ON QUADRATIC BINOMIAL VECTORIAL FUNCTIONS WITH MAXIMAL BENT COMPONENTS

XIANHONG XIE[1], YI OUYANG[2,3], AND SHENXING ZHANG[4,5]

ABSTRACT. Assume $n = 2m \geq 2$ and let $F(x) = x^{d_1} + x^{d_2}$ be a binomial vectorial function over $\mathbb{F}_{2^n}$ possessing the maximal number (i.e., $2^n - 2^m$) of bent components. Suppose the 2-adic Hamming weights $\mathrm{wt}_2(d_1)$ and $\mathrm{wt}_2(d_2)$ are both at most 2. We prove that $F(x)$ is EA-equivalent to either x^{2^m+1} or $x^{2^i}(x+x^{2^m})$, provided that $\ell(n) := \min_{\gamma:\ \mathbb{F}_2(\gamma)=\mathbb{F}_{2^n}} \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma > m$, where σ is the Frobenius ($x \mapsto x^2$) on $\mathbb{F}_{2^n}$, and $\gcd(d_1, d_2, 2^m - 1) > 1$. Under this condition, we also establish two bounds on the nonlinearity and the differential uniformity of F by means of the cardinality of its image set.

1. INTRODUCTION

In this paper, we fix a positive even integer $n = 2m$. Let $\mathbb{F}_{2^i}$ be the finite field of 2^i elements, σ be the Frobenius ($x \mapsto x^2$) on $\mathbb{F}_{2^i}$ and $\mathrm{Tr}_{2^i/2}$ be the trace function from $\mathbb{F}_{2^i}$ to $\mathbb{F}_2$. For a finite set X, we denote by $\#X$ its cardinality.

Suppose that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a vectorial function. For $a \in \mathbb{F}_{2^n}$, let F_a be the component function

$$F_a : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2, \quad v \longmapsto \mathrm{Tr}_{2^n/2}\big(a \cdot F(v)\big).$$

Let

$$S_F = \{a \in \mathbb{F}_{2^n} : F_a \text{ is not bent}\}.$$

In 2018, Pott et al. [12] proved that the cardinality $\#S_F \geq 2^m$, i.e., the number of bent components is at most $2^n - 2^m$. Further results about vectorial functions and their bent components were obtained by [1, 5, 10, 15, 14] and others.

Two fundamental questions arise in this subject: first, to classify all functions $F(x)$ that attain the maximal number of bent components; and second, to clarify key cryptographic properties—such as nonlinearity and differential uniformity—of such functions.

Research on functions attaining the maximal number of bent components has seen notable progress. In 2023, Hu et al. [5] established that the monomials $x^{2^i(2^m+1)}$ are the only monomials over $\mathbb{F}_{2^n}$ possessing $2^n - 2^m$ bent components. For binomial vectorial functions of the form $F(x) = x^{d_1} + x^{d_2}$, Pott et al. [12] demonstrated that $F(x)$ achieves this bound when $d_1 = 2^i + 1$ and $d_2 = 2^m + 2^i$ ($0 \leq i \leq m-1$). More recently, Xie et al. [14] refined this analysis for the specific family $F(x) = x^{2^i+1} + x^{2^m+1}$ ($0 \leq i \leq m-1$), proving it attains the bound

2020 *Mathematics Subject Classification.* 11T71, 94A60, 06E30.

Key words and phrases. Vectorial functions, Bent components, Walsh transform, Stickelberger's Theorem, Hamming weight.

Partially supported by NSFC (Grant No. 62402004), QNMP (Grant No. 2021ZD0302902), and State Key Laboratory of Cyberspace Security Defense (Grant No. 2025-MS-04).

Corresponding author: S. Zhang.

if and only if $i = 0$. Furthermore, for general exponents (d_1, d_2), computational evidence using Magma presented in [14] suggests that any such binomial $F(x)$ is EA-equivalent to either x^{2^m+1} or $x^{2^i}(x+x^{2^m})$ if it has the maximal number of bent components. However, a proof of this assertion remains elusive.

Anbar et al. [1] proved that the nonlinearity of a plateaued function with the maximal number of bent components is at most $2^{n-1} - 2^{\lfloor \frac{3n}{4} \rfloor}$. Xie et al. [14] presented examples of plateaued and non-plateaued vectorial functions attaining the upper bound. Whether this bound holds for non-plateaued functions remains an open question.

The main goal of this paper is to investigate properties of binomial functions $F(x) = x^{d_1} + x^{d_2}$ with the maximal number of bent components, using Stickelberger's Theorem as developed in [8, 6, 7, 5]. Assuming that

$$\ell(n) := \min_{\gamma:\, \mathbb{F}_2(\gamma)=\mathbb{F}_{2^n}} \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma > m, \quad \gcd(d_1, d_2, 2^m - 1) > 1,$$

our contributions can be summarized as follows.

(A). We show that $S_F = \mathbb{F}_{2^m}$ and $d_2 - d_1 \equiv 0 \pmod{2^m - 1}$ whenever F has $2^n - 2^m$ bent components. Moreover, F is EA-equivalent to x^{2^m+1} if $\mathrm{wt}_2(d_1) = 1$, and to $x^{2^i+1} + x^{2^i+2^m}$ if $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$. This generalizes the results in [14, Theorem 9] and [15, Theorem 4.16].

(B). Using the cardinality of the image set, we establish theoretical bounds on the nonlinearity and differential uniformity of general functions F over $\mathbb{F}_{2^n}$ satisfying $\ell(n) > m$, $\#S_F = 2^m$, and $\sigma \circ F = F \circ \sigma$. If in addition $F(x) = x^{d_1} + x^{d_2}$, we prove that

$$\#\,\mathrm{Im}(F) = \frac{(2^m - 1)c}{s} + 1,$$

and

$$\mathcal{N}_F \le 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{3m}}{T}\left(\frac{2^{3m}s}{s + (2^m - 1)c} - 2^{m+1} + 1\right)},$$
$$\delta_F \ge \left\lceil \frac{2^n}{\#\Delta}\left(\frac{2^n s}{s + (2^m - 1)c} - 1\right)\right\rceil,$$

where α is a generator of $\mathbb{F}_{2^n}^*$ and

$$s = \gcd(d_1, d_2, 2^m - 1),$$
$$c = \#\big\{F(\alpha^i)^{(2^m-1)/s} : i = 1, 2, \ldots, 2^m\big\},$$
$$T = \#\{a \in \mathbb{F}_{2^m}^* : W_{F_a}(0) \neq 0\},$$
$$\Delta = \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n},\, x \neq y,\, F(x) = F(y)\}.$$

The paper is organized as follows. In § 2, we provide some necessary preliminaries. In § 3, we establish further properties of binomial vectorial functions with the maximal number of bent components. In § 4, we derive equivalent forms of $F(x)$ for the cases where $\mathrm{wt}_2(d_1) = 1$ or $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$. In § 5, we determine the cardinality of the image set of F, and then use it to derive bounds on its nonlinearity and differential uniformity. In § 6, we conclude the paper.

2. Preliminaries

We always denote $N = 2^n - 1$.

2.1. **The components of vectorial functions.** We recall some facts about vectorial functions.

Definition 1. *Suppose that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a vectorial function.*

(i) *The component function F_a of F at $a \in \mathbb{F}_{2^n}$ is the Boolean function*

$$\begin{aligned} F_a : \mathbb{F}_{2^n} &\longrightarrow \mathbb{F}_2 \\ v &\longmapsto \mathrm{Tr}_{2^n/2}\big(a \cdot F(v)\big). \end{aligned}$$

(ii) *The Walsh transform of F is*

$$W_F(a,\omega) := W_{F_a}(\omega) = \sum_{v \in \mathbb{F}_{2^n}} (-1)^{F_a(v)+\mathrm{Tr}_{2^n/2}(\omega v)},$$

where $a \in \mathbb{F}_{2^n}^*$, $\omega \in \mathbb{F}_{2^n}$.

(iii) *If $W_{F_a}(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$, then F_a is called a bent component of F. Denote*

$$S_F := \{a \in \mathbb{F}_{2^n} : F_a \text{ is not bent}\}.$$

(iv) *If $W_{F_a}(\omega) \in \{0, \pm 2^{\frac{n+k}{2}}\}$ for all $\omega \in \mathbb{F}_{2^n}$, where $k \in \mathbb{Z}$ and $k \equiv n \bmod 2$, then F_a is called a k-plateaued component of F. If all F_a ($a \in \mathbb{F}_{2^n}^*$) are plateaued, then F is called plateaued.*

(v) *The nonlinearity of F is the minimal nonlinearity among its component functions, i.e.,*

$$\mathcal{N}_F := 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}^*, \omega \in \mathbb{F}_{2^n}} |W_{F_a}(\omega)|.$$

(vi) *The differential uniformity of F is*

$$\delta_F := \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \#\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}.$$

Pott et al. [12] proved the following result.

