

ON QUADRATIC BINOMIAL VECTORIAL FUNCTIONS WITH MAXIMAL BENT COMPONENTS

XIANHONG XIE¹, 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 binary Hamming weights $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$. We prove that $F(x)$ is EA-equivalent to $x^{2^l+1} + x^{2^l+2^m}$ for some $0 < l < m$, provided that $\gcd(d_1, d_2, 2^n - 1) > 1$. We also establish several bounds on the nonlinearity and the differential uniformity of general vectorial functions by means of the cardinality of related sets.

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 $\text{Tr}_{2^i/2}$ 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 $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is a vectorial function. For $a \in \mathbb{F}_{2^n}$, let F_a be the component function

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

Let

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

In 2018, Pott et al. [PPM+18] 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 [AKM+22, HWX+23, MZT+19, XOH25, ZPK+20] 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.

Considerable progress has been made in the study of functions attaining the maximal number of bent components. In 2023, Hu et al. [HWX+23] established that the monomials $x^{2^l(2^m+1)}$ 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. [PPM+18] demonstrated that $F(x)$ achieves this bound when $d_1 = 2^l + 1$ and $d_2 = 2^l + 2^m$ ($0 \leq l \leq m - 1$). More recently, Xie et al. [XOH25] refined this analysis for the specific family $F(x) = x^{2^l+1} + x^{2^m+1}$ ($0 \leq l \leq m - 1$), proving it attains the bound if and only if $l = 0$. Furthermore, for general exponents (d_1, d_2) ,

Date: October 7, 2026.

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

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

computational evidence using Magma presented in [XOH25] suggests that any such binomial $F(x)$ is EA-equivalent to either x^{2^m+1} or $x^{2^l+1} + x^{2^l+2^m}$ if it has the maximal number of bent components. However, a proof of this assertion remains elusive.

Anbar et al. [AKM+22] 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. [XOH25] 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 [HWX+23, LL08, LLM+11, LV05]. 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 a monomial x^{d_2} , which is a known case in [HWX+23]. Our contributions can be summarized as follows.

(A). Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. If F has $2^n - 2^m$ bent components, $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, and $\gcd(d_1, d_2, N) > 1$, then $F(x)$ is EA-equivalent to $x^{2^l+1} + x^{2^l+2^m}$. See Theorem 4.5. This generalizes the results in [XOH25, Theorem 9] and [ZPK+20, Theorem 4.16].

(B). We establish theoretical bounds on the nonlinearity and differential uniformity of general functions F over $\mathbb{F}_{2^n}$:

$$\mathcal{N}_F \leq 2^{n-1} - 2^{m-1} \sqrt{\frac{2^n - 1}{\#S_F - 1}} + 1.$$

If $T := \#\{0 \neq a \in S_F : W_{F_a}(0) \neq 0\}$ is non-empty and $\#\text{Im}(F) \leq 2^{n-1} + 2^{m-2}$, then

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

If F has no nonzero affine component, then

$$\mathcal{N}_F \geq 2^{n - \max_{0 \neq a \in S_F} \deg F_a}.$$

If F is not injective, then

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

where $\Delta = \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, x \neq y, F(x) = F(y)\}$. See Theorems 5.4, 5.8, 5.11 and 5.12. If $F(x) = x^{2^l+1} + x^{2^l+2^m}$ with $v_2(m) > v_2(l)$, then

$$\mathcal{N}_F \leq 2^{n-1} - 2^{\frac{3m}{2} + \gcd(l, m) - 1}.$$

See Theorem 5.1.

The paper is organized as follows. In Section 2, we provide some necessary preliminaries. In Section 3, we establish further properties of binomial vectorial functions with the maximal number of bent components. In Section 4, we derive equivalent forms of $F(x)$ for the cases where $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$. In Section 5, we give several estimates on the nonlinearity and differential uniformity. In Section 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 2.1. Suppose that $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is a vectorial function.

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

$$F_a : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$$

$$v \longmapsto \text{Tr}_{2^n/2}(a \cdot F(v)).$$

- (ii) The Walsh transform of F is

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

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 $k \equiv n \pmod{2}$, 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. [PPM+18] proved the following result.

Theorem 2.2. $\#S_F \geq 2^m$. 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 2.3. If $F(x) = x^{d_1}$ has the maximal number of bent components, then

- (1) (Zheng et al. [ZPK+20]) $S_F = \mathbb{F}_{2^m}$ and $(2^m + 1) \mid d_1$;
- (2) (Hu et al. [HWX+23]) $d_1 = 2^i(2^m + 1)$, where $0 \leq i \leq m - 1$.

