COUNTING PARTIAL SPREAD FUNCTIONS IN EIGHT VARIABLES

PHILIPPE LANGEVIN AND XIANG-DONG HOU

Abstract. In this paper we report the following computational results on partial spread functions in 8 variables: (i) the numbers of equivalence classes of partial spread functions (in 8 variables) of all possible orders; (ii) the total number of partial spread bent functions in 8 variables; (iii) the distribution of the cardinalities of stabilizers (in $\mathrm{GL}(8,\mathbb{F}_2)$) of partial spread bent functions in 8 variables. The computational method is also described.

1. Introduction

Bent functions (definition in Section 2) were introduced by Rothaus [14] and have since become ubiquitous in coding theory, cryptography and design theory. Many families of bent functions have been discovered and many constructions of bent functions have been developed. (See, for example, [1, 2, 4, 5, 8] and the references therein.) Bent functions in ≤ 6 variables have been classified [14]. The total number of bent functions in 8 variables has been determined [12]. However, the classification of bent functions in an arbitrary (even) number of variables is believed to be out of reach. Partial spread ($\mathcal{PS}$) bent functions are an important family of bent functions introduced by Dillon [4] based on certain collections of t-dimensional subspaces of $\mathbb{F}_2^{2t}$ called *partial spreads* (definition in Section 2). A partial spread consisting of n t-dimensional subspaces of $\mathbb{F}_2^{2t}$ is said to have *order* n. The partial spread bent functions in $2t$ variables are the indicator functions of partial spreads of order 2^{t-1} or $2^{t-1}+1$. The partial spread bent functions of order 2^{t-1} ($2^{t-1}+1$, respectively) form the $\mathcal{PS}^{(-)}$ ($\mathcal{PS}^{(+)}$, respectively) family and $\mathcal{PS} = \mathcal{PS}^{(-)} \cup \mathcal{PS}^{(+)}$; see Section 2 for more details. Classification of $\mathcal{PS}$ bent functions in $2t \geq 8$ variables was unknown previously. The $\mathcal{PS}$ bent functions in 8 variables are the partial spread functions in 8 variables of orders 8 and 9. We announce that the classification of partial spread functions in 8 variables of all possible orders (1 through 17) has been obtained through computer search. In this paper we report the following data from this classification; more data of the classification can be found at [9].

(i) the numbers of equivalence classes of partial spread functions in 8 variables of all possible orders under the action of $\mathrm{GL}(8,\mathbb{F}_2)$;
(ii) the total number of $\mathcal{PS}$ bent functions in 8 variables;
(iii) the distribution of the cardinalities of stabilizers (in $\mathrm{GL}(8,\mathbb{F}_2)$) of $\mathcal{PS}$ bent functions in 8 variables.

(In (iii), the *stabilizer* of a $\mathcal{PS}$ bent function is the subgroup of $\mathrm{GL}(8,\mathbb{F}_2)$ which fixes the bent function.) We also determined the equivalence classes of $\mathcal{PS}$ bent functions in 8 variables that contain $\mathcal{PS}_{\mathrm{ap}}$ bent functions, which are a special type of $\mathcal{PS}$ bent functions. These computational results indicate that in 8 variables,

$\mathcal{PS}$ bent functions constitute a small portion of all bent functions and $\mathcal{PS}_{\mathrm{ap}}$ bent functions constitute a small portion of all $\mathcal{PS}$ bent functions. On the theoretic side, the contribution of this paper is a classification of all partial spreads of order 4 in $\mathbb{F}^{2t}$ where $\mathbb{F}$ is an arbitrary field.

2. Partial Spreads and Bent functions

Throughout the paper, we assume that m is a positive even integer and we let $t = \frac{m}{2}$. The *Fourier transform* of a function $g\colon \mathbb{F}_2^m \to \mathbb{C}$ is the function $\widehat{g} : \mathbb{F}_2^m \to \mathbb{C}$ defined by

$$\widehat{g}(a) = \sum_{x \in \mathbb{F}_2^m} g(x)\mu(a \cdot x),$$

where μ is the canonical additive character of $\mathbb{F}_2$, i.e., $\mu(c) = (-1)^c$, and $a \cdot x$ the standard inner product of $\mathbb{F}_2^m$. When $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is a Boolean function, the Fourier transform of $\mu(f(x))$ is called the *Walsh transform* of f and is usually denoted by $f^{\mathcal{W}}$. Let $\epsilon : \mathbb{F}_2 \to \mathbb{C}$ be the map such that $\epsilon(0) = 0$ and $\epsilon(1) = 1$. (ϵ is the Teichmüller character of $\mathbb{F}_2$.) Then $\mu \circ f = 1 - 2(\epsilon \circ f)$ and

$$f^{\mathcal{W}}(a) = \begin{cases} -2\,\widehat{\epsilon \circ f}(a) & \text{if } a \neq 0, \\ 2^m - 2|f^{-1}(1)| = -2^m + 2|f^{-1}(0)| & \text{if } a = 0. \end{cases} \tag{1}$$

A *bent function* is a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ such that $|f^{\mathcal{W}}(a)| = 2^t$ for all $a \in \mathbb{F}_2^m$. Equivalently, using Parseval's identity, f is bent if and only if $\widehat{\epsilon \circ f}(a) = \pm 2^{t-1}$ for all $0 \neq a \in \mathbb{F}_2^m$.

