

Results on Constructions of Rotation Symmetric Bent and Semi-bent Functions

Claude Carlet¹, Guangpu Gao^{2,3(✉)}, and Wenfen Liu^{2,3}

¹ LAGA (UMR 7539), University of Paris 8 and University of Paris 13, CNRS,
2 Rue de la Liberté, 93526 Saint-Denis, Cedex, France

`claude.carlet@univ-paris8.fr`

² State Key Laboratory of Mathematical Engineering and Advanced Computing,
Zhengzhou, China

`guangpu.gao@gmail.com`

³ State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing, China

Abstract. In this paper, we introduce a class of cubic rotation symmetric (RotS) functions and prove that it can yield bent and semi-bent functions. To the best of our knowledge, this is the second primary construction of an infinite class of nonquadratic RotS bent functions which could be found and the first class of nonquadratic RotS semi-bent functions. We also study a class of idempotents (giving RotS functions through the choice of a normal basis of $GF(2^n)$ over $GF(2)$). We derive a characterization of the bent functions among these idempotents and we relate their precise determination to a problem studied in the framework of APN functions. Incidentally, the proofs of bentness given here are useful for a paper studying a construction of idempotents from RotS functions, entitled “A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions” by the same authors, to appear in the journal JCT series A.

Keywords: Rotation symmetric Boolean function · Bent · Semi-bent · Maiorana-McFarland class · Idempotent · Permutation

1 Introduction

Boolean functions play a critical role in cryptography as well as in the design of circuits and chips for digital computers. They can be defined over the finite field $GF(2^n)$ and represented as univariate polynomials, or over the vector space $GF(2)^n$ and represented as $f(x_0, x_1, \dots, x_{n-1})$, the latter representation being deduced from the former (and vice versa) through the choice of a basis of the

The work of G. Gao, and W. Liu is supported in part by 973 Program under Grant No. 2012CB315905 and Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications)(SKLNST-2013-1-06).

$GF(2)$ -vector space $GF(2^n)$. Idempotents, introduced by Filiol and Fontaine in [12, 13] are polynomials over $GF(2^n)$ such that $f(z) = f(z^2)$, for all $z \in GF(2^n)$. Rotation symmetric (RotS) Boolean functions, introduced by Pieprzyk and Qu [24], are invariant under circular translation of indices. They can be obtained from idempotents (and vice versa) through the choice of a normal basis of $GF(2^n)$. Such class of Boolean functions is of interest because of its smaller search space ($\approx 2^{\frac{2^n}{n}}$) comparably to the whole space ($= 2^{2^n}$), which allows investigating functions for a number of variables larger (by a factor of 2), and also because of the more compact representation of RotS functions. It has been experimentally demonstrated that the class of RotS Boolean functions is extremely rich in terms of cryptographically significant Boolean functions. For example, Kavut *et al.* have found Boolean functions on 9 variables with nonlinearity 241 [17], which solved an almost three-decade old open problem. Motivated by this study, important cryptographic properties such as nonlinearity, balancedness, correlation immunity, algebraic degree and algebraic immunity of these functions have been investigated at the same time and encouraging results have been obtained [10, 14, 27, 28]. Note that RotS functions are also interesting for the design of Substitution Boxes in block ciphers (see [16, 25]).

Plateaued functions [29] represent much interest for the study of Boolean functions in cryptography, as they can possess desirable cryptographic properties such as high nonlinearity, resiliency, propagation criteria, low additive autocorrelation and high algebraic degree. Their class is larger than that of “partially bent functions” introduced in [3]. Two important classes of plateaued functions are those of bent functions and of semi-bent functions, due to their algebraic and combinatorial properties. An n -variable (n even) bent function is a Boolean function with the maximum possible nonlinearity $2^{n-1} - 2^{n/2-1}$. Such functions provide the best resistance against attacks by affine approximations, such as the fast correlation cryptanalysis (but are weak against other attacks like the Siegenthaler correlation attack and the fast algebraic attack). They have been extensively investigated in cryptography (Rothaus who introduced them in [26] worked in this framework), spread spectrum, coding theory (the Kerdock codes are made of affine functions and bent functions) and combinatorial design (in relation with difference sets). A lot of research has been devoted to designing constructions of bent functions. The two best known constructions produce the so-called Maiorana-McFarland class, denoted by \mathcal{M} [11, 21] and the \mathcal{PS} class [11]. A survey on bent functions can be found in [2].

It is well known that the Walsh transform of a bent function only takes on the values $\pm 2^{\frac{n}{2}}$. Hence, bent functions are unbalanced and exist only for even number of variables. For even n , a semi-bent function has Walsh transform taking values 0 and $\pm 2^{\frac{n}{2}+1}$ only; it can also be called 3-valued almost optimal. Semi-bent functions can provide protection against fast correlation attack and more general cryptanalysis by affine approximation [22], and unlike bent functions can also be balanced and resilient. A number of constructions of semi-bent functions have been developed. For detailed discussion please see [5, 9, 23] and the references therein.

