The 5th International Workshop on

Boolean Functions and their Applications (BFA)

September 15-17, 2020

Loen, Norway

ABSTRACTS CONTRIBUTED TALKS

Contents

Analysis of APN functions and functions of small differential uniformity from the Maiorana-McFarland class

Nurdagül Anbar*, Tekgül Kalaycı*, and Wilfried Meidl**

*Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
**RICAM, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

Abstract

In the first part of the talk, we explain a method based on Bezout's Theorem on the intersection of two projective plane curves which can be used to analyse certain properties, like nonlinearity, of quadratic functions on $\mathbb{F}_{2^n}$, and apply the method to some classes of quadratic functions.

With the objective to find nontrivial examples of functions on $\mathbb{F}_{2^n}$, $n = 2m$, with the maximal possible number $2^n - 2^m$ of bent components, Pott et al. (2018) showed that for the quadratic function $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}_m^n(x)$ on $\mathbb{F}_{2^n}$, the component function $F_\gamma(x) = \mathrm{Tr}_1^n(\gamma\mathcal{F}(x))$, is bent if and only if $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Mesnager et al. showed more general the same result for $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}_m^n(\Lambda(x))$ under some conditions (which we will simplify) on a linearized polynomial $\Lambda \in \mathbb{F}_{2^m}[x]$.

In the second part of this talk, for the associated vectorial bent functions $F(x) = \mathrm{Tr}_m^n(\gamma x^{2^r}\mathrm{Tr}_m^n(\Lambda(x)))$, which are quadratic Maiorana-McFarland bent functions, we precisely describe the collection of the solution spaces of $\mathcal{D}_aF(x) = F(x) + F(x+a) + F(a)$, which forms a spread of $\mathbb{F}_{2^n}$. Analysing properties of several of those spreads, one arrives at neat conditions for $H(x) = (F(x), G(x))$ to have small differential uniformity. This also yields further candidates for APN functions in a nice representation. We point to an application of Bezout's Theorem in this connection.

1 Introduction

Many examples for some interesting classes of vectorial Boolean functions, like APN functions, are quadratic. One reason may be that quadratic functions permit several methods for their analysis, hence are easier to investigate. In this talk, we explain a method based on Bezout's Theorem on the intersection of two projective plane curves to analyse some properties of quadratic functions, which we introduced in [1] to determine the nonlinearity spectrum of Taniguchi's APN function.

In [4], it is shown that a function on $\mathbb{F}_{2^n}$, $n = 2m$, can have at most $2^n - 2^m$ bent components. Note that every vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ seen as a function on $\mathbb{F}_{2^n}$ trivially achieves this bound. Quadratic examples that are not obviously of this form, are presented in the papers [3, 4], namely $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}_m^n(\Lambda(x))$, some conditions on a linearized polynomial Λ imposed, see Section 3.

Though different functions of the form $x^{2^r}\mathrm{Tr}_m^n(\Lambda(x))$ are in general inequivalent, the associated vectorial bent functions $F(x) = \mathrm{Tr}_m^n(x^{2^r}\mathrm{Tr}_m^n(\Lambda(x)))$ are, as one can observe, all quadratic Maiorana-McFarland bent functions. In the first part of this talk we analyse the set of solution spaces of $\mathcal{D}_aF(x) = F(x) + F(x+a) + F(a)$ for our vectorial bent functions F, which all give spreads of $\mathbb{F}_{2^n}$ (a property which is an EA-equivalence invariant for vectorial bent functions). We remark that if $r = 0$ and $\Lambda(x) = x$, then F is equivalent to x^{2^r+1}, and as pointed out in [2], one obtains the standard representation of the Desarguesian spread. The properties of this representation of the spread (in bivariate form) are used in the constructions of Carlet's, the Zhou-Pott and Taniguchi's APN-function. Analysing properties of (representations of) the spreads for

other F, we get different neat conditions on $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $H(x) = (F(x), G(x))$ has a small differential uniformity. This can serve as tool to obtain various inequivalent classes of differentially k-uniform functions in a simple representation.

We then present results on the differential uniformity of functions $H(x) = (F(x), G(x))$ from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and point to an application of Bezout's points in the intersection in this connection.

2 Application of Bezout's Theorem

Let $\mathcal{X}_i$ be two projective curves over $\bar{\mathbb{F}}_2$ without common components of degree d_i, where $\bar{\mathbb{F}}_2$ is the algebraic closure of $\mathbb{F}_2$, and P be a point on $\mathcal{X}_i$ for $i = 1, 2$, i.e., $P \in \mathcal{X}_1 \cap \mathcal{X}_2$. We denote the multiplicity of $P \in \mathcal{X}_i$ by $m_P(\mathcal{X}_i)$ for $i = 1, 2$ and the intersection multiplicity of $P \in \mathcal{X}_1 \cap \mathcal{X}_2$ by $I(P, \mathcal{X}_1 \cap \mathcal{X}_2)$. It is well-known fact that $\mathcal{X}_1$ and $\mathcal{X}_2$ intersect at P with multiplicity

$$I(P, \mathcal{X}_1 \cap \mathcal{X}_2) \geq m_P(\mathcal{X}_1) m_P(\mathcal{X}_1) \tag{1}$$

and equality holds if and only if $\mathcal{X}_1$ and $\mathcal{X}_2$ have no common tangent lines at P. Then Bezout's Theorem states that

$$\sum_{P \in \mathcal{X}_1 \cap \mathcal{X}_2} I(P, \mathcal{X}_1 \cap \mathcal{X}_2) = d_1 d_2 \ . \tag{2}$$

In particular, by Bezout's theorem, we conclude that $\mathcal{X}_1$ and $\mathcal{X}_2$ intersect at most $d_1 d_2$ distinct points.

Let H be a function on $\mathbb{F}_{2^n}$ for $n = 2m$. By identifying $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we can consider H as a bivariate function. In particular, we can see Carlet's, the Zhou-Pott and Taniguchi's functions $H(x) = (F(x), G(x)) : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as a function $H(X, Y) = (F(X, Y), G(X, Y))$ on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Note that any directional derivative of the component function $H_{\lambda,\mu}$ of H corresponding to $(\lambda, \mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is linear as H is a quadratic function. Therefore, to determine the Walsh spectrum of H, it is enough to determine the dimensions of the solution spaces $\Lambda_{\lambda,\mu}$ consisting of $(u, v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ such that

$$\mathrm{Tr}_m \left(\lambda(F(X+u, Y+v) + F(X, Y) + F(u, v)) + \mu(G(X+u, Y+v) + G(X, Y) + G(u, v)) \right) = 0 \tag{3}$$

for all $(X, Y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. By using the fact that $\mathrm{Tr}_m(ux^{2^k}) = \mathrm{Tr}_m(u^{2^{i-k}} x^{2^i})$ we observe that Equation (3) is equivalent to

$$\mathrm{Tr}_m \left(A(u, v) X^{2^l} + B(u, v) Y^{2^j} \right) = 0$$

for some linearized polynomials $A(U, V), B(U, V) \in \mathbb{F}_{2^m}(U, V)$ of degree 2^{2i}, where i is an integer related to the degree of H with $\gcd(i, m) = 1$. That is, $\Lambda_{\lambda,\mu} = \{(u, v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid A(u, v) = B(u, v) = 0\}$. Then the fact $\gcd(i, m) = 1$ implies that the dimension of $\Lambda_{\lambda,\mu}$ over $\mathbb{F}_2$ is the same as the dimension of $\tilde{\Lambda}_{\lambda,\mu}$ over $\mathbb{F}_{2^i}$, where $\tilde{\Lambda}_{\lambda,\mu} = \{(u, v) \in \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}} \mid A(u, v) = B(u, v) = 0\}$. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves defined by the affine equations $A(U, V)$ and $B(U, V)$, respectively. We observe that $\mathcal{X}_i$ has a unique point P_i at infinity for $i = 1, 2$ such that $P_1 \neq P_2$. Note that this implies that $\mathcal{X}_1$ and $\mathcal{X}_2$ have no common components. Otherwise, they would have an intersection point at infinity. Then Bezout's theorem implies that $|\tilde{\Lambda}_{\lambda,\mu}| \leq 2^{4i}$ as $\mathcal{X}_1$ and $\mathcal{X}_2$ intersect at most 2^{4i} distinct affine points. In particular, we conclude that $\dim_{\mathbb{F}_2}(\Lambda_{\lambda,\mu}) \leq 4$. We suppose that they intersect at exactly 2^{4i} distinct affine points, i.e., the corresponding component function is 4-plateaued. In this case, we construct curves $\mathcal{Y}_1$ and $\mathcal{Y}_2$ of degrees 2^{2i+1} and $2^{2i} + 1$, respectively, satisfying the following properties.

(i) If $P \in \mathcal{X}_1 \cap \mathcal{X}_2$, then $P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$. In particular, $\mathcal{Y}_1$ and $\mathcal{Y}_2$ have 2^{4i} distinct affine intersection points.

(ii) If $P \in \mathcal{X}_1 \cap \mathcal{X}_2$, then $m_P(\mathcal{Y}_1) \geq 2$.

(iii) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ intersect at infinity, say Q, with $m_Q(\mathcal{Y}_1) = 2^{2i}$ and $m_Q(\mathcal{Y}_2) = 2^{2i} + 1$ with a common tangent line.

Then by Equations (1) and (2), we arrive a contradiction. That is, $\dim_{\mathbb{F}_2}(\Lambda_{\lambda,\mu}) \leq 2$, which gives the following result, see [1].

Theorem 2.1 *Carlet's, the Zhou-Pott and Taniguchi's APN-functions have classical spectrum.*

3 The Solution Spaces of $\mathcal{D}_a F(x) = F(x) + F(x+a) + F(a)$

In [4], it is shown that the function $F_\gamma(x) = \mathrm{Tr}_1^n(\gamma x^{2^r} \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(x))$, $r \geq 0$, is bent if and only if $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Hence $\mathcal{F}(x) = x^{2^r} \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(x)$ is an example of a function with maximal possible number of bent components, which is "nontrivial" if $r > 0$. If $r = 0$, then $\mathcal{F}$ is equivalent to x^{2^m+1}, which actually maps $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ and as pointed out in [2], is essentially the Maiorana-McFarland bent function xy in univariate representation.

In [3], where also two open problems of [4] are solved, it is shown that if for some $\alpha_j \in \mathbb{F}_{2^m}$, $1 \leq j \leq \sigma$, both $\mathcal{A}_1 = \sum_{j=1}^{\sigma} \alpha_j^{2^{m-t_j}} z^{2^{m-t_j}-1} + 1 = 0$ and $\mathcal{A}_2 = \sum_{j=1}^{\sigma} \alpha_j^{2^{m-r}} z^{2^{t_j}-1} + 1 = 0$ do not have a solution in $\mathbb{F}_{2^m}$, then the function $F_\gamma : \mathbb{F}_{2^n} \to \mathbb{F}_2$ given as

$$F_\gamma(x) = \mathrm{Tr}_n \left(\gamma x^{2^r} (\mathrm{Tr}_m^n(x) + \sum_{j=1}^{\sigma} \alpha_j \mathrm{Tr}_m^n(x^{2^{t_j}})) \right), \tag{4}$$

is bent if and only if $\gamma \notin \mathbb{F}_{2^m}$.

We first refine the observation in [3] on the above function by showing a simpler (and also necessary) condition.

Proposition 3.1 *Let $r \geq 0$ be an integer and $\Lambda(x) = x + \sum_{j=1}^{\sigma} \alpha_j x^{2^{t_j}} \in \mathbb{F}_{2^m}[x]$. The function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ given as*

$$F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r} \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x))) \tag{5}$$

is a vectorial bent function for all $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ if and only if Λ is a permutation of $\mathbb{F}_{2^m}$.

Our objective is now to describe the collection of the solution spaces for the vectorial bent functions in (5). We arrive at the following result.

Proposition 3.2 *Let Λ be a linear permutation of $\mathbb{F}_{2^m}$, and let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be the vectorial bent function in* (5)*.*

(i) For every $z \in \mathbb{F}_{2^m}$, $U_z = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_m^n(\gamma x^{2^r}) + z\mathrm{Tr}_m^n(\Lambda(x)) = 0\}$ is an m-dimensional subspace of $\mathbb{F}_{2^n}$. The subspaces U_z, $z \in \mathbb{F}_{2^m}$, together with $\mathbb{F}_{2^m}$ form a spread of $\mathbb{F}_{2^n}$.

(ii) For $a \in \mathbb{F}_{2^m}^*$ we have $F(x) + F(x+a) + F(a) = 0$ if and only if $x \in \mathbb{F}_{2^m}$, and the solution space of $F(x) + F(x+a) + F(a)$ is U_z if and only if $a \in U_z$.

Clearly, $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $H(x) = (F(x), G(x))$ and G quadratic, is differentially k-uniform if and only if G is differentially k-uniform on $\mathbb{F}_{2^m}$ and G restricted to the linear space U_z is differentially k-uniform for all $z \in \mathbb{F}_{2^m}$. We remark that the set of our solution spaces of $\mathcal{D}_a F$ for F being a spread, results in the smallest possible number of restrictions of this form on G. As remarked (see [2]), for $r = 0$, $\Lambda(x) = x$ we get the standard representation of the Desarguesian spread, i.e., the collection of the multiplicative cosets of $\mathbb{F}_{2^m}$ (0 added for each space). For $\gcd(r, m) < m$ we can also infer nice properties of some other flavour: Let $\alpha \in U_z$, $z \neq 0$, then for every $c \in \mathbb{F}_{2^m}^*$, the element $c\alpha$ lies in $U_{c^{2^r-1}z}$. In particular, if $\gcd(r, m) = 1$, then for $z \neq 0$ we have $U_z = cU_1$ for some $c \in \mathbb{F}_{2^m}^*$ (depending on z). For some classes of G we conclude the following conditions involving only 3 spread elements.

Theorem 3.3 *Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a quadratic function such that for every nonzero $c \in \mathbb{F}_{2^m}$ we have $G(c\alpha) = K(c)G(\alpha)$ for some nonzero constant $K(c) \in \mathbb{F}_{2^m}$ (depending on c) and every $\alpha \in \mathbb{F}_{2^n}$. If $\gcd(r, m) = 1$, then $H(x) = (\mathrm{Tr}_m^n(\gamma x^{2^r} \mathrm{Tr}_m^n(x)), G(x))$ is differentially k-uniform if and only if*

(i) G is differentially k-uniform on $\mathbb{F}_{2^m}$,

(ii) the function from U_0 to $\mathbb{F}_{2^m}$ given by $G(x) + G(x + a)$ is k-to-1 for every nonzero $a \in U_0$,

(iii) the function from U_1 to $\mathbb{F}_{2^m}$ given by $G(x) + G(x + a)$ is k-to-1 for every nonzero $a \in U_1$.

We remark that every monomial $G(x) = \mathrm{Tr}_m^n(\beta x^{2^i+1})$, and $G(x) = \mathrm{Tr}_m^n(\eta x^{2^i+1} + \delta x^{2^{m+i}+1})$ (suggested in [2]) for $r = 0$) satisfies $G(c\alpha) = K(c)G(\alpha)$, $c \in \mathbb{F}_{2^m}^*$. Therefore, our next aim is to investigate both the differential uniformity and the Walsh spectrum of H for these functions by using Theorem 3.3 and Bezout's Theorem.

We note that $U_1 = \{x \in \mathbb{F}_{2^n} \mid x + \gamma x^{2^r} \in \mathbb{F}_{2^m}\}$. As $\{1, \gamma, \gamma^{2^r+1}\}$ is linearly dependent over $\mathbb{F}_{2^m}$ and $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, there exist $a_1, a_0 \in \mathbb{F}_{2^m}$ such that $\gamma^{2^r+1} + a_1\gamma + a_0 = 0$. Let $c \in \mathbb{F}_{2^m}$ such that $c^{2^r} = a_1$. We define $\psi(T) := T + (\gamma + c)T^{2^r}$ and show that $\psi : \mathbb{F}_{2^m} \mapsto U_1$ is an isomorphism. Hence we can state Conditions (i) and (iii) in Theorem 3.3 together in a neater way as follows:
(i') G and $G \circ \psi$ are differentially k-uniform on $\mathbb{F}_{2^m}$.

In the rest of the talk we consider $H(x) = (F(x), G(x))$ for functions $G(x) = \mathrm{Tr}_m^n(\beta x^{2^r+1})$ and $G(x) = \mathrm{Tr}_m^n(\eta x^{2^r+1} + \delta x^{2^{m+r}+1})$, i.e., $r = i$. By above discussion, to decide differential uniformity of H, it is sufficient to examine the solution space of

(i′) $G(x + a) + G(x) + G(a) = 0$ in $a \in \mathbb{F}_{2^m}$ (resp., U_0) for $a \in \mathbb{F}_{2^m}^*$ (resp., $a \in U_0$) and

(ii′) $G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a)) = 0$ in $a \in \mathbb{F}_{2^m}$ for $a \in \mathbb{F}_{2^m}^*$.

By straightforward calculations, we show that $G(x + a) + G(x) + G(a) = 0$ has exactly 2 solutions in $\mathbb{F}_{2^m}$ for $a \in \mathbb{F}_{2^m}^*$, and in U_0 for $a \in U_0$ if $\beta, \beta\nu^{2^r+1} \notin \mathbb{F}_{2^m}$ for the first function, where $\nu^{2^r} = \gamma^{-1}$. Similarly, it has exact two solutions if $\eta + \delta, \eta\nu^{2^r+1} + \delta\nu^{(2^r+1)2^m} \notin \mathbb{F}_{2^m}$ for the second one. Moreover, $G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a)) = 0$ in $\mathbb{F}_{2^m}$ has at most 4 solutions for $a \in \mathbb{F}_{2^m}^*$. For the proof of the second argument we use Bezout's Theorem different than the one given in Section 2. By setting $X := x$ and $Y := x^{2^r}$, we can consider the solution space of $G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a)) = 0$ as the intersection of two curves $\mathcal{X}_1$ and $\mathcal{X}_2$ of degree 2^r such that each solution corresponds to an intersection point. We observe that $\mathcal{X}_i$ has a unique point at infinity P_i for $i = 1, 2$ such that $P_1 \neq P_2$. In other words, $\mathcal{X}_1$ and $\mathcal{X}_2$ are curves having no common components. Then Bezout's Theorem implies that $G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a)) = 0$ has at most 2^{2r} solutions in $\mathbb{F}_{2^{mr}}$, which implies the existence of at most 4 solutions in $\mathbb{F}_{2^m}$. That is, we obtain the following result.

Theorem 3.4 *Let $G(x) = \mathrm{Tr}_m^n(\beta x^{2^r+1})$ or $G(x) = \mathrm{Tr}_m^n(\eta x^{2^r+1} + \delta x^{2^{m+r}+1})$ and $\nu^{2^r} = \gamma^{-1}$. If $\gcd(r, m) = 1$ and $\beta, \beta\nu^{2^r+1} \notin \mathbb{F}_{2^m}$ or $\eta + \delta, \eta\nu^{2^r+1} + \delta\nu^{(2^r+1)2^m} \notin \mathbb{F}_{2^m}$, then $H(x) = (\mathrm{Tr}_m^n(\gamma x^{2^r} \mathrm{Tr}_m^n(x)), G(x))$ is differentially at most 4-uniform.*

Moreover, by similar calculations in Section 2, we can show that components functions are at most 4-plateaued. In particular, we see that any component function is bent or semibent if $n \equiv 2 \mod 4$. That is, we have the following result.

Corollary 3.5 *If $n \equiv 2 \mod 4$, then any APN function in Theorem 3.4 have classical spectrum.*

Our future work is to show the existence of elements $\eta, \delta \in \mathbb{F}_{2^n}$ giving low differential uniformity and high non-linearity as given in Theorem 2. Magma Calculation shows that there are many APN functions of these forms. Therefore, another aim is to find the conditions on these elements for which we obtain an infinite class of APN functions.

References

[1] N. Anbar, T. Kalaycı, W. Meidl, Determining the Walsh spectra of Taniguchi's and related APN-functions. Finite Fields Appl. 60 (2019), 0–0.

[2] C. Carlet, More constructions of APN and differentially 4-uniform functions by concatenation. Sci. China Math. 56 (2013), 1373–1384.

[3] S. Mesnager, F. Zhang, C. Tang, Y. Zhou, Further study on the maximum number of bent components of vectorial functions. Des. Codes Cryptogr. 87 (2019), 2597–2610.

[4] A. Pott, E. Pasalic, A. Muratovic-Ribic, S. Bajric, On the maximum number of bent components of vectorial functions. IEEE Trans. Inform. Theory 64 (2018), 403–411.

Differentially low uniform permutations from the Gold and the Bracken-Leander functions

Marco Calderini

Department of Informatics, University of Bergen, Norway

Abstract

Functions with low differential uniformity can be used in block ciphers as S-boxes since they have good resistance to differential attacks. In this extended abstract, we give two constructions of differentially 6-uniform permutations over $\mathbb{F}_{2^{2m}}$ by modifying the Gold function and the Bracken-Leander function on a subfield.

1 Introduction

Let n be a positive integer, we will denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements and its multiplicative group by $\mathbb{F}_{2^n}^\star$. Permutation maps defined over $\mathbb{F}_{2^n}$ are used as S-boxes of some symmetric cryptosystems. So, it is important to construct permutations with good cryptographic properties in order to design a cipher that can resist to the known attacks. In particular, among these properties we have a low differential uniformity for preventing differential attacks [1], high nonlinearity for avoiding linear cryptanalysis [6] and also high algebraic degree to resist to higher order differential attacks [5].

The best differential uniformity of a function F defined over $\mathbb{F}_{2^n}$ is 2. Functions achieving this value are called almost perfect nonlinear (APN). For odd values of n there are known families of APN permutations; while for n even there exists only one example of APN permutation over $\mathbb{F}_{2^6}$ [2] and the existence of more ones remains an open problem. For ease of implementation, usually, the integer n is required to be even in a cryptosystem. Therefore, finding permutations with good cryptographic properties over $\mathbb{F}_{2^n}$ with n even is an interesting research topic for providing more choices for the S-boxes.

The construction of low differentially uniform permutations with the highest nonlinearity over $\mathbb{F}_{2^n}$ (with n even) is a difficult task. In Table 1 we give 5 families of primarily constructed differentially 4-uniform permutations with the best known nonlinearity.

