Bent partitions and Maiorana-McFarland association schemes

Tekgül Kalaycı[1]
(joint work with Nurdagül Anbar[1], Wilfried Meidl[2] and Ferruh Özbudak[1])
[1]Sabancı University, İstanbul, Turkey
[2]Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Austria

The 9th International Workshop on Boolean Functions and their Applications (BFA)
September 9 - 13, 2024

Outline

- Bent functions and bent partitions
- Generalized semifield spreads and generalized PS_{ap} functions
- Association schemes from vectorial dual-bent functions
- Maiorana-McFarland association schemes

Definition Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a function. The Walsh transform of F is the complex valued function

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{\langle a, F(x) \rangle_m - \langle b, x \rangle_n}, \quad \epsilon_p = e^{2\pi i/p},$$

where $\langle , \rangle_k$ denotes a non-degenerate inner product in $\mathbb{V}_k^{(p)}$.

Definition Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a function. The Walsh transform of F is the complex valued function

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{\langle a, F(x) \rangle_m - \langle b, x \rangle_n}, \quad \epsilon_p = e^{2\pi i/p},$$

where $\langle , \rangle_k$ denotes a non-degenerate inner product in $\mathbb{V}_k^{(p)}$.
A function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is called a bent function if $|\mathcal{W}_F(a,b)| = p^{n/2}$ for all nonzero $a \in \mathbb{V}_m^{(p)}$ and $b \in \mathbb{V}_n^{(p)}$.

Definition Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a function. The Walsh transform of F is the complex valued function

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{\langle a, F(x) \rangle_m - \langle b, x \rangle_n}, \quad \epsilon_p = e^{2\pi i/p},$$

where $\langle , \rangle_k$ denotes a non-degenerate inner product in $\mathbb{V}_k^{(p)}$.
A function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is called a bent function if $|\mathcal{W}_F(a,b)| = p^{n/2}$ for all nonzero $a \in \mathbb{V}_m^{(p)}$ and $b \in \mathbb{V}_n^{(p)}$.

If $m = 1$, then F is also called a p-ary bent function (Boolean if $p = 2$). The Walsh transform of a p-ary function $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is of the form

$$\mathcal{W}_F(1,b) = \mathcal{W}_F(b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{F(x) - \langle b, x \rangle_n}.$$

Definition Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a function. The Walsh transform of F is the complex valued function

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{\langle a, F(x)\rangle_m - \langle b, x\rangle_n}, \quad \epsilon_p = e^{2\pi i/p},$$

where $\langle , \rangle_k$ denotes a non-degenerate inner product in $\mathbb{V}_k^{(p)}$.
A function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is called a bent function if $|\mathcal{W}_F(a,b)| = p^{n/2}$ for all nonzero $a \in \mathbb{V}_m^{(p)}$ and $b \in \mathbb{V}_n^{(p)}$.

If $m = 1$, then F is also called a p-ary bent function (Boolean if $p = 2$). The Walsh transform of a p-ary function $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is of the form

$$\mathcal{W}_F(1,b) = \mathcal{W}_F(b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{F(x) - \langle b, x\rangle_n}.$$

If $m > 1$, then F is also called a vectorial bent function. The p-ary functions $F_a(x) = < a, F(x) >_m$ for nonzero $a \in \mathbb{V}_m^{(p)}$ are called the component functions of F, and form a vector space of bent functions of dimension m.

Regularity Boolean bent function $f:\mathbb{V}_n^{(2)}\to\mathbb{F}_2$: $\mathcal{W}_f(b)=2^{n/2}(-1)^{f^*(b)}$,
f^* is a Boolean bent function.