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

$$\omega(a) \bmod 2 = a, \quad a \in \mathbb{F}_{2^n}. \quad (2.1)$$

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 :

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

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 2.4. 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 $\psi(x) = (-1)^{\text{Tr}_{2^n/2}(x)}$ 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 non-trivial. For any $x \in \mathbb{F}_{2^n}^*$, applying the inverse Fourier transform, we obtain

$$\psi(x) = \frac{1}{N} \sum_{\chi \in \widehat{\mathbb{F}_{2^n}^*}} G(\chi) \chi^{-1}(x) = \frac{1}{N} \sum_{j=0}^{N-1} G(\omega^{-j}) \omega^j(x). \quad (2.2)$$

We identify $\mathbb{Z}_N$ with the set $\{0, 1, \dots, N-1\}$. 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 $\text{wt}_2(j)$ denote its binary Hamming weight, namely

$$\text{wt}_2(j) = \sum_{i=0}^k c_i, \quad \text{where } j = \sum_{i=0}^k c_i 2^i$$

is the binary representation of j . If $0 \leq j < N$, then

$$N - j = \sum_{i=0}^{n-1} (1 - c_i) 2^i \quad \text{and} \quad \text{wt}_2(N - j) = \sum_{i=0}^{n-1} (1 - c_i) = n - \text{wt}_2(j).$$

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

Theorem 2.5 ([Sti90]). *For any $0 \leq i < N$,*

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

3. BINOMIAL VECTORIAL FUNCTIONS WITH THE MAXIMAL BENT COMPONENTS

From now on, let

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

be a binomial vectorial function, where $0 < d_1, d_2 < N$. 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. [PPM+18].

Theorem 3.1. *For $0 \leq l \leq m-1$, the function $F(x) = x^{2^l+1} + x^{2^l+2^m}$ has $2^n - 2^m$ bent components.*

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

Replacing l by $m-l$ in [Theorem 3.1](#), we obtain that $F(x) = x^{2^{m-l}+1} + x^{2^{m-l}+2^m}$ ($0 \leq l \leq m-1$) has $2^n - 2^m$ bent components. Set

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

Then $x^{2^{m-l}+1} + x^{2^{m-l}+2^m}$ is EA-equivalent to $x^{2^l+1} + x^{2^{m+l}+1}$. We obtain the following corollary.

Corollary 3.2. *For $0 \leq l \leq m-1$, the function $F(x) = x^{2^l+1} + x^{2^{m+l}+1}$ has $2^n - 2^m$ bent components.*

On the other hand, replacing $2^l + 2^m$ by $2^{m+l} + 2^m$ leads to the following result.

Proposition 3.3. *For $0 \leq l \leq m$, the number of bent components of $F(x) = x^{2^l+1} + x^{2^{m+l}+2^m}$ is not maximal.*

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

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

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

Let $L_a(x) := ax^{2^l} + (ax)^{2^{n-l}} + a^{2^{m-l}}x^{2^{n-l}} + a^{2^m}x^{2^l}$. By a result of Hu and Feng [HF07], $F_a(x)$ 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 $\text{Tr}_{2^n/2^m}$ is surjective, so there exists $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ such that $\text{Tr}_{2^n/2^m}(a) = a + a^{2^m} = 1$. For such a , $L_a(1) = 0$, hence F_a is not bent. $\square$

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

$$\begin{aligned} V_{d_1, d_2} &:= \left\{ (j_1, j_2) \in \mathcal{J} \mapsto \text{wt}_2(j_1) + \text{wt}_2(j_2) + \text{wt}_2((-d_1j_1 - d_2j_2)_N) \right\}; \\ \nu_{d_1, d_2} &:= \min\{V_{d_1, d_2}(j_1, j_2) : (j_1, j_2) \in \mathcal{J}\}; \\ \mathcal{J}_{d_1, d_2} &:= \{(j_1, j_2) \in \mathcal{J} : V_{d_1, d_2}(j_1, j_2) = \nu_{d_1, d_2}\}. \end{aligned} \tag{3.1}$$

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

Theorem 3.5. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. Let $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.*

- (1) We have $v_2(W_{F_a}(b)) \geq \nu_{d_1, d_2}$.
 (2) Denote the polynomial

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

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

$$v_2(W_{F_a}(b)) > \nu_{d_1, d_2} \iff g_a(b) = 0. \quad (3.2)$$

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

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

where S is given as follows by [Eq. \(2.2\)](#):

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

Since $N = 2^n - 1 \equiv -1 \pmod{2^n}$, one has

$$W_{F_a}(b) \equiv \sum_{(j_1, j_2) \in \mathcal{J}} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1 j_1 + d_2 j_2})\omega^{j_1+j_2}b^{-d_1 j_1 - d_2 j_2} \pmod{2^n}.$$

By [Theorem 2.5](#) and [Eq. \(3.1\)](#), we get

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

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

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. \(2.1\)](#),

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

and we have

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

This completes the proof. $\square$

Remark 3.6. 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 in [LV05, Lea04], where it was shown that for $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we have $v_2(W_{F_a}(b)) \geq \nu_{d_1,0}$. Moreover,

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

By [MSC+04, Theorem 13], we have the following estimate on ν_{d_1,d_2} .

