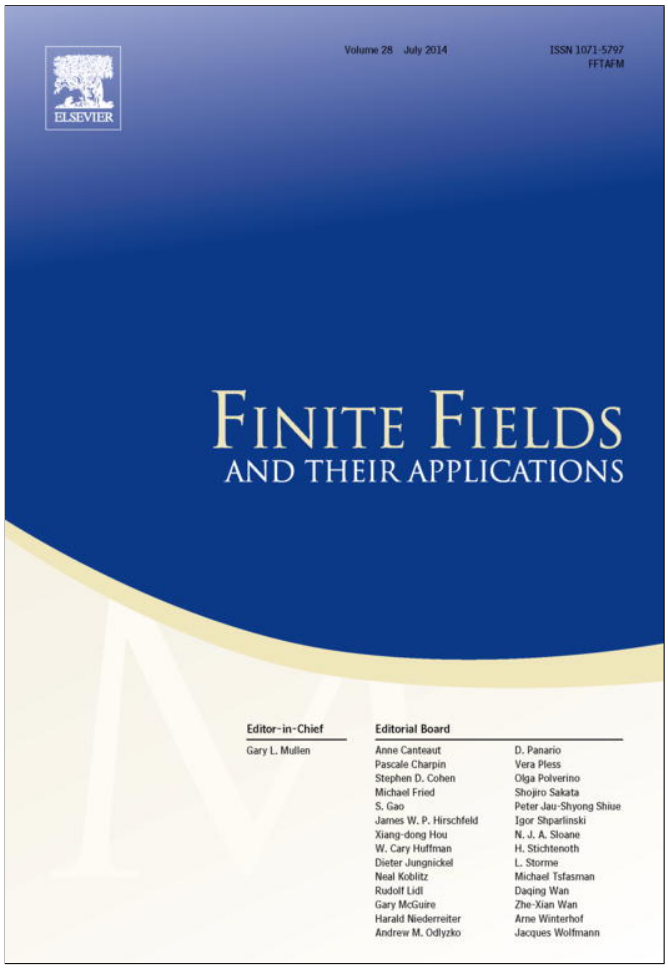

Finite Fields and Their Applications 28 (2014) 214–243

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Sparse permutations with low differential uniformity

Pascale Charpin [a,*], Gohar M. Kyureghyan [b], Valentin Suder [a]

[a] *INRIA projet SECRET, B.P. 105, 78153 Le Chesnay Cedex, France*
[b] *Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany*

ARTICLE INFO

Article history:
Received 13 May 2013
Received in revised form 7 February 2014
Accepted 10 February 2014
Available online 17 March 2014
Communicated by Rudolf Lidl

MSC:
12Y05
11T06
11T71

Keywords:
Permutation
Boolean function
Monomial function
Quadratic function
APN function
AB function
Cryptographic criteria
Differential uniformity

ABSTRACT

We study the functions $F_{s,t,\gamma}(x) = x^s + \gamma Tr(x^t)$ on $\mathbb{F}_{2^n}$. We describe the set of such permutations and the explicit expressions of their compositional inverses. Further we consider special classes of such functions, for which we determine the size of their image set, the algebraic degree and the differential uniformity.

* Corresponding author.
E-mail addresses: Pascale.Charpin@inria.fr (P. Charpin), Gohar.Kyureghyan@ovgu.de (G.M. Kyureghyan), Valentin.Suder@inria.fr (V. Suder).

http://dx.doi.org/10.1016/j.ffa.2014.02.003
1071-5797/

1. Introduction

To protect a block cipher against classical cryptanalysis, the involved functions must satisfy several criteria. Currently the best understood classes with respect to properties required in cryptology are monomial and quadratic ones. However quadratic functions are not suitable for many applications since they have small algebraic degree. Also the use of monomial functions in block ciphers is often criticized, since they exploit only the multiplicative structure of the underlying finite field.

The best resistance to differential attacks provide the *almost perfect nonlinear* (APN) functions. The classification of APN functions is far from being achieved. In particular, the existence of APN functions which permute $\mathbb{F}_{2^n}$, when n is even, is the mystery of the research on APN functions. Such functions exist for $n = 6$ as shown by the group of John Dillon [15]. However no example for even $n \geqslant 8$ is known.

We say that a function is *sparse* when it is expressed by a polynomial consisting of few non-zero terms. It is currently believed that APN sparse functions are rare, leading to more general studies on functions with low differential uniformity (see recent papers [2–4,7,23,24,26,27]).

In this paper, we construct sparse functions and explore their properties. In particular we are interested in the algebraic degree, the capacity to resist to differential attacks and the bijectivity of these functions. More precisely, we consider the functions

$$F_{s,t,\gamma}: \quad x \mapsto x^s + \gamma\, Tr\big(x^t\big) \tag{1}$$

on $\mathbb{F}_{2^n}$, where γ is a fixed non-zero element of $\mathbb{F}_{2^n}$, s, t are fixed positive integers and Tr is the absolute trace function on $\mathbb{F}_{2^n}$. These functions are constructed with two monomials and therefore they admit an efficient implementation; also, they are more or less easy to study. The study of functions $F_{s,t,\gamma}$, which are permutations on $\mathbb{F}_{2^n}$, was originated by the first two authors in [11,12]. This paper concentrates on finding special classes of such families having properties required in applications.

The paper is organized as follows: The next section includes basic properties and definitions. In Section 3, we describe functions $F_{s,t,\gamma}$ which are bijective and which are 2-to-1. We present several properties on these functions. In particular, we give the expression of the inverse of those permutations and show how to construct permutations from such 2-to-1 functions. Section 4 is devoted to specific classes. We first characterize all permutations of the form $x \mapsto x^s + \gamma\, Tr(x)$: for such a function, s must be the inverse modulo $2^n - 1$ of a quadratic exponent. Thus, for odd n, such *almost bent* (AB) function is 2-to-1. For even n we get permutations with differential uniformity 4. Furthermore these functions have a high algebraic degree. In Section 4.2, we study the case where $x \mapsto x^s$ in (1) is the multiplicative inverse function. Notably in this case for n even, we show that the differential uniformity of $F_{s,t,\gamma}$ is either 4 or 6 and construct permutations with differential uniformity 6. We also exhibit some such functions with differential uniformity 4. In Section 5, we study functions constructed with two quadratic monomials.

2. Preliminaries

In this section we recall definitions and properties which will be used later as well as the so-called *switching construction*.

2.1. Definitions and notation

Let $n \geqslant 2$ and $0 \leqslant s, t \leqslant 2^n - 1$ be integers. To identify s (resp. t) with its 2-*adic expansion* is to write

$$s = (s_0, \ldots, s_{n-1}) \quad \text{where } s = \sum_{i=0}^{n-1} s_i 2^i,\ s_i \in \{0, 1\}.$$

We call $wt(s) = \sum_{i=0}^{n-1} s_i$ the *Hamming weight* of s. We say that t *covers* s if and only if $s_i \leqslant t_i$ for all i. In this case, we use notation

$$s \preccurlyeq t \quad \text{and} \quad s \prec t \quad \text{if } s \neq t. \tag{2}$$

Any function F on $\mathbb{F}_{2^n}$ has a unique univariate polynomial representation as follows:

$$F(x) = \sum_{k=0}^{2^n-1} \alpha_k x^k, \quad \alpha_k \in \mathbb{F}_{2^n}.$$

Its *algebraic degree* is $\deg(F) = \max\{wt(k) \mid \alpha_k \neq 0\}$. The *derivative of* F in the direction a is the function $x \mapsto F(x) + F(x + a)$. The resistance of F to differential cryptanalysis is related to the following quantities:

Definition 1. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For any a and b in $\mathbb{F}_{2^n}$, we denote

$$\delta_F(a, b) = \left|\left\{x \in \mathbb{F}_{2^n},\ F(x) + F(x + a) = b\right\}\right|,$$

where $|E|$ is the cardinality of any set E, and

$$\delta(F) = \max_{a \neq 0, b \in \mathbb{F}_{2^n}} \delta_F(a, b).$$

The functions such that $\delta(F) = 2$, are said to be *almost perfect nonlinear* (*APN*). A function F is said to be *differentially k-uniform* if $\delta(F) = k$.

The following lemma is well-known and easy to prove.

Lemma 1. *Let F be a permutation of $\mathbb{F}_{2^n}$ and denote its compositional inverse by F^{-1}. Then $\delta_F(a, b) = \delta_{F^{-1}}(b, a)$ for any a, b. Consequently, $\delta(F) = \delta(F^{-1})$.*

The function F can also be represented by $2^n - 1$ Boolean functions

$$f_\lambda: \quad x \in \mathbb{F}_{2^n} \mapsto Tr\big(\lambda F(x)\big), \quad \lambda \in \mathbb{F}_{2^n}^*,$$

which are called the *component* functions of F.

We denote by $wt(g)$ the Hamming weight of a Boolean function g, i.e., the number of $x \in \mathbb{F}_{2^n}$ such that $g(x) = 1$. The *nonlinearity* $n\ell(f)$ of a Boolean function f is its Hamming distance to the set of all affine functions:

$$n\ell(f) = \min_{\beta \in \mathbb{F}_{2^n}, \epsilon \in \mathbb{F}_2} wt\big(f + Tr(\beta x) + \epsilon\big).$$

Further, the nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as follows

$$\mathcal{NL}(F) = \min_{\lambda \in \mathbb{F}_{2^n}^*} n\ell(f_\lambda). \tag{3}$$

The nonlinearity of F measures its vulnerability to linear attacks. The functions that have maximal nonlinearity are called *almost bent* (AB). The *Walsh transform* of F, denoted by W_F, is defined as

$$W_F(\lambda, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x) + \beta x)}, \tag{4}$$

for any $\beta \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$. For any fixed λ, the mapping $\beta \mapsto W_F(\lambda, \beta)$ is the Walsh transform of the component function f_λ. If there is an integer ℓ, such that $W_F(\lambda, \beta) \in \{0, \pm 2^\ell\}$ for all β, then the Boolean function f_λ is called *plateaued*. In particular it is said to be *bent* when $W_F(\lambda, \beta) \in \{\pm 2^{n/2}\}$ for even n. Moreover, F is called *plateaued* when all its component functions f_λ are plateaued.

Definition 2. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be almost bent (AB) if and only if its Walsh transform takes values $0, \pm 2^{\frac{n+1}{2}}$ only. Consequently, AB functions exist only for n odd.

Note that

$$W_F(\lambda, \beta) = 2^n - 2wt(f_{\lambda,\beta}), \quad \text{where } f_{\lambda,\beta}(x) = Tr\big(\lambda F(x) + \beta x\big).$$

We denote by $\mathcal{W}(F)$ the multiset of the values of the Walsh transform of F. Now, suppose that F is a permutation of $\mathbb{F}_{2^n}$ and F^{-1} its inverse. Then

$$wt(f_{\lambda,\beta}) = wt\big(y \mapsto \lambda y + \beta F^{-1}(y)\big).$$

This implies that $\mathcal{W}(F) = \mathcal{W}(F^{-1})$; in particular $\mathcal{NL}(F) = \mathcal{NL}(F^{-1})$ and we have clearly:

Lemma 2. *Let F be an AB permutation of $\mathbb{F}_{2^n}$ (with n odd). Then F^{-1} is an AB permutation too.*

It is also known that any AB function is an APN function. More details on APN/AB functions can be found, for instance, in [1,2,14,16] and lists of known such functions in [6,9].

