SIAM J. DISCRETE MATH.
Vol. 22, No. 2, pp. 650–665

CUBIC MONOMIAL BENT FUNCTIONS: A SUBCLASS OF $\mathcal{M}^*$

PASCALE CHARPIN† AND GOHAR M. KYUREGHYAN‡

Abstract. Based on a computer search, Anne Canteaut conjectured that the exponent $2^{2r}+2^r+1$ in $\mathbf{F}_{2^{6r}}$ and the exponent $(2^r+1)^2$ in $\mathbf{F}_{2^{4r}}$ yield bent monomial functions. These conjectures are proved in [A. Canteaut, P. Charpin, and G. Kyureghyan, *A new class of monomial bent functions*, in Proceedings of the 2006 IEEE International Symposium on Information Theory, (ISIT 06 Seattle), IEEE Press, Piscataway, NJ, 2006, pp. 903–906] and [N. G. Leander, *IEEE Trans. Inform. Theory*, 52 (2006), pp. 738–743]. Both exponents are of binary weight 3 and define functions from the Maiorana–McFarland class $\mathcal{M}$ of bent functions to the subfield. In this paper we show that these are the only such exponents. Our proof is based on the classification of the permutation binomials $X^{2^k+2}+\nu X$ of finite fields of even characteristics. We also extend the result of Leander, determining all bent monomial functions with the exponent $(2^r+1)^2$.

Key words. cubic bent function, monomial Boolean function, permutation polynomial, Maiorana–McFarland family of bent functions

AMS subject classifications. 11T71, 11T06, 68R01

DOI. 10.1137/060677768

1. Introduction.

A bent function is a Boolean function with an even number of variables which has the maximal possible Hamming distance from the set of affine Boolean functions. More precisely, a function $f : \mathbf{F}_2^n \to \mathbf{F}_2$ (n even) is called bent if

$$\sum_{x\in\mathbf{F}_2^{2t}} (-1)^{f(x)+\langle a,x\rangle} = \pm 2^{\frac{n}{2}}$$

for any $a \in \mathbf{F}_2^n$. Observe that the bent functions are defined in a vector space over $\mathbf{F}_2$ with an inner product. Sometimes it is more convenient to consider bent functions in the finite field $\mathbf{F}_{2^n}$ with the inner product taken to be the absolute trace function. Working in the finite field can be advantageous because of its additional multiplicative structure. The classification of the bent functions in finite fields and vector spaces is completely equivalent. Let us restate the definition of a bent function in $\mathbf{F}_{2^n}$, where n is even. A function $f : \mathbf{F}_{2^n} \to \mathbf{F}_2$ is called bent if

$$\sum_{x\in\mathbf{F}_{2^n}} (-1)^{f(x)+T_1^n(\alpha x)} = \pm 2^{\frac{n}{2}}$$

for any $\alpha \in \mathbf{F}_{2^n}$, where T_1^n is the absolute trace over $\mathbf{F}_{2^n}$.

Several recent papers are devoted to the study of bent functions which are *monomial*, i.e., which are of the form

$$x \in \mathbf{F}_{2^n} \longmapsto f(x) = T_1^n(\lambda x^d) \quad \text{for some} \quad \lambda \in \mathbf{F}_{2^n},$$

*Received by the editors December 15, 2006; accepted for publication (in revised form) September 4, 2007; published electronically March 28, 2008. An extended abstract of this paper was published in the proceedings of the workshop "Algebraic and Combinatorial Coding Theory-10," Zvenigorod, Russia, Moscow, IITP RAS, 2006, pp. 52–55.

http://www.siam.org/journals/sidma/22-2/67776.html

†INRIA projet CODES, B.P. 105, 78153 Le Chesnay Cedex, France (Pascale.Charpin@inria.fr).

‡Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätplatz 2, 39106 Magdeburg, Germany (Gohar.Kyureghyan@Mathematik.Uni-Magdeburg.de).

where d is said to be the *exponent of* f. One of the goals in this research is to find exponents d and the field elements λ defining a bent function. Also, some properties of bent functions are observed by studying monomial ones. For instance, the only known so-called nonnormal bent functions are constructed with monomial bent functions [3]. A further example is

$$\{\ f_\lambda\ :\ \mathbf{F}_{2^{6r}} \to \mathbf{F}_2 \mid f_\lambda(x) = T_1^{6r}(\lambda x^{2^{2r}+2^r+1}),\ \lambda \in \mathbf{F}_{2^{3r}}^* \text{ and } T_r^{3r}(\lambda) = 0\ \},$$

which is closed under the addition of different elements and consists of bent functions of degree 3 (see [1, 2]). To our knowledge, this is the first example of such a family of nonquadratic bent functions.

