Applicable Algebra in Engineering, Communication and Computing (2024) 35:507–523
https://doi.org/10.1007/s00200-022-00564-5

ORIGINAL PAPER

Quadratic bent functions and their duals

Kanat Abdukhalikov[1] · Rongquan Feng[2] · Duy Ho[1]

Received: 23 November 2021 / Accepted: 20 May 2022 / Published online: 14 June 2022

Abstract
We obtain geometric characterizations of the dual functions for quadratic bent and vectorial bent functions in terms of quadrics. Additionally, using the zeros of the polynomial $X^{q+1} + X + a$ which have been studied recently in the literature, we provide some examples of binomial quadratic bent functions on $\mathbb{F}_{q^4}$ and $\mathbb{F}_{q^6}$, where q is a power of 2.

Keywords Bent functions · Duals of bent functions · Quadratic bent functions.

Mathematics Subject Classification 94A60 · 51E15 · 51E20

1 Introduction

A Boolean function on $\mathbb{F}_{2^n}$ is a mapping from $\mathbb{F}_{2^n}$ to the prime field $\mathbb{F}_2$. If f is a Boolean function defined on $\mathbb{F}_{2^n}$, then the Walsh transform of f is defined as

$$W_f(b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+b \cdot x},$$

where $b \cdot x$ is a scalar product from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$ is considered as a vector space over $\mathbb{F}_2$. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be *bent* if its Walsh transform satisfies $W_f(b) = \pm 2^{n/2}$ for all $b \in \mathbb{F}_{2^n}$. Then n is an even integer.

Bent functions were introduced by Rothaus [17] and then they were studied by Dillon [8]. Bent functions are well-studied objects as they find applications not only in

✉ Kanat Abdukhalikov
abdukhalik@uaeu.ac.ae

Rongquan Feng
fengrq@math.pku.edu.cn

Duy Ho
duyho92@gmail.com

[1] Department of Mathematical Sciences, UAE University, Al Ain PO Box 15551, UAE

[2] LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China

cryptography but also in coding theory, sequences, combinatorics and design theory. They also have interesting connections with finite geometry [1–3]. Vectorial bent functions were investigated in [16] and their duals were considered recently in [7]. For a summary of background and recent development on bent functions, we refer the reader to [6, 15].

Quadratic Boolean functions are those in the form

$$f(x) = \sum_{i=0}^{n-1} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(c_i x^{1+2^i}), c_i \in \mathbb{F}_{2^n}. \tag{1}$$

In [13, 19], the bentness of functions of the form (1) with coefficients c_i from the subfield $\mathbb{F}_2$ were considered. In [9, 10], some cases with $c_i \in \mathbb{F}_{2^e}$, where n/e is an even integer, were considered. Concerning the cases with coefficients c_i from $\mathbb{F}_{2^n}$, only monomial bent functions were considered, cp. [18].

Given a bent function f on $\mathbb{F}_{2^n}$, one can define its dual function, denoted by $\tilde{f}$, by considering the signs of the values of the Walsh transform $W_f(b)$ of f. More precisely, $\tilde{f}$ is defined by the equation:

$$(-1)^{\tilde{f}(x)} 2^{n/2} = W_f(x).$$

The dual of a bent function is bent again, and $\tilde{\tilde{f}} = f$. The bentness property is independent of the choice of the scalar product, but the values of the dual function will be changed.

In the first part of the paper we consider general quadratic bent functions and give a geometric characterization of the dual functions for quadratic bent and vectorial bent functions in terms of quadrics. In particular, for a quadratic bent function $f(x)$, we show that the dual bent function $\tilde{f}(b)$ is equal to 0 or 1 depending whether $f(x) + b \cdot x = 0$ is a hyperbolic or elliptic quadric, respectively. It provides the value of dual function $\tilde{f}(b)$ directly from the original function $f(x)$. Such a direct connection between bent function and its dual has not been noticed before.

It is known that a quadratic function $f(x)$ is bent if and only if the associated bilinear form $B(x, y) = f(x + y) + f(x) + f(y)$ is non-degenerate. This statement implies the following characterization for quadratic bent functions.

Lemma 1.1 *The quadratic Boolean function* (1) *is bent if and only if*

$$L_f(x) = \sum_{i=1}^{n-1} (c_i + c_{n-i}^{2^i}) x^{2^i}$$

is a linearized permutation polynomial, i.e. $L_f(x) = 0$ *has only solution* 0.

In the remaining part of the paper, we consider some binomial quadratic bent functions with coefficients from $\mathbb{F}_{2^n}$. In the cases we study, application of Lemma 1.1 leads to equations of the form

$$X^{q+1} + X + a = 0.$$

The solutions of these types of equations were recently described in [14], from which we obtain our main results.

The paper is organized as follows. In Sect. 2, Theorems 2.1 and 2.2 describe the dual functions for quadratic bent and vectorial bent functions. In Sects. 3 and 4, we characterize binomial quadratic bent functions on $\mathbb{F}_{q^4}$ and $\mathbb{F}_{q^6}$ (Theorems 3.6, 3.7 and 4.6).

2 The dual functions of quadratic bent functions

In this section we consider general quadratic bent and vectorial bent functions. We show that the dual functions for bent and vectorial bent functions can be characterized in terms of quadrics.

Let $V = V(n, q)$ be a vector space of dimension $n = 2k$ over a field $F = \mathbb{F}_q$, where q is a power of 2. A *quadratic form* on V is a mapping $Q : V \to F$ such that

1. $Q(\lambda x) = \lambda^2 Q(x)$ for all $\lambda \in F$, $x \in V$,and
2. $B(x, y) = Q(x + y) + Q(x) + Q(y)$ is a bilinear form.

A quadratic form is *non-degenerate* if the property $B(x, y) = 0 = Q(x)$ for all $y \in V$ implies $x = 0$. A vector $x \in V$ is *singular* if $Q(x) = 0$. The set of singular points of Q defines a *quadric* in the projective space $PG(2k - 1, q)$.