Theorem 1. *$\#S_F \geq 2^m$. Moreover, $\#S_F = 2^m$ if and only if S_F is an m-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$.*

We say that F has the maximal number of bent components if $\#S_F = 2^m$, i.e. the number of bent components of F is exactly $2^n - 2^m$. A natural problem is to determine all vectorial functions with the maximal number of bent components.

Theorem 2. *If $F(x) = x^{d_1}$ has the maximal number of bent components, then*

(1) (*Zheng et al.* [15]) *$S_F = \mathbb{F}_{2^m}$ and $(2^m + 1) \mid d_1$;*
(2) (*Hu et al.* [5]) *$d_1 = (2^m + 1)s$, where $s \in \{1, 2, 2^2, \ldots, 2^{m-1}\}$.*

For the nonlinearity of plateaued functions with the maximal number of bent components, we know

Theorem 3. *If F is a plateaued function and $\#S_F = 2^m$, then*

$$\mathcal{N}_F \leq 2^{n-1} - 2^{\lfloor \frac{3n}{4} \rfloor}.$$

2.2. **Gauss sums and Stickelberger's Theorem.** Let $\mathbb{Q}_2$ denote the field of 2-adic numbers and $\overline{\mathbb{Q}}_2$ be a fixed algebraic closure of $\mathbb{Q}_2$. We regard $\overline{\mathbb{Q}}_2$ as a subfield of $\mathbb{C}$, the field of complex numbers.

Let ξ be a primitive N-th root of unity in $\overline{\mathbb{Q}}_2$ (recall $N = 2^n - 1$). The algebraic extension $\mathbb{Q}_2(\xi)/\mathbb{Q}_2$ is unramified of degree n. We identify $\mathbb{F}_{2^n}$ with the residue field of $\mathbb{Q}_2(\xi)$ that is $\mathbb{Z}_2[\xi]/(2)$. For any $a \in \mathbb{F}_{2^n}$, there exists a canonical lifting $\omega(a) \in \mathbb{Z}_2[\xi]$ such that $\omega(ab) = \omega(a)\omega(b)$ and

$$\omega(a) \bmod 2 = a, \ a \in \mathbb{F}_{2^n}. \tag{1}$$

The character ω is called the Teichmüller character of $\mathbb{F}_{2^n}$. The group $\widehat{\mathbb{F}^*_{2^n}}$ of multiplicative characters of $\mathbb{F}^*_{2^n}$ is a cyclic group of order N generated by ω:

$$\widehat{\mathbb{F}^*_{2^n}} = \{\chi : \ \mathbb{F}_{2^n} \to \mathbb{C}\} = \{\omega^j : \ 0 \le j \le N-1\}.$$

As is customary, the definition domain of a character χ is extended to $\mathbb{F}_{2^n}$ by setting $\chi(0) = 0$ if χ is nontrivial and $\chi(0) = 1$ if $\chi = \omega^0$ is trivial.

Definition 2. *For $\chi \in \widehat{\mathbb{F}^*_{2^n}}$, the Gauss sum $G(\chi)$ over $\mathbb{F}_{2^n}$ is defined by*

$$G(\chi) = \sum_{x \in \mathbb{F}^*_{2^n}} \psi(x)\chi(x),$$

where $\psi(x) = (-1)^{\mathrm{Tr}_{2^n/2}(x)}$ is the canonical additive character of $\mathbb{F}_{2^n}$.

Obviously, $G(\chi) = -1$ if χ is trivial, and $G(\chi)G(\chi^{-1}) = \chi(-1)2^n$ if χ is nontrivial. For any $x \in \mathbb{F}^*_{2^n}$, applying the inverse Fourier transform, we obtain

$$\psi(x) = \frac{1}{N} \sum_{\chi \in \widehat{\mathbb{F}^*_{2^n}}} G(\chi)\chi^{-1}(x) = \frac{1}{N} \sum_{j=0}^{N-1} G(\omega^{-j})\omega^j(x). \tag{2}$$

We identify $\mathbb{Z}_N$ with the set $\{0, 1, \cdots, N-1\}$. For any integer j, let $j_N = j \bmod N \in \mathbb{Z}_N$ be its minimal non-negative residue. For any positive integer j, let $\mathrm{wt}_2(j)$ denote its 2-adic Hamming weight, namely

$$\mathrm{wt}_2(j) = \mathrm{wt}_2(j_N) = \sum_{i=0}^{n-1} c_i, \ \text{where } j_N = \sum_{i=0}^{n-1} c_i 2^i$$

is the binary representation of $j_N = j \bmod N$.

Let $\bar{b}$ denote the bit-complement of $b \in \{0, 1\}$, i.e., $\bar{b} = 1 - b$. Then

$$(-j)_N = \sum_{i=0}^{n-1} \bar{c}_i 2^i \quad \text{and} \quad \mathrm{wt}_2(-j) = \sum_{i=0}^{n-1} \bar{c}_i = n - \mathrm{wt}_2(j).$$

The following theorem of Stickelberger is a well-known result in algebraic number theory and is very useful for analyzing exponential sums.

Theorem 4 ([13])**.** *For any $0 \le i < N$,*

$$G(\omega^{-i}) \equiv 2^{\mathrm{wt}_2(i)} \mod 2^{\mathrm{wt}_2(i)+1}.$$

3. Binomial vectorial functions with the maximal bent components

From now on, let

$$F(x) = x^{d_1} + x^{d_2} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

be a binomial vectorial function, where $d_1, d_2 \in \mathbb{Z}_N \backslash \{0\}$. Our goal is to characterize the functions $F(x)$ for which the number of bent components is maximal.

3.1. **Known results.** The following result is due to Pott et al. [12].

Theorem 5. *The function $F(x) = x^{2^i+1} + x^{2^i+2^m}$ $(0 < i < m)$ has the maximal number of bent components.*

Two vectorial functions $F, F' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called EA-equivalent if there exist affine automorphisms $A, A' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an affine function $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F' = A' \circ F \circ A + L$. Note that the property of having maximal number of bent components is invariant under EA-equivalence.

By Theorem 5, if replacing i by $m - i$, then $F(x) = x^{1+2^{m-i}} + x^{2^{m-i}+2^m}$ $(0 < i < m)$ has the maximal number of bent components. Set

$$A(x) = x^{2^{m+i}},\ A' = x,\ \text{and}\ L = 0.$$

Then we have

Corollary 1. *The function $F(x) = x^{1+2^i} + x^{1+2^{m+i}}$ has the maximal number of bent components.*

Moreover, if we replace $2^i + 2^m$ by $2^{m+i} + 2^m$, then

Proposition 1. *The number of bent components of $F(x) = x^{2^i+1} + x^{2^{m+i}+2^m}$ $(0 \le i \le m)$ is not maximal.*

Proof. This is trivial if $i = 0$ or m. Now we suppose $0 < i < m$.

For $a \in \mathbb{F}_{2^n}^*$, $F_a(x)$ is a quadratic form, whose associated bilinear form is

$$\begin{aligned} B_a(x,z) &= F_a(x+z) + F_a(x) + F_a(z) \\ &= \mathrm{Tr}_{2^n/2}\big(aF(x+z)\big) + \mathrm{Tr}_{2^n/2}\big(aF(x)\big) + \mathrm{Tr}_{2^n/2}\big(aF(z)\big) \\ &= \mathrm{Tr}_{2^n/2}\big(ax^{2^i}z + axz^{2^i} + ax^{2^m}z^{2^{m+i}} + ax^{2^{m+i}}z^{2^m}\big) \\ &= \mathrm{Tr}_{2^n/2}\big(z(ax^{2^i} + (ax)^{2^{n-i}} + a^{2^{m-i}}x^{2^{n-i}} + a^{2^m}x^{2^i})\big). \end{aligned}$$

Let $L_a(x) := ax^{2^i} + (ax)^{2^{n-i}} + a^{2^{m-i}}x^{2^{n-i}} + a^{2^m}x^{2^i}$. By a result of Hu and Feng [4], $F_a(x)$ is bent if and only if $F_a(x)$ is non-degenerate. As n is even, this is equivalent to the non-degeneracy of $B_a(x,z)$. As the trace map is non-degenerate, we get

$$F_a \text{ is not bent} \iff \exists\, x \neq 0, \text{ such that } L_a(x) = 0.$$

We conclude that F has more than 2^m non-bent components:

(i) If $a \in \mathbb{F}_{2^m}$, then $L_a(x) = 0$ for any $x \in \mathbb{F}_{2^n}$, so F_a is not bent.
(ii) The trace map $\mathrm{Tr}_{2^n/2^m}$ is surjective, so there exists $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ such that $\mathrm{Tr}_{2^n/2^m}(a) = a + a^{2^m} = 1$. For such a, $L_a(1) = 0$, hence F_a is not bent. □

3.2. **The study of $\mathcal{J}_{d_1,d_2}$.** For a positive integer i, we denote by $v_2(i)$ its 2-adic valuation.

