SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2018, Vol. 61 032104:1–032104:14
doi: 10.1007/s11432-016-0624-x

Three new infinite families of bent functions

Libo WANG[1,2], Baofeng WU[1*], Zhuojun LIU[2] & Dongdai LIN[1]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190*, China*

Received 29 September 2016/Accepted 6 December 2016/Published online 25 August 2017

Abstract Bent functions are maximally nonlinear Boolean functions with an even number of variables. They are closely related to some interesting combinatorial objects and also have important applications in coding, cryptography and sequence design. In this paper, we firstly give a necessary and sufficient condition for a type of Boolean functions, which obtained by adding the product of finitely many linear functions to given bent functions, to be bent. In the case that these known bent functions are chosen to be Kasami functions, Gold-like functions and functions with Niho exponents, respectively, three new explicit infinite families of bent functions are obtained. Computer experiments show that the proposed familes also contain such bent functions attaining optimal algebraic degree.

Keywords bent function, Hadamard matrix, Kasami function, Gold-like function, Niho exponent

Citation Wang L B, Wu B F, Liu Z J, et al. Three new infinite families of bent functions. Sci China Inf Sci, 2018, 61(3): 032104, doi: 10.1007/s11432-016-0624-x

1 Introduction

Let n be a positive integer. A Boolean function f with n variables is a map from the n-dimensional vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ is the binary finite field. Since $\mathbb{F}_{2^n}$, the finite filed with 2^n elements, naturally has an n-dimensional vector space structure over $\mathbb{F}_2$, f can also be viewed as a map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Boolean functions can play as important primitives in the design of cryptographic ciphers and their properties greatly influence the security of these ciphers [1–4].

Bent functions are Boolean functions with an even number of variables having the highest possible nonlinearity. They were introduced by Rothaus [5] in 1976, but already studied by Dillon [6] in his Ph.D thesis in 1974. Bent functions have been extensively studied not only for their own sake as interesting combinatorial objects but also due to their important applications in coding [7, 8], cryptography [9], sequence design [10] and graph theory [11, 12]. The complete classification of bent functions is still elusive and looks hopeless. Therefore, not only their characterizations, but also their generations are challenging problems. However, there has been a lot of progress in the constructions of bent functions. These constructions divides into two categories: the primary constructions—giving bent functions from scratch, and the secondary ones—building new bent functions from one or several given bent functions. For an non-exhaustive list of references dealing with these two kinds of constructions, see [13–24]. On the other hand, every bent function has a dual function, which is a bent function as well. Thus new bent

* Corresponding author (email: wubaofeng@iie.ac.cn)

functions can also be obtained by determining duals of known ones. However, it is generally very hard to explicitly compute dual functions of known bent functions.

Recently, Mesnager proved the sufficient condition for a Boolean function to be bent, given by Carlet in [25], is also necessary [23], and then she provided some new primary and secondary constructions of bent functions, whose dual functions were also explicitly determined. Two families of Mesnager's bent functions were constructed by adding the product of two linear functions to some known bent functions, which inspired Xu et al. [26] to construct several classes of Boolean functions with few Walsh spectra values by adding the product of two or three linear functions to some known bent functions. Motivated by these previous work, in this paper, we deal with a general case, that is, we construct new classes of bent functions by adding the product of finitely many linear functions to some known bent functions. In the case these known bent functions are chosen to be Kasami functions, Gold-like functions and functions with Niho exponents, respectively, three new explicit infinite families of bent functions are obtained. Computer experiments show that the proposed families also contain such bent functions attaining optimal algebraic degree. It is known that constructing bent functions with optimal algebraic degree is difficult in general, some classes of bent functions constructed in [15] having this property.

The rest of the paper is organized as follows. In Section 2, we fix our main notations and introduce some preliminaries. In Section 3, we investigate the Walsh transform of a special type of Boolean functions, giving a necessary and sufficient condition for such type of Boolean functions to be bent. In Section 4, we present three new infinite families of bent functions. Concluding remarks are given in Section 5.

2 Preliminaries

A Boolean function f on the finite field $\mathbb{F}_{2^n}$ is a mapping from $\mathbb{F}_{2^n}$ to the prime field $\mathbb{F}_2$. By Lagrange interpolation, it can be expressed as a univariate polynomial of the form $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$, where $a_i \in \mathbb{F}_{2^n}$, $0 \leqslant i \leqslant 2^n - 1$. Since f is a Boolean function, namely, f satisfies $f^2 = f$, there are some constraints on the coefficients of f. More precisely, we have $a_0, a_{2^n-1} \in \mathbb{F}_2$ and $a_{2i} = a_i^2$ for every $1 \leqslant i \leqslant 2^n - 2$, where $2i$ is taken modulo $2^n - 1$. This allows representing f in a unique trace expansion called its polynomial form. Recall that for any positive integers k, the absolute trace function over $\mathbb{F}_{2^k}$, denoted by $\mathrm{Tr}_1^k(\cdot)$, is defined as $\mathrm{Tr}_1^k(x) = \sum_{i=0}^{k-1} x^{2^i}$ for any $x \in \mathbb{F}_{2^k}$. The polynomial form of a Boolean function f defined on $\mathbb{F}_{2^n}$ is

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}),$$

where Γ_n is a set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and $\epsilon = \mathrm{wt}(f) \pmod 2$, where $\mathrm{wt}(f)$ is the cardinality of $\mathrm{supp} = \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$, the support of f. The algebraic degree of f is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$, and equal to n if $\epsilon = 1$. Note that the 2-weight of an integer j, denoted by $\mathrm{wt}_2(j)$, is referred to the number of 1's in its binary expansion.

The Walsh transform of a Boolean function f on $\mathbb{F}_{2^n}$ is defined as

$$\widehat{\chi_f}(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(wx)},$$

for any $w \in \mathbb{F}_{2^n}$. Bent functions are those Boolean functions having very special Walsh transform.

Definition 1. A Boolean function $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called bent if $\widehat{\chi_f}(w) = \pm 2^{\frac{n}{2}}$ for every $w \in \mathbb{F}_{2^n}$.

From the definition, it can be seen that a bent function must be with an even number of variables. It can be proved that the algebraic degree of an n-variable bent function is upper bounded by $n/2$. Besides, bent functions occur in pairs. In fact, given an n-variable bent function f, we can define its dual function, denoted by $\tilde{f}$, by the relation

$$(-1)^{\tilde{f}(x)} = \frac{\widehat{\chi_f}(x)}{2^{\frac{n}{2}}}.$$

Due to the involution law of Walsh transform, the dual of a bent function is bent as well, and we have $\tilde{\tilde{f}} = f$. A bent function f is said to be self-dual if $\tilde{f} = f$, while it is said to be anti-self-dual if $\tilde{f} = f + 1$. For more discussions on self-dual and anti-self-dual bent functions, we refer to [27].

To end this section, we recall the definition of Hadamard matrices. A Hadamard matrix H of order n is an $n \times n$ matrix whose entries are ± 1 satisfying

$$HH^{\mathrm{T}} = nI_n,$$

where H^{T} represents the transpose of H and I_n is the identity matrix of order n.

