Des. Codes Cryptogr. (2014) 73:209–216
DOI 10.1007/s10623-013-9820-9

Bent functions on partial spreads

Petr Lisoněk · Hui Yi Lu

Received: 21 May 2012 / Revised: 27 March 2013 / Accepted: 27 March 2013 /
Published online: 9 April 2013

Abstract For an arbitrary prime p we use partial spreads of $\mathbb{F}_p^{2m}$ to construct two classes of bent functions from $\mathbb{F}_p^{2m}$ to $\mathbb{F}_p$. Our constructions generalize the classes $PS^{(-)}$ and $PS^{(+)}$ of binary bent functions which are due to Dillon.

Keywords Bent function · Partial spread

Mathematics Subject Classification (2010) 94C10 · 51E14

1 Introduction

The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ that are as far as possible from the set of all linear (or affine) functions on the same domain have been widely studied as *bent functions* since mid-1960s when Rothaus introduced them [12,13]. Besides being interesting combinatorial objects, they have important applications in cryptography (design of stream ciphers and design of S-boxes for block ciphers). They also have applications in the design of sequences with favourable correlation properties. By extending Rothaus' definition in a natural way, Kumar, Scholtz and Welch in 1985 defined bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ for an arbitrary prime p, and these "generalized" bent functions have also enjoyed a lot of interest in the literature.

In Sect. 2 we review background material on bent functions. In Sect. 3 we prove combinatorial characterizations of two classes of bent functions from $\mathbb{F}_p^{2m}$ to $\mathbb{F}_p$ (where m is a positive integer and p is a prime) that generalize the classes $PS^{(-)}$ and $PS^{(+)}$ discovered by Dillon for $p = 2$ [1,2]. The ingredient of our constructions is a partial spread, which is a set of pairwise disjoint (except for the origin) m-dimensional subspaces of $\mathbb{F}_p^{2m}$. These

Communicated by C. Carlet.

P. Lisoněk (✉) · H. Y. Lu
Department of Mathematics, Simon Fraser University, Burnaby,
BC V5A 1S6, Canada
e-mail: plisonek@sfu.ca

constructions have been noted previously in the special case when one employs the spread obtained from the subfield $\mathbb{F}_{p^m}$ of $\mathbb{F}_{p^{2m}}$. We remove this restriction and we prove the results for an arbitrary partial spread.

2 Background

Throughout the article, p denotes a prime. For a positive integer s, let $\mathbb{F}_{p^s}$ denote the finite field of order p^s.

Let V be a vector space over $\mathbb{F}_p$ and for $a, b \in V$ denote by $\langle a, b\rangle$ an arbitrary inner product on V (that is, a non-degenerate symmetric bilinear form on V). It is well known that given any inner product $\langle x, y\rangle$ on $\mathbb{F}_p^n$, the set of linear functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is precisely the set of functions $f_a(x) = \langle a, x\rangle$ where a runs through all vectors in $\mathbb{F}_p^n$.

Let $\zeta_p = e^{2\pi\sqrt{-1}/p}$, a primitive pth root of unity.

Definition 2.1 For $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and a fixed inner product $\langle x, y\rangle$ on $\mathbb{F}_p^n$ we define the *Walsh transform* of f to be the mapping $\mathcal{W}_f : \mathbb{F}_p^n \to \mathbb{C}$ given by

$$\mathcal{W}_f(a) = \sum_{x\in\mathbb{F}_p^n} \zeta_p^{f(x)-\langle a,x\rangle}.$$

Since $f_a(x) = \langle a, x\rangle$ are precisely all linear functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, it is natural to consider f as highly non-linear if $|\mathcal{W}_f(a)|$ is small for all $a \in \mathbb{F}_p^n$. From Parseval's identity $\sum_{a\in\mathbb{F}_p^n} |\mathcal{W}_f(a)|^2 = p^{2n}$ (which holds for each function f) we see that $|\mathcal{W}_f(a)| \geq p^{n/2}$ for at least one $a \in \mathbb{F}_p^n$. Thus we naturally arrive at the following definition.

Definition 2.2 [7, Definition 2] We say that $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a *bent function* if $|\mathcal{W}_f(a)| = p^{n/2}$ for all $a \in \mathbb{F}_p^n$.