Let Q be a non-degenerate quadratic form on $2k$-dimensional vector space V over F. The coordinate system can be chosen so that Q is equivalent to one of the following two expressions:

1. $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$, or
2. $x_1^2 + ax_1x_2 + x_2^2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$, where $a \in F$ and the polynomial $\xi^2 + a\xi + 1$ is irreducible over F.

In the former case the quadratic form Q defines a *hyperbolic* quadric in $PG(2k - 1, q)$, and in the latter case Q defines an *elliptic* quadric. Hyperbolic quadric $Q(u) = 0$ in $PG(2k - 1, q)$ contains $\frac{(q^k-1)(q^{k-1}+1)}{q-1}$ points, elliptic quadric $Q(u) = 0$ in $PG(2k - 1, q)$ contains $\frac{(q^k+1)(q^{k-1}-1)}{q-1}$ points [4] .

2.1 Quadratic bent functions

For the dual of a quadratic bent function, we obtain the following geometric characterization.

Theorem 2.1 *Let $f : \mathbb{F}_{2^{2k}} \to \mathbb{F}_2$ be a quadratic bent function. Then the dual bent function $\tilde{f}$ for $f(x)$ is given by*:

$$\tilde{f}(b) = \begin{cases} 0, & \text{if } f(x) + b \cdot x = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } f(x) + b \cdot x = 0 \text{ is an elliptic quadric.} \end{cases}$$

Proof If $f(x)$ is a bent function then $f(x)$ is a non-degenerate quadratic form. So the bilinear form $B(x, y) = f(x + y) + f(x) + f(y)$ is non-degenerate. Then the bilinear form $B_b(x, y)$ for the quadratic form $f(x) + b \cdot x$ is equal to

$$B_b(x, y) = [f(x + y) + b \cdot (x + y)] + [f(x) + b \cdot x] + [f(y) + b \cdot y] = B(x, y).$$

Hence the quadratic form $f(x) + b \cdot x$ is either hyperbolic or elliptic. If it is hyperbolic then the equation $f(x) + b \cdot x = 0$ has

$$\frac{(q^k - 1)(q^{k-1} + 1)}{q - 1} + 1 = \frac{(2^k - 1)(2^{k-1} + 1)}{2 - 1} + 1 = 2^{2k-1} + 2^{k-1}$$

solutions, including 0. Therefore,

$$\begin{aligned} 2^k(-1)^{\tilde{f}(b)} =& W_f(b) \\ =& \sum_{x \in V} (-1)^{f(x)+b \cdot x} \\ =& (+1) \cdot (2^{2k-1} + 2^{k-1}) + (-1) \cdot (2^{2k} - 2^{2k-1} - 2^{k-1}) \\ =& 2^k. \end{aligned}$$

Hence $\tilde{f}(b) = 0$. Similarly, if $f(x) + b \cdot x$ is elliptic then the equation $f(x) + b \cdot x = 0$ has

$$\frac{(q^k + 1)(q^{k-1} - 1)}{q - 1} + 1 = \frac{(2^k + 1)(2^{k-1} - 1)}{2 - 1} + 1 = 2^{2k-1} - 2^{k-1}$$

solutions, including 0. Therefore,

$$\begin{aligned} 2^k(-1)^{\tilde{f}(b)} =& W_f(b) \\ =& \sum_{x \in V} (-1)^{f(x)+b \cdot x} \\ =& (+1) \cdot (2^{2k-1} - 2^{k-1}) + (-1) \cdot (2^{2k} - 2^{2k-1} + 2^{k-1}) \\ =& -2^k. \end{aligned}$$

Hence $\tilde{f}(b) = 1$. The proof is complete. □

The previous theorem provides the value of dual function $\tilde{f}(b)$ directly from the original function $f(x)$. Such a direct connection between bent function and its dual has not been noticed before.

Remark 1 We consider the special case when f is a monomial bent function with Gold exponent. Let $\alpha \in \mathbb{F}_{2^{2k}}$, $r \in \mathbb{N}$ and $d = 2^r + 1$. Let $f : \mathbb{F}_{2^{2k}} \to \mathbb{F}_2$ be defined by

$$f(x) = Tr_{\mathbb{F}_{2^{2k}}/\mathbb{F}_2}(\alpha x^d).$$

This type of functions were studied in [11, 12]. As shown in [11], f is bent if and only if

$$\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^{2k}}\}.$$

Using Theorem 2.1, the dual of f is

$$\tilde{f}(b) = \begin{cases} 0, & \text{if } Tr_{\mathbb{F}_{2^{2k}}/\mathbb{F}_2}(\alpha x^d) + b \cdot x = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } Tr_{\mathbb{F}_{2^{2k}}/\mathbb{F}_2}(\alpha x^d) + b \cdot x = 0 \text{ is an elliptic quadric.} \end{cases}$$

2.2 Quadratic vectorial bent functions

Let K/F be an extension of finite fields of characteristic 2 and $\dim_F K = 2k$. Let $\langle \cdot, \cdot \rangle : K \times K \to F$ be a non-degenerate bilinear form over F. For a finite field F we denote

$$tr(x) = Tr_{F/\mathbb{F}_2}(x).$$

A function $f : K \to F$ is a *vectorial bent function* if the Boolean function $f_\alpha(x) = tr(\alpha f(x))$ is bent for all $\alpha \in F^*$. The functions $f_\alpha(x) = tr(\alpha f(x))$ are called *component functions* of $f(x)$. Below we choose a scalar product from $K \times K$ to $\mathbb{F}_2$ as

$$b \cdot x = tr(\langle b, x \rangle).$$

Theorem 2.2 *Let $K \supset F$ be finite fields of characteristic 2 and let $f : K \to F$ be a quadratic vectorial bent function. Let $f_\alpha(x) = tr(\alpha f(x))$, where $\alpha \in F^*$. Then the dual bent function $\widetilde{f_\alpha}$ for component function f_α is given by*:

$$\widetilde{f_\alpha}(b) = \begin{cases} 0, & \text{if } \alpha f(x) + \langle b, x \rangle^2 = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } \alpha f(x) + \langle b, x \rangle^2 = 0 \text{ is an elliptic quadric.} \end{cases}$$