A *partial spread* of order n (an n-spread) in $\mathbb{F}_2^m$ is a set of n t-dimensional subspaces $H_1, \ldots, H_n$ of $\mathbb{F}_2^m$ such that $H_i \cap H_j = \{0\}$ for all $1 \leq i < j \leq n$. Clearly, the order of a partial spread is less or equal to $2^t + 1$, and such a maximal partial spread is called a *spread*. Let $\{H_1, \ldots, H_n\}$ be an n-spread. Let $f_i : \mathbb{F}_2^m \to \mathbb{F}_2$ be the indicator function of H_i, i.e., $f_i^{-1}(1) = H_i$. The Boolean function $f = \sum_{i=1}^n f_i$ is called an *n-spread function*. Note that

$$\epsilon \circ f = \sum_{i=1}^n \epsilon \circ f_i - 2\lfloor \frac{n}{2} \rfloor \delta_0,$$

where $\delta_0 : \mathbb{F}_2^m \to \mathbb{C}$ is the function that maps 0 to 1 and all $0 \neq x \in \mathbb{F}_2^m$ to 0. Thus for $0 \neq a \in \mathbb{F}_2^m$,

$$\widehat{\epsilon \circ f}(a) = \sum_{i=1}^n \widehat{\epsilon \circ f_i}(a) - 2\lfloor \frac{n}{2} \rfloor \widehat{\delta_0}(a) = \begin{cases} -2\lfloor \frac{n}{2} \rfloor & \text{if } a \not\perp H_i \text{ for all } 1 \leq i \leq n, \\ 2^t - 2\lfloor \frac{n}{2} \rfloor & \text{if } a \perp H_i \text{ for some } 1 \leq i \leq n. \end{cases} \tag{2}$$

Moreover the multiplicity of the second value is $n(2^t - 1)$ and the multiplicity of the first value is $(2^t + 1 - n)(2^t - 1)$. Clearly, f is bent if and only if $n = 2^{t-1} + 1$ or $n = 2^{t-1}$. The partial spread functions with $n = 2^{t-1} + 1$ or $n = 2^{t-1}$ form the classes $\mathcal{PS}^{(+)}$ and $\mathcal{PS}^{(-)}$ respectively [4].

If f is a bent function on $\mathbb{F}_2^m$, then for all $A \in \mathrm{GL}(m, \mathbb{F}_2)$, $a, b \in \mathbb{F}_2^m$ and $c \in \mathbb{F}_2$, the Boolean function $x \mapsto f(xA + a) + b \cdot x + c$ is also bent. The *affine closure* of a set $\mathcal{B}$ of bent functions is the set of bent functions obtained from those in $\mathcal{B}$ through the above transformation.

3. Enumeration of Partial Spread Functions

The general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ is the group of $m \times m$ invertible matrices over $\mathbb{F}_2$. We treat elements of $\mathbb{F}_2^m$ as *row* vectors. Each element of $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ can also be viewed as an invertible linear transformation of $\mathbb{F}_2^m$ defined by $\phi(x) = x\phi$. For $\phi, \psi \in \mathrm{GL}(m, \mathbb{F}_2)$, $\phi\psi$ is the matrix product but $\phi \circ \psi$ is the linear transformation of $\mathbb{F}_2^m$ defined by $(\phi \circ \psi)(x) = \phi(\psi(x)) = x(\psi\phi)$. So $\phi \circ \psi = \psi\phi$. Since $\phi(\psi(x)) = (\psi\phi)(x)$, the action of $\mathrm{GL}(m, \mathbb{F}_2)$ on $\mathbb{F}_2^m$ is a *right* action. For this reason, we denote $\phi(x)$ $(= x\phi)$ by x^ϕ. We will also consider the right action of $\mathrm{GL}(m, \mathbb{F}_2)$ on partial spreads. In that case, the action of $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ is also denoted by $(\ )^\phi$. If $f : \mathbb{F}_2^m \to X$ is a function, where X is any set, and $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$, we define $\phi(f) = f \circ \phi$. Note that for $\phi, \psi \in \mathrm{GL}(m, \mathbb{F}_2)$, $\phi(\psi(f)) = f \circ \psi \circ \phi = f \circ (\phi\psi) = (\phi\psi)(f)$. So the actions of $\mathrm{GL}(m, \mathbb{F}_2)$ on the set of all functions from $\mathbb{F}_2^m$ to X is a *left* action. Therefore we denote $\phi(f)$ by ϕf.

The action of $\mathrm{GL}(m, \mathbb{F}_2)$ on $\mathbb{F}_2^m$ induces a *right* action of $\mathrm{GL}(m, \mathbb{F}_2)$ on the set of n-spreads and a *left* action of $\mathrm{GL}(m, \mathbb{F}_2)$ on the set of n-spread functions. Two partial spreads (partial spread functions) are called *equivalent* if they belong to the same $\mathrm{GL}(m, \mathbb{F}_2)$-orbit. Note that inequivalent partial spreads can give equivalent partial spread functions. For example, we know from [3] that there are 8 inequivalent spreads when $m = 8$.[1] But of course, all these spreads represent the same Boolean function, i.e., the constant function 1.

