On sets determining the differential spectrum of mappings

Pascale Charpin, Gohar M. Kyureghyan

On sets determining the differential spectrum of mappings

Pascale Charpin* Gohar M. Kyureghyan†

May 17, 2018

Abstract

The differential uniformity of a mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as the maximum number of solutions x for equations $F(x+a)+F(x) = b$ when $a \neq 0$ and b run over $\mathbb{F}_{2^n}$. In this paper we study the question whether it is possible to determine the differential uniformity of a mapping by considering not all elements $a \neq 0$, but only those from a special proper subset of $\mathbb{F}_{2^n} \setminus \{0\}$.

We show that the answer is "yes", when F has differential uniformity 2, that is if F is APN. In this case it is enough to take $a \neq 0$ on a hyperplane in $\mathbb{F}_{2^n}$. Further we show that also for a large family of mappings F of a special shape, it is enough to consider a from a suitable multiplicative subgroup of $\mathbb{F}_{2^n}$.

Keywords: Boolean function, bent function, APN mappings, monomial binomial, permutation, hyperplane, cryptographic criteria, differential uniformity.

1 Introduction

The differential uniformity of a mapping on $\mathbb{F}_2^n$ is an important parameter for cryptological applications. It is defined as follows. Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ and

*INRIA, SECRET project-team, 2 rue Simone Iff, 75012, Paris, France, Pascale.Charpin@inria.fr

†Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany, Gohar.Kyureghyan@ovgu.de

$a \in \mathbb{F}_2^n$ be non-zero. The mapping

$$D_aF : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n,\ x \mapsto F(x+a) + F(x)$$

is called *the difference mapping of F defined by a*, or the derivative of F in direction a. Set

$$\delta(a,\gamma) = |\{x \in \mathbb{F}_{2^n},\ D_aF(x) = \gamma\}|, \tag{1}$$

for any $a \neq 0$ and γ in $\mathbb{F}_2^n$ (recall that $|A|$ denotes the cardinality of the set A). The *differential spectrum* of F is the multiset consisting of integers $\delta(a,\gamma)$ with their multiplicities. The *differential uniformity* of F is defined as

$$\delta(F) = \max_{a\neq 0,\ \gamma\in\mathbb{F}_2^n} \delta(a,\gamma). \tag{2}$$

The image set of a difference mapping D_aF contains at most 2^{n-1} elements, since $D_aF(x) = D_aF(x+a)$ for any $a \in \mathbb{F}_2^n$. Clearly, the image set of a difference mapping D_aF is of that maximal size if and only if D_aF is 2-to-1. A mapping is called *almost perfect nonlinear*, abbreviated APN, if all its difference mappings are 2-to-1. Note that the APN mappings can be defined also as those having differential uniformity 2. APN mappings provide the optimal resistance against the *differential cryptanalysis* when they are used as an S-BOX [11]. Whether there exist APN permutations on $\mathbb{F}_{2^n}$ for even n is an important research problem. Only one (up to affine equivalence) such mapping is known for $n = 6$. It was found by a group of NSA around John Dillon in 2009, [6]. Yet, seven years later, the *most famous and important open question* concerning the APN functions remains: Does there exist an APN permutation on $\mathbb{F}_{2^n}$ for n even and greater than 6?

To verify the APN property of F it necessitates, a priori, to check that all difference mappings D_aF are 2-to-1. Actually, it is well-known that not all D_aF must be checked: It was proved in [2, Eurocrypt 93] that it is sufficient to check 2^{n-1} well-chosen D_aF. In Section 2, we reconsider this result and show that it is equivalent to the statement: A mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ is APN if and only if D_aF are 2-to-1 for all non-zero a on a hyperplane of $\mathbb{F}_2^n$.

There are only few families of APN mappings which are known. Most of the known mappings with small differential uniformity are described as univariate polynomials over finite fields. In this paper we study possibilities to reduce the complexity of computing the differential uniformity of mappings. In particular we consider checking the APN property in Theorems 3 and 4.

In Section 3 we show that the differential spectrum of a class of permutations described by Zieve [13] is determined by a small number of derivatives (Theorem 6). Finally we focus on binomials and give some numerical results.

2 Verifying the APN property

2.1 A combinatorial problem

In [2], Beth and Ding introduced a so-called differential representation set of $\mathbb{F}_2^n$, which is defined as follows:

Definition 1 *Let S be a subset of $\mathbb{F}_2^n \setminus \{0\}$. If S satisfies*

$$x \in \mathbb{F}_2^n,\ y \in \mathbb{F}_2^n \text{ with } x \neq 0,\ y \neq 0,\ x \neq y \quad \Rightarrow \quad \{x, y, x+y\} \cap S \neq \emptyset, \quad (3)$$

then S is called a differential representation set of $\mathbb{F}_2^n$. Moreover, S is said minimal when it has minimal size.

It is proved in [2] that the size of differential representation set S is equal to or greater than $2^{n-1}-1$. This is easy to see. Indeed, set

$$S' = \mathbb{F}_2^n \setminus (S \cup \{0\}) = \{s_1, s_2, \ldots, s_\ell\},\ \ell = 2^n - |S| - 1.$$

Thus, the $\ell-1$ elements s_1+s_i, $2 \leq i \leq \ell$, belong to S so that $|S| \geq 2^n - |S| - 2$ providing $|S| \geq 2^{n-1}-1$. In particular, a minimal differential representation set of $\mathbb{F}_2^n$ has cardinality $2^{n-1}-1$. The next theorem shows that the minimal differential representation sets are exactly the hyperplanes of $\mathbb{F}_2^n$ without the zero element.