In the last years, many constructions of differentially 4-uniform permutations have been found by modifying the inverse function on some subsets of $\mathbb{F}_{2^n}$ (see for instance [7, 8, 9, 10, 11]). In particular, in [7, 10, 11] the authors change the inverse function on some subfields of $\mathbb{F}_{2^n}$.

Table 1: Primarily-constructed differentially 4-uniform over $\mathbb{F}_{2^n}$

Name	**F(x)**	**deg**	**Conditions**
Gold	x^{2^i+1}	2	$n=2k$, k odd $\gcd(i,n)=2$
Kasami	$x^{2^{2i}-2^i+1}$	i+1	$n=2k$, k odd $\gcd(i,n)=2$
Inverse	x^{2^n-2}	$n-1$	$n=2k$, $k\geq 1$
Bracken-Leander	$x^{2^{2k}+2^k+1}$	3	$n=4k$, k odd
Bracken-Tan-Tan	$\zeta x^{2^i+1}+\zeta^{2^m}x^{2^{-m}+2^{m+i}}$	2	$n=3m$, m even, $m/2$ odd, $\gcd(n,i)=2$, $3\vert m+i$ and ζ is a primitive element of $\mathbb{F}_{2^n}$

In this abstract, we investigate the piecewise construction as in [7, 10, 11] by modifying the image of the Gold and Bracken-Leander function on some subfields of $\mathbb{F}_{2^n}$. We show that in these cases it is possible to obtain permutations with differential uniformity at most 6. Moreover, if we modify these functions using the inverse function (or a function equivalent to it), then we can obtain permutations with algebraic degree $n-1$ (which is the highest possible) and high nonlinearity. These results extend those given in [12], where the authors modified the 4-uniform Gold function for constructing differentially 6-uniform permutations.

2 Preliminaries

Any function F from $\mathbb{F}_{2^n}$ to itself can be represented as a univariate polynomial of degree at most 2^n-1, that is

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i.$$

The *2-weight* of an integer $0 \leq i \leq 2^n-1$, denoted by $w_2(i)$, is the (Hamming) weight of its binary representation. The algebraic degree of a function F is given by $\deg(F) = \max\{w_2(i) \mid a_i \neq 0\}$. Functions of algebraic degree 1 are called *affine*. Linear functions are affine functions with constant term equal to zero and they can be represented as $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$. For any permutation F it is well known that $\deg(F) \leq n-1$.

For any $m \geq 1$ such that $m|n$ we can define the (linear) *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ by $\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$. When $m=1$ we will denote $\mathrm{Tr}_1^n(x)$ by Tr.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote the *Walsh transform* in $a, b \in \mathbb{F}_{2^n}$ by

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax+bF(x))}.$$

The *nonlinearity* of a vectorial Boolean function F is given by

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\star} |\mathcal{W}_F(a,b)|.$$

When n is odd, it has been proved that $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$; for n even, the best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$, and it is conjectured that $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n}{2}}$.

Definition 2.1 *For a function F from $\mathbb{F}_{2^n}$ to itself, and any $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_{2^n}$, we denote by $\delta_F(a,b)$ the number of solutions of the equation $F(x+a)+F(x)=b$. The maximum value δ among the $\delta_F(a,b)$'s is called the differential uniformity of F, and F is said to be differentially δ-uniform.*

There are several equivalence relations of functions for which the differential uniformity and the nonlinearity are preserved. Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- *affine equivalent* if $F' = A_1 \circ F \circ A_2$ where the mappings $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- *extended affine equivalent* (EA-equivalent) if $F' = F'' + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

Obviously, affine equivalence is included in the EA-equivalence, and it is also well known that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse [4]. The algebraic degree is invariant for the affine equivalence and also for the EA-equivalence for nonlinear functions, but not for the CCZ-equivalence (and inverse transformation).

3 Constructing differentially 6-uniform permutations

In this section we will study the piecewise construction for the case of Gold and the Bracken-Leander function. We refer to the full version of the paper [3] for more details on the proofs of the results given in this section.

The following lemma give a characterisation for the solutions of $(x+1)^{2^k+1} + x^{2^k+1} = b$, when b belongs to some specific subfield $\mathbb{F}_{2^s}$ of $\mathbb{F}_{2^n}$.

Lemma 3.1 *Let $n = sm$ with s even and m odd. Let k be such that $\gcd(k,n) = 2$. For any $b \in \mathbb{F}_{2^s}$ the equation*

$$x^{2^k} + x = b$$

does not admit any solution x in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$.

Proof: See [3]. □

Theorem 3.2 *Let $n = sm$ with s even such that $s/2$ is odd and m odd. Let k be such that $\gcd(k,n) = 2$ and f be at most differentially 6-uniform permutation over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$.

Proof: Using the Lemma 3.1 it is possible to analyse the solutions of the equation

$$F(x) + F(x+a) = b,$$

distinguishing the cases where: both x and $x+a$ are in $\mathbb{F}_{2^s}$; one is in $\mathbb{F}_{2^s}$ and the other not; none is contained in $\mathbb{F}_{2^s}$. See [3] for a detailed proof. □

Also for the Bracken-Leander function we can characterize the solutions of the equation $(x+1)^{2^{2k}+2^k+1} + x^{2^{2k}+2^k+1} = b$, when b is in some specific subfield.

Lemma 3.3 *Let $n = 4k = sm$ with k and m odd. For any $b \in \mathbb{F}_{2^s}$ the equation*

$$x^{2^{2k}+2^k} + x^{2^{2k}+1} + x^{2^k+1} + x^{2^{2k}} + x^{2^k} + x = b \tag{1}$$

does not admit any solution x in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$.

Proof: See [3]. □

Similarly to Theorem 3.2 we obtain:

Theorem 3.4 *Let $n = 4k = sm$, with k, m odd and s even. Let f be at most differentially 6-uniform permutation over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}+2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}+2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$.

From Theorem 3.2 and Theorem 3.2 we obtain a general construction for functions with differential uniformity at most 6. In the following, we will show that using a function f equivalent to the inverse function we can obtain a permutation of degree $n-1$ with high nonlinearity.

We, first, give the following result, which is a necessary and sufficient condition for a permutation to have maximal degree.

Lemma 3.5 *Let F be a function defined over $\mathbb{F}_{2^n}$. Then, F in its polynomial representation has a term of algebraic degree $n-1$ if and only if there exists a linear monomial x^{2^j} such that $\sum_{x\in\mathbb{F}_{2^n}} F(x)x^{2^j} \neq 0$. In particular, if F is a permutation then $\deg(F) = n-1$.*

Proof: See [3]. □

Corollary 3.6 *Let $n = sm$ with s even such that $s/2$ is odd and m. Let k be such that $\gcd(k, n) = 2$ and $f(x) = A_1 \circ Inv \circ A_2(x)$, where $Inv(x) = x^{-1}$ and A_1, A_2 are affine permutations over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 2$ then the algebraic degree of F is $n - 1$.

Proof: We need to prove only that the degree of F is $n-1$. From Lemma 3.5, since $\deg(f(x)) = s - 1$ there exists $h(x) = x^{2^j}$ in $\mathbb{F}_{2^s}[x]$ (with $j \leq s - 1$) such that $\sum_{x\in\mathbb{F}_{2^s}} f(x)h(x) \neq 0$.

Thus, since $\deg(x^{2^k+1}) = 2 < s - 1$ we obtain

$$\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) = \sum_{x\in\mathbb{F}_{2^s}} f(x)h(x) + \sum_{x\in\mathbb{F}_{2^n}} x^{2^k+1}h(x) + \sum_{x\in\mathbb{F}_{2^s}} x^{2^k+1}h(x) = \sum_{x\in\mathbb{F}_{2^s}} f(x)h(x) \neq 0.$$

Then, $\deg(F) = n - 1$ since F is a permutation. □

Similarly we have the following construction using the Bracken-Leander function.

Corollary 3.7 *Let $n = 4k = sm$ with k, m odd and s even. Let $f(x) = A_1 \circ Inv \circ A_2(x)$, where $Inv(x) = x^{-1}$ and A_1, A_2 are affine permutations over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}+2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}+2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 4$ then $\deg(F) = n - 1$.

Remark 3.8 *When $s = 2$ and $G(x) = x^{2^k+1}$ or $s = 4$ and $G(x) = x^{2^{2k}+2^k+1}$ we have $\deg(G) = s - 1$. Thus, we could obtain a permutation of degree less than $n - 1$ in Corollary 3.6 and Corollary 3.7.*

For the nonlinearity of the constructed functions we have the following.

Proposition 3.9 *The nonlinearity of the functions in Corollary 3.6 and Corollary 3.7 is at least $2^{n-1} - 2^{\frac{n}{2}} - 2^{\frac{s}{2}+1}$.*

Proof: See [3]. □

It is well known that the algebraic degree is not preserved by the CCZ-equivalence and in particular by the inverse transformation. However, for any permutation of maximal algebraic degree we have the following easy observation.

Proposition 3.10 *Let F be a permutation defined over $\mathbb{F}_{2^n}$. Then, $\deg(F) = n - 1$ if and only if $\deg(F^{-1}) = n - 1$.*

Proof: Suppose $\deg(F) = n-1$ and let $h(x)$ a linear monomial for which we have $\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) \neq 0$. Since F is a permutation we obtain $\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) = \sum_{x\in\mathbb{F}_{2^n}} xh(F^{-1}(x))$, which implies $\deg(h \circ F^{-1}) = n - 1$. Since h is linear we have that $\deg(F^{-1}) = n - 1$. □

From this result we have that also the compositional inverses of the functions given in Corollary 3.6 and Corollary 3.7 are differentially 6-uniform functions with high nonlinearity and algebraic degree $n - 1$.

Denoting by $\omega = \zeta^{\frac{2^n-1}{3}}$ the primitive element of $\mathbb{F}_4$, in Table 2 and Table 3 we give the CCZ-inequivalent functions that can be obtained by Corollary 3.6 for $n = 6, 10$ considering $f(x) = A \circ Inv$.

Table 2: CCZ-inequivalent permutations from Corollary 3.6 over $\mathbb{F}_{2^6}$

$A(x)$	deg	$\mathcal{NL}(G)$	Bound on $\mathcal{NL}$	δ
x	2	24	20	4
$x+\omega$	4	20	20	6
$\omega x^2+\omega$	5	20	20	6
ωx	5	22	20	6
$\omega^2 x^2+\omega$	5	22	20	6

Table 3: CCZ-inequivalent permutations from Corollary 3.6 over $\mathbb{F}_{2^{10}}$

$A(x)$	deg	$\mathcal{NL}(G)$	Bound on $\mathcal{NL}$	δ
x	2	480	476	4
$x+\omega$	8	476	476	6
$\omega x^2+\omega$	9	476	476	6
ωx	9	478	476	6
$\omega^2 x^2+\omega$	9	478	476	6

In Table 4 we report some permutations constructed from Corollary 3.7 for $n = 12$ (in this case $s = 4$ and $m = 3$). As before, we consider $f(x) = A \circ Inv$ with A affine permutations defined over $\mathbb{F}_4[x]$ (for $A(x) = x^2$ we obtain the Bracken-Leander function).

Table 4: CCZ-inequivalent permutations from Corollary 3.7 over $\mathbb{F}_{2^{12}}$

$A(x)$	deg	$\mathcal{NL}(G)$	Bound on $\mathcal{NL}$	δ
x^2	3	1984	1976	4
x^2+1	8	1976	1976	6
$\omega^2 x^2+\omega$	11	1976	1976	6
$x+\omega$	11	1978	1976	6
ωx^2	11	1980	1976	6

References

[1] E. Biham, A.Shamir, *Differential cryptanalysis of DES-like cryptosystems*. J. Cryptology 4(1), 3–72 (1991)

[2] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, *An APN permutation in dimension six*. In: Contemporary Mathematics, Vol. 518, Am. Math Soc., pp. 33–42 (2010).

[3] M. Calderini, *Differentially low uniform permutations from known 4-uniform functions*. arXiv preprint arXiv:1910.14337 (2019).

[4] C. Carlet, P. Charpin, V. Zinoviev, *Bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15**, 125–156 (1998).

[5] L. Knudsen, *Truncated and higher order differentials*. FSE 1994, Lecture Notes in Computer Sciences, vol. 1008, 196–211 (1995).

[6] L. Matsui, *Linear cryptanalysis method for DES cipher*. Advances in Cryptology EUROCRYPT93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin Heidelberg, 386–397 (1994).

[7] J. Peng, C. H. Tan, *New differentially 4-uniform permutations by modifying the inverse function on subfields*. Cryptogr. Commun. 9, 363–378 (2017) .

[8] L. J. Qu, Y. Tan, C. H. Tan, C. Li, *Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method*. IEEE Trans. Inf. Theory 59(7), 4675–4686 (2013).

[9] D. Tang, C. Carlet, X. Tang, *Differentially 4-uniform bijections by permuting the inverse function*. Des. Codes. Cryptogr. 77, 117–141 (2015).

[10] G. Xu, L. Qu, *Two classes of differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ with n even*. Adv. Math. Comm., 14(1), 97–110 (2019).

[11] Z. Zha, L. Hu, S. Sun, *Constructing new differentially 4-uniform permutations from the inverse function*. Finite Fields Appl. 25, 64–78 (2014) .

[12] Z. Zha, L. Hu, J. Shan, *Differentially 6-uniform permutations by modifying the Gold function*. In: IEEE Int. Conf. on Information and Automation (ICIA), 961–965 (2014).

C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity

Pål Ellingsen[*], Patrick Felke[**], Constanza Riera[*], Pantelimon Stănică[***], and Anton Tkachenko[*]

[*]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway
[**]University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden, Germany
[***]Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216

Abstract

We defined recently [3] a new (output) multiplicative differential, and the corresponding c-differential uniformity, which is first characterized via a convolution of Walsh transforms. With this new differential concept, even for characteristic 2, there are perfect c-nonlinear (PcN) functions. We looked at some of the known classes of perfect nonlinear (PN) functions and show that only one remains a PcN function, under a different condition on the parameters. Surprisingly, the p-ary Gold PN function increases its c-differential uniformity significantly, under some conditions on the parameters. We then characterize the c-differential uniformity of the inverse function (in any dimension and characteristic).

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables and denote the set of all such functions by $\mathcal{B}_n$. For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)},$$

where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

An (n,m)-*function* (often called a *vectorial Boolean function* if there is no need to explicitly specify the dimensions n and m) is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. When $m = n$, it can be represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$) of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}$. The algebraic degree of the function is then the largest Hamming weight of an exponent i, with $a_i \neq 0$. For an (n,m)-function F, we define the Walsh transform $W_F(a,b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}.$$

For an (n,n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} : F(x+a)+F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a,b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F = \delta$, then we say that F is differentially δ-uniform. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function.

At the Fast Software Encryption (FSE 2002) conference, N. Borisov, M. Chew, R. Johnson, D. Wagner used a new type of differential that is quite useful for the cryptanalysis of ciphers that utilize modular multiplication as a primitive operation. It is an extension of a type of differential cryptanalysis and it was used to cryptanalyse some existing ciphers (like a variant of the well-known IDEA cipher).

Inspired by the previously mentioned successful attempt, we started a theoretical analysis of an (output) multiplicative differential. Given a p-ary (n,m)-function $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^m}$, and $c\in\mathbb{F}_{p^m}$, the (multiplicative) c-derivative of F with respect to $a\in\mathbb{F}_{p^n}$ is the function

$$ {}_cD_aF(x)=F(x+a)-cF(x),\ \text{for all } x\in\mathbb{F}_{p^n}.$$

(Note that, if $c=1$, then we obtain the usual derivative, and, if $c=0$ or $a=0$, then we obtain a shift of the function.) For an (n,n)-function F, and $a,b\in\mathbb{F}_{p^n}$, we let ${}_c\Delta_F(a,b)=\#\{x\in\mathbb{F}_{p^n}: F(x+a)-cF(x)=b\}$. We call the quantity

$${}_c\Delta_F=\max\{{}_c\Delta_F(a,b)\ :\ a,b\in\mathbb{F}_{p^n},\ \text{and } a\neq 0 \text{ if } c=1\}$$

(surely, including $a=0$ for the case $c\neq 1$, the equation $F(x)-cF(x)=b$ is of course, $F(x)=b(1-c)^{-1}$, so we are looking here at how close F is to a permutation polynomial, and similarly in the case $c=0$ for any a) the *c-differential uniformity* of F. If ${}_c\Delta_F=\delta$, then we say that F is differentially (c,δ)-uniform. If $\delta=1$, then F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c=1$, they only exist for odd characteristic p; however, one wonders whether they can exist for $p=2$ for $c\neq 1$, and we shall argue later that that is actually true). If $\delta=2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function. It is easy to see that if F is an (n,n)-function, that is, $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, then F is PcN if and only if ${}_cD_aF$ is a permutation polynomial.

In the work [3] we first characterized the c-differential uniformity of a function via a generalized convolution of Walsh transforms. As particular examples, we show that if m,n are fixed positive integers and $c\in\mathbb{F}_{p^m}$, $c\neq 1$, F is an (n,m)-function, then

$$\sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}}|\mathcal{W}_F(u,v)|^2|\mathcal{W}_F(u,cv)|^2\geq p^{3n+m},$$

with equality if and only if F is a perfect c-nonlinear (PcN) function; Furthermore, we have

$$\begin{aligned}&\sum_{\substack{u_1,u_2\in\mathbb{F}_{p^n}\\ v_1,v_2\in\mathbb{F}_{p^m}}}\overline{\mathcal{W}_F}(u_1+u_2,v_1+v_2)\mathcal{W}_F(u_1+u_2,c(v_1+v_2))\\ &\qquad\cdot\overline{\mathcal{W}_F}(u_1,v_1)\overline{\mathcal{W}_F}(u_2,v_2)\mathcal{W}_F(u_1,cv_1)\mathcal{W}_F(u_2,cv_2)\\ &\geq 3\cdot p^{m+n}\sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}}|\mathcal{W}_F(u,v)|^2|\mathcal{W}_F(u,cv)|^2-2\cdot p^{2(2n+m)},\end{aligned}$$

with equality if and only if F is an almost perfect c-nonlinear (APcN).

We then proceeded to investigate some of the known perfect nonlinear functions. We therefore show the following major theorem [3].

Theorem 1 *Let $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be the monomial $F(x)=x^d$, and $c\neq 1$ be fixed. The following statements hold:*

(i) If $d=2$, then F is APcN, for all $c\neq 1$.

(ii) If $d=p^k+1$, $p>2$, then F is not PcN, for all $c\neq 1$. Moreover, when $(1-c)^{p^k-1}=1$ and $n/\gcd(n,k)$ is even, the c-differential uniformity ${}_c\Delta_F\geq p^g+1$, where $g=\gcd(n,k)$.

(iii) Let $p=3$. If $d=\dfrac{3^k+1}{2}$, then F is PcN, for $c=-1$ if and only if $\dfrac{n}{\gcd(n,k)}$ is odd.

(iv) If $p=3$ and $F(x)=x^{10}-ux^6-u^2x^2$, the c-differential uniformity of F is ${}_c\Delta_F\geq 2$.

We then looked at the inverse function, which is APN for n odd and has differential uniformity 4 for n even and show the next two theorems [3].

Theorem 2 *Let n be a positive integer, $1 \neq c \in \mathbb{F}_{2^n}$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(x) = x^{2^n-2}$. We have:*

(i) If $c = 0$, then F is PcN (that is, F is a permutation polynomial).

(ii) If $c \neq 0$ and $\mathrm{Tr}_n(c) = \mathrm{Tr}_n(1/c) = 1$, the c-differential uniformity of F is 2 (and hence F is APcN).

(iii) If $c \neq 0$ and $\mathrm{Tr}_n(1/c) = 0$, or $\mathrm{Tr}_n(c) = 0$, the c-differential uniformity of F is 3.

Theorem 3 *Let p be an odd prime, $n \geq 1$ be a positive integer, $1 \neq c \in \mathbb{F}_{p^n}$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the inverse p-ary function defined by $F(x) = x^{p^n-2}$. We have:*

(i) If $c = 0$, then F is PcN (that is, F is a permutation polynomial).

(ii) If $c \neq 0, 4, 4^{-1}$, $(c^2 - 4c) \in (\mathbb{F}_{p^n})^2$, or $(1 - 4c) \in (\mathbb{F}_{p^n})^2$, the c-differential uniformity of F is 3.

(iii) If $c = 4, 4^{-1}$, the c-differential uniformity of F is 2 (and hence F is APcN).

(iv) If $c \neq 0$, $(c^2 - 4c) \notin (\mathbb{F}_{p^n})^2$ and $(1 - 4c) \notin (\mathbb{F}_{p^n})^2$, the c-differential uniformity of F is 2 (and hence F is APcN).

The computational data on c-differential uniformity presented in [3] on the Gold and Kasami cases prompted more investigation and a first step was taken in [5] with a complete description of the Gold case, as well as an investigation of some of the APN entries from the Helleseth-Rong-Sandberg table [4].

It would be quite interesting to continue with some of the other entries in the table [4], Dobbertin et al. [2] further examples, or even newer PN or APN classes of functions, through the prism of the newly defined c-differentials concept we introduced in [3].

References

[1] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds) Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science, vol 2365. Springer, Berlin, Heidelberg, 2002.

[2] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, and W. Willems, *APN functions in odd characteristic*, Discr. Math. 267 (1-3) (2003), 95–112.

[3] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory, 2020.

[4] T. Helleseth, C. Rong, D. Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE Trans. Inf. Theory 45 (1999), 475–485.

[5] C. Riera, P. Stănică, *Investigations on c-(almost) perfect nonlinear functions*, manuscript, 2020.

On Differentially 4-uniform Permutations with Low Carlitz Rank

Jaeseong Jeong, Namhun Koo, Soonhak Kwon

Email: wotjd012321@naver.com, komaton@skku.edu, shkwon@skku.edu
Applied Algebra and Optimization Research Center,
Sungkyunkwan University, Suwon, Republic of Korea

Abstract

Finding permutation polynomials with low differential uniformity is an important topic in S-box designs of many block ciphers. For example, AES chooses the differentially 4-uniform inverse function as its S-box. This inverse function has good cryptographic properties with high algebraic degree and nonlinearity. Therefore, many variants of the inverse function has been researched ([5, 6, 8–10]). In this paper, we characterize the differential uniformity of a permutation polynomial having low Carlitz rank. We show that permutation of low Carlitz rank is affine equivalent to cycle or composition of cycle and the inverse function. As a result, we give a classification of the differential uniformity of the permutation polynomials of Carlitz rank at most 4 and we present new classes of differentially 4-uniform permutation polynomials.

