Noname manuscript No.
(will be inserted by the editor)

Image sets of perfectly nonlinear maps

Lukas Kölsch · Björn Kriepke · Gohar M. Kyureghyan

Received: date / Accepted: date

Abstract We consider image sets of d-uniform maps of finite fields. We present a lower bound on the image size of such maps and study their preimage distribution, by extending methods used for planar maps in [19,24,28]. We apply the results to study d-uniform Dembowsi-Ostrom polynomials. Further, we focus on a particularly interesting case of APN maps on binary fields $\mathbb{F}_{2^n}$. For these maps our lower bound coincides with the one from [15,21]. We show that APN maps fulfilling the lower bound have a very special preimage distribution. We observe that for an even n the image sets of several well-studied families of APN maps are minimal. In particular, for n even, a Dembowski-Ostrom polynomial of form $f(x) = f'(x^3)$ is APN if and only if f is almost-3-to-1, that is when its image set is minimal. Also, any almost-3-to-1 component-wise plateaued map is necessarily APN, if n is even. For n odd, we believe that the lower bound is not sharp. For n odd, we present APN Dembowski-Ostrom polynomials of form $f'(x^3)$ on $\mathbb{F}_{2^n}$ with image sizes 2^{n-1} and $5 \cdot 2^{n-3}$. We present results connecting the image sets of special APN maps with their Walsh spectrum. Especially, we show that a large class of APN maps has the classical Walsh spectrum. Finally, we present upper bounds on the image size of APN maps. In particular, we show that the image set of a non-bijective almost bent map contains at most $2^n - 2^{(n-1)/2}$ elements.

Keywords Image set · APN map · differential uniformity · Walsh spectrum · quadratic map · Dembowski-Ostrom polynomial · plateaued function

1 Introduction

Let p be a prime and $q = p^n$. A map $f : \mathbb{F}_q \to \mathbb{F}_q$ is called d-uniform, if

$$d = \max_{a \neq 0, b \in \mathbb{F}_q} |\{x \in \mathbb{F}_q : f(x+a) - f(x) = b\}|.$$

A 1-uniform map $f : \mathbb{F}_q \to \mathbb{F}_q$ is called planar, that is f is planar if $f(x+a) - f(x)$ is a permutation for any $a \in \mathbb{F}_q^*$. Planar functions exist if and only if q is odd. A

Lukas Kölsch, Björn Kriepke, Gohar M. Kyureghyan
University of Rostock, Institute of Mathematics Ulmenstrasse 69, 18057 Rostock
E-mail: {lukas.koelsch,bjoern.kriepke,gohar.kyureghyan}@uni-rostock.de

map f is called almost perfect nonlinear (APN) if f is 2-uniform. Observe that if q is even, then an equation $f(x+a)+f(x)=b$ has always an even number of solutions, since x solves it if and only if $x+a$ does so. In particular there are no 1-uniform maps for q even, and the APN maps have the smallest possible uniformity on binary fields. APN maps and more generally maps in characteristic 2 with low uniformity are an important research object in cryptography, mainly because they provide good resistance to differential attacks when used as an S-box of a block cipher. For a thorough survey detailing the importance of such mappings for cryptography, we refer to [4]. Moreover, functions with low uniformity are intimately connected to certain codes [10,11]. Planar functions can be used for the construction of various structures in combinatorics and algebra, for example difference sets, projective planes and semifields [25].

In this paper we first study the image sets of d-uniform maps. We generalize the methods used in [19,24,28] to obtain a lower bound for the size of d-uniform maps. This bound is sharp for several classes of d-uniform maps. However there are cases, where we expect that our bound can be improved. We prove several results on the preimage distribution of d-uniform maps. We show that some classes of d-uniform Dembowski-Ostrom polynomials are uniquely characterized by the size of their image set. Further we consider in more detail the case $d=2$, that is APN maps, on binary fields.

Presently, the only known primary families of APN maps are monomials $x \mapsto x^k$ or Dembowski-Ostrom polynomials. These maps serve as a basis for a handful known secondary constructions of APN maps. Whereas the image sets of monomial maps are multiplicative subgroups and so uniquely defined by $\gcd(q-1,k)$, the behavior of the image sets of Dembowski-Ostrom polynomials is complex and not very well understood yet. In this paper, we prove that if n is even, then Dembowski-Ostrom polynomials of shape $f(x^3)$ on $\mathbb{F}_{2^n}$ are APN if and only if they are almost-3-to-1 (precise definitions are given later). Moreover we show that any almost-3-to-1 component-wise plateaued map is necessarily APN. Recall that the set of component-wise plateaued maps includes quadratic maps, and hence DO polynomials. This observation simplifies the computer search as well as the theoretical checking of the APN property for such maps. For n odd, we show that the image size of APN DO polynomials with exponents divisible by 3 (as integers) is not unique. We present such families with image sizes $2^n, 2^{n-1}$ and $5\cdot 2^{n-3}$. We observe that no APN map with image size 2^{n-1} can be obtained as a composition of an APN map and a linear map with one-dimensional kernel. To show this we prove that a composition of an APN map with a linear map remains APN if and only if the linear map is bijective. The key step in our prove is the analogous result for linear binomials proved in [3].

For n even, we show that a component-wise plateaued, almost- 3-to-1 map is an APN map with the classical Walsh spectrum, that is it has the same Walsh spectrum as the Gold map $x \mapsto x^3$. This explains why various important families of APN maps have classical Walsh spectrum. For n odd we find a direct connection between the image set of an almost bent map and the number of its balanced component functions. As a consequence, we show that any almost bent map has a balanced component function. We conclude our paper with an upper bound on the image size of non-bijective almost bent maps and component-wise plateaued

APN maps. To our knowledge these are the only currently known non-trivial upper bounds on the image size of APN maps.

2 Images of d-uniform functions

Let $\mathrm{Im}(f)$ be the image set of a map $f : \mathbb{F}_q \to \mathbb{F}_q$. For $r \geq 1$ we denote by $M_r(f)$ the number of $y \in \mathbb{F}_q$ with exactly r preimages. Further, let $N(f)$ denote the number of pairs $(x, y) \in \mathbb{F}_q^2$, such that $f(x) = f(y)$. Note $N(f) \geq q$ and $N(f) = q$ exactly when f is a permutation on $\mathbb{F}_q$. Let m be the degree of f, that is the degree of its polynomial representation of degree not exceeding $q - 1$. Then $M_r(f) = 0$ for every $r > m$. The following identities follow directly from the definition of $M_r(f)$ and $N(f)$

$$\sum_{r=1}^{m} M_r(f) = |\,\mathrm{Im}(f)| \tag{1}$$

$$\sum_{r=1}^{m} rM_r(f) = q \tag{2}$$

$$\sum_{r=1}^{m} r^2 M_r(f) = N(f). \tag{3}$$

The quantities M_r and $N(f)$ appear naturally when studying the image sets of maps on finite fields, see for example [12,19,24]. A map $f : \mathbb{F}_q \to \mathbb{F}_q$ is called k-to-1, if every element in the image of f has exactly k preimages, that is if $M_r(f) = 0$ for any $0 < r \neq k$.

Lemma 1 *Any map $f : \mathbb{F}_q \to \mathbb{F}_q$ fulfills*

$$|\,\mathrm{Im}(f)| \geq \frac{q^2}{N(f)},$$

with equality if and only if f is k-to-1.

Proof It follows from the Cauchy-Schwarz inequality with (1), (2) and (3) that

$$q^2 = \left(\sum_{r=1}^{m} rM_r(f)\right)^2 \leq \left(\sum_{r=1}^{m} r^2 M_r(f)\right)\left(\sum_{r=1}^{m} M_r(f)\right) = N(f)|\,\mathrm{Im}(f)|.$$

The equality above holds if and only if there is a $k \in \mathbb{R}$ such that $r\sqrt{M_r(f)} = k\sqrt{M_r(f)}$ for all $1 \leq r \leq m$, that is $M_k(f) = |\,\mathrm{Im}(f)|$ and $M_r(f) = 0$ for $r \neq k$. □

A celebrated result of Ding and Yuan shows that image sets of planar maps yield skew Hadamard difference sets [22]. Further properties of the image sets of planar maps can be found for example in [19,24,27]. The image sets of d-uniform maps with $d > 1$ can be used to construct optimal combinatorial objects too, [13], but they are not well-studied yet.

The following proof is an adaption for any d of [24, Lemma 2], where planar functions were considered.

Lemma 2 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be d-uniform. Then*

$$N(f) \leq q + d \cdot t_0(f),$$

where $t_0(f)$ is the number of elements $a \neq 0$ in $\mathbb{F}_q$ for which $f(x+a) - f(x) = 0$ has a solution x in $\mathbb{F}_q$. The equality holds if and only if every of these $t_0(f)$ equations has exactly d solutions.

