Cluster Computing (2019) 22:S9281–S9291
https://doi.org/10.1007/s10586-018-2126-y

CrossMark

More constructions of semi-bent and plateaued functions in polynomial forms

Tao Xie[1]· Gaojun Luo[2]

Received: 2 January 2018 / Revised: 1 February 2018 / Accepted: 8 February 2018 / Published online: 1 March 2018

Abstract
Plateaued functions and their subclass semi-bent functions have useful applications in cryptography and communications. In this paper we give new constructions of quadratic semi-bent functions in polynomial forms on the finite field $\mathbb{F}_{2^n}$ for both odd and even n. We also present some characterizations of e-plateaued functions with few trace terms when n is even.

Keywords Boolean functions · Semi-bent functions · Plateaued functions

Mathematics Subject Classification 11T06 · 11T71

1 Introduction

In the 1960s and 1990s, two families of m-sequences having low cross correlation were introduced by Gold [1] and Boztas et al. [2] respectively. Each of them has period $2^n - 1$ and a plateaued cross-correlation spectra. That is, for two such m-sequences $u(t) = \mathrm{Tr}_1^n(\alpha^t)$ and $v(t) = \mathrm{Tr}_1^n(\beta^t)$, where α and β have order $2^n - 1$ in the finite field $\mathbb{F}_{2^n}$, we have

$$C_{u,v}(\tau) = \sum_{t=0}^{2^n-2}(-1)^{u(t+\tau)+v(t)} \in \left\{-1, -1 \pm 2^{\frac{n+1}{2}}\right\}.$$

These families of sequences have the trace representations

$$f(x) = \mathrm{Tr}_1^n\left(x^{1+2^i}\right)\ (\gcd(i,n) = 1) \quad \text{and} \quad f(x) = \sum_{i=1}^{\frac{n-1}{2}}\mathrm{Tr}_1^n\left(x^{1+2^i}\right)$$

respectively, where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Such families of maximum-length sequences, whose cross-correlation spectra attain exactly the values above, have a wide range of applications in cryptography and code-division multiple-access communication systems [3, 4]. Such sequences can be represented by Boolean functions which we call *semi-bent* functions, using the terminology of Khoo et al. [5].

In order to construct more sequences having the nice property as the above two sequences, Khoo et al. [6] investigated the problem of determining the function

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i\mathrm{Tr}_1^n\left(x^{1+2^i}\right), \quad c_i \in \mathbb{F}_2$$

defined on $\mathbb{F}_{2^n}$ with n odd is semi-bent, where this sum has more than one term. To such a function a cyclic code of length $2^n - 1$ was associated, spanned by

$$c(x), xc(x), \ldots, x^{n-1}c(x), \quad \text{where} \quad c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i\left(x^i + x^{n-i}\right).$$

Then it was proved that f is semi-bent if and only if $\gcd(c(x), x^n + 1) = x + 1$. This gives a very convenient tool for determining whether a function f having certain number of trace terms is semi-bent or not.

Following this work, Charpin et al. studied the following function [7]:

$$f(x) = \sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor} c_i\mathrm{Tr}_1^n\left(x^{1+2^i}\right), \quad c_i \in \mathbb{F}_2. \tag{1}$$

When n is odd, they provide some semi-bent functions with three or four trace terms. When n is even, they proved that

✉ Tao Xie
xietao1294@sina.com

Gaojun Luo
GJLuo1990@163.com

1 College of Mathematic and Statistic, Hubei Normal University, Huangshi 435002, China

2 School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

$f(x)$ is semi-bent if and only if $\gcd(c(x), x^n+1) = x^2+1$, where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i})$. Moreover, they found that the concatenation of two suitably chosen such semi-bent functions will yield a semi-bent function with higher algebraic degrees. After this work, a lot of research has been devoted to finding new families of quadratic semi-bent and bent functions in the form of Eq. (1) [8–16]. In 2013, Dong et al. present some new constructions of quadratic semi-bent functions. For odd $n = pq$ with $p(3 \nmid p), q$ odd, they proved that the function

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^q}\right),$$

is semi-bent. For even $n = 2m$ with odd m, a necessary and sufficient condition for the function defined on $\mathbb{F}_{2^n}$ by

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

to be semi-bent is given. For some special cases of $c_i(1 \le i \le \frac{m-1}{2})$, they proved that f is semi-bent.

Motivated by the paper [8], we present new constructions of quadratic semi-bent and e-plateaued functions in polynomial forms. We study the function defined by

$$f(x) = \sum_{i=1}^{s} c_i \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \sum_{j=1}^{t} d_j \mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right), \tag{2}$$

where $c_i, d_j \in \mathbb{F}_2$, $1 \le s \le \frac{q-1}{2}$, $1 \le t \le \frac{p-1}{2}$, $n = pq$, p, q odd, $\gcd(p,q) = 1$, and the function defined by

$$f(x) = \sum_{i=1}^{\frac{m-1}{2}} c_i \mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right), \tag{3}$$

where $n = em$, $e = 2^l$, m is odd, $c_i \in \mathbb{F}_2$ $(1 \le i \le \frac{m-1}{2})$, $\beta \in \mathbb{F}_{2^e}^*$. For odd n, we find five new classes of semi-bent functions of the form Eq. (2) by choosing suitable vectors $(c_1, \ldots, c_s) \in \mathbb{F}_2^s$ and $(d_1, \ldots, d_t) \in \mathbb{F}_2^t$. For even n, we give a necessary and sufficient condition under which $f(x)$ given by Eq. (3) is e-plateaued and provide some new e-plateaued and semi-bent functions with few trace terms.

To the best of our knowledge, we give a list of the quadratic semi-bent functions on $\mathbb{F}_{2^n}$ as follows:

When n is odd, the following functions are semi-bent.

(1) $f(x) = \mathrm{Tr}_1^n(x^{1+2^i})$, $\gcd(i,n) = 1$ [1].

(2) $f(x) = \sum_{i=1}^{\frac{n-1}{2}} \mathrm{Tr}_1^n(x^{1+2^i})$ [2].

(3) $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i \mathrm{Tr}_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$ for $1 \le i \le \frac{n-1}{2}$, $\gcd(\sum_{i=1}^{\frac{n-1}{2}} c_i\left(x^i + x^{n-i}\right), x^n+1) = x+1$ [6].

(4) $f(x) = \sum_{i=0}^{r} \mathrm{Tr}_1^n(x^{1+2^{a+id}})$, $\gcd(2a+rd, n) = \gcd((r+1)d, n) = 1$ [5].

(5) $f(x) = \mathrm{Tr}_1^n(x^{1+2^i}) + \mathrm{Tr}_1^n(x^{1+2^j})$, $\gcd(i+j, n) = \gcd(i-j, n) = 1$ [5].

(6) $f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^q}\right)$, $n = pq$, $p(3 \nmid p), q$ are odd positive integers such that $\gcd(p,q) = 1$ [8].

(7) $f(x) = \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n(x^{1+2^{qj}})$, $n = pq$, p, q odd, $\gcd(p,q) = 1$, and i, j are two positive integers such that $\gcd(i,q) = \gcd(j,p) = 1$ (Theorem 3 of this paper).

(8) $f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{1+2^{pi}}) + \mathrm{Tr}_1^n(x^{1+2^{qj}})$, $n = pq$, $p(3 \nmid p), q$ are odd positive integers such that $\gcd(p,q) = 1$, $\gcd(j,p) = 1$ (Theorem 4 of this paper).

(9) $f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{1+2^{pi}}) + \mathrm{Tr}_1^n(x^1 + 2^q) + \mathrm{Tr}_1^n(x^{1+2^{qj}})$, $n = pq, p$, q odd and $\gcd(p,q) = 1, j = 2^l$ and l is a positive integer such that $\gcd(l,n) = 1$ (Theorem 5 of this paper).

