Cryptography and Communications (2025) 17:1641–1657
https://doi.org/10.1007/s12095-025-00801-x

RESEARCH

Bent partitions and Maiorana-McFarland association schemes

Nurdagül Anbar[1] · Tekgül Kalaycı[1] · Wilfried Meidl[2] · Ferruh Özbudak[1]

Received: 1 November 2024 / Accepted: 2 May 2025 / Published online: 22 May 2025
© The Author(s) 2025

Abstract
The recently introduced generalized semifield spreads are partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, which are constructed from presemifields with a certain property, called right $\mathbb{F}_{p^k}$-linearity. These partitions have similar properties as spreads. In particular, they are bent partitions, hence they yield a large number of bent functions, vectorial bent functions and amorphic association schemes. We show that with a slight change of parameters, we obtain inequivalent bent partitions, non-isomorphic divisible designs, and bent functions with various algebraic degrees. This is in contrast to classical spreads of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, which yield bent functions all of which have algebraic degree $(p-1)m$. We show that with right $\mathbb{F}_{p^k}$-linear presemifields we can obtain a large variety of vectorial dual-bent functions, which yield, not necessarily amorphic, association schemes. We investigate fusions of these association schemes, which reveal information on their inner structure, and may provide a tool to distinguish non-isomorphic association schemes.

Keywords Bent functions · Bent partitions · Generalized semifield spreads · Maiorana-McFarland functions · Association schemes

Mathematics Subject Classification (2010) 94D10 · 05E30 · 05B10

1 Introduction

For a prime p, a function f from an n-dimensional vector space $\mathbb{V}_n^{(p)}$ over the prime field $\mathbb{F}_p$ to $\mathbb{F}_p$ is called a *bent function* if for every $b \in \mathbb{V}_n^{(p)}$, the *Walsh coefficient*

$$\mathcal{W}_f(b) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x)-\langle b,x\rangle_n}, \quad \zeta_p = e^{2\pi\iota/p},$$

✉ Tekgül Kalaycı
tekgulkalayci@sabanciuniv.edu

Nurdagül Anbar
nurdagulanbar2@gmail.com

Wilfried Meidl
meidlwilfried@gmail.com

Ferruh Özbudak
ferruh.ozbudak@sabanciuniv.edu

[1] Sabancı University, MDBF, Orhanlı, Tuzla, İstanbul 34956, Turkey

[2] Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria

has absolute value $p^{n/2}$, where ι is a complex primitive 4-th root of unity and $\langle b, x\rangle_n$ denotes a (nondegenerate) inner product of $\mathbb{V}_n^{(p)}$.

For a Boolean bent function ($p = 2$), we have $\mathcal{W}_f(b) = 2^{n/2}(-1)^{f^*(b)}$ for a Boolean function f^* called the *dual* of f, which is also a bent function.

Whereas Boolean bent functions exist only for even n, *p-ary bent functions* from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, p odd, exist for even and for odd n. For the Walsh transform, we then have

$$\mathcal{W}_f(b) = \begin{cases} \pm\zeta_p^{f^*(b)} p^{n/2} & : \ n \text{ even or } n \text{ odd and } p \equiv 1 \mod 4, \\ \pm\iota\, \zeta_p^{f^*(b)} p^{n/2} & : \ n \text{ odd and } p \equiv 3 \mod 4, \end{cases}$$

where f^* is a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, which we again call the dual of f, see [17].

If $\mathcal{W}_f(b) = \epsilon\zeta_p^{f^*(b)} p^{n/2}$ with $\epsilon \in \{\pm 1, \pm\iota\}$ independent from b, then f is called *weakly regular*, if $\epsilon = 1$, *regular*. If ϵ varies with b, then f is called *non-weakly regular*. The dual of a weakly regular bent function is also bent, which does not always apply to non-weakly regular bent functions.

A function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ is called a *vectorial bent function* if every *component function* $F_c = \langle c, F(x)\rangle_k$, $c \in \mathbb{V}_k^{(p)} \setminus \{0\}$, is a p-ary bent function.

In [9], a concept of duality for vectorial bent functions is introduced: A vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ is called a *vectorial dual-bent function* if there exists a vectorial bent function $F^* : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ such that $\{F_c^* : c \in \mathbb{V}_k^{(p)} \setminus \{0\}\} = \{(F_c)^* : c \in \mathbb{V}_k^{(p)} \setminus \{0\}\}$, i.e., the components of F^* are the duals of the components of F. Observe that then

$$F_c^* = (F_{\sigma(c)})^* \quad \text{for some permutation } \sigma \text{ of } \mathbb{V}_k^{(p)} \setminus \{0\}. \tag{1}$$

A large number of bent and vectorial bent functions can be obtained from (normal) bent partitions, a concept which was introduced recently in [8].

A partition of $\mathbb{V}_n^{(p)}$ into subsets $A_1, A_2, \ldots, A_K$ is called a *bent partition of depth K* if every function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ with the following property is a bent function:

> Every $c \in \mathbb{F}_p$ has precisely K/p of the sets A_j in its preimage set $f^{-1}(c) = \{x \in \mathbb{V}_n^{(p)} : f(x) = c\}$.

Bent partitions can only exist for even n, with the exception that $p = K = 3$, since the preimage set partition of every ternary bent function is a bent partition, see Section III in [3]. Therefore, in the remainder of this article, n will always be an even integer.

As pointed out in [8], all sets A_j in a bent partition have the same cardinality, except for A_1 (w.l.o.g.), and $|A_1| = |A_j| \pm p^{n/2}$, $j = 2, \ldots, K$. For all so far known bent partitions other than preimage set partitions of ternary bent functions, we have $|A_1| = |A_j| + p^{n/2}$, and A_1 contains an $(n/2)$-dimensional subspace U. These bent partitions then give rise to a normal bent partition. A partition of $\mathbb{V}_n^{(p)}$ into an $(n/2)$-dimensional subspace U and sets $A_1, A_2, \ldots, A_K$ is called a *normal bent partition of depth K* if every function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ satisfying the following properties is a bent function:

(I) Every $c \in \mathbb{F}_p$ has precisely K/p of the sets A_j in its preimage set $f^{-1}(c)$, and
(II) f is also constant on U.

Clearly, taking the union of U with any of the sets A_j (and leaving the other sets unchanged) yields a bent partition, i.e., with a normal bent partition, we have bent partitions.

Well-known (normal) bent partitions of $\mathbb{V}_n^{(p)}$, $n = 2m$, are the bent partitions $\{U_0, U_1^*, \ldots, U_{p^m}^*\}$, $U_j^* = U_j \setminus \{0\}$, obtained from a spread, i.e., from a collection of $p^m + 1$

subspaces U_j of $\mathbb{V}_n^{(p)}$, each of dimension m, which pairwise intersect trivially. The bent functions obtained from such bent partitions are called partial spread bent functions. Examples are semifield spreads of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, which consist of the subspaces $U_s = \{(x, s \circ x) : x \in \mathbb{F}_{p^m}\}$, $s \in \mathbb{F}_{p^m}$, and $U = \{(0, y) : y \in \mathbb{F}_{p^m}\}$ for some (pre)semifield $P = (\mathbb{F}_{p^m}, +, \circ)$.

The standard example is the *Desarguesian spread*, which is obtained if the finite field is taken for the semifield. The bent functions that can be obtained with the Desarguesian spread are called PS_{ap} *bent functions* and can explicitly be represented as

$$f(x, y) = B(xy^{p^m-2}),$$

where $B : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is any balanced function.

The article is organized as follows. In Section 2, we recall generalized semifield spreads, and some results on bent partitions, vectorial dual-bent functions and (amorphic) association schemes. In Section 3, we show results that indicate that with generalized semifield spreads one obtains a large variety of bent partitions giving rise to a vast diversity of bent functions. In particular, we show that in contrast to partial spread bent functions, bent functions with various algebraic degree can be obtained. In Section 4, we investigate structural properties of association schemes obtained from vectorial dual-bent functions in the Maiorana-McFarland class. This may provide a tool to distinguish non-isomorphic association schemes.

2 Preliminaries

Recall that a finite *presemifield* is an elementary abelian group, without loss of generality represented by $\mathbb{F}_{p^m}$, equipped with an additional binary operation $\circ$ that satisfies

I) $x \circ y = 0 \Rightarrow x = 0$ or $y = 0$,
II) $(x + y) \circ s = (x \circ s) + (y \circ s)$ and $s \circ (x + y) = (s \circ x) + (s \circ y)$

for all $x, y, s \in \mathbb{F}_{p^m}$. A presemifield, for which there is an element $v \neq 0$ such that $v \circ x = x \circ v = x$ for all $x \in \mathbb{F}_{p^m}$, is a *semifield*. A presemifield can always be turned into a semifield via an isotopism, see [7].