2.2. Permutations by switching

In [11] and [12], the authors are interesting in functions of the shape $G(x)+\gamma\, Tr(H(x))$ which permute $\mathbb{F}_{2^n}$. We first recall a general result based on the existence of a linear structure for Boolean functions.

Definition 3. Let f be a Boolean function on $\mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$. We say that $\alpha \in \mathbb{F}_{2^n}^*$ is a c-linear structure of f if

$$f(x) + f(x+\alpha) = c \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

Theorem 1. *(See [10, Theorem 2].) Let G be a permutation on $\mathbb{F}_{2^n}$, f be any Boolean function on $\mathbb{F}_{2^n}$. Then the function*

$$F(x) = G(x) + \gamma f(x), \quad \gamma \in \mathbb{F}_{2^n}^*, \tag{5}$$

is a permutation of $\mathbb{F}_{2^n}$ if and only if γ is a 0-linear structure of $f \circ G^{-1}$, where G^{-1} denotes the compositional inverse function of G.

Remark 1.

(a) Let F be defined by (5). For any $y = F(x)$ then

$$G^{-1}\big(G(x)\big) = x = G^{-1}\big(y + \gamma f(x)\big).$$

Since f is a Boolean function, the preimages of y (by F) contain at most two elements.

(b) Assume that $f(x) = Tr(x)$ in (5). The function F can be a permutation only if the Boolean function $x \mapsto Tr(G^{-1}(x))$ has a linear structure. We study the case where G is a monomial in Section 4.1 later.

For all permutations described by Theorem 1, we can compute their inverses using the knowledge of the inverse of G. We first give a result which is an instance of [19, Theorem 3]. We include the proof for clarity.

Lemma 3. *Let $Q(x) = x + \gamma g(x)$ be a function on $\mathbb{F}_{2^n}$ where $\gamma \in \mathbb{F}_{2^n}^*$ is a 0-linear structure of the Boolean function g. Then Q is involutive, i.e., $Q \circ Q$ equals the identity function.*

Proof. By hypothesis, we have: $g(x) + g(x + \gamma) = 0$ for all x. Now

$$Q\big(Q(x)\big) = \big(x + \gamma g(x)\big) + \gamma g\big(x + \gamma g(x)\big),$$

where clearly $Q(Q(x)) = x$ when $g(x) = 0$. When $g(x) = 1$

$$Q\big(Q(x)\big) = x + \gamma + \gamma g(x + \gamma) = x + \gamma + \gamma g(x) = x. \qquad \square$$

Theorem 2. *Let F be defined by (5) with the same hypothesis on G and f. Assume that F is a permutation. Then*

$$F^{-1} = G^{-1} \circ Q \quad \text{where } Q(x) = x + \gamma f\big(G^{-1}(x)\big).$$

Proof. Set $g = f \circ G^{-1}$. From Theorem 1, γ is a 0-linear structure of g. So, we can apply Lemma 3: Q is involutive. And we have for any x

$$\begin{aligned} F\big(G^{-1} \circ Q\big)(x) &= G\big(G^{-1} \circ Q\big)(x) + \gamma f\big(G^{-1} \circ Q\big)(x) \\ &= Q(x) + \gamma f\big(G^{-1}\big(Q(x)\big)\big) = (Q \circ Q)(x) = x. \qquad \square \end{aligned}$$

In [8] it was observed that any function $F(x) = G(x) + Tr(H(x))$ satisfies $\delta(F) \leqslant 4$ as soon as G is APN. A more general version of this fact was given in [12].

Proposition 1. *(See [12, Proposition 3].) Let G and H be functions on $\mathbb{F}_{2^n}$ and $\delta(G) = \rho$. Then the function $F(x) = G(x) + \gamma\, Tr(H(x))$ satisfies $\delta(F) \leqslant 2\rho$ for any $\gamma \in \mathbb{F}_{2^n}^*$.*

3. A class of sparse functions: a presentation

A class of sparse functions which, under certain hypothesis, are either bijective or 2-to-1, have a large algebraic degree and a low differential uniformity, was introduced in a recent paper [12]. In this section we recall and extend the results presented in [12, Section 4]. In particular, we are more explicit about the properties of this class, giving notably the inverse of such permutations. We also derive new permutations from such 2-to-1 functions.

Definition 4. Let us define the class of polynomials

$$F_{s,t,\gamma}(x) = x^s + \gamma\, Tr\big(x^t\big), \quad 1 \leqslant s, t \leqslant 2^n - 2,\ \gamma \in \mathbb{F}_{2^n}^*. \tag{6}$$

The corresponding function on $\mathbb{F}_{2^n}$ will be denoted by $x \mapsto F_{s,t,\gamma}(x)$.

Notation 1. Instead of $F_{s,t,\gamma}$, we will use simpler notation such as $F_{i,\gamma}, F_i, F$, as far as possible.

3.1. The subclass of permutations

First we characterize s, t, γ such that the corresponding $F_{s,t,\gamma}$ is a permutation of $\mathbb{F}_{2^n}$. In this context, note that s must satisfy $\gcd(s, 2^n - 1) = 1$:

Lemma 4. *If* $\gcd(s, 2^n - 1) > 1$ *then* $F_{s,t,\gamma}$ *is neither a permutation nor a* 2*-to-*1 *function on* $\mathbb{F}_{2^n}$.

Proof. Let $\ell = \gcd(s, 2^n - 1)$ with $\ell \geqslant 3$. Then there are exactly ℓ different elements $x_1, \ldots, x_\ell \in \mathbb{F}_{2^n}$, such that $x_i^s = \omega$ for some $\omega \in \mathbb{F}_{2^n}$, for $1 \leqslant i \leqslant \ell$. We have

$$F_{s,t,\gamma}(x_i) \in \{\omega, \omega + \gamma\}, \quad \text{for all } i \in [1, \ell].$$

Thus, $F_{s,t,\gamma}$ is not a permutation. Moreover, if $\ell \geqslant 5$ then $F_{s,t,\gamma}$ clearly cannot be 2-to-1 too. Assume that $\ell = 3$ and $F_{s,t,\gamma}$ is 2-to-1. Then there is $z \in \mathbb{F}_{2^n}$, $z \neq x_i$ for all i, such that $F_{s,t,\gamma}(z) \in \{\omega, \omega + \gamma\}$. This implies $z^s = \omega + \gamma$. But then there are further two elements z_1, z_2 such that $z_i^s = z^s$ implying $F_{s,t,\gamma}(z_i) \in \{\omega, \omega + \gamma\}$, a contradiction. □

The proof of the next theorem is given briefly in [12, Theorem 7], as an application. For clarity, we detail the proof below.

Theorem 3. *Let* $F_{s,t,\gamma}(x) = x^s + \gamma\, Tr(x^t)$ *with* $\gamma \in \mathbb{F}_{2^n}^*$. *Then* $F_{s,t,\gamma}$ *is a permutation on* $\mathbb{F}_{2^n}$ *if and only if* $\gcd(s, 2^n - 1) = 1$,

$$t \equiv 2^j \left(2^i + 1\right) s \pmod{2^n - 1} \quad \text{for some } 0 \leqslant i, j \leqslant n - 1,\ i \neq n/2,$$

and either (a) *or* (b) *holds:*

(a) $i = 0$ *and* $Tr(\gamma) = 0$.
(b) $i > 0$ *and* $\gamma \in \mathbb{F}_{2^k}$ *with* $Tr(\gamma^{2^i+1}) = 0$, *where* $k = \gcd(2i, n)$.

Moreover, if $Tr(\gamma) = 1$, *in case* (a), *or* $Tr(\gamma^{2^i+1}) = 1$ *in case* (b), *then* $F_{s,t,\gamma}$ *is a* 2*-to-*1 *function.*

Proof. From Lemma 4, we must have $\gcd(s, 2^n - 1) = 1$. Let s^{-1} be the inverse of s modulo $2^n - 1$.

In accordance with Theorem 1, the function $F_{s,t,\gamma}$ is a permutation if and only if γ is a 0-linear structure of $Tr(x^{ts^{-1}})$. This is possible if and only if

$$ts^{-1} \equiv 2^j \left(2^i + 1\right) \pmod{2^n - 1}, \quad \text{for some } i, j,$$

from [12, Theorem 5]. Case (a) corresponds to case (i) in theorem [12, Theorem 5]. Further, (b) follows from case (ii)(a) of this theorem. In this case $Tr(x^{ts^{-1}}) = Tr(x^{2^i+1})$ and γ is a $Tr(\gamma^{2^i+1})$-linear structure of $Tr(x^{2^i+1})$ if and only if $\gamma \in \mathbb{F}_{2^k}$.

Now, if γ is a 1-linear structure of $u \mapsto Tr(u^{ts^{-1}})$ then

$$Tr\big(u^{ts^{-1}}\big) + Tr\big((u+\gamma)^{ts^{-1}}\big) = 1 \quad \text{for all } u.$$

Thus $F_{s,t,\gamma}$ is 2-to-1. Indeed, according to Remark 1, $y_0 = F_{s,t,\gamma}(x)$ for at most two x, say x_1 and x_2 with $x_1 = (y_0+\gamma)^{1/s}$ and $x_2 = y_0^{1/s}$. We have only to prove that they are exactly two for any y_0. We have

$$\begin{aligned} F_{s,t,\gamma}(x_1) &= y_0 + \gamma + \gamma\, Tr\big((y_0+\gamma)^{ts^{-1}}\big) = y_0 + \gamma + \gamma\big(1 + Tr\big(y_0^{ts^{-1}}\big)\big) \\ &= y_0 + \gamma\, Tr\big(x_2^t\big) = F_{s,t,\gamma}(x_2). \end{aligned}$$

This proves that $F_{s,t,\gamma}(x_1) = y_0$ implies $Tr(x_2^t) = 0$ which implies $F_{s,t,\gamma}(x_2) = y_0$, and vice-versa.[1] □

The case (a) of Theorem 3 is the trivial case where $F_{s,t,\gamma}(x) = x^s + \gamma\, Tr(x^s)$ with $\gcd(s, 2^n-1) = 1$, i.e., it is the composition of the monomial permutation x^s with the function $x \mapsto x + \gamma\, Tr(x)$, the latter is a linear permutation if and only if $Tr(\gamma) = 0$. In this case, $F_{s,t,\gamma}$ is said to be *extended affine equivalent* (EA-equivalent) to $x \mapsto x^s$ and then has the same differential properties as x^s.

Corollary 1. *Let* $F(x) = x^s + \gamma\, Tr(x^s)$ *with* $\gcd(s, 2^n-1) = 1$ *and* $Tr(\gamma) = 0$. *Set* $\delta(x \mapsto x^s) = \rho$. *Then* F *is a permutation such that* $\delta(F) = \rho$.

Combining Theorem 3 and Proposition 1, we obtain an infinite class of sparse polynomials which are bijective and have an upper bounded differential uniformity.

Corollary 2. *Assume that* s *satisfies* $\gcd(s, 2^n-1) = 1$ *and* $\delta(x \mapsto x^s) = \rho$. *Further, let* $1 \leqslant i < n/2$, $k = \gcd(2i, n)$ *and define the function* $F_{s,i,\gamma}$ *on* $\mathbb{F}_{2^n}$ *by*

$$F_{s,i,\gamma}: \quad x \mapsto x^s + \gamma\, Tr\big(x^{s(2^i+1)}\big). \tag{7}$$

Then $F_{s,i,\gamma}$ *is a permutation when* $Tr(\gamma^{2^i+1}) = 0$ *(and a 2-to-1 function otherwise) with a provable bound on the differential uniformity:*

$$\delta(F_{s,i,\gamma}) \leqslant 2\rho.$$

[1] Note that this property was proved in a more general context (for any characteristic) by [11, Theorem 3].

