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.