HOKKAIDO UNIVERSITY

Title	A generalization of APN functions for odd characteristic
Author(s)	Kuroda, Masamichi; Tsujie, Shuhei
Citation	Finite fields and their applications, 47, 64-84 https://doi.org/10.1016/j.ffa.2017.05.001
Issue Date	2017-09
Doc URL	https://hdl.handle.net/2115/74584
Rights	© 2017. This manuscript version is made available under the CC-BY-NC-ND 4.0 license http://creativecommons.org/licenses/by-nc-nd/4.0/
Rights(URL)	https://creativecommons.org/licenses/by-nc-nd/4.0/
Type	journal article
File Information	GAPN.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

A Generalization of APN Functions for Odd Characteristic

Masamichi Kuroda, Shuhei Tsujie

Almost perfect nonlinear (APN) functions on finite fields of characteristic two have been studied by many researchers. Such functions have useful properties and applications in cryptography, finite geometries and so on. However, APN functions on finite fields of odd characteristic do not satisfy desired properties. In this paper, we modify the definition of APN function in the case of odd characteristic, and study its properties.

Keywords: APN function, Gold function, EA-equivalent, algebraic degree, dual arc, finite field
2010 MSC: 94A60, 05B25

1 Introduction

Let $F = \mathbb{F}_{p^n}$ be a finite field of characteristic p. A function $f\colon F \to F$ is called **almost perfect nonlinear** (APN) if the equation

$$D_a f(x) \coloneqq f(x+a) - f(x) = b$$

has at most two solutions x in F for all $a \in F^\times$ and $b \in F$. APN functions on a finite field of characteristic 2 were introduced by Nyberg [10] and have been studied by many researchers. There are a lot of applications in cryptography and finite geometry. APN functions for odd characteristic have been investigated by [6, 8] but their algebraic properties are quite different from the case of characteristic 2. In this paper, we give an algebraic generalization of APN functions as follows:

Definition 1.1. A function $f\colon F \to F$ is a **generalized almost perfect nonlinear** (GAPN) function if the equation

$$\tilde{D}_a f(x) \coloneqq \sum_{i \in \mathbb{F}_p} f(x+ia) = b$$

has at most p solutions x in F for all $a \in F^\times$ and $b \in F$.

Note that when $p = 2$ GAPN functions coincide with APN functions. For every $a, b \in F$, let

$$\tilde{N}_f(a,b) \coloneqq \#\left\{ x \in F \;\middle|\; \tilde{D}_a f(x) = b \right\}.$$

If the equation $\tilde{D}_a f(x) = b$ has a solution $x_0 \in F$, then it has at least p solutions contained in $x_0 + \mathbb{F}_p a$. Hence $\tilde{N}_f(a,b)$ is divisible by p, that is,

$$\tilde{N}_f(a,b) \in \{\, 0,\ p,\ 2p, \ldots, (p^n-1)p,\ p^n \,\}.$$

In particular, we have that f is a GAPN function if and only if

$$\tilde{N}_f(a,b) \in \{\, 0, p \,\} \quad \text{for any } a \in F^\times \text{ and } b \in F.$$

The value $\tilde{N}_f(a,b)$ measures the linearity of f in the following sense. Let $x_0 \in F$ be a solution of the equation $\tilde{D}_a f(x) = b$. Suppose that there exists $y_0 \in F \setminus \mathbb{F}_p a$ such that $f(y_0) + f(x_0 + ia) = f(y_0 + x_0 + ia)$ for every $i \in \mathbb{F}_p$. Then we have

$$\sum_{i \in \mathbb{F}_p} f(y_0 + x_0 + ia) = \sum_{i \in \mathbb{F}_p} f(x_0 + ia) = b,$$

that is, every element in $y_0 + x_0 + \mathbb{F}_p a$ is a solution of $\tilde{D}_a f(x) = b$. Hence $\tilde{N}_f(a,b) \geq 2p$. If we assume, as an extreme case, that f is linear, then for any $a \in F$ we have $\tilde{D}_a f(x) = \sum_{i \in \mathbb{F}_p} if(a)$, and hence

$$\tilde{N}_f(a,b) = \begin{cases} p^n & \text{if } b = \displaystyle\sum_{i \in \mathbb{F}_p} if(a), \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we may say that GAPN functions are the farthest from linear functions in view of this parameter $\tilde{N}_f(a,b)$.

Our main results are the following two theorems (see Section 3 and Section 4 for details). Firstly, we construct a generalization of the Gold functions, which are the most typical APN functions [7, 10]:

Theorem 1.2. *A monomial function $f : F \to F$ defined by*

$$f(x) = x^{p^i+p-1} \quad (i > 0 \text{ and } \gcd(i,n) = 1).$$

is a GAPN function of algebraic degree p.

Secondly, when $p = 3$, we obtain a partial generalization of a relation between APN functions and AB functions introduced in [5]:

Theorem 1.3. *Suppose that $p = 3$. Let f be a function of algebraic degree at most 3 with the condition $f(-x) = -f(x)$ for any $x \in \mathbb{F}_{3^n}$. If f is a generalized almost bent function, then f is a GAPN function. Here generalized almost bent functions are defined in Section 4.*

This paper is organized as follows. In Section 2, we give several characterizations for GAPN functions, which are generalizations of classical results for APN functions on $\mathbb{F}_{2^n}$. In Section 3, we raise two examples of GAPN functions. One is the inverse permutation and the other is a generalization of the Gold functions. In Section 4, we define a generalization of almost bent functions and prove Theorem 1.3. In Section 5, we introduce dual arcs and derive them from GAPN functions of algebraic degree p.

2 Characterizations of GAPN functions

2.1 The property of stability of GAPN functions

Two functions f and g are called **extended affine equivalent** (EA-equivalent) if $g = A_1 \circ f \circ A_2 + A_0$, where A_1 and A_2 are affine permutations and A_0 is an affine function. In [4], Carlet, Charpin and Zinoviev showed that EA-equivalence is a particular case of CCZ-equivalence. Here CCZ-equivalence corresponds to the affine equivalence of the graphs of functions, that is, functions f and g are CCZ-equivalent if and only if, for some affine permutation, the image of the graph of f is the graph of g.

Let

$$\mathcal{N}_f \coloneqq \left\{ \tilde{N}_f(a,b) \;\middle|\; a \in F^\times, b \in F \right\}.$$

When $p = 2$, Nyberg proved that EA-equivalence preserves the set $\mathcal{N}_f$ (see [10, Proposition 1]), and more generally, Budaghyan, Carlet and Pott proved that CCZ-equivalence also preserves the set $\mathcal{N}_f$ (see [3, Proposition 2]). The following proposition is a generalization of [10, Proposition 1].

Proposition 2.1. *Let f, $g\colon F \to F$ be EA-equivalent functions. Then $\mathcal{N}_f = \mathcal{N}_g$. In particular, f is a GAPN function if and only if g is a GAPN function.*

Proof. By definition, we have $g = A_1 \circ f \circ A_2 + A_0$ for some affine permutations A_1, A_2 and affine function A_0. For each $i \in \{0, 1, 2\}$, we may put $A_i = \alpha_i + c_i$, where α_i is a linear function on F and $c_i \in F$. Then α_1 and α_2 are bijective. We have

$$\sum_{i \in \mathbb{F}_p} A_0(x + ia) = \sum_{i \in \mathbb{F}_p} (\alpha_0(x + ia) + c_0) = \alpha_0(a) \sum_{i \in \mathbb{F}_p} i = \alpha_0(a) r$$

for any $a \in F^\times$, where r denotes $\sum_{i \in \mathbb{F}_p} i$. Then we obtain

$$\begin{aligned}\tilde{D}_a g(x) &= \sum_{i \in \mathbb{F}_p} (A_1 \circ f \circ A_2 + A_0)(x + ia) = \sum_{i \in \mathbb{F}_p} (\alpha_1 (f(\alpha_2(x + ia) + c_2)) + c_1) + \alpha_0(a) r \\ &= \alpha_1 \left(\sum_{i \in \mathbb{F}_p} f(A_2(x) + i\alpha_2(a)) \right) + \alpha_0(a) r = \alpha_1 \left(\tilde{D}_{\alpha_2(a)} f(A_2(x)) \right) + \alpha_0(a) r.\end{aligned}$$