Walsh coefficient $\mathcal{W}_f(b)$ for a p-ary bent function $f:\mathbb{V}_n^{(p)}\to\mathbb{F}_p$, at $b\in\mathbb{V}_n^{(p)}$:

$$\mathcal{W}_f(b)=\begin{cases}\pm\epsilon_p^{f^*(b)}p^{n/2} & : \quad p^n\equiv 1 \bmod 4;\\ \pm i\epsilon_p^{f^*(b)}p^{n/2} & : \quad p^n\equiv 3 \bmod 4,\end{cases}$$

$f^*:\mathbb{V}_n^{(p)}\to\mathbb{F}_p$, called the dual of f.
A bent function $f:\mathbb{V}_n^{(p)}\to\mathbb{F}_p$ is called weakly regular if, $\mathcal{W}_f(b)=\zeta\ \epsilon_p^{f^*(b)}p^{n/2}$ for all $b\in\mathbb{V}_n^{(p)}$, $\zeta\in\{\pm1,\pm i\}$ fixed,
regular $\zeta=1$,
otherwise f is called non-weakly regular.

The dual of a weakly regular bent function is also bent.

Example (Construction of bent functions with a complete spread)

Let $n = 2m$. Consider the partition of $\mathbb{V}_n^{(p)}$ via a spread, $\Omega = \{U_0, U_1^*, \ldots, U_{p^m}^*\}$ of $\mathbb{V}_n^{(p)}$, where

- $U_i \leq \mathbb{V}_n^{(p)}$ and $\dim(U_i) = m$ for all $0 \leq i \leq p^m$,
- $U_i \cap U_j = \{0\}$ for all $0 \leq i < j \leq p^m$,
- $U_i^* = U_i \setminus \{0\}$, for all $1 \leq i \leq p^m$, (i.e., $\{U_0, U_1, \ldots, U_{p^m}\}$ is a complete spread of $\mathbb{V}_n^{(p)}$).

Example (Construction of bent functions with a complete spread)

Let $n = 2m$. Consider the partition of $\mathbb{V}_n^{(p)}$ via a spread, $\Omega = \{U_0, U_1^*, \ldots, U_{p^m}^*\}$ of $\mathbb{V}_n^{(p)}$, where

- $U_i \le \mathbb{V}_n^{(p)}$ and $\dim(U_i) = m$ for all $0 \le i \le p^m$,
- $U_i \cap U_j = \{0\}$ for all $0 \le i < j \le p^m$,
- $U_i^* = U_i \setminus \{0\}$, for all $1 \le i \le p^m$, (i.e., $\{U_0, U_1, \ldots, U_{p^m}\}$ is a complete spread of $\mathbb{V}_n^{(p)}$).

One can obtain bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ as follows.

I) For every $c \in \mathbb{F}_p$, the elements of exactly p^{m-1} of U_j^*, $1 \le j \le p^m$ are mapped to c.

II) The elements of U_0 are mapped to a fixed $c_0 \in \mathbb{F}_p$.

Desarguesian spread

Let $n = 2m$ and $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Consider

- $U_s = \{(x, sx) \,:\, x \in \mathbb{F}_{p^m}\}$ for each $s \in \mathbb{F}_{p^m}$,
- $U = \{(0, y) \,:\, y \in \mathbb{F}_{p^m}\}$.

Then $\{U_0, U_s : s \in \mathbb{F}_{p^m}\}$ is the Desarguesian spread.

The class of bent functions obtained from the Desarguesian spread is called the class of PS_{ap} bent functions. The functions in the class of PS_{ap} bent functions are explicitly of the form

$$F(x, y) = B(yx^{p^m-2}),$$

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

Desarguesian spread

Let $n = 2m$ and $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Consider

- $U_s = \{(x, sx) \,:\, x \in \mathbb{F}_{p^m}\}$ for each $s \in \mathbb{F}_{p^m}$,
- $U = \{(0, y) \,:\, y \in \mathbb{F}_{p^m}\}$.

Then $\{U_0, U_s : s \in \mathbb{F}_{p^m}\}$ is the Desarguesian spread.

The class of bent functions obtained from the Desarguesian spread is called the class of PS_{ap} bent functions. The functions in the class of PS_{ap} bent functions are explicitly of the form

$$F(x, y) = B(yx^{p^m - 2}),$$

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

Semifield spread: Finite field multiplication $\longrightarrow$ semifield operation $\circ$.