Definition 3. *Let $\mathcal{J} = (\mathbb{Z}_N \times \mathbb{Z}_N) \setminus \{(0,0)\}$. Define*

$$\begin{aligned} V_{d_1,d_2} &:= \Big((j_1,j_2) \in \mathcal{J} \mapsto \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) + \mathrm{wt}_2(-d_1j_1 - d_2j_2)\Big); \\ \nu_{d_1,d_2} &:= \min\{V_{d_1,d_2}(j_1,j_2) : (j_1,j_2) \in \mathcal{J}\}; \\ \mathcal{J}_{d_1,d_2} &:= \{(j_1,j_2) \in \mathcal{J} : V_{d_1,d_2}(j_1,j_2) = \nu_{d_1,d_2}\}. \end{aligned} \tag{3}$$

Obviously, the set $\mathcal{J}_{d_1,d_2}$ is closed under multiplication by 2.

Theorem 6. (1) *For any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, $v_2\big(W_{F_a}(b)\big) \ge \nu_{d_1,d_2}$.*

(2) *Denote the polynomial*

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2} x^{(-d_1j_1-d_2j_2)_N}.$$

Then $g_a(b) \in \mathbb{F}_2$ *and*

$$v_2\big(W_{F_a}(b)\big) > \nu_{d_1,d_2} \iff g_a(b) = 0. \tag{4}$$

Proof. For $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we have

$$\begin{aligned} W_{F_a}(b) &= 1 + \sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_{2^n/2}(ax^{d_1}+ax^{d_2}+bx)} \\ &= 1 + \sum_{x\in\mathbb{F}_{2^n}^*} \psi(ax^{d_1})\psi(ax^{d_2})\psi(bx) = 1 + \frac{S}{N^3}, \end{aligned}$$

where S is given as follows by Eq. (2):

$$\begin{aligned} S &= \sum_{x\in\mathbb{F}_{2^n}^*} \sum_{j_1,j_2,j_3=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{-j_3})\omega^{j_1}(ax^{d_1})\omega^{j_2}(ax^{d_2})\omega^{j_3}(bx) \\ &= \sum_{j_1,j_2,j_3=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{-j_3})\omega^{j_1+j_2}(a)\omega^{j_3}(b) \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{d_1j_1+d_2j_2+j_3}(x) \\ &= N \sum_{j_1,j_2=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1j_1+d_2j_2})\omega^{j_1+j_2}(a)\omega^{-d_1j_1-d_2j_2}(b) \\ &= N \sum_{(j_1,j_2)\in\mathcal{J}} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1j_1+d_2j_2})\omega(a^{j_1+j_2}b^{-d_1j_1-d_2j_2}) - N. \end{aligned}$$

Recall that $N = 2^n - 1$, one has

$$W_{F_a}(b) \equiv \sum_{(j_1,j_2)\in\mathcal{J}} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1j_1+d_2j_2})\omega(a^{j_1+j_2}b^{-d_1j_1-d_2j_2}) \mod 2^n.$$

By Theorem 4 and Eq. (3), we get

$$W_{F_a}(b) = 2^{\nu_{d_1,d_2}} \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} \omega(a^{j_1+j_2}b^{-(d_1j_1+d_2j_2)}) \mod 2^{\nu_{d_1,d_2}+1}.$$

Thus $v_2\big(W_{F_a}(b)\big) \geq \nu_{d_1,d_2}$.

Since $\mathcal{J}_{d_1,d_2}$ is closed under multiplication by 2, we have $g_a^2(b) = g_a(b)$ and $g_a(b) \in \mathbb{F}_2$. By Eq.(1),

$$g_a(b) \equiv \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} \omega(a^{j_1+j_2}b^{-(d_1j_1+d_2j_2)}) \mod 2,$$

and we have

$$v_2\big(W_{F_a}(b)\big) > \nu_{d_1,d_2} \iff g_a(b) = 0.$$

The completes the proof. □

Remark 1. *Analogously, let $F(x) = x^{d_1} + 1$, i.e. $d_2 = 0$. The notions $\nu_{d_1,0}$ and $\mathcal{J}_{d_1} := \mathcal{J}_{d_1,0}$ were introduced and studied in* [8, 9]. *It was shown there that for $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, $v_2\big(W_{F_a}(b)\big) \geq \nu_{d_1,0}$ and*

$$v_2\big(W_{F_a}(b)\big) > \nu_{d_1,0} \iff \sum_{j_1 \in \mathcal{J}_{d_1}} a^{j_1} b^{-d_1 j_1} = 0.$$

By [11, Theorem 13], we have

Lemma 1. *For any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,*

$$v_2\big(W_{F_a}(b)\big) \geq \nu_{d_1,d_2} \geq \left\lceil \frac{n}{\max\{\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2)\}} \right\rceil. \tag{5}$$

3.3. **Auxiliary results.**

Lemma 2. *Assume $s = \gcd(d_1, d_2, N) > 1$. If F has at least one bent component, then s divides either $2^m + 1$ or $2^m - 1$, and is coprime to the other. Specifically,*

$$s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m \text{ for any } a \in \mathbb{F}_{2^n} \setminus S_F.$$

Proof. Let α be a primitive element of $\mathbb{F}_{2^n}$ and $W = \{\gamma \in \mathbb{F}_{2^n} : \gamma^s = 1\}$. Then

$$W = \langle \alpha^{\frac{N}{s}} \rangle, \qquad \mathbb{F}_{2^n}^* = \bigcup_{i=0}^{\frac{N}{s}-1} \alpha^i W.$$

Clearly, $F_a(x)$ is constant on each coset $\alpha^i W$, consequently

$$\begin{aligned} W_{F_a}(0) &= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_{2^n/2}(ax^{d_1} + ax^{d_2})} \\ &= 1 + s \sum_{i=0}^{\frac{N}{s}-1} (-1)^{\mathrm{Tr}_{2^n/2}(a\alpha^{d_1 i} + a\alpha^{d_2 i})} \equiv 1 \mod s. \end{aligned}$$

By definition, $W_{F_a}(0) = \pm 2^m$ for $a \in \mathbb{F}_{2^n} \setminus S_F$. Thus if $\mathbb{F}_{2^n} \setminus S_F \neq \emptyset$, then $s \mid (2^m \pm 1)$. As $\gcd(2^m - 1, 2^m + 1) = 1$, s is a factor of one of $2^m \pm 1$ and coprime to the other. □

Lemma 3 ([6, Lemma 2])**.** *If $0 < j < N$, then $\mathrm{wt}_2(j) + \mathrm{wt}_2(-j) = n$. Moreover, if $(2^m + 1) \nmid j$, then $\mathrm{wt}_2((2^m - 1)j) = m$.*

Lemma 4. *Suppose $(j_1, j_2) \in \mathcal{J}$.*

1. *If $(j_1 + j_2)_N \geq 2^n - 2^m + 1$, then $V_{d_1,d_2}(j_1, j_2) \geq m + 1$.*
2. *If $j_1 + j_2 \equiv 0 \mod (2^m - 1)$, $j_1 + j_2 \neq N$ and $V_{d_1,d_2}(j_1, j_2) = m$, then*

$$\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = \mathrm{wt}_2(j_1 + j_2) = m, \qquad d_1 j_1 + d_2 j_2 \equiv 0 \mod N.$$

Proof. (1) Write $(j_1 + j_2)_N = N - u$. Then $0 < u \leq 2^m - 2$. Note that $\mathrm{wt}_2(u) \leq m - 1$ and $\mathrm{wt}_2(j_1 + j_2) \leq \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2)$, so

$$\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) \geq \mathrm{wt}_2(j_1 + j_2) = \mathrm{wt}_2(N - u) = n - \mathrm{wt}_2(u) \geq m + 1.$$

Hence, $V_{d_1,d_2}(j_1, j_2) \geq m + 1 + \mathrm{wt}_2(-(d_1 j_1 + d_2 j_2)) \geq m + 1$.

(2) If $j_1 + j_2 \equiv 0 \mod (2^m - 1)$ and $j_1 + j_2 \neq N$, then $\mathrm{wt}_2(j_1 + j_2) = m$ by Lemma 3. Thus

$$\begin{aligned} V_{d_1,d_2}(j_1, j_2) &= \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) + \mathrm{wt}_2(-(d_1 j_1 + d_2 j_2)) \\ &\geq m + \mathrm{wt}_2(-(d_1 j_1 + d_2 j_2)) \geq m. \end{aligned}$$

The equality holds only if

$$d_1 j_1 + d_2 j_2 \equiv 0 \mod N, \qquad \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = \mathrm{wt}_2(j_1 + j_2) = m. \qquad \square$$

Lemma 5. *If $\gamma \in S_F$, then $\sigma(\gamma) = \gamma^2 \in S_F$. Hence if $\#S_F = 2^m$, then*

$$\mathbb{F}_2[\sigma]\gamma = \{f(\sigma)\gamma \mid f(x) \in \mathbb{F}_2[x]\}$$

is a subspace of S_F.