Based on a computer search carried out for $n \le 24$, Anne Canteaut conjectured that the exponent $2^{2r} + 2^r + 1$ in $\mathbf{F}_{2^{6r}}$ and the exponent $2^{2r} + 2^{r+1} + 1$ in $\mathbf{F}_{2^{4r}}$ yield bent monomial functions. These conjectures are proved in [1, 10]. Both exponents are of binary weight 3 and define bent functions from the Maiorana–McFarland class $\mathcal{M}$ of bent functions. More precisely, the obtained bent functions are concatenations of affine Boolean functions of the subfield $\mathbf{F}_{2^{\frac{n}{2}}}$ or shifts of such functions. Using the techniques introduced in [1], this paper continues the study of cubic monomial functions. After introducing some preliminary definitions and results in section 2, in section 3 the cubic monomial functions, which can be represented as a concatenation of affine Boolean functions of the subfield $\mathbf{F}_{2^{\frac{n}{2}}}$, are classified. Furthermore, it is shown that among these functions only the ones with the exponents $2^{\frac{n}{2}+2^j+1}$ may define new bent functions. In section 4 the Walsh spectrum of the corresponding monomial functions are studied. It is shown that only exponent $2^{2r} + 2^{r+1} + 1$ for $n = 4r$ of that type defines a bent function. This uses the classification of all permutation polynomials $X^{2^k+2}+\nu X$ over a finite field of even characteristics obtained in section 5. Finally, the result of [10] is extended by determining all bent monomial functions with the exponent $2^{2r} + 2^{r+1} + 1$. In particular, all presently known (found by computer search) monomial bent functions are proved to belong to an infinite family of bent monomial functions. These families are as follows:

- $d = 2^i + 1$ and $\lambda \notin \{y^d | y \in \mathbb{F}_{2^n}\}$ (folklore).
- $d = (2^{\frac{n}{2}} - 1)\ell,\ \gcd(\ell, 2^{\frac{n}{2}} + 1) = 1$, and λ corresponds to a zero of the Kloosterman sum (Dillon [6], Lachaud and Wolfmann [9]).
- If n is not a multiple of 3 and $(i, n) = 1$, then $d = 2^{2i} - 2^i + 1$ and $\lambda \notin \{y^3 | y \in \mathbb{F}_{2^n}\}$ (Dillon and Dobbertin [7]).
- If $n = 4r$ and r is odd, then $d = 2^{2r} + 2^{r+1} + 1$ (Leander [10]) and $\lambda = \lambda' a^{2^{2r}+2^{r+1}+1}$, where $\lambda' \in \omega\mathbf{F}_{2^r},\ \omega \in \mathbf{F}_4 \setminus \mathbf{F}_2$, and $a \in \mathbf{F}_{2^{4r}}$ (this paper).
- If $n = 6r$, then $d = 2^{2r} + 2^r + 1$ and $\lambda = \lambda' a^{2^{2r}+2^r+1}$, where $a \in \mathbf{F}_{2^{6r}}$ and $\lambda' \in \mathbf{F}_{2^{3r}}$ such that $T_r^{3r}(\lambda') = 0$ (Canteaut, Charpin, and Kyureghyan [1]).

2. Preliminaries. Let $\mathbf{F}_{2^n}$ be the finite field with 2^n elements. If $n = ms$, then T_m^n is the trace function from $\mathbf{F}_{2^n}$ onto $\mathbf{F}_{2^m}$ given by

$$T_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(s-1)}} \quad \text{for any} \quad x \in \mathbf{F}_{2^n}.$$

Note that T_m^n is an $\mathbf{F}_{2^m}$-linear function.

2.1. Boolean functions. Boolean functions on $\mathbf{F}_{2^n}$ are given by $T_1^n(p(x))$, where $p(x)$ is a polynomial over $\mathbf{F}_{2^n}$. Further, we will use the notation

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)}$$

for a given Boolean function f. The weight of f, denoted $wt(f)$, is the number of x such that $f(x) = 1$ and it holds that

$$\mathcal{F}(f) = 2^n - 2wt(f).$$

Recall that f is said to be *balanced* when $wt(f) = 2^{n-1}$ or, equivalently, $\mathcal{F}(f) = 0$. For a given $u \in \mathbf{F}_{2^n}$, a linear Boolean function φ_u is defined by

$$\varphi_u(x) = T_1^n(ux) \quad \text{for any} \quad x \in \mathbf{F}_{2^n},$$

and every linear Boolean function is of such form. The *Walsh spectrum* of f is the multiset

$$\{\ \mathcal{F}(f + \varphi_u) \mid u \in \mathbf{F}_{2^n}\ \}.$$

Thus a Boolean function is bent if and only if its Walsh spectrum contains only values $\pm 2^{n/2}$. In particular, the weight of a bent function is $2^{n-1} \pm 2^{\frac{n-2}{2}}$.

