathcal{S}_4^{(-1)}+\mathcal{S}_5^{(-1)}$ and $|\mathcal{S}_4 \cup \mathcal{S}_5| = (2^n - 1)(2^n - 2)$, we have $[(\mathcal{S}_4 + \mathcal{S}_5)^2]_0 = (2^n - 1)(2^n - 2)$. Consequently, $[\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2]_0 = (2^n - 1)(2^{n+1} - 3)$. On the other hand, $\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2 = (\mathcal{S}_3 + 2U_f)(\mathcal{S}_3 + 2U_f^{(-1)}) = \mathcal{S}_3^2+2\mathcal{S}_3U_f+2\mathcal{S}_3U_f^{(-1)}+4U_fU_f^{(-1)}$. It is easy to check that $[\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2]_0 = 2^n-1+4\sum_{g\in R\setminus\mathcal{S}_3} d_g^2$. Therefore, we have

$$\sum_{g\in R\setminus\mathcal{S}_3} d_g^2 = (2^n - 1)(2^{n-1} - 1). \tag{10}$$

By Equations (9)-(10), we have

$$\sum_{g\in R\setminus\mathcal{S}_3} d_g = \sum_{g\in R\setminus\mathcal{S}_3} d_g^2,$$

which implies that $d_g = 0$ or 1.

□

Now we proceed to determine U_f mentioned in the proof of Lemma 4.2.

Lemma 4.3. *Let $R = GR(4, n)$ and f be a pseudo-planar function over $\mathbb{F}_{2^n}$. Let $\mathcal{S}_i, 0 \le i \le 5$ be defined as above. Then we have*

1. *$\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_4$ when n is odd;*
2. *$\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_2 + 2\mathcal{S}_4$ when n is even.*

Proof. We only present the proof for Assertion 2, because a similar method can be applied to Assertion 1. The partition $\{\mathcal{E}_i \mid 0 \le i \le 5\}$ is given in (8). Define $m_i = |\mathcal{E}_i|$ for $0 \le i \le 5$, then $m_0 = 1$ and $m_1 = 2^n - 1$. As a preparation, we first consider the relations between m_2, m_3, m_4 and m_5. A straightforward computation shows that $\sum_{a\in R} \chi_a(D_f) = 2^{2n}$. On the other hand,

$$\begin{aligned}\sum_{a\in R} \chi_a(D_f) &= m_0 \cdot 2^n + m_1 \cdot 0 + m_2 \cdot 2^{n/2} + m_3 \cdot (-2^{n/2}) + m_4 \cdot 2^{n/2}\mathbf{i} + m_5 \cdot (-2^{n/2}\mathbf{i}) \\ &= 2^n + 2^{n/2}(m_2 - m_3) + 2^{n/2}(m_4 - m_5)\mathbf{i}.\end{aligned}$$

Consequently, we have

$$\begin{aligned} m_2 - m_3 &= 2^{3n/2} - 2^{n/2}, \\ m_4 - m_5 &= 0. \end{aligned}$$

By Lemma 4.2, $\mathcal{S}_1^2 = \mathcal{S}_3 + 2U_f$. For any $x, y \in T$, if $x + 2\sqrt{f(x)} + y + 2\sqrt{f(y)} = 0$, then $x = y + 2(\sqrt{f(x)} \oplus \sqrt{f(y)} \oplus y)$. The latter equation implies $x = y = 0$. Hence, 0 is not an element of $\mathcal{S}_1^2$, i.e., $U_f \cap \mathcal{S}_0 = \emptyset$. By definition, we see that $\mathcal{S}_4 \subset U_f$ and $\mathcal{S}_5 \cap U_f = \emptyset$. It remains to determine the relationship between $\mathcal{S}_1$, $\mathcal{S}_2$ and U_f.