Proof. We have

$$\begin{aligned} W_{F_{\gamma^2}}(b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(\gamma^2 F(x) + bx)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(\gamma^2 F(x^2) + b^{2^n} x^2)} = W_{F_\gamma}(b^{2^{n-1}}). \end{aligned}$$

Thus if $\gamma \in S_F$, then $\gamma^2 \in S_F$. If $\#S_F = 2^m$, then S_F is a vector space by Theorem 1, hence $\mathbb{F}_2[\sigma]\gamma \subseteq S_F$. $\square$

3.4. **The study of S_F.** We now give a general result, which also applies to the binomials $x^{d_1} + x^{d_2}$.

For any $\gamma \in \mathbb{F}_{2^n}$, define

$$\ell(\gamma) = \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma.$$

Clearly, $\ell(\gamma) \le [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$, and hence $\ell(\gamma) \le m$ if $\mathbb{F}_2(\gamma) \ne \mathbb{F}_{2^n}$. Denote

$$\ell(n) := \min\{\ell(\gamma) : \mathbb{F}_2(\gamma) = \mathbb{F}_{2^n}\}.$$

By definition, $\ell(n)$ can be regarded as the linear complexity of the Frobenius orbit.

Theorem 7. *Suppose that $F(x)$ is a vectorial function over $\mathbb{F}_{2^n}$ satisfying $\sigma \circ F = F \circ \sigma$ and $\#S_F = 2^m$. If $\ell(n) > m$, then $S_F = \mathbb{F}_{2^m}$.*

Proof. Assume $S_F \ne \mathbb{F}_{2^m}$. Let $S_1 = S_F \setminus \mathbb{F}_{2^m}$ and $S_2 = S_F \cap \mathbb{F}_{2^m}$. Since S_F is a vector space by Theorem 1, we have

$$\#S_1 \ge 1, \quad \#S_2 \le 2^{m-1}, \quad S_F = S_1 \cup S_2.$$

For any $\gamma \in S_1$, $\mathbb{F}_2(\gamma) \nsubseteq \mathbb{F}_{2^m}$. Note that $\mathbb{F}_2[\sigma]\gamma \subseteq S_F$ by Lemma 5. If γ is a generator of $\mathbb{F}_{2^n}$, then

$$m = \dim_{\mathbb{F}_2} S_F \ge \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma \ge \ell(n) > m,$$

which is impossible. Thus $\mathbb{F}_2(\gamma) \ne \mathbb{F}_{2^n}$, $\mathbb{F}_2(\gamma) \subseteq \mathbb{F}_{2^{n/p}}$ for some odd prime factor of n. This forces n to not be a power of 2.

Suppose that $p_1 < p_2 < \cdots < p_l$ are the odd prime factors of m. Then $\mathbb{F}_2(\gamma) \subseteq \mathbb{F}_{2^{n/p_i}}$ and $\gamma \in \mathbb{F}_{2^{n/p_i}} \setminus \mathbb{F}_{2^{m/p_i}}$ for some i. Thus

$$\begin{aligned} \#S_1 &\le \sum_{i=1}^{l} (2^{n/p_i} - 2^{m/p_i}) \le l(2^{n/3} - 2^{m/3}) \\ &\le 2^{3^{l-1}-1}(2^{2m/3} - 2^{m/3}) < 2^{m/3-1} \cdot 2^{2m/3} = 2^{m-1} \end{aligned}$$

and $\#S_F < 2^{m-1} + 2^{m-1} = 2^m$, which contradicts $\#S_F = 2^m$. Hence $S_F = \mathbb{F}_{2^m}$. $\square$

Remark 2. *Unfortunately there exist examples for which $\ell(n) \leq m$. We present experimental results on $\ell(n)$ in Table 1. It would be very interesting to learn more about $\ell(n)$.*

TABLE 1. Values of $\ell(n)$

n	$\ell(n)$	n	$\ell(n)$	n	$\ell(n)$
4	3	12	5	20	7
6	4	14	5	22	12
8	5	16	9	24	7
10	6	18	8	26	14

In the following, we present two cases for which the inequality $\ell(n) > m$ is satisfied.

Proposition 2. *We have $\ell(n) > m$ if*

(1) *$n = 2p$, where p is an odd prime and 2 is a primitive root modulo p, or*
(2) *$n = 2^k$, where k is a positive integer.*

Proof. (1) Note that

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

Let $\zeta \in \overline{\mathbb{F}}_2$ satisfy $\zeta \neq 1$ and $\zeta^p = 1$. Note that $\zeta^{2^k - 1} = 1$ if and only if $p \mid (2^k - 1)$. Since 2 is a primitive root modulo p, we have $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$ and thus the minimal polynomial Φ_p of ζ is irreducible.

Let $f_\alpha(x)$ be the minimal polynomial of σ on $\mathbb{F}_2[\sigma]\alpha$, where α is a generator of $\mathbb{F}_{2^n}$. By linear algebra, $\deg f_\alpha = \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\alpha = \ell(\alpha)$. Since $\sigma^{2p}(\alpha) = \alpha$ and $\sigma^p(\alpha) \neq \alpha$, we have

$$f_\alpha(x) \mid (x^{2p} - 1), \quad f_\alpha(x) \nmid (x^p - 1), \quad f_\alpha(x) \nmid (x^2 - 1).$$

Thus either $\Phi_p(x)^2 \mid f_\alpha$ or $(x-1)^2 \Phi_p(x) \mid f_\alpha$. This implies that

$$\ell(\alpha) = \deg f_\alpha \geq 2 + (p - 1) = p + 1.$$

Hence $\ell(2p) > p$.

(2) In this case, we have

$$f_\alpha(x) \mid (x^{2^k} - 1) = (x-1)^{2^k}, \quad f_\alpha(x) \nmid (x^{2^{k-1}} - 1) = (x-1)^{2^{k-1}}.$$

Hence $(x-1)^{2^{k-1}+1} \mid f_\alpha$ and then $\ell(\alpha) \geq 2^{k-1} + 1$. Thus $\ell(2^k) > 2^{k-1}$. □

4. The equivalence of quadratic binomial vectorial functions with the maximal bent components

In this section, we always assume

$$\ell(n) > m, \qquad \max\{\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2)\} = 2,$$

and denote $s = \gcd(d_1, d_2, N)$. Note that if $d_1 = 2^l$ for some integer $l \geq 0$, then $F(x) = x^{d_1} + x^{d_2}$ is EA-equivalent to x^{d_2}. By Theorem 2, this implies that $d_2 = (2^m + 1)2^i$ whenever $\#S_F = 2^m$. Hence, we proceed to show the equivalence for the case where $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$.

Lemma 6. *Assume that* $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$. *If* $V_{d_1,d_2}(j_1, j_2) = m$, *then* $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = m$ *and* $d_1j_1 + d_2j_2 \equiv 0 \mod N$.

Proof. If $V_{d_1,d_2}(j_1, j_2) = m$ and $d_1j_1 + d_2j_2 \not\equiv 0 \bmod N$, then

$$\begin{aligned}\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) &= m - \mathrm{wt}_2(-d_1j_1 - d_2j_2)\\ &= m - (n - \mathrm{wt}_2(d_1j_1 + d_2j_2)) = \mathrm{wt}_2(d_1j_1 + d_2j_2) - m\\ &\le \mathrm{wt}_2(d_1j_1) + \mathrm{wt}_2(d_2j_2) - m \le 2\,\mathrm{wt}_2(j_1) + 2\,\mathrm{wt}_2(j_2) - m.\end{aligned}$$

Thus $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) \ge m$. This implies that $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = m$ because $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) \le V_{d_1,d_2}(j_1, j_2) = m$. Then we have $\mathrm{wt}_2(-d_1j_1 - d_2j_2) = 0$, which contradicts $d_1j_1 + d_2j_2 \not\equiv 0 \bmod N$. Hence $d_1j_1 + d_2j_2 \equiv 0 \bmod N$ and $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = m$. □

Theorem 8. *Assume that* $\#S_F = 2^m$ *and* $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$. *Then* $\nu_{d_1,d_2} = m$ *and there exists* $(j_1, j_2) \in \mathcal{J}_{d_1,d_2}$ *such that*

$$\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = m \text{ and } d_1j_1 + d_2j_2 \equiv 0 \mod N.$$

Furthermore, there exists $0 \le j \le 2^m - 1$, *such that* $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$, *equivalently*

$$(d_1 - d_2)j + (2^m - 1)d_2 \equiv 0 \mod N.$$

Proof. Since $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$, we have $\nu_{d_1,d_2} \ge m$ by Eq. (5). For $a \in \mathbb{F}_{2^n} \setminus S_F$, $W_{F_a}(b) = \pm 2^m$ for all $b \in \mathbb{F}_{2^n}$. Hence $\nu_{d_1,d_2} = m$ by Eq. (5) and Theorem 6.