Proof Let $f(x)$ be a vectorial bent function. Then $f_\alpha(x) = tr(\alpha f(x))$ is bent and $f_\alpha(x)$ is a non-degenerate quadratic form for all $\alpha \in F^*$. Hence $f(x)$ is a non-degenerate quadratic form over F and the associated bilinear form $B(x, y) = f(x + y) + f(x) + f(y)$ is non-degenerate. Fix $\alpha \in F^*$. Then the bilinear form $B_b(x, y)$ for the quadratic form $\alpha f(x) + \langle b, x \rangle^2$ is equal to

$$B_b(x, y) = [\alpha f(x + y) + \langle b, x + y \rangle^2] + [\alpha f(x) + \langle b, x \rangle^2] + [\alpha f(y) + \langle b, y \rangle^2] = \alpha B(x, y),$$

and it is non-degenerate. Hence the quadratic form $\alpha f(x) + \langle b, x \rangle^2$ is either hyperbolic or elliptic. If it is hyperbolic (resp. elliptic) then the equation $\alpha f(x) + \langle b, x \rangle^2 = 0$ has $\frac{(q^k-1)(q^{k-1}+1)}{q-1}$ (resp. $\frac{(q^k+1)(q^{k-1}-1)}{q-1}$) solutions in $PG(2k - 1, F)$, where $2k = \dim_F K$.

Recall that $PG(2k - 1, F)$ can be considered as the set of all 1-dimensional F-subspaces in K. Let S be a subset in K^* which represents all elements of $PG(2k - 1, F)$

(elements of S generate distinct 1-dimensional F-subspaces in K). Hence $|S| = \frac{q^{2k}-1}{q-1}$ and $K^* = \{\lambda u \mid \lambda \in F^*, u \in S\}$. Therefore,

$$\begin{aligned}
q^k(-1)^{\widetilde{f_\alpha}(b)} =& W_{f_\alpha}(b)\\
=& \sum_{x\in K}(-1)^{f_\alpha(x)+tr(\langle b,x\rangle)}\\
=& \sum_{x\in K}(-1)^{tr(\alpha f(x))+tr(\langle b,x\rangle)}\\
=& 1+\sum_{\lambda\in F^*,\ u\in S}(-1)^{tr(\alpha f(\lambda u))+tr(\langle b,\lambda u\rangle)}\\
=& 1+\sum_{\lambda\in F^*,\ u\in S}(-1)^{tr(\alpha\lambda^2 f(u))+tr(\lambda\langle b,u\rangle)}\\
=& 1-\frac{q^{2k}-1}{q-1}+\sum_{\lambda\in F,\ u\in S}(-1)^{tr(\lambda(\sqrt{\alpha f(u)}+\langle b,u\rangle))}\\
=& \frac{q-q^{2k}}{q-1}+\sum_{u\in S}\sum_{\lambda\in F}(-1)^{tr(\lambda(\sqrt{\alpha f(u)}+\langle b,u\rangle))}\\
=& \frac{q-q^{2k}}{q-1}+|N_b|q,
\end{aligned}$$

where

$$N_b = \{u \in S \mid \sqrt{\alpha f(u)} + \langle b, u\rangle = 0\} = \{u \in S \mid \alpha f(u) + \langle b, u\rangle^2 = 0\}.$$

If $\alpha f(u) + \langle b, u\rangle^2 = 0$ is hyperbolic then $|N_b| = \frac{(q^k-1)(q^{k-1}+1)}{q-1}$. Therefore,

$$\frac{q-q^{2k}}{q-1}+|N_b|q = \frac{q-q^{2k}}{q-1}+\frac{q(q^k-1)(q^{k-1}+1)}{q-1} = q^k.$$

Hence

$$\widetilde{f_\alpha}(b) = 0.$$

If $\alpha f(u) + \langle b, u\rangle^2 = 0$ is elliptic then $|N_b| = \frac{(q^k+1)(q^{k-1}-1)}{q-1}$. Therefore,

$$\frac{q-q^{2k}}{q-1}+|N_b|q = \frac{q-q^{2k}}{q-1}+\frac{q(q^k+1)(q^{k-1}-1)}{q-1} = -q^k.$$

Hence

$$\widetilde{f_\alpha}(b) = 1.$$

The proof is complete. □

Theorem 2.2 provides the value of dual function $\widetilde{f_\alpha}(b)$ for the component function $f_\alpha(x)$ directly from the original function $f_\alpha(x)$.

Remark 2 We consider the special case when f is a monomial vectorial bent function with Gold exponent. Let $\beta \in K, r \in \mathbb{N}$ and $d = 2^r + 1$. Let $f : K \to F$ be defined by

$$f(x) = Tr_{K/F}(\beta x^d).$$

In [18], it was proved that f is vectorial bent if and only if $\beta \notin \{x^{\gcd(d,t)} \mid x \in K\}$, where $t = 2^k + 1$. For each $\alpha \in F^*$, the dual bent function $\widetilde{f_\alpha}$ for component function f_α is given by:

$$\widetilde{f_\alpha}(b) = \begin{cases} 0, & \text{if } \alpha Tr_{K/F}(\beta x^d) + \langle b, x\rangle^2 = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } \alpha Tr_{K/F}(\beta x^d) + \langle b, x\rangle^2 = 0 \text{ is an elliptic quadric.} \end{cases}$$

3 Binomial quadratic bent functions on $\mathbb{F}_{q^4}$

In this section, let $q = 2^m$, $n = 4m$, $F = \mathbb{F}_q, K = \mathbb{F}_{q^2}, E = \mathbb{F}_{q^4}$. Let $Tr_{M/L}(x)$ and $N_{M/L}(x)$ be the trace and the norm functions with respect to a finite field extension M/L. For convenience, we abbreviate

$$Tr(x) = Tr_{E/\mathbb{F}_2}(x),\ tr(x) = Tr_{F/\mathbb{F}_2}(x).$$

We consider the bentness of the function $f : E \to \mathbb{F}_2$ defined by

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^2+1}),$$

where $\alpha, \beta \in E$.