Firstly, we consider $\mathcal{S}_1$. By the inversion formula,

$$\begin{aligned} [D_f^2 D_f^{(-1)}]_0 &= \frac{1}{|R|} \sum_{a \in R} \chi_a(D_f^2 D_f^{(-1)}) \\ &= \frac{1}{|R|} \sum_{a \in R} |\chi_a(D_f)|^2 \chi_a(D_f) \\ &= \frac{1}{|R|}(2^{3n} + 2^{3n/2}(m_2 - m_3) + 2^{3n/2}(m_4 - m_5)\mathbf{i}) \\ &= 2^{n+1} - 1. \end{aligned}$$

Note that

$$D_f^2 D_f^{(-1)} = \mathcal{S}_1^2 \mathcal{S}_1^{(-1)} + 2\mathcal{S}_1 \mathcal{S}_1^{(-1)} + \mathcal{S}_1^2 + 2\mathcal{S}_1 + \mathcal{S}_2 + \mathcal{S}_0,$$

$[\mathcal{S}_1 \mathcal{S}_1^{(-1)}]_0 = 2^n - 1$ and $[\mathcal{S}_0]_0 = 1$. It follows that $[\mathcal{S}_1^2 \mathcal{S}_1^{(-1)}]_0$=0. Hence, $\mathcal{S}_1^2$ contains no element of $\mathcal{S}_1$, namely, $\mathcal{S}_1 \cap U_f = \emptyset$.

Secondly, we consider $\mathcal{S}_2$. By the inversion formula,

$$\begin{aligned} [D_f^3]_0 &= \frac{1}{|R|} \sum_{a \in R} \chi_a(D_f)^3 \\ &= \frac{1}{|R|}(2^{3n} + 2^{3n/2}(m_2 - m_3) - 2^{3n/2}(m_4 - m_5)\mathbf{i}) \\ &= 2^{n+1} - 1. \end{aligned}$$

From

$$D_f^3 = (\mathcal{S}_0 + \mathcal{S}_1)^3 = \mathcal{S}_0 + 3\mathcal{S}_1 + 3\mathcal{S}_1^2 + \mathcal{S}_1^3,$$

$[\mathcal{S}_0]_0 = 1$, and $[\mathcal{S}_1]_0 = [\mathcal{S}_1^2]_0 = 0$, it follows that $[\mathcal{S}_1^2 \mathcal{S}_2^{(-1)}]_0 = [\mathcal{S}_1^3]_0 = 2^{n+1} - 2$. By Lemma 4.2, $\mathcal{S}_1^2$ contains each element of $\mathcal{S}_2$ with multiplicity at most two. On the other hand, we have $[\mathcal{S}_1^2 \mathcal{S}_2^{(-1)}]_0 = 2|\mathcal{S}_2|$. Hence, each element of $\mathcal{S}_2$ appears in $\mathcal{S}_1^2$ with multiplicity exactly two. Therefore, when n is even, we have $\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_2 + 2\mathcal{S}_4$. $\square$

The partition $\{\mathcal{S}_i \mid 0 \le i \le 5\}$ of R induces a partition $\{\mathcal{R}_i \mid 0 \le i \le 5\}$ of $R \times R$, where

$$\mathcal{R}_i = \{(x, y) \in R \times R \mid x - y \in \mathcal{S}_i\} \quad (0 \le i \le 5).$$

Now we are ready to prove that $(R, \{\mathcal{R}_i\}_{i=0}^5)$ indeed forms an association scheme.

Theorem 4.4. *Let $R = GR(4,n)$ and $\mathcal{S}_i, 0 \le i \le 5$ be defined as above. Then $(R, \{\mathcal{S}_i\}_{i=0}^5)$ is a Schur ring, whose dual is $(\widehat{R}, \{\mathcal{E}_i\}_{i=0}^5)$. If $n \ge 3$, then $(R, \{\mathcal{R}_i\}_{i=0}^5)$ forms a 5-class association scheme, whose first eigenmatrix is given as follows. When n is odd, suppose $b = 2^{(n-1)/2}$, we have*

$$P = \begin{bmatrix} 1 & 2\,b^2-1 & 2\,b^2-1 & 2\,b^2-1 & 2\,b^4-3\,b^2+1 & 2\,b^4-3\,b^2+1 \\ 1 & -1 & -1 & 2\,b^2-1 & -b^2+1 & -b^2+1 \\ 1 & -1+b+b\mathbf{i} & -1+b-b\mathbf{i} & -1 & (1-b)\,(1-b\mathbf{i}) & (1-b)\,(1+b\mathbf{i}) \\ 1 & -1+b-b\mathbf{i} & -1+b+b\mathbf{i} & -1 & (1-b)\,(1+b\mathbf{i}) & (1-b)\,(1-b\mathbf{i}) \\ 1 & -1-b+b\mathbf{i} & -1-b-b\mathbf{i} & -1 & (1+b)\,(1-b\mathbf{i}) & (1+b)\,(1+b\mathbf{i}) \\ 1 & -1-b-b\mathbf{i} & -1-b+b\mathbf{i} & -1 & (1+b)\,(1+b\mathbf{i}) & (1+b)\,(1-b\mathbf{i}) \end{bmatrix}. \tag{11}$$