In [15], the authors presented a class of cubic RotS bent functions. But such examples of bent RotS functions are very few. Further research is needed to find other classes of cryptographically important RotS functions. In [6], the authors studied the following transformation of RotS functions into idempotents: given, $f(x_0, x_1, \dots, x_{n-1})$ a RotS function over $GF(2)^n$, the function f' is defined over $GF(2^n)$ as: $f'(z) = f(z, z^2, \dots, z^{2^{n-1}})$. If the ANF of f is $f(x_0, x_1, \dots, x_{n-1}) = \sum_{u \in GF(2)^n} a_u x^u$, where x_0, x_1, \dots, x_{n-1} and a_u belong to $GF(2)$, we have: $f'(z) = \sum_{u \in GF(2)^n} a_u \prod_{i=0}^{n-1} (z^{2^i})^{u_i} = \sum_{u \in GF(2)^n} a_u z^{\sum_{i=0}^{n-1} u_i 2^i}$. The transformation $f \mapsto f'$ maps any RotS Boolean function f to a Boolean idempotent f' over $GF(2^n)$. The algebraic degree is preserved. All Boolean idempotents are obtained this way, with uniqueness. This transformation, contrary to the decomposition of an idempotent over a normal basis, allows obtaining infinite classes from infinite classes. The question whether such infinite classes exist for all situations “ f bent / not bent” and “ f' bent / not bent” is studied in [6]. The proofs given in the present paper allow to reply positively.

We organize this paper as follows. Section 2 is an introductory part providing some preliminary definitions and results. In Sect. 3, we characterize the Walsh transform of a class of cubic RotS functions f_t . Necessary and sufficient conditions for f_t to be bent or semi-bent functions are obtained. Section 4 presents a class of idempotent bent functions.

2 Preliminaries

We first recall some general definitions about Boolean functions. Denote by $GF(2)^n$ the n -dimensional vector space over the finite field $GF(2)$ and by $+$ the addition operation over $GF(2)$. Let $\mathbf{0}$ and $\mathbf{1}$ be the all-zero vector and the all-one vector of $GF(2)^n$ respectively. An n -variable Boolean function $f(x)$, where $x = (x_0, x_1, \dots, x_{n-1}) \in GF(2)^n$, is a mapping from $GF(2)^n$ to $GF(2)$, which can be represented uniquely as a polynomial, called its algebraic normal form (ANF), of the form:

$$f(x_0, x_1, \dots, x_{n-1}) = \sum_{u \in GF(2)^n} \lambda_u \left(\prod_{i=0}^{n-1} x_i^{u_i} \right), \quad \lambda_u \in GF(2).$$

The number of variables in the highest order product term with nonzero coefficient is called its *algebraic degree*. A Boolean function is said to be *affine* if its degree does not exceed 1. The set of all n -variable affine functions is denoted by $A_n(x)$. We call a function nonlinear if it is not in $A_n(x)$. The *Hamming weight* $w_H(x)$ of a binary vector $x \in GF(2)^n$ is the number of its nonzero coordinates, and the Hamming weight $w_H(f)$ of a Boolean function f is the size of its support $\{x \in GF(2)^n | f(x) = 1\}$. If $w_H(f) = 2^{n-1}$, we call $f(x)$ *balanced*. We say two n -variable Boolean functions $f(x)$ and $g(x)$ are *affinely equivalent* if $g(x) = f(Ax + b)$ where b is an element of $GF(2)^n$ and A is an $n \times n$ nonsingular binary matrix. It is easy to see that if $f(x)$ and $g(x)$ are affinely equivalent then

$w_H(f) = w_H(g)$. Let $x = (x_0, x_1, \dots, x_{n-1})$ and $w = (w_0, w_1, \dots, w_{n-1})$ both belong to $GF(2)^n$ and $w \cdot x$ be an inner product in $GF(2)^n$, for instance the usual inner product $w_0x_0 + w_1x_1 + \dots + w_{n-1}x_{n-1}$. Then the Walsh transform of $f(x)$ is the real valued function over $GF(2)^n$ defined as: $W_f(w) = \sum_{x \in GF(2)^n} (-1)^{f(x)+w \cdot x}$.

Definition 1. Let n be even. A Boolean function $f(x)$ on $GF(2)^n$ is called bent if its Walsh transform satisfies $W_f(w) = \pm 2^{\frac{n}{2}}$, for all $w \in GF(2)^n$.

Definition 2. Let n be any positive integer. A Boolean function $f(x)$ on $GF(2)^n$ is called semi-bent if its Walsh transform satisfies $W_f(w) = 0, \pm 2^{\lceil \frac{n+1}{2} \rceil}$, for all $w \in GF(2)^n$.

Maiorana and McFarland [21] introduced independently a class of bent functions by concatenating affine functions. We call the Maiorana-McFarland class \mathcal{M} the set of all the Boolean functions on $GF(2)^{2m} = \{(x, y) \mid x, y \in GF(2)^m\}$, of the form:

$$f(x, y) = \pi(x) \cdot y + h(x), \tag{1}$$

where π is any mapping from $GF(2)^m$ to $GF(2)^m$ and $h(x)$ is any Boolean function on $GF(2)^m$. Then f is bent if and only if π is bijective.