For $p = 2$ binary bent functions were defined by Rothaus [12,13]. Note that n must be even in this case, as $\mathcal{W}_f(a)$ is always an integer when $p = 2$. In 1985, Kumar et al. [7] extended Rothaus' definition to the case of an arbitrary prime p.

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function. We say that f is *regular* if there exists $f^* : \mathbb{F}_p^n \to \mathbb{F}_p$ such that $\mathcal{W}_f(a) = p^{n/2}\zeta_p^{f^*(a)}$ for all $a \in \mathbb{F}_p^n$. The function f^* is called the *dual* of f.

In the next section we will use the following result on the distribution of values of a bent function due to Nyberg [9].

Theorem 2.3 (*[9],* Theorem 3.2) *Let m be a positive integer and p a prime. Suppose that $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ is a bent function and for $u \in \mathbb{F}_p$ denote $b_u := |f^{-1}(u)|$. Then there exists $k \in \mathbb{F}_p$ such that*

$$b_k = p^{2m-1} \pm (p-1)p^{m-1}$$
$$b_\ell = p^{2m-1} \mp p^{m-1} \quad \textit{for } \ell \in \mathbb{F}_p \setminus \{k\}.$$

Here the $\pm$ signs are taken correspondingly. Moreover, a regular bent function has the upper signs.

3 The constructions

Throughout this section we assume that m is a positive integer.

Definition 3.1 An *m-spread* of $\mathbb{F}_p^n$ is a set of pairwise disjoint (except for 0) m-dimensional subspaces of $\mathbb{F}_p^n$ whose union equals $\mathbb{F}_p^n$. A *partial m-spread* of $\mathbb{F}_p^n$ is a set of pairwise disjoint (except for 0) m-dimensional subspaces of $\mathbb{F}_p^n$.

Note that the prefix m in the term "(partial) m-spread" indicates the dimension of the subspaces that form the (partial) spread. It is well known that an m-spread of $\mathbb{F}_p^n$ exists if and only if m divides n.

In Chap. 6 of [1], Dillon used partial m-spreads of $\mathbb{F}_2^{2m}$ to construct two families of bent functions from $\mathbb{F}_2^{2m}$ to $\mathbb{F}_2$, which he named *family* $PS^{(-)}$ and *family* $PS^{(+)}$ respectively. In Sects. 3.1 and 3.2 we generalize these two families to an arbitrary prime characteristic.

Let $\mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$ and similarly for $T \subset \mathbb{F}_p^n$ denote $T^* := T \setminus \{0\}$. For $a \in \mathbb{F}_p^{2m}$ denote $a^\perp := \{x \in \mathbb{F}_p^{2m} : \langle a, x\rangle = 0\}$. In order to simplify some of the calculations that will follow later, we state one part of them as a separate lemma.

Lemma 3.2 *Let $a \in \mathbb{F}_p^{2m}$, $a \neq 0$, and assume that T is a subspace of $\mathbb{F}_p^{2m}$ such that $T \not\subset a^\perp$. Then $\sum_{x\in T^*} \zeta_p^{-\langle a,x\rangle} = -1$.*

Proof If $T \not\subset a^\perp$, then $\sum_{x\in T} \zeta_p^{-\langle a,x\rangle} = 0$ and the result follows immediately. □

3.1 p-ary Family $PS^{(-)}$

Theorem 3.3 *Let p be a prime number and let m be an integer such that $p^m > 3$. Suppose that $\mathcal{S}$ is a partial m-spread of $\mathbb{F}_p^{2m}$ and $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ is such that for each $T \in \mathcal{S}$, f is constant on T^*. Moreover suppose that*

$$f^{-1}(0) = \mathbb{F}_p^{2m} \setminus \bigcup_{T\in\mathcal{S}} T^*.$$

Then f is bent if and only if for each $x \in \mathbb{F}_p^*$, $f^{-1}(x) \cup \{0\}$ is the union of exactly p^{m-1} elements of $\mathcal{S}$. If f is bent, then it is a regular bent function.

Proof We first prove the "⇐" part of Theorem 3.3. Let us assume that $\mathcal{S}$ is a partial m-spread of $\mathbb{F}_p^{2m}$. We also assume that $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ is such that for each $j \in \mathbb{F}_p^*$, if we denote by D_j the preimage of j under f, then

$$D_j := f^{-1}(j) = \bigcup_{i=1}^{p^{m-1}} S_{ji}^*, \tag{1}$$

where S_{ji} is an element of $\mathcal{S}$ for each i and j, and $S_{ji} \neq S_{kl}$ for $(j, i) \neq (k, l)$. Let us also define $D_0 := f^{-1}(0)$ but note that no structure is assumed or needed on D_0. Under these assumptions we will show that f is regular bent.