Lemma 3.7. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$,*

$$v_2(W_{F_a}(b)) \geq \nu_{d_1,d_2} \geq \left\lceil \frac{n}{\max\{\text{wt}_2(d_1), \text{wt}_2(d_2)\}} \right\rceil. \quad (3.3)$$

3.3. Auxiliary results.

Lemma 3.8. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. 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

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

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

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

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. $\square$

Lemma 3.9 ([LL08, Lemma 2]). *If $0 < j < N$, then $\text{wt}_2(j) + \text{wt}_2(N - j) = n$. Moreover, if $(2^m + 1) \nmid j$, then $\text{wt}_2((2^m - 1)j)_N = m$.*

Lemma 3.10. *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 $j_1 + j_2$ is a multiple of $2^m - 1$, $j_1 + j_2 \neq N$, and $V_{d_1,d_2}(j_1, j_2) = m$, then*

$$\text{wt}_2(j_1) + \text{wt}_2(j_2) = \text{wt}_2((j_1 + j_2)_N) = m, \quad d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}.$$

Proof. (1) Write $(j_1 + j_2)_N = N - u$. Then $0 < u \leq 2^m - 2$ and thus

$$\begin{aligned} V_{d_1,d_2}(j_1, j_2) &\geq \text{wt}_2(j_1) + \text{wt}_2(j_2) \geq \text{wt}_2(j_1 + j_2) \\ &\geq \text{wt}_2(N - u) = n - \text{wt}_2(u) \geq m + 1. \end{aligned}$$

(2) If $j_1 + j_2$ is a multiple of $2^m - 1$ and $j_1 + j_2 \neq N$, then $\text{wt}_2((j_1 + j_2)_N) = m$ by [Lemma 3.9](#). Thus

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

Moreover, $V_{d_1, d_2}(j_1, j_2) = m$ if and only if

$$d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}, \quad \text{wt}_2(j_1) + \text{wt}_2(j_2) = \text{wt}_2((j_1 + j_2)_N) = m. \quad \square$$

4. THE EQUIVALENCE OF QUADRATIC BINOMIAL VECTORIAL FUNCTIONS WITH THE MAXIMAL BENT COMPONENTS

In this section, we proceed to show the equivalence for the case where

$$F(x) = x^{d_1} + x^{d_2}, \quad \text{wt}_2(d_1) = \text{wt}_2(d_2) = 2.$$

Lemma 4.1. *Assume that $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$. If $V_{d_1, d_2}(j_1, j_2) = m$, then*

$$\text{wt}_2(j_1) + \text{wt}_2(j_2) = m \quad \text{and} \quad d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}.$$

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

$$\begin{aligned} \text{wt}_2(j_1) + \text{wt}_2(j_2) &= m - \text{wt}_2((-d_1 j_1 - d_2 j_2)_N) = \text{wt}_2((d_1 j_1 + d_2 j_2)_N) - m \\ &\leq \text{wt}_2(d_1 j_1) + \text{wt}_2(d_2 j_2) - m \leq 2 \text{wt}_2(j_1) + 2 \text{wt}_2(j_2) - m. \end{aligned}$$

Thus $\text{wt}_2(j_1) + \text{wt}_2(j_2) \geq m$. This implies that $\text{wt}_2(j_1) + \text{wt}_2(j_2) = m$ because $\text{wt}_2(j_1) + \text{wt}_2(j_2) \leq V_{d_1, d_2}(j_1, j_2) = m$. Then we have $\text{wt}_2((-d_1 j_1 - d_2 j_2)_N) = 0$, which contradicts $d_1 j_1 + d_2 j_2 \not\equiv 0 \pmod{N}$. Hence $d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}$ and $\text{wt}_2(j_1) + \text{wt}_2(j_2) = m$. $\square$

Theorem 4.2. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. If F has $2^n - 2^m$ bent components, $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, then $\nu_{d_1, d_2} = m$ and there exists $(j_1, j_2) \in \mathcal{J}_{d_1, d_2}$ such that*

$$\text{wt}_2(j_1) + \text{wt}_2(j_2) = m \quad \text{and} \quad d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}.$$

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

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

Proof. Since $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, we have $\nu_{d_1, d_2} \geq m$ by [Eq. \(3.3\)](#). 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. \(3.3\)](#) and [Theorem 3.5](#).