Let $x_i \in GF(2)$ for $0 \leq i \leq n - 1$. For $0 \leq k \leq n - 1$, we define the left k -cyclic shift operator ρ_n^k as $\rho_n^k(x_i) = x_{(i+k) \bmod n}$ (this is an abuse of notation since $x_{(i+k) \bmod n}$ does not depend on x_i but on another coordinate of x ; but this notation will simplify the presentation below). Let $(x_0, x_1, \dots, x_{n-1}) \in GF(2)^n$, we can extend the definition of ρ_n^k on tuples as follows: $\rho_n^k(x_0, x_1, \dots, x_{n-1}) = (\rho_n^k(x_0), \rho_n^k(x_1), \dots, \rho_n^k(x_{n-1}))$, and on monomials as follows: $\rho_n^k(x_{i_0}x_{i_1} \dots x_{i_l}) = \rho_n^k(x_{i_0})\rho_n^k(x_{i_1}) \dots \rho_n^k(x_{i_l})$ with $0 \leq i_0 < i_1 < \dots < i_l \leq n - 1$.

Definition 3. A Boolean function f on $GF(2)^n$ is called rotation symmetric if for each input $(x_0, x_1, \dots, x_{n-1}) \in GF(2)^n$, we have:

$$f(\rho_n^k(x_0, x_1, \dots, x_{n-1})) = f(x_0, x_1, \dots, x_{n-1}), \quad \text{for } 0 \leq k \leq n - 1.$$

Let us denote by $G_n(x_{i_0}x_{i_1} \dots x_{i_l}) = \{\rho_n^k(x_{i_0}x_{i_1} \dots x_{i_l}), \text{ for } 0 \leq k \leq n - 1\}$ the orbit of the monomial $x_{i_0}x_{i_1} \dots x_{i_l}$. We select the representative element of $G_n(x_{i_0}x_{i_1} \dots x_{i_l})$ as the lexicographically first element. For instance, the representative element of the orbit $\{x_0x_1x_2, x_1x_2x_3, x_2x_3x_0, x_3x_0x_1\}$ is $x_0x_1x_2$. For a RotS function f , the existence of a representative term $x_0x_{i_1} \dots x_{i_l}$ implies the existence of all the terms from $G_n(x_0x_{i_1} \dots x_{i_l})$ in the ANF of f .

3 Constructions of Rotation Symmetric Bent and Semi-bent Functions

The lemma below is straightforward and well-known.

Lemma 1. Assume that a Boolean function $f : GF(2)^{2m} \rightarrow GF(2)$ can be expressed in the form (1). Then the following conditions hold.

1. If π is a 2-to-1 mapping, then f is a semi-bent function.
2. If, for every $b \in GF(2)^m$, the set $S_b = \{x \in GF(2)^m | \pi(x) = b\}$ is either empty or an s -dimensional affine subspace of $GF(2)^m$, then f is semi-bent if and only if $s = 1$, or $s = 2$ and the restriction of h to S_b , viewed as a 2-variable function, has algebraic degree 2 (i.e. has odd Hamming weight).

Now, we are able to prove our main theorem.

Theorem 1. Let $f_t(x)$ be the n -variable RotS Boolean function of the form:

$$f_t(x) = \sum_{i=0}^{n-1} \rho_n^i(x_0 x_r x_{2r}) + \sum_{i=0}^{2r-1} \rho_n^i(x_0 x_{2r} x_{4r}) + \sum_{i=0}^{\nu(t)-1} \rho_n^i(x_0 x_t) \quad (2)$$

where ρ_n^i is the left i -cyclic shift operator, and $n = 2m = 6r$ with $r \geq 1$, $t \leq m$, $\nu(t) = n$ if $0 < t < m$; $\nu(t) = m$ if $t = m$. Then we have

1. If $0 < t < m$, then $f_t(x)$ is semi-bent if and only if $\gcd(2t, m) = 1$ or if $\gcd(2t, m) = 2$ and $\gcd(t, m) = 1$.
2. If $t = m$, then $f_t(x)$ is a bent function.

Proof. We first note that

$$\begin{aligned} f_t(x) = & (x_0 + x_{3r})(x_r + x_{4r})(x_{2r} + x_{5r}) \\ & + (x_1 + x_{3r+1})(x_{r+1} + x_{4r+1})(x_{2r+1} + x_{5r+1}) \\ & \vdots \\ & + (x_{r-1} + x_{4r-1})(x_{2r-1} + x_{5r-1})(x_{3r-1} + x_{6r-1}) + \sum_{i=0}^{\nu(t)-1} \rho_n^i(x_0 x_t). \end{aligned}$$

Let

$$E = \{x \in GF(2)^n | x_i + x_{m+i} = 0, \forall i = 0, \dots, m-1\}$$

and

$$W = \{x \in GF(2)^n | x_{m+i} = 0, \forall i = 0, \dots, m-1\},$$

then E and W are two supplementary m -dimensional vector subspaces of $GF(2)^n$, that is, any vector $x \in GF(2)^n$ can then be uniquely represented as $x = a + y$ with $a \in W$ and $y \in E$. By replacing x by $a + y$ above, we deduce that:

1. If $0 < t < m$, then

$$\begin{aligned} f_t(x) = f_t(a + y) = & a_0 a_r a_{2r} + a_1 a_{r+1} a_{2r+1} + \dots + a_{r-1} a_{2r-1} a_{3r-1} \\ & + \sum_{i=0}^{n-1} \rho_n^i(a_0 + y_0)(a_t + y_t) \\ = & \sum_{i=0}^{r-1} \rho_m^i(a_0 a_r a_{2r}) + \sum_{i=0}^{n-1} \rho_n^i(a_0 a_t + a_0 y_t + a_t y_0 + y_0 y_t). \end{aligned}$$

Using $a_{m+i} = 0$ and $y_i = y_{m+i}$ for $0 \leq i \leq m-1$, we have:

$$\begin{aligned} \sum_{i=0}^{n-1} \rho_n^i(a_0 a_t) &= \sum_{i=0}^{m-t-1} \rho_n^i(a_0 a_t) \\ &= \sum_{i=0}^{m-t-1} \rho_m^i(a_0 a_t) \text{ (this is an abuse of notation),} \\ \sum_{i=0}^{n-1} \rho_n^i(a_0 y_t) &= a_0 y_t + \cdots + a_{m-t-1} y_{m-1} + a_{m-t} y_0 + \cdots + a_{m-1} y_{t-1} \\ &= \sum_{i=0}^{m-1} \rho_m^i(a_0 y_t) = \sum_{i=0}^{m-1} \rho_m^i(a_{m-t} y_0), \\ \sum_{i=0}^{n-1} \rho_n^i(a_t y_0) &= \sum_{i=0}^{n-1} \rho_n^i(a_0 y_{n-t}) = \sum_{i=0}^{m-1} \rho_m^i(a_0 y_{m-t}) = \sum_{i=0}^{m-1} \rho_m^i(a_t y_0). \end{aligned}$$

Therefore, since $\sum_{i=0}^{n-1} \rho_n^i(y_0 y_t) = 2 \sum_{i=0}^{m-1} \rho_n^i(y_0 y_t) \pmod{2} = 0$:

$$\begin{aligned} f_t(x) &= f_t(a + y) \\ &= \sum_{i=0}^{r-1} \rho_m^i(a_0 a_r a_{2r}) + \sum_{i=0}^{m-t-1} \rho_m^i(a_0 a_t) + \sum_{i=0}^{m-1} \rho_m^i((a_t + a_{m-t}) y_0) \\ &= \pi(a) \cdot y + h(a), \end{aligned}$$

where

$$\pi(a) = (a_t + a_{m-t}, a_{t+1} + a_{m-t+1}, \dots, a_{t-1} + a_{m-t-1}),$$

and

$$h(a) = \sum_{i=0}^{r-1} \rho_m^i(a_0 a_r a_{2r}) + \sum_{i=0}^{m-t-1} \rho_m^i(a_0 a_t).$$

If $t = m/2$, then $\pi = 0$ and the function is neither semi-bent nor bent. For $t \neq m/2$, according to the expression obtained for $\pi(a)$, we can assume without loss of generality that $0 < t < m/2$. Let $s = \gcd(2t, m)$. It follows from Theorem 1 of [20, p. 190] that π is a 2^s -to-1 mapping since $\gcd(x^t + x^{m-t}, x^m + 1) = x^s + 1$. This is equivalent to saying that S_w is either an empty set or an s -dimensional affine subspace of $GF(2)^m$. By Case 2 of Lemma 1, we deduce that f_t can be semi-bent only if $s = 1$, or $s = 2$.

- If $s = 1$, then π is a 2-to-1 mapping, which implies f_t is semi-bent by Case 1 of Lemma 1.
- If $s = 2$, denote by G the kernel of π , then

$$G = \{0, \mathbf{1}, (1, 0, 1, 0, \dots, 1, 0), (0, 1, 0, 1, \dots, 0, 1)\} \subset GF(2)^m.$$

Suppose that S_w is nonempty. Then, for any $a \in S_w$, there exists some vector $b \in GF(2)^m$ such that $\{b + e | e \in G\}$ (b can be unique if we require for instance that $b_0 = b_1 = 0$). Then the restriction g of h to S_w is:

$$\begin{aligned} g &= \sum_{i=0}^{r-1} \rho_m^i((b_0 + e_0)(b_r + e_r)(b_{2r} + e_{2r}) + \sum_{i=0}^{m-t-1} \rho_m^i((b_0 + e_0)(b_t + e_t)) \\ &= \sum_{i=0}^{r-1} \rho_m^i(b_0 b_r b_{2r} + b_0 b_r e_{2r} + b_0 b_{2r} e_r + b_r b_{2r} e_0 \\ &\quad + b_0 e_r e_{2r} + b_r e_0 e_{2r} + b_{2r} e_0 e_r + e_0 e_r e_{2r}) \\ &\quad + \sum_{i=0}^{m-t-1} \rho_m^i(b_0 b_t + b_0 e_t + b_t e_0 + e_0 e_t). \end{aligned}$$

Since $\gcd(2t, m) = 2$, then $\gcd(t, m) = 1, 2$ and r is even. Using $e_i = e_j$ if $i \equiv j \pmod{2}$, we shall calculate the non-linearized part B of g relative to e for the cases $\gcd(t, m) = 1$ and $\gcd(t, m) = 2$ respectively.