1 Introduction

A **Boolean function** of n variables is a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ and an **vectorial boolean function** ((n, m)**-function** or **S-box**) is a function $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ where $\mathbb{F}_{2^n}$ is denoted by finite field with 2^n elements. For a given function $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, the **difference distribution table**, denoting $\mathtt{DDT}_F$, whose entries are given as

$$\mathtt{DDT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : F(x) + F(x + a) = b\},$$

where $\#A$ denotes the cardinality of a set A. The function F is **differential δ-uniform** if $\Delta_F \leq \delta$ where

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n} \setminus \{0\},\ b \in \mathbb{F}_{2^n}} \mathtt{DDT}(a, b),$$

and Δ_F is called **differential uniformity** of F. It is clear that the smallest value of Δ_F is 2 and such function is called **Almost perfect nonlinear** (**APN**) function. APN permutations play a important role in designing S-box. But finding an APN permutation is very difficult, so finding differential 4-uniform permutation has been studied actively. ([5, 6, 8–10])

Now we introduce the Carlitz rank of permutation. We let denote $[a_0, a_1, \ldots, a_m]$ continued fraction

$$a_0 + (a_1 + (a_2 + \cdots (a_{m-1} + a_m^{2^n-2}) \cdots)^{2^n-2})^{2^n-2}$$

where $a_i \in \mathbb{F}_{2^n}$. We identify x^{2^n-2} with x^{-1} over $\mathbb{F}_{2^n}$ by defining as $0^{-1} = 0$. It is known that for any permutation $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, there is $m \geq 0$ and $a_i \in \mathbb{F}_{2^n}$, $0 \leq i \leq m$ such that

$$\begin{aligned} F(x) &= [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x] \\ &= (\cdots((a_0 x + a_1)^{-1} + a_2)^{-1} \cdots + a_m)^{-1} + a_{m+1}, \end{aligned} \tag{1}$$

where $a_0, a_2, \cdots, a_m \neq 0$([4]). For a given F, the above expression is not unique in general. However there is the least m among all possible expressions of F. The **Carlitz rank** of F is the least integer m satisfying the above expression. Suppose that a permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has Carlitz rank $\leq m$. Then one may write F as the form of Eq.(1). For given F and $0 \leq k \leq m$, we define

$$\begin{aligned} F_k(x) &= [a_{k+1}, a_k, \ldots, a_2, a_1 + a_0 x] \\ &= (\cdots((a_0 x + a_1)^{-1} + a_2)^{-1} \cdots + a_k)^{-1} + a_{k+1} \end{aligned}$$

Then one has $F_0(x) = a_0 x + a_1, F_1(x) = (a_0 x + a_1)^{2^n-2} + a_2, \cdots, F_m = F$. Also we inductively define $R_k(x)$ for $0 \leq k \leq m$ as follows

$$R_k(x) = \frac{\alpha_{k+1} x + \beta_{k+1}}{\alpha_k x + \beta_k}, \tag{2}$$

where

$$\alpha_{k+1} = a_{k+1}\alpha_k + \alpha_{k-1}, \quad \beta_{k+1} = a_{k+1}\beta_k + \beta_{k-1} \quad (1 \leq k \leq m)$$

with the initial conditions $\alpha_0 = 0, \alpha_1 = a_0$ and $\beta_0 = 1, \beta_1 = a_1$. Then it is known [4] that

$$R_k(x) = F_k(x) \text{ for all } x \notin \mathbf{O}_k \quad \left(\mathbf{O}_k = \left\{ x_i = \frac{\beta_i}{\alpha_i} : i = 1, \ldots, k \right\}, \mathbf{O}_k \subset \mathbb{F}_{2^n} \cup \{\infty\} \right)$$

where $x_i's$ are called **poles** of F_k and $x_i = \infty$ if and only if $\alpha_i = 0$.

2 Carlitz rank and inverse function

Two functions $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ and $F' : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ are called **affine equivalent** if there exist affine permutations A_1, A_2 satisfying $F' = A_1 \circ F \circ A_2$. (for details, see [1-3]) It is well-known that two affine equivalent functions have same differential uniformity.

Lemma 2.1. *A permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with Carlitz rank $\leq m$ is affine equivalent to inverse function Inv with at most m exceptional points. That is, there is a subset $U \subset \mathbb{F}_{2^n}$ with $\#U \leq m$ and affine permutations $\ell_1, \ell_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfying $\ell_2 \circ F \circ \ell_1(x) = \frac{1}{x}$ for all $x \notin U$.*

As a consequence of the above result, cryptographic properties of a permutation of low Carlitz rank are closely related with those of inverse function modified at some small set of points. In subsequent sections, we discuss cryptographic properties of a permutation of low Carlitz rank.

3 Differential uniformity

Before finding the differential uniformity of $F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x]$ on $\mathbb{F}_{2^n}$, we can set $a_0 = 1, a_1 = 0, a_2 = 1$ without loss of generality by the follwing proposition.

Proposition 3.1. *Let $F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x]$ on $\mathbb{F}_{2^n}$ where $a_0, a_2, \cdots, a_m \neq 0$.*
(i) If $m = 1$ then F is affine equivalent to G, given by $G(x) = x^{-1}$ on $\mathbb{F}_{2^n}$.
(ii) If $m \geq 2$ then F is affine equivalent to G, given by

$$G(x) = [0, \gamma_m, \ldots, \gamma_1, x] = (\cdots((x^{2^n-2} + \gamma_1)^{2^n-2} + \gamma_2)^{2^n-2} \cdots + \gamma_m)^{2^n-2}$$

where $\gamma_1 = 1$ and $\gamma_i = a_2^{(-1)^i} a_{i+1}$ for $i \geq 2$.

From now on we set

$$F(x) = [0, a_m, \ldots, a_3, 1, x], \tag{3}$$

Now we denote

$$A_i = [0, 1, a_3, \cdots, a_i] \text{ for } 1 \leq i \leq m, \tag{4}$$

i.e. $A_1 = [0], A_2 = [0, 1], A_3 = [0, 1, a_3], \cdots, A_m = [0, 1, a_3, \ldots, a_m]$, and

$$A'_u = [0, 1, a_3, \ldots, a_m, u]. \tag{5}$$

Then we have the following lemma:

Lemma 3.2. *Let $F(x) = [0, a_m, \ldots, a_3, 1, x]$ on $\mathbb{F}_{2^n}$ with $a_3, \ldots, a_m \neq 0$. Then*

$$\mathtt{DDT}_F(a, b) = \mathtt{DDT}_{F^{-1}}(b, a) = \#\{u \in \mathbb{F}_{2^n} : A'_u + A'_{u+b} = a\}.$$

For given $a, b \in \mathbb{F}_{2^n} \setminus \{0\}$, we now define 4 partitions of $\{u \in \mathbb{F}_{2^n} : A'_u + A'_{u+b} = a\}$, denoted by $P(a, b)$, as follows :

$$\begin{aligned}
P_A(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \exists\ 1 \leq i, j \leq m\ A'_u = A_i,\ A'_{u+b} = A_j\} \\
P_B(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \nexists\ 1 \leq i \leq m\ A'_u = A_i,\ \exists\ 1 \leq j \leq m\ A'_{u+b} = A_j\} \\
P_{B'}(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \exists\ 1 \leq i \leq m\ A'_u = A_i,\ \nexists\ 1 \leq j \leq m\ A'_{u+b} = A_j\} \\
P_C(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \nexists\ 1 \leq i, j \leq m\ A'_u = A_i,\ A'_{u+b} = A_j\}
\end{aligned} \tag{6}$$

It is clear that

$$\mathtt{DDT}_F(a, b) = \#P(a, b) = \#P_A(a, b) + \#P_B(a, b) + \#P_{B'}(a, b) + \#P_C(a, b).$$

Moreover we have $\#P_B(a, b) = \#P_{B'}(a, b)$, so

$$\mathtt{DDT}_F(a, b) = \#P(a, b) = \#P_A(a, b) + 2\#P_B(a, b) + \#P_C(a, b).$$

We now use the notation

$$u_i = [0, a_m, a_{m-1}, \ldots, a_{i+1}],$$

which is the root of $[0, 1, a_3, \ldots, a_m, u] = [0, 1, \ldots, a_i]$, i.e $A'_u = A_i$. The following theorem implies how $P_A(a, b), P_B(a, b)$ and $P_C(a, b)$ are constructed.

Theorem 3.3. *Let $F(x) = [0, a_m, \ldots, a_3, 1, x]$ on $\mathbb{F}_{2^n}$ with $a_3, \ldots, a_m \neq 0$. Let $U = \{u_i : 1 \leq i \leq m\}$ of cardinality m' and we have $1 \leq i_1 < i_2 < \cdots < i_{m'} \leq m$ such that $U = \{u_{i_1}, u_{i_2}, \ldots, u_{i_{m'}}\}$. Then the followings are satisfied:*

(i) $\#P_A(a,b) = \begin{cases} 2 & \text{if } (a,b) \in \{(A_{i_j}+A_{i_k}, u_{i_j}+u_{i_k}) : 1 \le j < k \le m'\} \\ 0 & \text{otherwise} \end{cases}$

(ii) $\#P_B(a,b) = \#\left\{1 \le j \le m' : b + u_{i_j} = \dfrac{(a+A_{i_j})\alpha_{m-1} + \beta_{m-1}}{(a+A_{i_j})\alpha_m + \beta_m},\ b + u_{i_j} \notin U\right\}$

(iii) *If* $\alpha_m \neq 0$ *then* $\#P_C(a,b) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\frac{1}{ab\alpha_m^2}) = 1 \text{ or } p(u) = 0 \text{ for some } u \in U \\ 2 & \text{otherwise} \end{cases}$; *and*

If $\alpha_m = 0$ *then* $\#P_C(a,b) = \begin{cases} 2^n - 2m' + \#\{(j,k) : u_{i_j} + u_{i_k} = b\} & \text{if } b = a\alpha_{m-1}^2 \\ 0 & \text{otherwise.} \end{cases}$

where $p(u) = a\alpha_m^2 u^2 + ab\alpha_m^2 u + ab\alpha_m\alpha_{m-1} + a\alpha_{m-1}^2 + b$.

By using the previous thoerem, we get the upper or lower bound of the differential uniformity of F.

Corollary 3.4. *Let* $F(x) = [0, a_m, \ldots, a_3, 1, x]$ *on* $\mathbb{F}_{2^n}$ *with* $a_3, \ldots, a_m \neq 0$. *Let* $m' = \#\{A_i : 1 \le i \le m\}$. *Then the followings are satisfied :*

(i) *If* $\alpha_m \neq 0$ *then* $\Delta_F \le 2m' + 4$.

(ii) *If* $\alpha_m = 0$ *then* $\Delta_F \ge 2^n - 2m' + 2$.

3.1 Carlitz rank of 3

Throughout this section, let $F(x) = [0, c, 1, x]$ on $\mathbb{F}_{2^n}$, which is obtained by setting $m = 3$ and $a_3 = c$ in (3). Note that in case $c = 1$, we can easily show that $\Delta_F = 2^n$. Now we consider $c \neq 1$ case, then we obtain the coefficients given by Table 1.

Table 1: The coefficients related with $F(x) = [0, c, 1, x]$ on $\mathbb{F}_{2^n}$ with $c \neq 1$.

i	0	1	2	3
α_i	0	1	1	$c+1$
β_i	1	0	1	c
A_i		0	1	$\frac{c}{c+1}$
u_i		$\frac{1}{c+1}$	$\frac{1}{c}$	0

Then by theorem 3.3 and Table 1 with $U = \{u_1, u_2, u_3\} = \{\frac{1}{c+1}, \frac{1}{c}, 0\}$, we have

$$
\begin{aligned}
&(i)\ \#P_A(a,b) = \begin{cases} 2 & \text{if } (a,b) \in \{(1,\frac{1}{c(c+1)}),(\frac{1}{c+1},\frac{1}{c}),(\frac{c}{c+1},\frac{1}{c+1})\} \\ 0 & \text{otherwise} \end{cases} \\
&(ii)\ \#P_B(a,b) = \begin{cases} 3 & \text{if } (a,b) \in C_1 := B_1 \cap B_2 \cap B_3 \\ 2 & \text{if } (a,b) \in C_2 := ((B_1 \cap B_2) \cup (B_2 \cap B_3) \cup (B_3 \cap B_1)) \setminus C_1 \\ 1 & \text{if } (a,b) \in C_3 := (B_1 \cup B_2 \cup B_3) \setminus (C_1 \cup C_2) \\ 0 & \text{otherwise} \end{cases} \\
&(iii)\ \#P_C(a,b) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\frac{1}{ab(c^2+1)}) = 1,\ b = \frac{a}{(c+1)a+1} \text{ or } b = \frac{a}{(c^2+c)a+c^2} \\ 2 & \text{otherwise} \end{cases}
\end{aligned} \tag{7}
$$

where $B_1 = \{(a,b) : b = \frac{1}{(c^2+1)a+c^2+c},\ (a,b) \neq (1,\frac{1}{c+1}),(0,\frac{1}{c^2+c}),(\frac{c}{c+1},0)\}$, $B_2 = \{(a,b) : b = \frac{a+1}{(c^2+c)a+c},(a,b) \neq (0,\frac{1}{c}),(1,0)\}$ and $B_3 = \{(a,b) : b = \frac{(c+1)a+1}{(c^2+1)a},\ (a,b) \neq (0,\frac{1}{c+1}),(\frac{1}{c+1},0)\}$.

The next lemma makes it easier to find (a,b) which makes $\mathtt{DDT}_F(a,b)$ maximum.

Lemma 3.5. *In (7) with $F(x) = [0,c,1,x]$ on $\mathbb{F}_{2^n}$ with $n \geq 3$ and $c \neq 1$, the followings are satisfied:*
(i) $\Delta_F \geq 4$.
(ii) $c \notin \mathbb{F}_4 \setminus \mathbb{F}_2$ if and only if $\#P_A(a,b)\#P_B(a,b) = 0$ for all $a,b \in \mathbb{F}_{2^n} \setminus \{0\}$, in other words neither $\#P_A(a,b)$ nor $\#P_B(a,b)$ can be positive for all $a,b \in \mathbb{F}_{2^n} \setminus \{0\}$.
(iii) Let us assume that $c \notin \mathbb{F}_4 \setminus \mathbb{F}_2$. Then

$$\Delta_F = \max_{(a,b)\in B'} \mathtt{DDT}_F(a,b)$$

where $B' = \{(a,b) : \#P_B(a,b) = \max_{a,b} \#P_B(a,b)\}$.

By using this lemma, we can induce the following proposition and theorem.

Proposition 3.6. *Let $F(x) = [0,c,1,x]$ on $\mathbb{F}_{2^n}$ with $c \neq 1$. Then the followings are satisfied :*
(i) If $c^3 + c^2 + 1 = 0$ then $\Delta_F = 8$.
(ii) If $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ then $\Delta_F = \begin{cases} 6 & \text{if } n \equiv 0 \pmod 4 \\ 4 & \text{if } n \equiv 2 \pmod 4 \end{cases}$.

Proof. (Sketch of (i)) We first consider $c^3 + c^2 + 1 = 0$ case. If $c^3 + c^2 + 1 = 0$ then we get for

$$B_1 \cap B_2 \cap B_3 = \{(\frac{1}{c^2+c}, 1)\}.$$

It is obvious that $c \notin \mathbb{F}_4$, so $\Delta_F = \mathtt{DDT}_F(\frac{1}{c^2+c}, 1)$ by lemma 3.5. Hence we obtain $\Delta_F = \mathtt{DDT}_F(\frac{1}{c^2+c}, 1) = 6 + \#P_C(\frac{1}{c^2+c}, 1) = 8$. □

Theorem 3.7. *Let $F(x) = [0,c,1,x]$ on $\mathbb{F}_{2^n}$ with $c \notin \mathbb{F}_4$ and $c^3 + c^2 + 1 \neq 0$. Then $\Delta_F \leq 6$ and the followings are satisifed:*

(i) If $\mathrm{Tr}(\frac{c}{c+1}) = \mathrm{Tr}(\frac{1}{c}) = 1$ then $\Delta_F = 4$.

(ii) *If* $\mathrm{Tr}(\frac{c}{c+1}) = 1, \mathrm{Tr}(\frac{1}{c}) = 0$ *then, letting* $\beta^2 + \beta = \frac{1}{c}$ *with* $\beta \in \mathbb{F}_{2^n}$,
– *If* n *is odd then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 0$ *if and only if* $\Delta_F = 4$.
– *If* n *is even then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 1$ *if and only if* $\Delta_F = 4$.

(iii) *If* $\mathrm{Tr}(\frac{c}{c+1}) = 0, \mathrm{Tr}(\frac{1}{c}) = 1$ *then, letting* $\gamma^2 + \gamma = \frac{1}{c+1}$ *with* $\gamma \in \mathbb{F}_{2^n}$,
it holds that $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.

(iv) *If* $\mathrm{Tr}(\frac{c}{c+1}) = \mathrm{Tr}(\frac{1}{c}) = 0$ *then,* $\beta^2 + \beta = \frac{1}{c}$ *and* $\gamma^2 + \gamma = \frac{1}{c+1}$ *with* $\beta, \gamma \in \mathbb{F}_{2^n}$,
– *If* n *is odd then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 0$ *and* $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.
– *If* n *is even then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = \mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.

Proof. (Sketch) Since $c \notin \mathbb{F}_4$ and $c^3 + c^2 + 1 \neq 0$, $\max_{a,b} \#P_B(a,b) \leq 2$, so $\Delta_F \leq 6$ by lemma 3.5. We now consider claim (i). The assumption implies that $B_1 \cap B_2 = B_2 \cap B_3 = B_3 \cap B_1 = \phi$, so that $\#P_B(a,b) \leq 1$. By lemma 3.5-$(i),(iii)$, we have $\Delta_F = 4$.

We next consider the claim (ii). The assumption implies that $B_1 \cap B_2 = B_2 \cap B_3 = \phi$ and $B_3 \cap B_1 = \{(a,b) : b = \frac{(c+1)a+1}{(c^2+1)a}, a^2 + \frac{c}{c+1}a + \frac{c}{c^2+1} = 0\}$, so we get

$$B' = \{(\tfrac{c}{c+1}\beta, \tfrac{c\beta+1}{(c^2+c)\beta}), (\tfrac{c}{c+1}(\beta+1), \tfrac{c(\beta+1)+1}{(c^2+c)(\beta+1)})\} = \{(\tfrac{\beta}{\beta^2+\beta+1}, \tfrac{\beta^3+\beta^2}{\beta^2+\beta+1}), (\tfrac{\beta+1}{\beta^2+\beta+1}, \tfrac{\beta^3+\beta}{\beta^2+\beta+1})\}.$$

where $\beta^2 + \beta = \frac{1}{c}$. For $(a,b) = (\frac{\beta}{\beta^2+\beta+1}, \frac{\beta+1}{\beta^2+\beta+1}) \in B'$, we get

$$\#P_C(a,b) = \begin{cases} 2 & \text{if } \mathrm{Tr}(\frac{\beta+1}{\beta}) = 0 \\ 0 & \text{if } \mathrm{Tr}(\frac{\beta+1}{\beta}) = 1 \end{cases}$$

by (7). For $(a,b) = (\frac{\beta+1}{\beta^2+\beta+1}, \frac{\beta^3+\beta}{\beta^2+\beta+1}) \in B'$, Therefore

$$\#P_C(a,b) = \begin{cases} 2 & \text{if } \mathrm{Tr}(\frac{\beta}{\beta+1}) = 0 \\ 0 & \text{if } \mathrm{Tr}(\frac{\beta}{\beta+1}) = 1. \end{cases}$$

by (7). Since $\Delta_F = \max_{(a,b)\in B'} \mathtt{DDT}_F(a,b)$ by lemma 3.5, $\Delta_F = 4$ if and only if $\mathrm{Tr}(\frac{\beta+1}{\beta}) = 1$ and $\mathrm{Tr}(\frac{\beta}{\beta+1}) = 1$. Note that $\mathrm{Tr}(1) = 0$ if and only if n is even, so we get the claim (ii). The claim (iii) and (iv) is simlar to the proof of claim (ii). □

Note that Theorem 3.7-(i) has been constructed in [5] but the others are new classes of differentially 4-uniform permutation polynomials.

3.2 Special case on Carlitz rank of 4

Throughout this section, let $F(x) = [0, d, 1, 1, x]$ on $\mathbb{F}_{2^n}$, which is obtained by setting $m = 4$, $a_3 = 1$ and $a_4 = d$ in (3). Similarly to the proof of Carlitz rank 3, we get the following theorem.

Theorem 3.8. *Let* $F(x) = [0, d, 1, 1, x]$ *on* $\mathbb{F}_{2^n}$ *with* $d \notin \mathbb{F}_4$. *Then* $\Delta_F = 4$ *or* $\Delta_F = 6$. *Moreover we get:*
(i) If n *is odd then* $\Delta_F = 4$.
(ii) If n *is even then* $\mathrm{Tr}(\frac{1}{d+1}) = \mathrm{Tr}(\frac{1}{d}) = 1$ *if and only if* $\Delta_F = 4$.

Note that Theorem 3.8-(ii) has been constructed in [5] but the other is new class of differentially 4-uniform permutation polynomials.

4 Conclusion

In this paper, we presented a methodology for calculating differential uniformity for low carlitz rank. As a result we found the bound of differential uniformity, so it was confirmed that the low carlitz rank guarantees a rather low differential uniformity.

We also gave a partial classification of the differential uniformity of the permutation polynomials of Carlitz rank at most 4. As a result, new classes of differentially 4-uniform permutations have been discovered. Since the permutation polynomials of low Carlitz rank are affine equivalent to inverse function except on a small subset in $\mathbb{F}_{2^n}$, and since the other cryptographic properties of the inverse function are well known, we can also find the other cryptographic invariants such as nonlinearity and Walsh spectrum of permutation polynomials with low Carlitz rank in a similar manner.