(10) $f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{1+2^{pi}}) + \mathrm{Tr}_1^n(x^{1+2^{qj}}) + \mathrm{Tr}_1^n(x^{1+2^{qk}})$, $n = pq$, p, q odd and $\gcd(p,q) = 1$, $j = 2^{u-1} - 2^{v-1}$, $k = 2^{u-1} + 2^{v-1}$, $u > v \ge 1$ (Theorem 6 of this paper).

(11) $f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{1+2^{pi}}) + \mathrm{Tr}_1^n(x^{1+2^{qj}}) + \mathrm{Tr}_1^n(x^{1+2^{qk}})$, $n = pq, p$, q odd and $\gcd(p,q) = 1, j = 2^u$, $k = 2^v$, $u > v \ge 1$, $\gcd(u-v, n) = 1$ (Theorem 7 of this paper).

When $n = 2m$ is even, the following functions are semi-bent:

(1) $f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i \mathrm{Tr}_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$, $\gcd(\sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}), x^n+1) = x^2+1$ [7].

(2) $f(x) = \mathrm{Tr}_1^n(\alpha x^{1+2^i})$, $\alpha \in \mathbb{F}_{2^n}^*$, i even, m odd [10].

(3) $f(x) = \mathrm{Tr}_1^n(\alpha x^{1+2^i})$, $\alpha \in \{x^3 \mid x \in \mathbb{F}_{2^n}^*\}$, i odd, m even [10].

(4) $f(x) = \mathrm{Tr}_1^n(\alpha x^{1+2^i})$, $\alpha \in \{x^3 \mid x \in \mathbb{F}_{2^n}^*\}$, i odd, m odd and $\gcd(i,m) = 1$ [10].

(5) $f(x) = \mathrm{Tr}_1^n(x^{1+2^i}) + \mathrm{Tr}_1^n(x^{1+2^j})$, m odd, $1 \le i < j \le m$, $\gcd(i+j, n) = \gcd(j-i, n) = 1$ or $\gcd(i+j, n) = \gcd(j-i, n) = 2$ [10].

(6) $f(x)=\sum_{i=1}^{\frac{m-1}{2}}\mathrm{Tr}_1^n(\beta x^{1+4^i})$, m odd, $\beta\in\mathbb{F}_4^*$ [8].

(7) $f(x)=\sum_{i=1}^{\frac{m-1}{2}}c_i\mathrm{Tr}_1^n(\beta x^{1+4^i})$, $c_i\in\mathbb{F}_2$, $\beta\in\mathbb{F}_4^*$, m odd, $\gcd(\sum_{i=1}^{\frac{m-1}{2}}c_i(x^i+x^{m-i}),x^m+1)=x+1$ [8].

(8) $f(x)=\sum_{i=1}^{k}\mathrm{Tr}_1^n(\beta x^{1+4^{di}})$, $\beta\in\mathbb{F}_4^*$, m odd, $d\geq 1$, $1\leq k\leq\frac{m-1}{2}$, $\gcd(k+1,m)=\gcd(k,m)=\gcd(d,m)=1$ [8].

(9) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+4^i}+\beta x^{1+4^j})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j\leq\lfloor\frac{n}{4}\rfloor$, $\gcd(i+j,m)=\gcd(j-i,m)=1$ [8].

(10) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+4^i}+\beta x^{1+4^j}+\beta x^{1+4^t})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j<t\leq\lfloor\frac{n}{4}\rfloor$, $i+j=t$, $\gcd(i,m)=\gcd(j,m)=\gcd(t,m)=1$ [8].

(11) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+4^i}+\beta x^{1+4^j}+\beta x^{1+4^t})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j<t\leq\lfloor\frac{n}{4}\rfloor$, $i+j=2t$, $j-i=3^hp$, $3\not| p$, $n=3^kq$, $3\not| q$, $\gcd(2t,m)=1$, $h\geq k$ [8].

(12) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+4^i}+\beta x^{1+4^j}+\beta x^{1+4^t})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j<t\leq\lfloor\frac{n}{4}\rfloor$, $j-i=2t$, $t\neq i$, $j+i=3^up$, $3\not| p$, $n=3^vq$, $3\not| q$, $\gcd(2t,m)=1$, $u\geq v$ [8].

(13) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+4^i}+\beta x^{1+4^j}+\beta x^{1+4^t}+\beta x^{1+4^s})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i,j,t,s\leq\lfloor\frac{n}{4}\rfloor$, $i<j$, $t<s$, $i+j=t+s=r$, $t\neq i$, $\gcd(r,m)=\gcd(s-i,m)=\gcd(s-j,m)=1$ [8].

(14) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{2i}})$, $1\leq i\leq m-1$, $\gcd(i,m)=1$ and m odd (Corollary 5 of this paper).

(15) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{2i}}+\beta x^{1+2^{2j}}+\beta x^{1+2^{2t}})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j<t\leq m-1$, $i+j=2t$, $\gcd(t,m)=1$ (Corollary 9 of this paper).

(16) $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{2i}}+\beta x^{1+2^{2j}}+\beta x^{1+2^{2t}})$, $\beta\in\mathbb{F}_4^*$, m odd, $1\leq i<j<t\leq m-1$, $j-i=2t$, $\gcd(t,m)=1$ (Corollary 10 of this paper).

2 Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, and we use $\mathcal{B}_n$ to denote the set of Boolean functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In this paper, we mainly investigate the Boolean function of the form

$$f(x)=\sum_{i=1}^{s}c_i\mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right)+\sum_{j=1}^{t}d_j\mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right),$$

where $c_i,d_j\in\mathbb{F}_2$, $1\leq s\leq\frac{q-1}{2}$, $1\leq t\leq\frac{p-1}{2}$, $n=pq$, p, q odd, $\gcd(p,q)=1$, and the function defined by

$$f(x)=\sum_{i=1}^{\frac{m-1}{2}}c_i\mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right),$$

where $n=em$, $e=2^l$, m is odd, $c_i\in\mathbb{F}_2$ $(1\leq i\leq\frac{m-1}{2})$, $\beta\in\mathbb{F}_{2^e}^*$. The Walsh transform of f at $\lambda\in\mathbb{F}_{2^n}$ is given by

$$W_f(\lambda)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(\lambda x)}.$$

Definition 1 ([17]) Let $f(x)\in\mathcal{B}_n$. For any $\lambda\in\mathbb{F}_{2^n}$, if $W_f(\lambda)\in\{0,\pm 2^{\frac{n+r}{2}}\}$, for some fixed r, $r=0,1,\ldots,n$, then $f(x)$ is called r-plateaued. 0-plateaued (when n is even) functions are called bent. 1-plateaued (when n is odd) and 2-plateaued (when n is even) functions are called semi-bent.

The r-plateaued functions exist only when $n-r$ is even, or equivalently, if n and r have the same parity [18]. It is well-known that all the quadratic functions are plateaued [19].

The quadratic Boolean functions on $\mathbb{F}_{2^n}$ are as follows:

$$f(x)=\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}c_i\mathrm{Tr}_1^n\left(x^{1+2^i}\right),\ c_i\in\mathbb{F}_2.$$

Any such Boolean function with n variables has rank $2t$ with $0\leq t\leq\lfloor\frac{n}{2}\rfloor$ [3], and the rank can be found as follows. Let

$$\Omega_f(x;y)=f(0)+f(x)+f(y)+f(x+y). \tag{4}$$

Then the rank of $f(x)$ is $2t$ if and only if the equation

$$\Omega_f(x;y)=0,\ \text{for any}\ y\in\mathbb{F}_{2^n}$$

in x just has 2^{n-2t} solutions. The rank of quadratic Boolean functions is connected with the distribution of its Walsh transform values. Furthermore, the following theorem holds.

