Some classification results on Maiorana-McFarland bent functions

Philippe Langevin[1] and Alexandr Polujan[2]

[1] Imath, Université de Toulon, La Garde, France
philippe.langevin@univ-tln.fr

[2] Otto-von-Guericke-Universität, Magdeburg, Germany
alexandr.polujan@gmail.com

Abstract

Langevin and Leander [1] computed the exact number of Boolean bent functions in $n = 8$ variables, which is $\approx 2^{106}$. In [1, 2], it was estimated that the number of bent functions equivalent to Maiorana-McFarland $\mathcal{M}$ and Partial Spread $\mathcal{PS}$ classes in dimension eight (up to addition of affine terms) is at most $\approx 2^{72}$ and $\approx 2^{76}$, respectively. While the classification of the $\mathcal{PS}$ class in the case $n = 8$ was achieved by Langevin and Hou [2], a similar result for the $\mathcal{M}$ class has been still missing. In this paper, we close this gap by providing the classification of Maiorana-McFarland bent functions in dimension eight. Based on this result, we provide the exact number of bent functions equivalent to the $\mathcal{M}$ class in eight variables (up to addition of affine terms), and discuss some theoretical questions related to the classification of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$.

Keywords: Bent function, Maiorana-McFarland class, Equivalence, General affine group.

1 Preliminaries

Let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2 = \{0, 1\}$. A mapping $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function*. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. Every Boolean function has a unique multivariate representation, called the *algebraic normal form (ANF)* :

$$f(x_1, x_2, \ldots, x_n) = f(x) = \sum_{S \subseteq \{1,2,\ldots,n\}} a_S X_S, \quad a_S \in \mathbb{F}_2, \quad X_S = \prod_{s \in S} x_s.$$

The *degree* of f is the maximal cardinality of S with $a_S = 1$ in its ANF. The *valuation* of $f \neq 0$, denoted by $\mathrm{val}(f)$, is the minimal cardinality of S for which $a_S = 1$. Conventionally, $\mathrm{val}(0)$ is ∞. We denote by $B(s, t, n) = \{f \in \mathcal{B}_n\colon \mathrm{val}(f) \geq s \text{ and } \deg(f) \leq t\}$ the space of Boolean functions of valuation greater than or equal to s and of degree less than or equal to t. The space $B(0, t, n)$ is identified with the *Reed-Muller code* $RM(t, n)$.

For $a \in \mathbb{F}_2^n$, the *Walsh transform* $\hat{\chi}_f\colon \mathbb{F}_2^n \to \mathbb{Z}$ of a Boolean function $f \in \mathcal{B}_n$ is defined by $\hat{\chi}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x\rangle_n}$, where $\langle a, x\rangle_n = a_1x_1 + \cdots + a_nx_n$ is a scalar product on $\mathbb{F}_2^n$. We define the *Walsh spectrum* of $f \in \mathcal{B}_n$ as the multiset $WS(f) = \{* \ |\hat{\chi}_f(a)|\colon a \in \mathbb{F}_2^n \ *\}$. We say that two Boolean functions $f, f' \in \mathcal{B}_n$ are *extended-affine equivalent (EA-equivalent)*, if $f'(x) = f(A(x)) + a(x)$ holds for all $x \in \mathbb{F}_2^n$, where $A \in \mathrm{AGL}(n, 2)$ and a is an *affine* Boolean function on $\mathbb{F}_2^n$, i.e., $\deg(a) \leq 1$.

Definition 1. *Let $n = 2m$ be even. A Boolean function $f \in \mathcal{B}_n$ is called* bent *if its Walsh transform satisfies $\hat{\chi}_f(a) = \pm 2^m$, for all $a \in \mathbb{F}_2^n$.*

The *Maiorana-McFarland class* [3] of Boolean bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ is the set of bent functions of the form

$$\mathcal{M} = \{f_{\pi,g}(x,y) = \langle x, \pi(y)\rangle_m + g(y) \colon \pi \text{ is a permutation of } \mathbb{F}_2^m,\ g \in \mathcal{B}_m\}. \quad (1)$$

The main aim of this paper is to classify the members of the $\mathcal{M}$ class for the case of $n = 2m = 8$ variables. As we shall see later, this question is closely related to the classification of permutations of $\mathbb{F}_2^m$ and, consequently, to the representatives of $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double cosets in permutation group $S(\mathbb{F}_2^m)$ of $\mathbb{F}_2^m$, see [4].