By Lemma 6, for any $(j_1, j_2) \in \mathcal{J}_{d_1,d_2}$, we have $d_1j_1 + d_2j_2 \equiv 0 \bmod N$. Thus the polynomial $g_a(x)$ defined in Theorem 6 is

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2}x^{-(d_1j_1+d_2j_2)} = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2}.$$

By Theorem 6 again, we have $g_a(b) = 1$ for any $a \in \mathbb{F}_{2^n} \setminus S_F$ and $b \in \mathbb{F}_{2^n}$. Since the non-zero polynomial

$$\sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} x^{(j_1+j_2)_N} - 1$$

has $2^n - 2^m$ zeros in $\mathbb{F}_{2^n} \setminus S_F$, its degree is at least $2^n - 2^m$. By Lemma 4(1), its degree must be $2^n - 2^m$. Thus there must exist some $(j_1, j_2) \in \mathcal{J}_{d_1,d_2}$ such that $(j_1 + j_2)_N = 2^n - 2^m$, $\mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = m$ and $d_1j_1 + d_2j_2 \equiv 0 \mod N$.

Suppose

$$j_1 = \sum_{a\in S_1} 2^a, \quad j_2 = \sum_{a\in S_2} 2^a, \quad j_1 + j_2 = \sum_{a\in T} 2^a = 2^n - 2^m \text{ or } 2^{n+1} - 2^m - 1,$$

where $S_1,\ S_2 \subseteq \{0, 1, \cdots, n-1\}$ and $T = \{m, m+1, \cdots, n-1\}$ or $\{0, 1, \cdots, m-1, m+1, \cdots, n-1, n\}$. Then $\#T \le \#S_1 + \#S_2$ with equality if and only if $S_1 \cap S_2 = \emptyset$. By the identity

$$m = \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) = \#S_1 + \#S_2 = \mathrm{wt}_2(j_1 + j_2) \le \#T \le \#S_1 + \#S_2,$$

one has $S_1 \cap S_2 = \emptyset$ and $T = S_1 \cup S_2 = \{m, m+1, \cdots, n-1\}$. Hence, $j_1 + j_2 = (j_1 + j_2)_N = 2^n - 2^m$. This means that $j_1 = 2^m j$ and $j_2 = 2^m(2^m - 1 - j)$ for some j. □

We define the polynomial

$$h_{\mathcal{J}_{d_1,d_2}}(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} x^{j_1+j_2} \in \mathbb{F}_2[x]. \tag{6}$$

Then by Lemma 4 and Theorem 8, we have $\deg h_{\mathcal{J}_{d_1,d_2}}(x) = 2^n - 2^m$. If $\ell(n) > m$, then $S_F = \mathbb{F}_{2^m}$ and $h_{\mathcal{J}_{d_1,d_2}}(a) - 1 = 0$ for all $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ by Theorem 7. Thus

$$h_{\mathcal{J}_{d_1,d_2}}(x) - 1 = \frac{x^{2^n} - x}{x^{2^m} - x} = x^{2^m(2^m-1)} + x^{(2^m-1)^2} + \cdots + x^{2^m-1} + 1,$$

i.e.,

$$h_{\mathcal{J}_{d_1,d_2}}(x) = x^{2^m(2^m-1)} + x^{(2^m-1)^2} + x^{(2^m-1)(2^m-3)} + \cdots + x^{2^m-1}. \tag{7}$$

Corollary 2. *Assume that $\ell(n) > m$, $\#S_F = 2^m$ and $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$. Then*

$$\begin{aligned} V &:= \{j_1 + j_2 : (j_1, j_2) \in \mathcal{J}_{d_1,d_2}\} \\ &\supseteq \{2^m - 1, 2(2^m - 1), 3(2^m - 1), \ldots, 2^m(2^m - 1)\}. \end{aligned}$$

By Theorem 8, there exists $0 \le j \le 2^m - 1$ such that $(j_1, j_2) = (j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$ and

$$(d_2 - d_1)j \equiv d_2(2^m - 1) \mod N. \tag{8}$$

Set $t := \gcd(j, 2^m - 1)$. Then we can write

$$d_2 - d_1 = \frac{2^m - 1}{t} k \tag{9}$$

for some integer k and Eq. (8) becomes

$$\frac{kj}{t} \equiv d_2 \mod (2^m + 1). \tag{10}$$

Set $r := \gcd(k, 2^m + 1)$. By Eqs. (9) and (10), r is a common factor of $d_1 - d_2$, d_2 and N. Thus $r \mid s := \gcd(d_1, d_2, N)$.

- If $s \mid (2^m - 1)$, then $r \mid \gcd(s, 2^m + 1) = 1$ and hence $r = 1$.
- If $s \mid (2^m + 1)$, then $s \mid k$ by Eq. (9). Hence $s \mid r$ and $r = s$.

Let $u := \gcd(t, k)$. Then $\gcd(u, r) = 1$ due to $t \mid (2^m - 1)$ and $r \mid (2^m + 1)$. Hence

$$\gcd(d_2 - d_1, N) = \frac{2^m - 1}{t} \gcd\big(k, t(2^m + 1)\big) = \frac{2^m - 1}{t} ur. \tag{11}$$

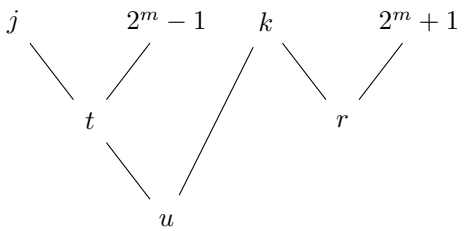

FIGURE 1. Division Relations of t, k, u, r

Theorem 9. *Assume that* $\ell(n) > m$, $\#S_F = 2^m$, $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$, *and* $\gcd(d_1, d_2, N) > 1$. *Then*

$$d_2 - d_1 \equiv 0 \mod (2^m - 1).$$

Proof. By Theorem 7, $S_F = \mathbb{F}_{2^m}$. If $s := \gcd(d_1, d_2, N) > 1$, then $s \mid (2^m + 1)$ or $s \mid (2^m - 1)$ by Lemma 2. Assume that $s \mid (2^m + 1)$. Then $W_{F_a}(0) = -2^m$ for any $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ by Lemma 2. Note that

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) &= \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} W_{F_a}(0) + \sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0)\\ &= -2^m(2^n - 2^m) + \sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0).\end{aligned} \tag{12}$$

By Eqs. (9), we also get

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) &= \sum_{a\in\mathbb{F}_{2^n}} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(ax^{d_1}+ax^{d_2})}\\ &= 2^n + 2^n\#\{x \in \mathbb{F}_{2^n}^* : x^{d_2-d_1} = 1\}\end{aligned}$$

Since $x^{d_2-d_1} = 1 \iff x^{(2^m-1)ur/t} = 1$ by Eq. (11), we have

$$\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) = 2^n + 2^n \cdot \frac{(2^m - 1)ur}{t}. \tag{13}$$

By Eqs. (12) and (13), we have

$$\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) = 2^n + 2^n \cdot \frac{(2^m - 1)ur}{t} + 2^m(2^n - 2^m) > 2^{n+m}, \tag{14}$$

which is impossible since $\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) \le 2^{n+m}$. Hence $s \nmid (2^m + 1)$. This means that

$$s \mid (2^m - 1),\ r = 1, \text{ and } W_{F_a}(0) = 2^m \text{ for any } a \in \mathbb{F}_{2^n} \setminus S_F.$$

Now Eq. (14) becomes

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) &= 2^n + 2^n \cdot \frac{(2^m - 1)t}{u} - 2^m(2^n - 2^m)\\ &= 2^n + 2^n(2^m - 1)\Big(\frac{u}{t} - 1\Big) \le 2^n.\end{aligned}$$

On the other hand,

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{a\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(a\,\mathrm{Tr}_{2^n/2^m}(x^{d_1}+x^{d_2}))}\\ &= 2^m\#\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_{2^n/2^m}(x^{d_1} + x^{d_2}) = 0\} \ge 2^n.\end{aligned}$$

This forces $t = u$. Hence $d_2 - d_1 = \frac{k}{u}(2^m - 1)$ is divisible by $2^m - 1$. □

Under the assumptions in Theorem 9, we may assume that

$$d_2 - d_1 = (2^m - 1)k, \qquad \gcd(k, 2^m + 1) = 1.$$

Then we have

$$s = \gcd(d_1, d_2, N) = \gcd(d_1, d_2 - d_1, N) = \gcd(d_1, (2^m - 1)k, N) = \gcd(d_1, 2^m - 1).$$

Remark 3. *In particular, if $d_1 = 2^i + 1$ and $d_2 = 2^m + 1$, $0 \le i \le m-1$, Xie et al.*[14] *showed that F has the maximal number of bent components if and only if $i = 0$. However, by Theorem 9, we can directly obtain that $i = 0$ if F has the maximal number of bent components and $s = \gcd(2^i + 1, 2^m - 1) > 1$.*

Theorem 10. *Assume that $\ell(n) > m$, $\#S_F = 2^m$, $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$, and $\gcd(d_1, d_2, N) > 1$. Then $F(x)$ is EA-equivalent to $x^{1+2^l} + x^{2^l+2^m}$, where $0 < l < m$.*

Proof. We can assume $d_1 = 1 + 2^l$ and $d_2 = 2^{k_1} + 2^{k_2}$ under EA-equivalent, where $0 < l < m, 0 \le k_1 < k_2 < n$ and $d_1 < d_2$. By Lemma 3, we get $\mathrm{wt}_2(d_2 - d_1) = \mathrm{wt}_2((2^m - 1)k) = m$.