3 Walsh transform of a type of Boolean functions

In this section, we investigate the Walsh transform of a class of n-variable Boolean functions having the polynomial form

$$f(x) = g(x) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x), \tag{1}$$

where $k \geqslant 2$ is an integer, $u_i \in \mathbb{F}_{2^n}^*$ for $1 \leqslant i \leqslant k$, and $g(x)$ is an n-variable Boolean function over $\mathbb{F}_{2^n}$, based on which we derive a necessary and sufficient condition for such Boolean functions to be bent.

To simplify the proof of our main result in the sequel, we fix some notations firstly.

For $1 \leqslant i \leqslant k-1$, we define the set U_i as

$$U_i = \left\{ \sum_{j=1}^{i} u_{t_j} \;\middle|\; \{t_1, t_2, \ldots, t_i\} \subseteq \{1, 2, \ldots, k-1\} \right\}, \tag{2}$$

and set $U_0 = \{0\}$.

For an integer $0 \leqslant i < 2^{k-1}$, denote its binary expansion by $i = \sum_{j=1}^{k-1} i_j 2^{j-1}$. We always distinguish the integer i with the binary vector $(i_{k-1}, i_{k-2}, \ldots, i_1) \in \mathbb{F}_2^k$, and use $\mathrm{wt}_2(i)$ to denote the Hamming weight of the corresponding binary vector. Let $x_i = \sum_{j=1}^{k-1} i_j u_j$ and denote the Walsh transform of g at x_i for $0 \leqslant i < 2^{k-1}$ by a column vector $(\widehat{\chi_g}(a + x_i))_{0 \leqslant i < 2^{k-1}}$. For $0 \leqslant i < 2^{k-1}$ we also define

$$T_i = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_1^n(u_j x) = i_j,\ 1 \leqslant j \leqslant k-1\}$$

and

$$S_i(a) = \sum_{x \in T_i} (-1)^{g(x) + \mathrm{Tr}_1^n(ax)},$$

for any $a \in \mathbb{F}_{2^n}$, and use a column vector $(S_i(a))_{0 \leqslant i < 2^{k-1}}$ to collect these values.

For any square matrix M and a positive integer r, we use $M^{\otimes r}$ to represent its r-fold tensor product.

The following lemma gives the Walsh transform of the Boolean function f.

Lemma 1. Notations as above. For every $a \in \mathbb{F}_{2^n}$, we have

$$\widehat{\chi_f}(a) = \widehat{\chi_g}(a) - \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^i \widehat{\chi_g}(a + u) + \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^i \widehat{\chi_g}(a + u_k + u). \tag{3}$$

Moreover, we have

$$\big(\widehat{\chi_g}(a + x_i)\big)_{0 \leqslant i < 2^{k-1}} = A_{2^{k-1}} \big(S_i(a)\big)_{0 \leqslant i < 2^{k-1}}, \tag{4}$$

where

$$A_{2^{k-1}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes (k-1)}$$

is a Hadamard matrix of order 2^{k-1}.

Proof. We proceed by induction on k. When $k=2$, for any $a\in\mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{\chi_f}(a) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(ax)}\\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{g(x)+\mathrm{Tr}_1^n(u_1x)\mathrm{Tr}_1^n(u_2x)+\mathrm{Tr}_1^n(ax)}\\ &= \sum_{x\in T_0}(-1)^{g(x)+\mathrm{Tr}_1^n(ax)}+\sum_{x\in T_1}(-1)^{g(x)+\mathrm{Tr}_1^n((a+u_2)x)}\\ &= S_0(a)+S_1(a+u_2)\\ &= \widehat{\chi_g}(a)-S_1(a)+S_1(a+u_2). \end{aligned}\tag{5}$$

The last equality is due to

$$\widehat{\chi_g}(a)=S_0(a)+S_1(a).\tag{6}$$

Besides, we have

$$\begin{aligned}\widehat{\chi_g}(a+u_1) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{g(x)+\mathrm{Tr}_1^n((a+u_1)x)}\\ &= \sum_{x\in T_0}(-1)^{g(x)+\mathrm{Tr}_1^n((a+u_1)x)}+\sum_{x\in T_1}(-1)^{g(x)+\mathrm{Tr}_1^n((a+u_1)x)}\\ &= S_0(a)-S_1(a). \end{aligned}\tag{7}$$

We can rewrite (6) and (7) into a matrix form as

$$\begin{pmatrix}\widehat{\chi_g}(a)\\ \widehat{\chi_g}(a+u_1)\end{pmatrix}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}S_0(a)\\ S_1(a)\end{pmatrix},$$

which indicates that Eq. (4) holds. Besides, it is easy to see

$$S_1(a)=\frac{1}{2}\big(\widehat{\chi_g}(a)-\widehat{\chi_g}(a+u_1)\big).\tag{8}$$

Substituting a by $a+u_2$ in (8), we can get

$$S_1(a+u_2)=\frac{1}{2}\big(\widehat{\chi_g}(a+u_2)-\widehat{\chi_g}(a+u_2+u_1)\big).\tag{9}$$

Plugging (8) and (9) into (5), we obtain

$$\begin{aligned}\widehat{\chi_f}(a) &= \widehat{\chi_g}(a)-S_1(a)+S_1(a+u_2)\\ &= \widehat{\chi_g}(a)-\frac{1}{2}\big(\widehat{\chi_g}(a)-\widehat{\chi_g}(a+u_1)\big)+\frac{1}{2}\big(\widehat{\chi_g}(a+u_2)-\widehat{\chi_g}(a+u_2+u_1)\big),\end{aligned}$$

which is in consistent with (3). Therefore, the conclusion holds when $k=2$.

Let $k>2$ and assume the conclusion holds for $k-1$, then we will prove that they also hold for k.

For any $a\in\mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{\chi_f}(a) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(ax)}\\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{g(x)+\prod_{i=1}^{k}\mathrm{Tr}_1^n(u_ix)+\mathrm{Tr}_1^n(ax)}\\ &= \sum_{0\leqslant i\leqslant 2^{k-1}-2} S_i(a)+S_{2^{k-1}-1}(a+u_k)\\ &= \widehat{\chi_g}(a)-S_{2^{k-1}-1}(a)+S_{2^{k-1}-1}(a+u_k).\end{aligned}\tag{10}$$

The last equality holds because

$$\widehat{\chi_g}(a) = \sum_{0\leqslant i\leqslant 2^{k-1}-1} S_i(a).$$

In order to prove (4), we firstly need to express each component of $\big(\widehat{\chi_g}(a+x_i)\big)_{0\leqslant i<2^{k-1}}$ by the components of $\big(S_i(a)\big)_{0\leqslant i<2^{k-1}}$.