2 Methodology

For $n = 2m \leq 6$, the members of $\mathcal{M}$ can be classified directly, since its cardinality $|\mathcal{M}| = (2^m)! \cdot 2^{2^m}$ is relatively small and checking equivalence of Boolean functions in these dimensions is very fast. However, already for $m = 4$, the number of permutations of $\mathbb{F}_2^m$ becomes already too large for such a naive approach. As we explain further, to classify the members of $\mathcal{M}$, it is enough to look at very special Maiorana-McFarland bent functions $f_{\pi,g}$, where the selection of π and g is explained by the double action of $\mathrm{AGL}(m,2) \times \mathrm{AGL}(m,2)$ on the group of permutations of $\mathbb{F}_2^m$.

In the remaining part of the paper, we explain the main four steps of our approach that helped to achieve the classification of the $\mathcal{M}$ class in $n = 2m = 8$ variables. They include: I. Complexity reduction using the group theory, II. Preclassification, III. Classification, IV. Description of the used invariants that uniquely label the obtained equivalence classes. The supporting data for our findings can be found on the web-page [5].

2.1 Complexity reduction using the group theory

We begin with some notation from group theory, which mainly follows the terminology from [4]. Let

$$\mathrm{AGL}(m,2) = \left\{ \begin{bmatrix} A & b \\ & 1 \end{bmatrix} : A \in \mathrm{GL}(m,2), b \in \mathbb{F}_2^m \right\}$$

be the *general affine group*. The action of $\mathrm{AGL}(m,2)$ on $\mathbb{F}_2^m$ is given by

$$\begin{bmatrix} A & b \\ & 1 \end{bmatrix}(x) = Ax + b \quad \text{for } x \in \mathbb{F}_2^m.$$

Let $S(\mathbb{F}_2^m)$ be the group of all permutations of $\mathbb{F}_2^m$. The product of $\mathrm{AGL}(m,2)$ by its opposite $\mathrm{AGL}(m,2)^{\mathrm{op}}$ acts naturally on $S(\mathbb{F}_2^m)$ by composition. The action of $(L,R) \in \mathrm{AGL}(m,2) \times \mathrm{AGL}(m,2)^{\mathrm{op}}$ on $\sigma \in S(\mathbb{F}_2^m)$, is $L \circ \sigma \circ R$. The orbits of this action are precisely the $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-*double cosets* in $S(\mathbb{F}_2^m)$. The *number of* $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-*double cosets in* $S(\mathbb{F}_2^m)$ is denoted by $\mathfrak{N}(m,2)$. This value can be computed with the Burnside lemma, for details, we refer to [4].

A pair $(L,R) \in \mathrm{AGL}(m,2) \times \mathrm{AGL}(m,2)^{\mathrm{op}}$ stabilizes a permutation $\pi \in S(\mathbb{F}_2^m)$ if and only if $L \circ \pi \circ R = \pi$. In this context, we define :

$$\mathrm{stab}(\pi) := \{R \in \mathrm{AGL}(m,2) \mid \pi \circ R \circ \pi^{-1} \in \mathrm{AGL}(m,2)\}.$$

If (L,R) stabilizes π then $R \in \mathrm{stab}(\pi)$. Conversely, for each $R \in \mathrm{stab}(\pi)$ there exists one and only one $L \in \mathrm{AGL}(m,2)$ such that (L,R) stabilizes π. With this definition, in order to determine $\mathrm{stab}(\pi)$, one enumerates $R \in \mathrm{AGL}(m,2)$ s.t. $\pi \circ R \circ \pi^{-1} \in S(\mathbb{F}_2^m)$ is affine. Note that the mapping ϕ on $\mathbb{F}_2^m$ is affine if and only if for all $(x,y,z,w) \in (\mathbb{F}_2^m)^4$ with $x+y+z+w = 0$ holds $\phi(x) + \phi(y) + \phi(z) + \phi(w) = 0$.