References

[1] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer International Publishing, DOI : 10.1007/978-3-319-12991-4 (2014)

[2] C. Carlet, Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, Cambridge (2010)

[3] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications 2nd Edition, Academic Press, eBook ISBN: 9780128111307 (2017)

[4] A. Çesmelioglu, W. Meidl, A. Topuzoglu, On the cycle structure of permutation polynomials, Finite Fields Appl. 14 (2008)

[5] Y. Li, M. Wang and Y. Yu, Constructing Differentially 4-uniform Permutations over $GF(2^{2k})$ from the Inverse Function Revisited, eprint.iacr.org/2013/731

[6] J. Peng, and C. Tan, New differentially 4-uniform permutations by modifying the inverse function on subfields, Crypt. Commun. 9 pp 363-378 (2017)

[7] K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 55-64, (1994)

[8] L. Qu, Y. Tan, C. Tan, and C. Li. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Information Theory, 59(7):4675–4686 (2013)

[9] D. Tang, C. Carlet and X. Tang, Differentially 4-uniform bijections by permuting the inverse function, Des. Codes. Cryptogr. 77 pp 117-141 (2015)

[10] Z. Zha, L. Hu and S. Sun, Constructing new differentially 4-uniform permutations from the inverse function, Finite Fields and Their Applications 25, pp 64-78 (2014)

On properties of a bent function secondary construction

Nikolay Kolomeec

Sobolev Institute of Mathematics, Novosibirsk, Russia

Novosibirsk State University, Novosibirsk, Russia

Laboratory of Cryptography JetBrains Research

Abstract

Properties of a secondary bent function construction, that inverts values of a given bent function on an affine subspace, are obtained. Some results regarding normal and weakly normal bent functions are generalized. Bent functions and their dual functions are considered in the construction context.

1 Preliminaries

Let us recall some definitions. *A bent function* is a Boolean function in even number of variables that is at the maximal possible Hamming distance from the set of all affine Boolean functions. Bent functions were introduced by O. Rothaus [1]. Additional information regarding them can be found in [2, 3]. Let $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$, where $x, y \in \mathbb{F}_2^n$. Let us denote by Ind_S the characteristic function of a set $S \subseteq \mathbb{F}_2^n$ and by $D_\alpha f(x) = f(x) \oplus f(x \oplus \alpha)$ *the derivative* of a Boolean function f *in the direction* α. For $x \in \mathbb{F}_2^n$ and $k \le n$, let us define

$$\begin{aligned} Proj_k(x) &= (x_1, \ldots, x_k), \\ Proj_k(S) &= \{Proj_k(x) \mid x \in S\}, \\ Elem_k(S) &= \{x \in \mathbb{F}_2^k \mid (x, \underbrace{0, \ldots, 0}_{n-k}) \in S\}. \end{aligned}$$

Hereinafter we suppose that n is even. By $\mathcal{B}_n$ we denote the set of all bent functions in n variables, by $\widetilde{f}$ *the dual* bent function of $f \in \mathcal{B}_n$.

In this work, we consider properties of a bent function construction

$$f \oplus Ind_U,$$

where $f \in \mathcal{B}_n$ is a given bent function and U is an affine subspace of an arbitrary dimension. Necessary and sufficient conditions for $f \oplus Ind_U$ to be a bent function were proven by C. Carlet [4].

Theorem 1.1 (C. Carlet, 1994) *Let $f \in \mathcal{B}_n$, $L \subseteq \mathbb{F}_2^n$ be a linear subspace and $a \in \mathbb{F}_2^n$. Then $f \oplus Ind_{a\oplus L}$ is a bent function if and only if any of the following equivalent conditions hold:*

- *$D_\alpha f$ is balanced on $a \oplus L$ for all $\alpha \in \mathbb{F}_2^n \setminus L$;*
- *$\widetilde{f}(x) \oplus \langle a, x\rangle$ is either constant or balanced on each coset of $L^\perp$.*

We will use the second condition. The next two sections describe properties of a dual bent function $\widetilde{f}$.

2 A balanced representation

Let us introduce the following notion.

Definition 2.1 *A Boolean function f in n variables has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$ if f is either constant or balanced on each coset of L.*

Note that any function has a balanced representation by the 0-dimensional linear subspace ("either constant or balanced" case allows us to ignore its odd cardinality). The same situation holds for a 1-dimensional linear subspace.

First of all, there are some additional details regarding balanced representations of bent functions.

Theorem 2.2 *Let $f \in \mathcal{B}_n$ and L be a linear subspace, $\dim L \leq n/2$. Then*

- *f has a balanced representation by L if and only if f is constant on each of some $2^{n-2\dim L}$ distinct cosets of L;*
- *f can not be constant on more than $2^{n-2\dim L}$ distinct cosets of L.*

Note that the case $\dim L = n/2$ is especially interesting for bent functions. A large class of normal bent functions for this representation was introduced by H. Dobbertin [5].

3 A balanced representation of iterative constructed functions

Let us consider the simplest iterative construction of a bent function f_{+2} by $f \in \mathcal{B}_n$:

$$f_{+2}(x_1, \ldots, x_{n+2}) = f(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Recall that $f_{+2} \in \mathcal{B}_{n+2}$ if and only if $f \in \mathcal{B}_n$. Also, it holds

$$\widetilde{f_{+2}}(x_1, \ldots, x_{n+2}) = \widetilde{f}(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

The question is the following: whether the balanced representations for f and f_{+2} are connected or not.

Proposition 3.1 *Let $f \in \mathcal{B}_n$ have a balanced representation by $L \subseteq \mathbb{F}_2^n$. Then the bent function f_{+2} has balanced representations by*

- *$L_0 = \{(x, 0, 0) \mid x \in L\}$, i. e. $\dim L_0 = \dim L$;*
- *$L_1 = \{(x, y, 0) \mid x \in L, y \in \mathbb{F}_2\}$, i. e. $\dim L_1 = \dim L + 1$.*

Moreover, there is a "feedback" from the f_{+2} to f.

Theorem 3.2 *Let $f \in \mathcal{B}_n$ and suppose that f_{+2} have a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$ with*

$$\dim L - 1 \leq \dim L' \leq \dim L$$

such that f has a balanced representation by L'. Moreover, it holds

$$Elem_n(L) \subseteq L' \subseteq Proj_n(L).$$

In case $\dim L = n/2 + 1$ Theorem 3.2 can be easily transformed to "f is normal if and only if f_{+2} is normal" that was proven in [6]. I. e. it is a generalization of weakly normal and normal bent function properties.

4 Subspaces for iterative constructed functions

Using Theorem 1.1, the results of Section 3 can be generalized to the construction properties.

Proposition 4.1 *Let $f \in \mathcal{B}_n$ and $f \oplus Ind_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$. Then for the bent function f_{+2} the following statements hold:*

- $f_{+2} \oplus Ind_{U_1} \in \mathcal{B}_{n+2}$, *where* $U_1 = \{(x, y, 0) \mid x \in U, y \in \mathbb{F}_2\}$, *i. e.* $\dim U_1 = \dim U + 1$;
- $f_{+2} \oplus Ind_{U_2} \in \mathcal{B}_{n+2}$, *where* $U_2 = \{(x, y, z) \mid x \in U, y, z \in \mathbb{F}_2\}$, *i. e.* $\dim U_2 = \dim U + 2$.

Theorem 4.2 *Let $f_{+2} \in \mathcal{B}_{n+2}$ and $f_{+2} \oplus Ind_{a \oplus L} \in \mathcal{B}_{n+2}$, where $L \subseteq \mathbb{F}_2^{n+2}$ is a linear subspace, $a \in \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$ with*

$$\dim L - 2 \leq \dim L' \leq \dim L - 1$$

such that $f \oplus Ind_{Proj_n(a) \oplus L'} \in \mathcal{B}_n$. Moreover, it holds

$$Elem_n(L) \subseteq L' \subseteq Proj_n(L).$$

Similarly to Theorem 3.2, in case $\dim L = n/2 + 1$, Theorem 4.2 can be reformulated in terms of weakly normal bent function properties.

Trivial subspace dimensions for $f \in \mathcal{B}_n$ are n (just negation of the function) and $n - 1$ (addition of an affine function). We can naturally exclude these dimensions from the construction.

Computational experiments (see Section 5) show that for the non-weakly normal bent function $f_{10} \in \mathcal{B}_{10}$ found in [7] (Fact 14) the following fact holds.

Fact 4.3 *For any affine subspace $U \subseteq \mathbb{F}_2^{10}$, $\dim U \leq 8$, it holds that $f_{10} \oplus Ind_U \notin \mathcal{B}_{10}$.*

Corollary 4.4 *For any $n \geq 10$, there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus \mathrm{Ind}_U \notin \mathcal{B}_n$ for any affine subspace $U \subseteq \mathbb{F}_2^n$ of dimension at most $n/2 + 3$.*

5 Search subspaces

For a given $f \in \mathcal{B}_n$, the algorithm described in [6] can help to construct all affine subspaces $U \subseteq \mathbb{F}_2^n$ (of an arbitrary dimension) such that $f \oplus Ind_U \in \mathcal{B}_n$. Though it constructs affine subspaces such that f is affine on each of them, it "sorts" cosets for a convenient usage in a balanced representation.

The algorithm complexity can be calculated in the following way:

$$n \sum_{m=1}^{n/2} \left(|L_m(\widetilde{f})| + (2^m - 2)|L_m^0(\widetilde{f})| \right) + \mathcal{O}(n2^n),$$

where $L_m(f)$ ($L_m^0(f)$) is the set of an m-dimensional affine subspaces such that f is affine (constant) on them.

6 Count of the constructed functions

For $f \in \mathcal{B}_n$ and $0 \leq m \leq n$, we define

$$Constr_m(f) = \{f \oplus Ind_U \mid U \text{ is an } m\text{-dimensional affine subspace of } \mathbb{F}_2^n\} \cap \mathcal{B}_n.$$

Theorem 6.1 *Let $f \in \mathcal{B}_n$ and $f \oplus Ind_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$ of dimension at most $n/2 + 1$. Then*

$$\mathrm{supp}\{\widetilde{f} \oplus \widetilde{(f \oplus Ind_U)}\}$$

is an affine subspace too.

Corollary 6.2 $|Constr_m(f)| = |Constr_m(\widetilde{f})|$ *for* $m \le n/2 + 1$.

Unlike $n/2$ and $n/2 + 1$ dimensions, for other cases we have

- $\mathrm{supp}\{\widetilde{f} \oplus \widetilde{(f \oplus Ind_U)}\}$ may not be an affine subspace;
- $|Constr_m(f)|$ and $|Constr_m(\widetilde{f})|$ may not be equal; such bent functions in 8 variables exist, for instance, in Maiorana–McFarland class [8].

Thus, for an arbitrary subspace dimensions, some construction properties differ from the case $m = n/2$.

It is well known that $|Constr_m(f)| = 0$ for $m < n/2$. The following theorem estimates cardinalities of all other $Constr_m(f)$.

Theorem 6.3 *For* $f \in \mathcal{B}_n$ *and* $m \ge n/2$, *it holds*

$$|Constr_m(f)| \le 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{2m+2i-n} - 1}{2^i - 1}.$$

Moreover, for $m \le n - 2$, *the bound is reached if and only if* f *is quadratic.*

This estimate generalizes the bound from [9] for the case $m = n/2$.

Acknowledgement

The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314–2019–0017) and supported by Russian Foundation for Basic Research (project no. 20–31–70043) and Laboratory of Cryptography JetBrains Research.

References

[1] O. Rothaus *On bent functions.* J. Combin. Theory. Ser. A, 20(3), 300–305, 1976.

[2] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko *Boolean Functions in Coding Theory and Cryptography.* American Mathematical Society, 2012.

[3] N. Tokareva *Bent Functions, Results and Applications to Cryptography.* Acad. Press. Elsevier, 2015.

[4] C. Carlet *Two new classes of bent functions.* LNCS, 765, 77–101, 1994.

[5] H. Dobbertin *Construction of bent functions and balanced Boolean functions with high nonlinearity.* LNCS, 1008, 61–74, 1995.

[6] A. Canteaut, M. Daum, H. Dobbertin, G. Leander. *Finding nonnormal bent functions.* Discrete Appl. Math., 154(2), 202–218, 2006.

[7] G. Leander, G. McGuire *Construction of bent functions from near-bent functions.* J. Combin. Theory. Ser. A, 116(4), 960–970, 2009.

[8] R. L. McFarland *A family of difference sets in non-cyclic groups* J. Combin. Theory. Ser. A, 15, 1–10, 1973.

[9] N. Kolomeec *The graph of minimal distances of bent functions and its properties.* Designs, Codes and Cryptography, 85(3), 395–410, 2017.

On metrical properties of self-dual generalized bent functions

Kutsenko Aleksandr*

Sobolev Institute of Mathematics, Novosibirsk, Russia

Novosibirsk State University, Novosibirsk, Russia

Abstract

Bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$ (K.-U Schmidt, 2006) are known as generalized bent (gbent) functions. In this paper we study self-dual generalized bent functions and some their metrical properties for the Hamming and Lee distance. Necessary and sufficient conditions for self-duality of Maiorana–McFarland gbent functions are given. We find the complete Hamming and Lee distance spectrums between self-dual Maiorana–McFarland gbent functions and, as a corollary, we obtain minimal distances between considered self-dual gbent functions. We prove that the set of quaternary self-dual gbent functions is metrically regular for the Lee distance. The mapping of the set of all generalized Boolean functions in n variables to itself is called isometric if it preserves the distance between any pair of functions. We consider the mappings obtained by a generalization of isometric mappings of the set of all Boolean functions in n variables to itself. Within this generalization we propose an isometric mapping that preserves both Hamming and Lee distances and transforms the set of (anti-)self-dual gbent functions to itself.

Let $\mathbb{F}_2^n$ be a set of binary vectors of length n. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$, where the sign $\oplus$ denotes a sum modulo 2.

A *generalized Boolean function* f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$, the integers modulo q. The set of generalized Boolean functions in n variables is denoted by $\mathcal{GF}_n^q$, for the Boolean case ($q = 2$) we use the notation $\mathcal{F}_n$. Let $\omega = e^{2\pi i/q}$. A *sign* function of $f \in \mathcal{GF}_n^q$ is a complex valued function ω^f, we will also refer to it as to a complex vector $\left(\omega^{f_0}, \omega^{f_1}, ..., \omega^{f_{2^n-1}}\right)$ of length 2^n, where $(f_0, f_1, ..., f_{2^n-1})$ is a vector of values of the function f.

The *Hamming weight* $\mathrm{wt}_H(x)$ of the vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates of x. The *Hamming distance* $\mathrm{dist}_H(f, g)$ between generalized Boolean functions f, g in n variables is the cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$. The Lee weight of the element $x \in \mathbb{Z}_q$ is $\mathrm{wt}_L(x) = \min\{x, q - x\}$. The Lee distance $\mathrm{dist}_L(f, g)$ between $f, g \in \mathcal{GF}_n^q$ is

$$\mathrm{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L\left(\delta(x)\right),$$

where $\delta \in \mathcal{GF}_n^q$ and $\delta(x) = f(x) + (q-1)g(x)$ for any $x \in \mathbb{F}_2^n$. For Boolean case $q = 2$ the Hamming distance coincides with the Lee distance.

The *(generalized) Walsh–Hadamard transform* of $f \in \mathcal{GF}_n^q$ is the complex-valued function:

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}.$$

A generalized Boolean function f in n variables is said to be *generalized bent* (gbent) if

$$|H_f(y)| = 2^{n/2},$$

*The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (project no. 18-07-01394, 20-31-70043) and Laboratory of Cryptography JetBrains Research.

for all $y \in \mathbb{F}_2^n$ [9]. If there exists such $\widetilde{f} \in \mathcal{GF}_n^q$ that $\mathcal{H}_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$, the gbent function f is said to be *regular* and $\widetilde{f}$ is called its *dual*. Note that $\widetilde{f}$ is generalized bent as well. A regular gbent function f in said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} + \frac{q}{2}$. Consequently, it is the case only for even q. So throughout this paper we assume that q is a natural even number.

A survey on different generalizations of bent functions can be found in [12].

Denote, according to [3], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in GL\left(n, \mathbb{F}_2\right) | LL^T = I_n \right\},$$

where L^T denotes the transpose of L and I_n is an identical matrix of order n over the field $\mathbb{F}_2$.

Bent functions in $2k$ variables which have a representation

$$f(x, y) = \langle x, \pi(y) \rangle \oplus g(y),$$

where $x, y \in \mathbb{F}_2^k$, $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a Boolean function in k variables, form the well known *Maiorana–McFarland* class of bent functions. It is known [1] that a dual of a Maiorana–McFarland bent function $f(x, y)$ is equal to

$$\widetilde{f}(x, y) = \langle \pi^{-1}(x), y \rangle \oplus g\left(\pi^{-1}(x)\right).$$

A generalization of this construction for the case $q = 4$ was given by Schmidt in [9]. In [11] this construction was given for any even q, thus, forming the following construction

$$f(x, y) = \frac{q}{2} \langle x, \pi(y) \rangle + g(y),$$

where $x, y \in \mathbb{F}_2^k$, $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a generalized Boolean function in k variables. Its dual is

$$\widetilde{f}(x, y) = \frac{q}{2} \langle \pi^{-1}(x), y \rangle + g\left(\pi^{-1}(x)\right).$$

In the article [2] necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions, were given. In [10] quaternary self-dual Maiorana–McFarland bent functions were studied and necessary and sufficient conditions of self-duality were obtained for them.

In the current work we generalize these results for any even q. Denote the sets of self-dual and anti-self-dual generalized Maiorana–McFarland bent functions by $\mathrm{SB}^+_{\mathcal{GM}^q}(n)$ ($\mathrm{SB}^-_{\mathcal{GM}^q}(n)$). For the Boolean case ($q = 2$) we will use the notation $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$).

Theorem 0.1 *A generalized Maiorana–McFarland bent function*

$$f(x, y) = \frac{q}{2} \langle x, \pi(y) \rangle + g(y), \ x, y \in \mathbb{F}_2^{n/2},$$

is (anti-)self-dual bent if and only if for any $y \in \mathbb{F}_2^{n/2}$

$$\pi(y) = L\left(y \oplus b\right), \quad g(y) = \frac{q}{2} \langle b, y \rangle + d,$$

where $L \in \mathcal{O}_{n/2}, b \in \mathbb{F}_2^{n/2}$, $\mathrm{wt}\,(b)$ *is even (odd),* $d \in \mathbb{Z}_q$.

It follows that the number of such functions is a function of q and the cardinality of the orthogonal group.

Corollary 0.2 *It holds*

$$\left|\mathrm{SB}^+_{\mathcal{GM}^q}(n)\right| = \left|\mathrm{SB}^-_{\mathcal{GM}^q}(n)\right| = q \cdot 2^{n/2-1} \left|\mathcal{O}_{n/2}\right|.$$

In paper [4] the possible Hamming distances between (anti-)self-dual Maiorana–McFarland bent functions for the Boolean case were studied and the complete Hamming distances spectrum was presented, namely it was shown that for $f, g \in \mathrm{SB}^{+}_{\mathcal{M}}(n) \cup \mathrm{SB}^{-}_{\mathcal{M}}(n)$, then

$$\mathrm{dist}(f,g) \in \left\{ 2^{n-1}, 2^{n-1}\left(1 \pm \frac{1}{2^r}\right), r = 0, 1, ..., n/2-1 \right\}.$$

Moreover, it was shown that if either $f, g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$ or $f, g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$, then all distances given above are attainable. If f is self-dual bent and g is anti-self-dual bent, then $\mathrm{dist}(f,g) = 2^{n-1}$.

In the current work we generalize this result for any even q in both Hamming and Lee distances. Denote the mentioned spectrum for the Hamming distance by $\mathrm{Sp}_H\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right)$, while for the Lee distance the notation $\mathrm{Sp}_L\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right)$ is used. The Hamming distance spectrum is described by the following

Theorem 0.3 *It holds*

$$\mathrm{Sp}_H\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right) = \left\{2^{n-1}\right\} \cup \bigcup_{r=0}^{n/2-1} \left\{ 2^{n-1}\left(1 \pm \frac{1}{2^r}\right) \right\}.$$

Moreover, all given distances are attainable.

The Lee distance spectrum is characterized by

Theorem 0.4 *It holds*

$$\mathrm{Sp}_L\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right) = \left\{q \cdot 2^{n-2}\right\} \cup \bigcup_{\mathrm{w}=0}^{q/2} \bigcup_{r=0}^{n/2-1} \left\{ q \cdot 2^{n-2}\left(1 \pm \frac{1}{2^r}\right) \mp \mathrm{w} \cdot 2^{n-r} \right\}.$$

Moreover, all given distances are attainable.

It is possible to derive the minimal distances from these spectrums.

Proposition 0.5 *The minimal Lee distance between generalized (anti-)self-dual Maiorana–McFarland bent functions in n variables is equal to $2^{n-3}q$, while the minimal Hamming distance is 2^{n-2}.*

Recall that $\mathrm{RM}_q(r,m)$ is the length 2^m linear code over $\mathbb{Z}_q$ that is generated by the monomials of order at most r in variables $x_1, x_2, ..., x_m$, its minimal Lee distance is equal to 2^{m-r} [8]. Hence for $\mathrm{RM}_q(2,m)$ minimal Lee distance is equal to 2^{n-2}. From the obtained results it follows that

Corollary 0.6 *The minimal Lee distance 2^{n-2} between quadratic (generalized) bent functions is attainable on (anti-)self-dual Maiorana–McFarland bent functions from $\mathcal{GM}^q_n$ only for $q = 2$ while the minimal Hamming distance 2^{n-2} is attainable on such functions for any even $q \geqslant 2$.*

Let $X \subseteq \mathbb{Z}_q^n$ be an arbitrary set and let $y \in \mathbb{Z}_q^n$ be an arbitrary vector. Define the *distance* between y and X as $\mathrm{dist}(y, X) = \min\limits_{x \in X} \mathrm{dist}(y, x)$. The *maximal distance* from the set X is

$$\mathrm{d}(X) = \max_{y \in \mathbb{Z}_q^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{Z}_q^n$ is called *maximally distant* from the set X if $\mathrm{dist}(z, X) = \mathrm{d}(X)$. The set of all maximally distant vectors from the set X is called the *metrical complement* of the set X and denoted by $\widehat{X}$. A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$. A subset of Boolean functions is said to be *metrically regular* if the set of corresponding vectors of values is metrically regular [13].