By a *collection* of n-spread functions, we mean a set of n-spread functions such that any n-spread function is equivalent to at least one in this collection. By a *system of representatives* of n-spread functions, we mean a collection of n-spread functions that are pairwise not equivalent. For each partial spread $\mathcal{P}$ of $\mathbb{F}_2^m$ let $\mathfrak{f}_\mathcal{P}$ denote the corresponding partial spread function. If a partial spread $\mathcal{P}$ contains another partial spread $\mathcal{Q}$, we say that $\mathcal{P}$ is an extension of $\mathcal{Q}$. A partial spread function f is called an extension of another partial spread function g if there exist partial spreads $\mathcal{P} \supset \mathcal{Q}$ such that $f = \mathfrak{f}_\mathcal{P}$ and $g = \mathfrak{f}_\mathcal{Q}$. The following lemma is the base of our approach; it allows us to construct a collection of $(n+1)$-spreads by extending the members of a collection of n-spreads.

Lemma 1. *Let X be a collection of n-spread functions. If g is an $(n+1)$-spread function, then it is equivalent to an extension of some $f \in X$.*

Proof. Write $g = g_1 + 1_H$, where g_1 is an n-spread function and 1_H is the indicator function of some t-dimensional subspace H of $\mathbb{F}_2^m$. There exists $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ such that $\phi g_1 \in X$. Put $f = \phi g_1$. We have $\phi g = f + 1_{H^{\phi^{-1}}}$. Write $f = \mathfrak{f}_\mathcal{P}$ where $\mathcal{P}$ is an n-spread. Since $\mathfrak{f}_\mathcal{P} + 1_{H^{\phi^{-1}}}$ is an $(n+1)$-spread function, it follows that $\mathcal{P} \cup \{H^{\phi^{-1}}\}$ is an $(n+1)$-spread and $\mathfrak{f}_\mathcal{P} + 1_{H^{\phi^{-1}}} = \mathfrak{f}_{\mathcal{P} \cup \{H^{\phi^{-1}}\}}$, which is an extension of $\mathfrak{f}_\mathcal{P}$. Namely, ϕg is an extension of f. □

Using Lemma 1, we can construct a system of representatives of partial spread functions by induction. Starting from a system of representatives X of n-spread functions, we build a system of representatives of $(n+1)$-spreads functions and we compute the corresponding number of partial spread functions in three phases :

(1) *Extension.* In this step, we build a collection of $(n+1)$-spread functions by constructing extensions of elements in X. Classification of 4-spreads

[1] A fact that we verified beside the present numerical experiment.

Table 1. The total running time for the Classification of Partial Spread Functions was 117484 secondes i.e. 33 hours. The column (3) reports the size of the collections generated in the extension phase.The column (6) reports the number of class found after the classification phase. The column (8) the number of partial spread functions.

	extension		classification			stabilization	
n	time	size	time	time	class	time	psf
4	1	5	1	0	3	1	64374841666437120
5	15	233	55	10	22	10	20267057123180937216
6	69	4893	1162	385	341	6	1339989812392369324032
7	415	29691	7038	7246	3726	62	17833337132662061531136
8	1076	60943	14449	33501	9316	229	46056096661467073413120
9	681	31715	7516	8594	5442	19529	24520650576127040978944
10	219	8871	2109	698	1336	23	4731497045822911021056
11	75	2759	654	148	303	6	713809537614313684992
12	20	675	160	30	42	10	38019657690425327616
13	3	96	23	4	6	2	129740065512357888
14	0	11	3	0	1	59	44213490155520
15	0	3	1	0	1	11186	6579388416
16	0	2	0	0	1	NC	200787
17	0	1	0	0	1	NC	1
	2574	139898	33171	50616	20541	31123	

(Proposition 1) and linear algebra techniques similar to those in the proof of Proposition 1 are used to avoid combinatorial explosion.

(2) *Classification*
   - *Splitting.* We use the classification of quartic forms in 8 variables to split the collection of $(n + 1)$-spread functions into several lists such that equivalent $(n + 1)$-spread functions belong to the same list.
   - *Reducing.* We use an equivalence testing algorithm to reduce each list up to equivalence.

(3) *Stabilization.* In this last step, we use an equivalence testing algorithm to determine the order of the stabilizers of the representatives obtained in the previous phase.

The details of the running time of the numerical experiment are reported in the table Tab. (3).

4. Spread Extension

Extension from n-spread functions to $(n + 1)$-spread functions is essentially extension from n-spreads to $(n + 1)$-spreads. The latter is implemented as follows.

For two $t \times t$ matrices A and B over $\mathbb{F}_2$ such that rank $[A\ B] = t$, we let $[A : B]$ denote the row space of $[A\ B]$, i.e., the linear span of the rows of $[A\ B]$. Any n-spread is equivalent to one of the form

$$\{[0 : I],\ [I : 0],\ [I : I],\ [I : A_4],\ \ldots,\ [I : A_n]\}$$

where $A_2(=0), A_3(=I), A_4, \dots, A_n$ have the property that $A_i - A_j$ is invertible for all $2 \le i < j \le n$; see [4, Theorems 5.3.1 and 5.3.2]. Therefore, to extend the above n-spread is to find matrices A_{n+1} such that $A_{n+1} - A_j$ is invertible for all $2 \le j \le n$.