Remark 2. We use the notation of Theorem 3.

(a) If n is odd then $k = \gcd(i, n)$ with k odd. Then $\gamma^{2^i} = \gamma$ so that $Tr(\gamma^{2^i+1}) = Tr(\gamma)$. For $n = 2m$ we have $k = 2\gcd(i, m)$.
(b) One can choose s and 2^i+1 as the smallest elements of their cyclotomic coset. Indeed $F_{s,2s(2^i+1),\gamma} = F_{s,s(2^i+1),\gamma}$ and

$$\left(F_{s,s(2^i+1),\gamma}(x)\right)^2 = x^{2s} + \gamma^2 Tr\left(x^{s(2^i+1)}\right).$$

(c) If $x \mapsto x^s$ is APN then $\delta(F_{s,s(2^i+1),\gamma}) \in \{2, 4\}$.

We conclude this section with some remarks on the permutations $F_{s,t,\gamma}$ with low differential uniformity.

Proposition 2. *Consider the function* $F_{s,t,\gamma}(x) = x^s + \gamma Tr(x^t)$, $\gamma \in \mathbb{F}_{2^n}^*$, $1 \leqslant s, t \leqslant 2^n - 2$, *on* $\mathbb{F}_{2^n}$. *Then we have:*

(i) *If* n *is even and* $x \mapsto x^s$ *is APN then* F *is not a permutation.*
(ii) *Let* n *be odd and* $t = s(2^i + 1)$ *where* $\gcd(i, n) = 1$. *Then* F *is not a permutation. It is a* 2*-to-*1 *function when* $\gcd(s, 2^n - 1) = 1$ *and* $\gamma = 1$.

Proof. (i) It is well known that if $x \mapsto x^s$ is APN then $\gcd(s, 2^n - 1) = 1$ when n is odd and $\gcd(s, 2^n - 1) = 3$ when n is even (see a proof in [1, Proposition 3]). Thus, $x \mapsto x^s$ is not bijective for n even. From Theorem 3, F cannot be a permutation.

(ii) We again apply Theorem 3 for odd n. When $\gcd(i, n) = 1$ we must have $\gamma \in \mathbb{F}_2$ to build a permutation F. Since n is odd, $Tr(1) = 1$ so that F is 2-to-1. □

The functions $F_{s,t,\gamma}$ which are known to be *at most* differentially 4-uniform must be checked whether they are APN. Presently, such functions which are known to be APN have algebraic degree 2. Notably, the functions $x \mapsto x^3 + Tr(x^9)$, introduced in [8], are APN for any n. We consider these functions in Section 5. The next proposition shows that such a function cannot be a permutation.

Proposition 3. *There is no permutation on* $\mathbb{F}_{2^n}$ *of the shape*

$$F(x) = x^{2^j+1} + \gamma Tr\left(x^{(2^i+1)(2^j+1)}\right) \quad \textit{with } \gcd(j, n) = 1 \textit{ and } \gcd(i, n) = 1.$$

This holds in particular for $x \mapsto x^3 + \gamma Tr(x^9)$, *for any* $\gamma \in \mathbb{F}_{2^n}^*$ *and any* n.

Proof. Since $x \mapsto x^{2^j+1}$ is APN, then F is not a permutation for n even, according to Proposition 2(i). For n odd, we apply Proposition 2(ii). □

Example 1. Let $s = 2^{2i} - 2^i + 1$ with $\gcd(i, n) = 1$ be the so-called *Kasami exponent*, and

$$F(x) = x^s + \gamma Tr\left(x^{2^{3i}+1}\right).$$

Note that $x \mapsto x^s$ is APN and that $2^{3i} + 1 = (2^i + 1)s$. So $\delta(F) \leqslant 4$. For even n, F cannot be a permutation. If n is odd then F is a 2-to-1 function for $\gamma = 1$. For $i = 1$ we get $F_{3,9,1}$ which is APN for any n.

3.2. The inverse of permutations of type (6)

Here, we give the inverse of permutations, say F, defined by Theorem 3. Note that the inverse F^{-1} can have a large number of terms and a high algebraic degree while it has the same nonlinearity and the same differential uniformity as F.

Theorem 4. *Let $F_{s,t,\gamma}$ be a permutation on $\mathbb{F}_{2^n}$, defined as in Theorem 3 with $t = s(2^i+1)$ for some i. Let $\sigma = s^{-1} \pmod{2^n - 1}$. Then,*

$$\begin{aligned} F^{-1}_{s,t,\gamma}(x) &= \left(x + \gamma Tr\left(x^{2^i+1}\right)\right)^{\sigma} \\ &= x^{\sigma} + \left(\sum_{j \prec \sigma} x^j \gamma^{\sigma - j}\right) Tr\left(x^{2^i+1}\right). \end{aligned}$$

Proof. We apply Theorem 2, with $G(x) = x^s$ (and thus $G^{-1}(x) = x^{\sigma}$) and

$$Q(x) = x + \gamma Tr\left(\left(G^{-1}(x)\right)^t\right) = x + \gamma Tr\left(x^{t\sigma}\right) = x + \gamma Tr\left(x^{2^i+1}\right).$$

Hence $F^{-1}_{s,t,\gamma} = G^{-1} \circ Q$. More precisely

$$F^{-1}_{s,t,\gamma}(x) = \left(x + \gamma Tr\left(x^{2^i+1}\right)\right)^{\sigma} = \sum_{j \preccurlyeq \sigma} x^j \left(\gamma Tr\left(x^{2^i+1}\right)\right)^{\sigma - j}.$$

It remains to observe that $(Tr(x^{2^i+1}))^{\sigma-j} = Tr(x^{2^i+1})$ for all $j \neq \sigma$. □

According to Theorem 3, if $F_{s,t,\gamma}$ is a permutation then $\gamma \in \mathbb{F}_{2^k}$ where $k = \gcd(2i, n)$. Consequently, the function $F_{s,t,\gamma}$ as well as its inverse function have coefficients in the subfield $\mathbb{F}_{2^k}$.

Assume that $n = 2m$ and thus $k = 2\gcd(i, m)$. If $\gcd(i, m) = 1$ or $\gamma \in \mathbb{F}_{2^m}$ then $F_{s,t,\gamma}$ cannot be APN. This is because there is no APN permutation which corresponds to a polynomial in $\mathbb{F}_4[x]$ or in $\mathbb{F}_{2^m}[x]$ (see [18] and [1, Theorem 3]).

In the following example and later in this paper we consider functions $F_{s,t,\gamma}$ with $s = 2^n - 2$. Since x^{2^n-2} is the multiplicative inverse of every non-zero element $x \in \mathbb{F}_{2^n}$, it is custom to write x^{-1} instead of x^{2^n-2}, where 0^{-1} is taken to be 0.

Example 2. Notation is as in the previous theorem. Let $n = 3d$, $s = 2^n - 2$, $i = 3$, $k = \gcd(6, n)$ and consider the permutation

$$F(x) = x^{-1} + \gamma\, Tr\big(x^{-(2^3+1)}\big), \quad \gamma \in \mathbb{F}_{2^k} \text{ with } Tr\big(\gamma^9\big) = 0.$$

Then, since $x^{-1} = x^{2^n-2} = x^{2(2^{n-1}-1)}$,

$$F^{-1}(x) = x^{-1} + \left(\sum_{j=0}^{2^{n-1}-2} x^j \gamma^{2^{n-1}-j-1} \right)^2 Tr\big(x^9\big).$$

Recall that $\delta(F) = \delta(F^{-1})$. If n is odd, then $k = 3$ and $\delta(F) \leqslant 4$. Hence $\gamma \in \mathbb{F}_{2^3}$ implying $\gamma^9 = \gamma^2$ and thus

$$Tr\big(\gamma^9\big) = Tr(\gamma) = T_1^3(\gamma) = \gamma + \gamma^2 + \gamma^4.$$

So, a half of $\gamma \in \mathbb{F}_{2^3}$ satisfy $Tr(\gamma) = 0$. When $n = 2m$ then $k = 6$ and $\gamma \in \mathbb{F}_{2^6}$. We will prove later, by Lemma 5, that in this case $4 \leqslant \delta(F) \leqslant 6$.

Proposition 4. *Let $F_{s,t,\gamma}$ be a permutation on $\mathbb{F}_{2^n}$ with $n = 2m$ and $\gamma \in \mathbb{F}_{2^k}$ where $k = 2\gcd(i, m)$ and $e = \gcd(i, m)$.*

If $\gamma \in \mathbb{F}_4$ or $\gamma \in \mathbb{F}_{2^e}$ then $F_{s,t,\gamma}$, as well as its inverse, cannot be APN.

Remark 3. According to the previous proposition, F is possibly APN when $\gamma \in \mathbb{F}_{2^k} \setminus (\mathbb{F}_4 \cup \mathbb{F}_{2^e})$, but there is no example of such APN function.

Remark 4. The algebraic degree of the inverse of the function $F_{s,t,\gamma}$ is clearly less than or equal to $wt(s^{-1}) + 1$. It seems difficult to have more explicit results for general cases. But we can have improvements for special classes (see, for example, Theorem 6). The value of $wt(s^{-1})$ is studied in [21].

We conclude this section with a brief discussion on the nonlinearity of functions $F_{s,t,\gamma}$. Recall that we denote by $\mathcal{NL}(F)$ the nonlinearity of a function F on $\mathbb{F}_{2^n}$ and by $n\ell(f)$ the nonlinearity of a Boolean function f (see Section 2.1).

Consider any function $F_{s,t,\gamma} = x^s + \gamma\, Tr(x^t)$ of type Definition 4 and denote by f_λ, $\lambda \in \mathbb{F}_{2^n}^*$, its component functions. According to (3), we have here

$$\mathcal{NL}(F_{s,t,\gamma}) = \min_{\lambda \in \mathbb{F}_{2^n}^*} \left\{ n\ell(f_\lambda),\ f_\lambda(x) = \begin{cases} Tr(\lambda x^s) & \text{if } Tr(\lambda\gamma) = 0 \\ Tr(\lambda x^s + x^t) & \text{if } Tr(\lambda\gamma) = 1 \end{cases} \right\}. \tag{8}$$

To compute the multiset $\mathcal{W}(F_{s,t,\gamma})$ collecting the values of the Walsh transform of $F_{s,t,\gamma}$ as defined by (4), seems a difficult problem. It is clear that it is related with the values of $\mathcal{W}(G)$ with $G(x) = x^s$. Also, when G is a permutation and $t = (2^i + 1)s$, the

nonlinearity of the Boolean function $x \mapsto Tr(x^{2^i+1})$ is involved since the weight of f_λ, when $Tr(\lambda) = 1$, equals the weight of

$$g_\lambda(y) = Tr\big(\lambda y + y^{2^i+1}\big), \quad \text{taking } y = x^s.$$

If $F_{s,t,\gamma}$ is bijective the components of its inverse function have a more complicated expression, according to Theorem 4.

Problem 1. Not much is known about the Walsh spectrum of functions which are built with two monomials. The main results are obtained for quadratic such functions (see a survey in [5] and the recent paper [7]). It is an open problem to find any general property in this context.