Lemma 1 ([3]) Let $f(x)\in\mathcal{B}_n$ is a quadratic function, and the rank of $f(x)$ is $2t$, $0\leq t\leq\lfloor\frac{n}{2}\rfloor$, then the distribution of its Walsh transform values is given by

$$W_f(\lambda)=\begin{cases}2^{n-t}, & 2^{2t-1}+2^{t-1}\ \text{times},\\ 0, & 2^{n-2t}\ \text{times},\\ -2^{n-t}, & 2^{2t-1}-2^{t-1}\ \text{times}.\end{cases}$$

From the above theorem, it is easy to see that a quadratic Boolean function is semi-bent if and only if the rank of $f(x)$ is $n-2$ when n is even, or the rank of $f(x)$ is $n-1$ when n is odd.

Definition 2 ([20]) The polynomials $l(x) = \sum_{i=0}^{n} a_i x^i$ and $L(x) = \sum_{i=0}^{n} a_i x^{q^i}$ over $\mathbb{F}_{q^m}$ (q is a prime integer) are called q-associates of each other. More specifically, $l(x)$ is the conventional q-associate of $L(x)$ and $L(x)$ is the linearized q-associate of $l(x)$.

Lemma 2 ([20]) Let $L_1(x)$ and $L(x)$ be q-polynomials over $\mathbb{F}_q$ with conventional q-associates $l_1(x)$ and $l(x)$. Then $L_1(x)$ divides $L(x)$ holds if and only if $l_1(x)$ divides $l(x)$.

Lemma 3 Let $\phi(x) = x + \frac{1}{x}$ be a function defined over $\mathbb{F}_{2^n}^*$. Then the following two statements hold.

(i) If $\phi(x) = \phi(y)$ for two elements x and y in $\mathbb{F}_{2^n}^*$, then $x = y$ or $xy = 1$.
(ii) $\phi(x) = 0$ if and only if $x = 1$.

Proof

(i) If $\phi(x) = \phi(y)$ for $x, y \in \mathbb{F}_{2^n}^*$, i.e.,

$$x + \frac{1}{x} = y + \frac{1}{y},$$

then

$$x^2 y + y = xy^2 + x,$$

which implies

$$(x + y)(xy + 1) = 0.$$

Therefore $x = y$ or $xy = 1$.

(ii) $\phi(x) = 0$ if and only if $x + \frac{1}{x} = 0$, which is equivalent to $x^2 = 1$. Since $\gcd(2, 2^n - 1) = 1$, the equation $x^2 = 1$ has only one solution $x = 1$ in $\mathbb{F}_{2^n}^*$.

Lemma 4 Let p, q and i, j be positive integers satisfying that p, q are odd and $\gcd(p, q) = 1$ and $\gcd(i, q) = \gcd(j, p) = 1$. Then $\gcd(pq, pi \pm qj) = 1$.

Proof If $\gcd(pq, pi \pm qj) \neq 1$, then there exists a prime integer t such that $t \mid \gcd(pq, pi \pm qj)$, i.e.,

$$t \mid pq \quad \text{or} \quad t \mid pi \pm qj. \tag{5}$$

Since t is a prime, by Eq. (5) we have $t \mid p$ or $t \mid q$.

If $t \mid p$, then by Eq. (5), we have $t \mid qj$. Therefore, $t \mid q$ or $t \mid j$. If $t \mid q$, then $t \mid \gcd(p, q) = 1$, which is impossible. If $t \mid j$, then $t \mid \gcd(j, p) = 1$, which is also a contradiction with the assumption that t is a prime.

If $t \mid q$, we can similarly deduce that $t = 1$, a contradiction. This completes the proof.

3 New constructions of semi-bent functions on $\mathbb{F}_{2^n}$ with n odd

In this section, several classes of semi-bent functions are constructed on $\mathbb{F}_{2^n}$, where $n = pq$ and p, q are odd integers such that $\gcd(p, q) = 1$.

Theorem 3 Let $n = pq$ with p, q odd and $\gcd(p, q) = 1$. Then the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right) \tag{6}$$

is semi-bent, where i, j are two positive integers such that $\gcd(i, q) = \gcd(j, p) = 1$.

Proof By Lemma 1, in order to prove that $f(x)$ is a semi-bent function, we just need to prove that the rank of $f(x)$ is $n - 1$. By Eq. (4), we have

$$\Omega_f(x; y) = \mathrm{Tr}_1^n\left(y\left(x^{2^{pi}} + x^{2^{pq-pi}} + x^{2^{qj}} + x^{2^{pq-qj}}\right)\right).$$

Let $L(x) = x^{2^{pi}} + x^{2^{pq-pi}} + x^{2^{qj}} + x^{2^{pq-qj}}$, and it is easy to see that $x^2 + x \mid L(x)$. To prove that the rank of $f(x)$ is $n - 1$, we need to show that $L(x)$ has two solutions in $\mathbb{F}_{2^n}$ or equivalently to prove $\gcd(L(x), x^{2^{pq}} + x) = x^2 + x$. By Lemma 2, we need to show

$$\gcd(l(x), x^{pq} + 1) = x + 1,$$

where $l(x) = x^{pi} + x^{pq-pi} + x^{qj} + x^{pq-qj}$. To do this, we divide the remaining proof into three cases.

If $\beta \neq 1$ is root of $x^{pq} + 1$ and $\beta^p = 1$, then $l(\beta) = \beta^{qj} + \beta^{-qj} \neq 0$. Otherwise, if $l(\beta) = 0$, then $\beta^{2qj} = 1$. Since $\gcd(2, 2^n - 1) = 1$, we have $\beta^{qj} = 1$. Recall that $\beta^p = 1$, $\gcd(p, q) = 1$ and $\gcd(p, j) = 1$, we have $\beta = 1$, which is a contradiction with the assumption $\beta \neq 1$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^q = 1$, we can similarly deduce that $l(\beta) = \beta^{pi} + \beta^{-pi} \neq 0$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^p \neq 1$, $\beta^q \neq 1$, then $l(\beta) = \beta^{pi} + \beta^{-pi} + \beta^{qj} + \beta^{-qj}$. If $l(\beta) = 0$, i.e., $\phi(\beta^{pi}) = \phi(\beta^{qj})$, where $\phi(x)$ is the function defined in Lemma 2. By Lemma 2, we have

$$\beta^{pi} = \beta^{qj} \quad \text{or} \quad \beta^{pi+qj} = 1. \tag{7}$$

Since $\gcd(p, q) = 1$ and $\gcd(i, q) = \gcd(j, p) = 1$, by Lemma 4 we have $\gcd(pq, pi \pm qj) = 1$. Recall that $\beta^{pq} = 1$, then by Eq. (7), we have $\beta = \beta^{\gcd(pq, pi+qj)} = 1$ or $\beta = \beta^{\gcd(pq, pi-qj)} = 1$, both of which contradict with the assumption $\beta \neq 1$.

From the analysis of above, we can see that $\gcd(l(x), x^{pq} + 1) = x + 1$. Thus the rank of $f(x)$ is $n - 1$, and this completes the proof.

Corollary 1 Let $n = pq$ with p, q distinct odd prime integers. Then the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right) \tag{8}$$

is semi-bent for any integers i, j.

Theorem 4 Let $n = pq$ with p, q odd, $\gcd(p, q) = 1$ and $3 \nmid p$. Then the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right) \tag{9}$$

is semi-bent, where j is a positive integer such that $\gcd(j, p) = 1$.