For an arbitrary permutation π of $\mathbb{F}_2^m$, and for an arbitrary Boolean function $g \in \mathcal{B}_m$, consider the action of (A, R) with $A \in GL(m, 2)$ and $R \in \mathrm{AGL}(m, 2)$ on the Maiorana-McFarland bent function $f_{\pi,g}(x, y) = \langle x, \pi(y)\rangle_m + g(y)$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$, where $\pi \in S(\mathbb{F}_2^m)$ and $g \in \mathcal{B}_m$:

$$\begin{aligned} f_{\pi,g}(x, y) \circ (A, R) =& \langle A(x), \pi(R(y))\rangle_m + g(R(y)) \\ =& \langle x, A^* \circ \pi \circ R(y)\rangle_m + g(R(y)), \end{aligned} \tag{2}$$

where A^* is the adjoint of A. Note that we can also add to $f_{\pi,g}(x, y)$ any linear function $\langle x, v\rangle_m$ without changing the EA-class :

$$f_{\pi,g}(x, y) \equiv \langle x, L \circ \pi \circ R(y)\rangle_m + g(R(y)) = f_{\pi',g'}(x, y), \tag{3}$$

where $\pi' := L \circ \pi \circ R$, $g' := g \circ R$, L is the composition of A^* by the translation $x \mapsto x + v$, for $v \in \mathbb{F}_2^m$. This computation indicates that in order to classify the elements of $\mathcal{M}$, it is enough to look at Maiorana-McFarland bent functions $f_{\pi',g'}$, where π' runs through the representatives of the $(\mathrm{AGL}(m, 2), \mathrm{AGL}(m, 2))$-*double cosets* in $S\left(\mathbb{F}_2^m\right)$ and g' runs through the orbit determined by the action of $\mathrm{stab}(\pi')$ on the set of Boolean functions $B(2, m, m)$.

2.2 Preclassification

In this section, we briefly describe how to obtain the representatives of double cosets and the orbits of their action the set of Boolean functions of valuation at least 2 in 4 variables.

Constructing the representatives of the $(\mathrm{AGL}(4, 2), \mathrm{AGL}(4, 2))$-double cosets in $S\left(\mathbb{F}_2^4\right)$. Here, we follow the methodology of Hou developed in [4]. For $m = 4$, to find representatives of $(\mathrm{AGL}(m, 2), \mathrm{AGL}(m, 2))$-double cosets in $S(\mathbb{F}_2^m)$, it is enough to find $\mathfrak{N}(4, 2) = 302$ pairwise inequivalent permutations. To do so, one can use the fact that for $\sigma, \tau \in S\left(\mathbb{F}_2^4\right), \sigma \sim \tau$ if and only if $\sigma\rho\tau^{-1} \in \mathrm{AGL}(4, 2)$ for some $\rho \in \mathrm{AGL}(4, 2)$. With this approach, we obtained the representatives π_i (where i ranges from 1 to 302) of the $(\mathrm{AGL}(4, 2), \mathrm{AGL}(4, 2))$-double cosets in $S\left(\mathbb{F}_2^4\right)$; they can be found in [5]. Alternative representatives (obtained with a different approach) can be also found in [6].

Computing the action of $\mathrm{stab}(\pi_i)$ on the space $B(2, 4, 4)$ and constructing the orbit representatives. For each permutation π_i, we compute the action of $\mathrm{stab}(\pi_i)$ on the space $B(2, 2, 4)$. The obtained orbit representatives $g \in O(\mathrm{stab}(\pi_i), B(2, 2, 4))$ are listed in the ANF format, see [5]. For $m = 4$, we were able to reduce the number of functions to check for equivalence as described by the following diagram.

$$\begin{array}{rcl} (2^m)! \cdot (2^{2^m - m - 1}) & \longrightarrow & \displaystyle\sum_{i=1}^{\mathfrak{N}(m,2)} |O(\mathrm{stab}(\pi_i), B(2, 2, m))| \\ 1\,371\,091\,344\,150\,528\,000 & \longrightarrow & 417\,914 \end{array}$$

2.3 Classification

We use the standard design-coding-theoretic approach for checking equivalence of Boolean bent functions, see [7, Section 2.2]. Using the described methodology, we classify the obtained 417 914 Maiorana-McFarland bent functions in the following two steps:

1. For a fixed permutation π_i with $1 \leq i \leq 302$, classify Maiorana-McFarland bent functions $f_{\pi_i,g}$, where $g \in O(\mathrm{stab}(\pi_i), B(2,2,4))$. Such a splitting of all the functions to check in 302 small collections helps the classification routine to assign quickly the right "preclass"and not spend a lot of time on showing that two functions are inequivalent. In this way, we were able to reduce the considered collection to 335 "preclasses".