- If $\gcd(t, m) = 2$, then t is even. We have

$$\begin{aligned} B &= \sum_{i=0}^{r-1} \rho_m^i(e_0 e_r e_{2r} + b_0 e_r e_{2r} + b_r e_0 e_{2r} + b_{2r} e_0 e_r) + \sum_{i=0}^{m-t-1} \rho_m^i(e_0 e_t) \\ &= \sum_{i=0}^{r-1} \rho_m^i(e_0 e_0 e_0 + b_0 e_0 e_0 + b_r e_0 e_0 + b_{2r} e_0 e_0) + \sum_{i=0}^{m-t-1} \rho_m^i(e_0 e_0) \\ &= \sum_{i=0}^{r/2-1} ((1 + b_{2i} + b_{r+2i} + b_{2r+2i})e_0 \\ &\quad + (1 + b_{2i+1} + b_{r+2i+1} + b_{2r+2i+1})e_1) \\ &\quad + (\frac{m-t}{2} \pmod{2})(e_0 + e_1). \end{aligned}$$

It shows that g is an affine function on $b + G$. According to Case 2 of Lemma 1, f_t can not be semi-bent if $\gcd(t, m) = 2$.

To complete our proof, it will suffice to check that g is quadratic when $\gcd(t, m) = 1$. In this case, t is odd and so is $m - t$.

- If $\gcd(t, m) = 1$, then

$$\begin{aligned} B &= \sum_{i=0}^{r-1} \rho_m^i(e_0 e_r e_{2r} + b_0 e_r e_{2r} + b_0 e_r e_{2r} + b_r e_0 e_{2r} + b_{2r} e_0 e_r) \\ &\quad + \sum_{i=0}^{m-t-1} \rho_m^i(e_0 e_t) \\ &= \sum_{i=0}^{r/2-1} ((1 + b_{2i} + b_{r+2i} + b_{2r+2i})e_0 \end{aligned}$$

$$\begin{aligned}
& +(1 + b_{2i+1} + b_{r+2i+1} + b_{2r+2i+1})e_1) \\
& +(m - t \bmod 2)(e_0e_1) \\
= & e_0e_1 + \sum_{i=0}^{r/2-1} ((1 + b_{2i} + b_{r+2i} + b_{2r+2i})e_0 \\
& +(1 + b_{2i+1} + b_{r+2i+1} + b_{2r+2i+1})e_1).
\end{aligned}$$

Hence g has algebraic degree 2. We conclude that $f_t(x)$ is semi-bent if $\gcd(2t, m) = 2$ and $\gcd(t, m) = 1$, completing the proof of Case 1 of Theorem 1.

2. If $t = m$, by a straightforward computation, we have

$$\begin{aligned}
f_m(x) &= f_m(a + y) \\
&= \sum_{i=0}^{r-1} \rho_m^i(a_0a_r a_{2r}) + \sum_{i=0}^{m-1} \rho_m^i((a_0 + y_0)(a_m + y_m)) \\
&= \sum_{i=0}^{r-1} \rho_m^i(a_0a_r a_{2r}) + \sum_{i=0}^{m-1} \rho_m^i((a_0 + y_0)a_m + (a_0 + y_0)y_m) \\
&= \sum_{i=0}^{r-1} \rho_m^i(a_0a_r a_{2r}) + \sum_{i=0}^{m-1} \rho_m^i((a_0 + y_0)y_m) \\
&= \sum_{i=0}^{r-1} \rho_m^i(a_0a_r a_{2r}) + \sum_{i=0}^{m-1} \rho_m^i((a_0 + y_0)y_0) \\
&= \sum_{i=0}^{r-1} \rho_m^i(a_0a_r a_{2r}) + \sum_{i=0}^{m-1} \rho_m^i((a_0 + 1)y_0)
\end{aligned}$$

Obviously, $f_m(x)$ is a bent function from the class \mathcal{M} , completing the proof.

Remark 1. From the proof of Theorem 2, one can claim that the homogenous RotS function $\sum_{i=0}^{n-1} \rho_n^i(x_0x_r x_{2r}) + \sum_{i=0}^{2r-1} \rho_n^i(x_0x_{2r}x_{4r})$ can not be bent. It is conjectured that there are no homogenous RotS bent functions [27].