Proof From Lemma 1, in order to prove that $f(x)$ is a semi-bent function, we just need to prove that the rank of $f(x)$ is $n - 1$. By Eq. (9), we have

$$\begin{aligned} f(x+y) &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x+y\right)^{1+2^{pi}} + \mathrm{Tr}_1^n(x+y)^{1+2^{qj}}\Big) \\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}} + y^{1+2^{pi}}\right) + \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}}y + y^{2^{pi}}x\right) \\ &\quad + \mathrm{Tr}_1^n\left(x^{1+2^{qj}} + y^{1+2^{qj}} + x^{2^{qj}}y + y^{2^{qj}}x\right). \end{aligned}$$

Hence,

$$\begin{aligned} \Omega_f(x; y) &= f(0) + f(x) + f(y) + f(x+y) \\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}}y + y^{2^{pi}}x\right) + \mathrm{Tr}_1^n\left(x^{2^{qj}}y + y^{2^{qj}}x\right) \\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}}y + yx^{2^{pq-pi}}\right) + \mathrm{Tr}_1^n\left(x^{2^{qj}}y + yx^{2^{pq-qj}}\right) \\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{\frac{q-1}{2}}\left(x^{2^{pi}} + x^{2^{pq-pi}}\right)\right)\right) + \mathrm{Tr}\mathrm{Tr}_1^n\left(y\left(x^{2^{qj}} + x^{2^{pq-qj}}\right)\right) \\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{q-1} x^{2^{pi}} + x^{2^{qj}} + x^{2^{pq-qj}}\right)\right). \end{aligned}$$

Let $L(x) = \sum_{i=1}^{q-1} x^{2^{pi}} + x^{2^{qj}} + x^{2^{pq-qj}}$, and it is easy to see that $x^2 + x \mid L(x)$. To prove that the rank of $f(x)$ is $n - 1$, we need to show that $\gcd(L(x), x^{2^{pq}} + x) = x^2 + x$, which is equivalent to show that

$$\gcd(l(x), x^{pq} + 1) = x + 1$$

from Lemma 2, where $l(x) = \sum_{i=1}^{q-1} x^{pi} + x^{qj} + x^{pq-qj}$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^p = 1$, then $l(\beta) = \beta^{jq} + \beta^{-jq} \neq 0$. Otherwise, we have $\beta^{2jq} = 1$. Since $\gcd(2, 2^n - 1) = 1$, $\beta^{jq} = 1$. From the conditions $\beta^p = 1$ and $\gcd(j, p) = 1$, we have $\beta = 1$, which is a contradiction with the assumption.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^q = 1$, then $l(\beta) = \frac{\beta^{pq}+\beta^p}{\beta^p+1} + \beta^{q(p-j)} + \beta^{qj} = 1 \neq 0$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^p \neq 1$, $\beta^q \neq 1$, thus

$$l(\beta) = \frac{\beta^{pq} + \beta^p}{\beta^p + 1} + \beta^{q(p-j)} + \beta^{qj} = 1 + \beta^{q(p-j)} + \beta^{qj}.$$

If $l(\beta) = 0$, then $\beta^{3jq} = 1$. Since $\beta^{pq} = 1$, $3 \nmid p$ and $\gcd(j, p) = 1$, $\beta^{\gcd(pq,3jq)} = \beta^{\gcd(p,3j)q} = \beta^q = 1$, which contradicts with the assumption $\beta^q \neq 1$. Hence we also have $l(\beta) \neq 0$ in this case.

From the analysis of above, we can see that $\gcd(l(x), x^{pq} + 1) = x + 1$. Thus the rank of $f(x)$ is $n - 1$, and this completes the proof.

For $j = 1$ in Theorem 4, we have the following corollary.

Corollary 2 ([8]) Let $n = pq$ with p, q odd, $\gcd(p, q) = 1$ and $3 \nmid p$. Then the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^q}\right) \tag{10}$$

is semi-bent.

Theorem 5 Let $n = pq$ with p, q odd and $\gcd(p, q) = 1$. Then the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n\left(x^{1+2^q}\right) + \mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right) \tag{11}$$

is semi-bent, where $j = 2^l$ and l is a positive integer such that $\gcd(l, n) = 1$.

Proof From Lemma 1, in order to prove that $f(x)$ is a semi-bent function, we just need to prove that the rank of $f(x)$ is $n - 1$. By Eq. (11), we have

$$\begin{aligned} f(x+y) &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\Big((x+y)^{1+2^{pi}} + \mathrm{Tr}_1^n((x+y)^{1+2^q}) + \mathrm{Tr}_1^n((x+y)^{1+2^{qj}}\Big) \\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{1+2^{pi}} + y^{1+2^{pi}}) + \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n(x^{2^{pi}}y + y^{2^{pi}}x) \\ &\quad + \mathrm{Tr}_1^n(x^{1+2^q} + y^{1+2^q} + x^{2^q}y + y^{2^q}x) \\ &\quad + \mathrm{Tr}_1^n(x^{1+2^{qj}} + y^{1+2^{qj}} + x^{2^{qj}}y + y^{2^{qj}}x). \end{aligned}$$

Hence,

$$\begin{aligned}\Omega_f(x;y) &= f(0)+f(x)+f(y)+f(x+y)\\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}}y+y^{2^{pi}}x\right)+\mathrm{Tr}_1^n\left(x^{2^q}y+y^{2^q}x\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{2^{qj}}y+y^{2^{qj}}x\right)\\ &= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}}y+yx^{2^{pq-pi}}\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{2^q}y+yx^{2^{pq-q}}\right)+\mathrm{Tr}_1^n\left(x^{2^{qj}}y+yx^{2^{pq-qj}}\right)\\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{\frac{q-1}{2}}\left(x^{2^{pi}}+x^{2^{pq-pi}}\right)\right)\right)+\mathrm{Tr}_1^n\left(y\left(x^{2^q}+x^{2^{pq-q}}\right)\right)\\ &\quad+\mathrm{Tr}_1^n\left(y\left(x^{2^{qj}}+x^{2^{pq-qj}}\right)\right)\\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{q-1}x^{2^{pi}}+x^{2^q}+x^{2^{pq-q}}+x^{2^{qj}}+x^{2^{pq-qj}}\right)\right).\end{aligned}$$

Let $L(x)=\sum_{i=1}^{q-1}x^{2^{pi}}+x^{2^q}+x^{2^{pq-q}}+x^{2^{qj}}+x^{2^{pq-qj}}$, and it is easy to see that $x^2+x\,|\,L(x)$. To prove that the rank of $f(x)$ is $n-1$, we need to show that $\gcd(L(x),x^{2^{pq}}+x)=x^2+x$, which equals

$$\gcd(l(x),x^{pq}+1)=x+1$$

from Lemma 2, where $l(x)=\sum_{i=1}^{q-1}x^{pi}+x^q+x^{pq-q}+x^{qj}+x^{pq-qj}$.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^p=1$, then $l(\beta)=\beta^q+\beta^{-q}+\beta^{jq}+\beta^{-jq}$. Let $w=\beta^q+\beta^{-q}$, then $l(\beta)=w+w^j$, where $j=2^l$ and $w\neq0,1$. We claim that $l(\beta)\neq0$. Otherwise, we have $w=w^{2^l}$. Since $\gcd(2^l-1,2^n-1)=1$, $w=0$ or 1, which is a contradiction.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^q=1$, then $l(\beta)=1\neq0$.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^p\neq1$, $\beta^q\neq1$, thus

$$l(\beta)=1+\beta^q+\beta^{-q}+\beta^{jq}+\beta^{-jq}.$$

If $l(\beta)=0$, then $w+w^{2^l}=1$. Since n is odd, $\mathrm{Tr}_1^n(1)=1$. But $\mathrm{Tr}_1^n(w+w^{2^l})=0$, leading to a contradiction. Hence we also have $l(\beta)\neq0$ in this case.

From the analysis of above, we can see that $\gcd(l(x),x^{pq}+1)=x+1$. Thus the rank of $f(x)$ is $n-1$, and this completes the proof.