Theorem 1 *A subset $S \subset \mathbb{F}_2^n$ is a minimal differential representation set of $\mathbb{F}_2^n$ if and only if $S \cup \{0\}$ is an hyperplane of $\mathbb{F}_2^n$.*

Proof. Let $k := |S| = 2^{n-1}-1$. Evidently, if $S \cup \{0\}$ is an hyperplane of $\mathbb{F}_2^n$ then S satisfies (3). So suppose that S satisfies (3) with $k = 2^{n-1}-1$. Our goal is to prove that $S \cup \{0\}$ is an hyperplane.

We proceed by induction. For $n = 2$ it is clear that the property holds. We assume that the statement is true until $n-1$ where $n \geq 3$.

Let H be any hyperplane of $\mathbb{F}_2^n$ and denote by $\overline{H}$ its complement in $\mathbb{F}_2^n$. Set

$$T = (S \cup \{0\}) \cap H \quad \text{and} \quad \overline{T} = S \cap \overline{H}.$$

Then $|T| \geq 2^{n-2}$ since T satisfies (3) in $H \setminus \{0\}$. Therefore $\overline{T} \leq 2^{n-2}$. Note that if $|T| = 2^{n-1}$ then $T = H$. So we suppose now that $|T| < 2^{n-1}$.

Fix $y \in H \setminus T$. Then for all $z \in \overline{H} \setminus \overline{T}$ we get $y + z \in \overline{H}$. But $y + z \in \overline{T}$ because $y \notin S$ and $z \notin S$. The set of elements $y + z$, z describing $\overline{H} \setminus \overline{T}$ has cardinality c with $c \geq 2^{n-2}$. This is impossible unless $|\overline{T}| = 2^{n-2}$.

If $|T| = 2^{n-2}$ then T is a subspace of dimension $n-2$, from the induction hypothesis applied to H. In this case, we have

$$\mathbb{F}_2^n = T \cup (a+T) \cup (b+T) \cup (a+b+T), \text{ with } H = (T \cup a) + T,$$

for some (a, b). If $\overline{T}$ is neither equal to $b + T$ nor equal to $(a + b) + T$ then there are

$$x \in b + T \setminus \overline{T}, \ y \in (a+b) + T \setminus \overline{T} \ \text{ providing } x + y \in a + T$$

which contradicts (3). So $\overline{T}$ is a coset of T, completing the proof. $\diamond$

Remark 1 *Theorem 1 is a special case of a result proven in [4] as mentioned in [12].*

2.2 The APN property

In the remaining of the paper we consider mappings on finite fields $\mathbb{F}_{2^n}$. We first state the APN property as a property on each derivative.

Definition 2 *Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$. We say that F satisfies the property (p_a), $a \in \mathbb{F}_{2^n}^*$, when the equation*

$$F(x) + F(x + a) = b \tag{4}$$

has either 0 or 2 solutions for every $b \in \mathbb{F}_{2^n}$, i.e. the derivative of F in direction a is 2-to-1.

Thus, F is APN if and only if F satisfies (p_a) for all nonzero $a \in \mathbb{F}_{2^n}$. In [2], it is shown that to verify that F is APN it is enough to check (p_a) for all elements a from a differential representation set of $\mathbb{F}_{2^n}$. The next theorem follows then from Theorem 1 and it was mentioned in [10, Theorem 2.1]. We sketch its proof for clarity.

Theorem 2 *Let H be a hyperplane in $\mathbb{F}_{2^n}$. A mapping $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is APN if and only if F satisfies (p_a) for all non-zero $a \in H$.*

Proof. Necessity of the condition follows clearly from definition of APN mappings. To prove that it is also sufficient, suppose that $\alpha \in \mathbb{F}_{2^n} \setminus H$ and $D_\alpha F$ is not 2-to-1. Then there are two distinct $x, y \in \mathbb{F}_{2^n}$ such that $x+y \neq \alpha$ and

$$D_\alpha F(x) = F(x) + F(x+\alpha) = F(y) + F(y+\alpha) = D_\alpha F(y).$$

After that, one prove easily that

$$D_{x+y}F(x) = D_{x+y}F(x+\alpha) \text{ and } D_{x+y+\alpha}F(x) = D_{x+y+\alpha}F(x+\alpha).$$

Thus, the functions $D_{x+y}F$ and $D_{x+y+\alpha}F$ are not 2-to-1, which is a contradiction since either $x+y$ or $x+y+\alpha$ belong to H. ◇

Next we apply Theorem 2 to a special class of mappings. Recall that the hyperplanes (that is $(n-1)$-dimensional $\mathbb{F}_2$-subspaces) of $\mathbb{F}_{2^n}$ are the sets

$$H_\alpha := \{x \in \mathbb{F}_{2^n} \mid Tr(\alpha x) = 0\},$$

defined by all nonzero $\alpha \in \mathbb{F}_{2^n}$. Further, we denote by $Im(G)$ the image set of a mapping G.