Proof Note that

$$\begin{aligned} N(f) &= |\{(u,v) \in \mathbb{F}_q^2 : f(u) = f(v)\}| \\ &= |\{(u,v) \in \mathbb{F}_q^2 : f(u) - f(v) = 0\}| \\ &= |\{(a,v) \in \mathbb{F}_q^2 : f(v+a) - f(v) = 0\}|. \end{aligned}$$

For $a = 0$ every pair $(0, v)$ with $v \in \mathbb{F}_q$ contributes to $N(f)$. If $a \neq 0$, then $f(v+a) - f(v) = 0$ has at most d solutions because f is d-uniform. Therefore

$$N(f) \leq q + d \cdot t_0(f).$$

□

Observe that for a planar map $N(f) = 2q - 1$, since $f(v+a) - f(v) = 0$ has a unique solution for every non-zero a. Generalizing this, a map $f : \mathbb{F}_q \to \mathbb{F}_q$ is called zero-difference d-balanced if the equation $f(x+a) - f(x) = 0$ has exactly d solutions for every non-zero a, see [13]. Hence $N(f) = q + (q-1)d = (d+1)q - d$ for a zero-difference d-balanced map.

Corollary 1 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be d-uniform. Then*

$$N(f) \leq (d+1)q - d.$$

The equality holds if and only if f is zero-difference d-balanced.

Proof The statement follows from Lemma 2 and $t_0(f) \leq q - 1$. □

Remark 1 Note that most of the results in this paper hold for any map f with $N(f) \leq (d+1)q - d$, and not only for d-uniform ones. Some of our proofs can easily be adapted if $N(f) = kq \pm \varepsilon$ is known.

Theorem 1 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be d-uniform. Then*

$$|\operatorname{Im}(f)| \geq \left\lceil \frac{q}{d+1} \right\rceil.$$

Proof With Lemma 1 and Corollary 1 it follows that

$$|\operatorname{Im}(f)| \geq \left\lceil \frac{q^2}{N(f)} \right\rceil \geq \left\lceil \frac{q^2}{(d+1)q - d} \right\rceil \geq \left\lceil \frac{q}{d+1} \right\rceil. \tag{4}$$

□

The proof of Theorem 1 shows that the gap between $|\operatorname{Im}(f)|$ and $\left\lceil \frac{q}{d+1} \right\rceil$ is small, when f is close to being k-to-1 and $N(f)$ is about $(d+1)q-d$. Furthermore, the bound in Theorem 1 is sharp; if $d+1$ is a divisor of $q-1$, then the map $x \mapsto x^{d+1}$ is d-uniform and reaches the lower bound of Theorem 1.

Theorem 2 extends [24, Theorem 2]. Besides of giving a different proof for Theorem 1, it additionally provides information on the possible preimage distribution of a d-uniform map with minimal image set. For a map $f : \mathbb{F}_q \to \mathbb{F}_q$ and $S \subseteq \mathbb{F}_q$, $a \in \mathbb{F}_q$, we denote by $f^{-1}(S)$ the preimage of S under f and by $\omega(a)$ the size of $f^{-1}(\{a\})$.

Theorem 2 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be d-uniform and $I = \operatorname{Im}(f)$. Then*

$$|I| \geq \left\lceil \frac{q}{d+1} \right\rceil.$$

If

$$|I| = \left\lceil \frac{q}{d+1} \right\rceil = \frac{q+\varepsilon}{d+1}$$

with $1 \leq \varepsilon \leq d$, then

$$\sum_{y \in I} (\omega(y) - (d+1))^2 \leq (d+1)(\varepsilon - 1) + 1. \tag{5}$$

Proof By Corollary 1

$$\sum_{y \in I} (\omega(y))^2 = \sum_{y \in \mathbb{F}_q} (\omega(y))^2 = N(f) \leq (d+1)q - d.$$

It is obvious, that

$$\sum_{y \in I} \omega(y) = q.$$

It follows

$$\begin{aligned} 0 &\leq \sum_{y \in I} (\omega(y) - (d+1))^2 = \sum_{y \in I} ((\omega(y))^2 - 2(d+1)\omega(y) + (d+1)^2) \\ &= N(f) - 2(d+1)q + (d+1)^2|I| \leq (d+1)q - d - 2(d+1)q + (d+1)^2|I| \\ &= -(d+1)q - d + (d+1)^2|I|, \end{aligned}$$

so that

$$(d+1)^2|I| \geq (d+1)q + d$$

and

$$|I| \geq \left\lceil \frac{(d+1)q+d}{(d+1)^2} \right\rceil = \left\lceil \frac{q}{d+1} + \frac{d}{(d+1)^2} \right\rceil \geq \left\lceil \frac{q}{d+1} \right\rceil.$$

Now let

$$|I| = \left\lceil \frac{q}{d+1} \right\rceil = \frac{q+\varepsilon}{d+1}$$

with $1 \leq \varepsilon \leq d$. Then

$$\begin{aligned} \sum_{y \in I} (\omega(y) - (d+1))^2 &\leq -(d+1)q - d + (d+1)^2 \frac{q+\varepsilon}{d+1} \\ &= \varepsilon d - d + \varepsilon = (d+1)(\varepsilon - 1) + 1. \end{aligned}$$

□

Let I be the image set of a d-uniform map f and

$$|I| = \frac{q+\varepsilon}{d+1}$$

and define

$$D = \{y \in I : \omega(y) \neq d+1\}.$$

Then we have

$$q = \sum_{y\in I} \omega(y) = \sum_{y\in I\setminus D} \omega(y) + \sum_{y\in D} \omega(y) = \left(\frac{q+\varepsilon}{d+1} - |D|\right)(d+1) + \sum_{y\in D} \omega(y),$$

implying

$$\sum_{y\in D} \omega(y) = |D|(d+1) - \varepsilon. \tag{6}$$

The following theorem is a generalization of [19, Theorem 1] and it provides information on the possible preimage distribution of a d-uniform map.

Theorem 3 *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be d-uniform. Then*

$$\sum_{r=1}^{d} r(d+1-r)M_r(f) \geq d \tag{7}$$

and

$$\sum_{r=1}^{d+1} r(d+2-r)M_r(f) \geq q+d. \tag{8}$$

The equality holds in (7) *if and only if it holds in* (8)*, which is the case if and only if $N(f) = (d+1)q - d$, $M_r(f) = 0$ for $r > d+2$ and*

$$\sum_{r=1}^{d} r(d+1-r)M_r(f) = (d+2)M_{d+2}(f) + d.$$

Proof Let m be the degree of f. With Corollary 1 we have $N(f) \leq (d+1)q - d$. Using (2) and (3) we get

$$\sum_{r=1}^{m} r^2 M_r(f) = N(f) \leq (d+1)q - d = (d+1)\sum_{r=1}^{m} rM_r(f) - d,$$

so that

$$\sum_{r=1}^{d+1} (r(d+1) - r^2)M_r(f) - d \geq \sum_{r=d+2}^{m} (r^2 - (d+1)r)M_r(f) \tag{9}$$

As the right hand side is non-negative, we have in particular

$$\sum_{r=1}^{d} r(d+1-r)M_r(f) \geq d.$$

Note that for $r \geq d+2$ it holds that $r^2-(d+1)r \geq r$, so that (9) turns into

$$\sum_{r=1}^{d+1} r(d+1-r)M_r(f) \geq \sum_{r=d+2}^{m} (r^2-(d+1)r)M_r(f)+d \geq \sum_{r=d+2}^{m} rM_r(f)+d. \quad (10)$$

Adding $\sum_{r=1}^{d+1} rM_r(f)$ on both sides of (10) and using (2) gives

$$\sum_{r=1}^{d+1} r(d+2-r)M_r(f) \geq \sum_{r=1}^{m} rM_r(f)+d = q+d.$$

For equality to hold, we need equality in (10). The first equality in (10) holds if and only if $N(f)=(d+1)q-d$, the second equality holds if and only if

$$\sum_{r=d+2}^{m} (r^2-(d+1)r)M_r(f) = \sum_{r=d+2}^{m} rM_r(f),$$

that is $M_r(f)=0$ for $r>d+2$. In that case

$$\sum_{r=1}^{d} r(d+1-r)M_r(f) = (d+2)M_{d+2}(f)+d.$$

□

3 Dembowski-Ostrom *d*-uniform polynomials

A polynomial/map $f \in \mathbb{F}_q[x]$ is called Dembowski-Ostrom (DO), if it can be written as

$$f(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j}$$

when q is odd and

$$f(x) = \sum_{\substack{i,j=0 \\ i\neq j}}^{n-1} a_{ij} x^{2^i+2^j}$$

when q even. Note that x^2 is a DO polynomial for any odd q, but not for even q. Maps obtained as the sum of a DO map with an $\mathbb{F}_p$-affine one are called quadratic.