An easy calculation shows $\mathcal{W}_f(0) = \sum_{j\in\mathbb{F}_p^*} p^{m-1}(p^m-1)\zeta_p^j + p^{2m} - (p-1)p^{m-1}(p^m - 1) = -p^{m-1}(p^m - 1) + p^{2m} - (p - 1)p^{m-1}(p^m - 1) = p^m$.

From now on let us assume that $a \in \mathbb{F}_p^{2m}$ and $a \neq 0$. Then $a^\perp$ is a $(2m - 1)$-dimensional subspace of $\mathbb{F}_p^{2m}$ and hence, from the partial spread condition combined with a dimension argument it follows that $a^\perp$ contains at most one subspace S_{ji} as introduced in Eq. 1. In the computation of $\mathcal{W}_f(a)$ we will distinguish two cases according to whether $a^\perp$ does or does not contain one of the subspaces S_{ji}.

First let us assume that none of the subspaces S_{ji} introduced in Eq. 1 is contained in $a^{\perp}$. Then using Lemma 3.2 and noting that $\sum_{x\in D_0}\zeta_p^{-\langle b,x\rangle} = -\sum_{j\in\mathbb{F}_p^*}\sum_{x\in D_j}\zeta_p^{-\langle b,x\rangle}$ we compute

$$\begin{aligned}\mathcal{W}_f(a) &= \sum_{x\in\mathbb{F}_p^{2m}} \zeta_p^{f(x)-\langle a,x\rangle} = \sum_{j\in\mathbb{F}_p^*}\sum_{x\in S_{ji}^*,1\le i\le p^{m-1}} \zeta_p^{j-\langle a,x\rangle} + \sum_{x\in D_0}\zeta_p^{-\langle a,x\rangle}\\ &= \sum_{j\in\mathbb{F}_p^*}\zeta_p^j p^{m-1}(-1) - (p-1)(-p^{m-1})\\ &= (-1)(-p^{m-1}) + (p-1)p^{m-1} = p^m.\end{aligned}$$

Next let us assume that $a^{\perp}$ contains the subspace S_{kl}. We compute

$$\begin{aligned}\mathcal{W}_f(a) &= \sum_{x\in\mathbb{F}_p^{2m}} \zeta_p^{f(x)-\langle a,x\rangle} = \sum_{j\in\mathbb{F}_p^*}\sum_{x\in S_{ji}^*,1\le i\le p^{m-1}} \zeta_p^{j-\langle a,x\rangle} + \sum_{x\in D_0}\zeta_p^{-\langle a,x\rangle}\\ &= \sum_{j\in\mathbb{F}_p^*}\zeta_p^j p^{m-1}(-1) - \zeta_p^k(-1) + \zeta_p^k(p^m-1) - [(p-1)(-p^{m-1}) + p^m]\\ &= (-1)(-p^{m-1}) + p^m\zeta_p^k - p^{m-1} = p^m\zeta_p^k.\end{aligned}$$

This finishes the proof of the "⇐" part of Theorem 3.3. Note that for each a we have $\mathcal{W}_f(a) = p^m\zeta_p^{f^*(a)}$ for some $f^*(a)\in\mathbb{F}_p$, thus f is regular bent.

Now we prove the "⇒" part of Theorem 3.3. Let us assume that $\mathcal{S}$ is a partial m-spread of $\mathbb{F}_p^{2m}$ and $p^m > 3$. We also assume that $f:\mathbb{F}_p^{2m}\to\mathbb{F}_p$ is a bent function such that for each $T\in\mathcal{S}$, f is constant on T^*, and

$$f^{-1}(0) = \mathbb{F}_p^{2m}\setminus\bigcup_{T\in\mathcal{S}} T^*.$$

For each $j\in\mathbb{F}_p^*$ let N_j be such that

$$f^{-1}(j) = \bigcup_{i=1}^{N_j} S_{ji}^*,$$

where all S_{ji} are pairwise distinct elements of $\mathcal{S}$. We have to show that $N_j = p^{m-1}$ for all $j\in\mathbb{F}_p^*$.

