An Open Problem on the Bentness of Mesnager's Functions

Chunming Tang[a], Peng Han[a], Qi Wang[b], Jun Zhang[c], Yanfeng Qi[d]

[a]*School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, 637002, China*
[b]*Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China*
[c]*School of Mathematical Sciences, Capital Normal University, Beijing 100048, China*
[d]*School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China*

Abstract

Let $n=2m$. In the present paper, we study the binomial Boolean functions of the form

$$f_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right),$$

where m is an even positive integer, $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_4^*$. We show that $f_{a,b}$ is a bent function if the Kloosterman sum

$$K_m\left(a^{2^m+1}\right)=1+\sum_{x\in\mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}_1^m\left(a^{2^m+1}x+\frac{1}{x}\right)}$$

equals 4, thus settling an open problem of Mesnager. The proof employs tools including computing Walsh coefficients of Boolean functions via multiplicative characters, divisibility properties of Gauss sums, and graph theory.

Keywords: Boolean function, bent function, Walsh transform, Gauss Sum, directed graph.
2000 MSC: 05B05, 51E10, 94B15

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, where $q=p^n$ and p is a prime. Let f be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ in univariate trace form. It's *Walsh coefficient* at $b\in\mathbb{F}_{2^n}$ can be defined as

$$\mathcal{W}_f(b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}, \tag{1}$$

where $\mathrm{Tr}_1^n(\cdot)$ is the *absolute trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The function f is said to be a bent function if its Walsh coefficients $\mathcal{W}_f(b)$ take values $\pm 2^m$ only for all $b\in\mathbb{F}_{2^n}$. Bent functions [5, 17] are the indicators of Hadamard difference sets in elementary Abelian 2-groups. They play important roles in symmetric cryptography, coding theory, combinatorial designs, sequences, etc.

☆This work was supported by the National Nature Science Foundation of China under Grant No. 11871058, 11931005 and 11971321, the National Key Research and Development Program of China under Grant No. 2018YFA0704703, and Zhejiang provincial Natural Science Foundation of China under Grant No. LY21A010013.

Email addresses: `tangchunmingmath@163.com` (Chunming Tang), `penghanmitp@163.com` (Peng Han), `wangqi@sustech.edu.cn` (Qi Wang), `junz@cnu.edu.cn` (Jun Zhang), `qiyanfeng07@163.com` (Yanfeng Qi)

A Boolean (bent) function f over $\mathbb{F}_{2^n}$ is called hyper-bent if $f(x^k)$ is bent for every k co-prime to 2^n-1. Bent functions exist for every even integer n. We shall denote $n=2m$ in the sequel. If f is a bent function, then there exists a Boolean function, that we shall denote by $\tilde{f}$, such that, for any b in $\mathbb{F}_{2^n}$,

$$\mathcal{W}_f(b)=2^m(-1)^{\tilde{f}(b)}.$$

This function $\tilde{f}$ is bent too, and we call it the dual of f.

It is usually difficult to compute the Walsh coefficients of Boolean functions explicitly; sometimes, even computing the absolute values of Walsh coefficients is difficult. However, such difficulties can sometimes be bypassed by divisibility considerations. In fact, the condition on Walsh coefficients of bent functions can be weakened, without losing the property of being necessary and sufficient [12]:

Lemma 1. *Let $n=2m$. A Boolean function f over $\mathbb{F}_{2^n}$ is bent if and only if for each $b\in\mathbb{F}_{2^n}^*$, $\mathcal{W}_f(b)\equiv 2^m \mod 2^{m+1}$. In that case, the dual $\tilde{f}$ of f can be determined by approximations modulo*

$$\mathcal{W}_f(b)\equiv(-1)^{\tilde{f}(b)}2^m \pmod{2^{m+2}}.$$

For more details about bent functions and their applications in cryptography and coding theory, see [4] and [16].

Finding bent functions in univariate trace form is in general difficult and of theoretical interest, since it gives more insight on bent functions. Moreover, the output to such functions is often faster to compute thanks to their particular form.