We include a proof of the above fact to familiarize the reader with our notation. Assume that $[B_1 : C_1], \dots, [B_n : C_n]$ is an n-spread where B_i and C_i are $t \times t$ matrices over $\mathbb{F}_2$. Since $\operatorname{rank}[B_1\ C_1] = t$, there exists $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ such that $[B_1 : C_1]^\phi = [0 : I]$. Write $[B_i : C_i]^\phi = [B_i' : C_i']$, $2 \le i \le n$. For $2 \le i \le n$, since $[B_i' : C_i'] \cap [0 : I] = \{0\}$, B_i' must be invertible. Thus $[B_i' : C_i'] = [I : A_i]$ where $A_i = B_i'^{-1} C_i'$. Since $[I : A_i] \cap [I : A_j] = \{0\}$, $2 \le i < j \le n$, $A_i - A_j$ must be invertible. Finally, let $\psi = \left[\begin{smallmatrix} I & -A_1(A_2-A_1)^{-1} \\ 0 & (A_2-A_1)^{-1} \end{smallmatrix}\right] \in \mathrm{GL}(m, \mathbb{F}_2)$. Then $[0 : I]^\psi = [0 : I]$, $[I : A_1]^\psi = [I : 0]$, $[I : A_2]^\psi = [I : I]$. So we may assume $A_2 = 0$ and $A_3 = I$.

All 2-spreads are equivalent to $\{[0 : I],\ [I : 0]\}$ and all 3-spreads are equivalent to $\{[0 : I],\ [I : 0],\ [I : I]\}$. In the remaining part of this section, we show that the equivalence classes of 4-spreads can also be theoretically determined.

5. Classification of 4-Spreads

For any $t \times t$ matrix A over $\mathbb{F}_2$, let $[A]$ denote the conjugacy class of A, i.e., $[A] = \{P^{-1}AP : P \in \mathrm{GL}(t, \mathbb{F}_2)\}$. Let $\mathcal{A}$ be the set of all $t \times t$ matrices having no eigenvalues 0 and 1 and let $\bar{\mathcal{A}} = \{[A] : A \in \mathcal{A}\}$. The symmetric group S_3 (the group of permutations on three letters) acts on $\bar{\mathcal{A}}$ as follows: Write S_3 in the form of presentation

$$S_3 = \langle \alpha, \beta \mid \alpha^2 = \beta^2 = 1,\ \alpha\beta\alpha = \beta\alpha\beta \rangle.$$

Then the action of S_3 on $\bar{\mathcal{A}}$ is defined by

$$\alpha[A] = [A^{-1}] \qquad \text{and} \qquad \beta[A] = [I - A].$$

The S_3-orbit of $[A]$ is

$$\{[A],\ [A^{-1}],\ [I - A],\ [(I - A)^{-1}],\ [I - A^{-1}],\ [I - (I - A)^{-1}]\}.$$

For $A, B \in \mathcal{A}$, we say $A \approx B$ if $[A]$ and $[B]$ are in the same S_3-orbit.

Proposition 1. *Let $B_1, \dots, B_k$ be a system of representatives of the $\approx$ equivalence classes in $\mathcal{A}$. Then*

$$\{[0 : I],\ [I : 0],\ [I : I],\ [I : B_i]\}, \quad 1 \le i \le k, \tag{3}$$

is a system of representatives of the equivalence classes of 4-spreads.

Proof. For each $A \in \mathcal{A}$, let $\mathcal{P}_A = \{[0 : I],\ [I : 0],\ [I : I],\ [I : A]\}$.

1° We first show that if $A, B \in \mathcal{A}$ such that $[A] = [B]$, then $\mathcal{P}_A$ is equivalent to $\mathcal{P}_B$. Assume that there exists $P \in \mathrm{GL}(t, \mathbb{F}_2)$ such that $P^{-1}AP = B$. Let $\sigma = \left[\begin{smallmatrix} P & \\ & P \end{smallmatrix}\right] \in \mathrm{GL}(m, \mathbb{F}_2)$. Then

$$[0 : I]^\sigma = [0 : I],\ [I : 0]^\sigma = [I : 0],\ [I : I]^\sigma = [I : I]$$

and

$$[I : A]^\sigma = [P : AP] = [I : P^{-1}AP] = [I : B].$$

So $\mathcal{P}_A^\sigma = \mathcal{P}_B$.

2° Next, we show that if $A, B \in \mathcal{A}$ such that $A \approx B$, then $\mathcal{P}_A$ is equivalent to $\mathcal{P}_B$. Since S_3 is generated by α and β, we only have to prove that $\mathcal{P}_A$ is equivalent to $\mathcal{P}_B$ under the assumption that $\alpha[A] = [B]$ or $\beta[A] = [B]$.

First assume $\alpha[A]=[B]$. By 1°, we may assume $A=B^{-1}$. Let $\sigma=\left[\begin{smallmatrix} & I\\ I & \end{smallmatrix}\right]\in \mathrm{GL}(m,\mathbb{F}_2)$. (Blocks of 0's in matrix are usually left blank.) Then

$$[0:I]^\sigma=[I:0],\ [I:0]^\sigma=[0:I],\ [I:I]^\sigma=[I:I]$$

and

$$[I:A]^\sigma=[A:I]=[I:A^{-1}]=[I:B].$$

Thus $\mathcal{P}_A^\sigma=\mathcal{P}_B$.

Now assume $\beta[A]=[B]$. By 1°, we may assume $A=I-B$. Let $\sigma=\left[\begin{smallmatrix} & -I\\ A^{-1} & A^{-1}\end{smallmatrix}\right]\in \mathrm{GL}(m,\mathbb{F}_2)$. Then

$$\begin{aligned}
&[0:I]^\sigma=[A^{-1}:A^{-1}]=[I:I],\\
&[I:0]^\sigma=[0:-I]=[0:I],\\
&[I:I]^\sigma=[A^{-1}:A^{-1}-I]=[I:B],\\
&[I:A]^\sigma=[I:0].
\end{aligned}$$

So we also have $\mathcal{P}_A^\sigma=\mathcal{P}_B$.