Definition (Anbar, Meidl, 2022) A partition $\Omega = \{U, A_1, \ldots, A_K\}$ of $\mathbb{V}_n^{(p)}$ into an $n/2$-dimensional subspace U and sets $A_1, \ldots, A_K$, is called a bent partition of $\mathbb{V}_n^{(p)}$ of depth K, if every function with the following properties is bent.

I) Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set $f^{-1}(c) = \{x \in \mathbb{V}_n^{(p)} : f(x) = c\}$,

II) $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Definition (Anbar, Meidl, 2022) A partition $\Omega = \{U, A_1, \ldots, A_K\}$ of $\mathbb{V}_n^{(p)}$ into an $n/2$-dimensional subspace U and sets $A_1, \ldots, A_K$, is called a bent partition of $\mathbb{V}_n^{(p)}$ of depth K, if every function with the following properties is bent.

I) Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set $f^{-1}(c) = \{x \in \mathbb{V}_n^{(p)} : f(x) = c\}$,

II) $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Examples: Generalized semifield spreads

Definition Let $\circ$ be a binary operation on an m dimensional vector space $\mathbb{V}_m^{(p)}$, without loss of generality $\mathbb{F}_{p^m}$, satisfying

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 $x, y, s \in \mathbb{F}_{p^m}$. Then $P = (\mathbb{F}_{p^m}, +, \circ)$ is called a presemifield.

Definition Let $\circ$ be a binary operation on an m dimensional vector space $\mathbb{V}_m^{(p)}$, without loss of generality $\mathbb{F}_{p^m}$, satisfying

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 $x, y, s \in \mathbb{F}_{p^m}$. Then $P = (\mathbb{F}_{p^m}, +, \circ)$ is called a presemifield.

A presemifield, for which there is an element $e \neq 0$ such that $e \circ x = x \circ e = x$ for all $x \in \mathbb{F}_{p^m}$, is a semifield.

Definition Let $\circ$ be a binary operation on an m dimensional vector space $\mathbb{V}_m^{(p)}$, without loss of generality $\mathbb{F}_{p^m}$, satisfying

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 $x, y, s \in \mathbb{F}_{p^m}$. Then $P = (\mathbb{F}_{p^m}, +, \circ)$ is called a presemifield.

A presemifield, for which there is an element $e \neq 0$ such that $e \circ x = x \circ e = x$ for all $x \in \mathbb{F}_{p^m}$, is a semifield.

Given a (pre)semifield $P = (\mathbb{F}_{p^m}, +, \circ)$, consider the (pre)semifield $P^d = (\mathbb{F}_{p^m}, +, \star)$ obtained by defining $x \star y$ with the equation

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

Then P^d is called the dual of P.

Generalized semifield spread

Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, m, $k, e \in \mathbb{Z}^+$ such that $k \mid m$, $e = p^k + p - 1$, $\gcd(p^m - 1, e) = 1$. Consider the following partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

$$\Omega = \{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$$

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

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

Generalized semifield spread

Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, m, $k, e \in \mathbb{Z}^+$ such that $k \mid m$, $e = p^k + p - 1$, $\gcd(p^m - 1, e) = 1$. Consider the following partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

$$\Omega = \{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$$

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

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

Theorem (Anbar, K., Meidl, 2023) Suppose that $P = (\mathbb{F}_{p^m}, +, \circ)$ is a (pre)semifield such that the dual $P^d = (\mathbb{F}_{p^m}, +, \star)$ satisfies

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

(i.e., P^d is right $\mathbb{F}_{p^k}$-linear). Then Ω is a bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Generalized semifield spread

Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, m, $k, e \in \mathbb{Z}^+$ such that $k \mid m$, $e = p^k + p - 1$, $\gcd(p^m - 1, e) = 1$. Consider the following partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

$$\Omega = \{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$$

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

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

Theorem (Anbar, K., Meidl, 2023) Suppose that $P = (\mathbb{F}_{p^m}, +, \circ)$ is a (pre)semifield such that the dual $P^d = (\mathbb{F}_{p^m}, +, \star)$ satisfies

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

(i.e., P^d is right $\mathbb{F}_{p^k}$-linear). Then Ω is a bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Remark. More general, $e \equiv p^l \bmod (p^k - 1)$.