Assume that $l < k_1$. Then

$$d_2 - d_1 = 2^{k_1} - 1 + 2^{k_2} - 2^l = 1 + 2 + \cdots + 2^{l-1} + 2^{l+1} + \cdots + 2^{k_1-1} + 2^{k_2}$$

and $m = \mathrm{wt}_2(d_2 - d_1) = k_1$. Since $d_2 - d_1 = (2^m - 1) + (2^{k_2} - 2^l)$ is divisible by $2^m - 1$, this forces $k_2 = m + l$, i.e., $d_1 = 1 + 2^l, d_2 = 2^m + 2^{m+l}$. This contradicts Proposition 1. Hence $k_1 \le l \le k_2$.

Now

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

and $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$, i.e., $k_2 = m + l - k_1$. Since

$$d_2 - d_1 = 2^{m+l-k_1} + 2^{k_1} - 2^l - 1 = 2^{l-k_1}(2^m - 1) + (2^{k_1} - 1)(1 - 2^{l-k_1}),$$

we obtain that $(2^{k_1} - 1)(2^{l-k_1} - 1)$ is divisible by $2^m - 1$. Since

$$(2^{k_1}-1)(2^{l-k_1}-1) \le (2^{k_1}-1)(2^{m-1-k_1}-1) = 2^{m-1}+1-2^{k-1}-2^{m-1-k_1} < 2^m-1,$$

we have $k_1 = 0$ or $k_1 = l$. If $k_1 = 0$, then $F(x) = x^{1+2^l} + x^{1+2^{l+m}}$ is EA-equivalent to $F(x^{2^{m-l}}) = x^{2^{m-l}+2^m} + x^{1+2^{m-l}}$. If $k_1 = l$, then $F(x) = x^{1+2^l} + x^{2^l+2^m}$. □

5. Bounds on the nonlinearity and differential uniformity

For a vectorial function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the *sum-of-square-indicator* of the component function F_a, $a \in \mathbb{F}_{2^n}^*$, is defined as

$$\nu(F_a) = 2^{-n} \sum_{\omega \in \mathbb{F}_{2^n}} W_{F_a}^4(\omega).$$

The lower bound on $\nu(F_a)$ is given by the following lemma.

Lemma 7 ([1])**.**

$$\sum_{a \in \mathbb{F}_{2^n}^*} \nu(F_a) \ge (2^n - 1)2^{2n+1},$$

and equality holds if and only if F is APN.

Theorem 11. *Assume that $\ell(n) > m$, $\sigma \circ F = F \circ \sigma$ and $\#S_F = 2^m$. Then the nonlinearity of $F(x)$ satisfies*

$$\mathcal{N}_F \le 2^{n-1} - \frac{1}{2}\sqrt{2^n(2^m + 2)}.$$

Furthermore, if F is plateaued, then

$$\mathcal{N}_F \le 2^{n-1} - 2^{\lfloor \frac{3n}{4} \rfloor}.$$

Proof. By Theorem 7 and Lemma 7, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}^*}\nu(F_a) &= \sum_{a\in\mathbb{F}_{2^n}^*}\nu(F_a) - \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}}\nu(F_a)\\ &\geq (2^n-1)2^{2n+1} - 2^{2n}(2^n-2^m) = 2^{2n}(2^n+2^m-2).\end{aligned}$$

By the definition of $\nu(F_a)$, we know

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}^*}\nu(F_a) &\leq 2^{-n}\max_{a\in\mathbb{F}_{2^m}^*,\omega\in\mathbb{F}_{2^n}} W_{F_a}^2(\omega)\sum_{a\in\mathbb{F}_{2^m}^*}\sum_{\omega\in\mathbb{F}_{2^n}} W_{F_a}^2(\omega)\\ &= 2^n(2^m-1)\max_{a\in\mathbb{F}_{2^m}^*,\omega\in\mathbb{F}_{2^n}} W_{F_a}^2(\omega).\end{aligned}$$

Therefore, we have

$$\max_{a\in\mathbb{F}_{2^m}^*,\omega\in\mathbb{F}_{2^n}} W_{F_a}^2(\omega) \geq \frac{2^{2n}(2^n+2^m-2)}{2^n(2^m-1)} = 2^n(2^m+2) \tag{15}$$

and then

$$\mathcal{N}_F = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_{2^n}^*,\omega\in\mathbb{F}_{2^n}}\left|W_{F_a}(\omega)\right| \leq 2^{n-1} - \frac{1}{2}\sqrt{2^n(2^m+2)}.$$

If F is plateaued, then there exists an even integer $k > n+m$ such that

$$\max_{a\in\mathbb{F}_{2^m}^*,\omega\in\mathbb{F}_{2^n}} W_{F_a}^2(\omega) = 2^k$$

by Definition 1(iv) and Eq. (15). This implies that

$$k \geq 2\left\lfloor\frac{n+m}{2}\right\rfloor + 2 = 2\left\lfloor\frac{3n}{4}\right\rfloor + 2.$$

Hence

$$\mathcal{N}_F = 2^{n-1} - 2^{\frac{k}{2}-1} \leq 2^{n-1} - 2^{\lfloor\frac{3n}{4}\rfloor}. \qquad \square$$

Remark 4. *The bound in Theorem 11 is still true for non-plateaued functions, but it may be weaker than the bound given in* [14, Conjecture 1].

Lemma 8. *Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$. Then*

$$\#\{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n} : F(x)=F(y)\} \geq \frac{2^{2n}}{\#\operatorname{Im}(F)}.$$

Proof. For any $b\in\mathbb{F}_{2^n}$, denote by $\#F^{-1}(b)$ the size of the pre-image of b under F. By the Cauchy-Schwarz inequality, we have

$$\text{LHS} = \sum_{b\in\operatorname{Im}(F)}\left(\#F^{-1}(b)\right)^2 \geq \frac{\left(\sum_{b\in\operatorname{Im}(F)}\#F^{-1}(b)\right)^2}{\#\operatorname{Im}(F)} = \frac{2^{2n}}{\#\operatorname{Im}(F)}. \qquad \square$$

We now give a bound which depends on the cardinality of the image set of F.

Theorem 12. *Assume that $\ell(n) > m$, $\sigma\circ F = F\circ\sigma$ and $\#S_F = 2^m$. Set*

$$T := \#\{a\in\mathbb{F}_{2^m}^* : W_{F_a}(0)\neq 0\}.$$

If $\#\operatorname{Im}(F) \leq 2^{n-1}+2^{m-2}$, then

$$\mathcal{N}_F \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{3m}}{T}\left(\frac{2^{3m}}{\#\operatorname{Im}(F)} - 2^{m+1} + 1\right)}.$$

Proof. By Lemma 8, we have

$$\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}^2(0) = 2^n \#\{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n} : F(x)=F(y)\} \geq \frac{2^{3n}}{\#\operatorname{Im}(F)}.$$

Meanwhile,

$$\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}^2(0) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} W_{F_a}^2(0) + \sum_{a\in\mathbb{F}_{2^m}} W_{F_a}^2(0) = 2^n(2^n-2^m) + \sum_{a\in\mathbb{F}_{2^m}} W_{F_a}^2(0).$$

Thus

$$\sum_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0) \geq \frac{2^{3n}}{\#\operatorname{Im}(F)} - 2^{2n+1} + 2^{n+m} > \frac{2^{3n}-2^{2n-2}}{2^{n-1}+2^{m-2}} - 2^{2n+1} + 2^{n+m} = 0$$

and

$$\begin{aligned}\max_{a\in\mathbb{F}_{2^m}^*, v\in\mathbb{F}_{2^n}} W_{F_a}^2(v) &\geq \max_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0) \geq \frac{1}{T}\sum_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0)\\ &\geq \frac{1}{T}\left(\frac{2^{3n}}{\#\operatorname{Im}(F)} - 2^{2n+1} + 2^{n+m}\right).\end{aligned}$$

We thus get the desired bound for $\mathcal{N}_F$. □

Remark 5. *Clearly, $T \leq 2^m - 1$. Hence Theorem 12 implies that*

$$\mathcal{N}_F \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{3m}}{2^m-1}\left(\frac{2^{3m}}{\#\operatorname{Im}(F)} - 2^{m+1} + 1\right)},$$

which is smaller than Carlet's bound $2^{n-1} - \sqrt{\frac{1}{2^n-1}\left(\frac{2^{3n-2}}{\#\operatorname{Im}(F)} - 2^{2n-2}\right)}$ in [2, Proposition 2]. *Moreover, this bound is also smaller than $2^{n-1} - \frac{1}{2}\sqrt{2^n(2^m+2)}$ given by Theorem 11 when $\#\operatorname{Im}(F) \leq \frac{2^{3n}}{3\cdot 2^{2n}-2^{n+1}}$.*

The following bound can be found in [2]. We will provide a whole proof for completeness.