3.3. The case of 2-to-1 functions

Consider the function on $\mathbb{F}_{2^n}$ given by

$$F_{s,i,\gamma}(x) = x^s + \gamma\, Tr\big(x^{s(2^i+1)}\big), \quad \text{with } i > 0 \text{ and } \gcd\big(s, 2^n - 1\big) = 1. \tag{9}$$

Assume that $\gamma \in \mathbb{F}_{2^k}$ with $k = \gcd(2i, n)$. Then, according to Theorem 3, $F_{s,i,\gamma}$ is a 2-to-1 function on $\mathbb{F}_{2^n}$ if and only if $Tr(\gamma^{2^i+1}) = 1$. The next theorem shows that also in this case we can construct a new permutation.

Theorem 5. *Consider a function $F_{s,i,\gamma}$, defined by (9) such that $\gamma \in \mathbb{F}_{2^k}$ with $k = \gcd(2i, n)$. Denote by ρ the differential uniformity of $x \mapsto x^s$ and let $\sigma = s^{-1} \pmod{2^n - 1}$. Then the function*

$$G_{s,i,\gamma}(x) = x^s + \gamma\, Tr\big(x^{s(2^i+1)} + \gamma^{2^i} x^s\big)$$

is a permutation on $\mathbb{F}_{2^n}$ and its inverse is as follows:

$$G^{-1}_{s,i,\gamma}(x) = x^\sigma + \left(\sum_{j \prec \sigma} x^j \gamma^{\sigma - j}\right) Tr\big(x^{2^i+1} + \gamma^{2^i} x\big).$$

Furthermore, $\delta(G_{s,i,\gamma}) \leqslant 2\rho$. In particular, for any odd n, if $x \mapsto x^s$ is APN, then the differential uniformity of permutations $G_{s,i,\gamma}$ is at most 4.

Proof. We apply Theorem 1. The function

$$R(y) = y + \gamma\, Tr\big(y^{2^i+1} + \gamma^{2^i} y\big) = y + \gamma f(y)$$

is a permutation on $\mathbb{F}_{2^n}$, since γ is a 0-linear structure of f. Indeed, since $\gamma \in \mathbb{F}_{2^k}$ where k divides $2i$, we have

$$Tr\big(y^{2^i+1} + (y+\gamma)^{2^i+1} + \gamma^{2^i+1}\big) = Tr\big(y^{2^i}\big(\gamma^{2^{2i}} + \gamma\big) + 2\gamma^{2^i+1}\big) = 0,$$

for all $y \in \mathbb{F}_{2^n}$. Since $y \mapsto y^s$ is a permutation, the composition $y \mapsto R(y^s)$ is a permutation too. Note that $G_{s,i,\gamma}(y) = R(y^s)$. Hence the inverse of $G_{s,i,\gamma}(y)$ is $(R^{-1}(y))^\sigma = (R(y))^\sigma$, where the latter equality holds by Lemma 3. Steps of the proof of Theorem 4 yield the expression for $G^{-1}_{s,i,\gamma}$. Proposition 1 completes the proof. □

Remark 5. In the previous method we can use $\gamma = 1$ when n is odd. Indeed, for any n (odd and even) the functions

$$G(x) = x^s + Tr\left(x^{s(2^i+1)} + x^s\right) \tag{10}$$

are permutations on $\mathbb{F}_{2^n}$. Such an example is treated in Proposition 8 later.

4. On specific classes

In this section, we study some specific classes of functions $F_{s,t,\gamma}$. Our main purpose is to exhibit such functions with low differential uniformity, which are preferably bijective. As we showed in the previous sections, it is easy to construct functions $F_{s,t,\gamma}$ with differential uniformity at most 4. For odd prime n, they are not bijective, but they are 2-to-1 functions, which is also of interest. When n is even, we get easily permutations with differential uniformity at most 8. It is known that, in this case, bijective functions with differential uniformity 4 are rare. We describe in this section two classes of functions $F_{s,t,\gamma}$ for which the differential uniformity is better than the bound of Proposition 1.

4.1. The functions $F_{s,1,\gamma}$

We determine here all permutations of the type $x^s + \gamma\, Tr(x)$ and give their parameters. This problem is an instance of the study of bijectivity of functions $x^s + L(x)$, where L is a linear function over $\mathbb{F}_2$, see [23,24]. A generalization to odd characteristic for $s = -1$ appeared recently in [17]. Here we consider the functions

$$F_{s,\gamma}(x) = x^s + \gamma\, Tr(x), \qquad \gcd\left(s, 2^n - 1\right) = 1, \quad \gamma \in \mathbb{F}^*_{2^n}, \tag{11}$$

where s is not a power of 2. Recall that, according to Theorem 3, the condition $\gcd(s, 2^n - 1) = 1$ is necessary in order to have $F_{s,\gamma}$ bijective.

Theorem 6. *A function $F_{s,\gamma}$, defined by (11), is bijective if and only if*

$$s = \frac{2^j}{2^i + 1} \pmod{2^n - 1} \quad \textit{for some } i, j \textit{ with } i > 0,$$

and both of the following conditions hold:

- *n/ℓ odd, with $\ell = \gcd(i, n)$;*
- *$\gamma \in \mathbb{F}_{2^k}$, $k = \gcd(2i, n)$, such that $Tr(\gamma^{2^i+1}) = 0$.*

In this case,

$$\delta(F_{s,\gamma}) = 2^{\ell} \quad \textit{and} \quad \deg(F_{s,\gamma}) = \frac{n-\ell+2}{2}.$$

The nonlinearity of $F_{s,\gamma}$ equals the nonlinearity of $x \mapsto x^{2^i+1}$. Moreover

$$F_{s,\gamma}^{-1} = x^{2^i+1} + \left(\gamma^{2^i+1} + \gamma^{2^i} x + \gamma x^{2^i}\right) Tr\left(x^{2^i+1}\right)$$

with $\deg(F_{s,\gamma}^{-1}) = 3$ and $\mathcal{NL}(F_{s,\gamma}^{-1}) = \mathcal{NL}(F_{s,\gamma}) = 2^{n-1} - 2^{(n+k-2)/2}$. All component functions of $F_{s,\gamma}$ and of its inverse are plateaued.

Proof. Let $g_s(x) = x^s$ and $\ell = \gcd(i,n)$. We first apply Theorem 1 to $F_{s,\gamma}(x) = g_s(x) + \gamma\, Tr(x)$. The function $F_{s,\gamma}$ is bijective if and only if γ is a 0-linear structure of $Tr(x^{1/s})$. We know from [12, Theorem 5] that such a monomial Boolean function has a linear structure if and only if it is quadratic. That is the case here since $2^j(1/s) = 2^i + 1$ for some i, j. Moreover for $i > 0$, the conditions on γ are obtained by Theorem 3. Note that $\gcd(s, 2^n - 1) = 1$ if and only if n/ℓ is odd, since s is the inverse of a quadratic exponent.

Thus the permutations of type (11) are of the form

$$F_{s,\gamma} = x^{\frac{2^j}{2^i+1}} + \gamma\, Tr(x), \quad n/\ell \text{ odd}, \quad \gamma \in \mathbb{F}_{2^k} \quad \text{and} \quad Tr\left(\gamma^{2^i+1}\right) = 0. \tag{12}$$

The values $\delta(a,b)$ for $F_{s,\gamma}$ are the same as those of $x \mapsto x^{2^i+1}$; they are in the set $\{0, 2^{\ell}\}$ where $\ell = \gcd(i,n)$.[2] The algebraic degree of $F_{s,\gamma}$ is obtained by computing the Hamming weight of $(2^i+1)^{-1}$: It is (see [20, Theorem 2] and [21]):

$$\frac{1}{2^i+1} = 1 + \sum_{u=1}^{n/\ell} 2^{ui-1}(-1)^u, \qquad wt\left(\frac{1}{2^i+1}\right) = \frac{n-\ell+2}{2}. \tag{13}$$

The function $F_{s,\gamma}^{-1}$ is computed by using Theorem 4 and its algebraic degree is clearly 3. For the nonlinearity, we simply look at the spectrum of component functions f_λ of $F_{s,\gamma}$. We have for any $\lambda \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^n}$

$$\begin{aligned} f_\lambda(x) + Tr(ax) &= Tr\left(\lambda\left(x^s + \gamma\, Tr(x)\right) + ax\right) \\ &= Tr\left(\lambda x^s + x Tr(\lambda\gamma) + ax\right) \\ &= Tr\left(y^{2^i+1}\left(Tr(\lambda\gamma) + a\right) + \lambda y\right), \quad a \in \mathbb{F}_{2^n}^*, \end{aligned}$$

where $y^{2^i+1} = x$. We get values of the spectrum of $x \mapsto x^{2^i+1}$ which is $\{0, \pm 2^{(n+k)/2}\}$ and it is the same for the spectrum of $F_{s,\gamma}^{-1}$ (see Sections 2.1 and 3.2). □

[2] These quadratic functions are *two-valued* as was explained in [2, Section 5]; the same holds for some Kasami exponents.

We now consider the functions $F_{s,\gamma}$ which have the lowest differential uniformity, that is $\delta(F_{s,\gamma}) = 4$ for even n and $\delta(F_{s,\gamma}) = 2$ for odd n.

Corollary 3. *Let $n = 2m$ with m odd. Let an integer i be such that $2 \leqslant i \leqslant m$ and $\gcd(i, n) = 2$. Let $\gamma \in \mathbb{F}_{2^n}^*$. Then the function*

$$F_{i,\gamma}(x) = x^{\frac{1}{2^i+1}} + \gamma Tr(x)$$

is a permutation on $\mathbb{F}_{2^n}$ if and only if $\gamma = 1$. It is a 2-to-1 function when $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Moreover this function is plateaued and satisfies

$$\delta(F_{i,\gamma}) = 4, \qquad \deg(F_{i,\gamma}) = m \quad \text{and} \quad \mathcal{NL}(F_{i,\gamma}) = 2^{n-1} - 2^{\frac{n}{2}}.$$

When $F_{i,\gamma}$ is a permutation, its inverse is

$$F_{i,\gamma}^{-1}(x) = x^{2^i+1} + \left(1 + x + x^{2^i}\right) Tr\left(x^{2^i+1}\right),$$

which has same differential uniformity and same nonlinearity as $F_{i,\gamma}$.

Proof. We apply Theorem 6. Note that $x \mapsto x^{2^i+1}$ is a permutation on $\mathbb{F}_{2^n}$, since $n/\gcd(i, n) = m$ where m is odd. Also $k = \gcd(2i, n) = 2$. Then $F_{i,\gamma}$ is a permutation if and only if $\gamma \in \mathbb{F}_4^*$ and $Tr(\gamma^{2^i+1}) = 0$. In this case, since i is even,

$$Tr\left(\gamma^{2^i+1}\right) = Tr(\gamma) = m \cdot \left(\gamma + \gamma^2\right) = \begin{cases} 0 & \text{if } \gamma \in \{0, 1\}, \\ 1 & \text{otherwise.} \end{cases}$$

So, only $\gamma = 1$ is possible. The proof is completed by applying directly Theorem 6. □

Remark 6. In the permutations $F_{i,\gamma}$ defined by Corollary 3, the expression of $s = (1 + 2^i)^{-1}$ is

$$s = 1 + \sum_{\ell=1}^{m} (-1)^\ell 2^{i\ell-1} \pmod{2^n - 1}, \qquad wt(s) = \frac{n}{2} = m$$

(according to (13)). In a recent paper [7], the authors point out that few permutations on $\mathbb{F}_{2^n}$, with n even, are known, which are differentially 4-uniform and have a high nonlinearity. By Corollary 3, we extend [7, Table 1]. Although $F_{i,\gamma}$ is derived from quadratic monomials, it is of high algebraic degree.