In 2009, Mesnager [13] has exhibited an infinite class of binomial Boolean functions defined on $\mathbb{F}_{2^n}$ whose expression is the sum of a Dillon monomial function and a trace function of the from $\mathrm{Tr}_1^2\left(x^{\frac{2^n-1}{3}}\right)$. More precisely, they are of the form

$$f_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right), \tag{2}$$

where $n=2m$, $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_4^*$. When m is odd, Mesnager [13, 14] has shown that such functions are bent if and only if the Kloosterman sum $K_m\left(a^{2^m+1}\right)=1+\sum_{x\in\mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}_1^m\left(a^{2^m+1}x+\frac{1}{x}\right)}$ associated with a^{2^m+1} is equal to 4. Not only does such a criterion give a concise and elegant characterization for bentness, but using the connection between Kloosterman sums and elliptic curves it also allows fast generation of bent functions. Unfortunately, the proof of the aforementioned characterization does not extend to the case where m is even. When m is even, the situation seems to be more complicated than that in the odd case. In particular, we are not able to say if a function $f_{a,b}$ is or not in the Partial Spread class, which is a key part in Mesnager's proof for the odd case. Nevertheless, it has been shown that $K_m\left(a^{2^m+1}\right)=4$ is still a necessary condition for $f_{a,b}$ to be bent [15], but it is an open problem to tell whether this condition is sufficient for all even m or not (see [2, Open Problem 3] and [3]). Further experimental evidence gathered by Flori, Mesnager and Cohen [6] supported the conjecture that it should also be a sufficient condition: for m up to 16, $f_{a,b}$ is bent if and only if $K_m\left(a^{2^m+1}\right)=4$. In the case when $m\equiv 2 \mod 4$, Flori [8] presented a link between the bentness of $f_{a,b}$ and a conjecture about exponential sums involving Kloosterman sums.

We will show that the binomial function $f_{a,b}$ is indeed bent if $K_m\left(a^{2^m+1}\right)=4$, whose proof is the objective of the present paper. We state our main result as the following.

Theorem 2. *Let m be an even positive integer, and let $n = 2m$. Let $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$. If the Kloosterman sum $K_m\left(a^{2^m+1}\right) = 4$, then the binomial function $f_{a,b} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined in Equation (2) is a bent function.*

The remainder of the paper is organized as follows. In Section 2, we fix our main notation and recall the necessary background on character sums over finite fields. Next, in Section 3, we give the proofs that the value 4 of the Kloosterman sum indeed leads to bent functions. Finally, in Section 4, we give the detailed discussions of binary weight inequality needed in the proof of our main theorem.

2. Gauss sums and Stickelberger's Theorem

We collect some auxiliary results on Gauss sums as a preparation for computing the Walsh coefficients of Boolean functions.

Let p be a prime number and $q = p^n$. Let $\mathbb{Z}_p$ be the ring of integers in the field $\mathbb{Q}_p$ of p-adic rational numbers. Let $\mathbb{Z}_q$ be the ring of integers in the unique unramified extension of $\mathbb{Q}_p$ with the residue field $\mathbb{F}_q$. Let ω_q be the Teichmüller character of the multiplicative group $\mathbb{F}_q^*$ consisting of all nonzero elements of $\mathbb{F}_q$. For $x \in \mathbb{F}_q^*$, the value $\omega_q(x)$ is just the $(q-1)$-th root of unity in $\mathbb{Z}_q$ such that $\omega_q(x)$ modulo p reduces to x. For any integer k, define the Gauss sum over $\mathbb{F}_q$ by

$$G(k) = \sum_{x \in \mathbb{F}_q^*} \omega_q^{-k}(x) \zeta_p^{\mathrm{Tr}_1^n(x)}, \tag{3}$$

where ζ_p is a fixed primitive p-th root of unity in an extension of $\mathbb{Q}_p$ and $\mathrm{Tr}_1^n(x) = x + x^p + \cdots + x^{p^{n-1}}$ is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Gauss sums are instrumental in the transition from the additive to the multiplicative structure of a finite field. We have the following well-known relation between the additive characters and the multiplicative characters.

Lemma 3. *For all $x \in \mathbb{F}_q^*$, the Gauss sums satisfy the following interpolation relation*

$$\zeta_p^{\mathrm{Tr}_1^n(x)} = \frac{1}{q-1} \sum_{k=0}^{q-2} G(k) \omega_q^k(x).$$

Let k be any integer not divisible by $q-1$. Then there are unique integers $k_0, k_1, \ldots, k_{n-1}$ with $0 \le k_i \le p-1$ for all i, $0 \le i \le n-1$ such that

$$k \equiv k_0 + k_1 p + \cdots + k_{n-1} p^{n-1} \pmod{q-1}.$$

We define the (p-ary) weight of k modulo $q-1$, denoted by $\mathrm{wt}_q(k)$, as $\mathrm{wt}_q(k) = k_0 + k_1 + \cdots + k_{n-1}$. For integers k divisible by $q-1$, we define $\mathrm{wt}_q(k) = 0$.

To get the first nonzero digit in the π-adic expansion of the Gauss sum, we can use the Stickelberger theorem (see [9] and [11]).