Recall The class of bent functions obtained from the Desarguesian spread is called the class of PS_{ap} bent functions. The functions in the class of PS_{ap} bent functions are explicitly of the form

$$F(x, y) = B(yx^{p^m-2}),$$

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

The bent functions from a generalized Desarguesian spread can be explicitly written as

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

where $k \mid m, e \equiv p^l \bmod (p^k - 1), \gcd(p^m - 1, e) = 1$, and $B : \mathbb{F}_{p^k} \to \mathbb{F}_p$ is a balanced function. We call a function of the form F a generalized PS_{ap} function.

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

We determined (Magma) the 2-ranks of every bent function from a generalized Desarguesian spread with different exponents e_1 and e_2

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

We determined (Magma) the 2-ranks of every bent function from a generalized Desarguesian spread with different exponents e_1 and e_2

(ii) For some given m and k, varying e, one can generate generalized PS_{ap} bent functions of various algebraic degree.

Recall. The algebraic degree of a (partial) spread bent function from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{F}_p$ is $(p-1)m$ (Dillon 1976, Anbar, Meidl 2022).

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

We determined (Magma) the 2-ranks of every bent function from a generalized Desarguesian spread with different exponents e_1 and e_2

(ii) For some given m and k, varying e, one can generate generalized PS_{ap} bent functions of various algebraic degree.

Recall. The algebraic degree of a (partial) spread bent function from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{F}_p$ is $(p-1)m$ (Dillon 1976, Anbar, Meidl 2022).

Theorem

- *The algebraic degree of the generalized PS_{ap} bent function $\mathrm{Tr}_1^m(yx^{-e})$ is a multiple of $(p-1)$.*

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

We determined (Magma) the 2-ranks of every bent function from a generalized Desarguesian spread with different exponents e_1 and e_2

(ii) For some given m and k, varying e, one can generate generalized PS_{ap} bent functions of various algebraic degree.

Recall. The algebraic degree of a (partial) spread bent function from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{F}_p$ is $(p-1)m$ (Dillon 1976, Anbar, Meidl 2022).

Theorem

- *The algebraic degree of the generalized PS_{ap} bent function $\mathrm{Tr}_1^m(yx^{-e})$ is a multiple of $(p-1)$.*
- *Explicitly we can construct such generalized PS_{ap} bent functions with algebraic degree $s(p-1)$ for $s = k, k+1, \ldots, m-1$.*

Theorem (Anbar, K., Meidl, Özbudak, 2024) Let k divide m, $\gcd(e, p^m - 1) = 1$ and $e \equiv p^l \bmod (p^k - 1)$.

(i) In general, two bent partitions (generalized Desarguesian spreads) obtained with different choices of e are not equivalent.

We determined (Magma) the 2-ranks of every bent function from a generalized Desarguesian spread with different exponents e_1 and e_2

(ii) For some given m and k, varying e, one can generate generalized PS_{ap} bent functions of various algebraic degree.

Recall. The algebraic degree of a (partial) spread bent function from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{F}_p$ is $(p-1)m$ (Dillon 1976, Anbar, Meidl 2022).

Theorem

- *The algebraic degree of the generalized PS_{ap} bent function $\mathrm{Tr}_1^m(yx^{-e})$ is a multiple of $(p-1)$.*
- *Explicitly we can construct such generalized PS_{ap} bent functions with algebraic degree $s(p-1)$ for $s = k, k+1, \ldots, m-1$.*

Remark. Experimental results (Magma) show that the generalized PS_{ap} class contains bent functions with many more algebraic degrees.

Vectorial dual-bent function

Definition (Çeşmelioğlu, Meidl, Pott, 2018) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial bent function, i.e., the component functions of F form an m-dimensional vector space of bent functions of dimension m. Then F is called vectorial dual-bent if the set

$$\{(F_a)^* : a \in \mathbb{V}_m^{(p)} \setminus \{0\}\} = \{\langle a, F\rangle_m^* : a \in \mathbb{V}_m^{(p)} \setminus \{0\}\}$$

of the duals of the component functions of F also forms an m-dimensional vector space of bent functions.