Let k be a divisor of $q-1$. We call a map f k-divisible, if it can be written as $f(x)=f'(x^k)$ for a suitable f'. Observe that f is k-divisible if and only if $f(x)=f(\omega x)$ for all $x \in \mathbb{F}_q$ and all $\omega \in \mathbb{F}_q^*$ whose order divides k. Further, we call a map f almost-k-to-1[1], if there is a unique element in $\mathrm{Im}(f)$ with exactly 1 preimage and all other images have exactly k preimages. When considering the d-uniform property of an almost-k-to-1 map f, we can without loss of generality assume that $f(0)=0$ and that 0 is the unique element with exactly one preimage. Indeed, if $f(x)$ is d-uniform, then so is $f(x+c)+d$ for arbitrary $c,d \in \mathbb{F}_q$.

[1] Note that in many papers such maps are called just k-to-1. However we use the terminology almost-k-to-1 to avoid confusion with k-to-1 maps considered in Section 2.

For a non-zero $a \in \mathbb{F}_q$ we define

$$D_a(f) := \{f(x+a) - f(x) : x \in \mathbb{F}_q\},$$

which we call a differential set of f in direction a. It is well-known and easy to see that the differential sets of quadratic maps are affine subspaces. The following result can be deduced from Proposition 3 and Corollary 1 in [13]. We include its proof for the convenience of the reader.

Lemma 3 *Let $d+1$ be a divisor of $q-1$ and $f : \mathbb{F}_q \to \mathbb{F}_q$ be a $(d+1)$-divisible DO polynomial which is almost-$(d+1)$-to-1. Then f is zero-difference d-balanced. In particular, such a map f is d-uniform and all its differential sets are linear subspaces.*

Proof Since f is a DO polynomial, it is d-uniform in the case it is zero-difference d-balanced. First we show that for any non-zero a the equation $f_a(x) = f(x+a) - f(x) = 0$ has a solution (equivalently, $D_a(f)$ is a subspace). Indeed, let $1 \neq \omega \in \mathbb{F}_q$ be a zero of $x^{d+1} - 1$ and set $x = (\omega - 1)^{-1}a$. This x fulfills $x + a = \omega x$, and hence $f_a(x) = f(\omega x) - f(x) = 0$. In particular, $f_a(x) = 0$ hast at least d solutions. On the other side, since f is $(d+1)$-divisible and almost-$(d+1)$-to-1, the equation $f(x+a) = f(x)$ is fulfilled if and only if $x + a = \omega x$ for an element ω satisfying $\omega^{d+1} = 1$. This implies that a solution x must be given by $a(\omega - 1)^{-1}$. And hence there are at most d solution for $f_a(x) = 0$, proving the statement. □

Corollary 2 *Let $q = p^n$ with p prime and $d+1$ be a divisor of $q-1$. A $(d+1)$-divisible almost-$(d+1)$-to-1 DO polynomials exist on $\mathbb{F}_q$ only if $d = p^i$ for some $i \geq 0$.*

Proof By Lemma 3, a $(d+1)$-divisible almost-$(d+1)$-to-1 DO polynomial is d uniform. The differential sets of DO polynomials are affine subspaces, proving that $d = p^i$ for some $i \geq 0$.

□

The converse of Lemma 3 also holds if f is not a DO polynomial.

Theorem 4 *Let $d+1$ be a divisor of $q-1$ and $f : \mathbb{F}_q \to \mathbb{F}_q$ be $(d+1)$-divisible and d-uniform. Then f is almost-$(d+1)$-to-1.*

Proof As f is $(d+1)$-divisible, we have $|\operatorname{Im}(f)| \leq \frac{q+d}{d+1}$. By Theorem 1 we have $|\operatorname{Im}(f)| \geq \frac{q+d}{d+1}$ and therefore $|\operatorname{Im}(f)| = \frac{q+d}{d+1}$ and f is almost-$(d+1)$-to-1. □

The following result is a direct consequence of Theorem 4 and Lemma 3.

Theorem 5 *Let $d+1$ be a divisor of $q-1$. A $(d+1)$-divisible DO polynomial f is d-uniform if and only if f is almost-$(d+1)$-to-1.*

If $d = p^i$ and $d+1 = p^i+1$ is a divisor of $q-1$, the map $x \mapsto x^{d+1}$ is a d-uniform DO Polynomial that is almost-$(d+1)$-to-1.

Later, in Theorem 15 we show that for APN maps over binary fields the condition of Lemma 3 that $f(x)$ is DO and 3-divisible can be relaxed to the one that f is almost-3-to-1 and component-wise plateaued.

4 Image sets of APN maps of binary finite fields

In the following sections we study the image sets of APN maps on binary fields. Such maps are of particular interest because of their applications in cryptography and combinatorics. Recently, Ingo Czerwinski showed that the image set of an APN map on $\mathbb{F}_{2^n}$ contains at least $(2^n+1)/3$ elements [21]. This bound is sharp for n even. Numerical results suggest that the minimal size of APN maps is much larger, probably around 2^{n-1}, if n is odd. The proof in [21] is based on linear programming. This lower bound appears (in an equivalent form) also in [14], where a lower bound on the differential uniformity via image set size is presented. The ideas from [14] are developed further in [15] and they are used to compare APN maps with affine ones.

The results of Section 2 yield an alternative proof for the lower bound on the size of the image set of an APN map on $\mathbb{F}_{2^n}$. Additionally, they imply possible preimage distributions of an APN map meeting the lower bound. Firstly, we state Theorem 3 for the APN maps on $\mathbb{F}_{2^n}$.

Corollary 3 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN. Then*

$$M_1(f) + M_2(f) \geq 1,$$

and hence there is at least one element with exactly 1 or 2 preimages. Furthermore

$$3M_1(f) + 4M_2(f) + 3M_3(f) \geq 2^n + 2.$$

The equality in the two inequalities above holds if and only if $N(f) = 3 \cdot 2^n - 2$, $M_r(f) = 0$ for $r > 4$ and

$$M_1(f) + M_2(f) = 2M_4(f) + 1.$$

The next theorem is a consequence of Theorem 1 and Theorem 2. Corollary 3 along with identity (6) and inequality (5) yield the possible preimage distributions of an APN map meeting the lower bound.

Theorem 6 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN and I be the image set of f. Then*

$$|I| \geq \begin{cases} \frac{2^n+1}{3} & n \text{ is odd,} \\ \frac{2^n+2}{3} & n \text{ is even.} \end{cases}$$

If n is odd and

$$|I| = \frac{2^n+1}{3},$$

then $\omega(y_0) = 2$ for one element $y_0 \in I$ and $\omega(y) = 3$ for $y \in I \setminus \{y_0\}$.

If n is even and

$$|I| = \frac{2^n+2}{3},$$

then one of the following cases must occur:

1. *$\omega(y_0) = 1$ for one element $y_0 \in I$ and $\omega(y) = 3$ for all $y \in I \setminus \{y_0\}$, that is f is almost-3-to-1.*
2. *$\omega(y_i) = 2$ for two elements $y_0, y_1 \in I$ and $\omega(y) = 3$ for all $y \in I \setminus \{y_0, y_1\}$.*

3. $\omega(y_i) = 2$ *for three elements* $y_0, y_1, y_2 \in I$, $\omega(y_3) = 4$ *for a unique* $y_3 \in I \setminus \{y_0, y_1, y_2\}$ *and* $\omega(y) = 3$ *for all* $y \in I \setminus \{y_0, \ldots, y_3\}$.

There are examples of APN maps meeting the lower bound for n even; we present several such families later in this paper. All such examples of APN maps are almost-3-to-1. We believe that cases 2. and 3. for n even never occur, and that there are no APN maps meeting the lower bound for n odd.

The lower bound in Theorem 6 can be used to prove several structural results for APN maps. For example, it gives an easy proof for the following well-known property of monomial APN maps.

Corollary 4 *Let* $q = 2^n$ *and* $f = x^k$ *be APN. Then* $\gcd(k, q-1) = 1$ *if* n *is odd and* $\gcd(k, q-1) = 3$ *if* n *is even.*

Proof Let I be the nonzero elements in the image set of f. Then

$$|I| = \frac{q-1}{\gcd(k, q-1)}.$$

With Theorem 6 this only leaves $\gcd(k, q-1) \leq 3$. For n odd we get $\gcd(k, q-1) = 1$.

Now let n be even and $\gcd(k, q-1) = 1$. Then f is an APN permutation on all subfields of $\mathbb{F}_q$, in particular it is an APN permutation on $\mathbb{F}_4$. However, no such permutation exists. Therefore $\gcd(k, q-1) = 3$. □

It is well-known that a DO polynomial is planar if and only if it is almost-2-to-1. As a direct consequence of Theorem 5 we obtain an analogue of this property for APN DO polynomials.