3° Finally, we show that if $\mathcal{P}_A$ is equivalent to $\mathcal{P}_B$, then $A\approx B$. Let $\sigma\in\mathrm{GL}(m,\mathbb{F}_2)$ such that $\mathcal{P}_A^\sigma=\mathcal{P}_B$. Then σ maps at least two of $[0:I]$, $[I:0]$ and $[I:I]$ to $\{[0:I],\,[I:0],\,[I:I]\}$. This statement comprises a handful of possibilities. Among those possibilities, we only consider two sample cases since the proofs in other cases are identical.

Sample case (i). Assume $[0:I]^\sigma=[I:0]$ and $[I:0]^\sigma=[0:I]$. Then $\sigma=\left[\begin{smallmatrix} & C\\ D & \end{smallmatrix}\right]$. Thus

$$\begin{aligned}
&[I:I]^\sigma=[D:C]=[I:D^{-1}C],\\
&[I:A]^\sigma=[AD:C]=[I:D^{-1}A^{-1}C].
\end{aligned}$$

Therefore

$$\begin{cases} D^{-1}C=I,\\ D^{-1}A^{-1}C=B\end{cases}\tag{4}$$

or

$$\begin{cases} D^{-1}C=B,\\ D^{-1}A^{-1}C=I.\end{cases}\tag{5}$$

If (4) holds, then $B=D^{-1}A^{-1}C=C^{-1}A^{-1}C$. Thus $[B]=[A^{-1}]$, so $A\approx B$. If (5) holds, then $B=D^{-1}C=(A^{-1}C)^{-1}C=C^{-1}AC$. Thus $[B]=[A]$, so $A\approx B$.

Sample case (ii). Assume $[0:I]^\sigma=[I:0]$ and $[I:0]^\sigma=[I:I]$. Then $\sigma=\left[\begin{smallmatrix} E & E\\ F & 0\end{smallmatrix}\right]$. Thus

$$\begin{aligned}
&[I:I]^\sigma=[E+F:E]=[I+E^{-1}F:I],\\
&[I:A]^\sigma=[E+AF:E]=[I+E^{-1}AF:I].
\end{aligned}$$

Therefore

$$\begin{cases} I+E^{-1}F=0,\\ I+E^{-1}AF=B^{-1},\end{cases}\tag{6}$$

or

$$\begin{cases} I+E^{-1}F=B^{-1},\\ I+E^{-1}AF=0.\end{cases}\tag{7}$$

If (6) holds, then

$$A = E(B^{-1} - I)F^{-1} = -F(B^{-1} - I)F^{-1} = F(I - B^{-1})F^{-1}.$$

Thus $[A] = [I - B^{-1}]$, hence $A \approx B$. If (7) holds, then $A = -EF^{-1}$ which is similar (conjugate) to $-F^{-1}E = (I - B^{-1})^{-1}$. Thus $[A] = [(I - B^{-1})^{-1}]$, hence $A \approx B$. □

Note. Proposition 1 still holds with $\mathbb{F}_2$ replaced by an arbitrary field. This is clear from the above proof.

Proposition 1 with $m \leq 6$ is essentially Theorem 5.4.4 of [4]. When $m = 8$, $\bar{\mathcal{A}} = \{[B_1], [B_2], [B_3], [B_4]\}$ where

$$B_1 = \begin{bmatrix} & 1 & & \\ 1 & 1 & & \\ & & & 1 \\ & & 1 & 1 \end{bmatrix}, \quad B_2 = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & 1 & & \end{bmatrix}, \quad B_3 = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad B_4 = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & & & 1 \end{bmatrix}.$$

(The lists of elementary divisors of $B_1, \ldots, B_4$ are $\{x^2+x+1, x^2+x+1\}$, $\{x^4+x+1\}$, $\{x^4 + x^3 + x^2 + x + 1\}$, $\{x^4 + x^3 + 1\}$, respectively.) It is easy to check that B_1, B_2, B_3 are pairwise not $\approx$-equivalent. However, $[B_4] = [B_2^{-1}]$, so $B_4 \approx B_2$. Therefore, we know from Proposition 1 that there are 3 equivalence classes of 4-spreads represented by $\mathcal{P}_{B_i}$, $1 \leq i \leq 3$.

6. Equivalence and classification

For the two last phases, we need an algorithm to test GL-equivalence of Boolean functions. The algorithm we used is described in this section, alternative choices are [13, 15, 6].

We first describe a naïve algorithm `equiv` for testing the equivalence of two mappings from $\mathbb{F}_2^m$ to X, where X is any finite set; the algorithm is based on the notions of *good basis* and *candidates*.

Let f and g be two mappings from $\mathbb{F}_2^m$ to X. They are said to be *equivalent* if there exists $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ such that $g = f \circ \phi$.

If f and g are equivalent then they have the same value distribution. For a value v of f, let $\nu(v)$ denote its multiplicity. We say that a basis $(b_1, b_2, \ldots, b_m)$ of $\mathbb{F}_2^m$ is a *good basis* relatively to f if it minimizes the quantity $\prod_{i=1}^m \nu(f(b_i))$.