For any $0\leqslant c<2^{k-1}$ distinguished with $(c_{k-1},c_{k-2},\ldots,c_1)$ by its binary expansion, from now on we use $\widehat{\chi_g}(a+x_c)_{2^{k-1}}$ to denote the c-th component of $\big(\widehat{\chi_g}(a+x_i)\big)_{0\leqslant i<2^{k-1}}$ for clarity. Then we have

$$\begin{aligned}
\widehat{\chi_g}(a+x_c)_{2^{k-1}} &= \widehat{\chi_g}\left(a+\sum_{j=1}^{k-1}c_ju_j\right)\\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{g(x)+\mathrm{Tr}_1^n\left((a+\sum_{j=1}^{k-1}c_ju_j)x\right)}\\
&= \sum_{0\leqslant i<2^{k-1}}\sum_{x\in T_i}(-1)^{g(x)+\mathrm{Tr}_1^n\left((a+\sum_{j=1}^{k-1}c_ju_j)x\right)}\\
&= \sum_{0\leqslant i<2^{k-1}}(-1)^{\sum_{j=1}^{k-1}c_ji_j}S_i(a)\\
&= \begin{cases}\sum\limits_{0\leqslant i<2^{k-1}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a), & \text{if } c_{k-1}=0,\\ \sum\limits_{0\leqslant i<2^{k-1}}(-1)^{\sum_{j=1}^{k-2}c_ji_j+i_{k-1}}S_i(a), & \text{if } c_{k-1}=1.\end{cases}\\
&= \begin{cases}\sum\limits_{0\leqslant i<2^{k-2}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a)+\sum\limits_{0\leqslant i<2^{k-2}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a), & \text{if } c_{k-1}=0,\\ \sum\limits_{0\leqslant i<2^{k-2}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a)-\sum\limits_{0\leqslant i<2^{k-2}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a), & \text{if } c_{k-1}=1.\end{cases}
\end{aligned}\tag{11}$$

Similarly, for any $0\leqslant c<2^{k-2}$ distinguished with a binary vector $(c_{k-2},c_{k-3},\ldots,c_1)\in\mathbb{F}_2^{k-2}$, the c-th component of $\big(\widehat{\chi}_g(a+x_i)\big)_{0\leqslant i<2^{k-2}}$ can be represented as

$$\begin{aligned}
\widehat{\chi_g}(a+x_c)_{2^{k-2}} &= \widehat{\chi_g}\left(a+\sum_{j=1}^{k-2}c_ju_j\right)\\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{g(x)+\mathrm{Tr}_1^n\left((a+\sum_{j=1}^{k-2}c_ju_j)x\right)}\\
&= \sum_{0\leqslant i<2^{k-2}}(-1)^{\sum_{j=1}^{k-2}c_ji_j}S_i(a).
\end{aligned}\tag{12}$$

By induction, we have

$$\big(\widehat{\chi_g}(a+x_i)\big)_{0\leqslant i<2^{k-2}} = A_{2^{k-2}}\big(S_i(a)\big)_{0\leqslant i<2^{k-2}},\tag{13}$$

where

$$A_{2^{k-2}} = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}^{\otimes(k-2)}.$$

From (11)–(13), we can get

$$\begin{aligned}
\big(\widehat{\chi_g}(a+x_i)\big)_{0\leqslant i<2^{k-1}} &= \begin{pmatrix}A_{2^{k-2}} & A_{2^{k-2}}\\ A_{2^{k-2}} & -A_{2^{k-2}}\end{pmatrix}\begin{pmatrix}\big(S_i(a)\big)_{0\leqslant i<2^{k-2}}\\ \big(S_{2^{k-1}+i}(a)\big)_{0\leqslant i<2^{k-2}}\end{pmatrix}\\
&= \begin{pmatrix}A_{2^{k-2}} & A_{2^{k-2}}\\ A_{2^{k-2}} & -A_{2^{k-2}}\end{pmatrix}\Big(S_i(a)\Big)_{0\leqslant i<2^{k-1}}.
\end{aligned}\tag{14}$$

Therefore, we have

$$A_{2^{k-1}} = \begin{pmatrix} A_{2^{k-2}} & A_{2^{k-2}} \\ A_{2^{k-2}} & -A_{2^{k-2}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes A_{2^{k-2}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes(k-1)}. \tag{15}$$

Thus Eq. (4) is proved. We next prove Eq. (3) also holds.

Let $A_{2^{k-1},j}$ denote the element of $A_{2^{k-1}}$ lying in the j-th column and the last row, $0 \leqslant j < 2^{k-1}$. We claim that $A_{2^{k-1},j}$ is completely determined by $\mathrm{wt}_2(j)$, more precisely, we have

$$A_{2^{k-1},j} = \begin{cases} 1, & \text{if } \mathrm{wt}_2(j) \text{ is even}, \\ -1, & \text{if } \mathrm{wt}_2(j) \text{ is odd}. \end{cases}$$

In fact, let $j = \sum_{i=1}^{k-1} j_i 2^{i-1}$. It is easy to observe that

$$A_{2^{k-1},j} = \begin{cases} A_{2^{k-2},j}, & \text{if } j_{k-1} = 0, \\ -A_{2^{k-2},j-2^{k-2}}, & \text{if } j_{k-1} = 1, \end{cases}$$

i.e., $A_{2^{k-1},j} = (-1)^{j_{k-1}} A_{2^{k-2},j-j_{k-1}2^{k-2}}$. Inductively, we can get

$$\begin{aligned} A_{2^{k-1},j} &= (-1)^{\sum_{i=2}^{k-1} j_i} A_{2,j-\sum_{i=2}^{k-1} j_i 2^{i-1}} = (-1)^{\sum_{i=2}^{k-1} j_i} A_{2,j_1} \\ &= \begin{cases} (-1)^{\sum_{i=2}^{k-1} j_i}, & \text{if } j_1 = 0, \\ (-1)^{\sum_{i=2}^{k-1} j_i + 1}, & \text{if } j_1 = 1 \end{cases} \\ &= (-1)^{\sum_{i=1}^{k-1} j_i} = (-1)^{\mathrm{wt}_2(j)}. \end{aligned} \tag{16}$$

At last, we compute $S_{2^{k-1}}(a)$ by (4). Note that $A_{2^{k-1}}$ is a symmetric Hadamard matrix of order 2^{k-1}. Combining (4) and (16), we can easily get

$$S_{2^{k-1}-1}(a) = \frac{1}{2^{k-1}} \sum_{i=0}^{2^{k-1}-1} (-1)^{\mathrm{wt}_2(i)} \widehat{\chi_g}(a + x_i) = \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} (-1)^i \sum_{u \in U_i} \widehat{\chi_g}(a + u), \tag{17}$$

where the last equality is due to $x_i \in U_{\mathrm{wt}_2(i)}$. Substituting a by $a + u_k$ in (17), we get

$$S_{2^{k-1}-1}(a + u_k) = \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} (-1)^i \sum_{u \in U_i} \widehat{\chi_g}(a + u + u_k). \tag{18}$$

Plugging (17) and (18) into (10), we can obtain (3). The proof is completed.

Remark 1. Note that if $u_i = u_j$ for some $1 \leqslant i,\ j \leqslant k$ with $i \neq j$, $f(x)$ degenerates to the form $f(x) = g(x) + \prod_{i=1}^{k-1} \mathrm{Tr}_1^n(u_i x)$. Besides, if $\sum_{i=1}^{k} u_i = 0$, we have

$$\begin{aligned} f(x) &= g(x) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x) = g(x) + \prod_{i=1}^{k-1} \mathrm{Tr}_1^n(u_i x) \mathrm{Tr}_1^n\left(\sum_{i=1}^{k-1} u_i x\right) \\ &= g(x) + (k-1) \prod_{i=1}^{k-1} \mathrm{Tr}_1^n(u_i x) \\ &= \begin{cases} g(x) + \prod_{i=1}^{k-1} \mathrm{Tr}_1^n(u_i x), & \text{if } k \text{ is even}, \\ g(x), & \text{if } k \text{ is odd}. \end{cases} \end{aligned}$$

This is also a degenerate case. Therefore, in the following we always assume u_i $(1 \leqslant i \leqslant k)$ pairwise distinct and $\sum_{i=1}^{k} u_i \neq 0$.