Vectorial dual-bent function

Definition (Çeşmelioğlu, Meidl, Pott, 2018) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial bent function, i.e., the component functions of F form an m-dimensional vector space of bent functions of dimension m. Then F is called vectorial dual-bent if the set

$$\{(F_a)^* : a \in \mathbb{V}_m^{(p)} \setminus \{0\}\} = \{\langle a, F\rangle_m^* : a \in \mathbb{V}_m^{(p)} \setminus \{0\}\}$$

of the duals of the component functions of F also forms an m-dimensional vector space of bent functions.

The set $\{(F_a)^* : a \in \mathbb{V}_m^{(p)} \setminus \{0\}\}$ is then the set of the component functions of some other vectorial bent function F^* from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, called a vectorial dual of F, and there exists a permutation σ of $\mathbb{V}_k^{(p)}$ with $\sigma(0) = 0$, such that

$$(F_\alpha)^* = F^*_{\sigma(\alpha)}, \quad \alpha \in \mathbb{F}_{p^k} \setminus \{0\}.$$

Theorem (Anbar, Meidl, 2022) Let $\{U, A_1, \ldots, A_K\}$ be a bent partition of $\mathbb{V}_n^{(p)}$, and suppose that $K = p^k$. Then every function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ such that every element $c \in \mathbb{V}_k^{(p)}$ has the elements of exactly one of the sets A_j, $1 \le j \le p^k$, in its preimage, and U is mapped to some element c_0, is a vectorial bent function.

Proposition (Wang, Fu, Wei, 2023) The vectorial bent function obtained from a generalized semifield spread is a vectorial dual-bent function for which the permutation σ is the identity permutation.

Definition

• 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) $R_0 = \{(x, x) : x \in V\}$ 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, $0 \leq i \leq d$, form a partition of $V \times V$.

III) For every $0 \leq i \leq d$, $R_i^t = R_{i'}$ for some $0 \leq i' \leq d$, 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 such that $(x, z) \in R_i$ and $(z, y) \in R_j$ equals ρ_{ij}^h.

Definition

• 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) $R_0 = \{(x, x) : x \in V\}$ 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, $0 \leq i \leq d$, form a partition of $V \times V$.

III) For every $0 \leq i \leq d$, $R_i^t = R_{i'}$ for some $0 \leq i' \leq d$, 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 such that $(x, z) \in R_i$ and $(z, y) \in R_j$ equals ρ_{ij}^h.

• A fusion of an association scheme $\{R_0, R_1, \ldots, R_d\}$ on V is a partition $\{S_0, S_1, \ldots, S_e\}$ of $V \times V$, such that $S_0 = R_0$, and S_i, $1 \leq i \leq e$, is the union of some of the relations R_j.

Definition

- 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) $R_0 = \{(x, x) : x \in V\}$ 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, $0 \leq i \leq d$, form a partition of $V \times V$.

III) For every $0 \leq i \leq d$, $R_i^t = R_{i'}$ for some $0 \leq i' \leq d$, 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 such that $(x, z) \in R_i$ and $(z, y) \in R_j$ equals ρ_{ij}^h.

- A fusion of an association scheme $\{R_0, R_1, \ldots, R_d\}$ on V is a partition $\{S_0, S_1, \ldots, S_e\}$ of $V \times V$, such that $S_0 = R_0$, and S_i, $1 \leq i \leq e$, is the union of some of the relations R_j.
- An association scheme is called amorphic if any of its fusions is again an association scheme.

Vectorial dual-bent functions and association schemes

Theorem (Anbar, K., Meidl, Özbudak, 2023, Wang et al., 2024) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial dual-bent function, $F(0) = 0$, $F(x) = F(-x)$. 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 $(x, y) \in R_\alpha$ iff $x - y \in D_{F,\alpha}$.