By [Lemma 4.1](#), for any $(j_1, j_2) \in \mathcal{J}_{d_1, d_2}$, we have $d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}$. Thus the polynomial $g_a(x)$ defined in [Theorem 3.5](#) is

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

By [Theorem 3.5](#) 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 3.10\(1\)](#), 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 $(j_1 + j_2)_N = 2^n - 2^m$, $\text{wt}_2(j_1) + \text{wt}_2(j_2) = m$ and $d_1 j_1 + d_2 j_2 \equiv 0 \pmod{N}$.

If $j_1 + j_2 \geq N$, then

$$j_1 + j_2 = 2^n - 2^m + N = 2^{n+1} - 2^m - 1$$

and

$$\text{wt}_2(j_1 + j_2) = n > m = \text{wt}_2(j_1) + \text{wt}_2(j_2),$$

a contradiction. Hence $j_1 + j_2 = 2^n - 2^m = (j_1 + j_2)_N$. This means that $j_1 = 2^m j$ and $j_2 = 2^m(2^m - 1 - j)$ for some $0 \leq j \leq 2^m - 1$. $\square$

Theorem 4.3. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. If F has $2^n - 2^m$ bent components, $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, and $\gcd(d_1, d_2, N) > 1$, then*

$$d_2 - d_1 \equiv 0 \pmod{(2^m - 1)}.$$

Proof. By Theorem 4.2, there exists $0 \leq j \leq 2^m - 1$ such that

$$(j_1, j_2) = (j, 2^m - 1 - j) \in \mathcal{J}_{d_1, d_2}$$

and

$$(d_2 - d_1)j \equiv d_2(2^m - 1) \pmod{N}. \quad (4.1)$$

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

$$d_2 - d_1 = \frac{2^m - 1}{t} k \quad (4.2)$$

for some integer k and Eq. (4.1) becomes

$$\frac{kj}{t} \equiv d_2 \pmod{(2^m + 1)}. \quad (4.3)$$

Set $r := \gcd(k, 2^m + 1)$. By Eqs. (4.2) and (4.3), 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. (4.2). 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

$$\gcd(d_2 - d_1, N) = \frac{2^m - 1}{t} \gcd(k, t(2^m + 1)) = \frac{2^m - 1}{t} ur. \quad (4.4)$$

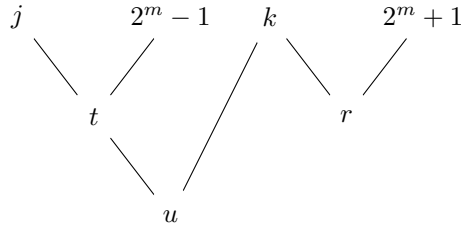


FIGURE 1. Division relations of t, k, u, r

By Eq. (4.2), we get

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

Since $x^{d_2-d_1} = 1 \iff x^{(2^m-1)ur/t} = 1$ by [Eq. \(4.4\)](#), we have

$$\sum_{a \in \mathbb{F}_{2^n}} W_{F_a}(0) = 2^n + 2^n \cdot \frac{(2^m-1)ur}{t}. \quad (4.5)$$

If $s > 1$, then $s \mid (2^m+1)$ or $s \mid (2^m-1)$ by [Lemma 3.8](#). If $s \mid (2^m+1)$, then $W_{F_a}(0) = -2^m$ for any $a \in \mathbb{F}_{2^n} \setminus S_F$ by [Lemma 3.8](#). Thus

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

which is impossible since $|W_{F_a}(0)| \leq 2^n$. Hence $s \nmid (2^m+1)$, which means that $s \mid (2^m-1)$, $r = 1$, and $W_{F_a}(0) = 2^m$ for any $a \in \mathbb{F}_{2^n} \setminus S_F$. Therefore,

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

Let

$$S_F^\perp = \{y \in \mathbb{F}_{2^n} : \text{Tr}_{2^n/2}(ay) = 0, \forall a \in S_F\}$$

be the orthogonal subspace of S_F with respect to the absolute-trace pairing. Then

$$\sum_{a \in S_F} (-1)^{F_a(v)} = \sum_{a \in S_F} (-1)^{\text{Tr}_{2^n/2}(aF(v))} = \begin{cases} 2^m, & \text{if } F(v) \in S_F^\perp; \\ 0, & \text{if } F(v) \notin S_F^\perp. \end{cases}$$