Theorem 7 *Let* n *be even and* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a 3-divisible DO polynomial. Then* f *is APN if and only if* f *is almost-3-to-1.*

We take a closer look at 3-divisible APN maps in the next section.

Next we show that APN quadratic maps constructed in [29] provide examples of almost-3-to-1 APN maps which are not 3-divisible.

Theorem 8 *Let* $n = 2m$, $m, i \geq 2$ *even,* $\gcd(k, m) = 1$ *and* $\alpha \in \mathbb{F}_{2^m}$ *not a cube. Then* $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ *given by*

$$f(x, y) = (x^{2^k+1} + \alpha y^{(2^k+1)2^i}, xy) \tag{11}$$

is almost-3-to-1. More precisely, $f(x, y) = f(u, v)$ *if and only if* $(x, y) = (\omega u, \omega^2 v)$ *with* $\omega \in \mathbb{F}_4^*$.

Proof Note that $\gcd(2^{2m} - 1, 2^k + 1) = 3$ and 3 is a divisor of both $2^m - 1$ and $2^i - 1$. Let $(x, y), (u, v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $f(x, y) = f(u, v)$. Then we have

$$x^{2^k+1} + \alpha y^{(2^k+1)2^i} = u^{2^k+1} + \alpha v^{(2^k+1)2^i}$$
$$xy = uv.$$

First suppose $v = 0$, and hence $x = 0$ or $y = 0$ too. For $x = 0$, we get

$$\alpha y^{(2^k+1)2^i} = u^{2^k+1},$$

which forces $y = u = 0$, since α is a non-cube. For $x, u \neq 0$ and $y = 0$ we get

$$x^{2^k+1} = u^{2^k+1},$$

which is satisfied if and only if $x = \omega u$ with $\omega \in \mathbb{F}_4^*$. Now let $v \neq 0$. Setting $u = \frac{xy}{v}$ and rearranging the first equation we get

$$x^{2^k+1} + \left(\frac{xy}{v}\right)^{2^k+1} = \alpha(y^{2^k+1} + v^{2^k+1})^{2^i}$$

or equivalently

$$x^{2^k+1}\left(1 + \left(\frac{y}{v}\right)^{2^k+1}\right) = \alpha v^{(2^k+1)2^i}\left(1 + \left(\frac{y}{v}\right)^{2^k+1}\right)^{2^i}.$$

If $1 + \left(\frac{y}{v}\right)^{2^k+1} \neq 0$, we can divide by it and obtain

$$x^{2^k+1} = \alpha v^{(2^k+1)2^i}\left(1 + \left(\frac{y}{v}\right)^{2^k+1}\right)^{2^i-1}. \tag{12}$$

Since x^{2^k+1}, $v^{(2^k+1)2^i}$ and $\left(1 + \left(\frac{y}{v}\right)^{2^k+1}\right)^{2^i-1}$ are all cubes and (12) does not have a solution as α is not a cube. Finally observe that $\left(\frac{y}{v}\right)^{2^k+1} = 1$ holds if and only if $y = \omega v$ with $\omega \in \mathbb{F}_4^*$, completing the proof. □

To see that the map considered in Theorem 8 is not a DO map, let (u_1, u_2) be a basis of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_{2^m}$ and (v_1, v_2) its dual basis. Then an element z of $\mathbb{F}_{2^{2m}}$ has the representation $(v_1 z + \overline{v_1 z})u_1 + (v_2 z + \overline{v_2 z})u_2$, where $\overline{a} = a^{2^m}$. Thus we get

$$\begin{aligned} f(z) &= f(v_1 z + \overline{v_1 z}, v_2 z + \overline{v_2 z}) \\ &= \left((v_1 z + \overline{v_1 z})^{2^k+1} + \alpha(v_2 z + \overline{v_2 z})^{(2^k+1)2^i}\right) u_1 \\ &+ (v_1 z + \overline{v_1 z}) \cdot (v_2 z + \overline{v_2 z}) u_2 \\ &= \ldots + ((v_1 \overline{v_2} + \overline{v_1} v_2) z^{2^m+1} + v_1 v_2 z^2 + \overline{v_1 v_2} z^{2 \cdot 2^m}) u_2. \end{aligned}$$

Since $k \neq 0$, there will be no term z^2 in the summand for u_1, and hence the above polynomial contains a non-zero term with z^2, showing that it is not DO.

A natural question is whether every quadratic APN map of $\mathbb{F}_{2^n}$ with even n is EA-equivalent to an almost-3-to-1 map. The answer is negative. As we show in Theorem 15, all almost-3-to-1 quadratic APN maps have the classical Walsh spectrum. And hence the EA-class of quadratic APN maps with non-classical Walsh spectra do not contain an almost-3-to-1 map.

5 3-divisible APN maps

Observe that by Theorem 7, every APN DO polynomial $f'(x^3)$ on $\mathbb{F}_{2^n}$, n even, is an example with the preimage distribution described in Case 1 of Theorem 6. Prominent examples for such APN maps are $x \mapsto x^3$ and $x \mapsto x^3 + \mathrm{Tr}(x^9)$. These maps are APN for any n. If n is odd, then $x \mapsto x^3$ is a permutation and $x \mapsto x^3 + \mathrm{Tr}(x^9)$ is 2-to-1, as we will see later in this section.

Next we present an interesting observation which could be helpful for performing numerical searches as well as theoretical studies of 3-divisible APN DO polynomials. In particular it could be used for classifying exceptional APN 3-divisible DO polynomials.

Theorem 9 *Let $n = 2^i m$ with $i \geq 1$ and $m \geq 3$ odd. Suppose $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a 3-divisible APN DO polynomial over the subfield $\mathbb{F}_{2^m}[x]$. Then f is an APN permutation on the subfield $\mathbb{F}_{2^m}[x]$.*

Proof Since the coefficients of f are from $\mathbb{F}_{2^m}$, it defines an APN map on it. By Theorem 7, f is almost-3-to-1 on $\mathbb{F}_{2^n}$. Moreover, $f(x) = f(\omega x) = f(\omega^2 x)$ for $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$. The statement now follows from the fact that $\mathbb{F}_4$ is not contained in $\mathbb{F}_{2^m}$. □

By Theorem 7, the substitution of x^3 in a polynomial of shape $f'(x) = L_1(x) + L_2(x^3)$, where L_1, L_2 are linearized polynomials, results in a DO polynomial $f(x) = f'(x^3) = L_1(x^3) + L_2(x^9)$. Hence by Theorem 7 any permutation of shape $L_1(x) + L_2(x^3)$ yields directly an APN DO polynomial if n is even. Observe that x^3 and $x^3 + \mathrm{Tr}(x^9)$ are of these type too. These and further APN DO polynomials $L_1(x^3) + L_2(x^9)$ are studied in [6,7]. Results from [18] can be used to construct and explain permutations of shape $f'(x) = L_1(x) + L_2(x^3)$. For example, Theorem 6 in [18] with $s = 3$ and $L(x) = x^2 + \alpha x$ gives the following family of APN 3-divisible DO polynomials.

Theorem 10 *Let α, β, γ be non-zero elements in $\mathbb{F}_{2^n}$ with n even. Further let $\gamma \notin \{x^2 + \alpha x \mid x \in \mathbb{F}_{2^n}\}$ and $\mathrm{Tr}(\beta\alpha) = 1$, then*

$$f'(x) = x^2 + \alpha x + \gamma \,\mathrm{Tr}(\alpha^{-3} x^3 + \beta x)$$

is a permutation on $\mathbb{F}_{2^n}$ and

$$f(x) = f'(x^3) = x^6 + \alpha x^3 + \gamma \,\mathrm{Tr}(\alpha^{-3} x^9 + \beta x^3)$$

is APN.

An APN map constructed in Theorem 10 is affine equivalent to one of form $x^3 + \alpha \,\mathrm{Tr}(\alpha^{-3} x^9)$. Indeed, the map $f'(x)$ can be reduced to

$$f'(x) = x^2 + \alpha x + \gamma \,\mathrm{Tr}(\beta x) + \gamma \,\mathrm{Tr}(\alpha^{-3} x^3) = L_1(x) + \gamma \,\mathrm{Tr}(\alpha^{-3} x^3),$$

where L_1 is linear over $\mathbb{F}_2$. Using [18, Theorem 5] the map L_1 is bijective. Then L_1^{-1} composed with $f'(x)$ yields

$$L_1^{-1} \circ f'(x) = x + \mathrm{Tr}(\alpha^{-3} x^3) L_1^{-1}(\gamma),$$

and thus

$$L_1^{-1} \circ f'(x^3) = x^3 + \mathrm{Tr}(\alpha^{-3}x^9)L_1^{-1}(\gamma) = x^3 + \alpha\,\mathrm{Tr}(\alpha^{-3}x^9),$$

where for the last equality we used $L_1(\alpha) = \gamma$. Note that this reduction remains true for n odd too, showing that the examples of Theorem 10 are APN for any n.