Corollary 4. *Let n be odd.*

(a) *If $2 \leqslant i \leqslant n$ with $\gcd(i, n) = 1$, then the function*

$$F_i(x) = x^{\frac{1}{2^i+1}} + Tr(x)$$

is 2-to-1 function which is AB of algebraic degree $(n + 1)/2$.

(b) *If* $2 \leqslant i \leqslant n$ *with* $\gcd(i,n) = 3$ *and* $\gamma \in \mathbb{F}_8$ *with* $Tr(\gamma) = 0$, *then the function*

$$F_{i,\gamma}(x) = x^{\frac{1}{2^i+1}} + \gamma\, Tr(x)$$

is a permutation on $\mathbb{F}_{2^n}$. *Moreover,* $\delta(F_{i,\gamma}) = 8$ *and* $\deg(F_{i,\gamma}) = (n-1)/2$.

Proof. When $\gcd(i,n) = 1$, the function $x \mapsto x^{2^i+1}$ is an AB function as well as the function $x \mapsto x^{\frac{1}{2^i+1}}$ and, further, the function F_i is also AB. The function F_i is 2-to-1 because $Tr(1) = 1$ and it is here the only possibility for γ ($\gamma = 1$ in Theorem 3). When $\gcd(i,n) > 1$ one can construct bijective functions of type $F_{i,\gamma}$. Their properties are directly obtained from Theorem 6. □

Remark 7. Note that the following functions G_i, derived from F_i above,

$$G_i(x) = x^{\frac{1}{2^i+1}} + Tr\big(x + x^{\frac{1}{2^i+1}}\big), \quad 2 \leqslant i \leqslant n \text{ with } \gcd(i,n) = 1,$$

are bijective and such that $\delta(G_i) \leqslant 4$, by Theorem 5. Actually $\delta(G_i) = 4$, since this function has a linear component function:

$$x \mapsto Tr\big(G_i(x)\big) = Tr(x).$$

Indeed, we know by [1, Theorem 2] that G_i is APN if and only if

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \Bigg(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{g_\lambda(x) + g_\lambda(x+a)} \Bigg)^2 = 2^{2n+1}, \quad \text{for all } a, \tag{14}$$

where g_λ are the component functions of G_i. If one component, say g_1, is linear then all its derivatives are constant and condition (14) cannot hold unless all g_λ, $\lambda \neq 1$, are bent, which is impossible (n is odd here).

Example 3. Let n be odd. Note that

$$\frac{1}{2^{(n+1)/2}+1} = 2^{(n+1)/2} - 1 \pmod{2^n - 1}.$$

Thus, the functions

$$F(x) = x^{2^{(n+1)/2}-1} + Tr(x) \quad \text{and} \quad G(x) = x^{2^{(n+1)/2}-1} + Tr\big(x + x^{2^{(n+1)/2}-1}\big)$$

are respectively 2-to-1 and bijective. The function F is AB while $\delta(G) = 4$.

4.2. The multiplicative inverse function

In this section, we study a subclass of functions on $\mathbb{F}_{2^n}$:

$$F(x) = x^{-1} + \gamma\, Tr\big(H(x)\big), \quad \gamma \in \mathbb{F}_{2^n}^*,$$

where $H(x)$ is any function. Actually, we will focus on the case where $H(x) = x^t$ for some t, after the general result given by Lemma 5 later. We first introduce notation and formula which will be used in all the section and do not depend on the choice of H. The (*multiplicative*) *inverse* function over a finite field is defined as $x \mapsto x^{-1} = 1/x$ assuming that $0^{-1} = 0$. A derivative of $F_{t,\gamma}$ in point $a \in \mathbb{F}_{2^n}^*$ can be written as follows

$$D_a F(x) = f_a(x) + \gamma\, Tr\big(h_a(x)\big), \quad \text{where } f_a(x) = \frac{1}{x} + \frac{1}{x+a}, \tag{15}$$

and $h_a(x) = H(x)+H(x+a)$. To compute $\delta(F)$ we must compute the number of solutions x of the equations

$$E(a,b)\colon \quad D_a F(x) = b, \quad a \in \mathbb{F}_{2^n}^*,\ b \in \mathbb{F}_{2^n}. \tag{16}$$

Note that $D_a F(x) = b$ implies $f_a(x) \in \{b, b+\gamma\}$. Also, we have:

(p1) An equation $E(a,b)$ is satisfied for $x \in \{0,a\}$ if and only if

$$\text{either} \quad b = \frac{1}{a} \quad \big(\text{with } Tr\big(h_a(0)\big) = 0\big)$$
$$\text{or} \quad b = \frac{1}{a} + \gamma \quad \big(\text{with } Tr\big(h_a(0)\big) = 1\big).$$

(p2) If $x \notin \{0,a\}$ then $f_a(x) = a(x^2+ax)^{-1}$.

(p3) Consider any equation $E(a,b)$. Then $E(a,b)$ is satisfied for x and $x+a$, with $x \notin \{0,a\}$, if and only if x satisfies at least one of these instances

$$x^2 + ax + \frac{a}{b} = 0 \quad \text{with } Tr\big(h_a(x)\big) = 0, \tag{17}$$
$$x^2 + ax + \frac{a}{b+\gamma} = 0 \quad \text{with } Tr\big(h_a(x)\big) = 1. \tag{18}$$

This is clear by writing $a(x^2+ax)^{-1} = \beta$, $\beta \in \{b, b+\gamma\}$. Note that for each such β the equation $x^2 + ax + a/\beta = 0$ has two solutions if and only if $Tr(1/(a\beta)) = 0$.

(p4) We can choose a such that

$$Tr\left(\frac{1}{a\beta}\right) = 0 \quad \text{for } \beta = \frac{1}{a} + \gamma \text{ and for any } \gamma,$$

since the function $a \mapsto 1/(1+\gamma a)$ is bijective on $\mathbb{F}_{2^n}^*$. Moreover if $\beta = 1/a$ then $Tr(1/(a\beta)) = Tr(1)$.
Thus, when n is even, there exists $a \in \mathbb{F}_{2^n}^*$ such that $Tr(1/(a\beta)) = 0$ for both $\beta = 1/a$ and $\beta = 1/a + \gamma$.

Note that we implicitly proved the well-known property that *the inverse function, say* $G(x) = x^{-1}$, *satisfies* $\delta(G) = 2$ *for odd* n *and* $\delta(G) = 4$ *for even* n [25].

Lemma 5. *Let* $F(x) = x^{-1} + \gamma\, Tr(H(x))$ *where* H *is any function on* $\mathbb{F}_{2^n}$. *Then*

$$\delta(F) \in \begin{cases} \{2,4\} & \text{when } n \text{ is odd,} \\ \{4,6\} & \text{when } n \text{ is even.} \end{cases}$$

Proof. When n is odd, it comes directly from Proposition 1; note that $\delta(F) = 2$ when H is linear.

Assume that n is even and choose a such that $Tr(1/(1+\gamma a)) = 0$ (see (p4)). According to (p1)–(p3), if $b \notin \{1/a, 1/a+\gamma\}$ then $E(a,b)$ has at most four solutions. We are going to prove that $E(a, 1/a)$ or, respectively $E(a, 1/a+\gamma)$, has at least four solutions.

We first suppose that the equation $E(a, 1/a)$ is satisfied for $x \in \{0, a\}$, i.e., that $Tr(h_a(0)) = 0$. Further, $E(a, 1/a)$ has at least two other solutions if and only if (17) or (18) holds for $x \notin \{0, a\}$. Since the choice of a, we have

$$f_a(x) = \frac{1}{a} \text{ has 2 solutions } y, y+a;$$

and

$$f_a(x) = \frac{1}{a} + \gamma \text{ has 2 solutions } z, z+a.$$

If $Tr(h_a(y)) = 0$ then y is a solution of $E(a, 1/a)$ else y is a solution of $E(a, 1/a+\gamma)$. Similarly, if $Tr(h_a(z)) = 1$ then z is a solution of $E(a, 1/a)$ else z is a solution of $E(a, 1/a+\gamma)$. This is exactly to say: if $E(a, 1/a)$ has no solution x, $x \notin \{0, a\}$, then $E(a, \gamma + 1/a)$ has four solutions y, z, $y+a$ and $z+a$.

If $Tr(h_a(0)) = 1$ then $E(a, \gamma+1/a)$ is satisfied for $x \in \{0, a\}$. Similarly, we prove that if $E(a, \gamma+1/a)$ has no solution x, $x \notin \{0, a\}$, then $E(a, 1/a)$ has four solutions. We can conclude that $\delta(F) \geqslant 4$.

Moreover, it is clear that we cannot have $\delta(F) = 8$ (when n is even). It is because an equation $E(a, b)$ can have more than four solutions only when 0 and a are solutions. In this case, $b \in \{1/a, 1/a+\gamma\}$ and for each such b the number of solutions is 4 or 6. □

Problem 2. It is of interest to study $x^{-1} + \gamma\, Tr(H(x))$ for specific classes of H. For instance, by taking $H(x) = x^2/(x+1)$, the authors of [26] obtain permutations F on $\mathbb{F}_{2^n}$ with n even and such that $\delta(F) = 4$. Does this property hold when H is a monomial? We

think that the answer is generally *no*. However it is easy to construct such permutations F with low differential uniformity as discussions of this section show.

From now on, we consider the following functions:

$$F_{t,\gamma}(x) = x^{-1} + \gamma\, Tr\big(x^t\big), \quad \gamma \in \mathbb{F}_{2^n}^*. \tag{19}$$

Proposition 5. *Let $\gamma \in \mathbb{F}_{2^n}^*$, $1 \leqslant i < n$, $i \neq n/2$, and*

$$F_{i,\gamma}(x) = x^{-1} + \gamma\, Tr\big(x^{2^{n-1}-2^{i-1}-1}\big). \tag{20}$$

Then $F_{i,\gamma}(x)$ is a permutation polynomial when

$$\gamma \in \mathbb{F}_{2^k} \quad \text{such that} \quad Tr\big(\gamma^{2^i+1}\big) = 0 \quad \text{where } k = \gcd(2i, n).$$

If $Tr(\gamma^{2^i+1}) = 1$ then $F_{i,\gamma}$ is 2-to-1. In both cases, $\delta(F_{i,\gamma}) \leqslant 4$ for odd n and $4 \leqslant \delta(F_{i,\gamma}) \leqslant 6$ for even n.