Assume that a good basis $(b_1, \ldots, b_m)$ of $\mathbb{F}_2^m$ relative to f has been chosen. For each i, we determine the ith set of *candidates*:

$$C_i = \{x \in \mathbb{F}_2^m : g(x) = f(b_i)\}.$$

Note that if $|C_i| \neq \nu(f(b_i))$ for some i, then we already know that g is not equivalent to f. If $|C_i| = \nu(f(b_i))$ for all $1 \leq i \leq m$, we search for $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ by choosing $\phi(b_i) \in C_i$. The total number of candidates for ϕ is $\prod_{i=1}^m |C_i|$. This is the reason we start with a good basis relative to f.

Let

$$B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

where $(b_1, \ldots, b_m)$ is a good basis relative to f. The algorithm `equiv` searches for $A \in \mathrm{GL}(m, \mathbb{F}_2)$ such $f(vB) = g(vA)$ for all $v \in \mathbb{F}_2^m$ until all candidates are exhausted or a survivor is found. vA is represented by *img* and vB by *src*. The algorithm is recursive. At the entrance of `equiv`(i, size), it is true that $f(vB) =$

$g(vA)$ for all binary vectors v representing integers $< size$. The procedure chooses the ith row of A from the candidates in C_i. The symbol $\oplus$ denotes the addition in $\mathbb{F}_2^m$. Implementing vectors as m-bits integers, $\oplus$ is the bitwise xor, and the ith canonical vector e_i is 2^{i-1}. Function $\texttt{rank}(A, i)$ is the rank of the first i rows of A.

The algorithm can also be modified to compute the size of the stabilizer in $\mathrm{GL}(m, \mathbb{F}_2)$ of a mapping $f : \mathbb{F}_2^m \to X$. Recall that the stabilizer of f is defined to be $\{\phi \in \mathrm{GL}(m, \mathbb{F}_2) : \phi(f) = f\}$ and that $|\mathrm{GL}(m, \mathbb{F}_2)|$ divided by cardinality of the stabilizer f gives the size of the equivalence class containing f.

The algorithm equiv

```
$A$ : table of $m$ vector // matrix
$B$ : table of $m$ vector // good basis
$C$ : candidates
$src$, $img$ : table of $2^m$ vectors // source, image

algorithm equiv ($i$ : integer; $size$ : integer)
begin
  if ( $i > m$ ) then exit fi;
  forall $c$ in $C_i$ do
    $A[i] := c$;
      if ( $\texttt{rank}(A, i) = i$ ) then
        $x := 0$; $y := 0$;
        $j := 0$;
        repeat
          $y := A[i] \oplus img[j]$;
          $x := B[i] \oplus src[j]$;
          $img[j \oplus e_i] := y$;
          $src[j \oplus e_i] := x$;
          $j := j + 1$;
        while ( ( $j < size$ ) and ( $f[x] = g[y]$ ) );
        if ( $j = size$ ) then
        equiv ($i + 1, 2 * size$);
        fi;
      fi;
    done;
  end
```

We now turn to the testing of equivalence of Boolean functions. Due to the fact that a Boolean function takes only two values, the algorithm `equiv` is not efficient for checking the equivalence between two Boolean functions. It is easy to see that two Boolean functions f and g are equivalent if and only if their Walsh transforms are equivalent. Thus the algorithm `equiv` can be applied to Walsh transforms of Boolean functions. However, this is still not efficient for determining equivalence between bent functions since the Walsh transforms of bent functions take only two values. In what follows, we propose a procedure to test equivalence of Boolean functions which is suitable for the purpose of this paper.

Let f be a Boolean function. The *derivative* of f in the direction of $u \in \mathbb{F}_2^m$, is the Boolean function $\mathrm{Der}_u f$ defined by $\mathrm{Der}_u f(x) = f(x + u) + f(x)$. We construct a mapping f^* from $\mathbb{F}_2^m$ to $\mathbb{Z}^{2^m}$ sending u to the Walsh spectrum of $\mathrm{Der}_u f$.

Note. The Walsh spectrum of a Boolean function f is the set of values of the Walsh transform of f counting multiplicities. For the computational purpose, the Walsh spectrum of a Boolean function is simply a sequence of 2^m integers in the increasing order.

Lemma 2. *Let f and g be two Boolean functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. If f and g are equivalent then f^* and g^* are equivalent.*

Proof. Let $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ such that $g = f \circ \phi$.

$$\mathrm{Der}_u g(x) = g(x+u) + g(x) = f(x^\phi + u^\phi) + f(x^\phi) = (\mathrm{Der}_{u^\phi} f)\big(x^\phi\big).$$

Hence the Walsh spectrum of $\mathrm{Der}_u g$ is equal to the Walsh spectrum of $\mathrm{Der}_{u^\phi} f$, so $g^* = f^* \circ \phi$. □

Therefore, we can use the following procedure to check the equivalence between two Boolean functions f and g.

A PROCEDURE TO DETERMINE EQUIVALENCE OF BOOLEAN FUNCTIONS

1. Compute the mappings f^* and g^*.
2. If the value distributions of f^* and g^* differ then f and g are not equivalent.
3. Apply the algorithm `equiv` to enumerate the linear transformations ϕ mapping f^* to g^*.
4. If some ϕ from step 3 maps f to g then the Boolean functions are equivalent. If no ϕ from step 3 maps f to g then the Boolean functions are not equivalent.