2.2. The Maiorana–McFarland bent functions. The Maiorana–McFarland class of bent functions was introduced in [12] and extensively studied by Dillon [6, pp. 90–95]. It is usually called the *class* $\mathcal{M}$ of bent functions. The Maiorana–McFarland bent functions on $\mathbf{F}_{2^n}$, $n = 2t$, are the concatenation of 2^t different affine functions, defined on some fixed subspace of dimension t of $\mathbf{F}_{2^{2t}}$. We are interested in the subclass of $\mathcal{M}$, where the fixed subspace is the subfield $\mathbf{F}_{2^t}$. This subclass we denote by $\mathcal{M}(\mathbf{F}_{2^t})$ and define more accurately in Corollary 2.2.

PROPOSITION 2.1. *Let W be a subspace of $\mathbf{F}_{2^{2t}}$ such that $\mathbf{F}_{2^{2t}} = \mathbf{F}_{2^t} \oplus W$. Assume that a Boolean function $f : \mathbf{F}_{2^{2t}} \to \mathbf{F}_2$ can be expressed in the form*

$$f(x) = f(y + a) = T_1^t\left(y\pi(a) + h(a)\right), \tag{2.1}$$

where $x = y + a$, with $y \in \mathbf{F}_{2^t}$ and $a \in W$, and $\pi, h : W \to \mathbf{F}_{2^t}$. Let us define, for any $u \in \mathbf{F}_{2^{2t}}$,

$$W_u = \{\ a \in W \mid \pi(a) = u + u^{2^t}\ \}.$$

Then

$$\mathcal{F}(f + \varphi_u) = \begin{cases} 0 & \text{if } W_u = \emptyset \\ 2^t \sum_{a \in W_u} (-1)^{T_1^t(h(a) + T_t^{2t}(ua))} & \text{otherwise.} \end{cases}$$

Proof. For any $u \in \mathbf{F}_{2^{2t}}$ it holds that

$$\begin{aligned} \mathcal{F}(f + \varphi_u) &= \sum_{x \in \mathbf{F}_{2^{2t}}} (-1)^{f(x) + T_1^{2t}(ux)} \\ &= \sum_{a \in W} \sum_{y \in \mathbf{F}_{2^t}} (-1)^{f(y+a) + T_1^{2t}(u(y+a))} \\ &= \sum_{a \in W} \sum_{y \in \mathbf{F}_{2^t}} (-1)^{T_1^t\left(y\pi(a) + h(a) + T_t^{2t}(u(y+a))\right)} \\ &= \sum_{a \in W} \left((-1)^{T_1^t\left(h(a) + T_t^{2t}(ua)\right)} \sum_{y \in \mathbf{F}_{2^t}} (-1)^{T_1^t\left(y(\pi(a) + T_t^{2t}(u))\right)}\right). \end{aligned}$$

The second sum over $\mathbf{F}_{2^t}$ is 0 unless $\pi(a) = u + u^{2^t}$; in this case it is equal to 2^t. Thus, this sum is 0 for all a if and only if W_u is empty. Otherwise we get

$$\mathcal{F}(f + \varphi_u) = 2^t \sum_{a \in W_u} (-1)^{T_1^t(h(a)+ua+(ua)^{2^t})},$$

completing the proof. ∎

COROLLARY 2.2. *Let $W \subset \mathbf{F}_{2^{2t}}$ be such that $\mathbf{F}_{2^{2t}} = \mathbf{F}_{2^t} \oplus W$. Assume that a Boolean function $f : \mathbf{F}_{2^{2t}} \to \mathbf{F}_2$ can be expressed in the form*

$$f(x) = f(y + a) = T_1^t\left(y\pi(a) + h(a)\right),$$

where $x = y + a$, with $y \in \mathbf{F}_{2^t}$ and $a \in W$, and $\pi, h : W \to \mathbf{F}_{2^t}$. Then f is bent if and only if π is bijective. Such functions are said to be the elements of the subclass $\mathcal{M}(\mathbf{F}_{2^t})$ of $\mathcal{M}$.