Theorem 4 (Stickelberger)**.** *For integer $0 \le k \le q-2$, write $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$ in p-adic expansion, where $0 \le k_i \le p-1$. Then,*

$$G(k) \equiv \frac{-\pi^{\mathrm{wt}_q(k)}}{k_0! k_1! \ldots k_{n-1}!} \pmod{\pi^{\mathrm{wt}_q(k)+p-1}},$$

where π is the unique element in $\mathbb{Z}_p[\zeta_p]$ satisfying $\pi^{p-1} = -p$ and $\pi \equiv \zeta_p - 1 \pmod{(\zeta_p - 1)^2}$. In particular, if $p = 2$ the following congruence holds:

$$G(k) \equiv 2^{\mathrm{wt}_q(k)} \pmod{2^{\mathrm{wt}_q(k)+1}}.$$

3. Proof of the main results

The goal of this section is to prove Theorem 2. In order to do so, we must first establish some results concerning exponential sums over finite fields.

Lemma 5. *Let $n = 2m$, $q = 2^n$ and $a \in \mathbb{F}_{2^m}^*$. It holds that*

$$\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)} = \frac{1}{2^m - 1} \sum_{0 \le i \le 2^m - 2} \overline{G}(i)^2 \omega_q^{(2^m+1)i}(a),$$

where $\overline{G}(i)$ denotes the Gauss sum $\sum_{x \in \mathbb{F}_{2^m}^*} \omega_q^{-(2^m+1)i}(x)(-1)^{\mathrm{Tr}_1^m(x)}$ over $\mathbb{F}_{2^m}$ with respect to the multiplicative character $\omega_q^{(2^m+1)i}$.

Proof. Note that $\omega_q^{2^m+1}$ is a generator of the multiplicative character group of $\mathbb{F}_{2^m}^*$. By Lemma 3, we have

$$\begin{aligned}
&\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)} \\
&= \frac{1}{(2^m - 1)^2} \sum_{0 \le i, j \le 2^m - 2} \overline{G}(i)\overline{G}(j) \sum_{x \in \mathbb{F}_{2^m}^*} \omega_q^{(2^m+1)i}(ax)\, \omega_q^{-(2^m+1)j}(x) \\
&= \frac{1}{(2^m - 1)^2} \sum_{0 \le i, j \le 2^m - 2} \overline{G}(i)\overline{G}(j) \omega_q^{(2^m+1)i}(a) \sum_{x \in \mathbb{F}_{2^m}^*} \omega_q^{(2^m+1)(i-j)}(x).
\end{aligned}$$

Since $\sum_{x \in \mathbb{F}_{2^m}^*} \omega_q^{(2^m+1)(i-j)}(x) = 2^m - 1$ if and only if $i \equiv j \pmod{2^m - 1}$, and is 0 otherwise, we thus have

$$\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)} = \frac{1}{2^m - 1} \sum_{0 \le i \le 2^m - 2} \overline{G}(i)^2 \omega_q^{(2^m+1)i}(a),$$

which completes the proof. □

Lemma 6. *Let $n = 2m$ and $q = 2^n$. Write $B = \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1} + cx\right)}$, where $a, c \in \mathbb{F}_{2^n}^*$. Then*

(1) $B = \frac{1}{q-1} \sum_{0 \le i \le q-2} G(i) G(-(2^m - 1)i)\, \omega_q\left(a^i c^{-(2^m-1)i}\right)$.

(2) $B \equiv K_m\left(a^{2^m+1}\right) + 2^m - 1 \pmod{2^{m+1}}$.

Proof. By Lemma 3, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\\
&=\frac{1}{(q-1)^2}\sum_{0\le i,j\le q-2}G(i)G(j)\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^i\left(ax^{2^m-1}\right)\omega_q^j(cx)\\
&=\frac{1}{(q-1)^2}\sum_{0\le i,j\le q-2}G(i)G(j)\omega_q\left(a^ic^j\right)\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^{(2^m-1)i+j}(x)\\
&=\frac{1}{(q-1)^2}\sum_{0\le i,j\le q-2}G(i)G(j)\omega_q\left(a^ic^j\right)\omega_q^{(2^m-1)i+j}(\mathbb{F}_{2^n}^*),
\end{aligned}$$

where $\omega_q^{(2^m-1)i+j}(\mathbb{F}_{2^n}^*)=\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q(x)^{(2^m-1)i+j}$. It is well known that

$$\omega_q^{(2^m-1)i+j}(\mathbb{F}_{2^n}^*)=\begin{cases}q-1, & if\ \ j\equiv-(2^m-1)i \pmod{q-1},\\ 0, & otherwise.\end{cases}$$

We thus have

$$\begin{aligned}
&\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\\
&=\tfrac{1}{q-1}\textstyle\sum_{0\le i\le q-2}G(i)G\left(-\left(2^m-1\right)i\right)\omega_q\left(a^ic^{-(2^m-1)i}\right).
\end{aligned}$$

This completes the proof of the first assertion of the lemma.