4 Rotation Symmetric Functions Obtained as Idempotents over $GF(2^n)$

In this section we identify the vector space $GF(2)^n$ with the finite field $GF(2^n)$. For any positive integer k dividing n , we denote the trace function from $GF(2^n)$ to $GF(2^k)$ by $Tr_k^n(z) = z + z^{2^k} + \dots + z^{2^{n-k}}$. Note that for every integer k dividing n , the trace function Tr_k^n satisfies the transitivity property $Tr_1^n = Tr_1^k \circ Tr_k^n$. Every nonzero Boolean function f defined over $GF(2^n)$ has a unique representation of the form: $f(z) = \sum_{i=0}^{2^n-1} u_i z^i$ where $u_i \in GF(2^n)$. Thanks to the fact that

f is Boolean, that is, satisfies $(f(z))^2 = f(z) \pmod{z^{2^n} + z}$, it can be written in the form (called its univariate polynomial form or trace form):

$$f(z) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j z^j) + \varepsilon(1 + z^{2^n - 1}), \tag{3}$$

where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$ (the most usual choice for j is the smallest element in its cyclotomic class, called the coset leader of the class), $o(j)$ is the size of the corresponding cyclotomic coset containing j , $a_j \in GF(2^{o(j)})$ and $\varepsilon \in GF(2)$. The algebraic degree of f equals the maximum 2-weight of those j such that $a_j \neq 0$, where the 2-weight of j is the Hamming weight of its binary expansion (see e.g. [2]). Let us denote by $\varphi_u(z) = Tr_1^n(uz)$, $u \in GF(2^n)$, the general linear Boolean function on $GF(2^n)$. The Walsh transform of f is defined as

$$W_f(u) = \sum_{z \in GF(2^n)} (-1)^{f(z) + Tr_1^n(uz)}, \quad u \in GF(2^n).$$

Thanks to the identification between the vectors space $GF(2)^n$ and the field $GF(2^n)$, the Maiorana-McFarland class \mathcal{M} of Boolean functions over $GF(2^{2m})$ can be expressed in the form: $f(x, y) = Tr_1^m(\pi(x)y + h(x))$, where π and h are mappings from $GF(2^m)$ to $GF(2^m)$. A function $f(z)$ given by (3) is an idempotent if and only if every coefficient a_j in every term $Tr_1^{o(j)}(a_j z^j)$ belongs to $GF(2)$.

4.1 The Bentness of Some Cubic Idempotents

It is known that the monomial function $Tr_1^{2m}(\lambda x^d)$, when cubic, can yield bent functions in \mathcal{M} only if $m = 3r, d = 1 + 2^r + 2^{2r}$ [1], or $d = 1 + 2^j + 2^m$ with $1 \leq j < m$ [8] respectively. But [1, Theorem 3] and [8, Theorem 5.1] imply that such cubic bent monomial functions can not be idempotent (i.e. such that $\lambda = 1$). In this subsection, we characterize the bentness of the idempotent functions of the form:

$$f_k^{(c)}(z) = Tr_1^n(z^{1+2^k+2^m}) + \sum_{i=1}^{m-1} c_i Tr_1^n(z^{1+2^i}) + c_m Tr_1^m(z^{1+2^m}), \tag{4}$$

where $n = 2m, 0 < k < m$, and $c = (c_1, \dots, c_m) \in GF(2)^m$.

The next theorem will show that function $f_k^{(c)}(z)$ is from the class \mathcal{M} , and then the bentness of $f_k^{(c)}(z)$ can be related to the bijectivity of some quadratic polynomial of the form $z^{1+2^k} + L(z)$, where $L(z)$ is a linearized polynomial over $GF(2^m)$. Such polynomials have received attention for their importance in constructing quadratic APN permutations [19].

Theorem 2. *Let $f_k^{(c)}(z)$ be defined over $GF(2^n)$ by relation (4) and let $L(z) = z^{2^{k-1}} + c_m z + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i + c_{m-i})(z^{2^i} + z^{2^{m-i}})$. Then $f_k^{(c)}(z)$ is bent if and only if $z^{1+2^k} + L(z)$ is a permutation polynomial of $GF(2^m)$.*

Proof. Let $V = GF(2^m)$ and denote by U a subspace supplementary to V in the vector space $GF(2^n)$. We have $GF(2^n) = \bigcup_{u \in U} (u + V)$. Then, for any $u \in U$ and $y \in V$, we have

$$\begin{aligned}
f_k^{(c)}(z) &= f_k^{(c)}(u + y) \\
&= Tr_1^n((u + y)^{1+2^k+2^m}) + \sum_{i=1}^{m-1} c_i Tr_1^n((u + y)^{1+2^i}) \\
&\quad + c_m Tr_1^m((u + y)^{1+2^m}) \\
&= Tr_1^n(u^{1+2^k+2^m}) + Tr_1^n(u^{2^m} y^{1+2^k} + u y^{2^k+2^m} + u^{2^k} y^{1+2^m}) \\
&\quad + Tr_1^n(u^{1+2^m} y^{2^k} + u^{2^k+2^m} y + u^{1+2^k} y^{2^m}) + Tr_1^n(y^{1+2^k+2^m}) \\
&\quad + \sum_{i=1}^{m-1} c_i Tr_1^n(u^{1+2^i} + u y^{2^i} + u^{2^i} y + y^{1+2^i}) \\
&\quad + c_m Tr_1^m(u^{2^m+1} + u^{2^m} y + u y^{2^m} + y^{2^m+1}).
\end{aligned} \tag{5}$$