Thus

$$\sum_{a \in S_F} W_{F_a}(0) = \sum_{v \in \mathbb{F}_{2^n}} \sum_{a \in S_F} (-1)^{F_a(v)} = 2^m \# S_F^\perp \geq 2^m.$$

Since $\sum_{a \in S_F} W_{F_a}(0)$ is a multiple of 2^n , it must be 2^n by the above two estimates. This forces $t = u$. Hence $d_2 - d_1 = \frac{k}{u}(2^m - 1)$ is divisible by $2^m - 1$. $\square$

Under the conditions in [Theorem 4.3](#), we assume that

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

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

Remark 4.4. In particular, if $d_1 = 2^i + 1$ and $d_2 = 2^m + 1$, $0 \leq i \leq m-1$, Xie et al. [\[XOH25\]](#) showed that F has the maximal number of bent components if and only if $i = 0$. However, by [Theorem 4.3](#), 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 4.5. *Let $F(x) = x^{d_1} + x^{d_2}$ be a binomial on $\mathbb{F}_{2^n}$ where $0 < d_1, d_2 < N$. If F has $2^n - 2^m$ bent components, $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, and $\gcd(d_1, d_2, N) > 1$, then $F(x)$ is EA-equivalent to $x^{2^{l'}+1} + x^{2^{k_1}+2^{k_2}}$ for some $0 < l < m$.*

Proof. Since $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$, we have $m > 1$. Up to an EA-equivalence, we may assume that $d_1 = 1 + 2^l$ and $d_2 = 2^{k_1} + 2^{k_2}$ for some $0 < l \leq m$, $0 \leq k_1 < k_2 < n$. Let $0 \leq l', k'_1, k'_2 \leq m-1$ such that

$$l' \equiv l, \quad k'_1 \equiv k_1, \quad k'_2 \equiv k_2 \pmod{m}.$$

Then

$$1 + 2^{l'} \equiv d_1 \equiv d_2 \equiv 2^{k'_1} + 2^{k'_2} \pmod{2^m - 1}$$

by [Theorem 4.3](#). Since $1 \leq 1 + 2^{l'}, 2^{k'_1} + 2^{k'_2} \leq 2^m - 1$ and they are congruent modulo $2^m - 1$, we have $1 + 2^{l'} = 2^{k'_1} + 2^{k'_2}$.

If $l = m$, $l' = 0$, then $k'_1 = k'_2 = 0$ and $d_2 = 1 + 2^m = d_1$, which is impossible. Thus $l < m$ and

$$\{0, l'\} \equiv \{k'_1, k'_2\} \pmod{m}.$$

Thus

- If $F(x) = x^{2^l+1} + x^{2^{l+m}+1}$, then $F(x)$ is EA-equivalent to $F(x)^{2^{m-l}} = x^{2^{m-l}+1} + x^{2^{m-l}+2^m}$.
- If $F(x) = x^{2^l+1} + x^{2^{l+m}+2^m}$, then F does not have $2^n - 2^m$ bent components by [Proposition 3.3](#).

Hence $F(x)$ is EA-equivalent to $x^{2^l+1} + x^{2^{l+m}}$ for some $0 < l < m$. $\square$

5. BOUNDS ON THE NONLINEARITY AND DIFFERENTIAL UNIFORMITY

5.1. Bounds on the nonlinearity of quadratic binomials with the maximal number of bent components.

Theorem 5.1. *Let $F(x) = x^{2^l+1} + x^{2^{l+m}}$ and $d = \gcd(l, m)$.*

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

Lemma 5.2. *Let $F(x) = x^{2^l+1} + x^{2^{l+m}}$ and $d = \gcd(l, m)$.*

- (1) *If $v_2(m) \leq v_2(l)$, 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*

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

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

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

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

belongs to

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

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

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

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

If $\text{Tr}(y^{2^{n-l}}) = u^{1+2^{n-l}}$, then $\text{Tr}(x) = u\zeta$ 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

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

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

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

Theorem 5.3 ([Cou99, Theorems 4.1 and 5.2]). *Let $d = \gcd(m, l)$ and $s = 2^d + 1$. Then*

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

Proof of Theorem 5.1. (1) This follows from Theorem 5.4 (2).