To prove part (2), recall that $\mathrm{wt}_q\left(-\left(2^m-1\right)i\right)=m$ if i is not a multiple of 2^m+1 (see [12, Lemma 2]). Combining Theorem 4 with the fact $G(0)=-1$ yields

$$\begin{aligned}
&\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\\
&\equiv\textstyle\sum_{0\le i\le 2^m-2}G((2^m+1)i)\omega_q\left(a^{(2^m+1)i}\right)\pmod{2^{m+1}}.
\end{aligned}\tag{4}$$

Observe that $\omega_q^{-(2^m+1)i}(x)=\omega_q^{-(2^m+1)i}\left(\sqrt{x}^{2^m+1}\right)$ for each $x\in\mathbb{F}_{2^n}^*$ and $0\le i\le 2^m-2$. We deduce that

$$\begin{aligned}
G((2^m+1)i) &= \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^{-(2^m+1)i}(x)(-1)^{\mathrm{Tr}_1^n(x)}\\
&= \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^{-(2^m+1)i}\left(\sqrt{x}^{2^m+1}\right)(-1)^{\mathrm{Tr}_1^n(x)}\\
&= \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^{-(2^m+1)i}\left(\sqrt{x}^{2^m+1}\right)(-1)^{\mathrm{Tr}_1^n(\sqrt{x})}\\
&= \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}\omega_q^{-(2^m+1)i}\left(x^{2^m+1}\right)(-1)^{\mathrm{Tr}_1^n(x)}\\
&= -\left(\textstyle\sum_{x\in\mathbb{F}_{2^m}^*}\omega_q^{-(2^m+1)i}(x)(-1)^{\mathrm{Tr}_1^m(x)}\right)^2,
\end{aligned}$$

where the last equality follows by the Davenport and Hasses lifting theorem (see Weil [18, p. 503–505]). Substituting $G((2^m+1)i)$ in the expression (4) by $-\overline{G}(i)^2$, we have

$$\begin{aligned}
&\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\\
&\equiv-\textstyle\sum_{0\le i\le 2^m-2}\overline{G}(i)^2\omega_q\left(a^{(2^m+1)i}\right)\pmod{2^{m+1}}.
\end{aligned}$$

Since $\omega_q\left(a^{(2^m+1)i}\right)=\omega_q^{(2^m+1)i}\left(\sqrt{a}^{2^m+1}\right)$, we have

$$\begin{aligned}
&\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\\
&\equiv -\textstyle\sum_{0\le i\le 2^m-2}\overline{G}(i)^2\omega_q^{(2^m+1)i}\left(\sqrt{a}^{2^m+1}\right)\\
&\equiv -(2^m-1)\cdot\textstyle\sum_{x\in\mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}_1^m\left(\sqrt{a}^{2^m+1}x+\frac{1}{x}\right)} \pmod{2^{m+1}},
\end{aligned}$$

where the last congruence follows from Lemma 5. Together with the fact

$$\sum_{x\in\mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}_1^m\left(\sqrt{a}^{2^m+1}x+\frac{1}{x}\right)}=\sum_{x\in\mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}_1^m\left(a^{2^m+1}x+\frac{1}{x}\right)},$$

we have

$$\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\equiv(2^m+1)\cdot\left(K_m\left(a^{2^m+1}\right)-1\right) \pmod{2^{m+1}},$$

Since $K_m\left(a^{2^m+1}\right)$ is an even integer, we have

$$\textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)}\equiv K_m\left(a^{2^m+1}\right)+2^m-1 \pmod{2^{m+1}},$$

which completes the proof of Part (2). □

The most important ingredient in the proof of Theorems 2 is the following result.

Theorem 7. *Let $q=2^{2m}$, where m is any positive integer, and let u equal $\frac{2^{2m}-1}{3}$ or $2\cdot\frac{2^{2m}-1}{3}$. For any integers a and b, if s and t satisfy*

$$s\equiv u-a+b,\quad t\equiv u+a-b \pmod{2^{2m}-1},$$

then $\mathrm{wt}_q(a)+\mathrm{wt}_q(b)+\mathrm{wt}_q(s)+\mathrm{wt}_q(t)\ge 2m$.