Corollary 1 *Let $H = \{x | Tr(x) = 0\}$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be defined by*

$$F(x) = G(x) + R(x)Tr(x),$$

where G and R are arbitrary mappings on $\mathbb{F}_{2^n}$. Then for every $a \in H$ we have

$$D_aF(x) = (G(x) + G(x+a)) + Tr(x)(R(x) + R(x+a)). \quad (5)$$

Suppose that the mappings $G(x)$ and $P(x) := G(x) + R(x)$ are APN. Set $I_a = Im(D_aG) \cap Im(D_aP)$. Then F is APN if and only if for any nonzero $a \in H$ and every $b \in I_a$ there is $x \in \mathbb{F}_{2^n}$ with

$$D_aG(x) = b \text{ and } Tr(x) = 1, \text{ or } D_aP(x) = b \text{ and } Tr(x) = 0.$$

Proof. The equality (5) is directly obtained by replacing $Tr(a) = 0$ in

$$D_aF(x) = D_aG(x) + Tr(x)R(x) + Tr(x+a)R(x+a).$$

Consider $a \in H$ and the equation $D_aF(x) = b$ for some $b \in \mathbb{F}_{2^n}$. Note that

$$D_aF(x) = \begin{cases} D_aG(x) & \text{if } Tr(x) = 0 \\ D_aP(x) & \text{if } Tr(x) = 1. \end{cases}$$

In particular, any solution of $D_aF(x) = b$ solves either $D_aG(x) = b$ or $D_aP(x) = b$ depending on its trace. This shows that $D_aF(x) = b$ has at most 4 solutions, since the mappings G and P are APN. Clearly, if $b \notin I_a$ then $D_aF(x) = b$ has at most two solutions. Observe, if x is a solution for $D_aG(x) = b$ then the second solution is $x+a$ and it holds $Tr(x) = Tr(x+a)$, since $a \in H$. Similarly the solutions x and $x + a$ of $D_aP(x)$ have the same trace, if they exist. Assume that $b \in I_a$. Suppose x_1 solves $D_aG(x) = b$ and x_2 solves $D_aP(x) = b$. Then the equation $D_aF(x) = b$ has 4 solutions if and only if $Tr(x_1) = 0$ and $Tr(x_2) = 1$, completing the proof. $\diamond$

Example 1 *Notation is as in Corollary 1 and its proof. Assume that R is a linear mapping. Then $G + R$ is APN as soon as G is APN and (5) reduces to*

$$D_aF(x) = D_aG(x) + T(x)R(a).$$

Also, $D_aP(x) = b$ is equivalent to $D_aG(x) = b + R(a)$.

Example 2 *The mapping $F(x) = x^3 + x^4 \cdot Tr(x)$ on $\mathbb{F}_{2^7}$ is of shape discussed in Example 1. It is easy to check that F(x) has differential uniformity 8. This example shows that for computing the differential uniformity of a generic mapping it is not enough to consider only the differential mappings defined by elements of a hyperplane, like it is the case for APN mappings by Theorem 2.*

Problem 1 *Suppose that $\delta(a, b) \leq 4$ for every nonzero a on hyperplane H_α and every $b \in \mathbb{F}_{2^n}$, as it is the case for the mapping F considered in Corollary 1. Under which conditions can we conclude that $\delta(F) = 4$?*

For several classes of mappings, it is well-known that to verify the APN property it is sufficient to check (p_a) for very particular values a. The most simple case is when $F(x) = x^t$ for some fixed positive integer t. In this case it is enough to check (p_1) only, since

$$x^t + (x + a)^t = a^t \left(\left(\frac{x}{a} \right)^t + \left(\frac{x}{a} + 1 \right)^t \right)$$

implying $\delta(a, \gamma) = \delta(1, \gamma/a^t)$. Note that in this case we get the differential uniformity of F by computing the derivative in point 1 only. When F is a polynomial whose coefficients are in a subfield of $\mathbb{F}_{2^n}$, Theorem 2 yields another general simplification.

Theorem 3 *Let $H = \{\ \alpha \in \mathbb{F}_{2^n} \mid Tr(\alpha) = 0\ \}$. Set $n = ks$ where $s > 1$ and $k \geq 1$. Let β be a primitive element of $\mathbb{F}_{2^n}$. Let F be a mapping on $\mathbb{F}_{2^n}$ which is given by a polynomial in $\mathbb{F}_{2^k}[x]$. Let I be a set of representatives of 2^k-cyclotomic cosets modulo $2^n - 1$ and $\mathcal{I} = \{i \in I \mid \beta^i \in H\}$.*

Then, F is APN if and only if it satisfies (p_a) for all $a \in \mathcal{I}$.

Proof. From Theorem 1, we can choose any hyperplane H to check the APN property. Here H is the hyperplane which is invariant under the Frobenius isomorphism $\sigma : a \mapsto a^2$. Thus, taking $a \in H$ we get $a^{2^k} \in H$ and

$$D_{a^{2^k}}F(y) = F(y + a^{2^k}) + F(y) = \left(F(x + a) + F(x)\right)^{2^k} = \left(D_aF(x)\right)^{2^k}$$

where $y = x^{2^k}$, since $F \in \mathbb{F}_{2^k}[x]$. It is clear that $D_{a^{2^k}}F$ is 2-to-1 if and only if D_aF is, completing the proof. ◇

If $2^n - 1$ is prime, then there are $(2^n - 2)/n$ cyclotomic cosets (all of size n) modulo $2^n - 1$, providing $|\mathcal{I}| = (2^n - 2)/(2n)$. Hence we have an obvious consequence of the previous theorem.