3.1 The roots of the polynomial $P_a(X) = X^{q+1} + X + a$

For $a \in E$, let

$$P_a(X) = X^{q+1} + X + a.$$

We recall the following sequence of polynomials from [14]:

$$A_0(X) = 0, A_1(X) = 1, A_2(X) = 1,$$
$$A_{r+2}(X) = A_{r+1}(X)^q + X^q A_r(X)^{q^2},$$

for $r \geq 0$. Also, adopting the notation in [14], we define

$$F(X) = A_4(X) = 1 + X^q + X^{q^2},$$
$$G(X) = A_5(X) + XA_3(X)^q = X^{q^3+q} + X^{q^2+1} + X^{q^3} + X^{q^2} + X^q + X + 1.$$

For $a \in E$, we denote $H(a) = tr\left(\dfrac{N_{E/F}(a)}{G(a)^2}\right)$ and $E(a) = \dfrac{aF(a)^{q+1}}{G(a)^2}$. From [14], we have the following characterization on the number of roots of $P_a(X)$.

Lemma 3.1 ([14]) *Let $a \in E$. Then the polynomial $P_a(X) = X^{q+1} + X + a$ has 0, 1, 2 or $q+1$ zeros in E. Furthermore, if N_a is the number of roots of $P_a(x)$ in E, then the following hold.*

1. $N_a = 0$ *if and only if* $G(a) \neq 0$ *and* $H(a) \neq 0$.
2. $N_a = 1$ *if and only if* $F(a) \neq 0$ *and* $G(a) = 0$.
3. $N_a = 2$ *if and only if* $G(a) \neq 0$ *and* $H(a) = 0$.
4. $N_a = q+1$ *if and only if there exists* $u \in E \backslash K$ *such that* $a = \dfrac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$. *Then the* $q+1$ *zeros in* E *of* $P_a(X)$ *are* $x_0 = \dfrac{1}{1+(u+u^q)^{q-1}}$ *and* $x_\alpha = \dfrac{(u+\alpha)^{q^2-q}}{1+(u+u^q)^{q-1}}$ *for* $\alpha \in F$.

Lemma 3.2 (*cp.* [5]) *The quadratic polynomial $Q(X) = aX^2 + bX + c \in K[X]$, $b \neq 0$, has two zeros in K if and only if $Tr_{K/\mathbb{F}_2}\left(\frac{ac}{b^2}\right) = 0$.*

3.2 Bent functions on $\mathbb{F}_{q^4}$

Let

$$S = \left\{x \in E \mid N_{E/F}(x) = 1\right\} = \left\{x \in E \mid x^{q^3+q^2+q+1} = 1\right\},$$

$$S_K = \left\{x \in K \mid N_{K/F}(x) = 1\right\} = \left\{x \in K \mid x^{q+1} = 1\right\}.$$

Lemma 3.3 $S \cap K = S_K$.

Proof Let θ be a primitive element of E. Hence $S = \langle \theta^{q-1} \rangle$. We have $\theta^{(q-1)i} \in K$ if and only if $(\theta^{(q-1)i})^{q^2-1} = 1$ if and only if $(q-1)(q^2-1)i \equiv 0 \pmod{q^4-1}$ if and only if $i \equiv 0 \pmod{q^2+1}$ since $\gcd(q-1, q^2+1) = 1$. On the other hand, $S_K = \langle \theta^{(q-1)(q^2+1)} \rangle$. □

Lemma 3.4 *Let $\alpha \in E^*$ and $\beta \in E$ such that $\beta + \beta^{q^2} = 1$. Let $f : E \to \mathbb{F}_2$ be defined by*

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^2+1}).$$

Let $a = \alpha^{q^3+q}$. Then $a \in K$, and f is bent if and only if the equation

$$X^{q+1} + X + a = 0$$

has no solution in $\alpha^q S$.

Proof By Lemma 1.1, the function f is bent if and only if the polynomial

$$L_f(x) = \alpha^{q^3} x^{q^3} + (\beta + \beta^{q^2}) x^{q^2} + \alpha x^q$$

is a linearized permutation polynomial. For $x \neq 0$, we have

$$\begin{aligned} L_f(x) = 0 &\iff \alpha^{q^2} x^{q^2} + x^q + \alpha^{q^3} x = 0 \\ &\iff x^{q^2-1} + \alpha^{-q^2} x^{q-1} + \alpha^{q^3-q^2} = 0. \end{aligned} \tag{2}$$

Let $y = \alpha^q x^{q-1}$. Then $y \in \alpha^q S$ and $x^{q-1} = \alpha^{-q} y$. Hence (2) is equivalent to

$$(\alpha^{-q} y)^{q+1} + \alpha^{-q^2} \alpha^{-q} y + \alpha^{q^3-q^2} = 0,$$

which is true if and only if $y^{q+1} + y + a = 0$, where $a = \alpha^{q^3+q}$. Therefore, $L_f(x)$ is a linearized permutation polynomial if and only if the equation

$$X^{q+1} + X + a = 0$$

has no solution in $\alpha^q S$, which completes the proof. □

For $a \in K$, we have

$$\begin{aligned} F(a) =& 1 + a + a^q \in F, \\ G(a) =& 1 + a^2 + a^{2q} = F(a)^2 \in F, \\ H(a) =& tr\left(\frac{a^{q+1}}{G(a)}\right) = tr\left(\frac{a^{q+1}}{1 + a^2 + a^{2q}}\right). \end{aligned}$$

Lemma 3.5 *Let $a \in K$. If $G(a) \neq 0$ and $H(a) = 0$, then the equation*

$$P_a(X) = X^{q+1} + X + a = 0$$

has two solutions in E, and these solutions are in K.

Proof From Lemma 3.1, we know that $P_a(X)$ has two roots in E. Let x be a root of $P_a(X)$. By [14, Lemma 5], x is also a solution of the quadratic equation

$$Q(X) = F(a)X^2 + G(a)X + aF(a)^q = 0.$$

Let

$$E(a) = \frac{aF(a)^{q+1}}{G(a)^2} = \frac{aF(a)^2}{G(a)^2} = \frac{a}{G(a)}.$$

Then

$$Tr_{K/\mathbb{F}_2}(E(a)) = tr\left(Tr_{K/F}\left(\frac{a}{G(a)}\right)\right) = tr\left(\frac{1 + F(a)}{G(a)}\right) = tr\left(\frac{1}{G(a)} + \frac{1}{F(a)}\right) = 0.$$

By Lemma 3.2, the solutions of $Q(X) = 0$ are in K, which proves the lemma. □

Now we obtain the main theorems.