Given a (pre)semifield $P = (\mathbb{F}_{p^m}, +, \circ)$, another (pre)semifield $P^d = (\mathbb{F}_{p^m}, +, \star)$ is obtained with the operation $\star$ defined by the equation

$$\mathrm{Tr}_1^m(x(b \star y)) = \mathrm{Tr}_1^m(b(x \circ y)) \text{ for all } b, x, y \in \mathbb{F}_{p^m}, \tag{2}$$

where Tr_k^m denotes the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^k}$ for a divisor k of m. The (pre)semifield P^d is called the *dual* of P.

Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, k a divisor of m, and let e be an integer satisfying $\gcd(p^m - 1, e) = 1$, $e \equiv p^l \mod (p^k - 1)$. Then we obtain a partition $\Omega = \{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$ of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ as follows:

$$\mathcal{A}(\gamma) = \bigcup_{s \in \mathbb{F}_{p^m} : \mathrm{Tr}_k^m(s) = \gamma} U_s^*, \quad \text{where} \quad U_s = \{(x, s \circ x^e) : x \in \mathbb{F}_{p^m}\}, \tag{3}$$

$$U_s^* = U_s \setminus \{(0, 0)\}, \quad \text{and} \quad U = \{(0, y) : y \in \mathbb{F}_{p^m}\}.$$

Proposition 1 *[7, Theorem 1] Suppose that $P = (\mathbb{F}_{p^m}, +, \circ)$ is a (pre)semifield such that the dual $P^d = (\mathbb{F}_{p^m}, +, \star)$ satisfies*

$$x \star (cy) = c(x \star y) \quad \textit{for all } x, y \in \mathbb{F}_{p^m}, c \in \mathbb{F}_{p^k}. \tag{4}$$

Then Ω is a (normal) bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Remark 1 In [7], the linearity condition in (4) is called *right $\mathbb{F}_{p^k}$-linearity*. Clearly, the finite field $\mathbb{F}_{p^m}$ is right $\mathbb{F}_{p^k}$-linear for every divisor k of m, but (pre)semifields are in general not. Infinitely many non-isotopic right $\mathbb{F}_{p^k}$-linear examples can be obtained from the construction in [15], see also [7, Example 3.2]. For more details on examples of right $\mathbb{F}_{p^k}$-linear presemifields, we refer to [7, Section 3].

Remark 2 In [7], three more closely related (normal) bent partitions are obtained from a right $\mathbb{F}_{p^k}$-linear (pre)semifield, which are also referred to as generalized semifield spreads.

In [19], a vectorial dual-bent function F is said to satisfy Condition A if all components of F are regular or all components of F are weakly regular but not regular, and σ in (1) is the identity permutation. A bent partition $\Omega = \{A_1, \ldots, A_{p^k}\}$ satisfies Condition C if $cA_j = A_j$, $c \in \mathbb{F}_p^*$, $1 \le j \le p^k$, and every bent function obtained from Ω is regular, or every bent function obtained from Ω is weakly regular but not regular. Close connections between such vectorial dual-bent functions and such bent partitions have been shown.

Proposition 2 *[19, Theorems 1 and 2] Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ be a vectorial dual-bent function satisfying Condition A, and let $D_F^c = \{x \in \mathbb{V}_n^{(p)} : F(x) = c\}$ be the preimage set of $c \in \mathbb{V}_k^{(p)}$. Then $\{D_F^c : c \in \mathbb{V}_k^{(p)}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k satisfying Condition C.*

Conversely, if p is odd and $\Omega = \{A_c : c \in \mathbb{V}_k^{(p)}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$ satisfying Condition C, then with $F(x) = c$ if $x \in A_c$, we obtain a vectorial dual-bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$, which satisfies Condition A.

In particular, for every generalized semifield spread, there exists a corresponding vectorial dual-bent function satisfying Condition A.

Remark 3 The vectorial dual of a vectorial dual-bent function F is not unique, i.e., it depends on the choice of the basis for the vector space. Hence, in the definition of Condition A, it is more precise to say that there exists a vectorial dual for which σ is the identity permutation. As shown in [2], this applies if and only if for every vectorial dual of F the permutation σ is linear, equivalently if and only if there exists a vectorial dual such that σ is linear.

An alternative formulation for F satisfying Condition A, independent from the representation, is that for F, F^* and $c_1, c_2 \neq -c_1$, we have (see [2, Proposition 7])

$$(F_{c_1})^* + (F_{c_2})^* = (F_{c_1} + F_{c_2})^*.$$

A *d-class association scheme* is a set of binary relations $R_0, R_1, \ldots, R_d$ on a set V satisfying the following properties:

(I) $R_0 = \{(x, x) : x \in V\} = id$ is the identity relation on V.
(II) $\bigcup_{i=0}^{d} R_i = V \times V$, $R_i \cap R_j = \emptyset$ if $i \neq j$, i.e., the relations R_i, $0 \le i \le d$, form a partition of $V \times V$.
(III) For every $0 \le i \le d$, $R_i^t = R_{i'}$ for some $0 \le i' \le d$, where $R_i^t = \{(x, y) : (y, x) \in R_i\}$.
(IV) For every $h, i, j \in \{0, 1, \ldots, d\}$, there exists a constant ρ_{ij}^h called an *intersection number*, such that for every $(x, y) \in R_h$, the number of z for which $(x, z) \in R_i$ and $(z, y) \in R_j$ equals ρ_{ij}^h.

All association schemes in this article are *symmetric*, i.e., $R_i^t = R_i$, $1 \le i \le d$.

A *fusion* of a d-class association scheme $R_0 = id, R_1, \ldots, R_d$ on V, is a partition $S_0, S_1, \ldots, S_c$ of $V \times V$ for which $S_0 = R_0$ and every S_j, $1 \le j \le c$, is a union of

some of the R_i. A fusion that is an association scheme as well, is called a *fusion scheme*. An association scheme is called *amorphic* if every of its fusions is a fusion scheme.

We remark that amorphic association schemes can equivalently be described as an edge decomposition of a complete graph into strongly regular graphs of (negative) Latin square type, see e.g. [4].

In [5, 20], it is shown that vectorial dual-bent functions induce (not necessarily amorphic) association schemes. We summarize some results of [5, 20] as follows:

Proposition 3 *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial dual-bent function with $F(0) = 0$ and $F(x) = F(-x)$. Suppose that all components of F are either regular or all are weakly regular but not regular. For the preimage sets $D_F^{\alpha *} = \{x \in \mathbb{V}_n^{(p)} \setminus \{0\} : F(x) = \alpha\}$ consider the binary relations R_α with $(x, y) \in R_\alpha$ if and only if $x - y \in D_F^{\alpha *}$.*

(i) Then the set of relations $\{id, R_\alpha : \alpha \in \mathbb{V}_m^{(p)}\}$ forms a p^m-class association scheme on $\mathbb{V}_n^{(p)}$, except for one case: All components of F are weakly regular but not regular and $m = \frac{n}{2}$ (only possible if $p = 3$). Then we have a $(p^m - 1)$-class association scheme.

(ii) If σ in (1) is the identity permutation, i.e., if F satisfies $(F_\beta)^* = F_\beta^*$ for every $\beta \in \mathbb{V}_m^{(p)} \setminus \{0\}$, then the association scheme in (i) is amorphic.

Let $\{U, A_1, \ldots, A_{p^k}\}$ be a generalized semifield spread of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, and let R_U, R_{A_j}, $j = 1, \ldots, p^k$, be the corresponding binary relations. Then id, R_U, R_{A_j}, $j = 1, \ldots, p^k$, form a $(p^k + 1)$-class amorphic association scheme on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Example 1 Let $\{U, U_s^* : s \in \mathbb{F}_{p^m}\}$, where $U = \{(0, y) : y \in \mathbb{F}_{p^m}\}$ and for $s \in \mathbb{F}_{p^m}$, $U_s = \{(x, sx) : x \in \mathbb{F}_{p^m}\}$, be the bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ obtained with the Desarguesian spread. Then the relations of the corresponding $(p^m + 1)$-class amorphic association scheme $id, R_U, R_{U_s}, s \in \mathbb{F}_{p^m}$, are given as follows. For distinct $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, we have:

- $(x_1, y_1) R_U (x_2, y_2)$ if and only if $x_1 = x_2$.
- $(x_1, y_1) R_{U_0} (x_2, y_2)$ if and only if $y_1 = y_2$.
- For $s \in \mathbb{F}_{p^m}^*$, $(x_1, y_1) R_{U_s} (x_2, y_2)$ if and only if $(x_1 - x_2) = s(y_1 - y_2)$.