In paper [5] it was proved that the set of Boolean self-dual bent functions is metrically regular within the Hamming distance. In current work we prove that within Lee distance this statement holds for the quaternary case $q = 4$ as well.

Theorem 0.7 *The sets of (anti-)self-dual generalized quaternary bent functions are metrically regular for the Lee distance.*

A mapping φ of the set of all (generalized) Boolean functions in n variables to itself is called *isometric* if it preserves the distance between functions, that is,

$$\mathrm{dist}(\varphi(f), \varphi(g)) = \mathrm{dist}(f, g)$$

for any $f, g \in \mathcal{GF}_n$. From Markov's theorem (1956) [7] it follows that the general form of isometric mappings of the set of all Boolean functions in n variables to itself is

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$ [7]. In [6] all isometric mappings of the set of all Boolean functions in n variables to itself, that preserve (anti-)self-duality of a bent function were characterized.

In the current work we consider the mappings of the set of all generalized Boolean functions in n variables to itself, which have the form

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{GF}_n$. It is clear that such mappings preserve both Hamming and Lee distances between generalized Boolean functions.

The following result provides the construction of isometric mappings that preserve both self-duality anti-self-duality of a gbent function.

Theorem 0.8 *The isometric mapping of the set of all generalized Boolean functions in n variables to itself of the form*

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

with

$$\pi(x) = L\left(x \oplus c\right), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{Z}_q$, preserves (anti-)self-duality of a gbent function.

References

[1] Carlet C. Boolean functions for cryptography and error correcting code. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. p. 257–397. Cambridge University Press, Cambridge (2010).

[2] Carlet C., Danielson L.E., Parker M.G., Solé. P., *Self-dual bent functions.* Int. J. Inform. Coding Theory, **1**, 384–399 (2010).

[3] Janusz G.J., Parametrization of self-dual codes by orthogonal matrices, Finite Fields Appl., **13**(3), 450–491 (2007).

[4] Kutsenko A.V., *The Hamming Distance Spectrum Between Self-Dual Maiorana–McFarland Bent Functions*, Journal of Applied and Industrial Mathematics, **12**(1), 112–125 (2018).

[5] Kutsenko A., *Metrical properties of self-dual bent functions*, Des. Codes Cryptogr. **88**, 201–222 (2020).

[6] Kutsenko A., *The group of automorphisms of the set of self-dual bent functions*, Cryptogr. Commun. (2020). DOI: 10.1007/s12095-020-00438-y

[7] Markov A. A., *On transformations without error propagation.* In: Selected Works, Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, p. 70–93, MTsNMO, Moscow (2003) [Russian].

[8] Paterson K.G., Jones A.E., *Efficient decoding algorithms for generalized Reed–Muller codes.* IEEE Trans. Commun., vol. 48, no. 8, pp. 1272–1285, 2000.

[9] Schmidt K.-U., *Quaternary constant-amplitude codes for multicode CDMA.* IEEE Trans. Inform. Theory, **55**, 1824–1832 (2009).

[10] Sok L., Shi M., Solé P., *Classification and Construction of quaternary self-dual bent functions.* Cryptogr. Commun. **10**(2), 277–289 (2018).

[11] Stănică P., Martinsen T., Gangopadhyay S., Singh B. K., *Bent and generalized bent Boolean functions.* Des. Codes Cryptogr. **69**, 77–94 (2013).

[12] Tokareva N.N., *Generalizations of bent functions — a survey.* J. Appl. Ind. Math. **5**(1), 110–129 (2011).

[13] Tokareva N., *Bent Functions, Results and Applications to Cryptography.* Acad. Press. Elsevier, 2015.

Walsh zero spaces of APN functions

Petr Lisoněk

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada

Abstract

We report on work in progress that is motivated by the "Big APN Problem" that concerns the existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n \geq 8$. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We define a Walsh zero space (WZ space) of f to be any $\mathbb{F}_2$-linear n-dimensional space of Walsh zeros of f. This definition is motivated by the fact that a function is CCZ-equivalent to a permutation if and only if it possesses a pair of WZ spaces that intersect trivially. We discuss characterization of Walsh zeros and construction of WZ spaces for quadratic functions, and we include examples and results for Gold functions and for the function $f(x) = x^3 + \mathrm{Tr}(x^9)$.

1 Background

Let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *almost perfect nonlinear (APN)* if for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, the equation $f(x + a) - f(x) = b$ has at most two solutions $x \in \mathbb{F}_{2^n}$. Without loss of generality, we can normalize any APN function such that $f(0) = 0$, and we will assume this throughout.

APN functions, and more generally functions with low differential uniformity, have been extensively studied due to their importance in the design of S-boxes of block ciphers in cryptography, where they offer the best possible protection against the differential cryptanalysis attack. In some block cipher designs, such as substitution-permutation networks (SPN), it is required that S-boxes are invertible mappings. Of special interest are therefore APN functions which are invertible, that is, they are *permutations* of $\mathbb{F}_{2^n}$. Many APN permutations of $\mathbb{F}_{2^n}$ are known for odd n. It is known that APN permutations of $\mathbb{F}_{2^n}$ do not exist for $n = 2, 4$. An APN permutation of $\mathbb{F}_{2^6}$ was discovered in 2009 [2]. We will briefly describe the method by which it was found. Our description is somewhat different from [2] but it is equivalent.

Let Tr_s^n denote the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^s}$. The absolute trace Tr_1^n will be denoted simply as Tr. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. For $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ we define the Walsh transform of f at (a, b) as $\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax + bf(x))}$. We say that (a, b) is a *Walsh zero* of f if $\mathcal{W}_f(a, b) = 0$. The *Walsh spectrum* of f is the set $\{\mathcal{W}_f(a, b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$.

Definition 1.1 *Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that S is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\dim_{\mathbb{F}_2} S = n$ and each element of S except $(0, 0)$ is a Walsh zero of f. We say that S is a* WZ space *of f.*

Note that $\mathbb{F}_{2^n} \times \{0\}$ is a WZ space of any function on $\mathbb{F}_{2^n}$. We say that two WZ spaces S, T of the same function *intersect trivially* if $S \cap T = \{(0, 0)\}$.

The *CCZ-equivalence* of functions was introduced by Carlet, Charpin and Zinoviev in [4]. It has many important features, in particular it preserves the APN property. The construction of APN permutation of $\mathbb{F}_{2^6}$ in [2] consists of choosing a certain APN function κ on $\mathbb{F}_{2^6}$, and then finding a permutation of $\mathbb{F}_{2^6}$ that is CCZ-equivalent to κ. For the latter task, the following characterization is used in [2], which we present in a different but equivalent form.

Proposition 1.2 *[2] Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that $f(0) = 0$. Then f is CCZ-equivalent to a permutation of $\mathbb{F}_{2^n}$ if and only if there exist two WZ spaces of f that intersect trivially.*

The existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n \geq 8$ is an important open problem, and it is called "The Big APN Problem" in [2].

Keeping in mind the approach of [2], one can attack this problem by considering a known APN function and using Proposition 1.2 to determine if it is CCZ-equivalent to a permutation. The first general results in this direction (i.e., involving infinite families of functions) were announced by Göloğlu (joint work with Langevin) in 2015 at the conference Fq12 [6]. Their work presently exists as preprint [7]. According to [7], Gold APN functions $f(x) = x^{2^k+1}$, where $\gcd(k, n) = 1$, are never CCZ-equivalent to permutations of $\mathbb{F}_{2^n}$ when n is even, and Kasami APN functions $f(x) = x^{2^{2k}-2^k+1}$, where $\gcd(k, n) = 1$, are never CCZ-equivalent to permutations of $\mathbb{F}_{2^n}$ when n is divisible by 4 (with the case $n \equiv 2 \pmod 4$ remaining open).

2 Characterizing WZ spaces

In order to complement the previous work, we envision a different approach, while still employing Proposition 1.2. In [7] the non-existence of two trivially intersecting WZ spaces is argued by assuming the contrary and driving this assumption to a contradiction. Instead, we plan to characterize many (preferably all) WZ spaces for a given APN function, and show the non-existence of two trivially intersecting WZ spaces in that way. This approach has some advantages. Examples of WZ spaces can be found with computer aid, which can inform the theoretical proofs. At the same time, this proof method can also target discovery of a trivially intersecting pair of WZ spaces should it in fact exist, which is something that the proof by contradiction can not target as an objective. Furthermore, computer searches suggest that some APN functions (such as Kasami and Dobbertin functions) may posses *only one* WZ space, namely the space $\mathbb{F}_{2^n} \times \{0\}$. This assertion can be then set as the proof objective instead of the original objective.

2.1 Quadratic functions

We give further details for the case when the APN function is *quadratic,* that is, assuming that the function is expressed in its unique polynomial form, then the exponent of each monomial has binary weight at most 2. We note that the function κ used to construct the APN permutation in dimension 6 is quadratic [2].

To characterize the WZ spaces of an APN function f we first have to characterize the Walsh zeros of f. One possible way to do this is known as the "squaring method" that computes $(\mathcal{W}_f(a, b))^2$, and it is often used to determine the entire Walsh spectrum of f. It associates a certain linear form $\mathcal{L}_b$ to f and (a, b). As the symbol suggests, the linear form depends on b but not on a. Then (a, b) is a Walsh zero of f if $\mathrm{Tr}(f(x))$ does not vanish completely on the kernel of $\mathcal{L}_b$. For the APN function $f(x) = x^3 + \mathrm{Tr}(x^9)$ this computation was carried out in detail by Bracken et al. in Section 2 of [1], see in particular equation (6) there. This computation was further generalized by Budaghyan et al. in [3] to compute Walsh spectra (hence, implicitly, also Walsh zeros) of the more general families of APN functions denoted F_0, F_1 and F_2 in [3]. In order to upper bound the cardinality of the kernel of the linear form, both [1] and [3] apply an ad-hoc method developed earlier by Dobbertin [5].

It is worth noting that for investigations of such kernels one can apply a more systematic theory developed by van der Geer and van der Vlugt [8]. While a more detailed exposition would exceed the size limit of this abstract, we at least survey the results that one obtains in this way for two families of quadratic APN functions.

Proposition 2.1 *Let n be even, $\gcd(k, n) = 1$, and $a, b \in \mathbb{F}_{2^n}$. If $b \neq 0$, then (a, b) is a Walsh zero of the Gold function $f(x) = x^{2^k+1}$ if and only if b is a (2^k+1)th power in $\mathbb{F}_{2^n}$ (equivalently, b is a cube in $\mathbb{F}_{2^n}$) and $\mathrm{Tr}_2^n(az) \neq 0$ for each $z \in \mathbb{F}_{2^n}$ such that $bz^{2^k+1} + 1 = 0$.*

Proposition 2.2 *Let n be even and $a, b \in \mathbb{F}_{2^n}$.*
(i) If $b \neq 0$ and $\mathrm{Tr}(b) = 0$ then (a, b) is a Walsh zero of $f(x) = x^3 + \mathrm{Tr}(x^9)$ if and only if it is a Walsh zero of $f(x) = x^3$.

(ii) If $\mathrm{Tr}(b) = 1$*, let* x^* *be the unique solution of* $x^9 + x^3 + bx + 1 = 0$ *in* $\mathbb{F}_{2^n}$*. Then* (a, b) *is a Walsh zero of* $f(x) = x^3 + \mathrm{Tr}(x^9)$ *if and only if* x^* *is a cube in* $\mathbb{F}_{2^n}$ *and* $\mathrm{Tr}_2^n(az) \neq 0$ *for each* $z \in \mathbb{F}_{2^n}$ *such that* $z^3 = x^*$*.*

We note that these characterizations are enabled by the fact that in *both* cases the kernels are either trivial or they are cosets of $\mathbb{F}_4$, where z denotes any non-zero element of the kernel in both propositions. This naturally leads to applying trace to $\mathbb{F}_4$. While Proposition 2.1 is likely "folklore" (as remarked in [7]), on the other hand Proposition 2.2 appears to characterize the kernels more explicitly than in [1].

Equipped with the previous two propositions we can construct some non-trivial WZ spaces for the two families of APN functions under consideration.

Proposition 2.3 *Let* n *be even and* $\gcd(k, n) = 1$*. Let* $u \in \mathbb{F}_{2^n}^*$*. The set*

$$G_{k,u} = \{(a, 0) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 0\} \cup \{(a, u^{-(2^k+1)}) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 1\}$$

is a WZ space of the Gold function $f(x) = x^{2^k+1}$ *on* $\mathbb{F}_{2^n}$*.*

Proposition 2.4 *Let* n *be even and* $f(x) = x^3 + \mathrm{Tr}(x^9)$*. Let* $b \in \mathbb{F}_{2^n}^*$*.*
(i) If $\mathrm{Tr}(b) = 0$ *and* b *is a cube in* $\mathbb{F}_{2^n}$*, then* $G_{1,u}$ *is a WZ space of* f *where* u *is any of the cube roots of* $1/b$*.*
(ii) If $\mathrm{Tr}(b) = 1$ *then let* x^* *be the unique solution of* $x^9 + x^3 + bx + 1 = 0$ *in* $\mathbb{F}_{2^n}$*. If* x^* *is a cube in* $\mathbb{F}_{2^n}$ *and* u *is any of the cube roots of* x^**, then the set*

$$S_u = \{(a, 0) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 0\} \cup \{(a, b) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 1\}$$

is a WZ space of f*.*

3 Outlook

This work is currently in progress. We hope that it would lead to an alternative and possibly simpler proof of CCZ-inequivalence of APN Gold functions with permutations in even dimensions. Computer searches suggest that in certain dimensions (e.g., $n = 8$) the spaces $G_{k,u}$ given in Proposition 2.3 and the space $\mathbb{F}_{2^n} \times \{0\}$ are the only WZ spaces of the Gold function. While additional WZ spaces will possibly exist in other dimensions, it seems that a complete classification of WZ spaces should be within reach for the Gold functions. As well, we will study Walsh zero sets of other families of quadratic APN functions with the view of possibly finding functions with richer sets of WZ spaces.

References

[1] C. Bracken, E. Byrne, N. Markin, G. McGuire, On the Walsh spectrum of a new APN function. Cryptography and coding, 92–98, Lecture Notes in Comput. Sci., 4887, Springer, Berlin, 2007.

[2] K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe, An APN permutation in dimension six. Finite fields: theory and applications, 33–42, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[3] L. Budaghyan, T. Helleseth, N. Li, B. Sun, Some results on the known classes of quadratic APN functions. Codes, cryptology and information security, 3–16, Lecture Notes in Comput. Sci., 10194, Springer, Cham, 2017.

[4] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15 (1998), no. 2, 125–156.

[5] H. Dobbertin, Another proof of Kasami's theorem. Des. Codes Cryptogr. 17 (1999), no. 1–3, 177–180.

[6] F. Göloğlu, Almost perfect nonlinear functions which are not equivalent to permutations. Fq12 conference abstract, July 2015.
Available at https://www.skidmore.edu/fq12/uploads/all-abstracts.pdf

[7] F. Göloğlu, P. Langevin, APN families which are not equivalent to permutations. Preprint, 22 March 2019. (private communication)

[8] G. van der Geer, M. van der Vlugt, Reed-Muller codes and supersingular curves. I. Compositio Math. 84 (1992), no. 3, 333–367.

Bent and $\mathbb{Z}_{2^k}$-bent functions from spread-like partitions

Wilfried Meidl* and Isabel Pirsic*

*RICAM, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

Abstract

Bent functions from a vector space $\mathbb{V}_n$ over $\mathbb{F}_2$ of even dimension $n = 2m$ into the cyclic group $\mathbb{Z}_{2^k}$, or equivalently, relative difference sets in $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ with forbidden subgroup $\mathbb{Z}_{2^k}$, can be obtained from spreads of $\mathbb{V}_n$ for any $k \leq n/2$. In this talk we show the existence of bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k \geq 3$, which do not come from the spread construction. We present a construction of bent functions from $\mathbb{V}_n$ into $\mathbb{Z}_{2^k}$, $k \leq n/6$, (and more general, into any abelian group of order 2^k) obtained from partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which can be seen as a generalization of the Desarguesian spread. As for the spreads, the union of a certain fixed number of sets of these partitions is always the support of a Boolean bent function. Finally we discuss generalizations to odd characteristic.

1 Introduction

Let $(A, +_A)$, $(B, +_B)$ be finite abelian groups. A function f from A to B is called a *bent function* if

$$|\sum_{x \in A} \chi(x, f(x))| = \sqrt{|A|} \tag{1}$$

for every character χ of $A \times B$ which is nontrivial on B. Equivalently, $f : A \to B$ is bent if the graph of f, $G = \{(x, f(x)) : x \in A\}$, is a *relative difference set* in $A \times B$ relative to B.

In the classical case, $A = \mathbb{V}_n$ and $B = \mathbb{V}_m$ are elementary abelian 2-groups, i.e., they are vector spaces of dimension n and m respectively over the prime field $\mathbb{F}_2$. By (1), $F : \mathbb{V}_n \to \mathbb{V}_m$ is bent, if $m > 1$ also called *vectorial bent*, if and only if the character sum

$$\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{V}_n} (-1)^{\langle a, f(x) \rangle_m \oplus + \langle b, x \rangle_n}$$

has absolute value $2^{n/2}$ for all nonzero $a \in \mathbb{V}_m$ and $b \in \mathbb{V}_n$, (here $\langle , \rangle_k$ denotes an inner product in $\mathbb{V}_k$). As is well known, n must then be even and m can be at most $n/2$. There are many examples and constructions of Boolean bent functions ($m = 1$) in the literature. Even several classes of bent functions from $\mathbb{V}_n$ to $\mathbb{V}_{n/2}$ are known, such as Maiorana-McFarland functions, Dillons H-class, see [2], and Kasami bent functions, cf.[1]. A particularly interesting construction is the (partial) spread construction, as it works not only for functions from $\mathbb{V}_n$ to elementary abelian groups $\mathbb{V}_k$, but for functions from $\mathbb{V}_n$ to any abelian group B of order 2^k, $k \leq m = n/2$.

Recall that a *partial spread* $\mathcal{S}$ of $\mathbb{V}_n$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n$ which pairwise intersect trivially. If $|\mathcal{S}| = 2^m + 1$, hence every nonzero element of $\mathbb{V}_n$ is in exactly one of those subspaces, then $\mathcal{S}$ is called a *(complete) spread*. The standard example is the Desarguesian spread, which has for $\mathbb{V}_n = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ the representation $\mathcal{S} = \{U, U_s : s \in \mathbb{F}_{2^m}\}$, with $U = \{(0, y) : y \in \mathbb{F}_{2^m}\}$ and for $s \in \mathbb{F}_{2^m}$, $U_s = \{(x, sx) : x \in \mathbb{F}_{2^m}\}$.

Given a (complete) spread $\mathcal{S}$ of $\mathbb{V}_n$, we obtain a bent function from $\mathbb{V}_n$ to B, $|B| = 2^k$, $k \leq n/2$, as follows.

- For every element γ of B, except from w.l.o.g. $0 \in B$, we assign the nonzero elements of exactly 2^{m-k} elements of $\mathcal{S}$ to the preimage of γ.

- All other elements, i.e., the elements of $2^{m-k}+1$ elements of $\mathcal{S}$, are mapped to $0 \in B$.

From this general construction we also infer that the union of any $2^{m-1}+1$ elements of $\mathcal{S}$ is always the support of a Boolean bent function.

In this talk we are interested in bent functions from $\mathbb{V}_n$ to the cyclic group $\mathbb{Z}_{2^k}$, equivalently in relative difference sets in $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ with forbidden subgroup $\mathbb{Z}_{2^k}$. By (1), this are functions f for which

$$\mathcal{H}_f(a,b) = \sum_{x \in \mathbb{V}_n} \zeta_{2^k}^{af(x)} (-1)^{\langle b,x \rangle},$$

where ζ_{2^k} is a complex primitive 2^kth root of unity, has absolute value $2^{n/2}$ for all nonzero $a \in \mathbb{Z}_{2^k}$ and $b \in \mathbb{V}_n$. Again such functions can only exist for $m \leq n/2$, [10]. We remark that functions $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ satisfying the much weaker condition that $|\mathcal{H}_f(1,b)| = 2^{n/2}$ for all $b \in \mathbb{V}_n$ are referred to as *generalized bent functions*. They have been intensively studied in many papers, see [3, 4, 5, 6, 7, 8, 11]. If not also bent, generalized bent functions do not correspond to relative difference sets.

Bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ can certainly be obtained with the spread construction. As far as we are aware, for $k \geq 3$ no construction is known that does not come from spread or a partial spread. In this talk we ask the question whether, and for which $k \geq 3$, there exist such bent functions that do not come from (partial) spreads. We present a construction of bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k \leq n/6$. With an argument via the algebraic degree of associated Boolean bent functions we show that this construction does not come from (partial) spreads. From the construction we infer partitions of $\mathbb{V}_n$ that have similar properties as spreads, in fact can be interpreted as a generalization of the Desarguesian spread. In particular, the union of a certain fixed number of sets of these partitions is always the support of a Boolean bent function.

2 Results

As we have to distinguish addition in different structures, we denote the addition in the complex numbers and in the ring $\mathbb{Z}_{2^k}$ by $+$, the addition in the elementary abelian groups $\mathbb{F}_2$, $\mathbb{V}_n$ and $\mathbb{F}_{2^m}$ is denoted by $\oplus$.

Let f be a function from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, then we can write f as

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$$

for uniquely determined Boolean functions a_j, $0 \leq j \leq k-1$, from $\mathbb{V}_n$ to $\mathbb{F}_2$.

As ingredients for our construction we will use the following facts.

- A function $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ is bent if and only if $2^t f$ is generalized bent for all t, $0 \leq t \leq k-1$.
- $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ is generalized bent if and only if all Boolean functions in the affine space of Boolean functions $\mathcal{A} = a_{k-1} \oplus \langle a_{k-2}, \ldots, a_0 \rangle$ are bent, and for any three functions $b_0, b_1, b_2 \in \mathcal{A}$ we have

  $$(b_0 \oplus b_1 \oplus b_2)^* = b_0^* \oplus b_1^* \oplus b_2^*,$$

  where b^* denotes the dual of a Boolean bent function b, see [3].
- Let d, e be integers such that $\gcd(2^m-1, d) = 1$ and $ed \equiv 1 \bmod 2^m-1$, and suppose that $\beta_0, \beta_1, \beta_2$ satisfy

  $$(\beta_0 \oplus \beta_1 \oplus \beta_2)^{-e} = \beta_0^{-e} \oplus \beta_1^{-e} \oplus \beta_2^{-e}.$$

  Then the Boolean bent functions $b_i(x) = \mathrm{Tr}_m(\beta_i x y^d)$, $i = 0, 1, 2$, satisfy $(b_0 \oplus b_1 \oplus b_2)^* = b_0^* \oplus b_1^* \oplus b_2^*$, see [9].