The proof of Theorem 7 involves graph-theory methods. To streamline the presentation of the paper, we postpone the proof to the next section.

The following lemma establishes a congruence relation between the Walsh coefficients of $f_{a,1}$ and the Kloosterman sum, which plays an important role in the proof of Theorem 2.

Lemma 8. *Let $a\in\mathbb{F}_{2^n}^*$, where $n=2m$ and m is an even positive integer. Let $f_{a,1}$ be the binomial function given in (2). Then for any $c\in\mathbb{F}_{2^n}^*$ we have*

$$\mathcal{W}_{f_{a,1}}(c)\equiv\frac{4-K_m\left(a^{2^m+1}\right)}{3}+2^m \pmod{2^{m+1}}.$$

Proof. Let $C_0=\left\{x^3:x\in\mathbb{F}_{2^n}^*\right\}$. By noting that

$$\mathrm{Tr}_1^2\left(x^{\frac{2^n-1}{3}}\right)=\begin{cases}0, & if\ \ x\in C_0\cup\{0\}\\ 1, & otherwise\end{cases},$$

we have

$$\begin{aligned}
&\mathcal{W}_{f_{a,1}}(c) \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)+\mathrm{Tr}_1^2\left(x^{\frac{2^n-1}{3}}\right)} \\
&= 1-\sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)} + 2\cdot\sum_{x\in C_0} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)} \\
&= 1-\sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}+cx\right)} + \frac{2}{3}\cdot\sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}+cx^3\right)}.
\end{aligned} \tag{5}$$

By Lemma 3, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}+cx^3\right)} \\
&= \frac{1}{(q-1)^2}\sum_{0\le i,j\le q-2} G(i)G(j)\sum_{x\in\mathbb{F}_{2^n}^*} \omega_q\left(ax^{3(2^m-1)}\right)^i \omega_q\left(cx^3\right)^j \\
&= \frac{1}{(q-1)^2}\sum_{0\le i,j\le q-2} G(i)G(j)\omega_q\left(a^ic^j\right)\sum_{x\in\mathbb{F}_{2^n}^*} \omega_q(x)^{3\cdot(2^m-1)i+3j}.
\end{aligned}$$

Note that

$$\sum_{x\in\mathbb{F}_{2^n}^*} \omega_q(x)^{3\cdot(2^m-1)i+3j} = \begin{cases} q-1, & \text{if } 3\cdot(2^m-1)i+3j\equiv 0 \pmod{q-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Since $3\cdot(2^m-1)i+3j\equiv 0 \pmod{q-1}$ if and only if $j=\frac{2^n-1}{3}\ell-(2^m-1)i$, where $0\le \ell\le 2$, we obtain

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}+cx^3\right)} \\
&= \frac{1}{q-1}\sum_{0\le i\le q-2} G(i)G\left(\frac{2^n-1}{3}-(2^m-1)i\right)\omega_q\left(a^ic^{\frac{2^n-1}{3}-(2^m-1)i}\right) \\
&\quad+\frac{1}{q-1}\sum_{0\le i\le q-2} G(i)G\left(2\cdot\frac{2^n-1}{3}-(2^m-1)i\right)\omega_q\left(a^ic^{2\cdot\frac{2^n-1}{3}-(2^m-1)i}\right) \\
&\quad+\frac{1}{q-1}\sum_{0\le i\le q-2} G(i)G\left(-(2^m-1)i\right)\omega_q\left(a^ic^{-(2^m-1)i}\right).
\end{aligned} \tag{6}$$

Combining (5) with (6) yields

$$\begin{aligned}
&\mathcal{W}_{f_{a,1}}(c) \\
&= 1-\frac{1}{3(q-1)}\sum_{0\le i\le q-2} G(i)G\left(-(2^m-1)i\right)\omega_q\left(a^ic^{-(2^m-1)i}\right) \\
&\quad+\frac{2}{3(q-1)}\sum_{0\le i\le q-2} G(i)G\left(\frac{2^n-1}{3}-(2^m-1)i\right)\omega_q\left(a^ic^{\frac{2^n-1}{3}-(2^m-1)i}\right) \\
&\quad+\frac{2}{3(q-1)}\sum_{0\le i\le q-2} G(i)G\left(2\cdot\frac{2^n-1}{3}-(2^m-1)i\right)\omega_q\left(a^ic^{2\cdot\frac{2^n-1}{3}-(2^m-1)i}\right).
\end{aligned} \tag{7}$$