(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 the case that all components of F are weakly regular but not regular and $m = \frac{n}{2}$, in which case we have a $(p^m - 1)$-class association scheme (p must then be 3).

Vectorial dual-bent functions and association schemes

Theorem (Anbar, K., Meidl, Özbudak, 2023, Wang et al., 2024) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial dual-bent function, $F(0) = 0$, $F(x) = F(-x)$. 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 $(x, y) \in R_\alpha$ iff $x - y \in D_{F,\alpha}$.

(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 the case that all components of F are weakly regular but not regular and $m = \frac{n}{2}$, in which case we have a $(p^m - 1)$-class association scheme (p must then be 3).

(ii) If σ is the identity permutation, that is, 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.

Vectorial dual-bent functions and association schemes

Theorem (Anbar, K., Meidl, Özbudak, 2023, Wang et al., 2024) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial dual-bent function, $F(0) = 0$, $F(x) = F(-x)$. 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 $(x, y) \in R_\alpha$ iff $x - y \in D_{F,\alpha}$.

(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 the case that all components of F are weakly regular but not regular and $m = \frac{n}{2}$, in which case we have a $(p^m - 1)$-class association scheme (p must then be 3).

(ii) If σ is the identity permutation, that is, 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.

Corollary. Every generalized semifield spread (bent partition of depth p^k) yields an amorphic p^k-class association scheme.

Examples (in the Maiorana-McFarland class)

Let e, d be integers such that $\gcd(e, p^m - 1) = 1$ and $ed \equiv 1 \bmod (p^m - 1)$.

- $F(x, y) = yx^{-e}$, $\gcd(e, p^m - 1) = 1$, is vectorial dual-bent from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, with vectorial dual $F(x, y) = -xy^{-d}$.

Examples (in the Maiorana-McFarland class)

Let e, d be integers such that $\gcd(e, p^m - 1) = 1$ and $ed \equiv 1 \bmod (p^m - 1)$.

- $F(x, y) = yx^{-e}$, $\gcd(e, p^m - 1) = 1$, is vectorial dual-bent from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, with vectorial dual $F(x, y) = -xy^{-d}$.
- For a divisor k of m, the projection $F_1(x, y) = \mathrm{Tr}_k^m(yx^{-e})$ is vectorial dual-bent. The association scheme for F_1 is a fusion scheme of the association scheme of F, which is amorphic if $e \equiv p^l \bmod (p^k - 1)$.

Examples (in the Maiorana-McFarland class)

Let e, d be integers such that $\gcd(e, p^m - 1) = 1$ and $ed \equiv 1 \bmod (p^m - 1)$.

- $F(x, y) = yx^{-e}$, $\gcd(e, p^m - 1) = 1$, is vectorial dual-bent from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, with vectorial dual $F(x, y) = -xy^{-d}$.
- For a divisor k of m, the projection $F_1(x, y) = \mathrm{Tr}_k^m(yx^{-e})$ is vectorial dual-bent. The association scheme for F_1 is a fusion scheme of the association scheme of F, which is amorphic if $e \equiv p^l \bmod (p^k - 1)$.
- Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, and $a(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be defined by

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

  If for a divisor k of m the dual presemifield P^{d} is right $\mathbb{F}_{p^k}$-linear, then $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ given by $F(x, y) = \mathrm{Tr}_k^m(a(x, y))$ is a vectorial dual-bent function. (Anbar, K., Meidl, Özbudak 2024)

Examples (in the Maiorana-McFarland class)

Let e, d be integers such that $\gcd(e, p^m - 1) = 1$ and $ed \equiv 1 \bmod (p^m - 1)$.