We have

$$p^{2m-1} + (p-1)p^{m-1} = (p^{m-1}+1)(p^m-1) + 1 \tag{2}$$

$$p^{2m-1} - (p-1)p^{m-1} = (p^{m-1}-1)(p^m-1) + 2p^{m-1} - 1. \tag{3}$$

As in Theorem 2.3 for $u\in\mathbb{F}_p$ denote $b_u := |f^{-1}(u)|$, then for $j\in\mathbb{F}_p^*$ we have

$$b_j = N_j(p^m-1). \tag{4}$$

For $p=2$ Theorem 3.3 was proved by Dillon [1, Chap. 6], hence we can assume without loss of generality that $p>2$. Then Eqs. 2–4 imply that we must have $k=0$ in Theorem 2.3.

Thus all numbers N_j are equal to each other for all $j\in\mathbb{F}_p^*$. Let $N_j = N$ for $j\in\mathbb{F}_p^*$. By Theorem 2.3 we have $N = \frac{p^{2m-1}\mp p^{m-1}}{p^m-1}$. We have

$$\frac{p^{2m-1}-p^{m-1}}{p^m-1} = p^{m-1} \tag{5}$$

$$\frac{p^{2m-1}+p^{m-1}}{p^m-1} = p^{m-1} + \frac{2p^{m-1}}{p^m-1}. \tag{6}$$

From the assumption $p^m > 3$ it follows that the number on the right-hand side of Eq. 6 is never an integer; thus we always have $N = p^{m-1}$ by Eq. 5. This finishes the proof of the "⇒" part of Theorem 3.3. □

Let us remark that the assumption $p^m > 3$ is necessary. For $p^m = 3$ consider the function $f : \mathbb{F}_{3^2} \to \mathbb{F}_3$ given by $f(x) = x^4$ and the 1-spread $\mathcal{S} = \{\{0, x, -x\} : x \in \mathbb{F}_{3^2}\}$ of $\mathbb{F}_{3^2}$. Then f is a bent function that is constant on T^* for all $T \in \mathcal{S}$. However, using the notation introduced above, $N_1 = N_2 = 2 \neq 3^{1-1}$. Similarly for $p^m = 2$ consider the function $f : \mathbb{F}_{2^2} \to \mathbb{F}_2$ given by $f(x) = x^3$.

For $p = 2$ the class of binary bent functions satisfying the conditions of Theorem 3.3 was named $PS^{(-)}$ class by Dillon [1, Chap. 6]. Thus we introduce the following generalization of this naming convention.

Definition 3.4 The class of bent functions satisfying the conditions of Theorem 3.3 will be called *p-ary* $PS^{(-)}$ *class*.

Corollary 3.5 *If f is a bent function that belongs to the p-ary $PS^{(-)}$ class, then the dual of f also belongs to the p-ary $PS^{(-)}$ class.*

Proof Assume that f belongs to the p-ary $PS^{(-)}$ class and recall that f^* denotes the dual of f. By the proof of Theorem 3.3 for $k \in \mathbb{F}_p^*$ we have $f^*(a) = k$ exactly when $S_{ki} \subset a^\perp$ for some i and $a \neq 0$, equivalently $a \in (S_{ki}^\perp)^*$, where $S_{ki}^\perp$ denotes the dual subspace of S_{ki}. Thus we see that f^* has the same structure as f after replacing all subspaces S_{ji} with their duals. Thus f^* belongs to the p-ary $PS^{(-)}$ class. □

3.2 p-ary Family $PS^{(+)}$

It follows from the definitions at once that $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a (regular) bent function if and only if $g(x) := f(x) + c$ is a (regular) bent function for each $c \in \mathbb{F}_p$. Thus, when studying a bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ we can assume without loss of generality that $f(0) \in U$ for any choice of $\emptyset \neq U \subseteq \mathbb{F}_p$.

Theorem 3.6 *Let p be a prime number and let m be an integer. Suppose that $\mathcal{S}$ is a partial m-spread of $\mathbb{F}_p^{2m}$ and $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ is such that for each $T \in \mathcal{S}$, f is constant on T^*. Moreover suppose that*

$$f^{-1}(0) = \left(\mathbb{F}_p^{2m}\right)^* \setminus \bigcup_{T \in S} T^*$$

and $f(0) = t$ where $t \in \mathbb{F}_p^*$. Then f is bent if and only if for each $x \in \mathbb{F}_p^* \setminus \{t\}$, $f^{-1}(x) \cup \{0\}$ is the union of exactly p^{m-1} elements of $\mathcal{S}$ and $f^{-1}(t)$ is the union of exactly $p^{m-1} + 1$ elements of $\mathcal{S}$. If f is bent, then it is a regular bent function.