We will then show the following Theorem.

Theorem 2.1 *Let m, j be integers such that $\gcd(2^m-1, 2^j+1) = 1$ and $\gcd(2^m-1, 2^j-1) = 2^k-1$, let $e = 2^m - 2^j - 2$, and let d be the inverse of e modulo 2^m-1. Then for a basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, the functions f_1 and f_2 given as*

$$f_1(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_m(\alpha_i x y^d) 2^i, \qquad f_2(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_m(\alpha_i^{-e} x^e y) 2^i \tag{2}$$

are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$.

With an argument via algebraic degrees, we will then conclude

Corollary 2.2 *Let m and $j > 0$ be integers such that $\gcd(2^m-1, 2^j+1) = 1$ and $\gcd(2^m-1, 2^j-1) = 2^k-1$, and let e, d, α_i, $0 \le i \le k-1$, be as in Theorem 2.1. Then the functions f_1, f_2 in (2) are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$, which do not come from partial spreads.*

The final part of the talk is dedicated to partitions which we infer from the functions in Theorem 2.1

Let m, k be integers such that k divides m and $\gcd(2^m-1, 2^k+1) = 1$, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$. For an element $s \in \mathbb{F}_{2^m}$ define

$$U_s := \{(x, sx^{-e}) \ : \ x \in \mathbb{F}_{2^m}\},\ U_s^* = U_s \setminus \{(0,0)\}, \text{ and } U = \{(0, y) \ : \ y \in \mathbb{F}_{2^m}\}.$$

Then U, U_s^*, $s \in \mathbb{F}_{2^m}$, form a partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Note that U, U_s, $s \in \mathbb{F}_{2^m}$, are the subspaces of the Desarguesian spread if $2^k+1 \equiv -e \equiv 1 \bmod 2^m-1$ (more general, if $-e \equiv 2^v \bmod 2^m-1$). Also note that U_s is not a subspace if we do not have $-e \equiv 2^v \bmod 2^m - 1$ for some integer v.

Similarly, for an element $s \in \mathbb{F}_{2^m}$ we define

$$V_s := \{(x^{-d}s, x) \ : \ x \in \mathbb{F}_{2^m}\},\ V_s^* = V_s \setminus \{(0,0)\}, \text{ and } V = \{(x, 0) \ : \ x \in \mathbb{F}_{2^m}\}.$$

Note that as above for the sets U and U_s, if $-d \equiv 2^v \bmod 2^m - 1$, then V_s and V are the subspaces of the Desarguesian spread.

For the divisor k of m and an element γ of $\mathbb{F}_{2^k}$ let

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} V_s^*.$$

With this definitions we obtain two partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{2^m}\}$$
$$\Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{2^m}\},$$

that have similar properties as spreads have:

Theorem 2.3 *Let m, k be integers such that k divides m and $\gcd(2^m-1, 2^k+1) = 1$, and let $\pi(i) = \gamma_i$ be a one-to-one map from $\mathbb{Z}_{2^k}$ to $\mathbb{F}_{2^k}$. Define functions $f_A, f_B : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ as follows:*

- *If $(x, y) \in \mathcal{A}(\gamma_i)$ then $f_A(x, y) = i$, and, w.l.o.g., $f_A(0, y) = 0$ for all $y \in \mathbb{F}_{2^m}$;*
- *If $(x, y) \in \mathcal{B}(\gamma_i)$ then $f_B(x, y) = i$, and, w.l.o.g., $f(x, 0) = 0$ for all $x \in \mathbb{F}_{2^m}$.*

Then f_A, f_B are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$.

Theorem 2.4 *Let m, k be integers such that k divides m and $\gcd(2^m-1, 2^k+1) = 1$, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$.*

I. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{A}(\gamma)$ is a bent function. Likewise, their complements, i.e., the Boolean functions with U and 2^{k-1} of the sets $\mathcal{A}(\gamma)$ as their support, are bent.

II. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{B}(\gamma)$ is a bent function. Likewise the Boolean functions with V and 2^{k-1} of the sets $\mathcal{B}(\gamma)$ as their support, are bent.

The duals of the bent functions of the class in I are in the class in II (and vice versa).

Remark 2.5 *(i) In the special case $k = m$, the partitions Γ_1, Γ_2 reduce to a Desarguesian spread partition, and f in Theorem 2.3 is a spread function on the complete Desarguesian spread. Theorem 2.4 describes then the well known PS^-_{ap} and PS^+_{ap} bent functions, cf. [2]. Hence we may see the bent functions in Theorem 2.3, and the Boolean bent functions in Theorem 2.4 as generalizations of the Desarguesian spread bent functions.*

(ii) As for the classical spread functions, also the proof of Theorem 2.3, holds not only for functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$, but for functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to any abelian group B of order 2^k. The bentness is a property of the partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. For instance, also many more vectorial bent functions in dimension k are obtained.

(iii) Clearly, as for the spreads, the partitions Γ_1 and Γ_2 represent a whole equivalence class of partitions. Numerically we confirmed that in general Γ_1 and Γ_2 are not equivalent.

References

[1] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. 59 (2011), 89–109.

[2] J.F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974.

[3] S. Hodžić, W. Meidl, E. Pasalic, Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image. IEEE Trans. Inform. Theory 64 (2018), 5432–5440.

[4] T. Martinsen, W. Meidl, P. Stanica, Generalized bent functions and their gray images. In: Arithmetic of finite fields, Lecture Notes in Comput. Sci., 10064, pp. 160–173, Springer, Cham, 2016.

[5] T. Martinsen, W. Meidl, P. Stanica, Partial spread and vectorial generalized bent functions. Des. Codes Cryptogr. 85 (2017), 1–13.

[6] W. Meidl, A secondary construction of bent functions, octal gbent functions and their duals. Math. Comput. Simulation 143 (2018), 57–64.

[7] W. Meidl, A. Pott, Generalized bent functions into $\mathbb{Z}_{p^k}$ from the partial spread and the Maiorana-McFarland class, Cryptogr. Commun. 11 (2019), 1233–1245.

[8] S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, K. Feng, Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory 64 (2018), 5441–5452.

[9] S. Mesnager, Several new infinite families of bent functions and their duals. IEEE Trans. Inform. Theory 60 (2014), no. 7, 4397–4407.

[10] K. Nyberg, Perfect nonlinear S-boxes, In: Advances in cryptology–EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., 547, pp. 378–386, Springer, Berlin, 1991.

[11] C. Tang, C. Xiang, Y. Qi, K. Feng, Complete characterization of generalized bent and 2^k-bent Boolean functions. IEEE Trans. Inform. Theory 63 (2017), 4668–4674.

On constructions of weightwise perfectly balanced functions

Sihem Mesnager* and Sihong Su**

*University of Paris VIII (Department of Mathematics), 93526 Saint-Denis, France, University of Paris XIII, Sorbonne Paris Cité 93430 Villetaneuse, LAGA, UMR 7539, CNRS, France Telecom Paris, 91120 Palaiseau, France. Email: smesnager@univ-paris8.fr

**School of Mathematics and Statistics, Henan University, Kaifeng, 475004, China, and the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France. Email: sush@henu.edu.cn

Abstract

The recent FLIP cipher is an encryption scheme described by Méaux et al. at the conference EUROCRYPT 2016. It is based on a new stream cipher model, called the filter permutator and tries to minimize some parameters (including the multiplicative depth). In the filter permutator, the input to the Boolean function has constant Hamming weight equal to the weight of the secret key. As a consequence, Boolean functions satisfying good cryptographic criteria when restricted to the set of vectors with constant Hamming weight play an important role in the FLIP stream cipher. Carlet et al. have shown that for Boolean functions with restricted input, balancedness and nonlinearity parameters continue to play an important role with respect to the corresponding attacks on the framework of FLIP ciphers. In particular, Boolean functions which are uniformly distributed over $\mathbb{F}_2$ on $E_{n,k} = \{x \in \mathbb{F}_2^n \mid \mathrm{w_H}(x) = k\}$ for every $0 < k < n$ are called weightwise perfectly balanced (WPB) functions, where $\mathrm{w_H}(x)$ denotes the Hamming weight of x. In this extended abstract, we firstly propose two methods of constructing weightwise perfectly balanced Boolean functions in 2^k variables (where k is a positive integer) by modifying the support of linear and quadratic functions. Furthermore, we derive a construction of n-variable weightwise almost perfectly balanced Boolean functions for any positive integer n.

1 Introduction

In a cryptographic framework, Boolean functions are classically studied with an input ranging over the vector space $\mathbb{F}_2^n$ of binary vectors of length n [2]. This is the case when the Boolean functions are used as the (main) nonlinear components of a stream cipher, in the so-called combiner and filter models of pseudo-random generators. However, the input of a Boolean function can be restricted to a subset of the vector space $\mathbb{F}_2^n$. A recent example of such a situation is given by the FLIP cipher [10]. The FLIP cipher is a new family of stream ciphers proposed by Méaux et al. at Eurocrypt 2016, which is intended to be combined with a homomorphic encryption scheme to create an acceptable system of fully homomorphic encryption [4, 8]. Essentially, the FLIP cipher is one of the encryption schemes specifically designed to be combined with a homomorphic encryption scheme to improve the efficiency of somewhat homomorphic encryption frameworks [1]. The FLIP cipher is based on a new stream cipher model, called the *filter permutator* and tries to minimize some parameters (including the multiplicative depth). The reader notices that Méaux et al [9] have proposed in 2019, an improved filter permutators for efficient FHE (in particular better Instances and implementations). A nice description of FLIP can be found in [10]. An early version of FLIP faces an attack given by Duval et al. [5], which leads the design of the filter function to become more complicated to reach better criteria on the subsets of $\mathbb{F}_2^n$. In 2017, Carlet, Méaux, and Rotella [3] provided a security analysis on FLIP cipher and gave the first study on cryptographic criteria of Boolean functions with restricted input. This produces a special situation for the structure of filter function: the input of the filter function consists of those vectors in $\mathbb{F}_2^n$ which have constant Hamming weight (in fact, by definition in

the filter permutator, the input to the Boolean function has constant Hamming weight equal to the weight of the secret key). Carlet et al. [3] have shown that for Boolean functions with restricted input, balancedness and nonlinearity parameters continue to play an important role with respect to the corresponding attacks on the framework of FLIP ciphers. In particular, Boolean functions which are uniformly distributed over $\mathbb{F}_2$ on $E_{n,k} = \{x \in \mathbb{F}_2^n \mid \mathrm{w_H}(x) = k\}$ for every $0 < k < n$ are called *weightwise perfectly balanced* (WPB) functions, where $\mathrm{w_H}(x)$ denotes the Hamming weight of x. To our best knowledge, the first known construction of WPB functions is due to [3] in 2017, which is designed through a recursive method. In 2008, Liu and Mesnager [6] proposed a large class of WPB functions, which is 2-rotation symmetric.In 2019, Tang and Liu [11] also gave a construction of WPB functions. Some upper bounds on the k-weight nonlinearity of Boolean functions are discussed in [3] and [7], respectively.

In this extended abstract, we firstly give a full study of the Hamming weight distributions of the linear function $f(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_m$ and the quadratic function $g(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_n \oplus 1)$, where $n = 2m$. And then, two concrete constructions of 2^k-variable (where k is a positive integer) WPB functions by modifying the support of the linear function and the quadratic function are respectively proposed. Lastly, a construction of n-variable almost-WPB functions for any positive integer n is given.

This extended abstract is organized as follows. Some definitions are presented in Section 2 but we assume the reader familiar with background on Boolean functions as well as standard notation. In Section 3, a construction of WPB functions on 2^k variables (where k is a positive integer) obtained by modifying the support of a linear function is given. Next, a construction of WPB functions on 2^k variables obtained by modifying the support of a quadratic function is proposed in Section 4. The construction of n-variable almost-WPB functions for any positive integer n is given in Section 5.

2 Some preliminaries

For $0 \le k \le n$, we always denote $E_{n,k} = \{x \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x) = k\}$. Obviously, $\bigcup_{k=0}^{n} E_{n,k} = \mathbb{F}_2^n$. We denote by $\mathcal{B}_n$ the set of all the n-variable Boolean functions. A function $f \in \mathcal{B}_n$ is said to be balanced if its truth table contains an equal number of 1's and 0's, i.e., if its Hamming weight $\mathrm{wt}(f) = 2^{n-1}$. The k-weight of the function $f \in \mathcal{B}_n$, denoted by $\mathrm{wt}_k(f)$, is the cardinality of the subset $\{x \in E_{n,k} \,|\, f(x) = 1\}$, i.e. $\mathrm{wt}_k(f) = |\{x \in E_{n,k} \,|\, f(x) = 1\}|$. It is known that the cardinality of the subset $E_{n,k}$ is $|E_{n,k}| = \binom{n}{k}$ for $0 \le k \le n$. Since $\binom{n}{0} = \binom{n}{n} = 1$, we have the following Definition.

Definition 2.1 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$*

for all integers $1 \le k \le n-1$, the function $f(x)$ is called a weightwise perfectly balanced (WPB) function.

Definition 2.2 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$ for all odd integers $k \in \{1, 2, \cdots, n-1\}$, then the function $f(x)$ is called an odd-weightwise perfectly balanced (odd-WPB) function.*

Definition 2.3 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \left\lfloor \frac{1}{2}\binom{n}{k} \right\rfloor$ for all integers $0 \le k \le n$, then the function $f(x)$ is called a weightwise almost perfectly balanced (almost-WPB) function.*

3 Construction of WPB functions by modifying a linear function

.

Define an n-variable Boolean function as

$$f(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_m, \tag{1}$$

where $n = 2m$ with m being a positive integer. Then, the support of the n-variable Boolean function $f(x)$ in (1) is

$$\mathrm{supp}(f) = \{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x_1, x_2, \cdots, x_m) \text{ is odd}\}. \tag{2}$$

.

Theorem 3.1 *For any odd integer $k \in \{1, 3, \cdots, n-1\}$ and $n = 2m$, the n-variable Boolean function $f(x)$ in (1) satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$. Hence, the function $f(x)$ in (1) is odd-WPB.*

Theorem 3.2 *For any even integer $k \in \{2, 4, 6, \cdots, n-2\}$ and $n = 2m$, the n-variable Boolean function $f(x)$ in (1) satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k} - \frac{(-1)^{\frac{k}{2}}}{2}\binom{m}{\frac{k}{2}}$.*

Corollary 3.3 *For any even integer $k \in \{2, 4, 6, \cdots, n-2\}$ and $n = 2m$, we have $\sum\limits_{\substack{0 \le i \le k \\ i \text{ is odd}}} \binom{m}{i}\binom{m}{k-i} = \frac{1}{2}\binom{n}{k} - \frac{(-1)^{\frac{k}{2}}}{2}\binom{m}{\frac{k}{2}}$.*

Given a positive integer m, define a 2^m-variable Boolean function as

$$\mathrm{supp}(f_m) = \bigsqcup_{i=1}^{m} \left\{(x, y, x, y, \cdots, x, y) \in \mathbb{F}_2^{2^m} \,|\, x, y \in \mathbb{F}_2^{2^{m-i}}, \mathrm{wt}(x) \text{ is odd}\right\}. \tag{3}$$

Theorem 3.4 *The function f_m in 2^m variables defined in (3) is weightwise perfectly balanced.*

Theorem 3.5 *The ANF of the 2^m-variable Boolean function $f_m(x)$ in (3) is $f_m(x_1, x_2, \ldots, x_{2^m}) = \bigoplus\limits_{i=1}^{2^{m-1}} x_i \oplus f_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}) \prod\limits_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1)$,*

where $f_1(x_1, x_2) = x_1$. Moreover, the algebraic degree of the 2^m-variable Boolean function $f_m(x)$ in (3) is $\deg(f_m) = 2^m - 1$.

In order to get a flexible construction of WPB functions, define

$$\begin{cases} I_1^{(1)} \subseteq \{1, 2, \cdots, n\}, I_2^{(1)} = \{1, 2, \cdots, n\} \setminus I_1, \\ I_1^{(2)} \subseteq I_1^{(1)}, I_2^{(2)} = I_1^{(1)} \setminus I_1^{(2)}, I_3^{(2)} \subseteq I_2^{(1)}, I_4^{(2)} = I_2^{(1)} \setminus I_3^{(2)}, \\ \cdots\cdots \\ I_1^{(m)} \subseteq I_1^{(m-1)}, I_2^{(m)} = I_1^{(m-1)} \setminus I_1^{(m)}, \cdots\cdots, I_{2^m-1}^{(m)} \subseteq I_{2^{m-1}}^{(m-1)}, I_{2^m}^{(m)} = I_{2^{m-1}}^{(m-1)} \setminus I_{2^m-1}^{(m)}, \end{cases}$$

where $|I_j^{(i)}| = 2^{m-i}$, for $1 \le i \le m$ and $1 \le j \le 2^i$. For convenience, denote $x_I = (x_{i_1}, x_{i_2}, \cdots, x_{i_t})$ for $x = (x_1, x_2, \cdots, x_n)$ and $I = \{i_1, i_2, \cdots, i_t\} \subseteq \{1, 2, \cdots, 2^m\}$. Then, a flexible construction of 2^m-vriable WPB function is given as

$$\mathrm{supp}(f_m) = \bigsqcup_{i=1}^{m} \left\{x \in \mathbb{F}_2^{2^m} \,|\, \mathrm{wt}(x_{I_1^{(i)}}) \text{ is odd}, x_{I_1^{(i)}} = x_{I_3^{(i)}} = \cdots = x_{I_{2^i-1}^{(i)}}, x_{I_2^{(i)}} = x_{I_4^{(i)}} = \cdots = x_{I_{2^i}^{(i)}}\right\},$$

where m is a positive integer. In fact, if the order of the entries in the vector $x_{I_j^{(i)}}$ is considered, a more flexible constructions of WPB functions can be obtained.

4 Construction of WPB functions by modifying the support of a quadratic function

Define an n-variable Boolean function as

$$g(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_n \oplus 1), \tag{4}$$

where $n = 2m$ with m being a positive integer.

Theorem 4.1 *For any integer $k \in \{1, 2, \cdots, n-1\}$ and $n = 2m$, the n-variable Boolean function $g(x)$ in (4) satisfies* $\mathrm{wt}_k(g) = \frac{1}{2}\binom{n}{k} - \frac{\delta_k}{2}\binom{m}{\frac{k}{2}}$, *where* $\delta_k = \begin{cases} 1, & k \text{ is even}, \\ 0, & k \text{ is odd}. \end{cases}$

According to the values of the k-weights of the n-variable Boolean function $g(x)$ defined in (4), $1 \le k \le n-1$, we can construct another WPB function as follows.

Define a 2^m-variable Boolean function $g_m(x)$ as

$$g_m(x_1, x_2, \ldots, x_{2^m}) = g(x_1, x_2, \ldots, x_{2^m}) \oplus g_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}) \prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1), \quad (5)$$

where $m \ge 1$, $g(x)$ is defined in (4), and $g_0(x_1) = 0$.

Theorem 4.2 *The Boolean defined in (5) is weightwise perfectly balanced. Its algebraic degree equals* $\deg(g_m) = 2^m$ *(hence it has a maximal algebraic degree).*

5 Construction of almost-WPB functions

In this section, a construction of almost-WPB functions by modifying the support of a quadratic Boolean function in any variables is proposed.

Define an n-variable Boolean function as

$$h(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_{2m} \oplus 1), \quad (6)$$

where n is a positive integer and $m = \lfloor \frac{n}{2} \rfloor$.

Theorem 5.1

- *For any integer $k \in \{1, 2, \cdots, n-1\}$ and $n = 2m+1$ with $m \ge 1$, the n-variable Boolean function $h(x)$ in (6) satisfies* $\mathrm{wt}_k(h) = \frac{1}{2}\binom{n}{k} - \frac{1}{2}\binom{m}{\lfloor \frac{k}{2} \rfloor}$.
- *For any integer $k \in \{1, 2, \cdots, n-1\}$ with $n \ge 2$, the n-variable Boolean function $h(x)$ in (6) satisfies* $\mathrm{wt}_k(h) = \begin{cases} \frac{1}{2}\binom{n}{k}, & n \text{ is even and } k \text{ is odd}, \\ \frac{1}{2}\binom{n}{k} - \frac{1}{2}\binom{\lfloor \frac{n}{2} \rfloor}{\lfloor \frac{k}{2} \rfloor}, & \text{otherwise}. \end{cases}$

Define an n-variable Boolean function $h_n(x)$ as

$$h_n(x_1, x_2, \ldots, x_n) = h(x_1, x_2, \ldots, x_n) \oplus h_{\lfloor \frac{n}{2} \rfloor}(x_1, x_2, \ldots, x_n) \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (x_i \oplus x_{\lfloor \frac{n}{2} \rfloor + i} \oplus 1), \quad (7)$$

where $n \ge 2$, $h(x_1, x_2, \ldots, x_n)$ is defined in (6), and $h_1(x_1) = 0$.

Theorem 5.2

- *The Boolean function h_n defined in (7) is almost weightwise perfectly balanced.*
- *Its Hamming weight equals* $\mathrm{wt}(h_n) = 2^{n-1} - 2^{\mathrm{wt}(n)-1}$, *where* $\mathrm{wt}(n) = \mathrm{wt}(n_1, n_2, \cdots, n_t)$ *satisfying* $n = n_1 2^0 + n_2 2^1 + \cdots + n_t 2^{t-1}$.
- *Its algebraic degree equals* $\deg(h_n) = n - \mathrm{wt}(n) + 1$, *where* $\mathrm{wt}(n) = \mathrm{wt}(n_1, n_2, \cdots, n_t)$ *satisfying* $n = n_1 2^0 + n_2 2^1 + \cdots + n_t 2^{t-1}$.