Corollary 2 *Notation I and $\mathcal{I}$ are as in Theorem 3. Let n be odd such that $2^n - 1$ is prime. Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ a mapping with coefficients in $\mathbb{F}_2$. Then F is APN if and only if D_aF satisfies (p_a) for only $(2^n - 2)/2n$ elements of $\mathbb{F}_{2^n}^*$, that is for $a \in \mathcal{I}$ where $\mathcal{I} = \{i \in I \mid Tr(\beta^i) = 0\}$.*

Example 3 *Let n be such that $2^n - 1$ is prime. Let F be any mapping on $\mathbb{F}_{2^n}$ expressed by a polynomial in $\mathbb{F}_2[x]$. Set $C = |\mathcal{I}| = (2^n - 2)/(2n)$. Then we have:*

- *If $n = 5$ then $C = 3$, and F is APN as soon as D_aF satisfies (p_a) for only 3 elements $a \in \{\alpha^i,\ i = 1, 7, 15\}$, where α is a root of the primitive polynomial $x^5 + x^2 + 1$.*
- *For $n = 7$ we have $C = 9$ and it is enough to check the derivatives for*

  $$a \in \{\ \alpha^i,\ i \in \{1, 3, 5, 9, 11, 15, 23, 29, 55\}\ \},$$

  where α is a root of $x^7 + x + 1$.

Problem 2 *By Theorem 2 if F is not APN then for any hyperplane H_α there is at least one a such that D_aF is not 2-to-1. Can we improve this observation in any direction? Such a belongs to 2^{n-1} hyperplanes. Thus there are at least two such elements a. Is it possible to have a better lower bound on the number of such a?*

2.3 Component functions

The components functions of the mapping $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ can be used to compute its differential uniformity. Using Theorem 2 we directly simplify the characterization of APN mappings given in [1, Theorem 2], which is stated in Theorem 4 below.

We use the notation from [1]: f_λ, with $\lambda \in \mathbb{F}_{2^n}^*$, are the *component functions* of F , *i.e.,* the Boolean functions $x \mapsto Tr(\lambda F(x))$. Further, for a Boolean function f, we set

$$\mathcal{F}(f) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \text{ and } D_a f(x) := f(x) + f(x+a).$$

Theorem 4 *Let H be any hyperplane in $\mathbb{F}_{2^n}$, and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with component functions f_λ, $\lambda \in \mathbb{F}_{2^n}$. Then, for any nonzero $a \in \mathbb{F}_{2^n}$, it holds*

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}, \tag{6}$$

where the equality holds if and only if $D_a F$ is 2-to-1. In particular, F is APN if and only if every nonzero $a \in H$ satisfies

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}. \tag{7}$$

Proof. We sketch the proof, which is similar to that of [1, Theorem 2]. Set $A = \sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$ for some a. Then

$$A = \sum_{\lambda, x, y \ \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda(F(x+a)+F(x)+F(y+a)+F(y)))},$$

and hence

$$\begin{aligned} A &= 2^n \ |\{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid D_a F(x) = D_a F(y)\}| \\ &= 2^{2n+1} + 2^n \ |\{(x,y)| \ D_a F(x) = D_a F(y), x \neq y \neq x+a\}|, \end{aligned}$$

implying (6). Moreover $A = 2^{2n+1}$ if and only if $D_a F$ is 2-to-1, *i.e.,*

$$D_a F(x) = D_a F(y) \text{ for } y \in \{x, x+a\} \text{ only.}$$

Theorem 2 completes the proof. ◇

Bent and *semi-bent* functions have been intensively studied since of their particular role in theory and applications of Boolean functions. The statement of Theorem 2 is related with Theorems V.2 and V.3 from [7]. These results show that for checking that a given Boolean function is bent (resp. semi-bent) it is enough to look on the derivatives defined by nonzero elements $a \in H$, where H is a hyperplane. For clarity we discuss this fact for bent functions in more detail below.

Let n be even. A Boolean function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ is said to be bent when

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)} = \pm 2^{n/2}, \text{ for all } a \in \mathbb{F}_{2^n}. \tag{8}$$

Equivalently, bent functions are those having all derivatives $D_a f(x)$ *balanced*. Recall that a Boolean function g is balanced if it takes equally often the values 0 and 1.

Theorem 5 *Let n be even and H be a hyperplane of $\mathbb{F}_{2^n}$. Then a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent if and only if the derivatives $D_a f(x)$ are balanced for all nonzero $a \in H$.*

Proof. Assume that $D_a f$ is balanced for $a \in H \setminus \{0\}$. Then for every $u \in \mathbb{F}_{2^n}$ the derivative of the function $x \mapsto f(x) + Tr(ux)$ in direction a is balanced as well. Further we use the classical formula

$$A_\lambda := \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(\lambda x)} \right)^2 = \sum_{a \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda a)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)},$$

for $\lambda \in \mathbb{F}_{2^n}$. If $H = H_\alpha = \{x | Tr(\alpha x) = 0\}$ for some nonzero $\alpha \in \mathbb{F}_{2^n}$, then

$$A_\alpha = \sum_{a \in H} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{D_a f(x)} - \sum_{a \notin H} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{D_a f(x)} = 2^n - \sum_{a \notin H} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{D_a f(x)},$$

and then

$$A_0 + A_\alpha = 2^n + \sum_{a \notin H} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)} + A_\alpha = 2^{n+1}.$$

It is easy now to prove that the last equality implies $A_0 = A_\alpha = 2^n$ (for instance by induction). Replacing f by $x \mapsto f(x) + Tr(ux)$ we get $A_{\alpha+u} = 2^n$ for any u and hence (8). ◇