Since $u^{1+2^m}, u + u^{2^m}, y \in GF(2^m)$, we have:

$$Tr_1^n(u^{2^m} y^{1+2^k} + u y^{2^k+2^m}) = Tr_1^n((u + u^{2^m}) y^{1+2^k}) = 0,$$

and

$$Tr_1^n(y^{1+2^i}) = Tr_1^n(y^{1+2^k+2^m}) = Tr_1^n(u^{1+2^m} y^{2^k}) = 0.$$

By using the transitivity of the trace function, the part depending on y is

$$\begin{aligned}
A &= Tr_1^n(u^{2^k} y^{1+2^m} + u^{2^k+2^m} y + u^{1+2^k} y^{2^m}) + \sum_{i=1}^{m-1} c_i Tr_1^n(u y^{2^i} + u^{2^i} y) \\
&\quad + c_m Tr_1^m(u^{2^m} y + u y^{2^m} + y^{2^m+1}) \\
&= Tr_1^n(u^{2^{k-1}} y + u^{2^k} (u + u^{2^m}) y) + \sum_{i=1}^{m-1} c_i Tr_1^n((u^{2^{n-i}} + u^{2^i}) y) \\
&\quad + c_m Tr_1^m((u^{2^m} + u + 1) y) \\
&= Tr_1^m(((u + u^{2^m})^{2^{k-1}} + (u + u^{2^m})^{2^k+1}) y) \\
&\quad + \sum_{i=1}^{m-1} c_i Tr_1^m(((u + u^{2^m})^{2^i} + (u + u^{2^m})^{2^{m-i}}) y) + c_m Tr_1^m((u + u^{2^m} + 1) y) \\
&= Tr_1^m(\pi(u) y),
\end{aligned}$$

where

$$\begin{aligned}
\pi(u) &= (u + u^{2^m})^{2^{k-1}} + (u + u^{2^m})^{2^k+1} + \sum_{i=1}^{m-1} c_i ((u + u^{2^m})^{2^i} + (u + u^{2^m})^{2^{m-i}}) \\
&\quad + c_m (u + u^{2^m} + 1).
\end{aligned}$$

Let

$$h(u) = Tr_1^m(u^{2^m+1}(u + u^{2^m})^{2^k}) + \sum_{i=1}^{m-1} c_i Tr_1^n(u^{2^i+1}) + c_m Tr_1^m(u^{2^m+1}).$$

Then the sum in Relation (5) is simplified as follows:

$$f_k^{(c)}(u + y) = Tr y_1^m(\pi(u)y) + h(u).$$

Denoting $u + u^{2^m}$ by ξ , we have:

$$\begin{aligned} \pi(u) &= \xi^{2^k+1} + \xi^{2^{k-1}} + c_m \xi + \sum_{i=0}^{m-1} c_i (\xi^{2^i} + \xi^{2^{m-i}}) + c_m \\ &= \xi^{2^k+1} + \xi^{2^{k-1}} + c_m \xi + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i + c_{m-i})(\xi^{2^i} + \xi^{2^{m-i}}) + c_m \\ &= \xi^{2^k+1} + L(\xi) + c_m. \end{aligned} \tag{7}$$

This completes the proof.

Reference [19] addresses the problem of the bijectivity of functions of the form $z^{2^k+1} + L(z)$. But it does not address completely the case where k is not co-prime with m :

Lemma 2. [19] *Let $\gcd(d, 2^m - 1) > 1$ and $L(z)$ be a linearized polynomial on $GF(2^m)$. Then if $L(z)$ is not a permutation on $GF(2^m)$, then $z^d + L(z)$ is not a permutation. If $d = 1 + 2^k$ with $\gcd(k, m) = 1$, then $z^{1+2^k} + L(z)$ is a permutation polynomial if and only if m is odd and $L(z) = \alpha^{2^i} z + \alpha z^{2^i}$ for some $\alpha \in GF(2^m)^*$.*

Proposition 1. *Let $\pi(z)$ be given by (7). Then the following statements hold:*

1. $\pi(z)$ is a permutation only if $c_m = 1$ and $m/\gcd(m, k)$ is odd.
2. If $k = 1$, then π is a permutation only if $c_i + c_{m-i} = 0$ for all $i = 1 \dots \lfloor \frac{m-1}{2} \rfloor$.

Proof. 1. If $c_m = 0$, then $\pi(z)$ can not be a permutation for $\pi(0) = \pi(1)$. Now we can assume that $c_m = 1$. Then $L(z)$ can not be a permutation on $GF(2^m)$ since $L(0) = L(1)$. And, if $m/\gcd(m, k)$ is even, then $\gcd(2^k + 1, 2^m - 1) > 1$. Hence $\pi(z)$ is not a permutation by Lemma 2.

2. From the conclusions above, we can suppose that $c_m = 1$. If $k = 1$, then $\pi(z) = z^3 + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i + c_{m-i})(z^{2^i} + z^{2^{m-i}}) + 1$. By Lemma 2, π can not be bijective if there exists some $1 \leq i \leq \lfloor \frac{m-1}{2} \rfloor$ such that $c_i + c_{m-i} \neq 0$. This closed the proof.