References

[1] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. Naya-Plasencia, P. Paillier, and R. Sirdey, Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression, In Thomas Peyrin, editor, FSE 2016, Lecture Notes in Computer Science, vol. 9783, pp. 313-333, Springer, 2016.

[2] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Y. Crama and P. Hammer eds, Cambridge University Press, 2010.

[3] C. Carlet, P. Méaux, and Y. Rotella, Boolean functions with restricted input and their robustness: application to the FLIP cipher. IACR Trans. Symmetric Cryptol. (3), pp. 192-227, 2017.

[4] J. Coron, T. Lepoint, M. Tibouchi, Scale-Invariant Fully Homomorphic Encryption over the Integers. in Krawczyk, H. (ed.) Public-Key Cryptography-PKC 2014. Lecture Notes in Computer Science, vol. 8383, pp. 311-328, Springer, 2014.

[5] S. Duval, V. Lallemand, and Y. Rotella, Cryptanalysis of the FLIP family of stream ciphers, In: Advances in Cryptology-CRYPTO 2016, Lecture Notes in Computer Science, vol. 9814, Berlin: Springer-Verlag, pp.457-475, 2016.

[6] J. Liu and S. Mesnager, Weightwise perfectly balanced functions with high weightwise nonlinearity profile, Designs, Codes and Cryptography, vol.87, no.8, pp.1797-1813, 2019.

[7] S. Mesnager, Z. Zhou, and C. Ding, On the nonlinearity of Boolean functions with restricted input, Cryptography and Communications, vol. 11, no. 1, pp. 63-76, 2019.

[8] P. Méaux, Symmetric Encryption Scheme adapted to Fully Homomorphic Encryption Scheme, in Journées Codage et Cryptographie-JC2, France 2015.

[9] P. Méaux, C. Carlet, A. Journault and F. X. Standaert, Improved Filter Permutators for Efficient FHE: Better Instances and Implementations. INDOCRYPT , pp. 68-91, 2019.

[10] P. Méaux, A. Journault, F. X. Standaert, and C. Carlet, Towards stream ciphers for efficient FHE with low-noise ciphertexts, in Advances in Cryptology EUROCRYPT 2016, Lecture Notes in Computer Science, vol.9665, pp.311-343, Berlin: Springer-Verlag, 2016.

[11] D. Tang and J. Liu, A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity, Cryptography and Communications. vol.11, no.6, pp.1185-1197, 2019.

Metric regularity of Reed-Muller codes *

Alexey Oblaukhov[1,2]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia
[2]Novosibirsk State University, Novosibirsk, Russia

Abstract

In this work we study metric properties of the well-known family of binary Reed-Muller codes. Let A be an arbitrary subset of the Boolean cube, and $\widehat{A}$ be the metric complement of A — the set of all vectors of the Boolean cube at the maximal possible distance from A. If the metric complement of $\widehat{A}$ coincides with A, then the set A is called a *metrically regular set*. The problem of investigating metrically regular sets appeared when studying *bent functions*, which have important applications in cryptography and coding theory and are also one of the earliest examples of a metrically regular set. In this work we describe metric complements and establish the metric regularity of the codes $\mathcal{RM}(0,m)$ and $\mathcal{RM}(k,m)$ for $k \geqslant m-3$. Additionally, the metric regularity of the codes $\mathcal{RM}(1,5)$ and $\mathcal{RM}(2,6)$ is proved. Combined with previous results by Tokareva N. (2012) concerning duality of affine and bent functions, this proves the metric regularity of most Reed-Muller codes with known covering radius. It is conjectured that all Reed-Muller codes are metrically regular.

1 Introduction

The problem of investigating and classifying *metrically regular sets* was posed by Tokareva [14, 15] when studying metric properties of *bent functions* [11]. A Boolean function f in even number of variables m is called a *bent function* if it is at the maximal possible distance from the set of affine functions.

Bent functions have various applications in cryptography, coding theory and combinatorics [6, 15]. In cryptography, bent functions are valued because of their outstanding nonlinearity, which allows one to construct S-boxes for block ciphers which possess high resistance to the linear cryptanalysis [6]. However, many problems related to bent functions remain unsolved; in particular, the gap between the best known lower and upper bound on the number of bent functions is extremely large; currently known constructions of bent functions are rather scarse. In 2012 [14], Tokareva has proved that, like bent functions are maximally distant from affine functions, affine functions are at the maximal possible distance from bent functions, thus establishing the *metric regularity* of both sets. This discovery arouses interest in studying the property of metric regularity in order to better understand the structure of the set of bent functions.

Let us briefly overview the results obtained in this area. Metric regularity of several classes of *partition set functions* is studied in [13]. The work [4] examines metric properties of self-dual bent functions. Metric regularity has been actively investigated by the author: metric complements of linear subspaces of the Boolean cube are studied in the paper [8], while the works [9] and [10] are studying possible sizes of the largest and smallest metrically regular set.

In this work we investigate metric properties of Reed-Muller codes. Among the codes of high order, covering radii of the codes $\mathcal{RM}(k,m)$, for $k \geqslant m-3$ are known. The covering radius of $\mathcal{RM}(1,m)$ for odd $m > 7$ is unknown, but has been determined for $\mathcal{RM}(1,5)$ [1] and $\mathcal{RM}(1,7)$ [7, 3]. In [12], Schatz has found the covering radius of $\mathcal{RM}(2,6)$, while recently Wang has

*The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394, 19-31-90093) and Laboratory of Cryptography JetBrains Research.

established the covering radius of $\mathcal{RM}(2,7)$ [16]. For $m > 7$, the covering radius of $\mathcal{RM}(2,m)$ is still unknown. We prove that the codes $\mathcal{RM}(k,m)$, for $k = 0$ and $k \geqslant m-3$ and the codes $\mathcal{RM}(1,5)$ and $\mathcal{RM}(2,6)$ are metrically regular and also describe their metric complements in most cases.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the space of binary vectors of length n with the Hamming metric. The *Hamming distance* $d(\cdot,\cdot)$ between two binary vectors is defined as the number of coordinates in which these vectors differ, while $wt(\cdot)$ denotes the *weight* of a vector, i.e. the number of nonzero values it contains. The plus sign + denotes addition modulo two (componentwise in case of vectors).

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and $y \in \mathbb{F}_2^n$ be an arbitrary vector. The distance from the vector y to the set X is defined as

$$d(y,X) = \min_{x \in X} d(y,x).$$

The *covering radius* of the set X is defined as

$$\rho(X) = \max_{z \in \mathbb{F}_2^n} d(z,X).$$

The set X with $\rho(X) = r$ is also called a *covering code* [2] of radius r.

Consider the set

$$Y = \{y \in \mathbb{F}_2^n | d(y,X) = \rho(X)\}$$

of all vectors at the maximal possible distance from the set X. This set is called the *metric complement* [8] of X and is denoted by $\widehat{X}$. Vectors from the metric complement are sometimes called *deep holes* of a code. If $\widehat{\widehat{X}} = X$ then the set X is said to be *metrically regular* [15].

Note that metrically regular sets always come in pairs, i.e. if A is a metrically regular set, then its metric complement $\widehat{A}$ is also a metrically regular set and both of them have the same covering radius. For some simple examples of metric complements and metrically regular sets, refer to [8, 9, 10].

The following trivial auxiliary lemma, established in [8], will be used throughout the paper.

Lemma 2.1 *Let $C \subseteq \mathbb{F}_2^n$ be a linear code. Then $\rho(\widehat{C}) = \rho(C)$ and a vector $x \in \mathbb{F}_2^n$ is in $\widehat{\widehat{C}}$ if and only if $x + \widehat{C} = \widehat{C}$.*

Let $\mathcal{F}^m$ be the set of all Boolean functions in m variables. The Reed-Muller code of order k is defined as:

$$\mathcal{RM}(k,m) = \{f \in \mathcal{F}^m : \deg(f) \leqslant k\},$$

where $\deg(\cdot)$ denotes the degree of the *algebraic normal form (ANF)* of the function.

Let f and g be two functions in m variables. Denote as $L_{\mathrm{A}}^{\mathrm{b}} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ the affine transformation of the variables with the matrix A and the vector b):

$$(f \circ L_{\mathrm{A}}^{\mathrm{b}})(\mathrm{x}) = f(\mathrm{Ax} + \mathrm{b}).$$

Here $\circ$ denotes the composition of the functions. If the vector b is zero, it will be omitted from the notation. Functions f and g are called *linearly equivalent* if one can be obtained from the other by applying a nonsingular linear transformation to the variables, i.e. $f = g \circ L_{\mathrm{A}}$, where $\det \mathrm{A} \neq 0$.

Extended affine equivalence is more common when classifying boolean functions: functions f and g are called EA-*equivalent* if there exists a nonsingular linear transformation of variables A, a boolean vector b of length m and a function h of degree at most 1 such that $f = g \circ L_{\mathrm{A}}^{\mathrm{b}} + h$.

For our study we will use a variant of these two equivalence relations, which will be referred to as *extended linear equivalence (to the power of k)*. Functions f and g are called EL^k*-equivalent* if there exists a nonsingular binary matrix A and a function h of degree at most k such that

$$f = g \circ L_{\mathrm{A}} + h.$$

It is easy to see that this relation is indeed an equivalence. We will denote this equivalence by $f \overset{k}{\sim} g$.

The Reed-Muller code of order k in m variables is usually denoted as $\mathcal{RM}(k, m)$. Since we will refer to these codes regularly, we will instead often use $\mathcal{R}_{k,m}$ to denote the Reed-Muller code of order k in m variables. We will sometimes omit the number of variables m if it is clear from the context.

3 The Reed-Muller code $\mathcal{RM}(1, 5)$

In the work [1], Berlekamp and Welch presented a partition of all cosets of the $\mathcal{R}_{1,5}$ code into 48 classes with respect to the EA-equivalence and obtained weight distributions for each class of cosets. Four of these cosets contain only codewords of weight 12 and higher, and those cosets constitute the metric complement of $\mathcal{R}_{1,5}$. Thus we can present the metric complement of this code as:

$$\widehat{\mathcal{R}}_{1,5} = \{f : f \overset{\mathrm{EA}}{\sim} g \text{ for some } g \text{ from one of 4 farthest classes}\}$$

Since $\mathcal{R}_{1,5}$ is linear, it follows that $\rho(\widehat{\mathcal{R}}_{1,5}) = \rho(\mathcal{R}_{1,5}) = 12$, and $f \in \widehat{\widehat{\mathcal{R}}}_{1,5}$ if and only if $f + \widehat{\mathcal{R}}_{1,5} = \widehat{\mathcal{R}}_{1,5}$. Thus, in order to establish the metric regularity of $\mathcal{R}_{1,5}$, we must prove that for every $f \notin \mathcal{R}_{1,5}$ it holds $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$.

This is done by taking a representative f_c from every class of cosets C (aside from $\mathcal{R}_{1,5}$ itself) and showing that there exists a function $g_c \in \widehat{\mathcal{R}}_{1,5}$ such that $f_c + g_c \notin \widehat{\mathcal{R}}_{1,5}$. Since the metric complement $\widehat{\mathcal{R}}_{1,5}$ consists of EA-equivalence classes, this proves that none of the functions from the class C belong to $\widehat{\mathcal{R}}_{1,5}$. Therefore, the following holds:

Theorem 3.1 *The code $\mathcal{R}_{1,5}$ is metrically regular.*

4 The Reed-Muller codes of orders 0, m, $m-1$ and $m-2$

The Reed-Muller codes of orders 0, m and $m-1$ coincide with the repetition code, the whole space and the even weight code respectively. It is trivial that all of them are metrically regular.

The Reed-Muller code of order $m-2$ has covering radius 2 [2]. By definition, it consists of all Boolean functions of degree at most $m-2$. Since all functions of degree m have odd weight, and all functions of smaller degree have even weight, functions of degree m are at distance 1 from $\mathcal{R}_{m-2}$, while functions of degree $m-1$ are at distance 2 and therefore

$$\widehat{\mathcal{R}}_{m-2} = \mathcal{R}_{m-1} \setminus \mathcal{R}_{m-2}.$$

Since $\mathcal{R}_{m-2}$ is linear, $\rho(\widehat{\mathcal{R}}_{m-2}) = \rho(\mathcal{R}_{m-2}) = 2$ and thus functions of degree m are at distance 1 from $\widehat{\mathcal{R}}_{m-2}$. It follows that $\widehat{\widehat{\mathcal{R}}}_{m-2} = \mathcal{R}_{m-2}$ and $\mathcal{R}_{m-2}$ is metrically regular.

5 The Reed-Muller code of order $m-3$

5.1 Covering radius

McLoughlin [5] has proved that

$$\rho(\mathcal{R}_{m-3}) = \begin{cases} m+1, & \text{if } m \text{ is odd,} \\ m+2, & \text{if } m \text{ is even.} \end{cases}$$

This result is reestablished by Cohen et al in the book "Covering codes" [2], using a method of syndrome matrices, different from that in [5]. This method allows us not only to obtain covering radius of the Reed-Muller code of order $m-3$, but also to describe the metric complement of this code. As with the covering radius, the cases of even and odd m are distinct.

5.2 Case m is even

In this case, the metric complement can be described as follows:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{g \in G} (g + \mathcal{R}_{m-3}),$$

where

$$G = \{g : \mathrm{supp}(g) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m, \mathrm{x}_1 + \ldots + \mathrm{x}_m\}, \\ \{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\}.$$

It is easy to see that all functions in G form an equivalence class with respect to the linear equivalence. Let us pick any function g^* from this class. We can now say that a function g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if $g = g^* \circ L_{\mathrm{A}} + h$ for some nonsingular matrix A and some function h of degree at most $m-3$, or, in other words, g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if g is EL^{m-3}-equivalent to g^*. Therefore,

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} g^*\},$$

where g^* is some function from the class G (or from $\widehat{\mathcal{R}}_{m-3}$, since all functions in metric complement are EL^{m-3}-equivalent).

5.3 Case m is odd

In this case, the metric complement can be described as follows:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{g \in G_1 \cup G_2} (g + \mathcal{R}_{m-3}),$$

where

$$G_1 = \{g : \mathrm{supp}(g) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m\}, \{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\},$$

and

$$G_2 = \{g : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_{m-1}, \mathrm{x}_1 + \ldots + \mathrm{x}_{m-1}\}, \\ \{\mathrm{x}_1, \ldots, \mathrm{x}_{m-1}\} \text{ are linearly independent}\}.$$

Same as with the case of even m, all functions in G_1 form an equivalence class with respect to the linear equivalence, so do functions from G_2. If we now choose a representative from each class, g_1^* from G_1 and g_2^* from G_2, we can describe metric complement in the following manner:

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} g_1^*\} \cup \{g : g \overset{m-3}{\sim} g_2^*\}.$$

5.4 Metric regularity

Since the code $\mathcal{R}_{m-3}$ is linear, it follows that $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3})$ and a function f is in $\widehat{\widehat{\mathcal{R}}}_{m-3}$ if and only if $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. Thus, like in the Section 3, we prove the metric regularity of $\mathcal{R}_{m-3}$ by proving that no functions other that those contained in $\mathcal{R}_{m-3}$ preserve the metric complement under addition, using the representations of metric complements obtained in the previous subsections.

6 The Reed-Muller code $\mathcal{RM}(2,6)$

Let us consider one other special case. If we change the order of values in the value vectors of functions so that the first half of values corresponds to the values of the function when the last variable is set to 0, and the other half corresponds to the values of the function when the last variable is set to 1, then each Reed-Muller code (for $m > 1$, $r > 0$) can be inductively defined as follows:

$$\mathcal{R}_{r,m} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) | \mathbf{u} \in \mathcal{R}_{r,m-1}, \mathbf{v} \in \mathcal{R}_{r-1,m-1}\}.$$

In particular,

$$\mathcal{R}_{2,6} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) | \mathbf{u} \in \mathcal{R}_{2,5}, \mathbf{v} \in \mathcal{R}_{1,5}\}.$$

Since both $\mathcal{R}_{2,5}$ and $\mathcal{R}_{1,5}$ were shown to be metrically regular, this construction proves useful and allows us to establish the metric regularity of the code $\mathcal{R}_{2,6}$ as well. From now on, vectors in bold will represent value vectors of functions in 5 variables (of length 32), while value vectors of 6-variable functions will be presented as pairs of value vectors of 5-variable functions.

Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. We will prove that $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}})$ is in $\mathcal{R}_{2,6}$ in two steps: first we establish that $\tilde{\mathbf{u}}$ is in $\mathcal{R}_{2,5}$, then we prove that $\tilde{\mathbf{v}}$ is in $\mathcal{R}_{1,5}$. The following results heavily rely on the fact that $\mathcal{R}_{2,6}$ attains the upper bound on the covering radius provided by the $(\mathbf{u}, \mathbf{u}+\mathbf{v})$ construction, i.e. $\rho(\mathcal{R}_{2,6}) = \rho(\mathcal{R}_{2,5}) + \rho(\mathcal{R}_{1,5})$ [12].

Recall (Section 5) that $\widehat{\mathcal{R}}_{2,5} = \{g : g \overset{2}{\sim} g_1\} \cup \{g : g \overset{2}{\sim} g_2\}$, where g_1 and g_2 are some representatives of two EL^2-equivalence classes. Let us denote

$$\widehat{\mathcal{R}}^1_{2,5} := \{g : g \overset{2}{\sim} g_1\},\ \widehat{\mathcal{R}}^2_{2,5} := \{g : g \overset{2}{\sim} g_2\}.$$

The following lemma is useful when proving that $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$:

Lemma 6.1 *For each $i = 1, 2$ one of the following statements holds:*

1. $\forall \mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}\ \forall \mathbf{w} \in \mathbb{F}_2^{32}$ *it holds* $(\mathbf{y}, \mathbf{w}) \notin \widehat{\mathcal{R}}_{2,6}$;
2. $\forall \mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}\ \exists \mathbf{w} \in \mathbb{F}_2^{32}$ *such that* $(\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$;

This lemma tells us that for each EL^2-equivalence class of $\widehat{\mathcal{R}}_{2,5}$, either all vectors appear in the metric complement of $\mathcal{R}_{2,6}$ as the first half of the vector, or no vectors do. Since for any $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$ it holds $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) + \widehat{\mathcal{R}}_{2,6} = \widehat{\mathcal{R}}_{2,6}$, it is easy to show that $\tilde{\mathbf{u}}$ must keep $\widehat{\mathcal{R}}_{2,5}$, $\widehat{\mathcal{R}}^1_{2,5}$ or $\widehat{\mathcal{R}}^2_{2,5}$ in place under addition. From the proof of the metric regularity of the code $\mathcal{R}_{m-3,m}$ for odd m it is not hard to see that only the vectors from $\mathcal{R}_{2,5}$ do that, and thus the following holds:

Proposition 6.2 *Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. Then $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$.*

Recall from Section 3 that $\widehat{\mathcal{R}}_{1,5}$ is composed of 4 EA-equivalence classes: $\widehat{\mathcal{R}}_{1,5} = \bigcup_{i=1}^4 \widehat{\mathcal{R}}^i_{1,5}$. Somewhat similar to Lemma 6.1, the following statement holds:

Lemma 6.3 *For each $i = 1, 2, 3, 4$ one of the following statements holds:*

1. $\forall \mathbf{w}' \in \widehat{\mathcal{R}}^i_{1,5}\ \forall (\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\ \forall \mathbf{u} \in \mathcal{R}_{2,5}\ (d(\mathbf{y}, \mathbf{u}) = 6 \to \mathbf{w} + \mathbf{u} \neq \mathbf{w}')$;
2. $\forall \mathbf{w}' \in \widehat{\mathcal{R}}^i_{1,5}\ \exists (\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\ \exists \mathbf{u} \in \mathcal{R}_{2,5} : (d(\mathbf{y}, \mathbf{u}) = 6 \wedge \mathbf{w} + \mathbf{u} = \mathbf{w}')$;

The following result shows that any of the EA-equivalence classes of the metric complement of $\mathcal{R}_{1,5}$ are also rather "unstable" when summed with a non-affine function:

Lemma 6.4 *For any $\mathbf{v} \notin \mathcal{R}_{1,5}$ and any $i = 1, 2, 3, 4$ there exists a vector $\mathbf{w} \in \widehat{\mathcal{R}}^i_{1,5}$ such that $\mathbf{v} + \mathbf{w} \notin \widehat{\mathcal{R}}_{1,5}$.*

These last two lemmas allow us to show that for any $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$, the vector $\tilde{\mathbf{v}}$ is in $\mathcal{R}_{1,5}$. Combined with Proposition 6.2, this results in the

Theorem 6.5 *Let* $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. *Then* $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \mathcal{R}_{2,6}$.

Since the inverse inclusion holds for any linear code, Theorem 6.5 establishes the metric regularity of the code $\mathcal{R}_{2,6}$.

7 Conclusion

We have established the metric regularity of the codes $\mathcal{RM}(1,5)$, $\mathcal{RM}(2,6)$ and of the codes $\mathcal{RM}(k,m)$ for $k \geqslant m-3$. Factoring in the result by Tokareva [14], which proves the metric regularity of $\mathcal{RM}(1,m)$ for even m, we have covered all infinite families of Reed-Muller codes with known covering radius. The only other Reed-Muller codes with known covering radius, metric regularity of which has not been yet established, are $\mathcal{RM}(1,7)$ and $\mathcal{RM}(2,7)$. Given these results, we formulate the following

Conjecture 1 *All Reed-Muller codes* $\mathcal{RM}(k,m)$ *are metrically regular.*

References

[1] Berlekamp E., Welch L. *Weight distributions of the cosets of the* $(32,6)$ *Reed-Muller code.* IEEE Transactions on Information Theory. **18**(1), 203–207 (1972).

[2] Cohen, G., Honkala, I., Litsyn, S., Lobstein, A. *Covering codes.* Elsevier. **54**, (1997).

[3] Hou X. D. *Radius of the Reed-Muller code* $R(1,7)$ *– A Simpler Proof.* Journal of Combinatorial Theory, Series A. **74**(2), 337–341 (1996).

[4] Kutsenko, A. *Metrical properties of self-dual bent functions. Designs, Codes and Cryptography (2019).* doi:10.1007/s10623-019-00678-x

[5] McLoughlin A. M. *Covering Radius of the* $(m-3)$*-rd Order Reed Muller Codes and a Lower Bound on the* $(m-4)$*-th Order Reed Muller Codes.* SIAM Journal on Applied Mathematics. **37**(2), 419–422 (1979).