2. For the obtained preclasses $f_{\pi_i,g}$ and $f_{\pi'_i,g'}$, we are checking the mutual equivalence with the same design-coding-theoretic approach. In total, out of 335 "preclasses" we obtained 325 equivalence classes.

2.4 Invariants

In order to guarantee the correctness of the obtained equivalence classes, it is always important to find the set of invariants that uniquely label the obtained representatives of equivalence classes. Even for the obtained 325 equivalence classes, this task was not trivial to achieve: the dimension is large enough and the functions to be distinguished apriori have a lot of similarities, since all of them belong to the same algebraic class $\mathcal{M}$. After trying most of the known invariants, we were able to show that the following triple $(J_4(f_{\pi,g}), M(f_{\pi,g}), K(f_{\pi,g}))$ uniquely labels the representatives $f_{\pi,g}$ of equivalence classes of Maiorana-McFarland bent functions. Here, the invariants $J_4(\cdot)$, $M(\cdot)$ and $K(\cdot)$ are defined as follows:

1. $J_k(f) = \{*WS(f+g)\colon g \text{ is a quadratic homogeneous function of rank } k\ *\}$. This invariant is a generalization of the invariant $\Theta(f)$, considered in [7].

2. $M(f)$ is a multiplicative version of J_2: Given f of degree 4, we consider the distribution of the absolute value of the Walsh spectra of gf modulo $RM(5,8)$, where g ranges the set of quadratic homogeneous functions of rank 2.

3. $K(f)$ is the dimension of the kernel of the map from $RM(2,8)$ into $B(4,6,8)$ that maps $g \mapsto gf \mod RM(3,8)$.

According to our computations, the invariant $J_k(f)$ takes 313 different values on 325 equivalence classes of Maiorana-McFarland bent functions. The remaining 12 collisions were further uniquely labeled by $M(f)$, $K(f)$ and their dual. The proof that $J_k(f)$ is an invariant under EA-equivalence is similar to $\Theta(\cdot)$ presented in [7], $M(f)$ is a multiplicative variant of $J_2(f)$ and $K(f)$ is a variant of the multiplicative invariant $\mathfrak{R}_{2,4}$ that could be found in [8].

3 Main results

In this section, we summarize the results in this paper. We begin with our main computational result:

Theorem 1. *Let $\mathcal{CM}(2m,2)$ denote the number of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8,2) = 325$.*

Proof. This follows from the computations above presented in Section 2. □

Based on this result, we derive the number of Maiorana-McFarland bent functions in 8 variables, up to addition of affine terms.

Theorem 2. *For $m = 4$, the number of bent functions equivalent to the $\mathcal{M}$ class (up to addition of affine terms) is equal to*

$$537\,611\,571\,837\,677\,338\,624 \approx 2^{68,86}. \tag{4}$$

Proof. Since the representatives of equivalence classes are known, one can compute the orders of stabilizers of the representatives and use them to compute the desired number using the orbit-stabilizer theorem. For $m = 4$, we get the value

$$\sum_{f_{\pi,g}} \frac{|\operatorname{AGL}(2m,2)|}{|\operatorname{stab}(f_{\pi,g})|} = \frac{2^{2m}\prod_{k=0}^{2m-1}\left(2^{2m}-2^k\right)}{\sum_{f_{\pi,g}}|\operatorname{stab}(f_{\pi,g})|} = \frac{1\,369\,104\,324\,918\,194\,995\,200}{12\,130\,107\,857\,920},$$

which is exactly the one in (4). □

Remark 1. *1. This result is in line with the upper bound on the number of bent functions equivalent to the $\mathcal{M}$ class (up to addition of affine terms), which as estimated in [1], is at most $2^{72,38}$.*
2. Using the same counting argument, we confirm the enumeration of bent functions in dimension 6 that was obtained by Preneel in [11, Table 8.7] with a different approach.