Theorem 3.6 *Let $\alpha \in E^*$. Let $\beta \in E$ such that $\beta + \beta^{q^2} = 1$. Let $f : E \to \mathbb{F}_2$ be defined by*

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^2+1}) = Tr(\alpha x^{q+1}) + Tr_{K/\mathbb{F}_2}(x^{q^2+1}).$$

Then f is bent if and only if

$$\alpha^{q^3+q} + \alpha^{q^2+1} \neq 1. \tag{3}$$

Proof Let $a = \alpha^{q^3+q}$. Then $a \in K$. Note that $F(a) = 1 + \alpha^{q^3+q} + \alpha^{q^2+1}$. Let $\alpha = \lambda w$, where $\lambda \in F$, $w \in S$.

1. Assume that $F(a) = 0$. By Lemma 3.1, there exists $u \in E \backslash K$ such that $a = \dfrac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$. Let $c = (u+u^q)^{q-1} \in S$. We have

$$\begin{aligned} a =& \frac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}} = \frac{(u+u^q)^{q^2+1}}{((u+u^q)+(u+u^q)^q)^{q+1}} \\ =& \frac{(u+u^q)^{q^2-q}}{(1+(u+u^q)^{q-1})^{q+1}} = \frac{((u+u^q)^{q-1})^q}{(1+(u+u^q)^{q-1})^{q+1}} \\ =& \frac{c^q}{(1+c)^{q+1}} = (1+c)^{-2}\frac{c^q}{(1+c)^{q-1}}. \end{aligned}$$

Hence $a \in (1+c)^{-2}S$. By Lemma 3.1, $P_a(X)$ has a root $x_0 = (1+c)^{-1}$. We have

$$x_0 \in \lambda S = \alpha^q S \iff (1+c)^{-1} \in \lambda S \iff (1+c)^{-2} \in \lambda^2 S \iff a \in \lambda^2 S.$$

Note that $a = \alpha^{q^3+q} = \lambda^2 u^{q^3+q} \in \lambda^2 S$. Hence $P_a(X) = 0$ has a root $x_0 \in \lambda S = \alpha^q S$. Now we apply Lemma 3.4 and conclude that $f(x)$ is not bent.

2. We now assume that $F(a) \neq 0$. If $H(a) \neq 0$, then the equation $P_a(X) = 0$ has no root in E by Lemma 3.1, and hence no root in λS. It remains to consider the case $H(a) = 0$. Then by Lemma 3.5, $P_a(X)$ has two roots in K. Let $x_1 \in K$ be a root of $P_a(X)$.

Suppose $x_1 \in \lambda S = \alpha^q S$. Then by Lemma 3.3, $x_1 = \lambda v$, for some $v \in S_K$. We have

$$x_1^{q+1} + x_1 + a = 0 \iff \lambda^2 + x_1 + a = 0 \iff x_1 = a + \lambda^2.$$

On the other hand,

$$\begin{aligned} \lambda^2 = x_1^{q+1} &= (a+\lambda^2)^{q+1} = (a^q + \lambda^2)(a+\lambda^2) \\ &= a^{q+1} + \lambda^2 a^q + \lambda^2 a + \lambda^4 \\ &= a^{q+1} + \lambda^2(F(a)+1) + \lambda^4. \end{aligned}$$

Therefore,

$$F(a) = \frac{a^{q+1} + \lambda^4}{\lambda^2}.$$

We have

$$a^{q+1} + \lambda^4 = \alpha^{q^4+q^3+q^2+q} + \lambda^4 = \lambda^4 u^{q^3+q^2+q+1} + \lambda^4 = \lambda^4 + \lambda^4 = 0,$$

which implies $F(a) = 0$, a contradiction to our assumption. Thus, if $H(a) = 0$, then $P_a(X)$ also has no root in λS. This completes the proof. □

Theorem 3.7 *Let $\alpha \in E^*$ and $\beta \in E$. Let $f : E \to \mathbb{F}_2$ be defined by*

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^2+1}) = Tr(\alpha x^{q+1}) + Tr_{K/\mathbb{F}_2}((\beta + \beta^{q^2})x^{q^2+1}).$$

Then f is bent if and only if

$$\alpha^{q^3+q} + \alpha^{q^2+1} \neq (\beta + \beta^{q^2})^{q+1}. \tag{4}$$

Proof 1. Suppose that $\beta + \beta^{q^2} \neq 0$. Consider the function $h(y) = Tr(\alpha y^{q+1}) + Tr_{K/\mathbb{F}_2}(y^{q^2+1})$. Making substitution $y = x(\beta + \beta^{q^2})^{1/2}$ we get

$$\begin{aligned} h'(x) = h(y) =& Tr(\alpha(\beta + \beta^{q^2})^{(q+1)/2} x^{q+1}) + Tr_{K/\mathbb{F}_2}((\beta + \beta^{q^2})x^{q^2+1}) \\ =& Tr(\delta x^{q+1} + \beta x^{q^2+1}), \end{aligned}$$

where $\delta = \alpha(\beta + \beta^{q^2})^{(q+1)/2}$. Then Condition (3) for the function $h(y)$ and α implies that

$$\begin{aligned} \frac{\delta^{q^2+1}}{(\beta + \beta^{q^2})^{q+1}} + \frac{\delta^{q^3+q^2}}{(\beta + \beta^{q^2})^{q+1}} &\neq 1, \\ \delta^{q^2+1} + \delta^{q^3+q^2} &\neq (\beta + \beta^{q^2})^{q+1}. \end{aligned}$$

2. Now suppose that $\beta + \beta^{q^2} = 0$. Then $f(x) = Tr(\alpha x^{q+1})$. Let θ be a primitive element of E. By Lemma 1.1, the function $f(x)$ is bent if and only if the polynomial $L_f(x) = \alpha^{q^3} x^{q^3} + \alpha x^q$ is a linearized permutation polynomial. For $x \neq 0$, we have $L_f(x) = 0 \iff \alpha x + \alpha^q x^{q^2} = 0 \iff \alpha^{q-1} x^{q^2-1} = 1 \iff (\alpha x^{q+1})^{q-1} = 1 \iff \alpha x^{q+1} \in F^*$.