An associated vectorial dual-bent function is the vectorial PS_{ap} function $F(x, y) = x^{p^m - 2} y$, of which the preimage set partition $\{U \cup U_0^*, U_s^* : s \in \mathbb{F}_{p^m}^*\}$ induces the fusion scheme $id, R_U \cup R_{U_0}, R_{U_s}, s \in \mathbb{F}_{p^m}^*$.

The amorphic association schemes obtained from a spread as in Example 1 above, are referred to as complete affine association schemes, see [10].

3 Results on the generalized desarguesian spread

As pointed out in [7], a generalized semifield spread can be seen as a generalization of a conventional semifield spread. In fact, the generalized semifield spread reduces to the classical semifield spread of $k = m$ (the right $\mathbb{F}_{p^m}$-linearity is then not required). In particular, if the semifield is the finite field, then the generalized semifield spread is a generalization of the Desarguesian spread. We hence use the term *generalized Desarguesian spread*.

Similar as for the Desarguesian spread, it is easy to infer an explicit representation of all bent functions generated with a generalized Desarguesian spread, see also [2, 6].

Let k be a divisor of m and let $e \equiv p^l \mod (p^k - 1)$, and $\gcd(e, p^m - 1) = 1$. Then all bent functions $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ obtained from the generalized Desarguesian spread defined as in (3) with the finite field multiplication, can be expressed as

$$f(x, y) = B(\mathrm{Tr}_k^m(yx^{-e})), \tag{5}$$

where $B : \mathbb{F}_{p^k} \to \mathbb{F}_p$ is a balanced function. In accordance with the classical case, we call the functions in (5) *generalized PS_{ap} bent functions*.

Remark 4 The duals of the bent functions in (5) are of the form

$$g(x, y) = B(\mathrm{Tr}_k^m(xy^{-d})), \tag{6}$$

where $B : \mathbb{F}_{p^k} \to \mathbb{F}_p$ is a balanced function, and $de \equiv 1 \mod (p^m - 1)$. The functions (6) are the bent functions obtained from yet another bent partition (see e.g. [2]), which also reduces to the Desarguesian spread if $k = m$. We refer to the functions in (6) also as generalized PS_{ap} bent functions.

Recall that two functions $f_1, f_2 : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ are called *extended affine equivalent (EA-equivalent)* if $f_2(x) = f_1(L(x) + a) + \ell(x) + b$ for some linear operator L on $\mathbb{V}_n^{(p)}$, linear map $\ell : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $a \in \mathbb{V}_n^{(p)}$, $b \in \mathbb{F}_p$. If ℓ is the 0-function, then f_1, f_2 are called *affine equivalent*, and *linear equivalent* if furthermore $a = 0$, $b = 0$. Linear equivalence can naturally be extended to partitions of $\mathbb{V}_n^{(p)}$. We call partitions $\Omega_1 = \{D_1^{(1)}, D_2^{(1)}, \ldots, D_r^{(1)}\}$ and $\Omega_2 = \{D_1^{(2)}, D_2^{(2)}, \ldots, D_r^{(2)}\}$ of $\mathbb{V}_n^{(p)}$ affine equivalent if Ω_1 can be transformed to Ω_2 with an affine coordinate transformation, i.e., there exists a linear operator L of $\mathbb{V}_n^{(p)}$ and a constant $a \in \mathbb{V}_n^{(p)}$ such that $D_j^{(2)} = L(D_j^{(1)}) + a$, $j = 1, 2, \ldots, r$. If $a = 0$, we say that Ω_1 and Ω_2 are linear equivalent. It is easy to infer that equivalent bent partitions yield (up to equivalence) the same set of bent functions. In fact, if two bent partitions Ω_1, Ω_2 of $\mathbb{V}_n^{(p)}$ are affine equivalent with linear operator L and constant a, then the bent function f_1 can be obtained from Ω_1 if and only if $f_2 = f_1(L^{-1}(x - a))$ is obtained from Ω_2. We therefore can confirm that two bent partitions Ω_1, Ω_2 are inequivalent by showing that with Ω_2 we can generate bent functions which are not equivalent to any bent function obtained from Ω_1.

In this section, some results are provided which indicate that there is a large variety of inequivalent bent partitions giving rise to a vast diversity of bent functions. More precisely, we show that:

(I) With different choices of e in (3), one can get inequivalent generalized semifield spreads.
(II) With generalized Desarguesian spreads, one can generate bent functions of various algebraic degree.

These observations add to [6, Theorem 2] on bent partitions from isotopic semifields:

(III) Two generalized semifield spreads (with the same m, k, e) obtained from two isotopic (pre)semifields are in general not equivalent.

Remark 5 The results in (II) and (III) are quite in contrast to the actual situation for conventional semifield spreads:

- The algebraic degree of every bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ obtained from a spread is $(p - 1)n/2$.
- The semifield spreads obtained from two isotopic (pre)semifields are equivalent.

On the 2-rank and equivalence

In this subsection, we restrict ourselves to the important case of Boolean generalized PS_{ap} bent functions. Let $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ be a Boolean function. The development $Dev(f)$ of f is the point-block incidence structure with $\mathbb{V}_n^{(2)}$ as point set and $\{Supp(f) + v : v \in \mathbb{V}_n^{(2)}\}$ as block set, where $Supp(f) = \{x \in \mathbb{V}_n^{(2)} : f(x) = 1\}$. The 2-*rank* of f is the rank of the $2^n \times 2^n$ incidence matrix of $Dev(f)$. If f is a Boolean bent function, then $Supp(f)$ is a Hadamard difference set and $Dev(f)$ is a divisible design. Clearly if f_1, f_2 have a different 2-rank, then $Dev(f_1)$ and $Dev(f_2)$ are not isomorphic, in particular f_1 and f_2 are then not EA-equivalent.

In [6, Section 5], the 2-rank of the Boolean generalized PS_{ap} bent functions of the form $f(x, y) = \mathrm{Tr}_1^m(x^{-e}y)$, $e = 2^k + 1$, is determined in terms of Fibonacci numbers. In general, statements on 2-ranks of Boolean bent functions are not easy to obtain. However, the 2-rank is a useful tool to show for bent functions not to be equivalent respectively for the corresponding designs not to be isomorphic.

With the help of MAGMA, we determined the 2-ranks for all bent functions obtained from two concrete examples of generalized Desarguesian spreads with the same m and k but different values for e.

Example 2 Let $p = 2, m = 6, k = 2, e_1 = 2^2 + 1, e_2 = 2^3 + 2^2 + 1$. Let Ω_1 and Ω_2 be the bent partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ obtained by using e_1 and e_2, respectively, see Equation (3). With MAGMA calculations, we determined the 2-ranks of all bent functions obtained from Ω_1 and Ω_2. Each bent function obtained from Ω_1 has 2-rank 96, whereas the 2-rank of any bent function obtained from Ω_2 is either 56 or 64. Hence not any bent function obtained with Ω_2 is equivalent to a bent function from Ω_1, and the bent partitions Ω_1 and Ω_2 are inequivalent.

The results on the 2-ranks do not only show that the generalized Desarguesian spreads in Example 2 are not equivalent, but also indicate that a variety of bent functions and non-isomorphic divisible designs can be obtained from generalized semifield spreads.

Corollary 1 *Let k be a divisor of m, e_1, e_2 be integers such that $\gcd(e_1, 2^m - 1) = \gcd(e_2, 2^m - 1) = 1$, and $e_1 \equiv 2^{l_1} \mod (2^k - 1)$, $e_2 \equiv 2^{l_2} \mod (2^k - 1)$ for some integers l_1, l_2.*

In general, the set of 2-ranks of the Boolean bent functions $B(\mathrm{Tr}_k^m(yx^{-e_1}))$ and of the Boolean bent functions $B(\mathrm{Tr}_k^m(yx^{-e_2}))$, $B : \mathbb{F}_{2^k} \to \mathbb{F}_2$ balanced, are not the same. Various non-isomorphic designs can be obtained with different generalized Desarguesian spreads. In particular, the generalized Desarguesian spreads for e_1 and for e_2 are in general not equivalent.

Similar considerations can be made for odd characteristic. One would expect that, as for the Boolean case, different choices of e in (3) can provide inequivalent partitions and a large amount of inequivalent bent functions.

Algebraic degree

In [8, Theorem 8], the classical result in Dillon's thesis [11] on the algebraic degree of a Boolean partial spread bent function is extended to arbitrary characteristic. It is shown that every bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ obtained from a spread of $\mathbb{V}_n^{(p)}$ has algebraic degree $(p - 1)n/2$. In this subsection, we show that varying e in (3), we can obtain bent functions of various algebraic degree from generalized Desarguesian spreads.