Hence for any $a \in F^\times$ and $b \in F$, $\tilde{D}_a g(x) = b$ if and only if $\tilde{D}_{\alpha_2(a)} f(A_2(x)) = \alpha_1^{-1}(b - \alpha_0(a) r)$. Since A_2 is a permutation, we obtain $\tilde{N}_g(a,b) = \tilde{N}_f(\alpha_2(a), \alpha_1^{-1}(b - \alpha_0(a) r))$ for any $a \in F^\times$ and $b \in F$. Thus $\mathcal{N}_f = \mathcal{N}_g$. □

Remark 2.2. Proposition 2.1 is not correct for CCZ-equivalence. Every permutation is CCZ-equivalent to its inverse (see [4]), and hence when $p = 2$, the inverse of APN permutation is also an APN permutation. This property is not, however, extended for GAPN functions. For example, the function $f\colon \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$ defined by $f(x) = x^{57}$, which is the composition of $f_1(x) = x^{19}$ and the Frobenius mapping $\mathrm{Fb}(x) = x^3$, is a GAPN function, since Fb is linear and f_1 is a GAPN function by Lemma 3.3. However, we can check easily that the inverse function $f^{-1}(x) = x^{17}$ is not a GAPN function (see Remark 4.4 (1) for details).

2.2 GAPN functions of algebraic degree p

For a positive integer r, let $\mathrm{Map}(F^r, F)$ denote the set of functions from F^r to F. This set equipped with pointwise operations becomes an F-algebra. It is well known that the evaluation map from the polynomial ring $F[t_1, \ldots, t_r]$ to $\mathrm{Map}(F^r, F)$ induces the isomorphism $F[t_1, \ldots, t_r]/(t_1^{p^n} - t_1, \ldots, t_r^{p^n} - t_r) \simeq \mathrm{Map}(F^r, F)$. Hence the set of monomial functions $\left\{ x_1^{d_1} \cdots x_r^{d_r} \;\middle|\; 0 \le d_i \le p^n - 1, 1 \le i \le r \right\}$ is a basis for $\mathrm{Map}(F^r, F)$ over F. In particular, every function $f\colon F \to F$ can be represented uniquely as a polynomial function $f(x) = \sum_{d=0}^{p^n-1} c_d x^d$. Then every exponent d has the p-adic expansion $d = \sum_{s=0}^{n-1} d_s p^s$, where $0 \le d_s < p$. Let $w_p(d)$ denote the sum of the coefficients $\sum_{s=0}^{n-1} d_s$, and we call it the **p-weight** of d.

Definition 2.3. Let $f = \sum_{d=0}^{p^n-1} c_d x_d$ be a non-zero function on F. The non-negative integer $\max\{ w_p(d) \mid 0 \le d \le p^n - 1, c_d \neq 0 \}$ is called the **algebraic degree** of f, denoted by $d^\circ(f)$. A function of algebraic degree 2 is called **quadratic**.

We characterize the algebraic degree as follows (see Proposition 2.5). The symmetric group $\mathfrak{S}_r$ of degree r acts on $\mathrm{Map}(F^r, F)$ by $f^\sigma(x_1, \ldots, x_r) \coloneqq f(x_{\sigma(1)}, \ldots, x_{\sigma(r)})$, where $\sigma \in \mathfrak{S}_r$. Let $\mathrm{Map}(F^r, F)^{\mathfrak{S}_r}$ denote the set of invariant functions, which forms an F-subalgebra of $\mathrm{Map}(F^r, F)$. For a non-increasing sequence $\lambda = (\lambda_1, \ldots, \lambda_r)$ of non-negative integers, we define the **monomial symmetric polynomial** $m_\lambda(x_1, \ldots, x_r) \in \mathrm{Map}(F^r, F)^{\mathfrak{S}_r}$ by

$$m_\lambda(x_1, \ldots, x_r) \coloneqq \sum_\alpha x_1^{\alpha_1} \cdots x_r^{\alpha_r},$$

where $\alpha = (\alpha_1, \ldots, \alpha_r)$ runs over the distinct rearrangements of λ. It is easy to show that the set

$$\left\{ m_\lambda(x_1, \ldots, x_r) \;\middle|\; \begin{array}{l} \lambda = (\lambda_1, \ldots, \lambda_r) \text{ is a non-increasing sequence} \\ \text{of integers with } 0 \le \lambda_i \le p^n - 1 \text{ for } 1 \le i \le r \end{array} \right\} \tag{1}$$

is a basis for $\mathrm{Map}(F^r, F)^{\mathfrak{S}_r}$ over F.

For a function $f\colon F \to F$, we define a function $[f]^r \in \mathrm{Map}(F^r, F)^{\mathfrak{S}_r}$ by

$$[f]^r(x_1, \ldots, x_r) \coloneqq \sum_{I \subset [r]} (-1)^{r-|I|} f\left(\sum_{i \in I} x_i \right),$$

where $[r]$ denotes the set $\{1,\dots,r\}$. We also define $[f]^0 \coloneqq f(0)$. For example

$$[f]^1(x) = f(x) - f(0), \quad [f]^2(x,y) = f(x+y) - f(x) - f(y) + f(0),$$
$$[f]^3(x,y,z) = f(x+y+z) - f(x+y) - f(x+z) - f(y+z) + f(x) + f(y) + f(z) - f(0).$$

Proposition 2.4. *Let d be a positive integer with the p-adic expansion $d = \sum_{s=0}^{n-1} d_s p^s$. Then, for any integer $r \geq w_p(d)$, we have*

$$\left[x^d\right]^r = \begin{cases} 0 & \text{if } r > w_p(d), \\ \gamma(d)\, m_{\lambda(d)}(x_1,\dots,x_r) & \text{if } r = w_p(d), \end{cases}$$

where $\gamma(d) \coloneqq \prod_{s=0}^{n-1} d_s!$ *and* $\lambda(d) \coloneqq (\underbrace{p^{n-1},\dots,p^{n-1}}_{d_{n-1}}, \underbrace{p^{n-2},\dots,p^{n-2}}_{d_{n-2}}, \dots, \underbrace{1,\dots,1}_{d_0})$.

Moreover, $\left[x^d\right]^{w_p(d)} \neq 0$.

Proof. Put $w \coloneqq w_p(d)$ and write $d = p^{s_1} + \cdots + p^{s_w}$, where $\lambda(d) = (p^{s_1},\dots,p^{s_w})$. For any subset $I \subset [m]$, we have

$$\left(\sum_{i\in I} x_i\right)^d = \left(\sum_{i\in I} x_i\right)^{p^{s_1}+\cdots+p^{s_w}} = \prod_{j=1}^{w}\left(\sum_{i\in I} x_i^{p^{s_j}}\right) = \sum_{i_1,\dots,i_w\in I} x_{i_1}^{p^{s_1}} \cdots x_{i_w}^{p^{s_w}}.$$

Hence we obtain

$$\begin{aligned}\left[x^d\right]^r &= \sum_{I\subset[r]} (-1)^{r-|I|}\left(\sum_{i\in I} x_i\right)^d = \sum_{I\subset[r]} (-1)^{r-|I|}\left(\sum_{i_1,\dots,i_w\in I} x_{i_1}^{p^{s_1}} \cdots x_{i_w}^{p^{s_w}}\right) \\ &= \sum_{i_1,\dots,i_w\in[r]} \left(\sum_{\{i_1,\dots,i_w\}\subset I\subset[r]} (-1)^{r-|I|}\right) x_{i_1}^{p^{s_1}} \cdots x_{i_w}^{p^{s_w}}.\end{aligned}$$

Let $\ell \coloneqq \#\{i_1,\dots,i_w\}$. For any $j \in \{0,\dots,r-\ell\}$, we have

$$\#\{\, I \subset [r] \mid \{i_1,\dots,i_w\} \subset I \ \text{ and } \ |I| = \ell + j \,\} = \binom{r-\ell}{j},$$

where $\binom{r-\ell}{j}$ denotes the binomial coefficients. Thus we obtain

$$\sum_{\{i_1,\dots,i_w\}\subset I\subset[r]} (-1)^{r-|I|} = \sum_{j=0}^{r-\ell} (-1)^{(r-\ell)-j}\binom{r-\ell}{j} = \begin{cases} 0 & (\ell < r), \\ 1 & (\ell = r). \end{cases}$$