Now we assume g is a bent function with dual function $\tilde{g}$ and f is the function defined in (1). By the definition of dual function and Lemma 1, we can easily obtain a sufficient and necessary condition for f to be bent.

Theorem 1. Notations as in Lemma 1 and assume g is a bent function on $\mathbb{F}_{2^n}$. Then the Boolean function f is bent if and only if

$$(-1)^{\tilde{g}(a)} - \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i+\tilde{g}(a+u)} + \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i+\tilde{g}(a+u+u_k)} = \pm 1,$$

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

4 Three new infinite families of bent functions

In this section, we explicitly give three new infinite families of bent functions of the form (1) by choosing the bent function g in Theorem 1 to be some well-known ones, namely, the Kasami bent functions, the Gold-like bent functions and bent functions with Niho exponents.

4.1 New infinite family of bent functions from Kasami functions

Let $m \geqslant 2$ be a positive even integer, $n = 2m$ and $\lambda \in \mathbb{F}_{2^m}^*$. Then the Kasami function $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$ is a bent function, whose dual function is

$$\tilde{g}(x) = \mathrm{Tr}_1^m(\lambda^{-1} x^{2^m+1}) + 1, \tag{19}$$

given by Mesnager in [23]. In the following, we make use of the Kasami functions to get a new infinite family of bent functions based on Theorem 1.

Theorem 2. Let $m \geqslant 2$ be a positive even integer, $n = 2m$ and $\lambda \in \mathbb{F}_{2^m}^*$. Assume u_i $(1 \leqslant i \leqslant k)$ are k $(k \geqslant 2)$ pairwise distinct elements in $\mathbb{F}_{2^n}^*$. Define a Boolean function f on $\mathbb{F}_{2^n}$ as

$$f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x).$$

If $\mathrm{Tr}_1^n(\lambda^{-1} u_i^{2^m} u_j) = 0$ for any $1 \leqslant i < j \leqslant k$, then f is bent.

Proof. Let $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$. By Theorem 1, we only need to verify that for each $a \in \mathbb{F}_{2^n}$,

$$\Delta_a := (-1)^{\tilde{g}(a)} - \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i+\tilde{g}(a+u)} + \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i+\tilde{g}(a+u+u_k)}$$

is equal to ± 1. By Eq. (19) we have

$$\begin{aligned} \Delta_a = & -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1} a^{2^m+1})} + \frac{1}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{u \in U_\ell} (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a+u)^{2^m+1}\right)} \\ & - \frac{1}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{u \in U_\ell} (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a+u_k+u)^{2^m+1}\right)}. \end{aligned} \tag{20}$$

For $0 \leqslant \ell \leqslant k-1$, $u \in U_\ell$, where U_ℓ is defined by (2), i.e., $u = \sum_{j=1}^{\ell} u_{i_j}$, we define c_u, t_u and t'_u as follows:

$$c_u = \begin{cases} 0, & \text{if } u \in U_0, \\ \sum\limits_{j=1}^{\ell} \mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m} u_{i_j} + a u_{i_j}^{2^m} + u_{i_j}^{2^m+1})\right), & \text{otherwise;} \end{cases}$$

$$t_u = \begin{cases} 0, & \text{if } u \in U_0 \text{ or } U_1, \\ \sum\limits_{\{j_1,j_2\}\subseteq\{i_1,\ldots,i_\ell\}} \mathrm{Tr}_1^n(\lambda^{-1}u_{j_1}^{2^m}u_{j_2}), & \text{otherwise;} \end{cases}$$

$$t'_u = \begin{cases} 0, & \text{if } u \in U_0, \\ \sum\limits_{\{j_1,j_2\}\subseteq\{i_1,\ldots,i_\ell,k\}} \mathrm{Tr}_1^n(\lambda^{-1}u_{j_1}^{2^m}u_{j_2}), & \text{otherwise.} \end{cases}$$

Note that $\{i_1, i_2 \ldots, i_\ell\} \subseteq \{1, 2, \ldots, k-1\}$. By induction, it is easy to get

$$\begin{aligned} (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a+u)^{2^m+1}\right)} &= (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}(-1)^{c_u+t_u}, \\ (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a+u+u_k)^{2^m+1}\right)} &= (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a+u_k)^{2^m+1}\right)}(-1)^{c_u+t'_u}. \end{aligned}$$

Since the condition $\mathrm{Tr}_1^n(\lambda^{-1}u_i^{2^m}u_j) = 0$ for $1 \leqslant i < j \leqslant k$ implies $t_u = t'_u = 0$, we have

$$(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+u)^{2^m+1})} = (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}(-1)^{c_u}, \tag{21}$$

$$(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+u+u_k)^{2^m+1})} = (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+u_k)^{2^m+1})}(-1)^{c_u}. \tag{22}$$

Combining (20)–(22), we get

$$\begin{aligned} \Delta_a = &-(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left(1 - \frac{1}{2^{k-1}}\sum_{\ell=0}^{k-1}(-1)^\ell \sum_{u\in U_\ell}(-1)^{c_u}\right) \\ &-(-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}u_k + au_k^{2^m} + u_k^{2^m+1} + a^{2^m+1})\right)}\left(\frac{1}{2^{k-1}}\sum_{\ell=0}^{k-1}(-1)^\ell \sum_{u\in U_\ell}(-1)^{c_u}\right). \end{aligned}$$

When $\mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}u_k + au_k^{2^m} + u_k^{2^m+1})) = 0$, we have

$$\Delta_a = -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}.$$

When $\mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}u_k + au_k^{2^m} + u_k^{2^m+1})) = 1$, we have

$$\Delta_a = -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left(1 - \frac{2}{2^{k-1}}\sum_{\ell=0}^{k-1}(-1)^\ell \sum_{u\in U_\ell}(-1)^{c_u}\right). \tag{23}$$

For $u = \sum_{j=1}^{\ell} u_{i_j} \in U_\ell$, where $\{i_1, i_2 \ldots, i_\ell\} \subseteq \{1, 2, \ldots, k-1\}$, we write $c_u = \sum_{j=1}^{\ell} c_{i_j}$ for simplicity and denote $C_\ell = \{c_u \mid u \in U_\ell\}$, $1 \leqslant \ell \leqslant k-1$. Then Eq. (23) can be written as

$$\begin{aligned} \Delta_a &= -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left(1 - \frac{2}{2^{k-1}}\sum_{\ell=0}^{k-1}(-1)^\ell \sum_{c_u\in C_\ell}(-1)^{c_u}\right) \\ &= -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left(1 - \frac{2}{2^{k-1}}\sum_{\ell=0}^{k-1}(-1)^\ell \sum_{\sum_{j=1}^{\ell} c_{i_j}\in C_\ell}(-1)^{\sum_{j=1}^{\ell} c_{i_j}}\right) \\ &= -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left(1 - \frac{2}{2^{k-1}}\prod_{i=1}^{k-1}\left(1-(-1)^{c_i}\right)\right) \\ &= \begin{cases} (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{if } c_i = 1 \text{ for } 1 \leqslant i \leqslant k-1, \\ -(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{otherwise.} \end{cases} \end{aligned}$$

So, we finally get $\Delta_a = \pm 1$ for each $a \in \mathbb{F}_{2^n}$, which implies that f is bent.