Proposition 4 *Let k be a divisor of m, let $1 \le e < p^m - 1$ be an integer satisfying $e \equiv p^l \mod (p^k - 1)$ for some nonnegative integer $l < k$.*

(i) The algebraic degree of $\mathrm{Tr}_1^m(yx^{-e})$ is a multiple of $(p-1)$.
(ii) There exists $\mathrm{Tr}_1^m(yx^{-e})$ of algebraic degree $(p-1)r$ for all $k \le r \le m$.

Proof (i) For $1 \le e < p^m - 1$, let $e = e_0 + e_1 p + \cdots + e_{m-1}p^{m-1}$ be the p-adic expansion of e, i.e., $0 \le e_i \le p-1$ for $i = 0, \ldots, m-1$. Then $e \equiv p^l \mod (p^k - 1)$ implies that $e \equiv \sum_{i=0}^{m-1} e_i \equiv 1 \mod (p-1)$. That is, we have $wt(e) \equiv 1 \mod (p-1)$. By the fact that $p^m - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{m-1}$, we have

$$-e = p^m - 1 - e = (p - 1 - e_0) + (p - 1 - e_1)p + \cdots + (p - 1 - e_{m-1})p^{m-1}. \quad (7)$$

As $0 \le p - 1 - e_i \le p - 1$ for $i = 0, \ldots, m-1$, Equation (7) is the p-adic expansion of $-e$. Hence,

$$wt(-e) = m(p-1) - \sum_{i=0}^{m-1} e_i = m(p-1) - wt(e). \quad (8)$$

Note that the algebraic degree of $\mathrm{Tr}_1^m(yx^{-e})$ is $wt(-e)+1$. Hence, Equation (8) together with $wt(e) \equiv 1 \mod (p-1)$ implies that

$$wt(-e) + 1 \equiv -wt(e) + 1 \equiv 0 \mod (p-1),$$

which gives the desired conclusion.

(ii) As $e \equiv p^l \mod (p^k - 1)$, we have $e = t(p^k - 1) + p^l$ for some nonnegative integer t. For $t = 0$, i.e., $e = p^l$, we have a PS_{ap} bent function. Hence, the algebraic degree is $(p-1)m$.

From now on, we suppose that t is a positive integer. Let $t = t_0 + t_1 p + \cdots + t_s p^s$ be the p-adic expansion of t. Note that $s + k \le m$, otherwise $e > p^m$. We determine the algebraic degree of $\mathrm{Tr}_1^m(yx^{-e})$, which is $wt(-e) + 1$, through a case-by-case analysis. We mainly use the equality

$$p^h = pp^c + (p-1)p^{c+1} + \cdots + (p-1)p^{h-1} \quad (9)$$

for positive integers $h > c$.

Case (I): $s + k < m$.

Suppose that $t = t_c p^c + \cdots + t_s p^s$, where $t_c, t_s \neq 0$, i.e.,

$$e = -t_c p^c - \cdots - t_s p^s + t_c p^{c+k} + \cdots + t_s p^{s+k} + p^l.$$

We consider the following subcases:

Case (A): $s < k$.

(a) $l > s$, i.e., $s < l < k$.

Then by Equation (9), the p-adic expansion of e is

$$\begin{aligned} e = {} & (p - t_c)p^c + (p - 1 - t_{c+1})p^{c+1} + \cdots + (p - 1 - t_s)p^s \\ & + (p-1)p^{s+1} + \cdots + (p-1)p^{l-1} + t_c p^{c+k} + \cdots + t_n p^{s+k}. \end{aligned}$$

Hence, $wt(e) = (p-1)(l-c-1) + p$, which implies that $wt(-e)+1 = (p-1)(m-(l-c))$. In this case, for varying values of c and l, we obtain all r values satisfying $m - (k-1) \le r \le m-1$.

(b) $l \le s$, i.e., $l \le s < k$.

If $l < c$, by Equation (9), the p-adic expansion of e is

$$\begin{aligned} e &= p^l + (p - t_c)p^c + (p - 1 - t_{c+1})p^{c+1} + \cdots + (p - 1 - t_s)p^s \\ &\quad + (p-1)p^{s+1} + \cdots + (p-1)p^{c+k-1} + (t_c - 1)p^{c+k} + t_{c+1}p^{c+k+1} + \cdots + t_s p^{s+k}. \end{aligned}$$

Hence, $wt(-e) + 1 = (p-1)(m-k)$.
Suppose that $c < l < s$. Let d be the integer such that $l \le d \le s$, $t_d \neq 0$ and $t_i = 0$ for all $l \le i < d$. Then the p-adic expansion of e is

$$\begin{aligned} e &= (p - t_c)p^c + (p - 1 - t_{c+1})p^{c+1} + \cdots + (p - 1 - t_{l-1})p^{l-1} \\ &\quad + (p - t_d)p^d + (p - 1 - t_{d+1})p^{d+1} + \cdots + (p - 1 - t_s)p^s \\ &\quad + (p-1)p^{s+1} + \cdots + (p-1)p^{c+k-1} + (t_c - 1)p^{c+k} + t_{c+1}p^{c+k+1} + \cdots + t_s p^{s+k}. \end{aligned}$$

Hence, $wt(-e) + 1 = (p-1)(m-k+(d-l))$.
In the case of $c = s$, we obtain $wt(-e) + 1 = (p-1)(m-k)$. Suppose that $c = l$. If $t_c > 1$, then $wt(-e) + 1 = (p-1)(m-(k+1))$. For the case $t_c = 1$, let d be the integer such that $c < d \le s$, $t_d \neq 0$ and $t_i = 0$ for all $c < i < d$. Then we have $wt(-e) + 1 = (p-1)(m-k+(d-c))$.

In this case, for varying values of c, d and l, we obtain all r values satisfying $m-(k+1) \le r \le m-1$.

Case (B): $s \ge k$, i.e., $l < k \le s$.

(a) $c + k > s$.

Then we have the Case (A)/(b) except $l = s$.

(b) $c + k \le s$.

By setting $b_i = t_{i-k} - t_i$ for $i = c+k, \ldots, s$, we can write e as follows:

$$\begin{aligned} e = -t_c p^c - \cdots - t_{c+k-1}p^{c+k-1} + b_{c+k}p^{c+k} + \cdots + b_s p^s \\ + t_{s-k+1}p^{s+1} + \cdots + t_s p^{s+k} + p^l. \end{aligned}$$

We only investigate the case $l < c$ as the case $l \ge c$ is similar.
We first suppose that $b_i \le 0$ for all $i = c+k, \ldots, s$, and t_d is the first nonzero term for $d > s-k$. Then the p-adic expansion of e is

$$\begin{aligned} e &= p^l + (p - t_c)p^c + (p - 1 - t_{c+1})p^{c+1} + \cdots + (p - 1 - t_{c+k-1})p^{c+k-1} \\ &\quad + (p - 1 + b_{c+k})p^{c+k} + \cdots + (p - 1 + b_s)p^s + (p-1)p^{s+1} + \cdots + (p-1)p^{d+k-1} \\ &\quad + (t_d - 1)p^{d+k} + t_{d+1}p^{d+k+1} + \cdots + t_s p^{s+k}. \end{aligned}$$

Hence, $wt(-e) + 1 = (p-1)(m-k-(d-c))$.
We now suppose that b_{d_1} is the first positive coefficient with $c + k \le d_1 \le s$. Then

$$e = e_1 + b_{d_1+1}p^{d_1+1} + \cdots + b_s p^s + t_{s-k+1}p^{s+1} + \cdots + t_s p^{s+k},$$

where $e_1 = p^l + (p-t_c)p^c + (p-1-t_{c+1})p^{c+1} + \cdots + (p-1+b_{d_1-1})p^{d_1-1} + (b_{d_1}-1)p^{d_1}$.
Suppose that b_{v_2} is the first negative coefficient with $d_1 + 1 \le v_2 \le s$, and that b_{d_2} is the first positive coefficient with $v_2 + 1 \le d_2 \le s$. That is,

$$e = e_1 + e_2 + b_{d_2+1}p^{d_2+1} + \cdots + b_s p^s + t_{s-k+1}p^{s+1} + \cdots + t_s p^{s+k},$$

where $e_2 = b_{d_1+1}p^{d_1+1} + \cdots + b_{v_2-1}p^{v_2-1} + (p + b_{v_2})p^{v_2} + (p - 1 + b_{v_2+1})p^{v_2+1} + \cdots + (p - 1 + b_{d_2-1})p^{d_2-1} + (b_{d_2} - 1)p^{d_2}$. Continuing in this way, we can write

$$e = e_1 + \cdots + e_\eta + b_{d_\eta+1}p^{d_\eta+1} + \cdots + b_s p^s + t_{s-k+1}p^{s+1} + \cdots + t_s p^{s+k}, \qquad (10)$$

where $d_\eta \le s$ such that there is at most one sign change in $\{b_{d_\eta}, b_{d_\eta+1}, \ldots, b_s\}$. If $b_i \ge 0$ for all $i = d_\eta, \ldots, s$, i.e., Equation (10) is the p-adic expansion of e, then $wt(-e) + 1 = (p-1)\left(m - (d_1 - c) - \sum_{i=2}^{\eta}(d_i - v_i)\right)$.