(2) Let $\text{Tr} = \text{Tr}_{2^n/2^m}$ and $s = \gcd(2^l + 1, 2^m - 1) = 2^d + 1$. 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 Lemma 5.2, we have

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

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

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

If $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, then $W_{F_a}(0) = 2^m$ by [PPM+18, Theorem 7]. If $a \in \mathbb{F}_{2^m}^*$, then

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

By Theorem 5.3, we conclude that

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

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

5.2. Bounds on the nonlinearity and differential uniformity for general vectorial functions.

Theorem 5.4. *Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a vectorial function.*

(1) *The nonlinearity of F satisfies*

$$\mathcal{N}_F \leq 2^{n-1} - 2^{m-1} \sqrt{\frac{2^n - 1}{\#S_F - 1} + 1}.$$

(2) *If F has $2^n - 2^m$ bent components, then*

$$\mathcal{N}_F \leq 2^{n-1} - 2^{m-1} \sqrt{2^m + 2}.$$

For a vectorial function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, 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 5.5 ([AKM+22]).

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

and equality holds if and only if $F(x)$ is almost perfect nonlinear (i.e., $\delta_F = 2$).

Proof of Theorem 5.4. (1) By Lemma 5.5, we have

$$\begin{aligned} \sum_{0 \neq a \in S_F} \nu(F_a) &= \sum_{a \in \mathbb{F}_{2^n}^*} \nu(F_a) - \sum_{a \in \mathbb{F}_{2^n} \setminus S_F} \nu(F_a) \\ &\geq (2^n - 1)2^{2n+1} - 2^{2n}(2^n - \#S_F) = 2^{2n}(2^n + \#S_F - 2). \end{aligned}$$

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

$$\begin{aligned} \sum_{0 \neq a \in S_F} \nu(F_a) &\leq 2^{-n} \max_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega) \sum_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega) \\ &= 2^n(\#S_F - 1) \max_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega). \end{aligned}$$

Therefore, we have

$$\max_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega) \geq \frac{2^{2n}(2^n + \#S_F - 2)}{2^n(\#S_F - 1)} = 2^n \left(\frac{2^n - 1}{\#S_F - 1} + 1 \right)$$

and then

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

(2) If F has $2^n - 2^m$ bent components, then $\#S_F = 2^m$ and

$$\mathcal{N}_F \leq 2^{n-1} - 2^{m-1} \sqrt{2^m + 2}. \quad \square$$

Theorem 5.4 gives a new proof of the following result on the nonlinearity of plateaued functions with the maximal number of bent components.

Corollary 5.6 ([AKM+22, Theorem 1]). *If F is a plateaued function and $\#S_F = 2^m$, then*

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

Proof. If F is plateaued and has $2^n - 2^m$ bent components, then there exists an even integer k such that

$$\max_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega) = 2^k \geq 2^n(2^m + 2).$$

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

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

Remark 5.7. For non-plateaued functions, the bound in [Theorem 5.4](#) may be weaker than the bound given in [\[XOH25, Conjecture 1\]](#).

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

Theorem 5.8. *Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a vectorial function. If*

$$T := \#\{0 \neq a \in S_F : W_{F_a}(0) \neq 0\}$$

is non-empty and $\#\text{Im}(F) \leq 2^{n-1} + 2^{m-2}$, then

$$\begin{aligned} \mathcal{N}_F &\leq 2^{n-1} - 2^{m-1} \sqrt{\frac{1}{T} \left(\frac{2^{2n}}{\#\text{Im}(F)} - 2^{n+1} + \#S_F \right)} \\ &\leq 2^{n-1} - 2^{m-1} \sqrt{\frac{1}{2^m - 1} \left(\frac{2^{2n}}{\#\text{Im}(F)} - 2^{n+1} + 2^m \right)}. \end{aligned}$$

Lemma 5.9. *Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a vectorial function. Then*

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

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

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

Proof of [Theorem 5.8](#). By [Lemma 5.9](#), we have

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

Thus

$$\begin{aligned}
\sum_{0 \neq a \in S_F} W_{F_a}^2(0) &= \sum_{a \in \mathbb{F}_{2^n}} W_{F_a}^2(0) - W_{F_0}^2(0) - \sum_{a \in \mathbb{F}_{2^n} \setminus S_F} W_{F_a}^2(0) \\
&\geq \frac{2^{3n}}{\#\text{Im}(F)} - 2^{2n} - 2^n(2^n - \#S_F) \\
&> \frac{2^{3n} - 2^{2n-2}}{2^{n-1} + 2^{m-2}} - 2^{2n+1} + 2^{n+m} = 0
\end{aligned}$$

and

$$\begin{aligned}
\max_{\substack{0 \neq a \in S_F \\ \omega \in \mathbb{F}_{2^n}}} W_{F_a}^2(\omega) &\geq \max_{0 \neq a \in S_F} W_{F_a}^2(0) \geq \frac{1}{T} \sum_{0 \neq a \in S_F} W_{F_a}^2(0) \\
&\geq \frac{2^n}{T} \left(\frac{2^{3n}}{\#\text{Im}(F)} - 2^{n+1} + \#S_F \right).
\end{aligned}$$