Proof The proof of Theorem 3.6 is analogous to the proof of Theorem 3.3. We first prove the "⇐" part of Theorem 3.6. Let us assume that $\mathcal{S}$ is a partial m-spread of $\mathbb{F}_p^{2m}$. We also assume that $f : \mathbb{F}_p^{2m} \to \mathbb{F}_p$ and $t \in \mathbb{F}_p^*$ are such that for each $j \in \mathbb{F}_p^* \setminus \{t\}$

$$D_j := f^{-1}(j) = \bigcup_{i=1}^{p^{m-1}} S_{ji}^* \tag{7}$$

and

$$D_t := f^{-1}(t) = \bigcup_{i=1}^{p^{m-1}+1} S_{ti}, \tag{8}$$

where S_{ji} is an element of $\mathcal{S}$ for each i and j, and $S_{ji} \neq S_{kl}$ for $(j,i) \neq (k,l)$. Let $D_0 := f^{-1}(0)$ and note that $|D_0| = p^{2m} - (1+((p-1)p^{m-1}+1)(p^m-1)) = p^{2m-1} - p^{m-1}$. Under these assumptions we will show that f is regular bent.

We compute $\mathcal{W}_f(0) = \sum_{x\in\mathbb{F}_p^{2m}} \zeta_p^{f(x)} = \sum_{j\in\mathbb{F}_p^*\setminus\{t\}} p^{m-1}(p^m-1)\zeta_p^j + ((p^{m-1}+1)(p^m-1)+1)\zeta_p^t + (p^{2m-1}-p^{m-1})\zeta_p^0 = p^{m-1}(p^m-1)(-1) + p^m\zeta_p^t + (p^{2m-1}-p^{m-1}) = p^m\zeta_p^t$.

From now on suppose that $a \neq 0$. First assume that none of the subspaces S_{ji} introduced in Eqs. 7, 8 is contained in $a^\perp$. Then using Lemma 3.2 and noting that $\sum_{x\in D_0} \zeta_p^{-\langle a,x\rangle} = -\sum_{j\in\mathbb{F}_p^*}\sum_{x\in D_j} \zeta_p^{-\langle a,x\rangle}$ we compute

$$\begin{aligned}\mathcal{W}_f(a) &= \sum_{j\in\mathbb{F}_p^*} \sum_{x\in S_{ji}^*, 1\le i\le p^{m-1}} \zeta_p^{j-\langle a,x\rangle} + \sum_{x\in S_{t,p^{m-1}+1}} \zeta_p^{t-\langle a,x\rangle} + \sum_{x\in D_0} \zeta_p^{-\langle a,x\rangle}\\ &= \sum_{j\in\mathbb{F}_p^*} \zeta_p^j p^{m-1}(-1) + 0 - (p-1)p^{m-1}(-1) = p^m.\end{aligned}$$

Next let us assume that $a^\perp$ contains the subspace S_{kl}. Without loss of generality we can assume $(k,l) \neq (t, p^{m-1}+1)$. (If $(k,l) = (t, p^{m-1}+1)$, then swap $S_{t,p^{m-1}+1}$ and $S_{t,p^{m-1}}$ without changing f.) We compute

$$\begin{aligned}\mathcal{W}_f(a) &= \sum_{j\in\mathbb{F}_p^*} \sum_{x\in S_{ji}^*, 1\le i\le p^{m-1}} \zeta_p^{j-\langle a,x\rangle} + \sum_{x\in S_{t,p^{m-1}+1}} \zeta_p^{t-\langle a,x\rangle} + \sum_{x\in D_0} \zeta_p^{-\langle a,x\rangle}\\ &= \sum_{j\in\mathbb{F}_p^*} \zeta_p^j p^{m-1}(-1) - \zeta_p^k(-1) + \zeta_p^k(p^m-1) + 0 - ((p-1)p^{m-1}(-1) + p^m)\\ &= (-1)(-p^{m-1}) + p^m\zeta_p^k - p^{m-1} = p^m\zeta_p^k.\end{aligned}$$

This finishes the proof of the "⇐" part of Theorem 3.6. Note that for each a we found that $\mathcal{W}_f(a) = p^m\zeta_p^{f^*(a)}$ for some $f^*(a) \in \mathbb{F}_p$, thus f is regular bent.