Otherwise, let b_μ be the first negative coefficient lying in $\{b_{d_\eta+1}, \ldots, b_s\}$ and t_j be the first nonzero integer for $s-k+1 \le j \le s$.

Then by the p-adic expansion of e, we obtain

$$wt(-e) + 1 = (p-1)\left(m - (d_1 - c) - \sum_{i=2}^{\eta}(d_i - v_i) - (j + k - \mu)\right).$$

In this case, we obtain all r values satisfying $k \le r \le m - (k+1)$.

Case (II): $s + k = m$.

If $m = \mu k$, then $s = (\mu - 1)k$. With the p-adic expansion $t = t_0 + t_1 p + \cdots + t_s p^s$, we have

$$e = -t_0 - \cdots - t_{k-1}p^k + b_k p^k + \cdots + b_s p^s + t_{s-k+1}p^{s+1} + \cdots + t_s p^{s+k} + p^l, \quad (11)$$

where $b_i = t_i - t_{i-k}$ for $i = k, \ldots, s$. We first observe that $t_s = 1$ and $l \le s$, otherwise $e \ge p^m$. Note that, for $i < m$, the first highest nonzero coefficient of p^i appearing in (11) has to have a minus sign. Otherwise, we also have $e \ge p^m$. Since $t_i \ge 0$, this implies that $t_{s-k+1} = \cdots = t_{s-1} = 0$. That is,

$$\begin{aligned} e = &-t_0 - \cdots - t_{k-1}p^k + b_k p^k + \cdots + b_{s-2k}p^{s-k} \\ &+ t_{s-2k+1}p^{s-k+1} + \cdots + t_{s-k-1}p^{s-1} + (t_{s-k} - 1)p^s + p^m + p^l \end{aligned}$$

and $l < s$. Since $t_{s-k} - 1 \le 0$, either $t_{s-k} = 1$ or $t_{s-k} = 0$. If $t_{s-k} = 1$, then we similarly have $t_{s-2k+1} = \cdots = t_{s-k-1} = 0$, i.e., we have

$$\begin{aligned} e = &-t_0 - \cdots - t_{k-1}p^k + b_k p^k + \cdots + b_{s-3k}p^{s-2k} \\ &+ t_{s-3k+1}p^{s-2k+1} + \cdots + t_{s-2k-1}p^{s-k-1} + (t_{s-2k} - 1)p^{s-k} + p^m + p^l \end{aligned}$$

and $l < s - k$.

That is, in the case that $b_{jk} = 0$ for all $j = 1, \ldots, \mu - 1$, we have $t = 1 + p^k + \cdots + p^{(\mu-1)k}$. This implies that $e = p^m - 1 + p^l$, which gives a contradiction to $e < p^m - 1$. Hence, there exists $i \in \{1, \ldots, \mu - 1\}$ such that $b_{ik} = -1$ and $b_{jk} = 0$ for all $i < j$. Without loss of generality, we can suppose that $i = \mu - 1$, i.e., $t_{s-k} = 0$ and

$$\begin{aligned} e = &-t_0 - \cdots - t_{k-1}p^k + b_k p^k + \cdots + b_{s-k-1}p^{s-k-1} \\ &+ t_{s-2k}p^{s-k} + t_{s-2k+1}p^{s-k+1} + \cdots + t_{s-k-1}p^{s-1} - p^s + p^m + p^l. \end{aligned}$$

That is, by Equation (9), the last part of the p-adic expansion of e is of the form $t_{s-2k}p^{s-k} + \cdots + t_{s-k-1}p^{s-1} + (p-1)p^s + (p-1)p^{s+1} + \cdots + (p-1)p^{m-1}$.

This implies that $r \ge k$. Similarly, we observe that $r \le s$. □

Proposition 4 and its proof reveals the possible values for the algebraic degree of a generalized PS_{ap} bent function of the form $\mathrm{Tr}_1^m(yx^{-e})$. Also observe that the algebraic degree of $\mathrm{Tr}_1^m(yx^{-e})$ is $m(p-1)$ if and only if $e = p^l$, hence x^e is linear. In this case $\mathrm{Tr}_1^m(yx^{-e})$ is a conventional Desarguesian spread bent function (with the linear coordinate change $x \to x^{p^l}$). We arrive at the following theorem.

Theorem 1 *Let k be a divisor of m, let $1 \le e < p^m - 1$ be an integer satisfying $\gcd(p^m - 1, e) = 1$ and $e \equiv p^l \mod (p^k - 1)$ for some nonnegative integer $l < k$. The algebraic*

degree of the generalized PS_{ap} bent function $f(x, y) = \mathrm{Tr}_1^m(yx^{-e})$ is $r(p-1)$ for some integer r satisfying $k \le r \le m$.

Moreover, the algebraic degree of $f(x, y)$ is $m(p-1)$ if and only if $f(x, y)$ is a conventional PS_{ap} bent function.

We present some specific examples below that demonstrate all possible values of r in Theorem 1 can be achieved.

Example 3 Let $k = 2$ and $m = 4$. Let p be an arbitrary prime number.

First, put $e = p$. It is clear that $e \equiv p \mod (p^2-1)$, $\gcd(e, p^4-1) = 1$ and the degree of $\mathrm{Tr}_1^m(yx^{-e})$ is $4(p-1)$. Note that $\mathrm{Tr}_1^m(yx^{-e})$ is PS_{ap} bent function in this case.

Secondly, put $e = 1 + (p-1)p^2$. It is clear that $e \equiv p \mod (p^2-1)$ and the degree of $\mathrm{Tr}_1^m(yx^{-e})$ is $3(p-1)$. Assume that $p \not\equiv 2 \mod 5$, which holds for infinitely many prime numbers p. Let I be the ideal of the ring of integers given by $I =< p^4-1, 1+(p-1)p^2 >$. By using Euclidean Algorithm, we obtain that $I =< p^3-p^2+1, p^2-p-2 >=< p^2-p-2, 2p+1 >=< 5, (p-1)/2+2 >=< 1 >$. This implies that we have $\gcd(e, p^4-1) = 1$. Note that the assumption $p \not\equiv 2 \mod 5$ is needed in general as $\gcd(e, p^4-1) = 5$ when $p = 7$.

Finally, put $e = 1+(p-1)p^2+(p-1)p^3$. It is clear that $e \equiv p^2 \mod (p^2-1)$ and the degree of $\mathrm{Tr}_1^m(yx^{-e})$ is $2(p-1)$. Moreover we have $\gcd(e, p^4-1) = 1$ for any prime number p. Indeed, by using Euclidean Algorithm we obtain $< p^4-1, 1+(p-1)p^2+(p-1)p^3 >=< p^4-p^2+1, p^2-2 >=< p^2-2, 3 >=< 1 >$.

Remark 6 Note that in the case Case (I)/((A)/(a)) in (ii) of Proposition 4, by choosing $s = c = 0$ and $l = 1$, i.e., $e = p^k + p - 1$, we have $wt(-e) + 1 = (p-1)(m-1)$, which gives the result in [8, Proposition 2].

Recall that all bent functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ obtained from the Desarguesian spread have the same algebraic degree, namely $(p-1)n/2$. We can observe a different behaviour for a generalized Desarguesian spread. As we confirmed with MAGMA, in general, the algebraic degree of $f(x, y) = B(\mathrm{Tr}_k^m(yx^{-e}))$, $B : \mathbb{F}_{p^k} \to \mathbb{F}_p$ balanced, may be different from the algebraic degree of $\mathrm{Tr}_1^m(yx^{-e})$.