Since $F^* = \langle \theta^{(q+1)(q^2+1)} \rangle$, we have that $f(x)$ is bent $\iff \alpha \notin \langle \theta^{q+1} \rangle \iff \alpha^{(q^2+1)(q-1)} \neq 1 \iff \alpha^{q^2+1} \notin F^* \iff \alpha^{q^2+1} + (\alpha^{q^2+1})^q \neq 0$, which completes the proof. □

Remark 3 Condition (4) can be written as

$$Tr_{K/F}(N_{E/K}(\alpha)) \neq N_{K/F}(Tr_{E/K}(\beta)).$$

Remark 4 For the special case $\beta + \beta^{q^2} = 0$ of Theorem 3.7, it was proved in [18, Theorem 2] that the function $f(x) = Tr(\alpha x^{q+1})$ is bent if and only if $\alpha \notin \langle \theta^{q+1} \rangle$, where θ is a primitive element of E.

Remark 5 From Theorem 2.1, the dual of f is given by

$$\tilde{f}(b) = \begin{cases} 0, & \text{if } Tr(\alpha x^{q+1} + \beta x^{q^2+1}) + b \cdot x = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } Tr(\alpha x^{q+1} + \beta x^{q^2+1}) + b \cdot x = 0 \text{ is an elliptic quadric.} \end{cases}$$

4 Binomial quadratic bent functions on $\mathbb{F}_{q^6}$

In this section, let $q = 2^m, F = \mathbb{F}_q, F' = \mathbb{F}_{q^2}, K = \mathbb{F}_{q^3}, E = \mathbb{F}_{q^6}$. We consider the bentness of the function $f : E \to \mathbb{F}_2$ defined by

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^3+1}),$$

where $\alpha, \beta \in E$.

4.1 The roots of the polynomial $P_a(X) = X^{q^2+1} + X + a$

For $a \in E$, let

$$P_a(X) = X^{q^2+1} + X + a.$$

We recall the following sequence of polynomials from [14]:

$$A_0(X) = 0, A_1(X) = 1, A_2(X) = 1,$$
$$A_{r+2}(X) = A_{r+1}(X)^{q^2} + X^{q^2} A_r(X)^{q^2},$$

for $r \geq 0$. Also, define

$$F(X) = A_3(X) = 1 + X^{q^2},$$
$$G(X) = A_4(X) + XA_2(X)^{q^2} = X^{q^4} + X^{q^2} + X + 1.$$

For $a \in E$, denote $H(a) = tr\left(\dfrac{N_{E/F}(a)}{G(a)^2}\right)$ and $E(a) = \dfrac{aF(a)^{q+1}}{G(a)^2}$.

Lemma 4.1 ([14]) *Let $a \in E$. Then the polynomial $P_a(X) = X^{q^2+1} + X + a$ has 0, 1, 2 or $q^2 + 1$ zeros in E. Furthermore, if N_a is the number of roots of $P_a(x)$ in E, then the following holds.*

1. $N_a = 0$ *if and only if* $G(a) \neq 0$ *and* $H(a) \neq 0$.
2. $N_a = 1$ *if and only if* $F(a) \neq 0$ *and* $G(a) = 0$. *In this case,* $(aF(a)^{q-1})^{\frac{1}{2}}$ *is the unique zero in* E.
3. $N_a = 2$ *if and only if* $G(a) \neq 0$ *and* $H(a) = 0$.
4. $N_a = q^2 + 1$ *if and only if* $F(a) = 0$.

4.2 Bent functions on $\mathbb{F}_{q^6}$

Let

$$S = \left\{x \in E \mid N_{E/F}(x) = 1\right\} = \left\{x \in E \mid x^{\frac{q^6-1}{q-1}} = 1\right\},$$
$$S_K = \left\{x \in K \mid N_{K/F}(x) = 1\right\} = \left\{x \in K \mid x^{\frac{q^3-1}{q-1}} = 1\right\},$$
$$S' = \left\{x \in E \mid N_{E/F'}(x) = 1\right\} = \left\{x \in E \mid x^{\frac{q^6-1}{q^2-1}} = 1\right\}.$$

Lemma 4.2 *Let $\alpha \neq 0$. Let $\beta \in E$ such that $\beta + \beta^{q^3} = 1$. Let $f : E \to \mathbb{F}_2$ be defined by*

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^3+1}).$$

Let $a = \alpha^{q^5+q^2} = (\alpha^{q^2})^{q^3+1} \in K$. Then f is bent if and only if the equation

$$P_a(X) = X^{q^2+1} + X + a = 0 \tag{5}$$

has no solution in $\alpha^{q^2} S'$.

Proof By Lemma 1.1, the function f is bent if and only if the polynomial

$$L_f(x) = \alpha^{q^5} x^{q^5} + (\beta + \beta^{q^3}) x^{q^3} + \alpha x^q$$

is a linearized permutation polynomial. For $x \neq 0$, we have

$$\begin{aligned} L_f(x) = 0 &\iff \alpha^{q^4} x^{q^4} + x^{q^2} + \alpha^{q^5} x = 0 \\ &\iff x^{q^4-1} + \alpha^{-q^4} x^{q^2-1} + \alpha^{q^5-q^4} = 0. \end{aligned} \tag{6}$$

Let $y = \alpha^{q^2} x^{q^2-1}$. Then $y \in \alpha^{q^2} S'$. By substituting $x^{q^2-1} = \alpha^{-q^2} y$, the equation (6) is equivalent to

$$(\alpha^{-q^2} y)^{q^2+1} + \alpha^{-q^4} \alpha^{-q^2} y + \alpha^{q^5-q^4} = 0,$$

which means $y^{q^2+1} + y + a = 0$, where $a = \alpha^{q^5+q^2}$. Therefore, $L_f(x)$ is a linearized permutation polynomial if and only if the equation

$$X^{q^2+1} + X + a = 0$$

has no solution in $\alpha^{q^2} S'$, which completes the proof. □

For $a \in K$, we have

$$F(a) = a^{q^2} + 1,$$
$$G(a) = a^{q^2} + a^q + a + 1.$$

In the following lemma we consider the case $F(a) = 0$, that is, when $a = 1$.