Proof. The bounds on $\delta(F_{i,\gamma})$ come from Lemma 5. Note that $-1 \equiv 2^n - 2 \pmod{2^n - 1}$ and

$$\begin{aligned}\big(2^n - 2\big)\big(2^i + 1\big) &= 2^i + 2^n - 2^{i+1} - 2 = 2^n - 2^i - 2 \\ &= 2\big(2^{n-1} - 2^{i-1} - 1\big) \pmod{2^n - 1}.\end{aligned}$$

To complete the proof, we apply Corollary 2. □

Now, we are going to study two subclasses of functions of type (19). The first subclass is given by (20) where we put $i = 1$. Note that, in this case,

$$Tr\big(x^{2^{n-1}-2^{i-1}-1}\big) = Tr\big(x^{2^{n-2}-1}\big) = Tr\big(x^{-3}\big).$$

Lemma 6. *Consider the function $F(x) = x^{-1} + Tr(x^{-3})$ on $\mathbb{F}_{2^n}$. Then we have:*

- *If n is even then F is a permutation. It satisfies $\delta(F) = 6$ if and only if there is $a \in \mathbb{F}_{2^n}^*$ such that*

$$Tr\big(a^{-3}\big) = 0, \qquad Tr\big((a+1)^{-1}\big) = 0 \quad \text{and} \quad Tr\big(a^{-1}\big) = 1.$$

- *If n is odd then F is 2-to-1. It satisfies $\delta(F) = 4$ when there is $a \in \mathbb{F}_{2^n}^*$ such that*

$$Tr\big(a^{-3}\big) = 0, \qquad Tr\big((a+1)^{-1}\big) = 0 \quad \text{and} \quad Tr\big(a^{-1}\big) = 1.$$

Proof. We apply Proposition 5. The function F is a permutation when n is even and a 2-to-1 function for odd n; we get also the upper bounds on $\delta(F)$. We use notation and formula from (19), (15) and (p1)–(p4). For any $a \in \mathbb{F}_{2^n}^*$, if $x \notin \{0, a\}$ we can write $f_a(x) = a(x^2 + ax)^{-1}$ and

$$h_a(x) = \frac{1}{x^3} + \frac{1}{(x+a)^3} = \frac{x^3 + (x+a)^3}{(x^2+ax)^3} = \frac{x^2a + xa^2 + a^3}{(x^2+ax)^3}$$
$$= \frac{a}{(x^2+ax)^2} + \big(f_a(x)\big)^3 = \frac{(f_a(x))^2}{a} + \big(f_a(x)\big)^3. \tag{21}$$

Note that

$$f_a(x) = \frac{1}{a}, \quad x \notin \{0, a\} \quad \Rightarrow \quad Tr\big(h_a(x)\big) = Tr\big(2/a^3\big) = 0. \tag{22}$$

Thus, $E(a, 1/a + 1)$ has at most 4 solutions, since $f_a(x) + Tr(h_a(x)) = 1/a + 1$ with $Tr(h_a(x)) = 1$ is impossible. For $u \in \mathbb{F}_2^3$, define the property $(\mathcal{E}_u)$ on $a \in \mathbb{F}_{2^n}^*$ as follows:

$$(\mathcal{E}_u): \quad Tr\big(a^{-3}\big) = u_1, \qquad Tr\big((a+1)^{-1}\big) = u_2 \quad \text{and} \quad Tr\big(a^{-1}\big) = u_3.$$

1. Assume that n is even. We take $u = (0, 0, 1)$. Our goal is to prove that $\delta(F) = 6$ if and only if there is a such that $(\mathcal{E}_u)$ holds. According to (22), the equation $E(a, 1/a)$ has 6 solutions x if and only if the following equations $(*)$ and $(**)$ have respectively 4 and 2 solutions

$$(*) \quad f_a(x) = \frac{1}{a} \quad \text{with } Tr\big(h_a(x)\big) = 0; \qquad (**) \quad f_a(x) = \frac{1+a}{a} \quad \text{with } Tr\big(h_a(x)\big) = 1.$$

The solutions of $(*)$ are $\{0, a\}$ and the two solutions of $x^2 + ax + a^2 = 0$. But $x = 0$ is a solution if and only if $Tr(h_a(0)) = Tr(a^{-3}) = 0$ and we get *the first condition of $(\mathcal{E}_u)$*. If $(**)$ is satisfied too then $f_a(x) = (1+a)/a$ where $a \neq 1$ because $f_a(x) = 0$ is impossible, since $x \mapsto x^{-1}$ is a permutation. $(**)$ is satisfied if and only if $Tr(1/(a+1)) = 0$ and $Tr(h_a(x)) = 1$, which is

$$Tr\big(h_a(x)\big) = Tr\left(\frac{(a+1)^3}{a^3} + \frac{(a+1)^2}{a^3}\right) = Tr\left(\frac{a^3 + a}{a^3}\right)$$
$$= Tr\big(1 + a^{-2}\big) = Tr\big(a^{-1}\big) = 1.$$

So we get respectively *the second and the third condition of $(\mathcal{E}_u)$*.

2. Assume that n is odd. The equation $E_{a,1/a}$ has 4 solutions when $(*)$ and $(**)$ have both 2 solutions. We are going to prove that it is the case when there is a such that $(\mathcal{E}_u)$ holds for $u = (0, 0, 0)$. We give a brief proof since the method is similar to even n.

The solutions of $(*)$ are $\{0, a\}$ with $Tr(a^{-3}) = 0$. Further, the equation $f_a(x) = (a+1)/a$ must have two solutions $(x, x+a)$ with $Tr(h_a(x)) = 1$. The conditions are

$$Tr\big(1/(a+1)\big) = 0 \quad \text{and} \quad Tr\big(1 + a^{-2}\big) = Tr\big(a^{-1}\big) + 1 = 1, \quad \text{i.e.} \quad Tr\big(a^{-1}\big) = 0. \qquad \square$$

For any triple $(u_1, u_2, u_3) \in \mathbb{F}_2^3$ and sufficiently large n, the existence of a satisfying $(\mathcal{E}_u)$ follows from [13, Theorem 1.1], which we adapted for our case in the next theorem. We first need the following definition:

Definition 5. Let $f_1(x), f_2(x), f_3(x) \in \mathbb{F}_{2^n}[x]$. We say that the $f_i(x)$ form a strongly linearly independent set over $\mathbb{F}_2$ if there is no $(v_1, v_2, v_3) \in \mathbb{F}_2^3$ such that

$$v_1 f_1(x) + v_2 f_2(x) + v_3 f_3(x) = h^2(x) + h(x) + \beta \tag{23}$$

for some $\beta \in \mathbb{F}_{2^n}$ and $h(x) \in \mathbb{F}_{2^n}[x]$.

Theorem 7. *(See [13].) Let $f_1(x), f_2(x), f_3(x) \in \mathbb{F}_{2^n}[x]$ form a* strongly linearly independent set *over $\mathbb{F}_2$. Further, for $1 \leqslant i \leqslant 3$ let*

$$f_i(x) = \frac{c_i(x)}{d_i(x)}, \quad \text{where } c_i(x), d_i(x) \in \mathbb{F}_{2^n}[x] \text{ are coprime polynomials.}$$

Set $m = \max\{\deg c_i(x), \deg d_i(x),\ 1 \leqslant i \leqslant 3\}$. Then there is a primitive element $\alpha \in \mathbb{F}_{2^n}$ with

$$Tr\big(f_1(\alpha)\big) = u_1, \qquad Tr\big(f_2(\alpha)\big) = u_2, \qquad Tr\big(f_3(\alpha)\big) = u_3$$

for any fixed $(u_1, u_2, u_3) \in \mathbb{F}_2^3$, whenever

$$n > 4\big(3 + \log_2(\ell m)\big), \quad \ell = 9 \cdot 8 \cdot 3. \tag{24}$$

Proposition 6. *Let $f_1(x) = x^{-3}$, $f_2(x) = (x+1)^{-1}$, $f_3(x) = x^{-1}$. Then, the $f_i(x)$ form a strongly linearly independent set over $\mathbb{F}_2$.*

Consequently, the property $(\mathcal{E}_u)$, $u \in \mathbb{F}_2^3$, holds whenever $n \geqslant 38$. In particular, in Lemma 6, F satisfies $\delta(F) = 4$ for such odd n and $\delta(F) = 6$ for such even n.

Proof. We suppose that (23) holds for some (v_1, v_2, v_3) and we write $h(x) = h_1(x)/h_2(x)$ where $h_1(x), h_2(x) \in \mathbb{F}_{2^n}[x]$ are coprime polynomials. Then we get:

$$\frac{v_1(x+1) + v_2x^3 + v_3x^2(x+1) + \beta x^3(x+1)}{x^3(x+1)} = \frac{h_1^2(x) + h_1(x)h_2(x)}{h_2^2(x)},$$

where $h_2^2(x)$ and $h_1^2(x) + h_1(x)h_2(x)$ are coprime. Therefore, we must have $h_2(x) \in \{1, x\}$, since $h_2^2(x)$ must divide $x^3(x+1)$. Hence, $x(x+1)$ divides

$$B(x) = v_1(x+1) + v_2x^3 + v_3x^2(x+1) + \beta x^3(x+1)$$

implying $B(0) = 0$ and $B(1) = 0$. This yields $v_1 = 0$ and $v_2 = 0$. Note that (23) implies now $Tr(v_3 f_3(x)) = Tr(\beta)$ for all x, which is impossible if $v_3 \neq 0$.

The inequality $n \geqslant 38$ is obtained by computing (24) with $m = 3$. We complete the proof by using Theorem 7. □

Remark 8. To extend Lemma 6, note that by Theorem 5, for odd n the function $G(x) = x^{-1} + Tr(x^{-3} + x^{-1})$, on $\mathbb{F}_{2^n}$ is a permutation such that $\delta(G) \leqslant 4$.

We noticed that sparse permutations with differential uniformity 4 are rare for even n. However there are functions $x \mapsto x^{-1} + \gamma Tr(x^t)$, on $\mathbb{F}_{2^n}$ with n even and for some t which are not bijective but have the same differential uniformity as $x \mapsto x^{-1}$.

Theorem 8. *Let n be even, $t \in \{3, 5\}$ and $\gamma \in \mathbb{F}_{2^n}^*$, and set*

$$F_{t,\gamma}(x) = x^{-1} + \gamma Tr\big(x^t\big). \tag{25}$$

Then $\delta(F_{t,\gamma}) = 4$ for any γ such that $\gamma^3 = 1$ when $t = 3$, as well as for any γ such that $\gamma^5 = 1$ when $t = 5$.

Proof. Notation is as we stated at the beginning of this section and the method is the same as for Lemma 6. Here h_a is the derivative of $x \mapsto x^t$ in point a and we begin by computing $h_a(x)$ for $x \notin \{0, a\}$. Recall that in this case $f_a(x) = a(x^2 + ax)^{-1}$. If $t = 3$ then

$$h_a(x) = x^2 a + xa^2 + a^3 = \frac{a^2}{f_a(x)} + a^3. \tag{26}$$

If $t = 5$ then

$$h_a(x) = x^4 a + xa^4 + a^5 = \frac{a^3}{(f_a(x))^2} + \frac{a^4}{f_a(x)} + a^5, \tag{27}$$

since

$$x^4 a + xa^4 = a^5 \left(\frac{(x^2 + ax)^2}{a^4} + \frac{x^2 + ax}{a^2} \right).$$

Now, according to (19), (15) and (p1)–(p4), we look at the solutions x of

$$F_a(x) = f_a(x) + \gamma Tr\big(h_a(x)\big) = b, \quad b \in \{1/a, 1/a + \gamma\}. \tag{28}$$

Note that if $x \in \{0, a\}$ then $Tr(h_a(x)) = Tr(a^t)$. Recall that $\delta(F_{t,\gamma}) = 6$ if and only if either $E(a, 1/a)$ or $E(a, 1/a + \gamma)$ has 6 solutions. We are going to prove that it is impossible.

Assume that $t = 3$. Note that when $f_a(x) = 1/a$, $x \notin \{0, a\}$, we get $Tr(h_a(x)) = 0$, from (26). This implies that $E(a, 1/a + \gamma)$ has at most 4 solutions, since it is impossible

to have $F_a(x) = 1/a + \gamma$ with $Tr(h_a(x)) = 1$. Now, $E(a, 1/a)$ has four solutions when $Tr(a^3) = 0$. These are $\{0, a\}$ and the two solutions of $x^2 + ax + a^2 = 0$.