When testing equivalence of partial spread functions in 8 variables, in addition to the above procedure, we also make use of the classification of quartic forms in 8 variables [10]. A Boolean function f has a unique reduced polynomial representation

$$f = \sum_{S \subset \{1,2,\ldots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2, \tag{8}$$

where X_S denotes the monomial $\prod_{i \in S} X_i$. The degree of this polynomial, denoted by $\deg f$, is called the *degree* of the Boolean function f. Note that the degree of the indicator function of a t-dimensional subspace is equal to $m - t = t$. Thus a partial spread function has degree less or equal to t. Two Boolean functions f and g of degree $\leq t$ are said to be *weakly equivalent* if there exists $\phi \in \mathrm{GL}(m, \mathbb{F}_2)$ such that

$$f \circ \phi = g + \text{a Boolean function of degree less than } t.$$

When $t = 4$, this weak equivalence corresponds to the equivalence of *quartic forms* in 8 variables under the action of $\mathrm{GL}(8, \mathbb{F}_2)$. We know there are 999 equivalence classes of quartic forms in 8 variables [7]. Efficient invariants for quartic forms in 8 are described in [10]. Those invariants can be used to split a collection of spread functions in up to 966 lists; see [10] for the details. Finally we apply the above procedure to each list to obtain a system of representatives.

Table 2. Numbers of equivalence classes of partial spread functions in 8 variables of order n ($2 \le n \le 17$)

n	nb of classes	n	nb of classes
2	1	10	1336
3	1	11	303
4	3	12	42
5	22	13	6
6	341	14	1
7	3726	15	1
8	9316	16	1
9	5442	17	1

Table 3. Distribution of the sizes of stabilizers of 8-spread functions ($\mathcal{P}S^{(-)}$ functions) in 8 variables

nb of classes	stab size	nb of classes	stab size	nb of classes	stab size
8149	1	2	21	1	120
743	2	8	24	1	180
144	3	2	30	1	192
79	4	7	36	1	288
102	6	6	48	1	480
5	7	1	56	1	576
12	8	1	60	1	1152
4	9	1	64	1	1296
30	12	1	72	1	1344
1	16	2	96	1	1290240
6	18				

Note. The cardinality of $\mathcal{P}S^{(-)}$ is 46056096661467073413120 $\approx 2^{75.29}$.

7. Computational Results and Observations

Our computational results are summarized in Tables 1 – 3. Table 1 gives the numbers of equivalence classes of n-spread functions in 8 variables for all possible orders. Table 2 enumerates the numbers of equivalence classes of 8-spread functions (i.e., the $\mathcal{PS}^{(-)}$ bent functions) in 8 variables according the sizes of stabilizers of these functions. Table 3 gives the same information for 9-spread functions (i.e., the $\mathcal{PS}^{(+)}$ bent functions) in 8 variables.

The computational results on partial spread functions in 8 variables allow us to observe some interesting phenomena.

Observation 1. Up to equivalence, there are only two partial spread functions in 8 variables of degree less than 4. They both belong to the $\mathcal{PS}^{(+)}$ class; one has degree 2 and a stabilizer of cardinality 348364800; the other has degree 3 and a stabilizer of cardinality 1008. The uniqueness of the quadratic partial spread function is easy to understand. In fact, let f be an n-spread function on $\mathbb{F}_2^m$ which is quadratic. Then the Walsh transform $f^{\mathcal{W}}(a)$ ($a \neq 0$) takes values $4\lfloor \frac{n}{2} \rfloor$ or $-2^{t+1} + 4\lfloor \frac{n}{2} \rfloor$; see (1) and

Table 4. Distribution of the sizes of stabilizers of 9-spread functions ($\mathcal{PS}^{(+)}$ functions) in 8 variables

nb of classes	stab size	nb of classes	stab size	nb of classes	stab size
4063	1	2	30	1	192
797	2	6	32	1	288
198	3	6	36	3	384
108	4	1	42	1	480
130	6	6	48	1	576
21	8	1	56	1	1008
4	9	1	60	1	1152
38	12	4	64	1	1296
11	16	3	72	1	18432
8	18	4	96	1	86016
2	21	1	120	1	348364800
13	24	1	180		

Note. The cardinality of $\mathcal{PS}^{(+)}$ is $24520650576127040978944 \approx 2^{74.38}$.

(2). On the other hand, since f is quadratic, $f^{\mathcal{W}}$ takes values $\pm 2^{m-\frac{k}{2}}$, where k is the quadratic rank of f. So we must have $n = 2^{t-1}$ or $2^{t-1}+1$ and $k = m$, i.e., f must be a $\mathcal{PS}$ and quadratic bent function. It is known that all $\mathcal{PS}^{(-)}$ bent functions have degree t (Remark 6.3.11 of [4]). So $f \in \mathcal{PS}^{(+)}$. Thus $|f^{-1}(1)| = 2^{m-1} + 2^{t-1}$ and $f(0) = 1$. Up to GL-equivalence, $x_1x_2 + x_3x_4 + \cdots + x_{2t-1}x_{2t} + 1$ is the only quadratic function having these properties. By Theorem 6.3.12 of [4], this quadratic function indeed belongs to $\mathcal{PS}^{(+)}$.

The uniqueness of the cubic partial spread function in 8 variables is yet to be explained.