Therefore

$$\left[x^d\right]^r = \sum_{\substack{i_1,\dots,i_w\in[r] \\ \#\{i_1,\dots,i_w\}=r}} x_{i_1}^{p^{s_1}} \cdots x_{i_w}^{p^{s_w}}.$$

Hence we have that $\left[x^d\right]^r = 0$ if $r > w$. When $r = w$,

$$\left[x^d\right]^r = \sum_{\beta} x_1^{\beta_1} \cdots x_r^{\beta_r},$$

where $\beta = (\beta_1, \ldots, \beta_r)$ runs over the rearrangements of $\lambda(d) = (p^{s_1}, \ldots, p^{s_r})$. For a fixed rearrangement α of $\lambda(d)$, the number of rearrangements of $\lambda(d)$ which equal α coincides with $\gamma(d)$. Therefore $\left[x^d\right]^r$ is equal to $\gamma(d)\, m_{\lambda(d)}(x_1, \ldots, x_r)$. Since $0 \leq d_i \leq p-1$ for each i, we have $\gamma(d) \neq 0$, and hence $\left[x^d\right]^w = \left[x^d\right]^r \neq 0$. □

Proposition 2.5. *Let $f\colon F \to F$ be a non-zero function. The maximum integer r_0 such that $[f]^{r_0} \neq 0$ coincides with the algebraic degree $d^\circ(f)$.*

Proof. From Proposition 2.4, if $r > d^\circ(f)$, then $[f]^r = 0$. Hence we have $r_0 \leq d^\circ(f)$. We prove the converse inequality. We can write $f(x) = \sum_{d=0}^{p^n-1} c_d x^d$. By Proposition 2.4,

$$[f]^{d^\circ(f)} = \sum_{\substack{w_p(d)=d^\circ(f) \\ c_d \neq 0}} c_d \gamma(d)\, m_{\lambda(d)}.$$

If $d \neq d'$ then $\lambda(d) \neq \lambda(d')$, and hence $m_{\lambda(d)} \neq m_{\lambda(d')}$. Since $c_d\gamma(d) \neq 0$ for each d, and the basis (1) is linearly independent over F, we obtain $[f]^{d^\circ(f)} \neq 0$, and hence $d^\circ(f) \leq r_0$. Therefore we have $r_0 = d^\circ(f)$. □

One can easily verify the following recurrence formula:

Proposition 2.6. *Let r be a positive integer. Then*

$$\begin{aligned} &[f]^{r+1}(x, y, z_1, \ldots, z_{r-1}) \\ &= [f]^r(x+y, z_1, \ldots, z_{r-1}) - [f]^r(x, z_1, \ldots, z_{r-1}) - [f]^r(y, z_1, \ldots, z_{r-1}) \end{aligned}$$

for any $x, y, z_1, \ldots, z_{r-1} \in F$.

Proposition 2.7. *Let $f\colon F \to F$ be a non-zero function and let r be a positive integer.*

(1) $d^\circ(f) = 0$ if and only if f is a non-zero constant function.

(2) $d^\circ(f) = r$ if and only if $[f]^r$ is a non-zero $\mathbb{F}_p$-multilinear form. In particular, $d^\circ(f) \leq r$ if and only if $[f]^r$ is an $\mathbb{F}_p$-multilinear form.

Proof. Clear from Proposition 2.5 and Proposition 2.6. □

EA-equivalence preserves algebraic degrees of functions, that is, we have the following proposition.

Proposition 2.8. *Let $f,\ g\colon F \to F$ be EA-equivalent functions, and let $d^\circ(f) \geq 2$. Then $d^\circ(g) = d^\circ(f)$.*

Proof. By definition, we have $g = A_1 \circ f \circ A_2 + A_0$ for some affine functions A_0, A_1 and A_2, where A_1 and A_2 are permutations. For each $i \in \{ 0, 1, 2 \}$, we may put $A_i = \alpha_i + c_i$, where α_i is a linear function on F and $c_i \in F$. Then α_1 and α_2 are bijective. For any integer $r \geq 2$, we have

$$[A_0]^r(x_1, \ldots, x_r) = \alpha_0 \left(\sum_{I \subset [r]} (-1)^{r-|I|} \sum_{i \in I} x_i \right) + c_0 \sum_{I \subset [r]} (-1)^{r-|I|} = 0.$$

Hence we obtain

$$\begin{aligned}[g]^r(x_1, \ldots, x_r) &= [A_1 \circ f \circ A_2 + A_0]^r(x_1, \ldots, x_r) = [A_1 \circ f \circ A_2]^r(x_1, \ldots, x_r) \\ &= \alpha_1([f]^{r+1}(\alpha_2(x_1), \ldots, \alpha_2(x_r), c_2) + [f]^r(\alpha_2(x_1), \ldots, \alpha_2(x_r))).\end{aligned}$$

By Proposition 2.6, if $[f]^r = 0$ then $[f]^{r+1} = 0$, and hence $[g]^r = 0$, since α_1 is linear. Therefore by Proposition 2.5, $d^\circ(g) = \max \{ r \mid [g]^r \neq 0 \} \leq \max \{ r \mid [f]^r \neq 0 \} = d^\circ(f)$. The converse inequality is given by similar arguments. □

For a function $f \colon F \to F$ we define $\tilde{B}_f(x, y) \coloneqq [f]^p(x, y, \ldots, y)$. Note that if $d^\circ(f) \leq p$ then $\tilde{B}_f(x, y)$ is linear in x by Proposition 2.7 and when $p = 2$ a function f is quadratic if and only if $\tilde{B}_f(x, y) = f(x + y) + f(x) + f(y) + f(0)$ is a non-zero bilinear form.

Proposition 2.9. *$\tilde{B}_f(x, a) = \tilde{D}_a f(x) - \tilde{D}_a f(0)$ for any x, $a \in F$ (see Definition 1.1).*

Proof. Let $(x_1, \ldots, x_p) = (x, a, \ldots, a)$. Since for each $I \subset [p]$,

$$\sum_{i \in I} x_i = \begin{cases} x + (|I| - 1)\, a & (1 \in I), \\ |I| a & (1 \notin I), \end{cases}$$

we have that

$$\begin{aligned}\tilde{B}_f(x, a) = [f]^p(x, a, \ldots, a) &= \sum_{I \subset [p]} (-1)^{p-|I|} f \left(\sum_{i \in I} x_i \right) \\ &= \sum_{\substack{I = J \cup \{1\} \\ J \subset \{2, \ldots, p\}}} (-1)^{p-|I|} f\left(x + (|I| - 1)\, a\right) + \sum_{J \subset \{2, \ldots, p\}} (-1)^{p-|J|} f\left(|J| a\right).\end{aligned}$$

Then $0 \leq |J| \leq p - 1$ and we have

$$\# \{ J \subset \{2, \ldots, p\} \mid |J| = j \} = \binom{p-1}{j} \equiv (-1)^j \pmod{p}.$$

Therefore we obtain

$$\tilde{B}_f(x, a) = \sum_{j=0}^{p-1} (-1)^{p-1-j} \binom{p-1}{j} \left(f(x + ja) - f(ja)\right) = \tilde{D}_a f(x) - \tilde{D}_a f(0).$$

□

Proposition 2.10. *Suppose that $d^\circ(f) \leq p$. Then*

$$\tilde{D}_a f(x \pm y) = \tilde{D}_a f(x) \pm \tilde{D}_a f(y) \mp \tilde{D}_a f(0).$$

In particular, if $\tilde{D}_a f(0) = 0$, then the mapping $\tilde{D}_a f$ is linear over $\mathbb{F}_p$.

Proof. By Proposition 2.7 (2), $\tilde{B}_f(x, a) = [f]^p(x, a, \ldots, a)$ is linear in x, since $d^\circ(f) \leq p$. Therefore by Proposition 2.9, we have

$$\begin{aligned}\tilde{D}_a f(x \pm y) &= \tilde{B}_f(x \pm y, a) + \tilde{D}_a f(0) = \tilde{B}_f(x, a) \pm \tilde{B}_f(y, a) + \tilde{D}_a f(0) \\ &= \left(\tilde{D}_a f(x) - \tilde{D}_a f(0)\right) \pm \left(\tilde{D}_a f(y) - \tilde{D}_a f(0)\right) + \tilde{D}_a f(0) \\ &= \tilde{D}_a f(x) \pm \tilde{D}_a f(y) \mp \tilde{D}_a f(0).\end{aligned}$$

□

We have two characterizations as follows for GAPN functions of algebraic degree at most p. These are generalizations of classical results for quadratic APN functions.