Theorem 6 Let $n=pq$, with p, q odd and $\gcd(p,q)=1$. Let $j=2^{u-1}-2^{v-1}$ and $k=2^{u-1}+2^{v-1}$, where u, v are positive integers such that $u>v$. Then

$$f(x)=\sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right)+\mathrm{Tr}_1^n\left(x^{1+2^{qj}}\right)+\mathrm{Tr}_1^n\left(x^{1+2^{qk}}\right) \tag{12}$$

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

Proof From Lemma 1, in order to prove that $f(x)$ is a semi-bent function, we just need to prove that the rank of $f(x)$ is $n-1$. By Eq. (12), we have

$$\begin{aligned}f(x+y) &= \sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left((x+y)^{1+2^{pi}}\right)+\mathrm{Tr}_1^n\left((x+y)^{1+2^{qj}}\right)\\ &\quad+\mathrm{Tr}_1^n\left((x+y)^{1+2^{qk}}\right)\\ &= \sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left(x^{1+2^{pi}}+y^{1+2^{pi}}\right)+\sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left(x^{2^{pi}}y+y^{2^{pi}}x\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{1+2^{qj}}+y^{1+2^{qj}}+x^{2^{qj}}y+y^{2^{qj}}x\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{1+2^{qk}}+y^{1+2^{qk}}+x^{2^{qk}}y+y^{2^{qk}}x\right).\end{aligned}$$

Hence,

$$\begin{aligned}\Omega_f(x;y) &= f(0)+f(x)+f(y)+f(x+y)\\ &= \sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left(x^{2^{pi}}y+y^{2^{pi}}x\right)+\mathrm{Tr}_1^n\left(x^{2^{qj}}y+y^{2^{qj}}x\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{2^{qk}}y+y^{2^{qk}}x\right)\\ &= \sum_{i=1}^{\frac{q-1}{2}}\mathrm{Tr}_1^n\left(x^{2^{pi}}y+yx^{2^{pq-pi}}\right)+\mathrm{Tr}_1^n\left(x^{2^{qj}}y+yx^{2^{pq-qj}}\right)\\ &\quad+\mathrm{Tr}_1^n\left(x^{2^{qk}}y+yx^{2^{pq-qk}}\right)\\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{\frac{q-1}{2}}\left(x^{2^{pi}}+x^{2^{pq-pi}}\right)\right)\right)+\mathrm{Tr}_1^n\left(y\left(x^{2^{qj}}+x^{2^{pq-qj}}\right)\right)\\ &\quad+\mathrm{Tr}_1^n\left(y\left(x^{2^{qk}}+x^{2^{pq-qk}}\right)\right)\\ &= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{q-1}x^{2^{pi}}+x^{2^{qj}}+x^{2^{pq-qj}}+x^{2^{qk}}+x^{2^{pq-qk}}\right)\right).\end{aligned}$$

Let $L(x)=\sum_{i=1}^{q-1}x^{2^{pi}}+x^{2^{qj}}+x^{2^{pq-qj}}+x^{2^{qk}}+x^{2^{pq-qk}}$, and it is easy to see that $x^2+x\,|\,L(x)$. To prove that the rank of $f(x)$ is $n-1$, we need to show that $\gcd(L(x),x^{2^{pq}}+x)=x^2+x$, which equals

$$\gcd(l(x),x^{pq}+1)=x+1$$

from Lemma 2, where $l(x)=\sum_{i=1}^{q-1}x^{pi}+x^{qj}+x^{pq-qj}+x^{qk}+x^{pq-qk}$.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^p=1$, then $l(\beta)=\beta^{qj}+\beta^{-qj}+\beta^{qk}+\beta^{-qk}$. If $l(\beta)=0$, then $\phi(\beta^{qj})=\phi(\beta^{qk})$, where ϕ is the function defined in Lemma 2. By Lemma 2, we have $\beta^{qj}=\beta^{qk}$ or $\beta^{q(j+k)}=1$. Since $\gcd(j\pm k,p)=1$, $\beta^p=1$ and $\gcd(p,q)=1$, we have $\beta=1$, which is a contradiction with the assumption $\beta\neq1$.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^q=1$, then $l(\beta)=1\neq0$.

If $\beta\neq1$ is a root of $x^{pq}+1$ and $\beta^p\neq1$, $\beta^q\neq1$, thus

$l(\beta) = 1 + \beta^{qj} + \beta^{-qj} + \beta^{qk} + \beta^{-qk}.$

If $l(\beta) = 0$, then

$$\beta^{qj} + \beta^{-qj} + \beta^{qk} + \beta^{-qk} = 1 \quad (13)$$

By Eq. (13), we have

$$\beta^{q(j+k)} + \beta^{q(k-j)} + \beta^{2qk} + \beta^{qk} = 1. \quad (14)$$

Since $k + j = 2^u$ and $k - j = 2^v$, Eq. (14) can be rewritten as

$$(\beta^q)^{2^u} + (\beta^q)^{2^v} + (\beta^{qk})^2 + \beta^{qk} = 1. \quad (15)$$

It is clear that $\mathrm{Tr}_1^n((\beta^q)^{2^u} + (\beta^q)^{2^v} + (\beta^{qk})^2 + \beta^{qk}) = 0$. But $\mathrm{Tr}_1^n(1) = 1$, leading to a contradiction. Hence we also have $l(\beta) \neq 0$ in this case.

From the analysis of above, we can see that $\gcd(l(x), x^{pq} + 1) = x + 1$. Thus the rank of $f(x)$ is $n - 1$, and this completes the proof.

Theorem 7 Let $n = pq$, with p, q odd and $\gcd(p, q) = 1$. Let $j = 2^u$ and $k = 2^v$, where u, v are positive integers such that $u > v$ and $\gcd(u - v, n) = 1$. Then

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \mathrm{Tr}_1^n(x^{1+2^{qj}}) + \mathrm{Tr}_1^n\left(x^{1+2^{qk}}\right) \quad (16)$$

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

Proof From Lemma 1, in order to prove that $f(x)$ is a semi-bent function, we just need to prove that the rank of $f(x)$ is $n - 1$. Through similar calculations as Theorem 5, we have

$$\begin{aligned}
\Omega_f(x; y) &= f(0) + f(x) + f(y) + f(x + y)\\
&= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}} y + y^{2^{pi}} x\right) + \mathrm{Tr}_1^n\left(x^{2^{qj}} y + y^{2^{qj}} x\right)\\
&\qquad + \mathrm{Tr}_1^n\left(x^{2^{qk}} y + y^{2^{qk}} x\right)\\
&= \sum_{i=1}^{\frac{q-1}{2}} \mathrm{Tr}_1^n\left(x^{2^{pi}} y + yx^{2^{pq-pi}}\right) + \mathrm{Tr}_1^n\left(x^{2^{qj}} y + yx^{2^{pq-qj}}\right)\\
&\qquad + \mathrm{Tr}_1^n\left(x^{2^{qk}} y + yx^{2^{pq-qk}}\right)\\
&= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{\frac{q-1}{2}}\left(x^{2^{pi}} + x^{2^{pq-pi}}\right)\right)\right) + \mathrm{Tr}_1^n\left(y(x^{2^{qj}} + x^{2^{pq-qj}})\right)\\
&\qquad + \mathrm{Tr}_1^n\left(y\left(x^{2^{qk}} + x^{2^{pq-qk}}\right)\right)\\
&= \mathrm{Tr}_1^n\left(y\left(\sum_{i=1}^{q-1} x^{2^{pi}} + x^{2^{qj}} + x^{2^{pq-qj}} + x^{2^{qk}} + x^{2^{pq-qk}}\right)\right).
\end{aligned}$$

Let $L(x) = \sum_{i=1}^{q-1} x^{2^{pi}} + x^{2^{qj}} + x^{2^{pq-qj}} + x^{2^{qk}} + x^{2^{pq-qk}}$, and it is easy to see that $x^2 + x \mid L(x)$. To prove that the rank of $f(x)$ is $n - 1$, we need to show that $\gcd(L(x), x^{2^{pq}} + x) = x^2 + x$, which equals

$$\gcd(l(x), x^{pq} + 1) = x + 1$$

from Lemma 2, where $l(x) = \sum_{i=1}^{q-1} x^{pi} + x^{qj} + x^{pq-qj} + x^{qk} + x^{pq-qk}$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^p = 1$, then $l(\beta) = \beta^{qj} + \beta^{-qj} + \beta^{qk} + \beta^{-qk}$. Let $w = \beta^q + \beta^{-q}$, then $l(\beta) = w^{2^u} + w^{2^v}$. If $l(\beta) = 0$, then $w^{2^u} = w^{2^v}$. Note that $w \neq 0$, then we have $w^{2^u - 2^v} = w^{2^v(2^{u-v}-1)} = 1$. Since $\gcd(2^v(2^{u-v} - 1), 2^n - 1) = \gcd(2^{u-v} - 1, 2^n - 1) = 2^{\gcd(u-v,n)} - 1 = 1$, we have $w = 1$. This is impossible, because the equality $w = 1$ will lead to $\beta = 1$, which is a contradiction with the assumption $\beta \neq 1$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^q = 1$, then $l(\beta) = 1 \neq 0$.