We thus get the desired bound for $\mathcal{N}_F$ together with $T \leq 2^m - 1$ and $\#S_F \geq 2^m$. $\square$

Remark 5.10. The bound in [Theorem 5.8](#) is smaller than Carlet's bound

$$2^{n-1} - \sqrt{\frac{1}{2^n - 1} \left(\frac{2^{3n-2}}{\#\text{Im}(F)} - 2^{2n-2} \right)}$$

in [\[Car21, Proposition 2\]](#). This bound is also smaller than $2^{n-1} - \frac{1}{2} \sqrt{2^n(2^m + 2)}$ given by [Theorem 5.4](#) when $\#\text{Im}(F) \leq \frac{2^{3n}}{3 \cdot 2^{2n} - 2^{n+1} + 1}$.

Theorem 5.11. *Assume that F has no nonzero affine component. For nonzero $a \in S_F$, define $r_a = \deg F_a$. Denote*

$$r = \max_{0 \neq a \in S_F} r_a.$$

Then $r_a \geq 2$ and

$$\mathcal{N}_F \geq \min\{2^{n-1} - 2^{m-1}, \min_{0 \neq a \in S_F} 2^{n-r_a}\} = 2^{n-r}.$$

Proof. If $a \notin S_F$, then F_a is bent and $\mathcal{N}_{F_a} = 2^{n-1} - 2^{m-1}$. For $0 \neq a \in S_F$, the component F_a is not affine, i.e.,

$$F_a + \text{Tr}_{2^n/2}(bx) \neq 0, \quad F_a + \text{Tr}_{2^n/2}(bx) + 1 \neq 0,$$

for every $b \in \mathbb{F}_{2^n}$, and both functions have degree at most r_a . The Reed-Muller code $\text{RM}(r_a, n)$ has minimum distance 2^{n-r_a} (see [\[MS77, Chapter 13, Theorem 3\]](#)), hence

$$\text{wt}_2(F_a + \text{Tr}_{2^n/2}(bx)) \geq 2^{n-r_a}, \quad \text{wt}_2(F_a + \text{Tr}_{2^n/2}(bx) + 1) \geq 2^{n-r_a}.$$

This yields that

$$\mathcal{N}_{F_a} \geq 2^{n-r_a}.$$

Taking the minimum over all components gives

$$\mathcal{N}_F \geq \min\{2^{n-1} - 2^{m-1}, \min_{a \in S_F \setminus \{0\}} 2^{n-r_a}\}.$$

Since $r \geq 2$,

$$2^{n-r} \leq 2^{n-2} \leq 2^{n-1} - 2^{m-1},$$

and therefore $\mathcal{N}_F \geq 2^{n-r}$. $\square$

The following bound can be found in [Car21]. For completeness, we provide a proof.

Theorem 5.12. *For any non-injective vectorial function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, we have*

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

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 2.1 (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 can then be obtained by Lemma 5.9. $\square$

5.3. Bound on the nonlinearity and differential uniformity of particular binomials.

Theorem 5.13. *Let $F(x) = x^{d_1} + x^{d_2} \in \mathbb{F}_{2^n}[x]$ with $d_2 - d_1 = (2^m - 1)k$. If $\gcd(k, 2^m + 1) = 1$, $s = \gcd(d_1, d_2, 2^n - 1) > 1$ and*

$$T := \#\{0 \neq a \in S_F : W_{F_a}(0) \neq 0\}$$

is non-empty, then

$$\begin{aligned} \mathcal{N}_F &\leq 2^{n-1} - 2^{m-1} \sqrt{\frac{1}{T} \left(\frac{2^{2n}s}{s + (2^m - 1)c} - 2^{n+1} + \#S_F \right)}, \\ \delta_F &\geq \max \left\{ 2^m, \left\lceil \frac{2^n}{\#\Delta} \left(\frac{2^n s}{s + (2^m - 1)c} - 1 \right) \right\rceil \right\}, \end{aligned}$$

where

$$\begin{aligned} c &= \#\{F(\alpha^i)^{(2^m-1)/s} : i = 1, 2, \dots, 2^m\}, \\ \Delta &= \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, x \neq y, F(x) = F(y)\}, \end{aligned}$$

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

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

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

If $a \in \mathbb{F}_{2^m}^*$, then $F(x+a) + F(x) = 0$ for all $x \in \mathbb{F}_{2^m}$. Therefore, $\delta_{a,0} \geq 2^m$. By Definition 2.1(vi), we have

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

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,

$$\#\text{Im}(F) = 1 + c\#D = 1 + \frac{(2^m-1)c}{s} \leq 1 + \frac{2^m(2^m-1)}{3} < 2^{n-1} + 2^{m-2}.$$

The result then follows by [Theorems 5.8](#) and [5.12](#). $\square$

Remark 5.14. Pott et al. [[PPM+18](#)] showed $\delta_F = 2^m$ when $d_1 = 2^l + 1$ and $d_2 = 2^m + 2^l$.