Proposition 2.11. *Suppose that $d^\circ(f) \leq p$. Then $\tilde{N}_f(a, b)$ equals zero or $\tilde{N}_f(a, \tilde{D}_a f(0))$ for any $a \in F^\times$ and $b \in F$. In particular, f is a GAPN function if and only if $\tilde{N}_f(a, \tilde{D}_a f(0)) \leq p$ for any $a \in F^\times$.*

Proof. If $\tilde{D}_a f(x) = b$ has no solutions in F, then $\tilde{N}_f(a, b) = 0$. Assume that $x_0 \in F$ is a solution of $\tilde{D}_a f(x) = b$. By Proposition 2.10

$$\tilde{D}_a f(x) - b = \tilde{D}_a f(x) - \tilde{D}_a f(x_0) = \tilde{D}_a f(x - x_0) - \tilde{D}_a f(0).$$

Hence $\tilde{D}_a f(x) = b$ if and only if $\tilde{D}_a f(x - x_0) = \tilde{D}_a f(0)$, and hence we have that $\tilde{N}_f(a, b) = \tilde{N}_f(a, \tilde{D}_a(0))$. □

Proposition 2.12. *(1) Suppose that $d^\circ(f) \leq p$. Then f is a GAPN function if and only if $\left\{ x \in F \;\middle|\; \tilde{B}_f(x, a) = 0 \right\} = \mathbb{F}_p a$ for any $a \in F^\times$.*

(2) If f is a GAPN function with $d^\circ(f) \leq p$, then $d^\circ(f) = p$. In particular, GAPN functions are algebraic degree at least p.

Proof. We first prove (1). By Proposition 2.11, f is a GAPN function if and only if $\tilde{N}_f(a, \tilde{D}_a f(0)) \leq p$ for any $a \in F^\times$. By Proposition 2.9, we have

$$\tilde{N}_f(a, \tilde{D}_a f(0)) = \# \left\{ x \in F \;\middle|\; \tilde{D}_a f(x) = \tilde{D}_a f(0) \right\} = \# \left\{ x \in F \;\middle|\; \tilde{B}_f(x, a) = 0 \right\}.$$

In addition, $0 = \tilde{B}_f(x, a) = [f]^p(x, a, \ldots, a)$ has trivial solutions $x \in \mathbb{F}_p a$. Therefore $\tilde{N}_f(a, \tilde{D}_a f(0)) \leq p$ if and only if $\left\{ x \in F \;\middle|\; \tilde{B}_f(x, a) = 0 \right\} = \mathbb{F}_p a$. Hence we obtain (1).

Next we prove (2). Let f be a GAPN function with $d^\circ(f) \leq p$. Suppose that $d^\circ(f) < p$. Then by Proposition 2.5, $[f]^p = 0$, and hence $\tilde{B}_f(x, a) = [f]^p(x, a, \ldots, a) = 0$ for any x and $a \in F$. By the assertion (1), this contradicts to that f is a GAPN function. Hence we obtain $d^\circ(f) = p$. □

2.3 Fourier-Walsh transform

For a function $f\colon F \to F$ and an element $b \in F$, we define

$$f_b\colon F \longrightarrow \mathbb{F}_p,\ x \longmapsto \mathrm{Tr}(bf(x)),$$

where Tr denotes the absolute trace on F. The functions f_b are called the **components** of f. For any function $g\colon F \to \mathbb{F}_p$, let $\mathcal{F}(g)$ denote the following value related to the Fourier-Walsh transform of g:

$$\mathcal{F}(g) \coloneqq \sum_{x\in F} \zeta_p^{g(x)},$$

where ζ_p is the primitive p-th root of unity. Note that $\mathcal{F}(f_b)$ $(b \in F)$ is the special case $\hat{f}(0,b)$ of the Fourier transform of f (see [9] for more details):

$$\hat{f}\,(a,b) \coloneqq \sum_{x\in F} \zeta_p^{\mathrm{Tr}(bf(x)-ax)} \quad (a,b \in F).$$

We have the following characterization for GAPN functions, which is a generalization of the characterization for APN functions introduced in [11].

Proposition 2.13. *Let $f\colon F \to F$ be a function. Then*

$$\sum_{a\in F, b\in F^\times} |\mathcal{F}(\tilde{D}_a f_b)|^2 \geq p^{2n+1}(p^n-1)$$

with equality if and only if f is a GAPN function.

Proof. We define $p^n \times p^n$ matrices X, T, N which are indexed by elements in $F \times F$. The (a,b)-components of these matrices are as follows:

$$X_{ab} \coloneqq \zeta_p^{\mathrm{Tr}(ab)},\ T_{ab} \coloneqq \mathcal{F}(\tilde{D}_a f_b),\ N_{ab} \coloneqq \tilde{N}_f(a,b).$$

Then we have $T = NX$ since

$$T_{ab} = \sum_{x\in F} \zeta_p^{\mathrm{Tr}(b\tilde{D}_a f(x))} = \sum_{y\in F} \tilde{N}_f(a,y)\zeta_p^{\mathrm{Tr}(yb)} = \sum_{y\in F} N_{ay}X_{yb}.$$

Moreover, we have $XX^* = p^n I$, where X^* denotes the adjoint matrix of X and I the identity matrix, since

$$\sum_{c\in F} X_{ac}\overline{X_{cb}} = \sum_{c\in F} \zeta_p^{\mathrm{Tr}((a-b)c)} = \begin{cases} p^n & (a=b), \\ 0 & (a\neq b). \end{cases}$$

Therefore we have

$$\sum_{a,b\in F} |T_{ab}|^2 = \mathrm{Tr}\,(TT^*) = \mathrm{Tr}\,(NXX^*N^*) = p^n\,\mathrm{Tr}\,(NN^*) = p^n \sum_{a,b\in F} \tilde{N}_f(a,b)^2.$$

On the other hand, we have $\tilde{N}_f(0,b)^2 = \begin{cases} p^{2n} & (b=0), \\ 0 & (b \neq 0), \end{cases}$ and if $a \neq 0$, then we have $\tilde{N}_f(a,b)^2 \geq p\tilde{N}_f(a,b)$. Hence we obtain

$$\begin{aligned}\sum_{a,b\in F} |T_{ab}|^2 &= p^n \left(\sum_{b\in F} \tilde{N}_f(0,b)^2 + \sum_{a\in F^\times, b\in F} \tilde{N}_f(a,b)^2 \right) \\ &= p^{3n} + p^n \sum_{a\in F^\times, b\in F} \tilde{N}_f(a,b)^2 \geq p^{3n} + p^{n+1} \sum_{a\in F^\times, b\in F} \tilde{N}_f(a,b).\end{aligned}$$

Moreover, we have $\sum_{b\in F} \tilde{N}_f(a,b) = \sum_{b\in F} \#\left((\tilde{D}_a f)^{-1}(b)\right) = p^n$, and hence we obtain $\sum_{a\in F^\times, b\in F} \tilde{N}_f(a,b) = (p^n-1)p^n$. We have $\sum_{a\in\mathbb{F}_{p^n}} T_{a0}^2 = \sum_{a\in\mathbb{F}_{p^n}} \left(\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(0\cdot D_a f(x))} \right)^2 = p^{3n}$ clearly. Thus we have

$$\sum_{a\in F, b\in F^\times} |\mathcal{F}(\tilde{D}_a f_b)|^2 = \sum_{a\in F, b\in F^\times} |T_{ab}|^2 \geq p^{2n+1}(p^n-1)$$

with equality if and only if $\tilde{N}_f(a,b)$ equals 0 or p for all $a \in F^\times$ and $b \in F$, that is, f is a GAPN function. □

3 Examples of GAPN functions

3.1 Inverse permutations

The inverse permutation f on F is defined by

$$f(x) := x^{p^n-2} = \begin{cases} x^{-1} & (x \neq 0), \\ 0 & (x = 0). \end{cases}$$

The following is well known:

Proposition 3.1 (Beth-Ding [2], Nyberg [10])**.** *Let f be the inverse permutation on $\mathbb{F}_{2^n}$. Then f is APN if and only if n is odd.*

This proposition is generalized as follows:

Proposition 3.2. *Let p be an odd prime. Then the inverse permutation on F is a GAPN function.*

Proof. For convenience let $0^{-1} := 0$. We consider an equation

$$\sum_{i\in\mathbb{F}_p} (x+ia)^{-1} = b,$$

where $a \in F^\times$ and $b \in F$. First suppose that there exists a solution $x \notin \mathbb{F}_p a$. Multiplying the equation by $\prod_{i\in\mathbb{F}_p}(x+ia)$ we have

$$b\prod_{i\in\mathbb{F}_p}(x+ia)+g(x)=0,$$

where $g(x)$ is a polynomial in x with degree at most $p-1$, and its constant term is $-(p-1)!\,a^{p-1} \neq 0$. Since every element in $x+\mathbb{F}_p a$ is a solution, we have $b \neq 0$ and the number of solutions outside $\mathbb{F}_p a$ is exactly p.