When n is even, suppose $b = 2^{(n-2)/2}$, we have

$$P = \begin{bmatrix} 1 & 4\,b^2-1 & 4\,b^2-1 & 4\,b^2-1 & 8\,b^4-10\,b^2+2 & 8\,b^4-2\,b^2 \\ 1 & -1 & -1 & 4\,b^2-1 & -2\,b^2+2 & -2\,b^2 \\ 1 & 2\,b-1 & 2\,b-1 & -1 & 2\,b^2-4\,b+2 & -2\,b^2 \\ 1 & -2\,b-1 & -2\,b-1 & -1 & 2\,b^2+4\,b+2 & -2\,b^2 \\ 1 & -1+2\,b\mathbf{i} & -1-2\,b\mathbf{i} & -1 & -2\,b^2+2 & 2\,b^2 \\ 1 & -1-2\,b\mathbf{i} & -1+2\,b\mathbf{i} & -1 & -2\,b^2+2 & 2\,b^2 \end{bmatrix}. \tag{12}$$

The second eigenmatrix is listed in Appendix.

Proof. According to the Bannai-Muzychuk criterion, it suffices to prove that $\chi_j(\mathcal{S}_i)$ is a constant for any $\chi_j \in \mathcal{E}_j$, where $0 \le i, j \le 5$. This is trivially true for any $0 \le j \le 5$ and $0 \le i \le 3$, which can be verified by direct computations. By Lemma 4.3, we can obtain $\chi_j(\mathcal{S}_4)$ for any $0 \le j \le 5$. Then we get the values of $\chi_j(\mathcal{S}_5)$. The information of $\chi_j(\mathcal{S}_4)$ and $\chi_j(\mathcal{S}_5)$ completes the proof. □

Remark 4.5.

(1) When $n = 1$, we have $\mathcal{S}_4 = \mathcal{S}_5 = \emptyset$. Then $(R, \{\mathcal{R}_i\}_{i=0}^5)$ is a 3-class association scheme. When $n = 2$, we get $\mathcal{S}_4 = \emptyset$. Then $(R, \{\mathcal{R}_i\}_{i=0}^5)$ forms a 4-class association scheme, whose first eigenmatrix can be easily determined as a submatrix of (11) or (12).

(2) The 5-class association scheme investigated in [5] can be regarded as a special case of our construction where the pseudo-planar function $f = 0$.

Corollary 4.6. *Suppose f is a pseudo-planar function over $\mathbb{F}_{2^n}$. Then the Fourier spectrum $\{\chi(D_f) \mid \chi \in \widehat{R}\}$ is that listed in Tables 2 or 3.*

Proof. Note that the frequency of each value can be obtained from the cardinality of the set $|\mathcal{E}_i|$. According to the second eigenmatrices listed in Appendix, the result now follows. □

Table 2: Fourier spectrum, n odd, $b = 2^{(n-1)/2}$

Value	Frequency
$2b^2$	1
0	$2b^2 - 1$
$b + b\mathbf{i}$	$\frac{b(2b^3+2b^2-b-1)}{2}$
$b - b\mathbf{i}$	$\frac{b(2b^3+2b^2-b-1)}{2}$
$-b + b\mathbf{i}$	$\frac{b(2b^3-2b^2-b+1)}{2}$
$-b - b\mathbf{i}$	$\frac{b(2b^3-2b^2-b+1)}{2}$

Table 3: Fourier spectrum, n even, $b = 2^{(n-2)/2}$

Value	Frequency
$4b^2$	1
0	$4b^2 - 1$
$2b$	$b(4b^3 + 4b^2 - b - 1)$
$-2b$	$b(4b^3 - 4b^2 - b + 1)$
$2b\mathbf{i}$	$b^2(4b^2 - 1)$
$-2b\mathbf{i}$	$b^2(4b^2 - 1)$

5 Concluding remarks

In this paper, three new classes of pseudo-planar binomial functions are provided. In addition, we present a class of association schemes derived from pseudo-planar functions, which can be considered as a natural generalization of the one studied in [5].