Lemma 4.3 *The equation*

$$X^{q^2+1} + X + 1 = 0$$

has no root in $\alpha^{q^2} S'$ if and only if $\alpha^{q^4+q^2+1} \neq 1$.

Proof By Lemma 4.1, the Eq. (5) has $q^2 + 1$ roots. If x is a root of (5), then

$$x^{\frac{q^6-1}{q^2-1}} = x^{q^4+q^2+1} = x^{q^4} x^{q^2+1} = x^{q^4}(x+1) = x^{q^4+1} + x^{q^4} = (x^{q^2+1} + x)^{q^4} = 1,$$

which implies $x \in S'$. Therefore, $x \notin \alpha^{q^2} S'$ if and only if $\alpha^{q^2} \notin S'$, if and only if

$$(\alpha^{q^2})^{q^4+q^2+1} = \alpha^{q^4+q^2+1} \neq 1,$$

which proves the lemma. □

We now consider the case $F(a) \neq 0$.

Lemma 4.4 *Let $F(a) \neq 0$ and $G(a) = 0$. The Eq. (5) has no root in $\alpha^{q^2} S'$ if and only if $\alpha^{(q-1)(q^4+q^2+1)} \neq 1$.*

Proof By Lemma 4.1, the Eq. (5) has the unique root

$$x = \left(aF(a)^{q^2-1} \right)^{1/2}.$$

We have $x \in \alpha^{q^2} S'$ if and only if $aF(a)^{q^2-1} \in \alpha^{2q^2} S'$, if and only if

$$a^{q^4+q^2+1} \left(\alpha^{-2q^2} \right)^{q^4+q^2+1} = 1,$$

which is if and only if

$$\alpha^{(q^3-1)(q^4+q^2+1)} = 1.$$

Modulo $(q^6 - 1)$, we have

$$(q^3-1)(q^4+q^2+1) = q^7 + q^5 + q^3 - q^4 - q^2 - 1 = q(1 + q^4 + q^2) - q^4 - q^2 - 1 = (q-1)(q^4+q^2+1).$$

This proves the lemma. □

Lemma 4.5 *Let $G(a) \neq 0$ and $H(a) = 0$. Let $N(\alpha) = N_{E/F'}(\alpha) = \alpha^{q^4+q^2+1}$. The Eq. (5) has no root in $\alpha^{q^2} S'$ if and only if at least one of the following is true.*

1. $\left(\frac{\alpha^{q^4+1}+\alpha^{q^5}}{\alpha^{q^4+q}+1}\right)^{q^4+q^2+1} \neq 1.$
2. $N(\alpha)^2 + G(a)N(\alpha) \neq a^{q^2+q+1}.$

Proof By Lemma 4.1, the Eq. (5) has two roots. Let x be a root of (5). Then $x \in \alpha^{q^2}S'$ if and only if

$$x^{q^4+q^2+1} = (\alpha^{q^2})^{q^4+q^2+1} = \alpha^{q^4+q^2+1} = N(\alpha).$$

Substituting $x^{q^2+1} = x + a$ into the above, we obtain $x^{q^4+1} + ax^{q^4} = N(\alpha)$, which gives

$$x^{q^2+1} + a^{q^2}x = N(\alpha). \tag{7}$$

We note that $a \neq 1$. From (5) and (7), we get

$$x = \frac{N(\alpha)+a}{a^{q^2}+1} = \frac{N(\alpha)+a}{F(a)}.$$

Since $x \in \alpha^{q^2}S'$, it follows that $x\alpha^{-q^2} \in S'$, which is equivalent to

$$\left(\frac{\alpha^{q^4+1}+\alpha^{q^5}}{\alpha^{q^4+q}+1}\right)^{q^4+q^2+1} = 1.$$

Since x is a root of (5),

$$\begin{aligned}
&\left(\frac{N(\alpha)+a}{F(a)}\right)^{q^2+1} + \frac{N(\alpha)+a}{F(a)} + a = 0\\
\iff &(N(\alpha)+a)^{q^2+1} + (N(\alpha)+a)F(a)^{q^2} = aF(a)^{q^2+1}\\
\iff &N(\alpha)^2 + G(a)N(\alpha) = a^{q^2+q+1}.
\end{aligned}$$

The proof follows. □

Theorem 4.6 *Let $\alpha \in E^*$. Let $\beta \in E$ such that $\beta + \beta^{q^3} = 1$. Let $f : E \to \mathbb{F}_2$ be defined by*

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^3+1}) = Tr(\alpha x^{q+1}) + Tr_{K/\mathbb{F}_2}(x^{q^3+1}).$$

Let $N(\alpha) = N_{E/F'}(\alpha) = \alpha^{q^4+q^2+1}$ and let $a = \alpha^{q^5+q^2}, G(a) = a^{q^2} + a^q + a + 1$. Then f is bent if and only if one of the following is true.

1. $a = 1$ and $N(\alpha) \neq 1$.
2. $a \neq 1, G(a) = 0$, and $N(\alpha)^{q-1} \neq 1$.
3. $G(a) \neq 0$ and $\left(\frac{\alpha^{q^4+1}+\alpha^{q^5}}{\alpha^{q^4+q}+1}\right)^{q^4+q^2+1} \neq 1.$

4. $G(a) \neq 0$ and $N(\alpha)^2 + G(a)N(\alpha) \neq a^{q^2+q+1}$.