Next we suppose that $x \in \mathbb{F}_p a$ is a solution. Then we have

$$b=\sum_{i\in\mathbb{F}_p}(x+ia)^{-1}=\sum_{i\in\mathbb{F}_p}(ia)^{-1}=a^{-1}\sum_{i=1}^{p-1}i^{-1}=a^{-1}\sum_{i=1}^{p-1}i=0.$$

Hence it is impossible that the equation has a solution in $\mathbb{F}_p a$ and a solution outside $\mathbb{F}_p a$ simultaneously. Therefore $\tilde{N}_f(a,b) \leq p$ for any $a \in F^\times$ and $b \in F$, and hence the inverse permutation f is a GAPN function. □

3.2 Generalized Gold functions

When $p=2$ the most typical quadratic APN functions are the Gold functions [7, 10], which are defined by

$$f(x)=x^{2^i+1} \text{ with } \gcd(n,i)=1.$$

In this subsection, we construct a generalization of the Gold functions.

Lemma 3.3. *Let f be a monomial function defined by*

$$f(x)=x^{1+p^{i_2}+\cdots+p^{i_p}} \quad (i_2,\ldots,i_p \geq 0,\ (i_2,\ldots,i_p) \neq (0,\cdots,0)).$$

Then

(i) $d^\circ(f)=p$.

(ii) $\tilde{B}_f(x,a)=(p-1)\left(a^{d-1}x+a^{d-p^{i_2}}x^{p^{i_2}}+\cdots+a^{d-p^{i_p}}x^{p^{i_p}}\right)$ *for any* $a \in F^\times$, *where* $d=1+p^{i_2}+\cdots+p^{i_p}$.

(iii) Assume that $\left\{ x\in F \;\middle|\; x+x^{p^{i_2}}+\cdots+x^{p^{i_p}}=0 \right\}=\mathbb{F}_p$. *Then f is a GAPN function of algebraic degree p.*

Proof. By the definition of the algebraic degree, we have that $d^\circ(f)=w_p(d)=p$, and hence we obtain the statement (i). We prove the statement (ii). When $p=2$, we have

$$\begin{aligned}\tilde{B}_f(x,a)&=f(x+a)+f(x)+f(a)+f(0)=(x+a)(x^{2^{i_2}}+a^{2^{i_2}})+x^{1+2^{i_2}}+a^{1+2^{i_2}}\\&=ax^{2^{i_2}}+a^{2^{i_2}}x.\end{aligned}$$

When $p \geq 3$, let $i_1 = 0$. Then we have

$$\tilde{D}_a f(0) = \left(\sum_{j \in \mathbb{F}_p} j^{p^{i_1} + \cdots + p^{i_p}} \right) a^{p^{i_1} + \cdots + p^{i_p}} = \left(\sum_{j \in \mathbb{F}_p} j \right) a^{p^{i_1} + \cdots + p^{i_p}} = 0.$$

Hence we obtain

$$\begin{aligned}
\tilde{B}_f(x,a) = \tilde{D}_a f(x) - \tilde{D}_a f(0) = \tilde{D}_a f(x) &= \sum_{j \in \mathbb{F}_p} \left(\prod_{\ell=1}^{p} \left(x^{p^{i_\ell}} + (ja)^{p^{i_\ell}} \right) \right) \\
&= \sum_{j \in \mathbb{F}_p} \left(\prod_{\ell=1}^{p} \left(x^{p^{i_\ell}} + j a^{p^{i_\ell}} \right) \right) = \sum_{j \in \mathbb{F}_p} \left(\sum_{K \subset [p]} j^{|K|} a^{\sum_{k \in K} p^{i_k}} x^{\sum_{k \in [p] \setminus K} p^{i_k}} \right) \\
&= \sum_{K \subset [p]} \left(\sum_{j \in \mathbb{F}_p} j^{|K|} \right) a^{\sum_{k \in K} p^{i_k}} x^{\sum_{k \in [p] \setminus K} p^{i_k}}.
\end{aligned}$$

Since we have $\displaystyle\sum_{j \in \mathbb{F}_p} j^{|K|} = \begin{cases} 0 & (|K| \neq p-1), \\ p-1 & (|K| = p-1), \end{cases}$ we obtain the desired equation.

We prove the statement (iii). Since $a \neq 0$, by the assumption and (ii), we have

$$\left\{ x \in F \;\middle|\; \tilde{B}_f(x,a) = 0 \right\} = \left\{ ay \;\middle|\; y + y^{p^{i_2}} + \cdots + y^{p^{i_p}} = 0 \right\} = \mathbb{F}_p a.$$

Hence f is a GAPN function with $d^\circ(f) = p$ by Proposition 2.12. □

By Lemma 3.3, we obtain a generalization of the Gold functions:

Theorem 3.4. *Let $f : F \to F$ be a monomial function defined by*

$$f(x) = x^{p^i + p - 1} \quad (i > 0 \text{ and } \gcd(i,n) = 1).$$

Then f is a GAPN function of algebraic degree p. We call them the ***generalized Gold functions****.*

Proof. In Lemma 3.3, let $(i_2, i_3, \ldots, i_p) = (i, 0, \cdots, 0)$ with $i > 0$. Then by (iii) in Lemma 3.3, the monomial function $f(x) = x^{p^i + p - 1}$ is a GAPN function of algebraic degree p, if we have

$$\left\{ x \in F \;\middle|\; x^{p^i} = x \right\} = \mathbb{F}_p, \text{ that is, } \left\{ x \in F \;\middle|\; x^{p^i - 1} = 1 \right\} = \mathbb{F}_p^\times. \tag{2}$$

Since $\gcd(i,n) = 1$, it can be verified that $\gcd(p^i - 1, p^n - 1) = p - 1$. Therefore we have $\# \left\{ x \in F \;\middle|\; x^{p^i - 1} = 1 \right\} = \gcd(p^i - 1, p^n - 1) = p - 1$, and hence, we obtain (2). □

When $p = 2$, there are no quadratic APN functions on $\mathbb{F}_{2^n}$ of the form

$$f(x) = \sum_{i=1}^{n-1} c_i x^{2^i+1}, \quad c_i \in \mathbb{F}_{2^n}$$

except the Gold functions [1]. Unfortunately, this property is not generalized for GAPN functions. In fact, we have

Proposition 3.5. *Assume that p is an odd prime and n is odd. Then the function $f\colon F \to F$ defined by*

$$f(x) = x^{p^i+p-1} - x^{p^{n-i}+p-1} \quad (i > 0 \ \text{ and } \ \gcd(i, n) = 1)$$

is a GAPN function of algebraic degree p.