- $F(x, y) = yx^{-e}$, $\gcd(e, p^m - 1) = 1$, is vectorial dual-bent from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, with vectorial dual $F(x, y) = -xy^{-d}$.
- For a divisor k of m, the projection $F_1(x, y) = \mathrm{Tr}_k^m(yx^{-e})$ is vectorial dual-bent. The association scheme for F_1 is a fusion scheme of the association scheme of F, which is amorphic if $e \equiv p^l \bmod (p^k - 1)$.
- Let $P = (\mathbb{F}_{p^m}, +, \circ)$ be a (pre)semifield, and $a(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be defined by

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

  If for a divisor k of m the dual presemifield P^{d} is right $\mathbb{F}_{p^k}$-linear, then $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ given by $F(x, y) = \mathrm{Tr}_k^m(a(x, y))$ is a vectorial dual-bent function. (Anbar, K., Meidl, Özbudak 2024)

Consequence. From a right $\mathbb{F}_{p^k}$-linear semifield $P = (\mathbb{F}_{p^m}, +, \circ)$ we get a vectorial dual-bent function, association scheme. With an exponent $e \equiv p^l \bmod (p^k - 1)$, the association scheme is amorphic, bent partition.

Fusions of MMF association schemes

Theorem (Anbar, K., Meidl, Özbudak 2024) Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ be a (Maiorana-McFarland) vectorial dual-bent function as above, i.e., $F(x,y) = yx^{-e}$ respectively $F(x,y) = \mathrm{Tr}_k^m(a(x,y))$. Let $\mathbb{F}_{p^s}$ be any subfield of $\mathbb{F}_{p^m}$ respectively $\mathbb{F}_{p^k}$.

(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. The preimage set partition of $F^{\gamma,s}$ induces a fusion scheme of the association scheme obtained from F. For different cosets of $\mathbb{F}_{p^s}$, we obtain different fusion schemes.

Fusions of MMF association schemes

Theorem (Anbar, K., Meidl, Özbudak 2024) Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ be a (Maiorana-McFarland) vectorial dual-bent function as above, i.e., $F(x, y) = yx^{-e}$ respectively $F(x, y) = \mathrm{Tr}_k^m(a(x, y))$. Let $\mathbb{F}_{p^s}$ be any subfield of $\mathbb{F}_{p^m}$ respectively $\mathbb{F}_{p^k}$.

(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. The preimage set partition of $F^{\gamma,s}$ induces a fusion scheme of the association scheme obtained from F. For different cosets of $\mathbb{F}_{p^s}$, we obtain different fusion schemes.

(ii) If $e \equiv p^j \bmod (p^s - 1)$, then the preimage set partition of $F^{\gamma,s}$ is a bent partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, the corresponding fusion scheme is amorphic.

Acknowledgement: 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.

References

- N. Anbar, W. Meidl, Bent partitions, Des., Codes, Cryptogr., vol.90, 1081–1101 (2022).
- N. Anbar, T.Kalaycı, W. Meidl, Bent partitions and partial difference sets, IEEE Trans. Inform. Theory, IEEE Trans. Inform. Theory 68 (2022), no. 10, 6894-6903.
- N. Anbar, T.Kalaycı, W. Meidl, Generalized semified spreads, Des. Codes Cryptogr. 91 (2023), 545–562.
- E. van Dam, M. Muzychuk, Some implications on amorphic association schemes, J. Combin. Theory Ser. A vol.117, 111–127 (2010).
- Ja.Ju. Gol'fand, A.V. Ivanov, M. Klin, Amorphic cellular rings, in: I.A. Faradev, et al. (Eds.), Investigations in Algebraic Theory of Combinatorial Objects, Kluwer, Dordrecht, pp. 167–186, (1994).
- W. Kantor, Exponential numbers of two-weight codes, difference sets and symmetric designs, Discret. Math. vol.46, 95–98 (1983).
- W. Kantor, Commutative semifields and symplectic spreads, J. Algebra vol.270, 96–114, (2003).
- S. L. Ma, A survey of partial difference sets, Des., Codes, Cryptogr. vol.4, 221–261, (1994).
- W. Meidl, A survey on *p*-ary and generalized bent functions. Cryptogr. Commun., vol.14, 737–782, (2022).
- W. Meidl, I. Pirsic, Bent and $\mathbb{Z}_{2^k}$-Bent functions from spread-like partitions, Des., Codes, Cryptogr., vol.89, 75–89 (2021).