6. CONCLUSION

In this paper, we focus on vectorial functions with the maximal number of bent components. Using Stickelberger's theorem, we study the Walsh transform of binomial vectorial functions $F(x) = x^{d_1} + x^{d_2}$, and show that $F(x)$ is EA-equivalent to $x^{2^l+1} + x^{2^l+2^m}$ for some $0 < l < m$ when $\text{wt}_2(d_1) = \text{wt}_2(d_2) = 2$ if $\gcd(d_1, d_2, 2^m - 1) > 1$. We also give several estimates on the nonlinearity and differential uniformity for general vectorial functions by means of the cardinality of related sets.

ACKNOWLEDGEMENTS

X. Xie is partially supported by the National Natural Science Foundation of China (Grant No. 62402004). Y. Ouyang is partially supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302902). S. Zhang is partially supported by State Key Laboratory of Cyberspace Security Defense (Grant No. 2025-MS-04).

REFERENCES

- [AKM+22] 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** (2022), no. 9, 6174–6186.
- [Car21] 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** (2021), no. 12, 8325–8334.
- [Cou99] R. Coulter. *On the evaluation of a class of Weil sums in characteristic 2*. New Zealand J. Math. **28** (1999), 171–184.
- [HF07] H. Hu and D. Feng. *On quadratic bent functions in polynomial forms*. IEEE Trans. Inf. Theory **53** (2007), no. 7, 2610–2615.
- [H WX+23] H. Hu, B. Wang, X. Xie and Y. Luo. *An open problem about monomial bent functions*. IEEE Trans. Inf. Theory **69** (2023), no. 12, 8111–8115.
- [LL08] P. Langevin and G. Leander. *Monomial bent functions and Stickelberger's theorem*. Finite Fields Appl. **14** (2008), no. 3, 727–742.
- [LLM+11] P. Langevin, G. Leander, G. McGuire and E. Zălinescu. *Analysis of Kasami-Welch functions in odd dimension using Stickelberger's theorem*. J. Comb. Number Theory **2** (2011), no. 1, 55–72.
- [LV05] P. Langevin and P. Véron. *On the nonlinearity of power functions*. Designs Codes Cryptogr. **37** (2005), 31–43.
- [Lea04] N. G. Leander. *Normality of bent functions, monomial and binomial bent functions*. Ph.D. thesis, Dept. Math., Ruhr-Univ. Bochum, Bochum, Germany, 2004.
- [MZT+19] 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** (2019), 2597–2610.

- [MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Math. Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–xv and 1–369.
- [MSC+04] O. Moreno, K. Shum, F. Castro and P. Kumar. *Tight bounds for Chevalley-Waring-Ax-Katz type estimates, with improved applications*. Proc. London Math. Soc. **3** (2004), no. 88, 545–564.
- [PPM+18] A. Pott, E. Pasalic, A. Muratovic and S. Bajric. *On the maximum number of bent components of vectorial functions*. IEEE Trans. Inf. Theory **64** (2018), no. 1, 403–411.
- [Sti90] J. Stickelberger. *Über eine Verallgemeinerung der Kreistheilung*. Math. Ann. **37** (1890), 321–367.
- [XOH25] X. Xie, Y. Ouyang and H. Hu. *On vectorial functions with maximal number of bent components*. Des. Codes Cryptogr. **93** (2025), 1889–1910.
- [ZPK+20] 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** (2020), no. 9, 2171–2186.

¹SCHOOL OF INFORMATION AND COMPUTER, ANHUI AGRICULTURAL UNIVERSITY, HEFEI 230036, CHINA

Email address: xianhxie@ahau.edu.cn

²SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA, HEFEI 230026, CHINA

³HEFEI NATIONAL LABORATORY, HEFEI 230088, CHINA

Email address: yiouyang@ustc.edu.cn

⁴SCHOOL OF MATHEMATICS, HEFEI UNIVERSITY OF TECHNOLOGY, HEFEI 230601, CHINA

⁵STATE KEY LABORATORY OF CYBERSPACE SECURITY DEFENSE, INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES, BEIJING 100085, CHINA

Email address: zhangshenxing@hfut.edu.cn