4 Maiorana-McFarland association schemes from semifields

In [19], it is pointed out that every bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ of depth p^k given with a generalized semifield spread is the preimage set partition of a certain vectorial bent function F from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^k}$ satisfying Condition A. Note that for odd p, this follows from the general result in [19], which we recalled in Proposition 2, with the easy observation that a generalized semifield spread satisfies Condition C. In [19, Section III], an explicit description of this vectorial dual-bent function is given: Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield and let $P^d = (\mathbb{F}_{p^m}, +, \star)$ be its dual (pre)semifield. Then with

$$\eta_0 = 0 \quad \text{and} \quad y \star \eta_y^{-1} = 1, \tag{12}$$

one obtains a permutation $y \to \eta_y$ of $\mathbb{F}_{p^m}$. For some given integer e, we define a function $a(x, y)$ from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ by

$$a(x, y) \circ x^e = y \quad \text{if} \quad x \neq 0 \quad \text{and} \quad a(x, y) = 0 \quad \text{if} \quad x = 0. \tag{13}$$

Suppose that P^d is right $\mathbb{F}_{p^k}$-linear for a divisor k of m, $\gcd(e, p^m-1)=1$, and $e \equiv p^l \mod (p^k-1)$ for some integer l. Then by [19, Proposition 3], $F(x,y)=\mathrm{Tr}_k^m(a(x,y))$ for $a(x,y)$ given in (13), is a vectorial dual-bent function satisfying Condition A, and the generalized semifield spread partition in (3) arises as the preimage set partition of F (with $F^{-1}(0)=U\cup\mathcal{A}(0)$). The vectorial dual of F is $F^*(x,y)=-\mathrm{Tr}_k^m(x\eta_y^{-d})$ with the convention $\eta_0^{-d}=0$, where $ed \equiv 1 \mod (p^m-1)$. With Proposition 3, the preimage set partition of $F(x,y)=\mathrm{Tr}_k^m(a(x,y))$ induces a p^k-class amorphic association scheme.

Remark 7 Note that the vectorial dual F^* is a projection of the Maiorana-McFarland bent function $x\eta_y^{-d}$ from $\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$.

With F, also F^* is a vectorial dual-bent function satisfying Condition A. The bent partition arising from the preimage set partition of this projection of a Maiorana-McFarland bent function, is the generalized semifield spread Θ_1 given in [7, Theorem 2].

The following theorem refines the results on the vectorial dual-bent functions F and F^* given as above.

Theorem 2 *Let e, d be integers such that $\gcd(e, p^m-1)=1$ and $ed \equiv 1 \mod (p^m-1)$. For a (pre)semifield $P=(\mathbb{F}_{p^m},+,\circ)$, consider the functions $x\eta_y^{-d}$ and $a(x,y)$ from $\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ defined as above.*

If the dual (pre)semifield P^{d} is right $\mathbb{F}_{p^k}$-linear for a divisor k of m, then $F, G : \mathbb{F}_{p^m}\times\mathbb{F}_{p^m}\to\mathbb{F}_{p^k}$ given by $F(x,y)=\mathrm{Tr}_k^m(a(x,y))$ and $G(x,y)=-\mathrm{Tr}_k^m(x\eta_y^{-d})$ are vectorial dual-bent functions, and $G(x,y)=F^*(x,y)$, the vectorial dual of F. Moreover, $(F_c)^*=F^*_{\sigma(c)}$ with $\sigma(c)=c^d$.

Proof First note that G is a vectorial bent function as it is a projection of a vectorial Maiorana-McFarland bent function. We have to show that for every nonzero c in $\mathbb{F}_{p^k}$, we have $(F_{c^e})^*=F_c^*$, where $F^*(x,y)=-\mathrm{Tr}_k^m(x\eta_y^{-d})=G(x,y)$. Then F is a vectorial dual-bent function with vectorial dual as claimed in the theorem and permutation $\sigma^{-1}(c)=c^e$.

Below we will deduce that for $c\in\mathbb{F}_{p^k}^*$,

$$F_{c^e}(x,y)=\mathrm{Tr}_1^m(c^e a(x,y))=\mathrm{Tr}_1^m(\rho^{-1}(c^{-1}x)y) \tag{14}$$

for the permutation $\rho(x)=\eta_x^{-d}$. Then using the fact that the dual of a Maiorana-McFarland bent function $m(x,y)=\mathrm{Tr}_1^m(\pi(x)y)$ is $m^*(x,y)=-\mathrm{Tr}_1^m(x\pi^{-1}(y))$, we obtain

$$(F_{c^e})^*(x,y)=(\mathrm{Tr}_1^m(\rho^{-1}(c^{-1}x)y))^*=-\mathrm{Tr}_1^m(cx\rho(y))=-\mathrm{Tr}_1^m(cx\eta_y^{-d}),$$

and the proof is completed.

It remains to show the identity (14). We first show that for any nonzero $x\in\mathbb{F}_{p^m}$, we have

$$\rho^{-1}(c^{-1}x)\star x^e=c^e. \tag{15}$$

For nonzero $x\in\mathbb{F}_{p^m}$, we set $\rho^{-1}(c^{-1}x)=z$. Then $\rho(z)=\eta_z^{-d}=c^{-1}x$. With $de\equiv 1 \mod (p^m-1)$, we then obtain $\eta_z^{-1}=c^{-e}x^e$. Therefore, by the definition of η_z in (12), we have

$$1=z\star\eta_z^{-1}=z\star(c^{-e}x^e)=c^{-e}(z\star x^e),$$

where in the last step we use the right $\mathbb{F}_{p^k}$-linearity of P^{d} and the assumption that $c\in\mathbb{F}_{p^k}$. Hence, $c^e=z\star x^e$, which confirms (15).

Consequently, for nonzero $x \in \mathbb{F}_{p^m}$ with (2) and (13), we obtain the following equalities:

$$\begin{aligned}\mathrm{Tr}_1^m(c^e a(x,y)) &= \mathrm{Tr}_1^m(a(x,y)(\rho^{-1}(c^{-1}x)\star x^e))\\ &= \mathrm{Tr}_1^m(\rho^{-1}(c^{-1}x)(a(x,y)\circ x^e))\\ &= \mathrm{Tr}_1^m(\rho^{-1}(c^{-1}x)y).\end{aligned}$$

If $x = 0$, then $a(0, y) = \rho^{-1}(0) = 0$, which shows (14). □

With the connection between vectorial dual-bent functions and association schemes given in Proposition 3, we can construct a variety of not necessarily amorphic association schemes from (pre)semifields, for which the dual is right $\mathbb{F}_{p^k}$-linear.

Corollary 2 *For some (pre)semifield $P = (\mathbb{F}_{p^m}, +, \circ)$ with right $\mathbb{F}_{p^k}$-linear dual, and for an integer e such that $\gcd(e, p^m - 1) = 1$, let F and F^* be the vectorial bent functions given as in Theorem 2.*

(i) The preimage set partitions of F and F^* induce p^k-class association schemes.
(ii) If $e \equiv p^l \mod (p^k - 1)$ for some integer l, then the corresponding association schemes are amorphic.

As pointed out, F^* is a projection of the vectorial Maiorana-McFarland bent function $x\eta_y^{-d}$. We hence call the association schemes in Corollary 2, *Maiorana-McFarland association schemes*. If P is the finite field, then the functions F and F^* in Theorem 2 reduce to $F(x, y) = \mathrm{Tr}_k^m(x^{-e}y)$ and $F^*(x, y) = -\mathrm{Tr}_k^m(xy^{-d})$.

The right $\mathbb{F}_{p^k}$-linearity of P^d is a crucial property for obtaining vectorial dual-bent functions. With MAGMA, we confirmed for the following examples that if P^d in Theorem 2 is not right $\mathbb{F}_{p^k}$-linear, then the functions F and F^* are not vectorial dual-bent functions:

(i) For $k = 2$, $e = 2^k + 1$, the presemifield $P = (\mathbb{F}_{2^6}, +, \circ)$ with $x \circ y = xy^2 + y\mathrm{Tr}_2^6(\gamma x) + \gamma\mathrm{Tr}_2^6(xy)$, which belongs to the class of presemifields introduced in [15], and $P^\bullet = (\mathbb{F}_{2^6}, +, \bullet)$, where $x \bullet y = y \circ x$.
(ii) For $k = 2, e = 2^k + 1$, the semifield $P = (\mathbb{F}_{2^6}, +, \circ)$ with $x \circ y = xy - \alpha x^{2^6} y^{2^3}$, where $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$, which belongs the class of Albert's twisted fields [1], and $P^\bullet = (\mathbb{F}_{2^6}, +, \bullet)$, where $x \bullet y = y \circ x$.

In the remainder of this section, we investigate fusions of the association schemes in Corollary 2. This can provide information on the inner structure of these association schemes.

Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ be a vectorial dual-bent function with a vectorial dual F^* and a permutation σ defined as in (1). A projection of F, $\tilde{F} : \mathbb{V}_n^{(p)} \to S$, S subspace of $\mathbb{V}_k^{(p)}$, is a vectorial bent function, but in general it is not vectorial dual-bent. The preimage set partition of $\tilde{F}$, of which the sets are unions of the preimage sets of F, is hence in general not inducing a fusion scheme of the association scheme of F. The following necessary and sufficient condition for a projection of a vectorial dual-bent function being vectorial dual-bent as well, is a version of [5, Corollary 16], which has been given in the multivariate framework.