It worth noting that $\mathrm{Tr}_1^n(\lambda^{-1}u_i^{2^m}u_j) = 0$ if $u_i,\ u_j \in \mathbb{F}_{2^m}^*$ (note that $\lambda \in \mathbb{F}_{2^m}^*$) for $1 \leqslant i, j \leqslant k$. The following Corollary is straightforward from Theorem 2.

Corollary 1. Let $m \geqslant 2$ be a positive even integer, $n = 2m$ and $\lambda \in \mathbb{F}_{2^m}^*$. Assume u_i $(1 \leqslant i \leqslant k)$ are k $(k \geqslant 2)$ pairwise distinct elements in $\mathbb{F}_{2^m}^*$. Define a Boolean function on $\mathbb{F}_{2^n}$ as

$$f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x).$$

Then f is bent.

Remark 2. When $k = 2$ and $k = 3$, the bent function f presented in Theorem 2 has already been given in [23] by Mesnager and in [26] by Xu et al., respectively.

Now we talk about the algebraic degree of f in Theorem 2. When $k > n/2$, it seems that the algebraic degree of f equals to k since the product of k linear functions is involved in the expression of f, which contradicts the well-known fact that the algebraic degree of a bent function over $\mathbb{F}_{2^n}$ no more than $n/2$. However, in the following we will observe that the algebraic degree of f does not exceed $n/2$, because the terms of algebraic degree exceeding $n/2$ can be canceled under the condition of Theorem 2.

Let l be an integer with $2 < l \leqslant k$ and assume $\{i_1, i_2, \ldots, i_l\} \subseteq \{0, 1, \ldots, n-1\}$ is a set of l pairwise distinct integers. Denote the set of all permutations on $\{i_1, i_2, \ldots, i_l\}$ by $\mathcal{P}_{i_1,i_2,\ldots,i_l}$. It is clear that the term of algebraic degree l in the expression of f has the form

$$t_l = \left(\sum_{\{i_1,\ldots,i_l\} \in \mathcal{P}_{i_1,i_2,\ldots,i_l}} \sum_{\{u_{j_1},\ldots,u_{j_l}\} \subseteq \{u_1,\ldots,u_k\}} \prod_{r=1}^{l} u_{j_r}^{2^{i_r}} \right) x^{\sum_{j=1}^{l} 2^{i_j}}. \tag{24}$$

If there exists a set $\{i_1, i_2, \ldots, i_l\} \subseteq \{0, 1, \ldots, n-1\}$ such that $t_l \neq 0$, then f must contain the term of algebraic degree l.

When $k > m$, now we show that under the condition $\mathrm{Tr}_1^n(\lambda^{-1} u_i^{2^m} u_j) = 0$ for $1 \leqslant i < j \leqslant k$, the terms of algebraic degree exceeding m does not exist. We just illustrate this fact under $m = 3$, $k = 4$; the general case can be similarly illustrated. In this case, the condition $\mathrm{Tr}_1^6(\lambda^{-1} u_i^{2^3} u_j) = 0$ for $1 \leqslant i < j \leqslant 4$ can be precisely written as

$$\begin{cases} \lambda^{-1}u_1^8u_2 + \lambda^{-2}u_1^{16}u_2^2 + \lambda^{-4}u_1^{32}u_2^4 + \lambda^{-1}u_1u_2^8 + \lambda^{-2}u_1^2u_2^{16} + \lambda^{-4}u_1^4u_2^{32} = 0, \\ \lambda^{-1}u_1^8u_3 + \lambda^{-2}u_1^{16}u_3^2 + \lambda^{-4}u_1^{32}u_3^4 + \lambda^{-1}u_1u_3^8 + \lambda^{-2}u_1^2u_3^{16} + \lambda^{-4}u_1^4u_3^{32} = 0, \\ \lambda^{-1}u_1^8u_4 + \lambda^{-2}u_1^{16}u_4^2 + \lambda^{-4}u_1^{32}u_4^4 + \lambda^{-1}u_1u_4^8 + \lambda^{-2}u_1^2u_4^{16} + \lambda^{-4}u_1^4u_4^{32} = 0, \\ \lambda^{-1}u_2^8u_3 + \lambda^{-2}u_2^{16}u_3^2 + \lambda^{-4}u_2^{32}u_3^4 + \lambda^{-1}u_2u_3^8 + \lambda^{-2}u_2^2u_3^{16} + \lambda^{-4}u_2^4u_3^{32} = 0, \\ \lambda^{-1}u_2^8u_4 + \lambda^{-2}u_2^{16}u_4^2 + \lambda^{-4}u_2^{32}u_4^4 + \lambda^{-1}u_2u_4^8 + \lambda^{-2}u_2^2u_4^{16} + \lambda^{-4}u_2^4u_4^{32} = 0, \\ \lambda^{-1}u_3^8u_4 + \lambda^{-2}u_3^{16}u_4^2 + \lambda^{-4}u_3^{32}u_4^4 + \lambda^{-1}u_3u_4^8 + \lambda^{-2}u_3^2u_4^{16} + \lambda^{-4}u_3^4u_4^{32} = 0. \end{cases} \tag{25}$$

Then we prove that there is no term of algebraic degree 4. Now, $l = 4$, $n = 2m = 6$, so $\{i_1, i_2, i_3, i_4\} \subseteq \{0, 1, 2, 3, 4, 5\}$ has $\binom{6}{4} = 15$ choices, and $\{u_{j_1}, u_{j_2}, u_{j_3}, u_{j_4}\} \subseteq \{u_1, u_2, u_3, u_4\}$ has only one choice. Therefore, once we select $\{i_1, i_2, i_3, i_4\}$, the coefficient of t_l in (24) becomes $\sum_{\{i_1,i_2,i_3,i_4\} \in \mathcal{P}_{i_1,i_2,i_3,i_4}} \prod_{r=1}^{4} u_r^{2^{i_r}}$. Specially, when $\{i_1, i_2, i_3, i_4\} = \{0, 1, 2, 3\}$, by multiplying the six equations of (25) by $u_3^2u_4^4 + u_3^4u_4^2$, $u_2^2u_4^4 + u_2^4u_4^2$, $u_2^2u_3^4 + u_2^4u_3^2$, $u_1^2u_4^4 + u_1^4u_4^2$, $u_1^2u_3^4 + u_1^4u_3^2$ and $u_1^2u_2^4 + u_1^4u_2^2$, respectively, and adding these six equations afterwards, we can get $\sum_{\{0,1,2,3\} \in \mathcal{P}_{0,1,2,3}} \prod_{r=1}^{4} u_{i_r}^{2^{i_r}} = 0$. Other cases can be computed similarly. So we observe that there is no term of algebraic degree 4 in f. For arbitrary m and k, we can do similarly as above, but the calculations and math expressions are rather complicated, we omit the details here.