As we mentioned earlier the polynomials x^3 and $x^3 + \mathrm{Tr}(x^9)$ define APN maps on $\mathbb{F}_{2^n}$ for every $n \geq 1$. For n odd, the first map is a permutation and the second is 2-to-1, as the following result shows.

Proposition 1 *Let n be odd and $a \in \mathbb{F}_{2^n}$ non-zero. Then the APN map $x \mapsto x^3 + a^{-1}\,\mathrm{Tr}(a^3x^9)$ is 2-to-1.*

Proof This follows from Theorem 3 in [17], since a^{-1} is a 1-linear structure of $\mathrm{Tr}(a^3x^3)$ for n odd, which can be easily checked by direct calculations. □

We believe that if n is odd, then 2^{n-1} is the minimal possible image size of an APN DO polynomial of shape $L_1(x^3) + L_2(x^9)$. However, an analog of Theorem 7 is not true for the size 2^{n-1}. There are such DO polynomials with image size 2^{n-1}, which are not APN. For example, if n is odd, the DO polynomial $(x^2 + x) \circ x^3$ is 2-to-1, but not APN, as a consequence of the following result:

Theorem 11 *[3, Theorem 2] Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $L(x) = x + ux^{2^i}$ with $u \in \mathbb{F}_{2^n}$ and $i \geq 1$. Then $L(f(x))$ is APN if and only if L is bijective on $\mathbb{F}_{2^n}$.*

Next we observe that the statement of Theorem 11 remains true for the substitution $f(x^2 + ux)$ too.

Proposition 2 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN and $u \in \mathbb{F}_{2^n}$ non-zero. Then $g(x) = f(x^2 + ux)$ is not APN.*

Proof Suppose $a = b^2 + ub \neq 0$ and $y = z^2 + uz \neq 0$ belong to the image set of $x^2 + ux$. Then $y + a = (z + b)^2 + u(z + b)$. Then the elements $z, z + u, z + b, z + b + u$ have the same image under $g(x + b) + g(x)$. □

It is worth to note that Theorem 11 and Proposition 2 hold for general linearized polynomials. To prove this, we use the following observation.

Proposition 3 *Let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a $\mathbb{F}_2$-linear map with kernel $\{0, u\}$.*

(a) Then there are 2^{n-1} different $\mathbb{F}_2$-linear permutations L' such that $L(x) = L'(x^2 + ux)$.
(b) Then there are 2^{n-1} different $\mathbb{F}_2$-linear permutations L'' such that $L(x) = L''(x)^2 + uL''(x)$.

Proof The existence of a suitable linear permutation L' follows by comparing the number of different L and $L'(x^2 + ux)$, see for example [5, Theorem 5.4.]. Further note that for two different permutations L' and L'_1 we have

$$L'(x^2 + ux) = L'_1(x^2 + ux)$$

if and only if

$$(L' - L'_1)(x^2 + ux) = 0.$$

That is when L' and L'_1 coincide on the image set V of x^2+ux, which is a subspace of dimension $n-1$. Let $v_1,\ldots,v_{n-1}$ be a basis of V and let v extend it to a basis of $\mathbb{F}_{2^n}$. Then $L'(v_i)=L'_1(v_i)$ for every $1\le i\le n-1$ and $L'(v)\neq L'_1(v)$. Since the linear maps L' and L'_1 are bijective, the image of v is an arbitrary element from the complement of $n-1$ dimensional subspace generated by $L'(v_1),\ldots,L'(v_{n-1})$. In particular, there are exactly 2^{n-1} possible choices for the image of v, proving (a). To prove (b), we first show that if L can be represented in this form, then there are 2^{n-1} different choices for L''. Then using (a), we have that any 2-to-1 L has such a representation. Note that

$$L''(x)^2+uL''(x)=L''_1(x)^2+uL''_1(x)$$

if and only if

$$(L''(x)+L''_1(x))^2=u(L''(x)+L''_1(x)).$$

The last equality holds if and only if the linear map $L''+L''_1$ has image set $\{0,u\}$, that is when there is an element $\beta\in\mathbb{F}_{2^n}$ such that

$$(L''+L''_1)(x)=u\,\mathrm{Tr}(\beta x),$$

or equivalently

$$L''_1(x)=L''(x)+u\,\mathrm{Tr}(\beta x).$$

By [18, Theorem 3(a)], given a permutation L'', the sum $L''(x)+u\,\mathrm{Tr}(\beta x)$ is a permutation if and only if $\mathrm{Tr}(L''^{-1}(u)\beta)=0$. This holds for exactly 2^{n-1} elements β, completing the proof. □

Theorem 12 is a generalization of Theorem 11. We are not aware of any reference proving it, although it answers a rather natural question for the study of APN maps.

Theorem 12 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be APN and $L:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ linear over $\mathbb{F}_2$. Then $L\circ f$ or $f\circ L$ is APN if and only if L is bijective.*

Proof If L is bijective then both maps $L\circ f$ and $f\circ L$ are APN. So suppose L is not bijective. If dimension of kernel of L is at least 2, the maps $L\circ f$ and $f\circ L$ are not APN by Theorem 6. So we need only to consider the case, when L is 2-to-1. Suppose the kernel of L is $\{0,u\}$. By Proposition 3, there is a linear permutation L' such that $L(x)=L'(x^2+ux)$. Then $L(f(x))=L'(f(x)^2+uf(x))$, which is not a permutation by Theorem 11. The map $f(L(x))=(f\circ L')(x^2+ux)$ is not APN by Proposition 2. □

Next we observe that for n odd there are APN DO polynomials of shape $L_1(x^3)+L_2(x^9)$, that are neither bijective nor have image size 2^{n-1}. For a divisor t of n we denote by $Tr_{q^n/q^t}(x)$ the trace map from $\mathbb{F}_{2^n}$ into the subfield $\mathbb{F}_{2^t}$, that is

$$Tr_{q^n/q^t}(x)=\sum_{k=0}^{n/t}x^{(q^t)^k}.$$

In [7], it is shown that for any non-zero $a\in\mathbb{F}_{2^{3m}}$, m arbitrary, the DO polynomials

$$f_1(x)=f'_1(x^3)=x^3+a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3x^9+a^6x^{18})$$

and

$$f_2(x) = f_2'(x^3) = x^3 + a^{-1}(\mathrm{Tr}_{2^n/2^3}(a^3x^9 + a^6x^{18}))^2$$

define APN maps on $\mathbb{F}_{2^{3m}}$. The maps f_1' and f_2' are bijective when m is even. For m odd, the image sets of these maps contain $5q/8$ elements, as Theorems 13 and 14 show.

Theorem 13 *Let $n = 3m$ be odd and $a \in \mathbb{F}_q^*$ be arbitrary. Then the APN map*

$$f(x) = x^3 + a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3x^9 + a^6x^{18})$$

satisfies $M_1(f) = \frac{q}{2}$, $M_4(f) = \frac{q}{8}$. In particular $|\,\mathrm{Im}(f)| = \frac{5}{8}q$.

Proof We consider the equation $f(x) = f(y)$ on $\mathbb{F}_{2^{3m}}$. Since $x \mapsto x^3$ is a permutation on $\mathbb{F}_{2^n}$ with n odd, it is sufficient to look at $f'(x) = f'(y)$, where

$$f'(x) = x + a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3x^3 + a^6x^6),$$

and $f(x) = f'(x^3)$. Suppose $f'(x) = f'(y)$. Then

$$x + a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3x^3 + a^6x^6) = y + a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3y^3 + a^6y^6)$$

or equivalently,

$$\mathrm{Tr}_{2^n/2^3}(a^3x^3 + a^6x^6 + a^3y^3 + a^6y^6) = a(x+y). \tag{13}$$

In particular, $f'(x) = f'(y)$ only if $a(x+y) \in \mathbb{F}_8$. Let $z = x+y$. Taking the absolute trace on both sides of (13), we get

$$\mathrm{Tr}_{2^3/2}(az) = \mathrm{Tr}_{2^n/2}(a^3x^3 + (a^3x^3)^2 + a^3(x+z)^3 + (a^3(x+z)^3)^2) = 0.$$