If $\beta \neq 1$ is a root of $x^{pq} + 1$ and $\beta^p \neq 1$, $\beta^q \neq 1$, thus

$$l(\beta) = 1 + \beta^{qj} + \beta^{-qj} + \beta^{qk} + \beta^{-qk} = w^{2^u} + w^{2^v}.$$

If $l(\beta) = 0$, then $w^{2^u} + w^{2^v} = 1$. Note that $\mathrm{Tr}_1^n(w^{2^u} + w^{2^v}) = 0$. But $\mathrm{Tr}_1^n(1) = 1$, leading to a contradiction. Hence we also have $l(\beta) \neq 0$ in this case.

From the analysis of above, we can see that $\gcd(l(x), x^{pq} + 1) = x + 1$. Thus the rank of $f(x)$ is $n - 1$, and this completes the proof.

4 New constructions of *e*-plateaued and semi-bent functions on $\mathbb{F}_{2^n}$ with *n* even

In this section, we give some new constructions of quadratic *e*-plateaued and semi-bent functions in polynomial forms with even n. We suppose $n = em$, where e and m are even and odd positive integers respectively in this section.

Theorem 8 For any $\beta \in \mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \sum_{i=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right) \quad (17)$$

is e-plateaued.

Proof By Lemma 1, in order to prove that $f(x)$ is an e-plateaued function, we just need to prove that the rank of $f(x)$ is $n - e$. By Eq. (17), we have

$$\begin{aligned}\Omega_f(x;y) &= f(0)+f(x)+f(y)+f(x+y)\\ &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n\left(\beta x y^{2^{ei}} + \beta x^{2^{ei}} y\right)\\ &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n\left(\beta x^{2^{em-ei}} y + \beta x^{2^{ei}} y\right)\\ &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n\left(\beta x^{2^{em-ei}} y + \beta x^{2^{ei}} y\right)\\ &= \sum_{i=1}^{m-1} \mathrm{Tr}_1^n\left(\beta y x^{2^{ei}}\right)\\ &= \mathrm{Tr}_1^n\left(\beta y\left(\mathrm{Tr}_e^n(x)+x\right)\right).\end{aligned}$$

It follows that

$$\Omega_f(x;y) = 0, \quad \text{for any } \; y \in \mathbb{F}_{2^n} \tag{18}$$

holds if and only if

$$\mathrm{Tr}_e^n(x) + x = 0.$$

So $x = \mathrm{Tr}_e^n(x) \in \mathbb{F}_{2^e}$, and for any $x \in \mathbb{F}_{2^e}$, $\mathrm{Tr}_e^n(x) = x\mathrm{Tr}_e^n(1) = x$. This implies that $\mathrm{Tr}_e^n(x) + x = 0$ holds if and only if $x \in \mathbb{F}_{2^e}$. Hence Eq. (18) has only 2^e solutions, so the rank of $f(x)$ is $n-e$. By Lemma 1 and Definition 1, $f(x)$ is an e-plateaued function.

For $e = 2$, we have the following corollary.

Corollary 3 ([8]) For any $\beta \in \mathbb{F}_{2^2}^*$, the function defined on $\mathbb{F}_{2^n}$ by

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

is a semi-bent function.

Now we consider the general case. We study the function defined by

$$f(x) = \sum_{i=1}^{\frac{m-1}{2}} c_i \mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right), \tag{19}$$

where $c_i \in \mathbb{F}_2$, $(1 \le i \le \frac{m-1}{2})$, $\beta \in \mathbb{F}_{2^e}^*$.

Theorem 9 If $e = 2^l$ for some positive integer l, then for any $\beta \in \mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by Eq. (19) is e-plateaued if and only if

$$\gcd\left(\sum_{i=1}^{\frac{m-1}{2}} c_i(x^i + x^{m-i}), x^m + 1\right) = x+1.$$

Proof By Lemma 1, we only need to prove that the rank of $f(x)$ is $n-e$. Similar to the proof of Theorem 7, the rank of $f(x)$ is $n-e$ if and only if the equation

$$\sum_{i=1}^{\frac{m-1}{2}} c_i\left(x^{2^{ei}} + x^{2^{em-ei}}\right) \tag{20}$$

has only 2^e solutions in $\mathbb{F}_{2^n}$. For any $x \in \mathbb{F}_{2^e}$, it is obvious that $x^{2^{ei}} + x^{2^{em-ei}} = 0\,(1 \le i \le \frac{m-1}{2})$ holds. So

$$x^{2^e} + x \,\Big|\, \sum_{i=1}^{\frac{m-1}{2}} c_i\left(x^{2^{ei}} + x^{2^{em-ei}}\right).$$

In order to show that Eq. (20) has only 2^e solutions in $\mathbb{F}_{2^n}$, we just need to prove that

$$\gcd\left(\sum_{i=1}^{\frac{m-1}{2}} c_i\left(x^{2^{ei}} + x^{2^{em-ei}}\right), x^{2^n} + x\right) = x^{2^e} + x \tag{21}$$

holds. By Lemma 3, Eq. (21) holds if and only if

$$\gcd\left(\sum_{i=1}^{\frac{m-1}{2}} c_i\left(x^{ei} + x^{em-ei}\right), x^{em} + 1\right) = x^e + 1 = (x+1)^e. \tag{22}$$

Eq. (22) holds if and only if

$$\gcd\left(\sum_{i=1}^{\frac{m-1}{2}} c_i\left(x^{i} + x^{m-i}\right), x^{m} + 1\right) = x+1.$$

Theorem 10 If $e = 2^l$ for some positive integer l, then for any $\beta \in \mathbb{F}_{2^e}^*$, $r \ge 1$, $1 \le k \le \frac{m-1}{2}$, the function defined on $\mathbb{F}_{2^n}$ by

$$f(x) = \sum_{i=1}^{k} \mathrm{Tr}_1^n\left(\beta x^{1+2^{eri}}\right)$$

is e-plateaued if and only if

$$\gcd(k+1, m) = \gcd(k, m) = \gcd(r, m) = 1.$$

Proof Similar to the proof of Theorem 8, $f(x)$ is e-plateaued if and only if

$$\gcd(L(x), x^m + 1) = x + 1, \quad \text{where} \;\; L(x) = \sum_{i=1}^{k}\left(x^{ri} + x^{m-ri}\right).$$

We have

$$
\begin{aligned}
L(x) &= \sum_{i=1}^{k}\left(x^{ri}+x^{-ri}\right)\\
&= \sum_{i=0}^{2k}\frac{x^{ri}}{x^{rk}}+1\\
&= \frac{x^{(2k+1)r}+1}{x^{rk}(x^r+1)}+1\\
&= \frac{x^{(2k+1)r}+x^{rk+r}+x^{rk}+1}{x^{rk}(x^r+1)}\\
&= \frac{(x^{rk+r}+1)(x^{rk}+1)}{x^{rk}(x^r+1)}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
\gcd(L(x),x^m+1) &= \gcd\left(\frac{(x^{rk+r}+1)(x^{rk}+1)}{x^{rk}(x^r+1)},x^m+1\right)\\
&= x+1
\end{aligned}
$$

holds if and only if

$$\gcd(r(k+1),m)=\gcd(rk,m)=\gcd(r,m)=1,$$

which equals

$$\gcd(k+1,m)=\gcd(k,m)=\gcd(r,m)=1.$$

Corollary 4 ([8]) For any $\beta\in\mathbb{F}_{2^2}^*$, $r\geq 1$, $1\leq k\leq\frac{m-1}{2}$, the function defined on $\mathbb{F}_{2^n}$ by

$$f(x)=\sum_{i=1}^{k}\mathrm{Tr}_1^n\left(\beta x^{1+2^{2ri}}\right)$$

is semi-bent if and only if

$$\gcd(k+1,m)=\gcd(k,m)=\gcd(r,m)=1.$$

Theorem 11 If $e=2^l$ for some positive integer l, then for any $\beta\in\mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{ei}})\,(1\leq i\leq m-1)$ is e-plateaued if and only if $\gcd(i,m)=1$ and m is odd.