Example 1. Let $m = 3$, $k = 4$, α be a primitive element of $\mathbb{F}_{2^6}$ with minimal polynomial $x^6 + x^4 + x^3 + x + 1$. Take $\lambda = 1$, $u_1 = \alpha$, $u_2 = \alpha^{10}$, $u_3 = \alpha^{43}$, $u_4 = \alpha^{48}$. With the aid of a computer, we can check $\mathrm{Tr}_1^6(\lambda^{-1} u_i^8 u_j) = 0$ for $1 \leqslant i < j \leqslant 4$ and $f(x) = \mathrm{Tr}_1^3(\lambda x^9) + \prod_{i=1}^{4} \mathrm{Tr}_1^6(u_i x)$ is a bent function, which is in consistent with the conclusion of Theorem 2.

Moreover, for each set $\{i_1, i_2, i_3, i_4\} \subseteq \{0, 1, 2, 3, 4, 5\}$, $\sum_{\{i_1,i_2,i_3,i_4\} \in \mathcal{P}_{i_1,i_2,i_3,i_4}} \prod_{r=1}^{4} u_r^{2^{i_r}} = 0$, but when $\{i_1, i_2, i_3\} = \{0, 1, 3\}$, $\sum_{\{i_1,i_2,i_3\} \in \mathcal{P}_{0,1,3}} \sum_{\{u_{j_1},u_{j_2},u_{j_3}\} \subseteq \{u_1,u_2,u_3,u_4\}} \prod_{r=1}^{3} u_{j_r}^{2^{i_r}} = \alpha^{47} \neq 0$, which implies that the algebraic degree of f does not exceed m, but can attain m. That is to say, Theorem 2 also contains such bent functions attaining optimal algebraic degree.

4.2 New infinite family of bent functions from gold-like functions

In this subsection, we construct a new infinite family of bent functions from Gold-like monomial functions. Firstly we comments on some results given in [23, 27].

In [27], Carlet et al. have shown that the quadratic Boolean function $f(x) = \mathrm{Tr}_1^{4t}(\lambda x^{2^t+1})$ defined on $\mathbb{F}_{2^{4t}}$, where $t \geqslant 2$ and $\lambda \in \mathbb{F}_{2^{4t}}^*$, is self-dual or anti-self-dual if $\lambda^{2^{3t+1}} + \lambda^2 = 1$ and $\lambda^{2^t+1} + \lambda^{2^{2t}+2^{3t}} = 0$. We point out that the condition $\lambda^{2^t+1} + \lambda^{2^{2t}+2^{3t}} = 0$ is redundant, that is, $\lambda^{2^{3t+1}} + \lambda^2 = 1$ implies $\lambda^{2^t+1} + \lambda^{2^{2t}+2^{3t}} = 0$. In fact, $\lambda^{2^{3t+1}} + \lambda^2 = 1$ if and only if $\lambda^{2^{3t}} + \lambda = 1$, which gives $\lambda + \lambda^{2^t} = 1$. Then we have $\lambda^{2^{3t}} = \lambda^{2^t}$, i.e., $\lambda = \lambda^{2^{2t}}$, from which $\lambda^{2^t+1} + \lambda^{2^{3t}+2^{2t}} = 0$ follows. In [23], Mesnager proved if $\lambda \in \mathbb{F}_{2^{4t}}^*$ satisfied $\lambda^{2^{3t}} + \lambda = 1$ or $\lambda^{(2^t+1)^2(2^t-1)} = 1$, then $\mathrm{Tr}_1^{4t}(\lambda x^{2^t+1})$ was self-dual bent. We point out that this result is not correct exactly. First, note that $\lambda^{2^{3t}} + \lambda = 1$ implies $\lambda = \lambda^{2^{2t}}$, i.e., $\lambda \in \mathbb{F}_{2^{2t}}^*$, and then $\lambda^{(2^t+1)^2(2^t-1)} = \lambda^{(2^{2t}-1)(2^t+1)} = 1$ follows. Next, we give an example, indicating that $\mathrm{Tr}_1^{4t}(\lambda x^{2^t+1})$ is not self-dual bent function when λ satisfies $\lambda^{(2^t+1)^2(2^t-1)} = 1$ but does not satisfy $\lambda^{2^{3t}} + \lambda = 1$.

Example 2. Let $t = 3$, α be a primitive element of $\mathbb{F}_{2^{12}}$ with minimal polynomial $x^{12} + x^8 + x^7 + x^5 + x^4 + x + 1$. Take $\lambda = \alpha^{65}$. With the aid of a computer, we can check $\lambda^{(2^3+1)^2(2^3-1)} = 1$, while $\lambda^{2^9} + \lambda = \alpha^{585} \neq 1$, and $\mathrm{Tr}_1^{12}(\lambda x^9)$ is not a self-dual bent function.

In fact, the condition $\lambda^{(2^t+1)^2(2^t-1)} = 1$ is equivalent to $\lambda \in \mathbb{F}_{2^{2t}}^*$. This is because $\lambda^{(2^t+1)^2(2^t-1)} = 1$ implies $\lambda^{\gcd((2^t+1)^2(2^t-1),2^{4t}-1)} = 1$, whereas

$$\begin{aligned}\gcd((2^t+1)^2(2^t-1), 2^{4t}-1) &= \gcd((2^t+1)(2^{2t}-1), 2^{4t}-1)\\ &= (2^{2t}-1)\cdot\gcd(2^t+1, 2^{2t}+1)\\ &= 2^{2t}-1.\end{aligned}$$

Anyway, Mesnager's statement is valid under the condition $\lambda^{2^{3t}} + \lambda = 1$, i.e., $\lambda^{2^t} + \lambda = 1$ (see the proof of [23, Lemma 23]). That is to say, when $\lambda^{2^t} + \lambda = 1$, we have

$$\tilde{f}(a) = \mathrm{Tr}_1^{4t}(\lambda a^{2^t+1}). \tag{26}$$

Then we can use the Gold-like monomial function $f(x)$ to construct a new infinite family of bent functions.

Theorem 3. Let t, $k \geqslant 2$ be two positive integers and u_i $(1 \leqslant i \leqslant k)$ be k pairwise distinct elements in $\mathbb{F}_{2^{4t}}^*$. Let $\lambda \in \mathbb{F}_{2^{4t}}^*$ such that $\lambda^{2^t} + \lambda = 1$. If $\mathrm{Tr}_1^{4t}(\lambda(u_i^{2^t}u_j + u_i u_j^{2^t})) = 0$ for all $1 \leqslant i < j \leqslant k$, then the Boolean function

$$f(x) = \mathrm{Tr}_1^{4t}(\lambda x^{2^t+1}) + \prod_{i=1}^{k} \mathrm{Tr}_1^{4t}(u_i x)$$

over $\mathbb{F}_{2^{4t}}$ is a bent function.

Proof. The proof is similar as that of Theorem 2, which will be omitted here.

The algebraic degree of $f(x)$ in Theorem 3 can also be studied as what has been done in the previous subsection. In the following we give an example to state that the function in Theorem 3 can attain optimal algebraic degree.