Let $D_1, D_2 \subset G$ be two $(2^n, 2^n, 2^n, 1)$ relative difference sets. They are *equivalent* if there exist some $\alpha \in \mathrm{Aut}(G)$ and $a \in G$ such that $\alpha(D_1) = D_2 + a$. Suppose f is a function from $\mathbb{F}_{2^n}$ to itself. It is proved in [20] that D_f is a $(2^n, 2^n, 2^n, 1)$-RDS in $R = GR(4, n)$ with respect to Z if and only if f is pseudo-planar. So we say that two pseudo-planar functions f_1 and f_2 are *equivalent* if the relative difference sets D_{f_1} and D_{f_2} are equivalent. By Corollary 4.6, the p-ranks and Smith normal forms of the relative difference set D_f associated with pseudo-planar functions are all the same. Therefore some other techniques are to be developed to solve the equivalence problem. The equivalence problem of pseudo-planar functions will be investigated in a manuscript prepared by Yue Zhou.

The following are several open problems.

1. All pseudo-planar binomials constructed in this paper are of type

$$f(x) = ax^{2^i+2^j} + bx^{2^k+2^l},$$

   where $i \neq j, k \neq l$, and $\{i, j\} \neq \{k, l\}$. For $n \leq 9$, an exhaustive computer search shows that these pseudo-planar binomials can only exist on the finite field of the form $\mathbb{F}_{2^n} = \mathbb{F}_{2^{3m}}$. Therefore, it is interesting to examine that whether these pseudo-planar binomials can only exist in $\mathbb{F}_{2^n}$ with $3|n$ or not.

2. The necessary and sufficient condition we provided in Proposition 3.2 is not easily handled. It is desirable if one can derive a simpler characterization.

Acknowledgements

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of this paper, and to Prof. Claude Carlet, the Associate Editor, for his excellent editorial job. We would like to thank Professor Qing Xiang and the anonymous reviewer for suggestions on the proofs of Proposition 3.6 and Proposition 3.8, and Dr. Yue Zhou for valuable comments and suggestions. S. Hu was supported by the Scholarship Award for Excellent Doctoral Student granted by Ministry of Education. T. Feng was supported in part by Fundamental Research Fund for the Central Universities of China, Zhejiang Provincial Natural Science Foundation under Grant No. LQ12A01019, in part by the National Natural Science Foundation of China under Grant No. 11201418, and in part by the Research Fund for Doctoral Programs from the Ministry of Education of China under Grant No. 20120101120089. G. Ge was supported by the National Natural Science Foundation of China under Grant No. 61171198 and Zhejiang Provincial Natural Science Foundation of China under Grant No. LZ13A010001.

Appendix

When n is odd, the second eigenmatrix of the association scheme is

$$Q=\begin{bmatrix} 1 & 2b^2-1 & \frac{b}{2}\left(2b^3+2b^2-b-1\right) & \frac{b}{2}\left(2b^3+2b^2-b-1\right) & \frac{b}{2}\left(2b^3-2b^2-b+1\right) & \frac{b}{2}\left(2b^3-2b^2-b+1\right) \\ 1 & -1 & \frac{b}{2}\left(b^2-1-(b^2+b)\mathbf{i}\right) & \frac{b}{2}\left(b^2-1+(b^2+b)\mathbf{i}\right) & \frac{b}{2}\left(1-b^2-(b^2-b)\mathbf{i}\right) & \frac{b}{2}\left(1-b^2+(b^2-b)\mathbf{i}\right) \\ 1 & -1 & \frac{b}{2}\left(b^2-1+(b^2+b)\mathbf{i}\right) & \frac{b}{2}\left(b^2-1-(b^2+b)\mathbf{i}\right) & \frac{b}{2}\left(1-b^2+(b^2-b)\mathbf{i}\right) & \frac{b}{2}\left(1-b^2-(b^2-b)\mathbf{i}\right) \\ 1 & 2b^2-1 & -\frac{b}{2}(1+b) & -\frac{b}{2}(1+b) & \frac{b}{2}(1-b) & \frac{b}{2}(1-b) \\ 1 & -1 & -\frac{b}{2}(1+b\mathbf{i}) & \frac{b}{2}(-1+b\mathbf{i}) & \frac{b}{2}(1+b\mathbf{i}) & \frac{b}{2}(1-b\mathbf{i}) \\ 1 & -1 & \frac{b}{2}(-1+b\mathbf{i}) & -\frac{b}{2}(1+b\mathbf{i}) & \frac{b}{2}(1-b\mathbf{i}) & \frac{b\left(b^2+1\right)}{2(1-b\mathbf{i})} \end{bmatrix}.$$