Example 4 *We consider the components of the function F studied in Example 1:*

$$f_\lambda(x) = Tr(\lambda F(x)) = Tr\left(\lambda(G(x) + Tr(x)R(x))\right),\ \lambda \in \mathbb{F}_{2^n}^*,$$

where G is APN and R is linear. Suppose that λ is such that the function $x \mapsto Tr(\lambda G(x))$ is bent. Then f_λ is bent when R satisfies

$$Tr(\lambda R(a)) = 0 \quad \textit{for all } a \in H \tag{9}$$

where $H = \{a | Tr(a) = 0\}$. Indeed

$$\begin{aligned}\mathcal{F}(D_a f_\lambda) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr(\lambda(G(x+a)+G(x)+Tr(x)R(a)))} \\ &= \sum_{x\in H}(-1)^{Tr(\lambda D_a G(x))} + (-1)^{Tr(\lambda R(a))}\sum_{x\notin H}(-1)^{Tr(\lambda D_a G(x))}.\end{aligned}$$

The sum above equals 0 for all $a \in H$ when (9) is satisfied.

3 On differential spectrum of a class of permutations

In this section we consider mappings on $\mathbb{F}_{2^n}$ of shape $F(x) = x^k(h(x^\rho))$, where k is a fixed positive integer and $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. The subset of such bijective mappings was characterized by Zieve in [13]. Lemma 1 is the binary version of [13, Lemma 2.1]. We denote by $\mathcal{G}_V$ the subgroup of $\mathbb{F}_{2^n}^*$ of order V, where V is a divisor of $2^n - 1$.

Lemma 1 *Let $2^n - 1 = \rho V$, $k \in \mathbb{N}$ and $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then the mapping $F(x) = x^k(h(x^\rho))$ is a permutation on $\mathbb{F}_{2^n}$ if and only if*

(i) $\gcd(k, \rho) = 1$ *and*

(ii) $x \mapsto x^k h(x)^\rho$ *permutes $\mathcal{G}_V$.*

Using the above lemma it is easy to describe families of permutations on $\mathbb{F}_{2^n}$, for example we have:

Proposition 1 *Let* $2^n - 1 = \rho V$ *where* $\gcd(\rho, V) = 1$. *Then*

$$F(x) = x^k(h(x^\rho)), \quad \text{where } k = iV \text{ with } 1 \le i \le \rho - 1, \tag{10}$$

is a permutation on $\mathbb{F}_{2^n}$ *if and only if* $\gcd(i, \rho) = 1$ *and* $h(\mathcal{G}_V)^\rho = \mathcal{G}_V$.

Proof. To apply Lemma 1, we prove that the conditions on F correspond to (i) and (ii) respectively. Obviously, $\gcd(i, \rho) = 1$ is here equivalent to (i). Set $P(x) = x^{iV} h(x)^\rho$. For $y \in \mathcal{G}_V$ we have $P(y) = h(y)^\rho$. Thus, P permutes $\mathcal{G}_V$ if and only if $h(\mathcal{G}_V)^\rho = \mathcal{G}_V$. ◇

Permutations described in Lemma 1 are among a large class of mappings whose differential uniformity can be computed by considering elements from a suitable subgroup of $\mathbb{F}_{2^n}^*$ only:

Theorem 6 *Assume that* n *is such that* $2^n - 1 = \rho V$ *with* $\rho > 1$, $V > 1$ *and* $\gcd(\rho, V) = 1$. *Let* $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ *be defined by*

$$F(x) = x^k(h(x^\rho)), \text{ where } h(x) = \sum_{i=0}^{\ell} \nu_i x^i, \ 1 \le \ell < V \tag{11}$$

and $\nu_i \in \mathbb{F}_{2^n}$. *Then* F *is APN if and only if for any* $a \in \mathcal{G}_V$ *the mapping*

$$y \mapsto \sum_{i=0}^{\ell} \nu_i u^{i\rho} \left(y^{k+i\rho} + (y+1)^{k+i\rho} \right)$$

is 2*-to-*1. *Moreover, to compute the differential spectrum of* F *it is sufficient to study the equations* $D_u F(x) = b$ *for* $u \in \mathcal{G}_V$, *and then*

$$\delta(F) = \max\{ \ \delta(u, b) \mid u \in \mathcal{G}_V, \ b \in Im(D_u F) \ \}.$$

Proof. We compute $D_a F(x)$ for $a \in \mathbb{F}_{2^n}, a \neq 0$:

$$\begin{aligned} D_a F(x) &= x^k(h(x^\rho)) + (x+a)^k(h((x+a)^\rho)) \\ &= \sum_{i=0}^{\ell} \nu_i \left(x^{k+i\rho} + (x+a)^{k+i\rho} \right) \\ &= a^k \left(\sum_{i=0}^{\ell} \nu_i a^{i\rho} \left((x/a)^{k+i\rho} + ((x/a)+1)^{k+i\rho} \right) \right). \end{aligned} \tag{12}$$

Since $\gcd(\rho, V) = 1$, every $a \in \mathbb{F}_{2^n}^*$ can be written as $a = uv$ with $u \in \mathcal{G}_V$ and $v \in \mathcal{G}_\rho$. Replacing in (12) $x = ay$ and $a = uv$ we get

$$D_aF(ay) = (uv)^k \left(\sum_{i=0}^{\ell} \nu_i u^{i\rho} \left(y^{k+i\rho} + (y+1)^{k+i\rho} \right) \right). \tag{13}$$