Example 3. Let $t = 2$, $k = 5$, α be a primitive element of $\mathbb{F}_{2^8}$ with minimal polynomial $x^8 + x^4 + x^3 + x^2 + 1$. Take $\lambda = \alpha^{68}$, $u_1 = \alpha^{17}$, $u_2 = \alpha^{22}$, $u_3 = \alpha^{93}$, $u_4 = \alpha^{43}$ and $u_5 = \alpha^{171}$. By a Magma program, we can check $\lambda + \lambda^{2^6} = 1$, $\mathrm{Tr}_1^8(\lambda(u_i^4 u_j + u_i u_j^4)) = 0$ for all $1 \leqslant i < j \leqslant 5$, and $f(x) = \mathrm{Tr}_1^8(\lambda x^5) + \prod_{i=1}^5 \mathrm{Tr}_1^8(u_i x)$ given by Theorem 3 is a bent function. Besides, for $\{i_1, i_2, i_3, i_4, i_5\} = \{0, 1, 2, 3, 4\}$, we have $\sum_{\{i_1,i_2,i_3,i_4,i_5\}\in\mathcal{P}_{0,1,2,3,4}} \prod_{r=1}^5 u_r^{2^{i_r}} = 0$, while when $\{i_1, i_2, i_3, i_4\} = \{0, 1, 2, 3\}$, $\sum_{\{i_1,i_2,i_3,i_4\}\in\mathcal{P}_{0,1,2,3}} \sum_{\{u_{j_1},u_{j_2},u_{j_3},u_{j_4}\}\subseteq\{u_1,u_2,u_3,u_4,u_5\}} \prod_{r=1}^4 u_{j_r}^{2^{i_r}} = \alpha^{185} \neq 0$, which implies that the algebraic degree of f does not exceed $2t$, but can be optimal.

Theorems 2 and 3 can also be extended to more general form. In fact, the Kasami function and the Gold-like monomial function belong to the more large family of bent functions known as quadratic bent functions. An important feature of such bent functions is that their dual functions are also quadratic ones. By quadratic bent functions whose duals are explicitly known, we can construct new infinite families of bent functions based on Theorem 1.

Theorem 4. Let g be a quadratic bent function over $\mathbb{F}_{2^n}$ and its dual has the form $\tilde{g}(x) = \sum_{i=1}^{l} \mathrm{Tr}_1^{n_i}(a_i x^{2^{k_i}+1}) + \mathrm{Tr}_1^n(bx) + c$, where $a_i \in \mathbb{F}_{2^{n_i}}$, $1 \leqslant i \leqslant l$, $b \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$. If $\sum_{i=1}^{l} \mathrm{Tr}_1^{n_i}(a_i(u_r^{2^{k_i}} u_s + u_r u_s^{2^{k_i}})) = 0$ for any $1 \leqslant r, s \leqslant l$, then the Boolean function

$$f(x) = g(x) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x)$$

over $\mathbb{F}_{2^n}$ is bent.

Theorem 4 can be proved with similarly arguments as those used in the proof of Theorem 2. The importance of this theorem lies in that, bent functions of higher or even optimal algebraic degree can be produced by quadratic bent functions.

4.3 New infinite family of bent functions from functions with Niho exponents

In this subsection, we construct a new infinite family of bent functions of the form $f(x) = g(x) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x)$ in the case $g(x)$ is a Niho bent function.

Niho bent functions were introduced by Dobbertin et al. in [28]. The authors constructed three infinite families of binomial Niho bent functions, one of which was later generalized by Leander and Kholoshainto to a family of bent functions with 2^r Niho exponents [29] having the form

$$g(x) = \mathrm{Tr}_1^n\left(ax^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\right),$$

where $r > 1$, $\gcd(r, m) = 1$, $a \in \mathbb{F}_{2^n}$ and $a + a^{2^m} = 1$. Note that for $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$,

$$\mathrm{Tr}_1^n(ax^{2^m+1}) = \mathrm{Tr}_1^m(ax^{2^m+1} + a^{2^m}x^{2^m+1}) = \mathrm{Tr}_1^m(x^{2^m+1}),$$

thus the expression of g can be rewritten as

$$g(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\right).$$

Take any $\alpha \in \mathbb{F}_{2^n}$ with $\alpha + \alpha^{2^m} = 1$. It was shown in [30] that the dual function of g is

$$\tilde{g}(x) = \mathrm{Tr}_1^m\left((\alpha(1 + x + x^{2^m}) + \alpha^{2^{n-r}} + x^{2^m}) \times (1 + x + x^{2^m})^{1/(2^r-1)}\right). \tag{27}$$

Theorem 5. Let $n = 2m$, r be a positive integer with $\gcd(r, m) = 1$ and $u_i \in \mathbb{F}_{2^m}^*$, $1 \leqslant i \leqslant k$. Then the Boolean function

$$f(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\right) + \prod_{i=1}^{k} \mathrm{Tr}_1^n(u_i x)$$

defined on $\mathbb{F}_{2^n}$ is bent.

Proof. Let

$$g(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\right).$$

For each $a \in \mathbb{F}_{2^n}$, by Theorem 1, we need only to verify that $\Delta_a = \Delta_1 + \Delta_2 = \pm 1$, where

$$\Delta_1 = (-1)^{\tilde{g}(a)} - \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i + \tilde{g}(a+u)},$$

$$\Delta_2 = \frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \sum_{u \in U_i} (-1)^{i+\tilde{g}(a+u+u_k)}.$$

Set $A = 1 + a + a^{2^m}$ and choose $\alpha \in \mathbb{F}_{2^n}$ with $\alpha + \alpha^{2^m} = 1$. It follows from (27) that

$$\tilde{g}(a) = \mathrm{Tr}_1^m \left((\alpha A + \alpha^{2^{n-r}} + a^{2^m}) A^{1/(2^r-1)} \right).$$

For $0 \leqslant i \leqslant k-1,\ u \in U_i$, i.e., $u = \sum_{j=1}^{i} u_{i_j}$, let

$$c_u = \mathrm{Tr}_1^m(uA^{1/(2^r-1)}) = \sum_{j=1}^{i} \mathrm{Tr}_1^m(u_{i_j} A^{1/(2^r-1)}).$$

Now we can write Δ_1 and Δ_2 as

$$\Delta_1 = (-1)^{\mathrm{Tr}_1^m((\alpha A+\alpha^{2^{n-r}}+a^{2^m})A^{1/(2^r-1)})} \left(1 - \frac{1}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{u \in U_\ell} (-1)^{c_u} \right),$$

$$\Delta_2 = (-1)^{\mathrm{Tr}_1^m((\alpha A+\alpha^{2^{n-r}}+a^{2^m}+u_k)A^{1/(2^r-1)})} \left(\frac{1}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{u \in U_\ell} (-1)^{c_u} \right).$$

When $\mathrm{Tr}_1^m(u_k A^{1/(2^r-1)}) = 0$, we have

$$\Delta_a = (-1)^{\mathrm{Tr}_1^m((\alpha A+\alpha^{2^{n-r}}+a^{2^m})A^{1/(2^r-1)})}.$$

When $\mathrm{Tr}_1^m(u_k A^{1/(2^r-1)}) = 1$, we have

$$\Delta_a = (-1)^{\mathrm{Tr}_1^m((\alpha A+\alpha^{2^{n-r}}+a^{2^m})A^{1/(2^r-1)})} \left(1 - \frac{2}{2^{r-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{u \in U_\ell} (-1)^{c_u} \right). \tag{28}$$