Proof. Clearly, $d^\circ(f) = p$, and $\tilde{D}_a f(0) = 0$ for any $a \in F^\times$. Thus by Proposition 2.11, all we have to do is to show that $\tilde{N}_f(a, 0) \leq p$ for any $a \in F^\times$. Let g_i be the generalized Gold function $g_i(x) = x^{p^i+p-1}$. Since $\tilde{D}_a f(0) = 0$, by Proposition 2.9, we have $\tilde{D}_a f(x) = \tilde{B}_f(x, a) = \tilde{B}_{g_i}(x, a) - \tilde{B}_{g_{n-i}}(x, a)$. Hence, by Lemma 3.3 (ii), we have

$$\begin{aligned}\tilde{D}_a f(x) = \tilde{B}_{g_i}(x, a) - \tilde{B}_{g_{n-i}}(x, a) &= \left(a^{p^i+p-2}x - a^{p-1}x^{p^i}\right) - \left(a^{p^{n-i}+p-2}x - a^{p-1}x^{p^{n-i}}\right) \\ &= a^{p-1}x\left(-x^{p^i-1} + x^{p^{n-i}-1} + a^{p^i-1} - a^{p^{n-i}-1}\right).\end{aligned}$$

Thus it is sufficient to show that the equation $-x^{p^i-1} + x^{p^{n-i}-1} + a^{p^i-1} - a^{p^{n-i}-1} = 0$ has only trivial $p - 1$ solutions a, $2a$, $\ldots$, $(p-1)a$ for any $a \in F^\times$. It follows immediately from Lemma 3.6. □

Lemma 3.6. *The mapping $\varphi\colon F^\times \to F$ defined by $\varphi(a) = a^{p^i-1} - a^{p^{n-i}-1}$ is $(p-1)$-to-1.*

Proof. We consider the composition of φ and the Frobenius automorphism $\mathrm{Fb}(x) = x^{p^i}$. Then we have

$$\mathrm{Fb} \circ \varphi(a) = \left(a^{p^i-1} - a^{p^{n-i}-1}\right)^{p^i} = \left(a^{p^i-1}\right)^{p^i} - \frac{1}{a^{p^i-1}} = \psi_2 \circ \psi_1(a),$$

where ψ_1 and ψ_2 are defined by

$$\psi_1\colon F^\times \longrightarrow F^\times, \quad a \longmapsto a^{p^i-1}, \quad \text{and} \quad \psi_2\colon F^\times \longrightarrow F, \quad \alpha \longmapsto \alpha^{p^i} - \frac{1}{\alpha}.$$

Since Fb is a bijection, it is sufficient to show the following two properties:

- $\psi_1\colon F^\times \to F^\times$ is a $(p-1)$-to-1 mapping.
- ψ_2 is injective on $\mathrm{Im}(\psi_1)$.

We show the first property. For any two elements a and $b \in F^\times$ such that $a^{p^i-1} = b^{p^i-1}$, we have $(a/b)^{p^i-1} = 1$. Since $\gcd(i, n) = 1$, we obtain that a/b is contained in $\mathbb{F}_p^\times$. Hence ψ_1 is a $(p-1)$-to-1 mapping. Next we show the second property. Since $\mathrm{Im}(\psi_1)$ is the subgroup of $F^\times$ whose cardinality equals $\frac{p^n-1}{p-1}$, we obtain $\mathrm{Im}(\psi_1) = \langle \gamma^{p-1} \rangle$, where γ is a generator of $F^\times$. Let $\gamma^{(p-1)m_1}$ and $\gamma^{(p-1)m_2}$ be two elements in $\mathrm{Im}(\psi_1)$ such that

$$\left(\gamma^{(p-1)m_1}\right)^{p^i} - \frac{1}{\gamma^{(p-1)m_1}} = \left(\gamma^{(p-1)m_2}\right)^{p^i} - \frac{1}{\gamma^{(p-1)m_2}},$$

$$\text{that is,} \quad \gamma^{(p-1)(m_1+m_2)} \left(\gamma^{(p-1)m_1} - \gamma^{(p-1)m_2}\right)^{p^i} = -\left(\gamma^{(p-1)m_1} - \gamma^{(p-1)m_2}\right).$$

Assume that $\gamma^{(p-1)m_1} \neq \gamma^{(p-1)m_2}$. Then $\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1}$ is odd, since n is odd. Hence we have

$$\begin{aligned}\left(\left(\gamma^{(p-1)m_1} - \gamma^{(p-1)m_2}\right)^{\frac{p^n-1}{p-1}}\right)^{p^i-1} &= \left(\gamma^{(p-1)(m_1+m_2)} \left(\gamma^{(p-1)m_1} - \gamma^{(p-1)m_2}\right)^{p^i-1}\right)^{\frac{p^n-1}{p-1}} \\ &= (-1)^{\frac{p^n-1}{p-1}} = -1.\end{aligned}$$

Since $\left(\gamma^{(p-1)m_1} - \gamma^{(p-1)m_2}\right)^{\frac{p^n-1}{p-1}}$ is a $(p-1)$-th root of unity and $p^i - 1$ is divisible by $p-1$, we obtain $1 = -1$, which is absurd when p is an odd prime. □

4 Relation to generalized almost bent functions

For a function $f\colon F \to F$, we define the p^n-**Walsh coefficients** of f as follows:

$$W_f(a, b) \coloneqq \mathcal{F}(\varphi_a + f_b) \quad (a \in F,\ b \in F^\times),$$

where φ_a is the components of the identity mapping on F. Similarly to the case that $p = 2$, we define generalized almost bent functions.

Definition 4.1. $f\colon F \to F$ is a **generalized almost bent** (GAB) function if

$$W_f(a, b) \in \left\{0,\ \pm p^{\frac{n+1}{2}}\right\} \quad \text{for all } a \in F \text{ and } b \in F^\times.$$

Note that when $p = 2$, GAB functions coincide with AB functions. We have the following characterization of GAB functions. It is a generalization of the characterization of AB functions introduced in [12].

Proposition 4.2. *Let $S_{a,b}^{(m)}$ be the number of solutions of the system of equations*

$$\begin{cases} x_1 + x_2 + \cdots + x_m = a, \\ f(x_1) + f(x_2) + \cdots + f(x_m) = b. \end{cases}$$

Then f is a GAB function if and only if

$$S_{a,b}^{(3)} = \begin{cases} p^n - p & (f(a) \neq b), \\ (p+1)p^n - p & (f(a) = b) \end{cases} \quad \textit{for any } a,\ b \in F.$$

Proof. We first define $p^n \times p^n$ matrices $W^{(m)}$, $S^{(m)}$, E and J which are indexed by elements in $F \times F$. The (a,b)-components of these matrices are as follows:

$$W^{(m)}_{a,b} := W_f(a,b)^m,\ S^{(m)}_{ab} := S^{(m)}_{a,b},\ E_{ab} := \begin{cases} 1 & (a,b) = (0,0), \\ 0 & \text{otherwise.} \end{cases},\ J_{ab} := 1.$$

By definition, f is a GAB function if and only if

$$W_f(a,b)^3 - p^{n+1} W_f(a,b) = 0 \quad (a \in F,\ b \in F^\times). \tag{3}$$

Since if $b = 0$, then $W_f(a,0) = \sum_{x \in F} \zeta_p^{\mathrm{Tr}(ax)} = \begin{cases} p^n & (a = 0), \\ 0 & (a \neq 0), \end{cases}$ the equation (3) is equivalent to

$$W^{(3)} - p^{n+1} W^{(1)} = \left(p^{3n} - p^{2n+1}\right) E. \tag{4}$$

For any $m \in \mathbb{N}$, we have

$$\begin{aligned} W_f(a,b)^m &= \left(\sum_{x \in F} \zeta_p^{\mathrm{Tr}(ax) + \mathrm{Tr}(bf(x))} \right)^m = \sum_{x_1, \ldots, x_m \in F} \zeta_p^{\mathrm{Tr}(a(x_1 + \cdots + x_m))} \zeta_p^{\mathrm{Tr}(b(f(x_1) + \cdots + f(x_m)))} \\ &= \sum_{s,t \in F} S^{(m)}_{s,t} \zeta_p^{\mathrm{Tr}(as)} \zeta_p^{\mathrm{Tr}(bt)} = \sum_{s,t \in F} X_{as} S^{(m)}_{st} X_{tb}, \end{aligned}$$

where $X = [X_{ab}]$ is defined in the proof of Proposition 2.13. Hence we obtain

$$W^{(m)} = X S^{(m)} X \quad (m \in \mathbb{N}).$$

On the other hand, we have $XJX = \left[\sum_{s,t \in F} X_{as} J_{st} X_{tb} \right]$ and

$$\sum_{s,t \in F} X_{as} J_{st} X_{tb} = \sum_{s,t \in F} \zeta_p^{\mathrm{Tr}(as+bt)} = \begin{cases} p^{2n} & ((a,b) = (0,0)), \\ 0 & (\text{otherwise}). \end{cases}$$