Proof Let $l(x)=x^i+x^{m-i}$. By Theorem 8, the function is e-plateaued if and only if $\gcd(l(x),x^m+1)=x+1$. As $x^i+x^{m-i}=x^i(x^{m-2i}+1)$ and $\gcd(x^i,x^m+1)=1$. The equality $\gcd(l(x),x^m+1)=x+1$ holds if and only if $\gcd(i,m)=1$ and m is odd.

Corollary 5 For any $\beta\in\mathbb{F}_{2^2}^*$, the function defined by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{2i}})$ $(1\leq i\leq m-1)$, is semi-bent if and only if $\gcd(i,m)=1$ and m odd.

When $k=1$ and $r=1$ in Theorem 10, we have the following corollary.

Corollary 6 If $e=2^l$ for some positive integer l, then for any $\beta\in\mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{ei}}+\beta x^{1+2^{ej}})\,(1\leq i<j\leq\lfloor\frac{n}{4}\rfloor)$ is e-plateaued if and only if $\gcd(m,j+i)=1$, $\gcd(m,j-i)=1$ and m is odd.

Corollary 7 If $e=2^l$ for some positive integer l, then for any $\beta\in\mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{ei}}+\beta x^{1+2^{ej}})$ is e-plateaued for any i,j with $1\leq i<j\leq\lfloor\frac{n}{4}\rfloor$ if and only if m is an odd prime integer.

Corollary 8 ([8]) For any $\beta\in\mathbb{F}_{2^2}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{2i}}+\beta x^{1+2^{2j}})\,(1\leq i<j\leq\lfloor\frac{n}{4}\rfloor)$ is semi-bent if and only if $\gcd(m,j+i)=1$, $\gcd(m,j-i)=1$ and m is odd.

Theorem 12 If $e=2^l$ for some positive integer l, then for any $\beta\in\mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n(\beta x^{1+2^{ei}}+\beta x^{1+2^{ej}}+\beta x^{1+2^{et}})\,(1\leq i<j<t\leq\lfloor\frac{n}{4}\rfloor, i+j=t)$ is e-plateaued if and only if $\gcd(m,i)=1$, $\gcd(m,j)=1$ and $\gcd(m,t)=1$.

Proof Let $l(x)=x^i+x^{m-i}+x^j+x^{m-j}+x^t+x^{m-t}$. By Theorem 8, the function is e-plateaued if and only if $\gcd(l(x),x^m+1)=x+1$. Note that

$$
\begin{aligned}
l(x) &= (1+x^i)(1+x^j)+1+x^m+x^m(1+x^{-i})(1+x^{-j})\\
&= (1+x^i)(1+x^j)(1+x^{m-i-j})+1+x^m.
\end{aligned}
$$

Then the equality $\gcd(l(x),x^m+1)=x+1$ holds if and only if $\gcd(m,i)=1$, $\gcd(m,j)=1$ and $\gcd(m,t)=1$.

Theorem 13 If $e=2^l$ for some positive integer l, then for any $\beta\in\mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x)=\mathrm{Tr}_1^n$ $betax^{1+2^{ei}}+\beta x^{1+2^{ej}}+\beta x^{1+2^{et}})\,(1\leq i<j\leq m-1,\quad i+j=2t)$ is e-plateaued if and only if $\gcd(t,m)=1$.

Proof Let $L(x)=x^i+x^{m-i}+x^j+x^{m-j}+x^t+x^{m-t}$. By Theorem 8, the function is e-plateaued if and only if $\gcd(L(x),x^m+1)=x+1$. Note that

$$
\begin{aligned}
L(x) &= x^i+x^j+x^{\frac{i+j}{2}}+x^{m-i}+x^{m-j}+x^{m-\frac{i+j}{2}}\\
&= x^i+x^j+x^{\frac{i+j}{2}}+x^{m-(i+j)}\left(x^i+x^j+x^{\frac{i+j}{2}}\right)\\
&= x^i\left(1+x^{j-i}+x^{\frac{j-i}{2}}\right)\left(1+x^{m-(i+j)}\right),
\end{aligned}
\tag{23}
$$

and $\gcd(x^i,x^m+1)=1$, we have $\gcd(L(x),x^m+1)=\gcd((1+x^{j-i}+x^{\frac{j-i}{2}})(1+x^{m-(i+j)}),x^m+1)$. Since m is odd, $\mathrm{Tr}_1^m(1)=1$. Consequently, $\mathrm{Tr}_1^m(1+x^{j-i}+x^{\frac{j-i}{2}})=1$. That is, for any $a\in\mathbb{F}_{2^m}$, $1+a^{j-i}+a^{\frac{j-i}{2}}\neq 0$. Hence, $\gcd(x+x^{2^{j-i}}+x^{2^{\frac{j-i}{2}}},x^{2^m}+x)=1$. By Lemma 2, we have $\gcd(1+x^{j-i}+x^{\frac{j-i}{2}},x^m+1)=1$. Therefore, $\gcd(L(x),x^m+1)=\gcd\ (x^{m-(i+j)}+1,x^m+1)$. By Theorem 8, $f(x)$ is e-plateaued if and only if $\gcd(x^{m-(i+j)}+1,x^m+1)=x+1$, which is equivalent to the condition $\gcd(i+j,m)=\gcd\ (2t,m)=\gcd(t,m)=1$.

Corollary 9 If $n = 2m$ with $m(>1)$ odd, then for any $\beta \in \mathbb{F}_{2^2}^*$,

$$f(x) = \mathrm{Tr}_1^n\left(\beta x^{1+2^{2i}} + \beta x^{1+2^{2j}} + \beta x^{1+2^{2t}}\right)$$

$(i + j = 2t, 1 \le i < j \le m - 1)$ is semi-bent if and only if $\gcd(t, m) = 1$.

Theorem 14 If $e = 2^l$ for some positive integer l, then for any $\beta \in \mathbb{F}_{2^e}^*$, the function defined on $\mathbb{F}_{2^n}$ by $f(x) = \mathrm{Tr}_1^n(\beta x^1 + 2^{ei} + \beta x^{1+2^{ej}} + \beta x^{1+2^{et}})$ $(1 \le i < j \le m - 1, j - i = 2t)$ is e-plateaued if and only if $\gcd(t, m) = 1$.