Observation 2. The number of bent functions in 8 variables in the $\mathcal{PS}$ ($= \mathcal{PS}^{(+)} \cup \mathcal{PS}^{(-)}$) class is $70576747237594114392064 \approx 2^{75.9}$. Applying the affine translations to this set, we get at most $2^{83.9}$ bent functions in the affine closure of the set of $\mathcal{PS}$ bent functions, up to affine terms. On the other hand, the number of bent functions in 8 variables up to affine terms is about $2^{97.29}$ as computed in [11]. The portion of $\mathcal{PS}$ bent functions in 8 variables among all bent functions in 8 variables is at most $2^{83.9-97.29} = 2^{-13.39}$ which is very small. We also mention that according to [11], there are at most about 2^{72} in the affine closure of the set of Maiorana-McFarland bent functions in 8 variables (up to affine terms) which also represent a very small position of all bent functions in 8 variables. These comparisons suggest the possible existence of new classes of bent functions in 8 variables (and in more than 8 variables).

Observation 3. Let $K = \mathbb{F}_{2^t}$ and let $L = \mathbb{F}_{2^m}$. There are $2^t + 1$ K-lines in L which form a spread in L. Let $\alpha \in K^*$ be an element of order $2^t + 1$. The K-lines in L are precisely $\alpha^i K$, $0 \le i \le 2^t$. Let l_i denote the indicator function of $\alpha^i K$ in L. The sum of any 2^{t-1} of l_i's is called a $\mathcal{PS}_{\text{ap}}$ bent function, so the family of

$\mathcal{PS}_{\rm ap}$ functions is

$$\mathcal{PS}_{\rm ap} = \Big\{ \sum_{i \in I} l_i : I \subset \{0, \dots, 2^t\},\ |I| = 2^{t-1} \Big\} \subset \mathcal{PS}^{(-)};$$

see [4]. Note that $\mathcal{PS}_{\rm ap}$ functions are invariant under the action by K^* through multiplication. Also note that if $f \in \mathcal{PS}_{\rm ap}$, then $f + 1 \in \mathcal{PS}^{(+)}$ and $f + 1$ has the same stabilizer as f. Therfore, in the case $m = 8$, the size of the stabilizer of a $\mathcal{PS}_{\rm ap}$ bent function must be a multiple of $|K^*| = 15$ and must also appear as the size of the stabilizer of some $\mathcal{PS}^{(+)}$ bent function. According to Tables 2 and 3, among 9316 classes of $\mathcal{PS}^{(-)}$ bent functions, there are 6 classes whose stabilizer sizes have these properties; the stabilizer sizes are 30 (2 times), 60, 120, 180 and 480. On the other hand, the number of elements in $\mathcal{PS}_{\rm ap}$ is small ($\binom{17}{8} = 24310$) and it is an easy task to generate all these functions to check their equivalence with the representatives from the 6 classes. The computation shows that all the 6 classes contain $\mathcal{PS}_{\rm ap}$ bent function. Hence up to GL-equivalence there are exactly 6 classes of $\mathcal{PS}_{\rm ap}$ bent functions in 8 variables.

References

[1] C. Carlet. On the secondary constructions of resilient and bent functions. In *Coding, Cryptography and Combinatorics*, Progr. Comput. Sci. Appl. Logic, 23, pages 3–28, Birkhäuser, Basel, 2004.

[2] C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Comput. Sci., volume 3857, pages 1–28, Springer, Berlin, 2006.

[3] U. Dempwolff and A. Reifart. The classification of the translation planes of order 16. I. *Geom. Dedicata*, 15(2):137–153, 1983.

[4] J. F. Dillon. *Elementary Hadamard Difference Sets.* PhD Thesis, University of Maryland, 1974.

[5] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, P. Gaborit. Construction of bent functions via Niho power functions. *J. Combin. Theory Ser. A*, 113:779–798, 2006.

[6] J. Fuller, W. Millan. Linear Redundancy in S-Boxes. FSE 2003: 74-86

[7] X. Hou. GL$(m, 2)$ acting on R(r, m)/R$(r-1, m)$. *Discrete Mathematics*, 149:99–122, 1996.

[8] X. Hou and P. Langevin. Results on bent functions. *J. Combin. Theory Ser. A*, 80:232–246, 1997.

[9] P. Langevin. Numerical Projects Website, 2008.
http://langevin.univ-tln.fr/project/spread/psp.html

[10] P. Langevin and G. Leander. Classification of boolean quartic forms in eight variables. In *Boolean Functions in Cryptology and Information Security*, volume 18, pages 139–147, 2008.

[11] P. Langevin and G. Leander. Number of bent functions in 8 variables. *Preproceedings WCC 2009*, 2009.

[12] P. Langevin, P. Rabizzoni, P. Véron, J-P. Zanotti. On the number of bent functions with 8 variables. In *BFCA'06*, pages 125–135, Rouen, France, 2006.

[13] G. Leander. *Normality of Bent Functions Monomial- and Binomial-Bent Functions.* PhD Thesis, Ruhr University Bochum, Germany, 2004.

[14] O. S. Rothaus. On "bent" functions. *J. Combin. Theory Ser. A*, 20:300–305, 1976.

[15] M. Serwecinski. A linear equivalence algorithm, *Tatra Mt. Math. Publ*, 37:113122, 2007.

Imath, université du sud Toulon Var, 83957 La Garde Cedex, France
E-mail address: langevin@univ-tln.fr

Department of Mathematics, University of South Florida, Tampa, FL 33620
E-mail address: xhou@math.usf.edu