Hence $XJX = p^{2n} E$. Therefore we obtain

$$W^{(3)} - p^{n+1} W^{(1)} - (p^{3n} - p^{2n+1}) E = X \left(S^{(3)} - p^{n+1} S^{(1)} - (p^n - p) J \right) X$$

Then X is regular, since $XX^* = p^n I$. Therefore the equation (4) is equivalent to

$$S^{(3)} = p^{n+1} S^{(1)} + (p^n - p) J,$$

that is, $S^{(3)}_{a,b} = \begin{cases} p^n - p & (f(a) \neq b), \\ (p+1)p^n - p & (f(a) = b) \end{cases}$ for any $a,\ b \in F$ since we have clearly $S^{(1)}_{a,b} = \begin{cases} 0 & (f(a) \neq b), \\ 1 & (f(a) = b). \end{cases}$ □

4.1 The case that $p = 3$

In this subsection, we assume that $p = 3$ and

$$f(-x) = -f(x) \text{ for any } x \in F = \mathbb{F}_{3^n}. \tag{5}$$

Then we have $f(0) = 0$ clearly. We have the following theorem which is a partial generalization of a relation between APN functions and AB functions introduced in [5].

Theorem 4.3. *Let $f\colon F \to F$ be a function with (5). Assume that $d^\circ(f) \leq 3$. If f is a GAB function, then f is a GAPN function of algebraic degree* 3.

Proof. Let f be a GAB function. Since $f(0) = 0$, the system of equations

$$\begin{cases} x_1 + x_2 + x_3 = 0, \\ f(x_1) + f(x_2) + f(x_3) = 0 \end{cases} \tag{6}$$

has $(3+1)3^n - 3 = 3(3^n - 1) + 3^n$ solutions by Proposition 4.2. Since for any $b \in F$,

$$f(0) + f(b) + f(2b) = f(b) + f(-b) = f(b) - f(b) = 0,$$

the solutions of (6) are only trivial solutions, that is

$$\left\{ (0, b, 2b), (b, 2b, 0), (2b, 0, b) \;\middle|\; b \in F^\times \right\}, \ \left\{ (x, x, x) \mid x \in F \right\}. \tag{7}$$

Assume that f is not a GAPN function. Then by Proposition 2.11, $\tilde{D}_a f(x) = \tilde{D}_a f(0)$ has a nontrivial solution $x_0 \in F \setminus \{ 0, a, 2a \}$ for some $a \in F^\times$. On the other hand, by (5), we have $\tilde{D}_a f(0) = 0$. Hence $(x_0, x_0 + a, x_0 + 2a)$ is a solution of the system (6), but this solution is not contained in any set of (7), which is absurd. Therefore f is a GAPN function, and we have $d^\circ(f) = 3$ by Proposition 2.12. □

Remark 4.4. (1) When $p = 2$, any AB function is APN by [5]. However, the assumption of Theorem 4.3 is necessary. In fact, there exists a function f on $\mathbb{F}_{3^n}$ such that it is a GAB function but not a GAPN function when $d^\circ(f) > 3$. For example, let $n = 5$ and $\mathbb{F}_{3^5} = \mathbb{F}_3(\alpha)$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the function $f : \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$ defined by $f(x) = x^{17}$ has algebraic degree 5, and it is a GAB function by a simple computation. However, we have

$$\left\{ x \in \mathbb{F}_{3^5} \;\middle|\; D_1 f(x) = \alpha^3 + 2\alpha^2 + \alpha + 1 \right\} = \left\{ 2\alpha + j, \alpha^4 + \alpha^3 + j \;\middle|\; j \in \mathbb{F}_3 \right\},$$

and hence, $\tilde{N}_f(1, \alpha^3 + 2\alpha^2 + \alpha + 1) = 6$. Thus f is not a GAPN function.

(2) When $p = 2$, any quadratic APN function on $\mathbb{F}_{2^n}$ is an AB function if n is odd by [1]. Unfortunately, this property is not generalized in our case, that is, there exists a function f on $\mathbb{F}_{3^n}$ such that f is a GAPN function of algebraic degree 3 but not a GAB function. In particular, the converse of Theorem 4.3 is not true. For example, the function $f : \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$ defined by $f(x) = x^{11}$ is a GAPN function of algebraic degree 3 (see Theorem 3.4). However, by a simple computation, we can see that the set of all Walsh coefficients of f is $\{0, -9, 18, \pm 27, -36, 45, -54\}$, and hence f is not a GAB function.

5 Construction of dual arcs

Let V be a vector space over a finite field $\mathbb{F}_q$. A collection $\mathcal{S}$ of m-dimensional subspaces of V is called an $(m-1)$-**dimensional dual arc** over $\mathbb{F}_q$ if the following conditions are satisfied:

(i) $\dim(X \cap Y) = 1$ for any different $X, Y \in \mathcal{S}$.

(ii) $X \cap Y \cap Z = 0$ for any three mutually different $X, Y, Z \in \mathcal{S}$.

If $|\mathcal{S}| = (q^m - q)/(q-1) + 1$ then $\mathcal{S}$ is called an $(m-1)$-**dimensional dual hyperoval**.

Let f be a quadratic function on $\mathbb{F}_{2^n}$. We regard $\mathbb{F}_{2^n}$ as an n-dimensional vector space over $\mathbb{F}_2$. For every $a \in \mathbb{F}_{2^n}$ we define a set $X_f(a) \subset \mathbb{F}_{2^n} \oplus \mathbb{F}_{2^n}$ by

$$X_f(a) \coloneqq \{\, (x, B_f(x,a)) \mid x \in \mathbb{F}_{2^n} \,\},$$

where $B_f(x,a) = f(x+a) + f(x) + f(a) + f(0)$. Since f is quadratic, the form B_f is bilinear and the map $x \mapsto (x, B_f(x,a))$ is a injective linear map. Hence $X_f(a)$ is n-dimensional subspace in $\mathbb{F}_{2^n} \oplus \mathbb{F}_{2^n}$ for every $a \in \mathbb{F}_{2^n}$. Let $\mathcal{S}_f$ denote the collection of subspaces $X_f(a)$. Yoshiara characterized quadratic APN functions on $\mathbb{F}_{2^n}$ as follows:

Theorem 5.1 (Yoshiara [13, Theorem 2.1])**.** *Let $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic function. Then f is APN if and only if $\mathcal{S}_f$ is an $(n-1)$-dimensional dual hyperoval.*

The bilinearity of B_f is very useful. However, our form $\tilde{B}_f$ is hardly bilinear for $p \geq 3$. We may resolve this problem with some modification. Let μ be a map from $F^\times = \mathbb{F}_{p^n}^\times$ to the set of $\mathbb{F}_p$-linear automorphisms on F and let μ_a denote the image of a by μ. Let ν be a permutation on F fixing 0.

For such maps μ, ν and a function $f\colon F \to F$, we define

$$\tilde{B}_{f,\mu,\nu}(x,a) \coloneqq \begin{cases} (\mu_a \circ \tilde{B}_f)(x, \nu(a)) & (a \neq 0), \\ 0 & (a = 0). \end{cases}$$

Note that for any $a \in F^\times$ we have $\tilde{B}_{f,\mu,\nu}(x,a) = 0$ if and only if $\tilde{B}_f(x, \nu(a)) = 0$. Hence when $d^\circ(f) \leq p$ we have that f is a GAPN function if and only if

$$\left\{ x \in F \;\middle|\; \tilde{B}_{f,\mu,\nu}(x,a) = 0 \right\} = \mathbb{F}_p \nu(a) \text{ for any } a \in F^\times$$

by Proposition 2.12.