To prove the "⇒" part of Theorem 3.6, for $j \in \mathbb{F}_p^*$ let N_j be such that for $j \neq t$

$$f^{-1}(j) = \bigcup_{i=1}^{N_j} S_{ji}^*$$

and

$$f^{-1}(t) = \bigcup_{i=1}^{N_t} S_{ti},$$

where all S_{ji} are pairwise distinct elements of $\mathcal{S}$, an m-spread of $\mathbb{F}_p^{2m}$. We have to show that $N_j = p^{m-1}$ for all $j \in \mathbb{F}_p^* \setminus \{t\}$ and $N_t = p^{m-1}+1$.

Again as in Theorem 2.3 for $u \in \mathbb{F}_p$ denote $b_u := |f^{-1}(u)|$, then for $j \in \mathbb{F}_p^* \setminus \{t\}$ we have

$$b_j = N_j(p^m-1) \tag{9}$$

and further

$$b_t = N_t(p^m - 1) + 1. \tag{10}$$

Since for $p = 2$ Theorem 3.6 was proved by Dillon [1, Chap. 6], we can again assume without loss of generality that $p > 2$. Let k be as in Theorem 2.3. By considering Eqs. 2, 3, 9 and 10 we see that only the following cases (i) and (ii) may possibly occur.

(i) We have $k = t$ and the upper signs are chosen in Theorem 2.3. Then $N_t = p^{m-1} + 1$ by Eq 2 and for $j \in \mathbb{F}_p^* \setminus \{t\}$

$$N_j = \frac{p^{2m-1} - p^{m-1}}{p^m - 1} = p^{m-1}.$$

(ii) We have $k = t$, $m = 1$ and the lower signs are chosen in Theorem 2.3. But then $b_t = 1$, hence D_t does not contain an m-dimensional subspace of $\mathbb{F}_p^{2m}$, which means that this case never occurs.

□

Definition 3.7 The class of bent functions satisfying the conditions of Theorem 3.6 will be called *p-ary* $PS^{(+)}$ *class*.

The reason for this naming convention is the fact that for $p = 2$ the class of binary bent functions satisfying the conditions of Theorem 3.6 was named $PS^{(+)}$ class by Dillon [1, Chap. 6].

Corollary 3.8 *If f is a bent function that belongs to the p-ary $PS^{(+)}$ class, then the dual of f also belongs to the p-ary $PS^{(+)}$ class.*

Proof The proof is analogous to the proof of Corollary 3.5. Assume that f belongs to the p-ary $PS^{(+)}$ class. Using the proof of Theorem 3.6 we deduce that f^* has the same structure as f after replacing all subspaces S_{ji} with their duals. Thus f^* belongs to the p-ary $PS^{(+)}$ class. □

3.3 Spreads from subfields

Let Tr denote the trace function from $\mathbb{F}_{p^{2m}}$ to $\mathbb{F}_p$. Since $\mathbb{F}_{p^{2m}}$ is a $2m$-dimensional vector space over $\mathbb{F}_p$, by taking the inner product $\langle x, y\rangle = \mathrm{Tr}(xy)$ on $\mathbb{F}_{p^{2m}}$ we can consider bent functions from $\mathbb{F}_{p^{2m}}$ to $\mathbb{F}_p$ and all definitions and statements given above apply.

Let α be a primitive element of $\mathbb{F}_{p^{2m}}$. Then $\{\alpha^i \mathbb{F}_{p^m} : 0 \le i \le p^m\}$ is an m-spread of $\mathbb{F}_{p^{2m}}$, which we will call the *subfield spread*. For partial spreads that are subsets of a subfield spread, the constructions that we gave in Theorems 3.3 and 3.6 above produce the same bent functions (up to a shift by a constant), and for reference we now state this special case explicitly:

Theorem 3.9 *([10]* Theorem 2.5) *Let p be a prime and m a positive integer with $p^m > 3$. Let α be a primitive element of $\mathbb{F}_{p^{2m}}$. Suppose that $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ is such that $f(0) = 0$ and for each $0 \le i \le p^m$ and for each $v \in \mathbb{F}_{p^m}^*$ we have $f(\alpha^i v) = f(\alpha^i)$. Then f is bent if and only if for each $u \in \mathbb{F}_p^*$ there are exactly p^{m-1} elements $i \in \{0, \ldots, p^m\}$ such that $f(\alpha^i) = u$. If f is bent, then it is a regular bent function.*

Theorem 3.9 has been discovered previously by several authors. The earliest reference, giving the statement in a slightly weaker form, appears to be Theorem 2.5 in [10]. The statement also occurs as a special case of Theorem 4.1 in [5].