Let $\beta \in \mathbb{F}_8$ with $\beta^3 = \beta + 1$, then

$$\mathrm{Tr}_{2^3/2}(\beta) = \mathrm{Tr}_{2^3/2}(\beta^2) = \mathrm{Tr}_{2^3/2}(\beta^4) = 0,$$

so that

$$az \in \{0, \beta, \beta^2, \beta^4\}.$$

If $az = 0$ we have $z = 0$ and $x = y$. So let $z = a^{-1}\beta^k$ with $k \in \{1, 2, 4\}$. Note that $x \mapsto x^k$ is a linear permutation on $\mathbb{F}_{2^{3m}}$. We have

$$\begin{aligned}
&a^3x^3 + a^6x^6 + a^3(x+z)^3 + a^6(x+z)^6\\
&= a^3x^3 + a^6x^6 + a^3(x^3 + x^2z + xz^2 + z^3) + a^6(x^6 + x^4z^2 + x^2z^4 + z^6)\\
&= a^3x^2z + a^3xz^2 + a^3z^3 + a^6x^4z^2 + a^6x^2z^4 + a^6z^6\\
&= a^2x^2\beta^k + ax\beta^{2k} + \beta^{3k} + a^4x^4\beta^{2k} + a^2x^2\beta^{4k} + \beta^{6k}\\
&= (\beta^{3k} + \beta^{6k}) + ax\beta^{2k} + a^2x^2(\beta^k + \beta^{4k}) + a^4x^4\beta^{2k}.
\end{aligned}$$

As $\beta^3 = \beta + 1$, we get $\beta^6 = \beta^2 + 1$ and therefore $\beta^3 + \beta^6 = \beta^2 + \beta = \beta^4$. Further $\beta + \beta^4 = \beta^2$, so that

$$a^3x^3 + a^6x^6 + a^3(x+z)^3 + a^6(x+z)^6 = \beta^{4k} + \beta^{2k}(ax + (ax)^2 + (ax)^4). \tag{14}$$

We now need to ensure that (13) holds. Using (14) and m odd this turns into

$$\begin{aligned}\beta^k &= \mathrm{Tr}_{2^n/2^3}(\beta^{4k} + \beta^{2k}(ax + (ax)^2 + (ax)^4)) \\ &= \beta^{4k} + \beta^{2k}\,\mathrm{Tr}_{2^n/2^3}(ax + (ax)^2 + (ax)^4) = \beta^{4k} + \beta^{2k}\,\mathrm{Tr}_{2^n/2}(ax). \\ &= (\beta^4 + \beta^2\,\mathrm{Tr}_{2^n/2}(ax))^k\end{aligned}$$

Using again that $x \mapsto x^k$ is a permutation and that $\beta^4 = \beta^2 + \beta$ we obtain

$$\beta^2(\mathrm{Tr}_{2^n/2}(ax) + 1) = 0,$$

which has a solution x if and only if $\mathrm{Tr}_{2^n/2}(ax) = 1$.

Concluding, we have $f'(x) = f'(x+z)$ if and only if $\mathrm{Tr}_{2^n/2}(ax) = 1$ and $z \in \{0, a^{-1}\beta, a^{-1}\beta^2, a^{-1}\beta^4\}$. Since there are $\frac{q}{2}$ elements x with $\mathrm{Tr}_{2^n/2}(ax) = 1$, we get $M_4(f) = \frac{q}{8}$. The map f' is injective on the hyperplane $\{x \in \mathbb{F}_{2^{3m}} \mid \mathrm{Tr}_{2^n/2}(ax) = 0\}$, yielding $M_1(f) = \frac{q}{2}$. □

The proof of Theorem 13 works almost identically for the second case too.

Theorem 14 *Let $n = 3m$ be odd and $a \in \mathbb{F}_q^*$ be arbitrary. Then the APN map*

$$f(x) = x^3 + a^{-1}\,\mathrm{Tr}_{2^n/2^3}(a^3x^9 + a^6x^{18})^2$$

satisfies $M_1(f) = \frac{q}{2}$, $M_4(f) = \frac{q}{8}$. In particular $|\mathrm{Im}(f)| = \frac{5}{8}q$.

6 Relations between the image sets of APN maps and their Walsh spectrum

Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. The Boolean fuctions $f_\lambda(x) = \mathrm{Tr}(\lambda f(x))$ for $\lambda \in \mathbb{F}_{2^n}^*$ are called the component functions of f. We call f_λ a balanced component of f, if it takes the values 0 and 1 equally often, that is both 2^{n-1} times. The Walsh transform of f is defined by

$$W_f(b,a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bf(x)+ax)} \in \mathbb{Z},$$

where $a, b \in \mathbb{F}_{2^n}, b \neq 0$. The multiset $\{*W_f(b,a)\colon b \in \mathbb{F}_{2^n}^*, a \in \mathbb{F}_{2^n}*\}$ is called the Walsh spectrum of f and $\{*|W_f(b,a)|\colon b \in \mathbb{F}_{2^n}^*, a \in \mathbb{F}_{2^n}*\}$ is called the extended Walsh spectrum of f.

Definition 1 Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, n even. We say that a map f has the classical Walsh spectrum if $|W_f(b,a)| \in \{0, 2^{n/2}, 2^{(n+2)/2}\}$ for $b \in \mathbb{F}_{2^n}^*, a \in \mathbb{F}_{2^n}$ and the extended Walsh spectrum of f contains $0, 2^{n/2}, 2^{(n+2)/2}$ precisely $(2^n-1)\cdot 2^{n-2}$-times, $(2/3)(2^n-1)(2^n)$-times and $(1/3)(2^n-1)(2^{n-2})$-times, respectively.

Most of the known APN maps in even dimension have the classical Walsh spectrum, for instance the monomial APN maps with Gold and Kasami exponents, but there are also APN maps with non-classical Walsh spectra, see e.g. [1] for such examples.

Definition 2 Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. We call a component function f_λ plateaued with amplitude t, if there exists an integer $t \geq 0$ such that $W_f(\lambda, a) \in \{0, \pm 2^{\frac{n+t}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$. If all component functions of f are plateaued, we call f component-wise plateaued. If n is odd and all components f_λ are plateaued with $t = 1$, we call f almost bent. A plateaued component with $t = 0$ is called a bent component.

Note that bent components can exist only for n even. It is well known that an almost bent function is necessarily APN, but not vice versa. Quadratic maps are always component-wise plateaued. Also a crooked map, which is defined by the property that all its differential sets are affine hyperplanes, is component-wise plateaued [23]. Properties of component functions of crooked maps are studied in [16]. Further examples of component-wise plateaued maps can be found in [9].

The next result gives a sufficient condition for an APN map.

Proposition 4 ([2, Corollary 3]) *Let n be even and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a component-wise plateaued map. If f has $(2/3)(2^n - 1)$ bent components and $(1/3)(2^n - 1)$ components with amplitude $t = 2$ then f is APN.*

Further, by Parseval's equation, a component-wise plateaued map f with $(2/3)(2^n - 1)$ bent components and $(1/3)(2^n - 1)$ plateaued components with amplitude $t = 2$ has always the classical Walsh spectrum.

Next we show that component-wise plateaued almost-3-to-1 maps are APN with the classical Walsh spectrum. This can be deduced also from results in [9] (see in particular, Corollary 10 and 11 and discussions preceding them). Our proof differs from the one in [9].

Theorem 15 *Let $n = 2m$ and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a component-wise plateaued, almost-3-to-1 map. Then f is an APN map with the classical Walsh spectrum. Moreover, if $f(0) = 0$ and $\omega(0) = 1$, i.e. 0 is the only element with precisely one preimage, then*

$$W_f(b, 0) \in \{(-1)^m 2^m, (-1)^{m+1} 2^{m+1}\}$$

for any $b \in \mathbb{F}_{2^n}^*$.

Proof Without loss of generality we may assume that $f(0) = 0$ and $\omega(0) = 1$. Indeed, otherwise we consider $f(x + c) + d$ with suitable $c, d \in \mathbb{F}_{2^n}$, which has the same extended Walsh spectrum as f:

$$\begin{aligned} W_{f(x+c)+d}(b, a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(b(f(x+c)+d)+ax)} \\ &= (-1)^{\mathrm{Tr}(bd)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bf(x)+a(x+c))} \\ &= (-1)^{\mathrm{Tr}(bd+ac)} W_f(b, a). \end{aligned}$$

Since f is component-wise plateaued, $W_f(b, 0)$ can only attain the values $\pm 2^{m+k}$ with $k \geq 0$ or 0 for $b \neq 0$. We first determine the possible signs of the Walsh transform.

Note that since f is almost-3-to-1 with $f(0) = 0$ and $\omega(0) = 1$, the value $|\{x \in \mathbb{F}_{2^n}^* \colon \mathrm{Tr}(bf(x)) = c\}|$ is divisible by 3 for any $c \in \mathbb{F}_2$ and any $b \in \mathbb{F}_{2^n}^*$. In particular,

$$W_f(b, 0) = |\{x \in \mathbb{F}_{2^n}^* \colon \mathrm{Tr}(bf(x)) = 0\}| - |\{x \in \mathbb{F}_{2^n}^* \colon \mathrm{Tr}(bf(x)) = 1\}| + 1$$

$$\equiv 1 \pmod 3.$$

We conclude that $W_f(b,0) \neq 0$ for any b. Further, if $W_f(b,0) = 2^{m+k}$ then $|\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(bf(x)) = 0\}| = 2^{n-1} + 2^{m+k-1} \equiv 1 \pmod 3$. Recall, that for a positive integer r, we have $2^r \equiv 1 \pmod 3$ if r is even and $2^r \equiv 2 \pmod 3$ if r is odd. Thus, since n is even, $2^{n-1} \equiv 2 \pmod 3$ and $2^{m+k-1} \equiv 2 \pmod 3$ if and only if $m+k$ is even. Thus $W_f(b,0) = 2^{m+k}$ necessarily implies that $m+k$ is even. Similarly, $W_f(b,0) = -2^{m+k}$ implies that $m+k$ must be odd. So for any $b \in \mathbb{F}_{2^n}^*$, we have $W_f(b,0) = (-1)^{m+k}2^{m+k}$ for some non-negative integer k.