Thus F is APN if and only if

$$y \mapsto \sum_{i=0}^{\ell} \nu_i u^{i\rho} \left(y^{k+i\rho} + (y+1)^{k+i\rho} \right)$$

is 2-to-1 for any $u \in \mathcal{G}_V$. To compute $\delta(F)$ we need to compute the number $\delta(a, b)$ of solutions x of the equations

$$D_aF(x) = b,\ a \in \mathbb{F}_{2^n}^*,\ b \in \mathbb{F}_{2^n}.$$

According to (13), the equation above reduces

$$u^k \left(\sum_{i=0}^{\ell} \nu_i u^{i\rho} \left(y^{k+i\rho} + (y+1)^{k+i\rho} \right) \right) = b', b' = \frac{b}{v^k},$$

showing that $\delta(a, b) = \delta(u, b')$. Further $\delta(F)$ is the maximal value of the $\delta(u, b')$, $u \in \mathcal{G}_V,\ b' \in \mathbb{F}_{2^n}$, completing the proof. $\diamond$

The next result is derived from [1, Theorem 2] similarly to Theorem 4:

Corollary 3 *Notation is as in Theorem 6. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be given by (11) with components f_λ, $\lambda \in \mathbb{F}_{2^n}$. Then F is APN if and only if for all $a \in \mathcal{G}_V$:*

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}. \tag{14}$$

If for example $\rho = (2^n - 1)/3$ we need to do very few computations:

Example 5 *Let $n = 2m$, $2^n - 1 = 3\rho$ where 3 does not divide ρ. In this case, to compute the differential spectrum of F (given by (11)) we need to compute the image of D_uF for $u \in \mathbb{F}_4^*$ only. Note that 3 divides ρ if and only if 3 divides m.*

3.1 Binomials with low differential uniformity

In this section we study specific families of binomials derived from (11). Let $2^n - 1 = \rho V$, we consider binomials given by:

$$F(x) = \nu x^k + x^{k+\ell\rho}, \quad \nu \in \mathbb{F}_{2^n}^*, \ 1 \leq k \leq 2^n - \rho - 2, \ 1 \leq \ell < V. \tag{15}$$

As we showed in Theorem 6 the differential spectrum of $F(x)$ can be computed with elements of a suitable subgroup of $\mathbb{F}_{2^n}^*$, if $\gcd(\rho, V) = 1$. Recall that $\mathcal{G}_\rho$ denotes the subgroup of $\mathbb{F}_{2^n}^*$ of order ρ.

The first natural question to be answered is whether there are APN binomials given by (15). The next example shows that such an APN mapping is known.

Example 6 *Let $n = 2m$ with m odd and consider the binomials on $\mathbb{F}_{2^n}$ given by*

$$F(x) = x^3(\nu + x^{2^m+1}) = \nu x^3 + x^{2^m+4}$$

where $\nu \in \omega\mathbb{F}_{2^m}$ with $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. By Theorem 6, to compute the differential uniformity of $F(x)$ it is enough to consider $a \in \mathbb{F}_{2^m}^*$.

Note that $x \mapsto \nu x + x^{2^m+2}$ is a permutation [8, Theorem 5.1].

This class includes the first example of an APN mapping which is not equivalent to a power mapping. It was presented in [9, Theorem 2]*, due to Edel, Kyureghyan and Pott:*

$$x \mapsto x^3 + ux^{36}, \ u \in \omega\mathbb{F}_{2^5}^* \quad \text{where} \quad \omega \in \mathbb{F}_4 \setminus \{0, 1\}.$$

The latter mapping is not bijective.

It is mentioned in [9] that a complete computer search for APN binomials $x^r + ux^s$ on $\mathbb{F}_{2^n}$ was done for $n \leq 10$.

In the remaining of this work we are interested in bijective binomials, defined by (15), of degree at least 3, which have low differential uniformity. Proposition 1 yields a large class of bijective binomials of type (15):

Corollary 4 (cf. [8, Corollary 4]) *Let $2^n - 1 = \rho V$, $\rho > 1$ and $V > 1$, where $\gcd(\rho, V) = 1$. Let $\nu \in \mathbb{F}_{2^n}^*$ and*

$$F(x) = x^k(\nu + x^\rho), \ k = jV \text{ where } 1 \leq j \leq \rho - 1. \tag{16}$$

Then F is a permutation on $\mathbb{F}_{2^n}$ if and only if $\gcd(j, \rho) = 1$, $\nu \notin \mathcal{G}_V$ and $(\nu + \mathcal{G}_V)^\rho = \mathcal{G}_V$.

Note that, concerning the differential spectrum of binomials (16), by Theorem 6 we need to study the derivatives

$$y \mapsto \nu \left(y^{jV} + (y+1)^{jV}\right) + u^{\rho} \left(y^{jV+\rho} + (y+1)^{jV+\rho}\right), \ u \in \mathcal{G}_V.$$

3.2 Numerical results

In this section, we present some interesting numerical results that we obtained for binomials discussed in Section 3.1. We did experiments for binomials $F(x) = ax^k + x^{k+\rho}$ with the smallest values of V or for small n. Finding such bijective F having $\delta(F) = 4$ seems difficult; actually we obtained no example unless when F is affine equivalent to a monomial, as we explain below.