Proposition 5.2. *Let $f(x) = x^d$ be a monomial function with $d^\circ(f) \leq p$. Define maps μ, ν by $\mu_a(x) = a^d x$ and $\nu(a) = a^{-1}$. Then $\tilde{B}_{f,\mu,\nu}(x,a)$ is $\mathbb{F}_p$-bilinear.*

Proof. Since $d^\circ(f) \leq p$ the form $[f]^p$ is $\mathbb{F}_p$-multilinear by Proposition 2.7 (2). Hence $\tilde{B}_f(x,a)$ is $\mathbb{F}_p$-linear in x. Moreover $\tilde{B}_f(x,a)$ is homogeneous of degree d as a polynomial in x and a. Therefore

$$\tilde{B}_f(x,a) = \sum_i c_i x^{p^i} a^{d-p^i}$$

for some $c_i \in \mathbb{F}_p$. Then

$$\tilde{B}_{f,\mu,\nu}(x,a) = (\mu_a \circ \tilde{B}_f)(x,\nu(a)) = a^d \left(\sum_i c_i x^{p^i} a^{p^i - d} \right) = \sum_i c_i (xa)^{p^i},$$

which is $\mathbb{F}_p$-bilinear. □

For the generalized Gold functions, we have another choice of maps μ, ν such that $\tilde{B}_{f,\mu,\nu}$ is $\mathbb{F}_p$-bilinear.

Proposition 5.3. *Let $f(x) = x^{p^i+p-1}$ be the generalized Gold function. Define maps μ, ν by $\mu_a(x) = a^{2-p}x$ and $\nu(a) = a$. Then $\tilde{B}_{f,\mu,\nu}(x,a)$ is $\mathbb{F}_p$-bilinear.*

Proof. By (ii) in Lemma 3.3, we have $\tilde{B}_f(x,a) = -a^{p-1}x^{p^i} + a^{p^i+p-2}x$. Hence we get

$$\tilde{B}_f(x,a) = (\mu_a \circ \tilde{B}_f)(x,\nu(a)) = a^{2-p}\left(-a^{p-1}x^{p^i} + a^{p^i+p-2}x\right) = -ax^{p^i} + a^{p^i}x,$$

which is $\mathbb{F}_p$-bilinear. □

Proposition 5.4. *Let f be a GAPN function with $d^\circ(f) = p$ and μ, ν as above. Suppose that $\tilde{B}_{f,\mu,\nu}$ is $\mathbb{F}_p$-bilinear. Then the following hold:*

(1) $\mathbb{F}_p\nu(a) = \mathbb{F}_p\nu(ia)$ for any $a \in F$ and $i \in \mathbb{F}_p^\times$.

(2) Three mutually different elements $a, b, c \in F$ lie on the same line if and only if $\nu(a-b)$ and $\nu(a-c)$ are linearly dependent.

Proof. (1) Since $\tilde{B}_{f,\mu,\nu}$ is $\mathbb{F}_p$-bilinear, we have that $\tilde{B}_{f,\mu,\nu}(x,a) = 0$ if and only if $\tilde{B}_{f,\mu,\nu}(x,ia)$ for any $a \in F$ and $i \in \mathbb{F}_p^\times$. Hence

$$\mathbb{F}_p\nu(a) = \left\{ x \in F \;\middle|\; \tilde{B}_{f,\mu,\nu}(x,a) = 0 \right\} = \left\{ x \in F \;\middle|\; \tilde{B}_{f,\mu,\nu}(x,ia) = 0 \right\} = \mathbb{F}_p\nu(ia).$$

(2) Suppose that mutually different elements $a, b, c \in F$ lie on the same line. Then there exists $i \in \mathbb{F}_p^\times$ such that $a - b = i(a-c)$. We have $\nu(a-b) = \nu(i(a-c))$. By (1), there exists $j \in \mathbb{F}_p^\times$ such that $\nu(i(a-c)) = j\nu(a-c)$. Hence we have $\nu(a-b) = j\nu(a-c)$. Thus $\nu(a-b)$ and $\nu(a-c)$ are linearly dependent. The converse is similar. □

Let f be a GAPN function with $d^\circ(f) = p$ and μ, ν as above. Suppose that $\tilde{B}_{f,\mu,\nu}$ is $\mathbb{F}_p$-bilinear. For any $a \in F$, we define

$$X_{f,\mu,\nu}(a) \coloneqq \left\{ (x, \tilde{B}_{f,\mu,\nu}(x,a)) \;\middle|\; x \in F \right\} \subset F \oplus F.$$

The bilinearity of $\tilde{B}_{f,\mu,\nu}$ implies that $X_{f,\mu,\nu}(a)$ is an n-dimensional subspace in $F \oplus F$. Let $M \subset F$ be a set in which three mutually different elements do not lie on the same line. Let $\mathcal{S}_{f,\mu,\nu,M}$ denote the collection of subspaces $X_{f,\mu,\nu}(a)$, where $a \in M$.

Proposition 5.5. *Suppose that $n \geq 2$. Then the collection $\mathcal{S}_{f,\mu,\nu,M}$ is an $(n-1)$-dimensional dual arc.*

Proof. Let $a, b \in M$ be different elements. Suppose that $(x, y) \in X_{f,\mu,\nu}(a) \cap X_{f,\mu,\nu}(b)$. Then we have $y = \tilde{B}_{f,\mu,\nu}(x, a) = \tilde{B}_{f,\mu,\nu}(x, b)$. Hence $\tilde{B}_{f,\mu,\nu}(x, a-b) = 0$. Therefore $x \in \mathbb{F}_p\nu(a-b)$, and hence $\dim(X_{f,\mu,\nu}(a) \cap X_{f,\mu,\nu}(b)) = 1$. Since $n \geq 2$, $X_{f,\mu,\nu}(a)$ is different from $X_{f,\mu,\nu}(b)$.

Next we suppose that a, b, c are mutually different elements in M. Then by the above argument, $X_{f,\mu,\nu}(a)$, $X_{f,\mu,\nu}(b)$, $X_{f,\mu,\nu}(c)$ are mutually different subspaces. On the other hand, since a, b, c do not lie on the same line, $\nu(a-b)$ and $\nu(a-c)$ are linearly independent by Proposition 5.4. Therefore

$$X_{f,\mu,\nu}(a) \cap X_{f,\mu,\nu}(b) \cap X_{f,\mu,\nu}(c) \subset \mathbb{F}_p\nu(a-b) \cap \mathbb{F}_p\nu(a-c) = 0.$$

Hence $\mathcal{S}_{f,\mu,\nu,M}$ is a dual arc. □

Acknowledgements

The authors would like to thank the reviewers for valuable suggestions and comments, which were very helpful in making this paper more readable.

References

[1] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On almost perfect nonlinear functions over $\mathbb{F}_2^n$, *IEEE Trans. Inform. Theory* **52** (2006), no. 9, 4160–4170.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations, in *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 65–76.

[3] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inform. Theory* **52** (2006), no. 3, 1141–1152.

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

[5] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, in *Advances in cryptology—EUROCRYPT '94 (Perugia)*, Lecture Notes in Comput. Sci., vol. 950, Springer, Berlin, 1995, pp. 356–365.

[6] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, and W. Willems, APN functions in odd characteristic, *Discrete Math.* **267** (2003), no. 1-3, 95–112, Combinatorics 2000 (Gaeta).

[7] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inform. Theory* **14** (1968), no. 1, 154–156.

[8] T. Helleseth, C. Rong, and D. Sandberg, New families of almost perfect nonlinear power mappings, *IEEE Trans. Inform. Theory* **45** (1999), no. 2, 474–485. MR 1677012

[9] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, 1st ed., Chapman & Hall/CRC, 2013.

[10] K. Nyberg, Differentially uniform mappings for cryptography, in *Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings* (T. Helleseth, ed.), Springer Berlin Heidelberg, Berlin, Heidelberg, 1994, pp. 55–64.

[11] K. Nyberg, S-boxes and round functions with controllable linearity and differential uniformity, in *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings* (B. Preneel, ed.), Springer Berlin Heidelberg, Berlin, Heidelberg, 1995, pp. 111–130.

[12] E. R. van Dam and D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, *European J. Combin.* **24** (2003), no. 1, 85–98.

[13] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, *Innov. Incidence Geom.* **8** (2008), 147–169.

Masamichi Kuroda
Department of Mathematics
Hokkaido University
Sapporo 060-0810
Japan
m-kuroda@math.sci.hokudai.ac.jp

Shuhei Tsujie
Department of Mathematics
Hokkaido University
Sapporo 060-0810
Japan
tsujie@math.sci.hokudai.ac.jp