Define $N_k = |\{b \in \mathbb{F}_{2^n}^* : |W_f(b,0)| = 2^{m+k}\}|$ for an integer $k \geq 0$.

Since $f(x) = 0$ holds only for $x = 0$, we have

$$\sum_{b \in \mathbb{F}_{2^n}} W_f(b,0) = 2^n,$$

which directly implies

$$\sum_{b \in \mathbb{F}_{2^n}^*} W_f(b,0) = 0.$$

Substituting the possible values for $W_f(b,0)$ in the above equation, we get

$$2^m(N_0 - 2N_1 + 4N_2 - 8N_3 + \dots) = 0,$$

implying

$$N_0 - 2N_1 + 4N_2 - 8N_3 + \cdots = 0. \tag{15}$$

Now since f is almost-3-to-1, $f(x)+f(x+a) = 0$ has for every nonzero x exactly 3 solutions as an equation in a, and for $x = 0$ only the solution $a = 0$. We thus have

$$\begin{aligned}\sum_{b \in \mathbb{F}_{2^n}} (W_f(b,0))^2 &= \sum_{b \in \mathbb{F}_{2^n}} \sum_{x \in \mathbb{F}_{2^n}} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(b(f(x)+f(x+a)))} \\ &= 2^n(3 \cdot (2^n - 1) + 1) = 3 \cdot 2^{2n} - 2^{n+1}.\end{aligned}$$

In particular,

$$\sum_{b \in \mathbb{F}_{2^n}^*} (W_f(b,0))^2 = 2^{2n+1} - 2^{n+1}.$$

Again, substituting the possible values for $W_f(b,0)$, we get

$$2^n(N_0 + 4N_1 + 16N_2 + 64N_3 + \dots) = 2^{2n+1} - 2^{n+1},$$

which immediately leads to

$$N_0 + 4N_1 + 16N_2 + 64N_3 + \cdots = 2^{n+1} - 2. \tag{16}$$

Clearly, we also have

$$N_0 + N_1 + N_2 + \cdots = 2^n - 1. \tag{17}$$

Adding Eq.s (15) and (16), we get

$$2N_0 + 2N_1 + 20N_2 + 56N_3 + \cdots = 2^{n+1} - 2. \tag{18}$$

Observe that all coefficients in Eq. (18) are positive. Now, subtracting Eq. (17) twice from Eq. (18) yields

$$18N_2 + 54N_3 + \cdots = 0.$$

Here, all coefficients are again positive, so we conclude $N_2 = N_3 = \cdots = 0$. From Eq. (15) and Eq. (17) we then immediately deduce that $N_0 = (2/3)(2^n - 1)$ and $N_1 = (1/3)(2^n - 1)$, so f is an APN map with the classical Walsh spectrum by Proposition 4. □

It is well known that quadratic (not necessarily APN) maps as well as crooked maps are component-wise plateaued. Hence Theorem 15 implies

Corollary 5 *Let $n = 2m$ and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.*

(a) If f is almost-3-to-1 crooked map, then f has the classical Walsh spectrum.
(b) If f is almost-3-to-1 quadratic map, then it is APN with the classical Walsh spectrum.

Note that Corollary 5 and Theorem 7 confirm Conjecture 1 stated in [26], that all APN maps of the form $f(x) = L_1(x^3) + L_2(x^9)$ in even dimension have the classical Walsh spectrum.

Remark 2 (i) Almost-3-to-1 APN maps with non-classical Walsh spectra exist; an example is the Dobbertin map $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ where $10|n$, $n = 5g$ and $d = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ [8].
(ii) Theorem 15 combined with Theorem 8 gives an alternative proof that the Zhou-Pott map in (11) is an APN map with the classical Walsh spectrum.

For almost bent maps, there is a direct connection between $N(f)$ and the number of balanced component functions as the following proposition implies.

Lemma 4 *Let f be an almost bent map. Set*

$$\begin{aligned} N_0 &= |\{b \in \mathbb{F}_{2^n}^* : W_f(b, 0) = 0\}| \\ N_+ &= |\{b \in \mathbb{F}_{2^n}^* : W_f(b, 0) = 2^{(n+1)/2}\}| \\ N_- &= |\{b \in \mathbb{F}_{2^n}^* : W_f(b, 0) = -2^{(n+1)/2}\}|. \end{aligned}$$

Then these three values are determined by $N(f)$ in the following way:

$$\begin{aligned} N_0 &= 2^n - 1 + 2^{n-1} - N(f)/2 \\ N_+ &= N(f)/4 - 2^{n-2} + 2^{(n-3)/2}(\omega(0) - 1) \\ N_- &= N(f)/4 - 2^{n-2} - 2^{(n-3)/2}(\omega(0) - 1). \end{aligned}$$

Proof Clearly, we have

$$N_0 + N_+ + N_- = 2^n - 1. \tag{19}$$

Further, we have

$$\begin{aligned} \sum_{b \in \mathbb{F}_{2^n}} (W_f(b, 0))^2 &= \sum_{b \in \mathbb{F}_{2^n}} \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(b(f(x)+f(y)))} \\ &= 2^n N(f), \end{aligned}$$

which implies

$$\sum_{b \in \mathbb{F}_{2^n}^*} (W_f(b,0))^2 = 2^n N(f) - 2^{2n}.$$

Rewriting this equation yields

$$2^{n+1}(N_+ + N_-) = 2^n N(f) - 2^{2n}$$

or, equivalently,

$$N_+ + N_- = N(f)/2 - 2^{n-1}. \tag{20}$$

Moreover, we have

$$\sum_{b \in \mathbb{F}_{2^n}} W_f(b,0) = 2^n \cdot \omega(0),$$

which directly implies

$$\sum_{b \in \mathbb{F}_{2^n}^*} W_f(b,0) = 2^n \cdot (\omega(0) - 1),$$

which yields

$$2^{(n+1)/2}(N_+ - N_-) = 2^n \cdot (\omega(0) - 1),$$

and

$$N_+ - N_- = 2^{(n-1)/2} \cdot (\omega(0) - 1). \tag{21}$$

Subtracting Eq. (20) from Eq. (19) yields

$$N_0 = 2^n + 2^{n-1} - N(f)/2 - 1.$$

Similarly adding Eq. (20) and Eq. (21) we get that $N(f)$ must be divisible by 4 and that

$$N_+ = N(f)/4 - 2^{n-2} + 2^{(n-3)/2}(\omega(0) - 1).$$

The value of N_- then follows immediately from Eq. (19). □

Lemma 4 directly implies

Corollary 6 *Let n be odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be almost bent. Then*

(a) $N(f)$ is divisible by 4.
(b) The number of balanced component functions of f is odd. In particular, every almost bent function has at least one balanced component function.
(c) $N(f) \leq 3 \cdot 2^n - 4$ and f is not zero-difference 2-balanced.

Proof Statement (a) holds since N_+ and N_- in Lemma 4 are integers. Then (b) is a direct consequence of (a) and Lemma 4. Using Corollary 1 and (a), we get that $N(f) \leq 3 \cdot 2^n - 4$ and hence f is not zero-difference 2-balanced. □

Remark 3 Recall that any crooked map is almost bent if n is odd. Property (c) in Corollary 6 implies that at least one differential set of a crooked map on $\mathbb{F}_{2^n}$ with n odd is a complement of a hyperplane. To the contrary there are bijective crooked maps, for which necessarily all differential sets are complements of hyperplanes. Interestingly, this property is the other way around if n is even. Then crooked maps, for which all differential sets are hyperplanes, do exist (for instance, $x \mapsto x^3$ as observed in [23]). But there are no crooked maps with all their differential sets being complements of hyperplanes. The latter is a consequence of the non-existence of bijective crooked maps in even dimension [23].

7 Upper bounds on the image sets of APN maps

In previous sections we used the value $N(f)$ to obtain a lower bound for the image size of some special maps. In [20], information on $N(f)$ was used to prove an *upper* bound on the image size of maps, significantly for planar maps. We recall their result.