Proof Let $H(a) = Tr_{F'/\mathbb{F}_2}\left(\frac{N_{E/F'}(a)}{G(a)^2}\right)$. We have

$$N_{E/F'}(a) = a^{q^4+q^2+1} = a^{q^2+q+1} = N_{K/F}(a) \in F,$$
$$G(a) = a^{q^4} + a^{q^2} + a + 1 = a^{q^2} + a^q + a + 1 = Tr_{K/F}(a) + 1 \in F,$$

and so

$$H(a) = Tr_{F'/\mathbb{F}_2}\left(\frac{N_{E/F'}(a)}{G(a)^2}\right) = Tr_{F/\mathbb{F}_2} \cdot Tr_{F'/F}\left(\frac{N_{E/F'}(a)}{G(a)^2}\right) = 0.$$

Hence, the Eq. (5) always has a solution. From Lemma 4.2, the function f is bent if and only if (5) has no solutions in $\alpha^{q^2}S'$. In view of Lemma 4.1, we only need to consider the following cases.

1. $F(a) = 0$, that is, when $a = 1$. By Lemma 4.3, the Eq. (5) has no root in $\alpha^{q^2}S'$ if and only if $\alpha^{q^4+q^2+1} \neq 1$.
2. $F(a) \neq 0$ and $G(a) = 0$. By Lemma 4.4, the Eq. (5) has no root in $\alpha^{q^2}S'$ if and only if $\alpha^{(q-1)(q^4+q^2+1)} \neq 1$.
3. $G(a) \neq 0$. By Lemma 4.5, the Eq. (5) has no root in $\alpha^{q^2}S'$ if and only if

$$\left(\frac{\alpha^{q^4+1} + \alpha^{q^5}}{\alpha^{q^4+q} + 1}\right)^{q^4+q^2+1} \neq 1,$$

or

$$N(\alpha)^2 + G(a)N(\alpha) \neq a^{q^2+q+1}.$$

The proof now follows. □

Remark 6 It was proved in [18, Theorem 2] that the function $f(x) = Tr(\alpha x^{q+1})$ is bent if and only if $\alpha \notin \langle \theta^{q+1} \rangle$, where θ is a primitive element of E.

Remark 7 Similar to Sect. 2, the condition $\beta + \beta^{q^3} = 1$ in Theorem 4.6 can be replaced by $\beta + \beta^{q^3} \neq 0$ with a change of variable $y = x(\beta + \beta^{q^3})^{1/2}$.

Remark 8 From Theorem 2.1, the dual of f is given by

$$\tilde{f}(b) = \begin{cases} 0, & \text{if } Tr(\alpha x^{q+1} + \beta x^{q^3+1}) + b \cdot x = 0 \text{ is a hyperbolic quadric,} \\ 1, & \text{if } Tr(\alpha x^{q+1} + \beta x^{q^3+1}) + b \cdot x = 0 \text{ is an elliptic quadric.} \end{cases}$$

Remark 9 Let $\alpha, \beta \in E$. Let $f : E \to \mathbb{F}_2$ be defined by

$$f(x) = Tr(\alpha x^{q+1} + \beta x^{q^2+1}).$$

By Lemma 1.1, the function f is bent if and only if the polynomial

$$L_f(x) = \alpha^{q^5} x^{q^5} + \beta^{q^4} x^{q^4} + \beta x^{q^2} + \alpha x^q$$

is a linearized permutation polynomial. Unfortunately, the polynomial L_f is not in the form of $P_a(X)$ in Lemma 4.1 and a different method will be required to study its roots.

Acknowledgements This research was supported by UAEU grants G00003490 and G00003491.

References

1. Abdukhalikov, K.: Bent functions and line ovals. Finite Fields Appl. **47**, 94–124 (2017)
2. Abdukhalikov, K.: Hyperovals and bent functions. Eur. J. Comb. **79**, 123–139 (2019)
3. Abdukhalikov, K.: Equivalence classes of Niho bent functions. Designs Codes Cryptogr. **89**(7), 1509–1534 (2021)
4. Bierbrauer, J.: Introduction to Coding Theory, 2nd edn. CRC Press, Boca Raton, FL (2017)
5. Berlekamp, E.R., Rumsey, H., Solomon, G.: On the solution of algebraic equations over finite fields. Inf. Control **10**, 553–564 (1967)
6. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
7. Çeşmelioğlu, A., Meidl, W., Pott, A.: Vectorial bent functions and their duals. Linear Algebra Appl. **548**, 305–320 (2018)
8. Dillon, J.K.: Elementary Hadamard difference sets, PhD dissertation, University of Maryland, Baltimore, MD (1974)
9. Hu, H., Feng, D.: On quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory **53**(7), 2610–2615 (2007)
10. Huang, D., Tang, C., Qi, Y., Xu, M.: New quadratic bent functions in polynomial forms with coefficients in extension fields. Appl. Algebra Engrg. Comm. Comput. **30**(4), 333–347 (2019)
11. Leander, N.: Monomial bent functions. IEEE Trans. Inform. Theory. **52**, 738–743 (2006)
12. Langevin, P., Leander, G.: Monomial bent functions and Stickelberger's theorem. Finite Fields Appl. **14**, 727–742 (2008)
13. Ma, W., Lee, M., Zhang, F.: A new class of bent functions, IEICE Trans. Fundamentals, vol. E88-A, no. 7, 2039–2040 (2005)
14. Kim, K.H., Choe, J., Mesnager, S.: Solving $X^{q+1} + X + a = 0$ over finite fields. Finite Fields Appl. **70**, 101797, 16 pp (2021)
15. Mesnager, S.: Bent Functions. Fundamentals and Results. Springer, Cham (2016)
16. Nyberg, K.: Perfect nonlinear S-boxes. In: Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science. 547, pp. 378–386 (1991)
17. Rothaus, O.S.: On "bent" functions, J. Combin. Theory, Series A, **20**, 300–305 (1976)
18. Xu, Y., Carlet, C., Mesnager, S., Wu, C.: Classification of bent monomials, constructions of bent multinomials and upper bounds on the nonlinearity of vectorial functions. IEEE Trans. Inf. Theory **64**(1), 367–383 (2018)
19. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inform. Theory **52**(7), 3291–3299 (2006)