Proof Let $L(x) = x^i + x^{m-i} + x^j + x^{m-j} + x^t + x^{m-t}$. By Theorem 8, the function is e-plateaued if and only if $\gcd(L(x), x^m + 1) = x + 1$. Consider

$$\begin{aligned} x^tL(x) &= x^{t+i} + x^{t+j} + x^{2t} + x^{m-i+t} + x^{m-j+t} + x^m \\ &= x^{t+j} + x^{m-i+t} + x^{2t} + x^{t+i} + x^{m-(j-t)} + x^m \\ &= x^{t+j} + x^{m-i+t} + x^{2t} + x^{\frac{i+j}{2}} + x^{m-\frac{i+j}{2}} + x^m \\ &= \left(x^{2t} + 1)(x^{\frac{i+j}{2}} + x^{m-\frac{i+j}{2}} + 1\right) + x^m + 1. \end{aligned} \tag{24}$$

Since $\gcd(x^t, x^m + 1) = 1$, we have

$$\begin{aligned} &\gcd(L(x), x^m + 1) = \gcd(x^tL(x), x^m + 1) \\ &= \gcd\left((x^{2t} + 1)\left(x^{\frac{i+j}{2}} + x^{m-\frac{i+j}{2}} + 1\right), x^m + 1\right). \end{aligned}$$

Suppose that a is a root of $x^tL(x)$, $a \notin \mathbb{F}_2$ and $a^m = 1$, then $a^{\frac{i+j}{2}} + a^{m-\frac{i+j}{2}} + 1 \ne 0$. Otherwise, we have $a^{\frac{i+j}{2}}(a^{\frac{i+j}{2}} + a^{m-\frac{i+j}{2}} + 1) = 0$, i.e.,

$$1 + a^{\frac{i+j}{2}} + a^{i+j} = 0. \tag{25}$$

Note that $\mathrm{Tr}_1^m(1) = 1$, and $\mathrm{Tr}_1^m(a^{\frac{i+j}{2}} + a^{i+j}) = 0$. This induces a contradiction with Eq. (25).

By the analysis above, we have

$$\begin{aligned} \gcd(L(x), x^m + 1) &= \gcd(x^tL(x), x^m + 1) \\ &= \gcd(x^{2t} + 1, x^m + 1). \end{aligned}$$

Consequently, $f(x)$ is e-plateaued if and only if $\gcd(x^{2t} + 1, x^m + 1) = x + 1$, which is equivalent to the condition $\gcd(t, m) = 1$.

Since m is odd, $\mathrm{Tr}_1^m(1) = 1$. Consequently, $\mathrm{Tr}_1^m(1 + x^{j-i} + x^{\frac{j-i}{2}}) = 1$. That is, for any $a \in \mathbb{F}_{2^m}$, $1 + a^{j-i} + a^{\frac{j-i}{2}} \ne 0$. Hence, $\gcd(x + x^{2^{j-i}} + x^{2^{\frac{j-i}{2}}}, x^{2^m} + x) = 1$. By Lemma 2, we have $\gcd(1 + x^{j-i} + x^{\frac{j-i}{2}}, x^m + 1) = 1$. Therefore, $\gcd(L(x), x^m + 1) = \gcd(x^{m-(i+j)} + 1, x^m + 1)$. By Theorem 8, $f(x)$ is e-plateaued if and only if $\gcd(x^{m-(i+j)} + 1, x^m + 1) = x + 1$, which is equivalent to the condition $\gcd(i + j, m) = \gcd(2t, m) = \gcd(t, m) = 1$.

Corollary 10 If $n = 2m$ with $m(>1)$ odd, then for any $\beta \in \mathbb{F}_{2^2}^*$,

$$f(x) = \mathrm{Tr}_1^n(\beta x^{1+2^{2i}} + \beta x^{1+2^{2j}} + \beta x^{1+2^{2t}})$$

$(j - i = 2t, 1 \le i < j \le m - 1)$ is semi-bent if and only if $\gcd(t, m) = 1$.

5 Concluding remarks

In this paper, we study the function defined by

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} c_i \mathrm{Tr}_1^n\left(x^{1+2^{pi}}\right) + \sum_{i=1}^{\frac{p-1}{2}} d_i \mathrm{Tr}_1^n\left(x^{1+2^{qi}}\right),$$

where $c_i, d_j \in \mathbb{F}_2$, $1 \le i \le \frac{q-1}{2}$, $1 \le j \le \frac{p-1}{2}$, $n = pq$, p, q odd, $\gcd(p, q) = 1$, and the function defined by

$$f(x) = \sum_{i=1}^{\frac{m-1}{2}} c_i \mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right),$$

where $n = em$, $e = 2^l$, m is odd, $c_i \in \mathbb{F}_2$ $(1 \le i \le \frac{m-1}{2})$, $\beta \in \mathbb{F}_{2^e}^*$. We prove that these two kinds of functions contain semi-bent ones in certain cases. Moreover, we present some characterizations of e-plateaued functions with few trace terms when n is even. Furthermore, their are still some problems that need to be studied such as how to obtain semi-bent functions with higher degree by the primary constructions.

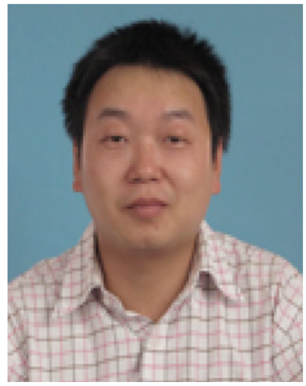
Acknowledgements We are grateful to the anonymous referees and the editor for useful comments and suggestions that improved the presentation and quality of this paper.

Funding This work was supported by Youth Research Project of educational department of Hubei province of China (B2017149) and Doctoral Program of Hubei Normal University (R201707).

References

1. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
2. Boztas, S., Kumar, P.V.: Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory **40**(2), 532–537 (1994)
3. Helleseth, T., Kummar, P.V.: Sequences with low correlation. In: Pless, P.S., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of Coding Theory, Part 3: Applications, pp. 1765–1853. Elsevier, Amsterdam (1998). (Chap. 21)
4. Golomb, S., Gong, G.: Signal Designs with Good Correlation: For Wireless Communications. Cryptography and Radar Applications. Cambridge University Press, Cambridge (2005)
5. Khoo, K., Gong, G., Stinson, D.R.: A new characterization of semi-bent and bent functions on finite fields. Des. Codes Cryptogr. **38**(2), 279–295 (2006)

6. Khoo, K., Gong, G., Stinson, D.R.: A new family of Gold-like sequences. In: Proceeding of IEEE International Symposium on Information Theory. Lausanne, Switzerland (2002)
7. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
8. Dong, D., Qu, L., Fu, S., Li, C.: New constructions of semi-bent functions in polynomial forms. Math. Comput. Model. **57**, 1139–1147 (2013)
9. Jia, W., Zeng, X., Helleseth, T., Li, C.: A class of binomial Bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **58**(9), 6054–6063 (2012)
10. Sun, G., Wu, C.: Construction of semi-bent Boolean functions in even number of variables. Chin. J. Electron. **18**(2), 231–237 (2009)
11. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
12. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)
13. Hu, H., Feng, D.: On quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **53**(7), 2610–2615 (2007)
14. Li, N., Tang, X., Helleseth, T.: New constructions of quadratic bent functions in polynomial form. IEEE Trans. Inf. Theory **60**(9), 5760–5767 (2014)
15. Li, S., Hu, L., Zeng, X.: Constructions of p-ary quadratic bent functions. Acta Appl. Math. **100**, 227–245 (2008)
16. Meidl, W., Topuzoglu, A.: Quadratic functions with prescribed spectra. Des. Codes Cryptogr. **66**, 257–273 (2013)
17. Zheng, Y., Zhang, X.: On plateaued functions. In: Proceedings of the Advances in Cryptology ICICS'99, LNCS 1726. Springer, Heidelberg (1999)
18. Canteaut, A., Charpin, P., Kyureghyan, G.M.: A new class of monomial bent functions. Finite Fields Appl. **14**(1), 221–241 (2008)
19. Carlet, C.: Boolean Functions for cryptography and Eerror Correcting Codes in the Monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, Cambridge (2010)
20. Lidl, R., Niederreiter, H.: Finite fields. In: Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading (1983)



Tao Xie received the Ph.D. degree in College of Mathematics and Statistics from Hubei University, China, in 2016. He is currently an Associate Professor with the College of Mathematics and Statistics, Hubei Normal University, China. His interests include cryptography, linear algebra and coding theory.

Gaojun Luo is currently a Ph.D. student at the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include sequences, quantum information theory and coding theory.