Lemma 1 *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ be a vectorial dual-bent function with permutation σ of $\mathbb{V}_k^{(p)}$ given as in (1), and let S be a subspace of $\mathbb{V}_k^{(p)}$. The projection $\tilde{F} : \mathbb{V}_n^{(p)} \to S$ of F onto the subspace S is a vectorial dual-bent function if and only if $\sigma(S) = S'$ for some subspace S' of $\mathbb{V}_k^{(p)}$. The vectorial dual $\tilde{F}^*$ of $\tilde{F}$ is then the projection of F^* to the vector space $S' = \sigma(S)$.*

Proof The function $\tilde{F}$ is vectorial dual-bent if and only if the set of the dual functions of the set of the component functions $\{F_c : c \in S \setminus \{0\}\}$ forms a vector space of bent functions (together with the 0-function). By assumption, $\{(F_c)^* : c \in S \setminus \{0\}\} = \{F^*_{\sigma(c)} : c \in S \setminus \{0\}\}$, where F^* is the vectorial dual of F. Clearly, $\{F^*_{\sigma(c)} : c \in S \setminus \{0\}\}$ forms a vector space of bent function (together with the 0-function) if and only if $S' = \{\sigma(c) : c \in S\}$ is a subspace of $\mathbb{V}_k^{(p)}$ (note that $\sigma(0) = 0$). The last statement then immediately follows. □

Theorem 3 *Let k be a divisor of m, and let e, d be integers such that $\gcd(e, p^m - 1) = 1$ and $de \equiv 1 \mod (p^m - 1)$. For a (pre)semifield $P = (\mathbb{F}_{p^m}, +, \circ)$ with the right $\mathbb{F}_{p^k}$-linear dual, let $F(x, y) = \mathrm{Tr}_k^m(a(x, y))$ and $F^*(x, y) = -\mathrm{Tr}_k^m(x\eta_y^{-d})$ be the vectorial dual-bent functions given in Theorem 2. Let $\mathbb{F}_{p^s}$ be any subfield of $\mathbb{F}_{p^k}$.*

(i) The projection $F^{\gamma,s}$ of F to any coset $\gamma\mathbb{F}_{p^s}$ of $\mathbb{F}_{p^s}$ is a vectorial dual-bent function.
(ii) The preimage set partition of $F^{\gamma,s}$ induces a fusion scheme of the association scheme obtained from F. If $e \equiv p^l \mod (p^s - 1)$, then the preimage set partition of $F^{\gamma,s}$ is a bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and the corresponding fusion scheme is amorphic.

Proof (i) With $\sigma(c) = c^d$, we infer that $\sigma(\gamma\mathbb{F}_{p^s}) = \gamma^d\mathbb{F}_{p^s}$, hence it is a subspace of $\mathbb{F}_{p^k}$. Consequently, $F^{\gamma,s}$ is vectorial dual-bent by Lemma 1. A vectorial dual of $F^{\gamma,s}$ is the projection of F^* to the coset $\gamma^d\mathbb{F}_{p^s}$ of $\mathbb{F}_{p^s}$.

(ii) The first statement follows from Proposition 2.

For the second, we apply Remark 3 and show that for $c_1, c_2 \in \gamma\mathbb{F}_{p^s}$ with $c_1 \neq -c_2$, we have $(F_{c_1})^* + (F_{c_2})^* = (F_{c_1} + F_{c_2})^*$. Let $c_1 = \gamma u_1$ and $c_2 = \gamma u_2$ for $u_1, u_2 \in \mathbb{F}_{p^s}$. Then with $\sigma(c) = c^d$,

$$\begin{aligned}(F_{c_1})^*(x, y) + (F_{c_2})^*(x, y) &= -\mathrm{Tr}_1^m(c_1^d x\eta_y^{-d}) - \mathrm{Tr}_1^m(c_2^d x\eta_y^{-d})\\ &= -\mathrm{Tr}_1^m(\gamma^d(u_1^d + u_2^d)x\eta_y^{-d}).\end{aligned}$$

If $e \equiv p^l \mod (p^s - 1)$, then $z \mapsto z^e$ is a linear permutation over $\mathbb{F}_{p^s}$ as $z^e = z^{p^l}$ for $z \in \mathbb{F}_{p^s}$. Hence, the inverse map $z \mapsto z^d$ is linear over $\mathbb{F}_{p^s}$ as well. Therefore,

$$\begin{aligned}(F_{c_1})^*(x, y) + (F_{c_2})^*(x, y) &= -\mathrm{Tr}_1^m(\gamma^d(u_1 + u_2)^d x\eta_y^{-d})\\ &= -\mathrm{Tr}_1^m((\gamma u_1 + \gamma u_2)^d x\eta_y^{-d}) = -\mathrm{Tr}_1^m((c_1 + c_2)^d x\eta_y^{-d})\\ &= (F_{c_1+c_2})^*(x, y) = (F_{c_1} + F_{c_2})^*(x, y).\end{aligned}$$

With Proposition 2, we complete the proof. □

As many functions have the same preimage set partition, it is important to point out that the preimage set partitions of projections $F^{\gamma_1,s}$ and $F^{\gamma_2,s}$ to different cosets of $\mathbb{F}_{p^s}$ are different. Otherwise, they would induce one and the same fusion scheme.

Proposition 5 *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ be a surjective function, and for a divisor s of k, let $F^{\gamma_1,s}$ and $F^{\gamma_2,s}$ be the projections of F to two different cosets $\gamma_1\mathbb{F}_{p^s}$ and $\gamma_2\mathbb{F}_{p^s}$ of $\mathbb{F}_{p^s}$ in $\mathbb{F}_{p^k}$. Then the preimage sets of $F^{\gamma_1,s}$ and $F^{\gamma_2,s}$ are different.*

Proof Let $w_1, \ldots, w_s$ be a basis for $\mathbb{F}_{p^s}$. Then $\gamma_i w_1, \ldots, \gamma_i w_s$ is a basis for $\gamma_i\mathbb{F}_{p^s}$ for $i = 1, 2$. Under the fixed basis, we can represent the projection of F to $\gamma_i\mathbb{F}_{p^s}$ as

$$F^{\gamma_i,s}(z) = (\mathrm{Tr}_1^k(\gamma_i w_1 F(z)), \ldots, \mathrm{Tr}_1^k(\gamma_i w_s F(z))).$$

Note that $z_1, z_2 \in \mathbb{V}_n^{(p)}$ are in the same preimage set under the projection to $\gamma_i \mathbb{F}_{p^s}$ if and only if $\mathrm{Tr}_1^k(\gamma_i w_j F(z_1)) = \mathrm{Tr}_1^k(\gamma_i w_j F(z_2))$ for all $j = 1, \ldots, s$. This holds if and only if

$$\mathrm{Tr}_1^k(\gamma_i w_j F(z_1) - \gamma_i w_j F(z_2)) = \mathrm{Tr}_1^s(w_j \mathrm{Tr}_s^k(\gamma_i (F(z_1) - F(z_2)))) = 0$$

for all $j = 1, \ldots, s$. Since $w_1, \ldots, w_s$ is a basis for $\mathbb{F}_{p^s}$, this holds if and only if $\mathrm{Tr}_s^k(\gamma_i (F(z_1) - F(z_2))) = 0$.

Set $X = F(z_1) - F(z_2)$. From the observation above, we conclude that $z_1, z_2 \in \mathbb{V}_n^{(p)}$ are in the same preimage set under the projection to $\gamma_i \mathbb{F}_{p^s}$ for $i = 1, 2$ if and only if $\mathrm{Tr}_s^k(\gamma_1 X) = \mathrm{Tr}_s^k(\gamma_2 X) = 0$. Hence, to prove our claim, it is sufficient to show the existence of $z_1, z_2 \in \mathbb{V}_n^{(p)}$ for which

$$\mathrm{Tr}_s^k(\gamma_1 X) = 0 \quad \text{and} \quad \mathrm{Tr}_s^k(\gamma_2 X) \neq 0. \tag{16}$$

Note that F being surjective implies that for given $X \in \mathbb{F}_{p^k}$ and $z_1 \in \mathbb{V}_n^{(p)}$, there exists $z_2 \in \mathbb{V}_n^{(p)}$ satisfying $X = F(z_1) - F(z_2)$. Hence, to prove our claim, it is enough to show the existence of $X \in \mathbb{F}_{p^k}$ satisfying Equation (16). Since γ_1, γ_2 are linearly independent over $\mathbb{F}_{p^s}$, otherwise $\gamma_1 \mathbb{F}_{p^s} = \gamma_2 \mathbb{F}_{p^s}$, for every $b \in \mathbb{F}_{p^s}$, the linear system $\mathrm{Tr}_s^k(\gamma_1 x) = 0$, $\mathrm{Tr}_s^k(\gamma_2 x) = b$ has p^{k-2s} solutions in $\mathbb{F}_{p^k}$. Therefore the existence of X satisfying (16) is guaranteed. □

By [16, Corollary 2.7], any bent function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$, $k \leq m$, is surjective. Hence, we obtain the following result by Proposition 5.