For $n = 8$ we obtained easily such binomials F satisfying $\delta(F) = 6$ (see, for instance, Table 1). This holds (not so easily) for $n = 10$ and $V = 3$. However we have no example for $n = 12$ and $V = 5$ and incline to conjecture that for $n > 10$ such binomials F satisfy $\delta(F) > 6$.

Table 1. With notation of (15): $n = 8$, $\ell = 1$, $\rho = 85$ and $V = 3$. We give the differential spectrum of bijective differentially 6-uniform binomials of the form

$$F(x) = \nu x^k + x^{k+85}, \ \nu = \alpha^3, \ 1 \leq k \leq 169,$$

where α is a root of the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$. The subgroup $\mathcal{G}_3$ is $\mathbb{F}_4^* = \{ \alpha^{i \cdot 85}, \ i = 0, 1, 2\}$. The spectrum is presented as follows:

$$\{\delta(e, b), \ b \in Im(D_e F)\}, \ (\textit{number of times } \delta(e, b) \textit{ occur}),$$

for any $e \in \mathbb{F}_4^*$, *i.e.,* $i \in \{0, 1, 2\}$. There are other values of k for which F is bijective but has a differential spectrum already in the table, corresponding to some k', where $k' < k$. Note that k is not always a multiple of V (as it was assumed in Corollary 4).

Example 7 *With notation of (15):*

$$n = 10, \ \ell = 1, \ \rho = (2^{10} - 1)/3 = 341 \textit{ and } V = 3.$$

There are bijective differentially 6*-uniform binomials of the form*

$$F(x) = \nu x^k + x^{k+341}, \quad 1 \leq k \leq 681.$$

We give below two examples where $\nu = \alpha^3$, α being a root of the primitive polynomial $X^{10} + X^3 + 1$.

k	i	spectrum	k	i	spectrum
3	0	{2, 4, 6}, (76, 20, 4)	7	0	{2, 4, 6}, (78, 19, 4)
	1	{2, 4, 6}, (82, 20, 2)		1	{2, 4}, (76, 26)
	2	{2, 4, 6}, (82, 17, 4)		2	{2, 4, 6}, (83, 21, 1)
42	0	{2, 4, 6}, (87, 19, 1)	54	0	{2, 4, 6}, (84, 16, 4)
	1	{2, 4}, (94, 17)		1	{2, 4, 6}, (75, 22, 3)
	2	{2, 4, 6}, (89, 18, 1)		2	{2, 4, 6}, (89, 18, 1)
57	0	{2, 4, 6}, (73, 20, 5)	106	0	{2, 4}, (90, 19)
	1	{2, 4,6}, (81, 22, 1)		1	{2, 4, 6}, (93, 16, 1)
	2	{2, 4, 6}, (80, 15, 6)		2	{2, 4, 6}, (87, 19, 1)
126	0	{2, 4, 6}, (77, 21, 3)			
	1	{2, 4,6}, (83, 21, 1)			
	2	{2, 4, 6}, (77, 18, 5)			

Table 1: Permutations $F(x) = \nu x^k + x^{k+85}$ ($n = 8$) which are differentially 6-uniform. Notation is explained in Section 3.2

- $F(x) = \alpha^3 x^{85} + x^{426}$. *The spectrum of the three derivatives are*

  $$\{2,4,6\},\ (348,70,8);\ \{2,4,6\},\ (360,70,4);\ \{2,4,6\},\ (366,64,6),$$

  where (a,b,c) *means that* 2 *appeared* a *times,* 4 *appeared* b *times and* 6 *appeared* c *times.*

- $F(x) = \alpha^3 x^{213} + x^{554}$. *The spectrum of the three derivatives are*

  $$\{2,4,6\},\ (370,59,8);\ \{2,4,6\},\ (360,70,4);\ \{2,4,6\},\ (344,75,6).$$

Some binomials with differential uniformity 4 appeared when $n = 10$. They are of the form:

$$F(x) = \nu x^k + x^{k+\rho},\ k = iV + 1 \text{ for } i \text{ in the range } [1, \rho - 1] \qquad (17)$$

where $\nu \in \mathbb{F}_{2^n}^*$, $n = 2m$, $\rho = 2^m - 1$ and $V = 2^m + 1$.

Claim 1 *Let F be given by (17). Then F is affine equivalent to the monomial of exponent $k = i(2^m+1)+1$. More precisely $F(x) = L(x^k)$, $L(x) = \nu x + x^{2^m}$, and F is a permutation if and only if $\nu \notin \mathcal{G}_{2^m+1}$ and* $\gcd(2i+1, 2^m-1) = 1$.

Proof. We have $k+\rho = i(2^m+1)+1+(2^m-1) = i(2^m+1)+2^m$ and then

$$F(x) = \nu x^{i(2^m+1)+1} + x^{i(2^m+1)+2^m} = L(x^{i(2^m+1)+1})$$

where $L : x \mapsto \nu x + x^{2^m}$. Clearly L is a permutation if and only if $\nu \notin \mathcal{G}_V$. Further, F is permutation if and only if

$$\gcd(i(2^m+1)+1, 2^m-1) = \gcd(2i+1, 2^m-1) = 1,$$

completing the proof. ◇

Claim 1 shows that some properties of F, given by (17), are actually properties of the monomial mapping $M : x \mapsto x^k$, in particular the differential spectrum of F is the differential spectrum of M. For $n = 10$, we found 9 such binomials F which are differentially 4-uniform.