When m is even, it is routine to check that

$$\frac{2^n-1}{3}-(2^m-1)i\equiv 2^m\left(\frac{2^n-1}{3}+(2^m-1)i\right) \pmod{2^n-1}$$

and

$$2\cdot\frac{2^n-1}{3}-(2^m-1)i\equiv 2^m\left(2\cdot\frac{2^n-1}{3}+(2^m-1)i\right) \pmod{2^n-1}.$$

Applying Theorem 7 with $u=\frac{2^n-1}{3}$, $a=i$ and $b=2^m\cdot i$, we then have

$$\mathrm{wt}_q(i)+\mathrm{wt}_q\left(\frac{2^n-1}{3}-(2^m-1)\,i\right)\geq m.$$

Similarly, we have

$$\mathrm{wt}_q(i)+\mathrm{wt}_q\left(2\cdot\frac{2^n-1}{3}-(2^m-1)\,i\right)\geq m.$$

By Theorem 4, we have

$$G(i)G\left(\frac{2^n-1}{3}-(2^m-1)\,i\right)\equiv 0 \pmod{2^m}$$

and

$$G(i)G\left(2\cdot\frac{2^n-1}{3}-(2^m-1)\,i\right)\equiv 0 \pmod{2^m}.$$

Continuing from (7), we have

$$\mathcal{W}_{f_{a,1}}(c)\equiv 1+\tfrac{1}{3}\textstyle\sum_{0\leq i\leq q-2}G(i)G(-(2^m-1)\,i)\,\omega_q\left(a^i c^{-(2^m-1)i}\right) \pmod{2^{m+1}}.$$

By Lemma 6, we get

$$\mathcal{W}_{f_{a,1}}(c)\equiv 1+\tfrac{1-K_m\left(a^{2^m+1}\right)+2^m}{3} \pmod{2^{m+1}},$$

which further gives

$$\mathcal{W}_{f_{a,1}}(c)\equiv \tfrac{4-K_m\left(a^{2^m+1}\right)}{3}+2^m \pmod{2^{m+1}}.$$

This completes the proof of the lemma. □

Having dealt with these preliminaries, we can now prove the main theorem.

Proof of Theorem 2. Substituting $K_m\left(a^{2^m+1}\right)$ in the expression for $\mathcal{W}_{f_{a,1}}(c)$ in Lemma 8 by 4, we have

$$\mathcal{W}_{f_{a,1}}(c)\equiv 2^m \pmod{2^{m+1}}.$$

Combining the above congruence with Lemma 1, the proof of Theorem 2 is concluded, by noting that $f_{a,b}$ is bent if and only if $f_{a,1}$ is bent [7]. □

Example 9. *Let $\mathbb{F}_{2^6}$ be the finite field represented as $\mathbb{F}_2[z]/(z^6+z^4+z^3+z+1)$ and $a=z^3$. Then $K_6(a)=4$ and the binomial function $f_{a,1}(x)=\mathrm{Tr}_1^{12}\left(ax^{2^6-1}\right)+\mathrm{Tr}_1^2\left(x^{\frac{2^{12}-1}{3}}\right)$ over $\mathbb{F}_{2^{12}}$ is bent. Its dual $\tilde{f}_{a,1}(x)$ is given by $\mathrm{Tr}_1^{12}\left(z^{48}x^{357}\right)+\mathrm{Tr}_1^{12}\left(z^{28}x^{147}\right)+\mathrm{Tr}_1^{12}\left(z^{3}x^{63}\right)+\mathrm{Tr}_1^{12}\left(z^{62}x^{21}\right)+\mathrm{Tr}_1^{12}\left(z^{60}x^{105}\right)+\mathrm{Tr}_1^{4}\left(x^{273}\right)+\mathrm{Tr}_1^{2}\left(x^{1365}\right)$. However, the Boolean function $f_{a,1}(x^{11})$ is not bent as its Walsh spectrum $\left\{\mathcal{W}_{f_{a,1}}(c):c\in\mathbb{F}_{2^{12}}\right\}$ is $\{0,\pm32,\pm64,\pm96,\pm128,\pm160\}$. Note that* g.c.d$(11,2^{12}-1)=1$. *Hence $f_{a,1}$ is not a hyper-bent funcition.*

4. Proof of the weight inequality

Let $\{s_j\}_{j\in\mathbb{Z}}$ be a sequence. If for a positive integer n the terms of $\{s_j\}_{j\in\mathbb{Z}}$ satisfy $s_j = s_{j+n}$ for all $j\in\mathbb{Z}$, then we say that $\{s_j\}_{j\in\mathbb{Z}}$ is n-periodic. If $s_j\in\{0,1\}$ for all $j\in\mathbb{Z}$, $\{s_j\}_{j\in\mathbb{Z}}$ is said to be a binary sequence. Let $0^{\mathbb{Z}}$ (resp., $1^{\mathbb{Z}}$) denote the sequence $\{s_j\}_{j\in\mathbb{Z}}$ with $s_j = 0$ (resp., $s_j = 1$) for all j. Any sequence of length n can be extended to a periodic sequence with period n.