When n is even, the second eigenmatrix of the association scheme is

$$Q=\begin{bmatrix} 1 & 4b^2-1 & b\left(4b^3-b+4b^2-1\right) & b\left(4b^3-4b^2-b+1\right) & b^2\left(4b^2-1\right) & b^2\left(4b^2-1\right) \\ 1 & -1 & b\left(b+2b^2-1\right) & -\left(2b^2-b-1\right)b & -b^2(1+2b\mathbf{i}) & b^2(-1+2b\mathbf{i}) \\ 1 & -1 & b\left(b+2b^2-1\right) & -\left(2b^2-b-1\right)b & b^2(-1+2b\mathbf{i}) & -b^2(1+2b\mathbf{i}) \\ 1 & 4b^2-1 & -b(1+b) & -b(-1+b) & -b^2 & -b^2 \\ 1 & -1 & b(-1+b) & b(1+b) & -b^2 & -b^2 \\ 1 & -1 & -b(1+b) & -b(-1+b) & b^2 & b^2 \end{bmatrix}.$$

References

[1] K. Abdukhalikov. Symplectic spreads, planar functions and mutually unbiased bases. arXiv:1306.3478.

[2] K. Abdukhalikov, E. Bannai, and S. Suda. Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets. *J. Combin. Theory Ser. A*, 116(2):434–448, 2009.

[3] E. Bannai. Subschemes of some association schemes. *J. Algebra*, 144(1):167–188, 1991.

[4] E. Bannai and T. Ito. *Algebraic combinatorics I. Association schemes.* The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.

[5] A. Bonnecaze and I. M. Duursma. Translates of linear codes over Z_4. *IEEE Trans. Inform. Theory*, 43(4):1218–1230, 1997.

[6] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18. Springer-Verlag, Berlin, 1989.

[7] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, 51(6):2089–2102, 2005.

[8] P. Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.

[9] C. Ding. Cyclic codes from APN and planar functions. arxiv:1206.4687.

[10] C. Ding and H. Niederreiter. Systematic authentication codes from highly nonlinear functions. *IEEE Trans. Inform. Theory*, 50(10):2421–2428, 2004.

[11] C. Ding and J. Yin. Signal sets from functions with optimum nonlinearity. *IEEE Trans. Commun.*, 55(5):936–940, 2007.

[12] C. Ding and J. Yuan. A family of optimal constant-composition codes. *IEEE Trans. Inform. Theory*, 51(10):3668–3671, 2005.

[13] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé. The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40(2):301–319, 1994.

[14] Nicholas LeCompte, William J. Martin, and William Owens. On the equivalence between real mutually unbiased bases and a certain class of association schemes. *European J. Combin.*, 31(6):1499–1512, 2010.

[15] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.

[16] R. A. Liebler and R. A. Mena. Certain distance-regular digraphs and related rings of characteristic 4. *J. Combin. Theory Ser. A*, 47(1):111–123, 1988.

[17] M. E. Muzychuk. *V-rings of permutation groups with invariant metric*. PhD thesis, Kiev State University, 1987.

[18] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in cryptology—CRYPTO '92 (Santa Barbara, CA, 1992)*, volume 740 of *Lecture Notes in Comput. Sci.*, pages 566–574. Springer.

[19] Z. Scherr and M. E. Zieve. Planar monomials in characteristic 2. arXiv:1302.1244.

[20] K.-U. Schmidt and Y. Zhou. Planar functions over fields of characteristic two. *J. Algebraic Combin.*, 2014.

[21] Z. X. Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co. Inc., River Edge, NJ, 2003.

[22] G. Weng, W. Qiu, Z. Wang, and Q. Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44(1-3):49–62, 2007.

[23] J. Yuan, C. Carlet, and C. Ding. The weight distribution of a class of linear codes from perfect nonlinear functions. *IEEE Trans. Inform. Theory*, 52(2):712–717, 2006.

[24] Y. Zhou. $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations. *J. Combin. Designs.*, 21(12):563–584, 2013.