[6] Mesnager S.: *Bent Functions: Fundamentals and Results.* Springer International Publishing, (2016).

[7] Mykkeltveit J. *The covering radius of the* $(128,8)$ *Reed-Muller code is* 56. IEEE Transactions on Information Theory. **26**(3), 359–362 (1980).

[8] Oblaukhov A. K. *Metric complements to subspaces in the Boolean cube.* Journal of Applied and Industrial Mathematics. **10**(3), 397–403 (2016).

[9] Oblaukhov A. K. *Maximal metrically regular sets.* Siberian Electronic Mathematical Reports. **15**, 1842–1849 (2018).

[10] Oblaukhov A. *lower bound on the size of the largest metrically regular subset of the Boolean cube.* Cryptography and Communications. **11**(4), 777–791 (2019).

[11] Rothaus O. S. *On "bent" functions.* Journal of Combinatorial Theory, Series A. **20**(3), 300–305 (1976).

[12] Schatz J. *The second order Reed-Muller code of length* 64 *has covering radius* 18. IEEE Transactions on Information Theory. **27**(4), 529–530 (1981).

[13] Stanica P., Sasao T., Butler J. T. *Distance duality on some classes of Boolean functions.* Journal of Combinatorial Mathematics and Combinatorial Computing. 2018.

[14] Tokareva N. *Duality between bent functions and affine functions.* Discrete Mathematics. **312**(3), 666–670 (2012).

[15] Tokareva N. *Bent functions: results and applications to cryptography.* Academic Press, (2015).

[16] Wang Q. *The covering radius of the Reed–Muller code* $RM(2,7)$ *is* 40. Discrete Mathematics. **342**(12), Article 111625 (2019).

Non-linearity of the Carlet-Feng function, and repartition of Gauss sums

François Rodier*

Abstract

The search for Boolean functions that can withstand the main crypyographic attacks is essential. In 2008, Carlet and Feng studied a class of functions which have optimal cryptographic properties with the exception of nonlinearity for which they give a good but not optimal bound. After several people have worked on this problem of nonlinearity they have asked for a new answer to this issue. We provide a new solution to improve the evaluation of the nonlinearity of the Carlet-Feng function, by means of the estimation of the distribution of Gauss sums. This work is in progress and we give some suggestions to improve this work.

Keywords: Carlet-Feng function, nonlinearity, Gaussian sums, equidistribution, discrepancy

1 Introduction

Boolean functions on the space $\mathbb{F}_2^m$ are important in cryptography, where they occur in stream ciphers or private key systems. In both cases, the properties of systems depend on the nonlinearity of a Boolean function. The nonlinearity of a Boolean function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ is the distance from f to the set of affine functions with m variables. The nonlinearity is therefore an important cryptographic parameter. We refer to [1] for a global survey on the Boolean functions.
It is useful to have at one's disposal Boolean functions with highest nonlinearity. The problem of the research of the maximum of the degree of nonlinearity comes down to minimize the Fourier transform of Boolean functions.

1.1 The Carlet-Feng function

Let n be a positive integer and $q = 2^n$. In 2008, Carlet and Feng [2] studied a class of Boolean functions f on $\mathbb{F}_{2^n}$ which is defined by their support

$$\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\}$$

where α is a primitive element of the field $\mathbb{F}_{2^n}$. In the same article they show that these functions when n varies have optimum algebraic immunity, good nonlinearity and optimum algebraic degree. These computations are very good but still not good enough: in fact these bounds are not enough for ensuring a sufficient nonlinearity. Some works have been done on that by Q. Wang and P. Stanica [10] and other authors (cf. Li et al [7] and Tang et al. [9]). They find the bound

$$2^{n-1} - nl(f) \leq \frac{1}{\pi} q^{1/2} \left(n \ln 2 + \gamma + \ln \left(\frac{8}{\pi} \right) + o(1) \right)$$

*Aix Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, UMR 7373, 13288 Marseille, France

where γ is the Euler's constant. Nevertheless, there is a gap between the bound that they can prove and the actual computed values for a finite numbers of functions which are very good, of order $2^{n-1} - 2^{n/2}$. Carlet and some authors cited above [7, 9, 10] who have also worked on this nonlinearity asked for new answer to this problem. In this paper we bring a new solution to improve the evaluation of the nonlinearity of the Carlet-Feng function, by means of the estimation of the distribution of Gauss sums. We will find a slightly better asymptotic bound (see (2)) but this work is in progress and we give some suggestions to improve this work and hopefully to get a result closer to what expected. It will be the same for other classes of Boolean functions which are based on Carlet-Feng construction.

1.2 The nonlinearity

The nonlinearity of these functions is given by

$$nl(f) = 2^{n-1} - \max_{\lambda \in \mathbb{F}_{2^n}^*} |S_\lambda| \quad \text{where} \quad S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{\mathrm{Tr}(\lambda \alpha^i)}. \tag{1}$$

We define $\zeta = \exp\left(\frac{2i\pi}{2^n-1}\right)$, χ be the multiplicative character of $\mathbb{F}_{2^n}$ such that $\chi(\alpha) = \zeta$. For $a \in \mathbb{F}_q^*$ let us define the Gaussian sum $G(a, \chi)$ by

$$G(a, \chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \exp(\pi i \,\mathrm{Tr}(ax))$$

and $G(\chi) = G(1, \chi)$. Let $\lambda = \alpha^\ell$ with $1 \leq \ell \leq q-2$. By Fourier transformation of (1) we get

$$S_\lambda = \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} G(\chi^\mu) \zeta^{-\mu\ell} \frac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}} - \frac{q}{2} \right).$$

Carlet and Feng deduced from that the bound

$$|S_\lambda| \leq \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} \sqrt{q} \left| \frac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}} \right| + \frac{q}{2} \right).$$

The upperbound of $|S_\lambda|$ is attained if the arguments of $G(\chi^\mu)\zeta^{-\mu\ell}$ are the opposite of the ones of $\frac{\zeta^{-\mu(\frac{q}{2}-1)}-1}{1-\zeta^{-\mu}}$. I will show that this situation is impossible and that will lead us to a better bound.

2 Equidistribution of the arguments of Gauss sums

2.1 A result of Nicolas Katz

Nicolas Katz (chapter 9 in [5]) has proved that

Proposition 2.1 *For a fixed in $\mathbb{F}_{2^n}^*$ the arguments of $G(a, \chi^\mu)$ for $1 \leq \mu \leq q-2$ are equidistributed on the segment $[-\pi, \pi]$.*

For l fixed in $\mathbb{F}_{2^n}^*$ the arguments of $G(\chi^\mu)\zeta^{-\mu l}$ for $1 \leq \mu \leq q-2$ are also equidistributed on the segment $[-\pi, \pi]$ since by [8] theorem 5.12, they satisfy: $G(\chi^\mu)\zeta^{-\mu l} = G(\alpha^l, \chi^\mu)$.

2.2 Discrepancy

To get a result a little more precise than Katz's we need the notion of discrepancy. We define the discrepancy (see [4] or [6]) of a sequence of N real numbers $x_1, \ldots, x_N \in [0,\ 1[$ by

$$D_N(x_N) = \max_{0 \le x \le 1} |\frac{A(x,N)}{N} - x|$$

where $A(x,N)$ = number of $m \le N$ such that $x_m \le x$.

Proposition 2.2 *A sequence $(x_N)_{N \ge 1}$ is uniformly distributed mod 1 if and only if*

$$\lim_{N \to \infty} D_N(x_N) = 0.$$

We have an estimate of the discrepancy thanks to Erdös-Turan-Koksma's inequality.

Lemma 2.3 (Erdös-Turan-Koksma's inequality) *There is an absolute constant C (independent of x_N) such that for every $H \ge 1$,*

$$D_N(x_N) < C\left(\frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h}\left|\frac{1}{N}\sum_{m=1}^{N} \exp(2\pi i h x_m)\right|\right)$$

We will use also a result of Deligne obtained by using Algebraic Geometry "à la Grothendieck".

Proposition 2.4 (Deligne [3]) *For ψ an additive character of $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, we have*

$$|\sum_{x_1 x_2 \ldots x_r = 1} \psi(x_1 + x_2 + \cdots + x_r)| \le r q^{(r-1)/2}.$$

With this proposition, we can show that, for $a \neq 0$ one has $|\sum_{1 \le \mu \le q-2} G(a, \chi^\mu)^r| \le 1 + r q^{(r+1)/2}$. So we can show more than Katz's result with the help of proposition (2.2).

Proposition 2.5 *For l fixed in $\mathbb{F}_{2^n}^*$ the arguments $\arg(z_\mu)$ of $z_\mu = G(\chi^\mu)\zeta^{-\mu l}$ for $1 \le \mu \le q-2$ fulfill*

$$D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) < O(q^{-1/4})$$

Proof: We use Erdös-Turan-Koksma's inequality to evaluate this dicrepancy, and use Deligne's result to bound $|\sum_{1 \le \mu \le q-2} G(a, \chi^\mu)^r|$ which gives the result. Whence, if $H \le q^{1/2}$

$$\begin{aligned} D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) &< O\left(\frac{1}{H} + \frac{1}{q-2}\sum_{h=1}^{H} \frac{1}{h q^{h/2}}\left|\sum_{\mu=1}^{q-2} G((-1)^{\mathrm{Tr}(\alpha^l)}, \chi^\mu)^h\right|\right) \\ &< O\left(\frac{1}{H} + \frac{1}{q-2}\sum_{h=1}^{H} \frac{1}{h q^{h/2}} h q^{(h+1)/2}\right) \\ &= O\left(\frac{1}{H} + \frac{H q^{1/2}}{q-2}\right) \end{aligned}$$

If $H = q^{1/4}$, then $D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) < O\left(\frac{q^{3/4}+q^{3/4}}{q-2}\right) = O\left(q^{-1/4}\right)$. □

Lemma 2.6 *If the a_m is an increasing sequence and if the discrepancy of a_m is D, then $|a_i - \frac{i}{m}| \le D$.*

Proof: The lemma is a consequence of [6, Section 2, Discrepancy, theorem 1.4]. □

3 Distribution of the arguments of a_μ

Let $a_\mu = \dfrac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}}$.

Proposition 3.1 *The a_μ are on the singular plane cubic which is the image of the unit circle by the map*

$$z \to \frac{1}{z + z^2}$$

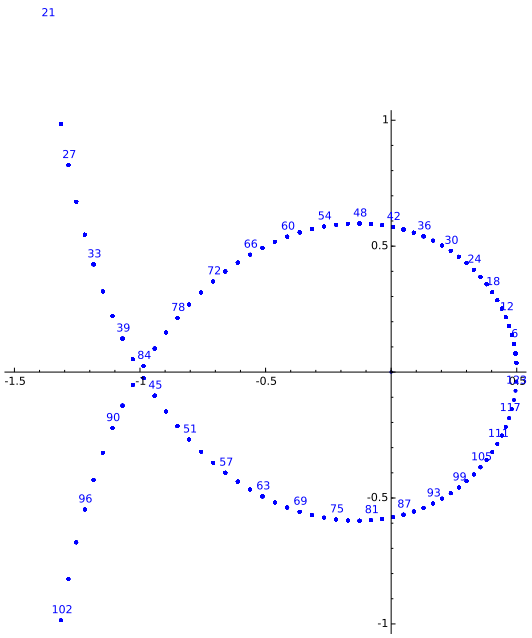
with $|z| = 1$. The absolute value is $|a_\mu| = (2\cos(\frac{\pi\mu}{2(q-1)}))^{-1}$. The argument is $\arg a_\mu = \frac{3\pi\mu}{2(q-1)}$ for μ even or $\pi/2 + \frac{3\pi\mu}{2(q-1)}$ for μ odd. The complex conjugate of a_μ is $a_{q-1-\mu}$.

Proof: If μ is even, let us take $z = \exp(-\frac{\pi\mu i}{q-1})$. One has $z^2 = \zeta^{-\mu}$. And one has also

$$z^{q-1} = \exp(-\pi\mu i) = \exp(-2\pi i\mu/2) = 1.$$

Thus $z^{q-2} = z^{-1}$, hence $a_\mu = \frac{z^{2(\frac{q}{2}-1)}-1}{1-z^2} = \frac{z^{(q-2)}-1}{1-z^2} = \frac{z^{-1}-1}{1-z^2} = \frac{1-z}{z-z^3} = \frac{1}{z+z^2}$. If μ is odd, we just use $z = -\exp(-\frac{\pi\mu i}{q-1})$. To compute the absolute value and the argument of a_μ, you just have to consider the rhombus of vertices $0, z, z + z^2, z^2$. □

3.1 Exemple: with $m = 7$



4 Applications

So we conclude from the preceding sections that for a fixed ℓ the arguments of $G(\chi^\mu)\zeta^{-\mu\ell}$ are equidistributed on $[-\pi,\ \pi]$, and the arguments of a_μ are equidistributed on $[-3\pi/2,\ 3\pi/2]$

so, as we said before, it is impossible to have $\arg(G(\chi^\mu)\zeta^{-\mu\ell}) + \arg(a_\mu) = 0 \pmod{2\pi}$ and the upperbound of $|S_\lambda|$ is not attained.
So, in place of computing the sum $\sum_{\mu=1}^{q-2} G(\chi^\mu)\zeta^{-\mu\ell}a_\mu$ we can replace it by the sum $\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)$ where $H = \{h_\mu\}$ is the set of Gauss sums and σ is some permutation of this set. Let us renumber the h_μ for μ even (with multiplicities) in the anticlockwise orientation: from h_2 which will be of weakest positive or zero argument up to h_{q-2} which will be of higher positive argument. Let $k_x = q^{1/2}\exp\left(i\left(\frac{2\pi x}{q-1}\right)\right)$. Let σ runs over the set of all permutation of the set H. The preceding proposition implies $\sum_{\mu=1}^{q-2} G(\chi^\mu)\zeta^{-\mu\ell}a_\mu \leq 2\max_\sigma\left(\Re e\sum_{\substack{\mu=2\\ \mu \text{ even}}}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)\right)$.

Lemma 4.1 *For $2 \leq \mu \leq q-2$ and μ even, we have*

$$\left|\Re e(\overline{h_{\sigma(\mu)}}a_\mu - \overline{k_{\sigma(\mu)}}a_\mu)\right| = O\left(\frac{q^{1/4}}{\cos\frac{\pi\mu}{2(q-1)}}\right)$$

Proof: We use Proposition 2.5 and Lemma 2.6. □

From Proposition 2.5, we get the following lemma.

Lemma 4.2 *The sums* $\Re e\sum_{\substack{\mu=2\\ \mu \text{ even}}}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)$ *satisfy*

$$\max_\sigma\left(\Re e\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)\right) \leq 2\Re e\sum_{\substack{\mu=2\\ \mu \text{ even}}}^{q/2}(\overline{b_\mu}a_\mu) + O(q^{5/4}\log q)$$

where we denote by b_μ the following numbers for μ even and $2 \leq \mu \leq q-2$: if $2 \leq \mu \leq q/2$, then $b_\mu = k_{\mu/2}$, if $q/2 < \mu \leq 2q/3$, then $b_\mu = k_{3\mu/2-q/2}$, if $2q/3 < \mu \leq q-2$, then $b_\mu = k_{3\mu/4}$.

Proof: We use the lemma 4.1 to replace $\max_\sigma\left(\Re e\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)\right)$ by $\max_\sigma\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}}a_\mu)\right) + O(q^{5/4}\log q)$.
Then denote by D the discrepancy of the sequence H. Let β be the largest integer (if there is some) such that $|\arg k_{\sigma(\beta)} - \arg(b_\beta)| > 2\pi D$. Then for all $\mu > \beta$ we have $|\arg k_{\sigma(\mu)} - \arg(b_\mu)| \leq 2\pi D$. From the lemma 2.6 there exists γ such that $|\arg k_{\sigma(\gamma)} - \arg(b_\beta)| \leq 2\pi D$. Let τ be the transposition between β and $\sigma(\gamma)$. Then one can check that

$$\Re e(\overline{b_\beta}a_\beta + \overline{k_{\sigma(\gamma)}}a_{\sigma(\gamma)}) > \Re e(\overline{k_{\sigma(\gamma)}}a_\beta + \overline{b_\beta}a_{\sigma(\gamma)})$$

therefore $2\Re e\sum_{\substack{\mu=1\\ \mu \text{ even}}}^{q-2}(\overline{k_{\sigma(\mu)}}a_\mu) < 2\Re e\sum_{\substack{\mu=1\\ \mu \text{ even}}}^{q-2}(\overline{k_{\sigma\circ\tau(\mu)}}a_\mu)$ and the sum is not maximal. So, if the sum is maximal, then there does not exist such a β, that is for all μ we have $|\arg k_{\sigma(\mu)} - \arg(b_\mu)| \leq 2\pi D$. Whence $\left|\Re e\sum_{\mu=1}^{q-2}(\overline{b_\mu}a_\mu) - \max_\sigma\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}}a_\mu)\right)\right| \leq O(q^{5/4}\log q)$.
Let B be the set of all b_μ's for μ even. Now we have to take also in consideration the μ odd. When you make the same reasoning, you end up with a set $\overline{B}$ which is just the complex conjugate of B. When you take the union $B \cup \overline{B}$, you get q elements uniformly distributed in the interval $[0,\ 2\pi]$. □

Proposition 4.3 *The upper bound of* $\sum_{\mu=1}^{q-2} G(\chi^\mu)\zeta^{-\mu\ell}a_\mu$ *is at most equal to*

$$\frac{q^{3/2}}{\pi}(\ln q - 0.3786 + o(1)).$$

Proof: Up to $O(q^{5/4}\log q)$ it is enough to compute:

$$\begin{aligned}\max_\sigma\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}}a_\mu)\right) &\leq 2q^{1/2}\sum_{\substack{\mu=1\\ \mu\text{even}}}^{q/2}\frac{1}{2} - 2q^{1/2}\sum_{\substack{\mu=q/2\\ \mu\text{even}}}^{2q/3}\frac{\cos\frac{3\pi\mu}{2(q-1)}}{2\cos\frac{\pi\mu}{2(q-1)}} + 2q^{1/2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}}\\ &\leq \frac{q^{3/2}}{2} - 4q^{1/2}\sum_{\substack{\mu=q/2\\ \mu\text{even}}}^{2q/3}\cos^2\frac{\pi\mu}{2(q-1)} + 2q^{1/2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}}.\end{aligned}$$

Since the function $\frac{1}{2\cos(x\pi/2)} - \frac{1}{\pi(1-x)}$ is continuous on $[2/3,\ 1]$, and since the $\frac{\mu}{q-1}$ are uniformly distributed on $[2/3,\ 1]$ we get by [6, theorem 1.1]:

$$\begin{aligned}&\frac{2}{q-2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}} - \frac{2}{\pi}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{q-\mu} = (1+o(1))\int_{2/3}^{1}\left(\frac{1}{2\cos\frac{x\pi}{2}} - \frac{1}{\pi}\frac{1}{1-x}\right)dx\\ =\ &\frac{\ln 2\ -\ln\pi + \ln 3}{\pi} - \frac{\ln(7+4\sqrt{3})}{2\pi} + o(1).\end{aligned}$$

Then, using Euler's formula on harmonic series:

$$\frac{2}{q^{1/2}(q-2)}\Re e\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}(\overline{\sigma(h_\mu)}a_\mu) \leq \frac{\log q - \ln\pi + \gamma}{\pi} - \frac{\ln(7+4\sqrt{3})}{2\pi} + o(1).$$

Finally, it is easy to compute the other terms, and we get the result. □

4.1 Final result

Having noticed that

$$\left|\sum_{\mu=1}^{q-2}G(\chi^\mu)\zeta^{-\mu\ell}a_\mu\right| \leq 2\max_\sigma\left(\Re e\sum_{\substack{\mu=2\\ \mu\text{even}}}^{q-2}(\overline{h_{\sigma(\mu)}}a_\mu)\right) + O(q^{5/4}\log q)$$

we get finally

Theorem 4.4 *The nonlinearity of the Carlet-Feng function fulfills*

$$2^{n-1} - nl(f) \leq \frac{q^{1/2}}{\pi}\left(\log q - 0.3786 + o(1)\right). \tag{2}$$

5 Conclusion

The improvement is not very important, but this argument may be optimised by

- taking in account the invariance of Gauss sums under the Frobenius automorphism;
- making it possible to make our argument work for all n instead of having an asymptotic result;
- taking in account the irregularity of the distribution of Gauss sums (one way to do this might be to look at the equidistribution of several Gauss sums simultaneously);
- improving the bound of nonlinearity for other classes of Boolean functions which are based on Carlet-Feng construction.

References

[1] Claude Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monography, Boolean Models and Methods in Mathematics, Computer Science and Engineering published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257-397, 2010.

[2] Claude Carlet, Keqin Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. Advances in cryptology- ASIACRYPT 2008, 425-440, Lecture Notes in Comput. Sci., 5350, Springer, Berlin, 2008.

[3] Deligne, P., Applications de Ia formule des traces aux sommes trigonometriques, in: Cohomologie Etale (SGA 4 1/2), Lecture Notes in Mathematics, vol. 569, Springer-Verlag.

[4] M. Drmota and R. Tichy, Sequences, discrepancies and applications, Springer-Verlag, Berlin, 1997.

[5] Katz, N.: Gauss Sums, Kloosterman Sums and Monodromy Groups, Annals of math. Studies 116, Princeton Univ. Press, 1988

[6] L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Wiley-Interscience, New York-London-Sydney, 1974.

[7] Jiao Li , Claude Carlet , Xiangyong Zeng , Chunlei Li, Lei Hu , Jinyong Shan, *Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks* Des. Codes Cryptogr. 76 (2015), no. 2, 279-305.

[8] R. Lidl, and H. Niederreiter, *Introduction to finite fields and their applications.* Cambridge university press, 1994.

[9] Tang D., Carlet C., Tang X. *Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks.* IEEE Trans. Inform. Theory 59 (2013), no. 1, 653-664.

[10] Qichun Wang, Pantelimon Stanica, Trigonometric Sum Sharp Estimate and New Bounds on the Nonlinearity of Some Cryptographic Boolean Functions, Des. Codes Cryptogr. 87 (2019), no. 8, 1749-1763.