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.: A new class of monomial bent functions. *Finite Fields Appl.* **14**(1), 221–241 (2008)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Carlet, C.: Partially-bent functions. *Des. Codes Cryptogr.* **3**, 135–145 (1993)
4. Carlet, C., Mesnager, S.: On Dillon’s class \mathcal{H} of bent functions Niho bent functions and o-polynomials. *J. Combin. Theory Ser. A* **118**(8), 2392–2410 (2011)
5. Carlet, C., Mesnager, S.: On semi-bent Boolean functions. *IEEE Trans. Inform. Theory* **58**, 3287–3292 (2012)
6. Carlet, C., Gao, G., Liu, W.: A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. *J. Combin. Theory Ser. A* **127**, 161–175 (2014)
7. Charpin, P., Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. *IEEE Trans. Inform. Theory* **54**(9), 4230–4238 (2008)
8. Charpin, P., Kyureghyan, G.: On cubic monomial bent functions in the class \mathcal{M} . *SIAM J. Discrete Math.* **22**(2), 650–665 (2008)
9. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. *IEEE Trans. Inf. Theory* **51**, 4286–4298 (2005)
10. Dalai, D.K., Maitra, S., Sarkar, S.: Results on rotation symmetric bent functions. *Discrete Math.* **309**, 2398–2409 (2009)
11. Dillon, J.: Elementary Hadamard difference sets. Ph.D. Dissertation, University of Maryland (1974)
12. Filiol, É., Fontaine, C.: Highly nonlinear balanced boolean functions with a good correlation-immunity. In: Nyberg, K. (ed.) *EUROCRYPT 1998*. LNCS, vol. 1403, pp. 475–488. Springer, Heidelberg (1998)
13. Fontaine, C.: On some cosets of the first-order Reed-Muller code with high minimum weight. *IEEE Trans. Inform. Theory* **45**, 1237–1243 (1999)
14. Fu, S., Qu, L., Li, C., Sun, B.: Blanced $2p$ -variable rotation symmetric Boolean functions with maximum algebraic immunity. *Appl. Math. Lett.* **24**, 2093–2096 (2011)
15. Gao, G., Zhang, X., Liu, W., Carlet, C.: Constructions of quadratic and cubic rotation symmetric bent functions. *IEEE Trans. Inform. Theory* **58**, 4908–4913 (2012)
16. Gao, G., Cusick, T.W., Liu, W.: Families of rotation symmetric functions with useful cryptographic properties, to appear in *IET Information Security*
17. Kavut, S., Maitra, S., Yücel, M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. *IEEE Trans. Inform. Theory* **53**, 1743–1751 (2007)
18. Khoo, K., Gong, G., Stinson, D.: A new characterization of semi-bent and bent functions on finite fields. *Des. Codes Cryptogr.* **38**, 279–295 (2006)
19. Li, Y., Wang, M.: On EA-equivalence of certain permutations to power mappings. *Des. Codes Cryptogr.* **58**, 259–269 (2011)
20. MacWilliams, F.J., Sloane, J.: *The Theory of Error-Correcting Codes*. North Holland, Amsterdam (1977)
21. McFarland, R.L.: A family of noncyclic difference sets. *J. Combin. Theory Ser. A* **15**, 1–10 (1973)

22. Meier, W., Staffelbach, O.: Fast correlation attacks on stream ciphers. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 301–314. Springer, Heidelberg (1988)
23. Mesnager, S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums, and Dickson polynomials. *IEEE Trans. Inform. Theory* **57**, 7443–7458 (2011)
24. Pieprzyk, J., Qu, C.: Fast Hashing and rotation symmetric functions. *J. Univers. Comput. Sci.* **5**, 20–31 (1999)
25. Rijmen, V., Barreto, P., Gazzoni, D.: Filho, Rotation symmetry in algebraically generated cryptographic substitution tables. *Inf. Process. Lett.* **106**, 246–250 (2008)
26. Rothaus, O.S.: On bent functions. *J. Combin. Theory Ser. A* **20**, 300–305 (1976)
27. Stănică, P., Maitra, S.: Rotation symmetric Boolean functions-count and cryptographic properties. *Discrete Appl. Math.* **156**, 1567–1580 (2008)
28. Stănică, P., Maitra, S., Clark, J.A.: Results on rotation symmetric bent and correlation immune boolean functions. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 161–177. Springer, Heidelberg (2004)
29. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: Varadharajan, V., Mu, Y. (eds.) ICICS 1999. LNCS, vol. 1726, pp. 284–300. Springer, Heidelberg (1999)



<http://www.springer.com/978-3-319-12324-0>

Sequences and Their Applications – SETA 2014
8th International Conference, Melbourne, VIC, Australia,
November 24–28, 2014, Proceedings
Schmidt, K.-U.; Winterhof, A. (Eds.)
2014, XI, 315 p. 25 illus., Softcover
ISBN: 978-3-319-12324-0