Theorem 16 ([20, Theorem 2]) *Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a map. Then*

$$|\operatorname{Im}(f)| \le 2^n - \frac{2N(f) - 2^{n+1}}{1 + \sqrt{4N(f) - 2^{n+2} + 1}} = 2^n - \frac{1}{2}(\sqrt{4N(f) - 2^{n+2} + 1} - 1).$$

The equality

$$\frac{2N(f) - 2^{n+1}}{1 + \sqrt{4N(f) - 2^{n+2} + 1}} = \frac{1}{2}(\sqrt{4N(f) - 2^{n+2} + 1} - 1)$$

is not mentioned in [20], but it can be verified easily by expanding the fraction with $1 - \sqrt{4N(f) - 2^{n+2} + 1}$.

Using Lemma 4, we derive an upper bound for the image size of almost bent maps. Since almost bent maps, contrary to planar ones, can be permutations, our bound is a bit more involved.

Theorem 17 *Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an almost bent map. Set $k = \max\{\omega(a) | a \in \mathbb{F}_{2^n}\}$, i.e. there exists an element $c \in \mathbb{F}_{2^n}$ with k preimages under f and there is no element with more than k preimages. Then*

$$|\operatorname{Im}(f)| \le 2^n - \frac{k-1}{k} 2^{(n+1)/2}.$$

In particular, if f is not a permutation, then

$$|\operatorname{Im}(f)| \le 2^n - 2^{(n-1)/2}. \tag{22}$$

Proof By Eq.s (2) and (3)

$$N(f) - 2^n = \sum_{r=1}^{k} r(r-1)M_r \le k \sum_{r=1}^{k} (r-1)M_r,$$

implying

$$\sum_{r=1}^{k} (r-1)M_r \ge \frac{N(f) - 2^n}{k}. \tag{23}$$

Set $f'(x) = f(x) + c$ with $\omega(c) = k$. Clearly, f' is also almost bent and it satisfies $N(f) = N(f')$ and $|\operatorname{Im}(f)| = |\operatorname{Im}(f')|$, and additionally for f' we have $\omega(0) = k$. We apply Lemma 4 to f'. Then

$$0 \le N_- \le N(f)/4 - 2^{n-2} - (k-1)2^{(n-3)/2},$$

which leads to

$$N(f) - 2^n \ge (k-1)2^{(n+1)/2}.$$

Then, using Eq. (23),

$$|\operatorname{Im}(f)| = \sum_{r=1}^{k} M_r = \sum_{r=1}^{k} rM_r - \sum_{r=1}^{k}(r-1)M_r$$
$$= 2^n - \sum_{r=1}^{k}(r-1)M_r \leq 2^n - \frac{N(f)-2^n}{k} \leq 2^n - \frac{k-1}{k}2^{(n+1)/2}.$$

If f is not a permutation, then $k > 1$ and $\frac{k-1}{k} \geq 1/2$, completing the proof. □

Remark 4 From Theorem 17, it is clear that almost bent maps that satisfy the bound in (22) with equality must satisfy $\max\{\omega(a)|a \in \mathbb{F}_{2^n}\} = 2$. For such a map we then necessarily have $M_1(f) = 2^n - 2^{(n+1)/2}$ and $M_2(f) = 2^{(n-1)/2}$.

In even dimension, it is well known that maps with bent component functions cannot be permutations since bent functions are never balanced. Using Theorem 16, we present an upper bound on the image size of a map depending on the number of bent component functions. This also yields an upper bound for the image size of component-wise plateaued APN maps in even dimension since such maps have always many bent component functions.

Theorem 18 *Let n be even and $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a map with t bent component functions. Then $N(f) \geq t + 2^n$ and*

$$|\operatorname{Im}(f)| \leq 2^n - \frac{1}{2}(\sqrt{4t+1} - 1).$$

Proof We use again the relation

$$2^n N(f) = \sum_{b \in \mathbb{F}_{2^n}} W_f(b,0)^2 = 2^{2n} + \sum_{b \in \mathbb{F}_{2^n}^*} W_f(b,0)^2.$$

If $x \mapsto \operatorname{Tr}(bf(x))$ is bent, then $W_f(b,0)^2 = 2^n$, so

$$2^n N(f) \geq 2^{2n} + t \cdot 2^n,$$

implying $N(f) \geq t + 2^n$. The remaining follows from Theorem 16. □

Theorems 17 and 18 yield an upper bound on the image size for component-wise plateaued APN maps.

Theorem 19 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a component-wise plateaued APN map, and non-bijective if n is odd. Then*

$$|\operatorname{Im}(f)| \leq \begin{cases} 2^n - 2^{(n-1)/2} & n \text{ is odd,} \\ 2^n - \frac{1}{2}(\sqrt{\frac{8}{3}(2^n-1)+1} - 1) < 2^n - \sqrt{\frac{2}{3}(2^n-1)} + 1/2 & n \text{ is even.} \end{cases}$$

Proof The statement for n odd follows from Theorems 17, since every component-wise plateaued APN map is almost bent. The upper bound for n even is a direct consequence from Theorem 18 and the fact that a component-wise plateaued APN map has at least $(2/3)(2^n - 1)$ bent component functions [2, Corollary 3]. □

References

1. C. Beierle and G. Leander. New instances of quadratic APN functions. 2020, accessed November 2020.
2. T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.
3. J. Bierbrauer and G. M. Kyureghyan. Crooked binomials. *Designs, Codes and Cryptography*, 46(3):269–301, 2008.
4. C. Blondeau and K. Nyberg. Perfect nonlinear functions and cryptography. *Finite Fields and Their Applications*, 32:120 – 147, 2015.
5. L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa. Constructing APN functions through isotopic shifts. *Cryptology ePrint Archive,* Report 2018/769, accessed November 2020.
6. L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.
7. L. Budaghyan, C. Carlet, and G. Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378. IEEE, 2009.
8. A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1):105–138, 2000.
9. C. Carlet. Boolean and vectorial plateaued functions and APN functions. *IEEE Transactions on Information Theory*, 61(11):6272–6289, 2015.
10. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.
11. C. Carlet, Cunsheng Ding, and Jin Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.
12. C. Carlet and C. Ding. Nonlinearities of S-boxes. *Finite Fields and Their Applications*, 13(1):121 – 135, 2007.
13. C. Carlet, G. Gong, and Y. Tan. Quadratic zero-difference balanced functions,APN functions and strongly regular graphs. *Designs, Codes and Cryptography*, 78(3):629–654, 2016.
14. C. Carlet, A. Heuser and S. Picek. Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience. *Proceedings of ACNS 2017*, Lecture Notes in Computer Science 10355, 393-414, 2017.
15. C. Carlet. Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions. *Cryptology ePrint Archive*, Report 2020/1529, accessed Januar 2021.
16. P. Charpin. Crooked functions. In *Finite Fields and Their Applications*, ed. J.Davis, 87–102, 2020.
17. P. Charpin and G. Kyureghyan. When does $g(x) + tr(h(x))$ permute $\mathbb{F}_{p^n}$. *Finite Fields and Their Applications*, 15(5):615–632, 2009.
18. P. Charpin and G. M. Kyureghyan. On a class of permutation polynomials over $\mathbb{F}_{2^n}$. In *International Conference on Sequences and Their Applications - SETA 2008*, Lecture Notes in Comput. Sci. 5203, Springer, 368–376, 2008.
19. R. S. Coulter and R. W. Matthews. On the number of distinct values of a class of functions over a finite field. *Finite Fields and Their Applications*, 17(3):220–224, 2011.
20. R. S. Coulter and S. Senger. On the number of distinct values of a class of functions with finite domain. *Annals of Combinatorics*, 18(2):233–243, 2014.
21. I. Czerwinski. On the minimal value set size of APN functions. *Cryptology ePrint Archive,* Report 2020/705, accessed August 2020.
22. C. Ding and Y. Jin. A family of skew Hadamard difference sets. *J.Comb.Theory A*, 113(7):1526–1535, 2006.
23. G. M. Kyureghyan. Crooked maps in $\mathbb{F}_{2^n}$. *Finite Fields and Their Applications*, 13(3):713 – 726, 2007.
24. G. M. Kyureghyan and A. Pott. Some theorems on planar mappings. In *International Workshop on the Arithmetic of Finite Fields*, Lecture Notes in Comput. Sci., 5130, 117–122, 2008.
25. A. Pott. Almost perfect and planar functions. *Designs, Codes and Cryptography*, 78(1):141–195, 2016.

26. I. Villa. On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2. *Cryptography and Communications*, 11(1):3–20, 2019.
27. G. Weng, W. Qiu, Z. Wang, and Q. Xiang. Pseudo-paley graphs and skew Hadamard difference sets from presemifields. *Designs, Codes and Cryptography*, 44(1-3):49–62, 2007.
28. G. Weng and X. Zeng. Further results on planar DO functions and commutative semifields. *Designs, Codes and Cryptography*, 63(3):413–423, 2012.
29. Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.