Theorem 4 *Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$, $k \leq m$, be a vectorial dual-bent function, and let $F^{\gamma_1,s}$ and $F^{\gamma_2,s}$ be the projections of F to two different cosets $\gamma_1 \mathbb{F}_{p^s}$ and $\gamma_2 \mathbb{F}_{p^s}$ of $\mathbb{F}_{p^s}$ in $\mathbb{F}_{p^k}$. Then the fusion schemes induced by the preimage sets of $F^{\gamma_1,s}$ and $F^{\gamma_2,s}$ are different. Consequently, every subfield $\mathbb{F}_{p^s}$ of $\mathbb{F}_{p^k}$ gives rise to $(p^k - 1)/(p^s - 1)$ different p^s-class fusion schemes.*

Remark 8 Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be the vectorial dual-bent functions given by $F(x, y) = xy^{-e}$ and $F(x, y) = x\eta_y^{-d}$, which are defined as in Theorems 1 and 2 respectively. Then the fusion schemes induced by the preimage sets of the projections to different cosets of a subfield of $\mathbb{F}_{p^m}$ are not the same. However, as for instance, the linear map $(x, y) \mapsto (\gamma x, y)$ gives a bijection from the preimage sets of $F^{\gamma_1,s}$ to the preimage sets of $F^{\gamma_2,s}$, where $\gamma = \gamma_2/\gamma_1$, the corresponding fusion schemes are isomorphic (see also the discussion below).

By the results in Sections 3 and 4, we have a large variety of non-equivalent bent partitions and vectorial dual-bent functions. An interesting question, though probably difficult to answer, is whether these constructions also yield a large variety of non-isomorphic association schemes.

Let $R_0 = id, R_1, \ldots, R_d$ be a d-class association scheme of V and let τ be a permutation of V. Note that $\tau(R_0) = R_0 = id$, and $\tau(R_1), \ldots, \tau(R_d)$ is also a d-class association scheme of V. Hence, two association schemes $R_0 = id, R_1, \ldots, R_d$ and $R'_0 = id, R'_1, \ldots, R'_d$ on a set V are called isomorphic if there exists a permutation τ of V such that for each relation R_i, there exists a relation R'_j for which $\{(\tau(x), \tau(y)) : (x, y) \in R_i\} = R'_j$, see for instance [12]. As one can see from the definition of isomorphic association schemes, two d-class association schemes, of which one has a k-class fusion scheme and the other one does not, are also not isomorphic. In particular, an amorphic association scheme and a non-amorphic association scheme are not isomorphic.

For $1 \leq j \leq d$, we denote with A_j the adjacency matrix of R_j, and with A'_j the adjacency matrix of R'_j. In [14, 18] it is shown that one can distinguish non-isomorphic association schemes with the same intersection numbers (they are then also called algebraically isomorphic, see [13]), with the p-ranks, i.e., the ranks over $\mathbb{F}_p$, of the adjacency matrices A_j and A'_j.

Whereas the concept of equivalence of bent functions is based on the structure of $\mathbb{V}_n^{(p)}$, this does not apply to the isomorphisms of the associations schemes. Hence, similarly to bent functions and the corresponding divisible designs, non-equivalent bent partitions respectively the preimage set partitions of non-equivalent vectorial dual-bent functions, may still induce isomorphic association schemes. Having information on the inner structure of the association schemes in Theorem 2 may provide a tool to distinguish non-isomorphic association schemes.

Example 4 Let F_1, F_2 be the vectorial Maiorana-McFarland bent functions $F_1(x, y) = yx^{-7}$ and $F_2(x, y) = yx^{-11}$ from $\mathbb{F}_{3^4} \times \mathbb{F}_{3^4}$ to $\mathbb{F}_{3^4}$. Then the preimage set partition of F_1 and the preimage set partition of F_2 induce 3^4-class association schemes on $\mathbb{F}_{3^4} \times \mathbb{F}_{3^4}$.

The projections to $\mathbb{F}_{3^2}$, $\tilde{F}_1(x, y) = \mathrm{Tr}_2^4(F_1(x, y))$ and $\tilde{F}_2(x, y) = \mathrm{Tr}_2^4(F_2(x, y))$ induce 3^2-class fusion schemes of the schemes for F_1 and F_2. Since $11 \equiv 3 \mod (3^2 - 1)$, the fusion scheme for F_2 is amorphic. We confirmed with MAGMA that not all preimage sets of $\tilde{F}_1$ are partial difference sets, i.e., the fusion scheme for F_1 is not amorphic, and the 3^2-class association schemes are not isomorphic. To employ the structure of the fusions for showing that the two 3^4-class association schemes are not isomorphic, it requires to show that the association scheme for F_1 does not have any amorphic fusion of the size of the amorphic fusion of F_2. Using MAGMA, we also confirmed that the adjacency matrices of the relations of the association schemes for $\tilde{F}_1$ and $\tilde{F}_2$ have different 3-ranks. The 3-ranks of the adjacency matrices for $\tilde{F}_1$ are 6561 and 508, whereas for $\tilde{F}_2$, they are 6561 and 440.

Acknowledgements This study was supported by Scientific and Technological Research Council of Turkey (TUBITAK) under the Grant Number 123F360. N.A., T.K. and F.Ö. thank to TUBITAK for their supports. W. M. is supported by the FWF Project P 35138. F.Ö. is supported by Sabancı University projects B.A.CG-24-02873 and F.A.CF-24-02904.

Author Contributions All authors have equal contribution.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Albert, A.: On nonassociative division algebras. Trans. Am. Math. Soc. **72**, 296–309 (1952)
2. Alkan, S., Anbar, N., Kalaycı, T., Meidl, W.: Bent partition, vectorial dual-bent function and LP-packing constructions. IEEE Trans. Inform. Theory **71**, 752–767 (2025)
3. Alkan, S., Anbar, N., Kalaycı, T., Meidl, W.: Bent partitions and LP-packings. IEEE Trans. Inform. Theory **70**, 5365–5375 (2024)
4. Anbar, N., Kalaycı, T., Meidl, W.: Amorphic association schemes from bent partitions. Discrete Math. **347**, Paper No. 113658, 13 pp (2024)
5. Anbar, N., Kalaycı, T., Meidl, W., Özbudak, F.: Vectorial dual-bent functions and association schemes. Preprint (2023). (https://www.researchgate.net/publication/372046942)
6. Anbar, N., Kalaycı, T., Meidl, W.: On generalized spread bent partitions. Cryptogr. Commun. **15**, 1217–1234 (2023)
7. Anbar, N., Kalaycı, T., Meidl, W.: Generalized semifield spreads. Des. Codes Cryptogr. **91**, 545–562 (2023)
8. Anbar, N., Meidl, W.: Bent partitions. Des. Codes Cryptogr. **90**, 1081–1101 (2022)
9. Çeşmelioğlu, A., Meidl, W.: A. Pott, Vectorial bent functions and their duals. Linear Algebra Appl. **548**, 305–320 (2018)
10. van Dam, E., Muzychuk, M.: Some implications on amorphic association schemes. J. Combin. Theory Ser. A **117**, 111–127 (2010)
11. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. dissertation, University of Maryland (1974)
12. Fujisaki, T.: A construction of non-isomorphic amorphous association schemes from pseudo-cyclic association schemes. Discrete Math. **308**, 2944–2948 (2008)
13. Hanaki, A.: Modular adjacency algebras, standard representations, and p-ranks of cyclotomic association schemes. J. Algebr. Comb. **44**, 587–602 (2016)
14. Hanaki, A., Yoshikawa, M.: On modular standard modules of association schemes. J. Algebr. Comb. **21**, 269–279 (2005)
15. Kantor, W., Williams, M.: Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Trans. Amer. Math. Soc. **356**, 895–938 (2004)
16. Kölsch, L., Polujan, A.: Value Distributions of Perfect Nonlinear Functions. Combinatorica **44**, 231–268 (2024)
17. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**, 90–107 (1985)
18. Peeters, R.: On the p-ranks of the adjacency matrices of distance-regular graphs. J. Algebr. Comb. **15**, 127–149 (2002)
19. Wang, J., Fu, F.-W., Wei, Y.: Bent partitions, vectorial dual-bent functions and partial difference sets. IEEE Trans. Inform. Theory **69**, 7414–7425 (2023)
20. Wang, J., Fu, F.-W., Wei, Y., Yang, J.: A further study of vectorial dual-bent functions. IEEE Trans. Inform. Theory **70**, 7472–7483 (2024)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.