For $u = \sum_{j=1}^{\ell} u_{i_j} \in U_\ell$, where $\{i_1, i_2 \ldots, i_\ell\} \subseteq \{1, 2, \ldots, k-1\}$, we write $c_u = \sum_{j=1}^{\ell} c_{i_j}$ for simplicity and denote $C_\ell = \{c_u \mid u \in U_\ell\}$, $1 \leqslant \ell \leqslant k-1$. Then Eq. (28) can be written as

$$\begin{aligned}
\Delta_a &= (-1)^{\tilde{g}(a)} \left(1 - \frac{2}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{c_u \in C_\ell} (-1)^{c_u} \right) \\
&= (-1)^{\tilde{g}(a)} \left(1 - \frac{2}{2^{k-1}} \sum_{\ell=0}^{k-1} (-1)^{\ell} \sum_{\sum_{j=1}^{\ell} c_{i_j} \in C_\ell} (-1)^{\sum_{j=1}^{\ell} c_{i_j}} \right) \\
&= (-1)^{\tilde{g}(a)} \left(1 - \frac{2}{2^{k-1}} \prod_{i=1}^{k-1} \left(1 - (-1)^{c_i}\right) \right) \\
&= \begin{cases} -(-1)^{\tilde{g}(a)}, & \text{if } \ c_i = 1, \ \text{ for } \ 1 \leqslant i \leqslant k-1, \\ (-1)^{\tilde{g}(a)}, & \text{otherwise.} \end{cases}
\end{aligned}$$

So $\Delta_a = \pm 1$ for each $a \in \mathbb{F}_{2^n}$, which implies that $f(x)$ is bent.

Example 4. Let $m = 4,\ r = 3,\ k = 6$, α be a primitive element of $\mathbb{F}_{2^8}$ with minimal polynomial $x^8 + x^4 + x^3 + x^2 + 1$. We Take $u_1 = \alpha^{17},\ u_2 = \alpha^{51},\ u_3 = \alpha^{68},\ u_4 = \alpha^{102},\ u_5 = \alpha^{153}$ and $u_6 = \alpha^{170}$. Computer experiments show that $f(x) = \mathrm{Tr}_1^4(x^{17}) + \mathrm{Tr}_1^8(x^{226}) + \mathrm{Tr}_1^8(x^{196}) + \mathrm{Tr}_1^8(x^{166}) + \prod_{i=1}^{6} \mathrm{Tr}_1^8(u_i x)$ given by Theorem 5 is a bent function.

5 Concluding remarks

In this paper, three new infinite families of bent functions are obtained by adding the product of finitely many linear functions to such known bent functions as Kasami bent functions, Gold-like monomial bent functions and bent functions with 2^r Niho exponents, generalizing some recent work due to Mesnager and Xu et al. Computer experiments show that the proposed families also contain such bent functions attaining optimal algebraic degree. It remains to check whether the bent functions presented in this paper are affine inequivalent to known ones. Another interesting problem is to investigate their dual functions and other cryptographic properties.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61502482, 61379139, 11526215), National Key Research Program of China (Grant No. 2016YFB0800401), and "Strategic Priority Research Program" of Chinese Academy of Sciences (Grant No. XDA06010701).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Li L, Zhang W. Constructions of vectorial Boolean functions with good cryptographic properties. Sci China Inf Sci, 2016, 59: 119103
2 Matsui M. Linear cryptanalysis of DES cipher. In: Advances in Cryptology—Eurocrypt'93. Berlin: Springer, 1994. 386–397
3 Nyberg K. Perfect nonlinear S-boxes. In: Advances in Cryptology—EUROCRYPT. Berlin: Springer, 1991. 547: 378–386
4 Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans Inform Theory, 1984, 30: 776–780
5 Rothaus O S. On bent functions. J Comb Theory Ser A, 1976, 20: 300–305
6 Dillon J F. Elementary hadamard difference sets. Dissertation for Ph.D. Degree. Washington: University of Maryland, 1974
7 Canteaut A, Carlet C, Charpin P, et al. On cryptographic properties of the cosets of R(1; m). IEEE Trans Inform Theory, 2001, 47: 1494–1513
8 MacWilliams F J, Sloane N J. The Theory of Error-Correcting Codes. Amsterdam: North Holland, 1977
9 Carlet C. Boolean functions for cryptography and error correcting codes. Boolean Models Meth Math Comput Sci Eng, 2010, 2: 257–397
10 Olsen J, Scholtz R, Welch L. Bent-function sequences. IEEE Trans Inform Theory, 1982, 28: 858–864
11 Bernasconi A, Codenottl B, Vanderkam J M. A characterization of bent functions in terms of strongly regular graphs. IEEE Trans Comput, 2001, 50: 984–985
12 Tan Y, Pott A, Feng T. Strongly regular graphs associated with ternary bent functions. J Comb Theory Ser A, 2010, 117: 668–682
13 Budaghyan L, Kholosha A, Carlet C, et al. Univariate Niho bent functions from o-polynomials. IEEE Trans Inform Theory, 2016, 62: 2254–2265
14 Carlet C, Mesnager S. On Dillons class H of bent functions, Niho bent functions and o-polynomials. J Combin Theory Ser A, 2011, 118: 2392–2410
15 Jia W, Zeng X, Helleseth T, et al. A class of binomial bent functions over the finite fields of odd characteristic. IEEE Trans Inform Theory, 2012, 58: 6054–6063
16 Kocak N, Mesnager S, Ozbudak F. Bent and semi-bent functions via linear translators. In: Cryptography and Coding. Berlin: Springer, 2015. 205–224
17 Li N, Helleseth T, Tang X, et al. Several new classes of bent functions from Dillon exponents. IEEE Trans Inform Theory, 2013, 59: 1818–1831
18 Li N, Tang X, Helleseth T. New constructions of quadratic bent functions in polynomial form. IEEE Trans Inform Theory, 2014, 60: 5760–5767
19 Mesnager S. A new family of hyper-bent Boolean functions in polynomial form. In: Cryptography & Coding. Berlin: Springer, 2009. 402–417

20 Mesnager S. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans Inform Theory, 2011, 57: 5996–6009
21 Mesnager S, Flori J P. Hyperbent functions via Dillon-like exponents. IEEE Trans Inf Theory, 2013, 59: 836–840
22 Mesnager S. Further constructions of infinite families of bent functions from new permutations and their duals. Cryptogr Commun, 2016, 8: 229–246
23 Mesnager S. Several new infinite families of bent functions and their duals. IEEE Trans Inform Theory, 2014, 60: 4397–4407
24 Zheng D B, Zeng X Y, Hu L. A family of p-ary binomial bent functions. IEICE Trans Fundamentals, 2011, 94: 1868–1872
25 Carlet C. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In: Proceedings of the 16th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Las Vegas, 2006. 1–28
26 Xu G K, Cao X W, Xu S D. Several new classes of Boolean functions with few Walsh transform values. arXiv:1506.04886
27 Carlet C, Danielsen L E, Parker M G, et al. Self-dual bent functions. Int J Inf Coding Theory, 2010, 1: 384–399
28 Dobbertin H, Leander G, Canteaut A, et al. Construction of bent functions via Niho power functions. J Combin Theory Ser A, 2006, 113: 779–798
29 Leander G, Kholosha A. Bent functions with 2^r Niho exponents. IEEE Trans Inform Theory, 2006, 52: 5529–5532
30 Budaghyan L, Carlet C, Helleseth T, et al. Further results on Niho bent functions. IEEE Trans Inform Theory, 2012, 58: 6979–6985