Theorem 13. *For any non-injective vectorial function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we have*

$$\delta_F \geq \left\lceil \frac{2^n}{\#\Delta}\left(\frac{2^n}{\#\operatorname{Im}(F)} - 1\right)\right\rceil,$$

where

$$\Delta = \{x+y : (x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}, x\neq y, F(x)=F(y)\}.$$

Proof. Define

$$\delta_{a,b} := \#\{x\in\mathbb{F}_{2^n} : F(x+a)+F(x)=b\}.$$

Then for any nonzero $a\notin\Delta$, $\delta_{a,0}=0$. By Definition 1 (vi), we have

$$\delta_F \geq \max_{a\in\mathbb{F}_{2^n}^*}\delta_{a,0} \geq \frac{\sum_{a\in\mathbb{F}_{2^n}^*}\delta_{a,0}}{\#\Delta} = \frac{\#\{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n} : F(x)=F(y)\}-2^n}{\#\Delta}.$$

The bound then can be obtained by Lemma 8. □

Remark 6. *From the definition of* Δ*, if* $\ell(n) > m$*,* $\sigma \circ F = F \circ \sigma$ *and* $\#S_F = 2^m$*, then*

$$\begin{aligned}\#\Delta &\le \frac{1}{2}\#\{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : F(x) = F(y)\} - 2^{n-1} \\ &= \frac{1}{2^{n+1}} \sum_{x,y,a \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(a(F(x)+F(y)))} - 2^{n-1} \\ &= \frac{1}{2^{n+1}} \sum_{a \in \mathbb{F}_{2^n}^*} W_{F_a}^2(0) = \frac{1}{2^{n+1}} \sum_{a \in \mathbb{F}_{2^m}^*} W_{F_a}^2(0) + 2^{n-1} - 2^{m-1}.\end{aligned}$$

In [12, Theorem 7]*, we know that* $W_{F_a}(0) = 0$ *for all* $a \in \mathbb{F}_{2^m}^*$ *if* $s = \gcd(d_1, 2^m - 1) = 1$*. Then* $\#\Delta \le 2^{n-1} - 2^{m-1}$ *and*

$$\delta_F \ge \left\lceil \frac{2^n(2^n - \#\,\mathrm{Im}(F))}{(2^{n-1} - 2^{m-1})\#\,\mathrm{Im}(F)} \right\rceil \ge \left\lceil \frac{2^{n+1}}{\#\,\mathrm{Im}(F)} \right\rceil - 2.$$

We next give the differential uniformity and the cardinality of the image set of binomial vectorial function $F(x) = x^{d_1} + x^{d_2} \in \mathbb{F}_{2^n}[x]$ with $d_2 - d_1 = (2^m - 1)k$ and $\gcd(k, 2^m + 1) = 1$.

Theorem 14. *Suppose* $\mathbb{F}_{2^n}^* = \langle \alpha \rangle$*,* $d_2 - d_1 = (2^m - 1)k$ *and* $\gcd(k, 2^m + 1) = 1$*. Then*

$$\delta_F \ge 2^m \quad \textit{and} \quad \#\,\mathrm{Im}(F) = \frac{(2^m - 1)c}{s} + 1,$$

where $c = \#\{F(\alpha^i)^{(2^m-1)/s} : \ i = 1, 2, \ldots, 2^m\}$.

Proof. Note that $F^{-1}(0) = \mathbb{F}_{2^m}$ and

$$F(x+a) + F(x) = (x+a)^{d_1}\big(1 + (x+a)^{(2^m-1)k}\big) + x^{d_1}\big(1 + x^{(2^m-1)k}\big).$$

If $a \in \mathbb{F}_{2^m}^*$, we then get $F(x+a)+F(x) = 0$ for all $x \in \mathbb{F}_{2^m}$. Therefore, $\delta_{a,0} \ge 2^m$. By Definition 1(vi), we have

$$\delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_{a,b} \ge \delta_{a,0} \ge 2^m.$$

If $x \in \alpha^i \mathbb{F}_{2^m}^*$, then

$$F(x) = x^{d_1}(1 + x^{d_2 - d_1}) = x^{d_1}(1 + x^{(2^m-1)k}) = x^{d_1} f(\alpha^{(2^m-1)i}),$$

where $f(x) = 1 + x^k$. Let

$$D = \langle \alpha^{(2^m+1)s} \rangle \subseteq \mathbb{F}_{2^m}^*$$

be the image of the map $x^{d_1} : \mathbb{F}_{2^m}^* \mapsto \mathbb{F}_{2^m}^*$. Then x^{d_1} maps each coset $\alpha^i \mathbb{F}_{2^m}^*$ onto $\alpha^{d_1 i} D$, and the image of the map

$$F : \alpha^i \mathbb{F}_{2^m}^* \mapsto \alpha^{d_1 i} f(\alpha^{(2^m-1)i}) D = F(\alpha^i) D$$

is the set $\{0\}$ or a coset of D. Note that $F(\alpha^i)D = F(\alpha^j)D$ if and only if $F(\alpha^i)^{(2^m-1)/s} = F(\alpha^j)^{(2^m-1)/s}$. Hence,

$$\#\,\mathrm{Im}(F) = 1 + c\#D = 1 + \frac{(2^m - 1)c}{s}.$$

This completes the proof. □

By Theorems 12-14, we have

Corollary 3. *Adopt the same notations as Theorem 14. Then the nonlinearity and differential uniformity of F satisfy*

$$\mathcal{N}_F \le 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{3m}}{T}\cdot\left(\frac{2^{3m}s}{s+(2^m-1)c} - 2^{m+1}+1\right)},$$
$$\delta_F \ge \left\lceil \frac{2^n}{\#\Delta}\left(\frac{2^n s}{s+(2^m-1)c} - 1\right)\right\rceil.$$

Remark 7. *Since $s = \gcd(d_1, 2^m-1) \ge 3$ and*

$$s + (2^m-1)c \le s + 2^m(2^m-1) < (2^m+1)(2^m-1) = 2^n - 1,$$

we have

$$\begin{aligned}&\frac{2^{3m}}{T}\cdot\left(\frac{2^{3m}s}{s+(2^m-1)c} - 2^{m+1}+1\right)\\ &\quad> \frac{2^{3m}}{2^m-1}\left(\frac{2^{3m}s}{2^n-1} - 2^{m+1}+1\right) > \frac{2^{2n}(s-2)+2^{n+m}}{2^m-1}\\ &\quad\ge \frac{2^{2n}+2^{n+m}}{2^m-1} > 2^n(2^m+2).\end{aligned}$$

Thus the bound of $\mathcal{N}_F$ in Corollary 3 is smaller than $2^{n-1} - \frac{1}{2}\sqrt{2^n(2^m+2)}$. Moreover, we get

$$\delta_F \ge \left\lceil \frac{2^n s}{s+(2^m-1)c} - 1\right\rceil \ge \left\lceil \frac{2^n s}{2^n-1} - 1\right\rceil \ge s-1.$$

In particular, for $d_1 = 1, d_2 = 2^{m-1}(2^m+1)$ and $d_1 = 2^l+1, d_2 = 2^m+2^l$, we can determine $\mathrm{Im}(F)$ explicitly. This will a bound for $\mathcal{N}_F$.

Theorem 15. *Let $F(x) = x^{2^l+1} + x^{2^l+2^m}$ and $d = \gcd(l,m)$.*

1. *If $v_2(m) \le v_2(l)$, then F is a bijection on $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.*
2. *If $v_2(m) > v_2(l)$, then F is a (2^d+1)-to-1 map from $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ onto*

$$\left\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} : \mathrm{Tr}_{2^n/2^m}(y) \in (\mathbb{F}_{2^m}^*)^{2^d+1}\right\}.$$

Proof. Let $\mathrm{Tr} = \mathrm{Tr}_{2^n/2^m}$. Then $F(x) = x^{2^l}\,\mathrm{Tr}(x)$. If $x \in \mathbb{F}_{2^m}$, then $\mathrm{Tr}(x) = 0$ and $F(x) = 0$.

If $F(x) = y \notin \mathbb{F}_{2^m}$, then $x \ne 0, \mathrm{Tr}(x) = x^{-2^l}y$ and

$$\mathrm{Tr}(y^{2^{n-l}}) = \mathrm{Tr}\big(x\,\mathrm{Tr}(x)^{2^{n-l}}\big) = \mathrm{Tr}(x)^{1+2^{n-l}}$$

belongs to

$$D := \{u^{1+2^{n-l}} : u \in \mathbb{F}_{2^m}^*\} \subseteq \mathbb{F}_{2^m}^*,$$

which is equivalent to $\mathrm{Tr}(y) \in D$. Since

$$\gcd(2^{n-l}+1, 2^m-1) = \gcd(2^l+1, 2^m-1) = \begin{cases} 1, & \text{if } v_2(m) \le v_2(l);\\ 2^d+1, & \text{if } v_2(m) > v_2(l),\end{cases}$$

we have $D = \mathbb{F}_{2^m}^*$ or $(\mathbb{F}_{2^m}^*)^{2^d+1}$.