There are two other solutions if and only if there is $x \notin \{0, a\}$ such that $f_a(x) = \gamma + 1/a$ with $Tr(h_a(x)) = 1$. Note that $f_a(x) = \gamma + 1/a$ if and only if

$$x^2 + ax + \frac{a^2}{a\gamma + 1} = 0, \quad \text{i.e.,} \quad Tr\left(\frac{1}{a\gamma + 1}\right) = 0. \tag{29}$$

But from (26)

$$Tr\big(h_a(x)\big) = Tr\left(\frac{a^3}{a\gamma + 1} + a^3\right) = Tr\left(\frac{1}{a\gamma + 1} + a^3\right) = 0.$$

This is because (with $\gamma^3 = 1$)

$$\frac{a^3}{a\gamma + 1} = \frac{((a\gamma + 1) + 1)^3}{a\gamma + 1} = (a\gamma + 1)^2 + (a\gamma + 1) + 1 + \frac{1}{a\gamma + 1}.$$

So, it is impossible to have $f_a(x) = \gamma + 1/a$, with $Tr(h_a(x)) = 1$, $x \notin \{0, a\}$. Hence $E(a, 1/a)$ has at most four solutions.

Now $t = 5$. When $f_a(x) = 1/a$, $x \notin \{0, a\}$, we get $Tr(h_a(x)) = Tr(a^5)$, from (27).

Assume that $Tr(a^5) = 0$. In this case we get four solutions, which are $\{0, a\}$ and the two solutions of $x^2 + ax + a^2 = 0$, $x \notin \{0, a\}$. We proceed as previously to prove that there are no other solutions. With $f_a(x) = \gamma + 1/a$, and assuming (29), we get:

$$Tr\big(h_a(x)\big) = Tr\left(\frac{a^5}{(a\gamma + 1)^2} + \frac{a^5}{(a\gamma + 1)} + a^5\right) = Tr\left(\frac{1}{a\gamma + 1} + a^5\right) = 0,$$

by expanding

$$\frac{a^5}{(a\gamma + 1)^\ell} = \frac{((a\gamma + 1) + 1)^5}{(a\gamma + 1)^\ell}, \quad \text{for } \ell = 1, 2, \text{ where } \gamma^5 = 1.$$

Thus $Tr(h_a(x)) \neq 1$, a contradiction.

Now $f_a(x) = 1/a$ with $Tr(a^5) = 1$, the case where $b = 1/a + \gamma$. We have four solutions, as above. There are two other solutions when $f_a(x) = \gamma + 1/a$, assuming (29), and $Tr(h_a(x)) = 0$. But, in this case

$$Tr\big(h_a(x)\big) = Tr\left(\frac{1}{a\gamma + 1} + a^5\right) = 0 + 1 = 1,$$

a contradiction. □

Problem 3. Is there other values of t for which the functions $F_{t,\gamma}$ (given by (25)) satisfy $\delta(F_{t,\gamma}) = 4$ for some γ?

5. Two quadratic monomials

In this section, we study the functions over $\mathbb{F}_{2^n}$ of the form

$$F(x) = x^{2^j+1} + \gamma\, Tr\big(x^{2^k+1}\big) \quad \text{with } \gcd(j,n) = 1,\ \gamma \in \mathbb{F}_{2^n}^*, \tag{30}$$

where j and k are nonzero integers.

Corollary 5. *Let F be given by (30). Then*

(i) $\delta(F) \leqslant 4$;
(ii) *F cannot be a permutation unless $k = j$ and $Tr(\gamma) = 0$.*

Proof. The condition on j means that $x \mapsto x^{2^j+1}$ is an APN function. Thus, (i) comes from Proposition 1. Proposition 2 implies (ii) when n is even. When n is odd, F can be a permutation only if

$$2^k + 1 \equiv 2^\ell \big(2^j + 1\big)\big(2^i + 1\big) \pmod{2^n - 1}, \quad \text{for some } i, \ell$$

(see Theorem 3). But this is impossible unless two cases:

- $k = j$, $i = 0$. When $Tr(\gamma) = 0$, this case provides permutations from Theorem 3(a).
- $i = j = 1$. This case is treated by Proposition 3. □

5.1. APN or not

In this subsection we study the derivatives of F, that is we consider the functions $x \mapsto G_a(x) + F(a)$, $a \in \mathbb{F}_{2^n}^*$, where

$$\begin{aligned} G_a(x) &= g_a(x) + \gamma\, Tr\big(h_a(x)\big), \\ g_a(x) &= x^{2^j} a + x a^{2^j}, \qquad h_a(x) = x^{2^k} a + x a^{2^k}. \end{aligned} \tag{31}$$

Note that g_a and h_a are linear functions so that G_a is linear too. Hence G_a is 2-to-1 if and only if its kernel has dimension 1. Recall that a function is APN if and only if all its derivatives are 2-to-1. Our goal is to compute the kernel of the functions G_a of the form (31).

Remark 9. Since $x \mapsto x^{2^j+1}$ is APN, because j and n are coprime, the function g_a is 2-to-1 for every non-zero a. Thus the image set of g_a is a hyperplane in $\mathbb{F}_{2^n}$, which we denote H_a. Recall that a hyperplane H in $\mathbb{F}_{2^n}$ is defined by a unique non-zero $\lambda \in \mathbb{F}_{2^n}$ such that $H = \{y \in \mathbb{F}_{2^n} \mid Tr(\lambda y) = 0\}$. Next we determine λ defining H_a. It must hold:

$$Tr\big(\lambda\big(x^{2^j} a + x a^{2^j}\big)\big) = Tr\big(x\big(\lambda a^{2^j} + (\lambda a)^{2^{n-j}}\big)\big) = 0,$$

for all x. Thus $\lambda a = \lambda^{2^j} a^{2^{2j}}$ providing $\lambda = a^{-(2^j+1)}$, and we have:

$$H_a = \left\{ y \in \mathbb{F}_{2^n} \;\middle|\; Tr\left(\frac{y}{a^{2^j+1}}\right) = 0 \right\}.$$

The next theorem is a binary version of [11, Theorem 6].

Theorem 9. *Let $L_1 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a linear function with kernel $\{0, \alpha\}$ and γ, $\beta \in \mathbb{F}_{2^n}^*$ with $Tr(\beta\alpha) = 0$. Define*

$$L(x) = L_1(x) + \gamma\, Tr(\beta x).$$

Then the kernel K of L has dimension at most 2. Moreover this kernel has dimension 1 if and only if either (i) *or* (ii) *is satisfied:*

(i) *there exists an element $u \in \mathbb{F}_{2^n}$ satisfying $L_1(u) = \gamma$ and $Tr(\beta\, u) = 0$;*
(ii) *γ does not belong to the image set of L_1.*

The next corollary is an instance of the theorem above. We include a sketch of proof for completeness.

Corollary 6. *Let F be given by (30) and G_a by (31).*
Then G_a is 2-to-1 if and only if either (i) *or* (ii) *is satisfied:*

(i) *there exists an element $u \in \mathbb{F}_{2^n}$ such that $\gamma = g_a(u)$ and $Tr(h_a(u)) = 0$;*
(ii) *γ does not belong to the image set of g_a, i.e. $Tr(\gamma/a^{2^j+1}) \neq 0$.*

If G_a is not 2-to-1, its kernel has dimension 2.

Proof. We apply Theorem 9 with $L_1(x) = g_a(x)$, K is the kernel of G_a and $\beta = a^{2^{n-k}} + a^{2^k}$, since

$$Tr\big(h_a(x)\big) = Tr\big(ax^{2^k} + a^{2^k} x\big) = Tr\big(\big(a^{2^{n-k}} + a^{2^k}\big)x\big).$$

Because g_a is a 2-to-1 function, the kernel of g_a is $\{0, a\}$. Note that $Tr(\beta a) = 0$, since

$$Tr\big(\big(a^{2^{n-k}} + a^{2^k}\big)a\big) = Tr\big(a^{2^{n-k}+1} + a^{2^k+1}\big) = 0.$$

Thus, the result comes directly from Theorem 9. □

Note that, from Remark 9, the fact that γ belongs to the image set of g_a means that $Tr(\gamma/a^{2^j+1}) = 0$. Also, we know that $\delta(F) \in \{2, 4\}$. Thus we have directly

Corollary 7. *Let* $F(x) = x^{2^j+1} + \gamma Tr(x^{2^k+1})$ *with* $\gcd(j,n) = 1$ *and* $k > 0$. *Then* F *is APN if and only if for all* $a \in \mathbb{F}_{2^n}^*$

$$Tr\left(\frac{\gamma}{a^{2^j+1}}\right) = 0 \quad \Rightarrow \quad Tr\left(u^{2^k}a + ua^{2^k}\right) = 0, \quad \text{where } u^{2^j}a + ua^{2^j} = \gamma. \tag{32}$$

Otherwise $\delta(F) = 4$.

Remark 10. The previous corollary shows that $F(x) = x^{2^j+1} + \gamma Tr(x^{2^j+1})$ with $\gcd(n,j) = 1$ is APN for any γ such that $Tr(\gamma) = 0$. Moreover such F is a permutation when n is odd (see Corollary 1).

Note that $F(x) = (x + \gamma Tr(x)) \circ x^{2^j+1}$, where $x + \gamma Tr(x)$ is a bijective linear function and x^{2^j+1} is APN. Hence $F(x)$ is EA-equivalent to x^{2^j+1}. Moreover, any function $(x + \gamma Tr(x)) \circ G(x)$ is (bijective) APN whenever $G(x)$ is (bijective) APN.

The following result extends Corollary 7. Note that the linear function L (below) can be obtained in the context of Hilbert's Theorem, an explanation (and a proof) of which can be found in [22, Chapter VI, § 6].

Corollary 8. *Let* $F(x) = x^{2^j+1} + \gamma Tr(x^{2^k+1})$ *with* $\gcd(j,n) = 1$ *and* $k > 0$. *Let* $\mu \in \mathbb{F}_{2^n}^*$ *such that* $Tr(\mu) = 1$ *and define the linear function* $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *by*

$$L(y) = \sum_{i=0}^{n-1} y^{2^{ij}} \sum_{\ell=0}^{i} \mu^{2^{\ell j}}. \tag{33}$$

Then F *is APN if and only if for all* $a \in \mathbb{F}_{2^n}^*$ *such that* $Tr(\gamma/a^{2^j+1}) = 0$, *we have*

$$Tr\left(a^{2^k+1}\left(\left(L(A)\right)^{2^k} + L(A)\right)\right) = 0, \quad \text{where } A = \frac{\gamma}{a^{2^j+1}}. \tag{34}$$

Proof. Suppose that there is u such that $u^{2^j}a + ua^{2^j} = \gamma$ or, equivalently, taking $v = u/a$, there is $v \in \mathbb{F}_{2^n}$ as follows

$$v^{2^j} + v = \frac{\gamma}{a^{2^j+1}}. \tag{35}$$

Since $\gcd(j,n) = 1$, there are only two solutions of (35) if $Tr(\gamma/a^{2^j+1}) = 0$, namely v and $v+1$, and no solution otherwise. Let μ be such that $Tr(\mu) = 1$ and set $A = \gamma/a^{2^j+1}$. It is easy to check that if $Tr(A) = 0$ then $v = L(A)$. Indeed, for any y we have:

$$\begin{aligned}\left(L(y)\right)^{2^j} + L(y) &= \sum_{i=0}^{n-1} y^{2^{(i+1)j}} \sum_{\ell=0}^{i} \mu^{2^{(\ell+1)j}} + \sum_{i=0}^{n-1} y^{2^{ij}} \sum_{\ell=0}^{i} \mu^{2^{\ell j}} \\ &= \sum_{i=1}^{n} y^{2^{ij}} \sum_{\ell=1}^{i} \mu^{2^{\ell j}} + \sum_{i=0}^{n-1} y^{2^{ij}} \sum_{\ell=0}^{i} \mu^{2^{\ell j}}\end{aligned}$$

$$= \sum_{i=1}^{n-1} y^{2^{ij}}\mu + y\sum_{\ell=1}^{n}\mu^{2^{\ell j}} + y\mu$$
$$= \mu Tr(y) + yTr(\mu).$$