Finally, we note that equivalence of permutations π and ϕ implies the equivalence of the corresponding Maiorana-McFarland bent functions $f_{\pi,0}$ and $f_{\phi,0}$:

Theorem 3. *Let $\pi, \phi \in S(\mathbb{F}_2^m)$. If $\pi \sim \phi$, then Maiorana-McFarland bent functions $f_{\pi,0}$ and $f_{\phi,0}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are equivalent.*

Proof. This fact follows from Eqs. (2) and (3). □

4 Conclusion and open problems

In this paper, we classified and enumerated all Maiorana-McFarland bent functions in eight variables. In the following table, we summarize the known values of $\mathcal{CM}(2m,2)$ and $\mathfrak{N}(m,2)$ for the small values of m. Note that the first row of this table is taken from [9] and that the value of $\mathfrak{N}(5,2)$ given in [4] is wrong; the correct value is given in [9]. The second row of the table below is composed from the values obtained in [10] and this paper.

Table 1. The known values of $\mathcal{CM}(2m,2)$ and $\mathfrak{N}(m,2)$, for m small

m	1	2	3	4	5
$\mathfrak{N}(m,2)$	1	1	4	302	2 569 966 041 123 963 092
$\mathcal{CM}(2m,2)$	1	1	4	325	$\geq \mathfrak{N}(5,2)$?

Combining our theoretical results from Theorem 3 and computational results given in Table 1, it is natural to conjecture:

Conjecture 1. *If Maiorana-McFarland bent functions $f_{\pi,0}$ and $f_{\phi,0}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are equivalent, then $\pi \sim \phi$.*

Proving this conjecture is the first important step towards understanding when two given Maiorana-McFarland bent functions are equivalent. Additionally, the answer to the classification problem of "simple" Maiorana-McFarland bent functions will provide a good lower bound on the number of inequivalent Maiorana-McFarland bent functions.

Acknowledgments

Philippe Langevin is partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012.

References

[1] Langevin, P., Leander, G.: Counting all bent functions in dimension eight 99270589265934370305785861242880. Designs, Codes and Cryptography **59**(1), 193–205 (2011). doi: https://doi.org/10.1007/s10623-010-9455-z pp. 1 and 5.

[2] Langevin, P., Hou, X.D.: Counting partial spread functions in eight variables. IEEE Transactions on Information Theory **57**, 2263–2269 (2011). doi: https://doi.org/10.1109/tit.2011.2112230 p. 1.

[3] McFarland, R.L.: A family of difference sets in non-cyclic groups. Journal of Combinatorial Theory, Series A **15**(1), 1–10 (1973). doi: https://doi.org/10.1016/0097-3165(73)90031-9 p. 2.

[4] Hou, X.D.: Affinity of permutations of $\mathbb{F}_2^n$. Discrete Applied Mathematics **154**(2), 313 – 325 (2006). doi: https://doi.org/10.1016/j.dam.2005.03.022 pp. 2, 3, and 5.

[5] Langevin, P.: Double coset of AGL(4) \ S(16)/AGL(4). URL `https://langevin.univ-tln.fr/project/permut/permut.html` pp. 2 and 3.

[6] Cannière, C.D.: Analysis and design of symmetric encryption algorithms. Ph.D. thesis, Katholieke Universiteit Leuven (2007). URL `http://image.sciencenet.cn/olddata/kexue.com.cn/upload/blog/file/2009/3/20093320521938772.pdf` p. 3.

[7] Polujan, A., Pott, A.: Towards the classification of quadratic vectorial bent functions in 8 variables. In: The 7th international workshop on Boolean functions and their applications (2022). URL `https://boolean.w.uib.no/bfa-2022/` pp. 3 and 4.

[8] Langevin, P., Leander, G.: Classification of boolean quartic forms in eight variables. In: Boolean Functions in Cryptology and Information Security, vol. 18, pp. 139–147 (2008). doi: https://doi.org/10.3233/978-1-58603-878-6-139 p. 4.

[9] Sloane, N.J.A.: OEIS — Invertible Boolean functions with AG$(n, 2)$ acting on the domain and range. URL `https://oeis.org/A001537` p. 5.

[10] Dillon, J.F.: A survey of bent functions. NSA Technical Journal **Special Issue**, 191–215 (1972). URL `https://cryptome.org/2015/11/nsa-survey-of-bent-functions.pdf` p. 5.

[11] Preneel, B.: Analysis and design of cryptographic hash functions. Ph.D. thesis, Katholieke Universiteit Leuven (1993). URL `https://www.esat.kuleuven.be/cosic/publications/thesis-2.pdf` p. 5.