If $\mathrm{Tr}(y^{2^{n-l}}) = u^{1+2^{n-l}}$, then $\mathrm{Tr}(x) = u\zeta$ for some ζ in

$$H := \{\zeta \in \mathbb{F}_{2^m}^* : \zeta^{1+2^{n-l}} = 1\} \subseteq \mathbb{F}_{2^m}^*,$$

which has cardinality $\#H = [\mathbb{F}_{2^m}^* : D]$. Thus

$$x = \left(\frac{y}{\mathrm{Tr}(x)}\right)^{2^{n-l}} = \left(\frac{y}{u\zeta}\right)^{2^{n-l}} = \frac{\zeta y^{2^{n-l}}}{u^{2^{n-l}}}$$

lies in the pre-image of y, which has $\#H$ possible values. Hence we obtain the result. □

We need the following result to calculate $W_{F_a}(0)$.

Theorem 16 ([3, Theorems 4.1,5.2])**.** *Let $d = \gcd(m, l)$ and $s = 2^d + 1$. Then*

$$\sum_{z\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(az^s)} = \begin{cases} 0, & \text{if } v_2(m) \le v_2(l); \\ (-1)^{\frac{m}{2d}} 2^{\frac{m}{2}}, & \text{if } v_2(m) > v_2(l), a \in \mathbb{F}_{2^m}^* \setminus (\mathbb{F}_{2^m}^*)^s; \\ -(-1)^{\frac{m}{2d}} 2^{\frac{m}{2}+d}, & \text{if } v_2(m) > v_2(l), a \in (\mathbb{F}_{2^m}^*)^s. \end{cases}$$

Theorem 17. *Let $F(x) = x^{2^l+1} + x^{2^l+2^m}$.*

(1) *If $v_2(m) \le v_2(l)$, then $\mathcal{N}_F \le 2^{n-1} - 2^{m-1}$.*
(2) *If $v_2(m) > v_2(l)$, then $\mathcal{N}_F \le 2^{n-1} - 2^{\frac{3m}{2}+d-1}$, where $d = \gcd(l, m)$.*

Proof. Let $\mathrm{Tr} = \mathrm{Tr}_{2^n/2^m}$ and

$$s = \gcd(2^l + 1, 2^m - 1) = \begin{cases} 1, & \text{if } v_2(m) \le v_2(l); \\ 2^d + 1, & \text{if } v_2(m) > v_2(l). \end{cases}$$

If $a = 0$, then clearly $W_{F_a}(0) = 2^n$. Assume that $a \neq 0$. Let $\widehat{\mathbb{F}}_{2^m}^*$ be the set of the multiplicative characters of $\mathbb{F}_{2^m}^*$. By Theorem 15, we have

$$\begin{aligned} W_{F_a}(0) &= \sum_{v\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(aF(v))} = 2^m + \sum_{v\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^n/2}(aF(v))} \\ &= 2^m + s \sum_{\mathrm{Tr}(y)\in(\mathbb{F}_{2^m}^*)^s} (-1)^{\mathrm{Tr}_{2^n/2}(ay)} \\ &= 2^m + \sum_{\chi^s=1} \sum_{y\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^n/2}(ay)} \chi\big(\mathrm{Tr}(y)\big), \end{aligned}$$

where $\chi \in \widehat{\mathbb{F}}_{2^m}^*$. Take $\beta \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}(\beta) = 1$. Then any $y \in \mathbb{F}_{2^n}$ can be written as $y = x + \beta u$, where $x, u = \mathrm{Tr}(y) \in \mathbb{F}_{2^m}$. Thus

$$\begin{aligned} W_{F_a}(0) &= 2^m + \sum_{\chi^s=1} \sum_{x\in\mathbb{F}_{2^m}} \sum_{u\in\mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^n/2}(a(x+\beta u))} \chi(u) \\ &= 2^m + \sum_{\chi^s=1} \Bigg(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^n/2}(ax)} \cdot \sum_{u\in\mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^n/2}(a\beta u)} \chi(u) \Bigg). \end{aligned}$$

If $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, then $W_{F_a}(0) = 2^m$ by [12]. If $a \in \mathbb{F}_{2^m}^*$, then

$$\begin{aligned} W_{F_a}(0) &= 2^m + s \sum_{\mathrm{Tr}(y)\in(\mathbb{F}_{2^m}^*)^s} (-1)^{\mathrm{Tr}_{2^n/2}(ay)} \\ &= 2^m + s2^m \sum_{z\in(\mathbb{F}_{2^m}^*)^s} (-1)^{\mathrm{Tr}_{2^m/2}(az)} = 2^m \sum_{z\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(az^s)}. \end{aligned}$$

By Theorem 16, we conclude that

$$W_{F_a}(0)=\begin{cases}2^n, & \text{if } a=0;\\ 2^m, & \text{if } a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m};\\ 0, & \text{if } v_2(m)\le v_2(l);\\ (-1)^{\frac{m}{2d}}2^{\frac{3m}{2}}, & \text{if } v_2(m)>v_2(l), a\in\mathbb{F}_{2^m}^*\setminus(\mathbb{F}_{2^m}^*)^s;\\ -(-1)^{\frac{m}{2d}}2^{\frac{3m}{2}+d}, & \text{if } v_2(m)>v_2(l), a\in(\mathbb{F}_{2^m}^*)^s.\end{cases}$$

The estimate of $\mathcal{N}_F$ then follows. □

6. Conclusion

In this paper, we use Stickelberger's Theorem to study the Walsh transform of binomial vectorial function $F(x)=x^{d_1}+x^{d_2}$, and show that $F(x)$ is equivalent to x^{2^m+1} when $\mathrm{wt}_2(d_1)=1$, and to $x^{2^i+1}+x^{2^m+2^i}$ when $\mathrm{wt}_2(d_1)=\mathrm{wt}_2(d_2)=2$ under a technical condition, where $0<i\le m-1$. Moreover, we give the cardinality of the image set of F, and then give the bounds on the nonlinearity and differential uniformity of $F(x)$ by means of the cardinality of its image set.

References

[1] N. Anbar, T. Kalaycı, W. Meidl and L. Mérai, "On a class of functions with the maximal number of bent components." *IEEE Trans. Inf. Theory*, **68**(9), 6174–6186 (2022).

[2] C. Carlet, "Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions." *IEEE Trans. Inf. Theory*, **67**(12), 8325–8334 (2021).

[3] R. Coulter, "On the evaluation of a class of Weil sums in characteristic 2." *New Zealand J. Math.*, **28**, 171–184 (1999).

[4] H. Hu and D. Feng, "On quadratic bent functions in polynomial forms." *IEEE Trans. Inf. Theory*, **53**(7), 2610–2615 (2007).

[5] H. Hu, B. Wang, X. Xie and Y. Luo, "An open problem about monomial bent functions." *IEEE Trans. Inf. Theory*, **69**(12), 8111–8115 (2023).

[6] P. Langevin and G. Leander, "Monomial bent functions and Stickelberger's theorem." *Finite Fields Appl.*, **14**(3), 727–742 (2008).

[7] P. Langevin, G. Leander, G. Mcguire and E. Zalinescu, "Analysis of Kasami-Welch functions in odd dimension using Stickelberger's theorem." *J. Comb. Number Theory*, **2**(1), 55–72 (2011).

[8] P. Langevin and P. Véron, "On the nonlinearity of power functions." *Designs Codes Cryptogr.*, **37**, 31–43 (2005).

[9] N. G. Leander, "Normality of bent functions, monomial and binomial bent functions." Ph.D. thesis, Dept. Math., Ruhr-Univ. Bochum, Bochum, Germany, (2004).

[10] S. Mesnager, F. Zhang, C. Tang and Y. Zhou, "Further study on the maximum number of bent components of vectorial functions." *Des., Codes Cryptogr.*, **87**, 2597–2610 (2019).

[11] O. Moreno, K. Shum, F. Castro, P. Kumar, "Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications." *Proc. London Soc.*, **3**(88), 545–564 (2004).

[12] A. Pott, E. Pasalic, A. Muratovic and S. Bajric, "On the maximum number of bent components of vectorial functions." *IEEE Trans. Inf. Theory*, **64**(1), 403–411 (2018).

[13] J. Stickelberger, "Úber eine Verallgemeinerung der Kreistheilung." *Math. Ann.*, **37**, 321–367 (1890).

[14] X. Xie, Y. Ouyang and H. Hu, "On vectorial functions with maximal number of bent components." *Des. Codes Cryptogr.*, **93**, 1889–1910 (2025).

[15] L. Zheng, J. Peng, H. Kan, Y. Li and J. Luo, "On constructions and properties of (n,m)-functions with maximal number of bent components." *Des. Codes Cryptogr.*, **88**(9), 2171–2186 (2020).

[1]School of Information and Computer, Anhui Agricultural University, Hefei 230036, China
Email address: xianhxie@ahau.edu.cn

[2]School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China

[3]Hefei National Laboratory, Hefei 230088, China
Email address: yiouyang@ustc.edu.cn

[4]School of Mathematics, Hefei University of Technology, Hefei 230601, China

[5]State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
Email address: zhangshenxing@hfut.edu.cn