Claim 2 *Let $n = 10$. Consider the mapping $M : x \mapsto x^k$ over $\mathbb{F}_{2^n}$ where k takes the following values*

$$k = 33i+1,\ i \in \{\ (1,10),\ (7,14),\ (9,24),\ (26,27)\ \} \text{ and } i = 30 \qquad (18)$$

(where we give by pairs one exponent and its compositional inverse). These mappings are bijective and satisfy $\delta(M) = 4$.

The pair $(1, 10)$ corresponds to the quadratic one with its inverse and $i = 30$ corresponds to the inverse function since

$$(2^5-2)(2^5+1)+1 = -(2^5+1)+1 = -2^5 = 2^5(-1).$$

More generally, it is easy to check that

$$(33i+1)(33j+1) \equiv 1 \pmod{2^{10}-1} \iff 2ji+i+j \equiv 0 \pmod{31}.$$

since

$$((2^m+1)i+1)((2^m+1)j+1) \equiv (2^m+1)(2ji+i+j)+1 \pmod{2^{2m}-1}.$$

Thus, for any i we compute j to have the compositional inverse of $x \mapsto x^k$.

Claim 3 *Let F be given by*

$$F(x) = x^d,\ d = i(2^m+1)+1,\ i \in [1,\ 2^m-1] \text{ with } \gcd(2i+1, 2^m-1) = 1.$$

Then F is a permutation with compositional inverse $x \mapsto x^\ell$ where

$$\ell = j(2^m+1)+1 \text{ such that } j(2i+1)+i \equiv 0 \pmod{2^m-1}.$$

In [3, Table 1] all differentially 4-uniform bijective monomials are listed when $6 \leq n \leq 25$. For $n = 10$ there are 3 sporadic differentially 4-uniform monomials appearing in this list (in fact there are 6 by including for each exponent also its inverse). In Claim 2 we identified, accidentally, the expressions for these sporadic differentially 4-uniform monomials.

Remark 2 *Bracken and Leander proved in [5] that the mapping,*

$$M(x) = x^{2^{2r}+2^r+1}, \ r \text{ odd, on the field } \mathbb{F}_{2^n} \text{ with } n{=}4r,$$

which is a highly nonlinear permutation, satisfies $\delta(M) = 4$. Note that

$$2^{3r}(2^{2r} + 2^r + 1) = 2^r + 1 + 2^{3r} = 2^r(2^{2r} + 1) + 1.$$

According to Claim 3, we can express the compositional inverse of such mapping $M^{2^{3r}}$. It is

$$M'(x) = x^{j(2^{2r}+1)+1}, \ j(2^{r+1} + 1) + 2^r \equiv 0 \pmod{2^{2r} - 1}.$$

4 Conclusion

Many questions arise when the computational aspects of the differential uniformity of mappings are discussed. In this paper our purpose was to create restricted corpus that it is easier to explore. We are conscious that the main problem is the size of n (when considering mappings on $\mathbb{F}_{2^n}$). For high values of n computations become impossible; in this case finding some iterative tools seems to be a possible solution, which need to be understood.

Another research direction, which need to be explored is identifying families of mappings for which the computation of differential spectrum is considerably easier than for a generic case. As Section 3 shows after identifying such families, easy computations lead already to interesting observations.

Acknowledgment

In this version we correct the statements of Proposition 1 and Corollary 4 in our previous version. We thank deeply Hubert Kiechle for his careful reading of our paper and for pointing us a gap in the proof of Proposition 1

Fortunately, Proposition 1 and Corollary 4 are quite isolated from the rest of our results, which aim to reduce computation complexity of the differential uniformity. All numerical results reported in [1] were doublechecked and are correct.

References

[1] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On Almost Perfect Nonlinear functions over $\mathbf{F}_2^n$, *IEEE Trans. Inform. Theory*, vol. 52, n. 9, pp. 4160-70, September 2006.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations, Advances in Cryptology–EUROCRYPT 93 (Lofthus, 1993), Lecture Notes in Comput. Sci. 765, Springer, Berlin, 1994, pp. 65–76.

[3] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. *Int. J. Inform. and Coding Theory*, 1(2):149–170, 2010. Special Issue dedicated to Vera Pless.

[4] R. C. Bose, and R. C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes, Journal of Comb. Theory 1, pp. 96-104 (1966).

[5] C. Braken and G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields and Their Applications 16, pp. 231–242 (2010).

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

[7] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, *IEEE Trans. Inform. Theory*, 47(4):1494–1513, 2001.

[8] P. Charpin and G. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}$, *SIAM J. of Discrete Math.* , 22(2):650–665, 2008.

[9] Y. Edel, G. Kyureghyan, and A. Pott, A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, 52(2):744–747, 2006.

[10] G. M. Kyureghyan, Special mapping of finite fields, invited survey in Finite Fields and Their Applications, eds. P. Charpin, A. Pott and A. Winterhof, De Gruyter (2013) pp. 117-144.

[11] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in cryptology—EUROCRYPT '91 (Brighton, 1991)*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 378–386. Springer, Berlin, 1991.

[12] A. Pott, E. Pasalic, A. Muratovic-Ribic and S. Bajric, Vectorial quadratic bent functions as a product of two linearized polynomials, Proceedings of the 9th International Workshop on Coding and Cryptography, WCC2015, `https://hal.archives-ouvertes.fr/WCC2015/`,

[13] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. *Proc. Amer. Math. Soc.* 137 (2009), 2209-2216.