Given a and b, we use a modular add-and-carry method inspired by [10] to help compute the weights of $u-a+b$ and $u+a-b$ that appear in the inequality in Theorem 7. The basic result we need is a technical result related to [10, Theorem 13].

Theorem 10. *Let $\{s_j\}_{j\in\mathbb{Z}}$ and $\left\{a_j^{(i)}\right\}_{j\in\mathbb{Z}}$, $1\le i\le r$, be binary sequences of period n with $\left\{a_j^{(i)}\right\}_{j\in\mathbb{Z}}\notin\{0^{\mathbb{Z}},1^{\mathbb{Z}}\}$ for some i. Let $t_1,\dots,t_r$ be nonzero integers. Suppose that*

$$s\equiv t_1a^{(1)}+\cdots+t_ra^{(r)}\pmod{2^n-1},$$

where $s=\sum_{i=0}^{n-1}s_j2^j$ and $a^{(i)}=\sum_{j=0}^{n-1}a_j^{(i)}2^j$. Then there exists a unique n-periodic sequence $\{c_i\}_{i\in Z}$ with terms in $\{t_-,t_-+1,\dots,t_+-1\}$ such that

$$2c_j+s_j=t_1a_j^{(1)}+\cdots+t_ra_j^{(r)}+c_{j-1}\quad(j\in\mathbb{Z}),$$

where $t_-=\sum_{i,t_i<0}t_i$ and $t_+=\sum_{i,t_i>0}t_i$. Moreover, we have that

$$\sum_{j=0}^{n-1}c_j=\sum_{i=1}^{r}t_i\sum_{j=0}^{n-1}a_j^{(i)}-\sum_{j=0}^{n-1}s_j.$$

The numbers s_j and c_j will be referred to as the digits and carries, respectively, for the computation modulo 2^n-1 of the number s.We now give the promised proof of Theorem 7.

Proof of Theorem 7. Let s and t be defined as in the theorem, and write $n=2m$. Assume that a, b, u, s and t have the binary digits a_j, b_j, u_j, s_j and t_j, for $j=0,\dots,n-1$. Note that

$$\begin{aligned} s &\equiv u-a+b\pmod{2^n-1},\\ t &\equiv u+a-b\pmod{2^n-1}.\end{aligned}$$

Now apply Theorem 10 to the defining additions for s and t. In both cases, $t_+=1$ and $t_-=-1$, hence there are carry sequences $\{c_j\}_{j\in\mathbb{Z}}$ and $\{d_j\}_{j\in\mathbb{Z}}$ with $-1\le c_j,d_j\le 1$ such that

$$\begin{aligned} 2c_j+s_j &= u_j-a_j+b_j+c_{j-1},\\ 2d_j+t_j &= u_j+a_j-b_j+d_{j-1}.\end{aligned}\tag{8}$$

Moreover, $\sum_{j=0}^{n-1}c_j+\sum_{j=0}^{n-1}d_j+\sum_{j=0}^{n-1}s_j+\sum_{j=0}^{n-1}t_j=n$. Using this relation, we see that the weight inequality in the theorem is equivalent to

$$\sum_{j=0}^{n-1}\left(a_j+b_j-c_j-d_j\right)\ge 0.\tag{9}$$

In order to analyze the contribution of the individual binary digits a_j, b_j, c_j, d_j to the sum $\sum_{j=0}^{n-1}\left(a_j+b_j-c_j-d_j\right)$, we construct the following weighted directed graph G.

The graph G will have a vertex (u', a', b', c', d') whenever $u', a', b' \in \{0,1\}$ and $c', d' \in \{-1,0,1\}$, and a weighted directed arc

$$(u', a', b', c', d') \xrightarrow{a'+b'-c''-d''} (u'', a'', b'', c'', d''),$$

whenever $u'' = 1-u'$,

$$s' = u' - a' + b' + c' - 2c'' \in \{0,1\},$$

and

$$t' = u' + a' - b' + d' - 2d'' \in \{0,1\}.$$

Note that, according to these definitions, whenever (8) holds there is an arc

$$(u_j, a_j, b_j, c_{j-1}, d_{j-1}) \xrightarrow{a_j+b_j-c_j-d_j} (u_{j+1}, a_{j+1}, b_{j+1}, c_j, d_j),$$