Theorems 3.3 and 3.6 proved in this paper are more general than Theorem 3.9 due to the following two reasons: It is well known that there do exist m-spreads of $\mathbb{F}_p^{2m}$ that are not equivalent under $\mathrm{GL}(2m, \mathbb{F}_p)$ to the subfield m-spread, see for example [4, Chap. 17]. Moreover, there do exist partial m-spreads of $\mathbb{F}_p^{2m}$ that are not extendible to an m-spread, see for example [11] and the references therein.

Bent functions constructed from Theorem 3.9 belong to both classes $PS^{(-)}$ and $PS^{(+)}$ introduced in Definitions 3.4 and 3.7 above, up to a shift by a constant as discussed at the beginning of Sect. 3.2.

A function $f : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ given by a sum of traces of monomials $\beta_j x^{j(p^m-1)}$ where $j \in \{0, \ldots, p^m\}$ and $\beta_j \in \mathbb{F}_{p^{2m}}$ is said to have *Dillon type exponents*. In general the traces may be taken either from $\mathbb{F}_{p^{2m}}$ or from some subfields thereof, as certain values of j will guarantee that $x^{j(p^m-1)}$ belongs to a proper subfield of $\mathbb{F}_{p^{2m}}$ and then the choices for β_j and the trace function are made accordingly. The function may involve traces from different fields [6,8]. For any f that has Dillon type exponents, using the notation of Theorem 3.9 we always have $f(0) = 0$ and $f(\alpha^i v) = f(\alpha^i)$ because $v^{j(p^m-1)} = 1$ if $v \in \mathbb{F}_{p^m}^*$. Hence by Theorem 3.9, f is (regular) bent if and only if for each $u \in \mathbb{F}_p^*$ there are exactly p^{m-1} elements $i \in \{0, \ldots, p^m\}$ such that $f(\alpha^i) = u$. This condition can be rewritten in terms of exponential sums when f is restricted to certain particular forms. The resulting classes of bent functions with Dillon type exponents have been studied in several papers recently. The interested reader is referred to [3, Section II], [6,8].

Acknowledgments Research partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

1. Dillon J.F.: Elementary Hadamard difference sets. PhD thesis, University of Maryland (1974).
2. Dillon J.F.: Elementary Hadamard difference sets. In: Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic University, Boca Raton, 1975), pp. 237–249. Congressus Numerantium, No. XIV, Utilitas Math., Winnipeg (1975).
3. Helleseth T., Kholosha A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory **52**(5), 2018–2032 (2006).
4. Hirschfeld J.W.P.: Finite projective spaces of three dimensions. The Clarendon Press,Oxford University Press, New York (1985).
5. Hou X.: q-ary bent functions constructed from chain rings. Finite Fields Appl. **4**(1), 55–61 (1998).
6. Jia W., Zeng X., Helleseth T., Li C.: A class of binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory **58**(9), 6054–6063 (2012).
7. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**(1), 90–107 (1985).
8. Li N., Helleseth T., Tang X., Kholosha A.: Several new classes of bent functions from Dillon exponents. IEEE Trans. Inform. Theory **59**(3), 1818–1831 (2013).
9. Nyberg K.: Constructions of bent functions and difference sets. Advances in cryptology, EUROCRYPT ’90 (Aarhus, 1990), Lecture Notes in Computer Science, vol. 473, pp. 151–160. Springer, Berlin (1991).
10. Nyberg K.: Perfect nonlinear S-boxes. Advances in cryptology, EUROCRYPT ’91 (Brighton, 1991), Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer, Berlin (1991).
11. Rajola S., Scafati Tallini M.: Maximal partial spreads in PG(3, q). J. Geom. **85**(1–2), 138–148 (2006).
12. Rothaus O.: On bent functions. IDA CRD Working Paper No. 169 (1966).
13. Rothaus O.S.: On “bent” functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).