Thus

$$\big(L(y)\big)^{2^j} + L(y) = y \quad \text{when } Tr(y) = 0 \text{ and } Tr(\mu) = 1. \tag{36}$$

By applying Corollary 7, we obtain that F is APN if and only if for all $a \in \mathbb{F}_{2^n}^*$ such that $Tr(A) = 0$ we have

$$Tr\big(au^{2^k} + a^{2^k}u\big) = Tr\big(a^{2^k+1}\big(\big(L(A)\big)^{2^k} + L(A)\big)\big) = 0,$$

where $A = \gamma/a^{2^j+1}$ and $u = L(A)a$. □

5.2. A special case

To illustrate the results of the previous subsection we propose some complements on the function $x \mapsto x^3 + \gamma Tr(x^9)$, which is APN for any n with a suitable γ. First we observe:

Lemma 7. *Notation is as in Corollary 8. Assume that $k = \ell j$, $\ell > 1$. Then, the condition (34) becomes*

$$Tr\left(a^{2^{\ell j}+1}\left(\left(\frac{\gamma}{a^{2^j+1}}\right)^{2^{(\ell-1)j}} + \cdots + \left(\frac{\gamma}{a^{2^j+1}}\right)^{2^j} + \frac{\gamma}{a^{2^j+1}}\right)\right) = 0. \tag{37}$$

Proof. We simply use that $(L(A))^{2^j} = L(A) + A$:

$$\big(L(A)\big)^{2^{\ell j}} = \big(L(A) + A\big)^{2^{(\ell-1)j}} = \big(L(A) + A\big)^{2^{(\ell-2)j}} + A^{2^{(\ell-1)j}} = \cdots. \qquad \square$$

Then, we have directly

Proposition 7. *Let $F(x) = x^3 + \gamma Tr(x^9)$. Then F is APN for all n when $\gamma = 1$. When n is even, F is APN for all $\gamma \in \mathbb{F}_4$.*

Proof. It comes directly from (37), by replacing $j = 1$ and $k = \ell = 3$. For all $a \in \mathbb{F}_{2^n}^*$ such that $Tr(\gamma/a^3) = 0$, we must have

$$Tr\left(a^9\left(\left(\frac{\gamma}{a^3}\right)^{2^2} + \left(\frac{\gamma}{a^3}\right)^2 + \frac{\gamma}{a^3}\right)\right) = Tr\left(\frac{\gamma^4}{a^3} + a^3\gamma^2 + a^6\gamma\right) = 0.$$

This obviously holds when $\gamma = 1$, for any n. But when n is even, it holds also for $\gamma \in \mathbb{F}_4$. Indeed, in this case, we get

$$Tr\left(\frac{\gamma}{a^3} + a^6\left(\gamma^4 + \gamma\right)\right) = 0. \qquad \square$$

In Section 3.3, we showed how 2-to-1 functions yield permutations. The function $F(x) = x^3 + Tr(x^9)$ is 2-to-1 for odd n.

Proposition 8. *Let n be odd. The function*

$$G(x) = x^3 + Tr\left(x^9 + x^3\right)$$

is bijective on $\mathbb{F}_{2^n}$ and satisfies $\delta(G) = 4$.

Proof. The function G is bijective such that $\delta(G) \leqslant 4$, from Theorem 5. We compute the dimension of the kernel of $G(x) + G(x + a) + G(a)$ for any $a \in \mathbb{F}_{2^n}^*$. Consider the equation

$$G_a(x) = x^2a + xa^2 + Tr\left(x^8a + xa^8 + x^2a + xa^2\right) = 0.$$

First $x = 0$ and $x = a$ are solutions, for any a. Further, if $Tr(a^{-3}) = 0$, there is u such that $u^2a + ua^2 = 1$. Since $x^3 + Tr(x^9)$ is APN, we have in this case $Tr(u^8a + ua^8) = 0$ by Corollary 7. Then u and $u + a$ are solutions of

$$x^2a + xa^2 + 1 = 0 \quad \text{with } Tr\left(x^8a + xa^8 + x^2a + xa^2\right) = 1,$$

implying that G_a is not 2-to-1 when $Tr(a^{-3}) = 0$. $\square$

6. Conclusion

In this paper we focused on the permutations introduced in [10,11] which are as sparse as possible and have a low differential uniformity δ. While it is easy to obtain an upper bound on δ, it is difficult to give the exact value of δ. In this context, we present new methods and new tools expecting that they can be used for other kinds of functions too.

The main question remained open whether do exist new classes of APN functions of form $x^s + \gamma\, Tr(x^t)$. We are more precise in the paragraph below. There is the remarkable class of functions $x \mapsto x^3 + Tr(x^9)$, and few sporadic examples. Our studies and our numerical results lead us to conjecture that there is no other infinite class of such APN functions.

Another open problem is the determination of the Walsh spectrum of functions of type $x^s + \gamma\, Tr(x^t)$. Little is known about this, especially for such non-quadratic functions. This problem is difficult since it is related to finding the spectrum of Boolean functions

including two monomials, or with the weight enumerator of cyclic codes with three zeros. This appears clearly when one studies the component functions (see Section 3.2).

Further functions $F_{s,t,\gamma}$. The set of functions $F_{s,t,\gamma}$ on $\mathbb{F}_{2^n}$ is very rich. It is of interest to identify specific sets of integers s and t yielding such functions with particular properties. For example it would be interesting to study the properties of functions

$$F_{j,i,\gamma}(x) = x^{2^j+1} + \gamma\, Tr\big(x^{(2^i+1)(2^j+1)}\big),$$

where $x \mapsto x^{2^j+1}$ is a permutation on $\mathbb{F}_{2^n}$. It is easy to see that the algebraic degree d of $F_{i,j,\gamma}$ is

$$d = \begin{cases} 4 & \text{if } i \neq j, \\ 3 & \text{if } i = j \text{ with } 1 < j < n/2, \\ 2 & \text{if } i = j = 1. \end{cases}$$

It is worth to note that with $i = j = 1$ we get the APN function $x \mapsto x^3 + \gamma\, Tr(x^9)$ which is not a permutation.

Another interesting choice for s would be the so-called Kasami exponent. Recall that the integers

$$d = 2^{2i} - 2^i + 1 \pmod{2^n - 1}, \quad 1 \leqslant i \leqslant n-1,$$

are called *Kasami exponents* and the corresponding power functions on $\mathbb{F}_{2^n}$

$$K_d(x) = x^d$$

are called Kasami functions. The Kasami exponents yielding permutations on $\mathbb{F}_{2^n}$ are characterized in [21, §3.1]. Let $d = 2^{2i} - 2^i + 1$, then the set of functions

$$F_{i,\gamma} = x^d + \gamma\, Tr\big(x^{2^{3i}+1}\big)$$

includes permutations with low differential uniformity. Again, we would like to remark that with $i = 1$ we get the function $x^3 + \gamma\, Tr(x^9)$.

References

[1] T.P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, On almost perfect nonlinear functions, IEEE Trans. Inf. Theory 52 (9) (September 2006) 4160–4170.
[2] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, in: Special Issue Dedicated to Vera Pless, Int. J. Inf. Coding Theory 1 (2) (2010) 149–170.
[3] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of $x \mapsto x^{2^t-1}$, IEEE Trans. Inf. Theory 57 (12) (2011) 8127–8137.
[4] C. Blondeau, L. Perrin, More differentially 6-uniform power functions, in: Proceedings of Workshop on Coding and Cryptography, WCC 2013, Bergen, Norway, April 2013.

[5] C. Bracken, E. Byrne, N. Markin, G. McGuire, Fourier spectra of binomial APN functions, SIAM J. Discrete Math. 23 (2) (2009) 596–608.
[6] C. Bracken, E. Byrne, N. Markin, G. McGuire, A few more quadratic APN functions, Cryptogr. Commun. 3 (1) (2011) 43–53.
[7] C. Bracken, C. How Tan, Y. Tan, Binomial differentially 4 uniform permutations with high nonlinearity, Finite Fields Appl. 18 (3) (2012) 537–546.
[8] L. Budaghyan, C. Carlet, G. Leander, Constructing new APN from known ones, Finite Fields Appl. 15 (2) (2009) 150–159.
[9] A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: A proof of Welch conjecture, IEEE Trans. Inf. Theory 46 (1) (Jan. 2000) 4–8.
[10] P. Charpin, G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, in: SETA 2008, in: Lect. Notes Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368–376.
[11] P. Charpin, G. Kyureghyan, When does $G(x)+\gamma Tr(H(x))$ permute $\mathbb{F}_{2^n}$?, Finite Fields Appl. 15 (5) (2009) 615–632.
[12] P. Charpin, G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, in: Finite Fields: Theory and Applications – FQ9, in: Contemp. Math., vol. 518, AMS, 2010, pp. 99–111.
[13] S.D. Cohen, Finite field elements with specified order and traces, Des. Codes Cryptogr. 36 (2005) 331–340.
[14] J.F. Dillon, Geometry, codes and difference sets: exceptional connections, in: Codes and Design, Colombus, OH, 2000, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 10, de Gruyter, Berlin, 2002, pp. 73–85.
[15] J.F. Dillon, APN polynomials: An update, Invited talk at Fq9, the 9th International Conference on Finite Fields, Dublin, July 13–17, 2009.
[16] Y. Edel, A. Pott, A new perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3 (1) (2009) 59–81.
[17] F. Göloğlu, G. McGuire, When is $x^{-1}+L(x)$ a permutation in odd characteristic?, in: Proceedings of Workshop on Coding and Cryptography, WCC 2013, Bergen, Norway, April 2013.
[18] X.-D. Hou, Affinity of permutations of $\mathbf{F}_2^n$, Discrete Appl. Math. 154 (2006) 313–325.
[19] G.M. Kyureghyan, Constructing permutations of finite fields via linear translators, J. Comb. Theory, Ser. A 118 (2011) 1052–1061.
[20] G.M. Kyureghyan, V. Suder, On inverses of APN exponents, in: Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT'12, Boston, USA, July 2012.
[21] G.M. Kyureghyan, V. Suder, On inversion in $\mathbb{Z}_{2^n-1}$, Finite Fields Appl. 25 (2014) 234–254.
[22] S. Lang, Algebra, third edition, Addison–Wesley Publishing Company, Inc., 2002.
[23] Y. Li, M. Wang, On EA-equivalence of certain permutations to power mappings, Des. Codes Cryptogr. 58 (2011) 259–269.
[24] Y. Li, M. Wang, Permutation polynomials EA-equivalent to the inverse function over $GF(2^n)$, Cryptogr. Commun. 3 (2011) 175–186.
[25] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology – EUROCRYPT'93, in: Lect. Notes Comput. Sci., vol. 765, Springer-Verlag, 1993, pp. 55–64.
[26] Y. Tan, L. Qu, C. How Tan, C. Li, New families of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$, in: SETA 2012, in: Lect. Notes Comput. Sci., vol. 7280, Springer-Verlag, Berlin, Heidelberg, 2012, pp. 25–39.
[27] Z. Zha, L. Hu, S. Sun, Constructing new differentially 4-uniform permutations from the inverse function, Finite Fields Appl. 25 (2014) 64–78.