in the graph. Therefore, there is a one-to-one correspondence between n-periodic sequences $\{u_j\}_{j\in\mathbb{Z}}$, where $u_j + u_{j-1} = 1$, $\{a_j\}_{j\in\mathbb{Z}}$, $\{b_j\}_{j\in\mathbb{Z}}$, $\{c_j\}_{j\in\mathbb{Z}}$, $\{d_j\}_{j\in\mathbb{Z}}$ satisfy relation (8) with the corresponding sum of weights $w = \sum_{j=0}^{n-1}\left(a_j+b_j-c_j-d_j\right)$ and the directed walks of length n in the graph for which the sum of the weights of the arcs equals w. Thus to verify (9), it suffices to show that the graph does not contain any walk of strictly negative weight.

We investigated the weighted directed graph G with the aid of a computer. It turns out that G, a digraph on 72 vertices, has 33 strongly connected components. Here, two vertices of a directed graph are said to be strongly connected if they are contained together in a directed cycle. The relation of being strongly connected is an equivalence relation on the set of vertices; the equivalence classes of this relation are called the the strongly connected components of the directed graph.

One of these strongly connected components has size 40 (that is, contains 40 vertices), denoted by H, and further 32 strongly connected components have size 1. Obviously, all strongly connected components of size 1 contain no arc at all. The weighted directed graph H has 8 arcs of weight -1, 32 arcs of weight 0, 80 arcs of weight 1, 32 arcs of weight 2, and further 8 arcs of weight 3.

So we are done if we can show that the weight of each directed walk in the directed graph H is nonnegative. Using standard graph-theory tools of MAGMA [1] it is easy to verify that the component H has no negative-weight walk. Note that the running time is negligible. This completes the proof. $\square$

5. Concluding remarks

Combining our results with the work of Mesnager in [13, 14], the bentness of binomial function $f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$, where m is an positive integer, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$, has been completely characterized: $f_{a,b}$ is bent if and only if the Kloosterman sum $K_m(a^{2^m+1}) = 1 + \sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^m\left(a^{2^m+1}x+\frac{1}{x}\right)}$ equals 4. A related question is whether the bent function arising from Theorem 2 is hyper-bent. We have checked by computer that the answer is no in all cases when $m = 4, 6, 8$ and 10, and we believe that the answer is no in general.

References

[1] W. Bosma, J . Cannon, *Handbook of Magma Functions*, School of Mathematics and Statistics, University of Sydney, Sydney, 1999.

[2] C. Carlet, *Open problems on binary bent functions*, Open problems in mathematics and computational science, Springer, Cham, 203–241, 2014.

[3] C. Carlet, S. Mesnager, Four decades of research on bent functions, *Designs, Codes and Cryptography* 78(1), 5–50, 2016.

[4] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge,2020.

[5] J. Dillon, *Elementary Hadamard difference sets*, PhD dissertation, Univ. of Maryland, 1974.

[6] J-P. Flori, S. Mesnager, G. Cohen, *Binary Kloosterman sums with value* 4, IMA International Conference on Cryptography and Coding, Springer, Berlin, Heidelberg, 61–78, 2011.

[7] J-P Flori, S. Mesnager, Dickson polynomials, hyperelliptic curves and hyper-bent functions, *7th International conference SETA* 2012, LNCS 7280, Springer, 40–52, 2012.

[8] J-P. Flori, *A conjecture about Gauss sums and bentness of binomial Boolean functions*, International Workshop on the Arithmetic of Finite Fields, Springer, Cham, 143–159, 2016.

[9] B. Gross, N. Koblitz, Gauss sums and the p-adic Γ-function, *Ann. Math.* 109, 569–581, 1979.

[10] H. D. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, *Finite Fields and Their Applications* 7(2), 253–286, 2001.

[11] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

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

[13] S. Mesnager, A new class of bent boolean functions in polynomial forms, *Proceedings of international Workshop on Coding and Cryptography, WCC* 2009, 5–18, 2009.

[14] S. Mesnager, A new class of bent and hyper-bent Boolean functions in polynomial forms, *Design, Codes and Cryptography* 59(1-3), 265–279, 2011.

[15] S. Mesnager, Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials, *IEEE Transactions on Information Theory*, 57(9): 5996–6009, 2011.

[16] S. Mesnager, *Bent functions*, Springer International Publishing, 2016.

[17] O. S. Rothaus, On bent functions, *J. Comb. Theory*, Ser. A 20, 300–305, 1976.

[18] A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* 55, 497–508, 1948.