Proof. Suppose that π is not a permutation. Then there is an element $b \in \mathbf{F}_{2^t}$ such that $\pi(a) \neq b$ for any $a \in W$. For every $u \in \mathbf{F}_{2^{2t}}$ with $u + u^{2^t} = b$ it holds that $W_u = \emptyset$, and thus Proposition 2.1 implies $\mathcal{F}(f + \varphi_u) = 0$, proving the necessity of the condition. To derive the sufficiency, note that in the case of bijective π the cardinality of W_u equals 1 for any $u \in \mathbf{F}_{2^{2t}}$. ∎

3. Decomposable cubic monomial Boolean functions. In [1], it is shown that the monomial Boolean functions on $\mathbf{F}_{2^n}$ defined by the new bent exponents $2^{2r} + 2^r + 1$ (for $n = 6r$) and $(2^r + 1)^2$ (for $n = 4r$), can be decomposed in form (2.1). In this section we describe all cubic monomial Boolean functions possessing such a decomposition.

Let $0 \leq k \leq 2^n - 2$. We denote by C_k the cyclotomic coset modulo $2^n - 1$ containing k, i.e.,

$$C_k = \{k, 2k, \ldots, 2^{n-1}k\} \pmod{2^n - 1}.$$

Recall that if $|C_k| = l$, then $\{x^k : x \in \mathbf{F}_{2^n}\} \subset \mathbf{F}_{2^l}$ and $\mathbf{F}_{2^l}$ is the smallest subfield of $\mathbf{F}_{2^n}$ with this property.

Let $d = 2^i + 2^j + 1$ and $\lambda \in \mathbf{F}_{2^{2t}}$. We consider the function $f : x \mapsto T_1^{2t}(\lambda x^d)$ on $\mathbf{F}_{2^{2t}}$. Taking the smallest representative of C_d, we may assume that

$$d = 2^i + 2^j + 1 \text{ with } 0 < j < t,\ i - j < t \text{ and } j < i. \tag{3.1}$$

If $\mathbf{F}_{2^{2t}} = \mathbf{F}_{2^t} \oplus W$, then setting $x = y + a$ ($y \in \mathbf{F}_{2^t}$ and $a \in W$), we have

$$\begin{aligned} T_1^{2t}(\lambda x^d) &= T_1^{2t}\left(\lambda(y+a)^{2^i+2^j+1}\right) \\ &= T_1^{2t}\left(\lambda y^{2^i+2^j+1}\right) \\ &\quad + T_1^{2t}\left(\lambda a^{2^i} y^{2^j+1} + \lambda a^{2^j} y^{2^i+1} + \lambda a y^{2^i+2^j}\right) \\ &\quad + T_1^{2t}\left(\lambda y^{2^i} a^{2^j+1} + \lambda y^{2^j} a^{2^i+1} + \lambda y a^{2^i+2^j}\right) \\ &\quad + T_1^{2t}\left(\lambda a^{2^i+2^j+1}\right). \end{aligned}$$

Using the transitivity of the trace function we get that $T_1^{2t}(\lambda x^d)$ is equal to the

following sum:

$$T_1^t\left(T_t^{2t}(\lambda)y^{2^i+2^j+1}\right) \tag{3.2}$$

$$\begin{aligned} &+\ T_1^t\left(T_t^{2t}(\lambda a^{2^i})y^{2^j+1}+T_t^{2t}(\lambda a^{2^j})y^{2^i+1}+T_t^{2t}(\lambda a)y^{2^i+2^j}\right)\\ &+\ T_1^t\left(T_t^{2t}(\lambda a^{2^j+1})y^{2^i}+T_t^{2t}(\lambda a^{2^i+1})y^{2^j}+T_t^{2t}(\lambda a^{2^i+2^j})y\right)\\ &+\ T_1^{2t}\left(\lambda a^{2^i+2^j+1}\right). \end{aligned} \tag{3.3}$$

Our goal is to describe the set of pairs (i,j) defining a function $T_1^{2t}(\lambda x^{2^i+2^j+1})$ of form (2.1). Equivalently, we are going to find i,j, and λ such that (3.2) and (3.3) are constant or linear on y for any $a\in W$. The following easy result will be used several times in what follows. We present a brief proof of it for the convenience of the reader.

LEMMA 3.1. *Consider the function on $\mathbf{F}_{2^n}$ given by $f(x)=T_1^n(\delta x^d)$, $\delta\in\mathbf{F}_{2^n}^*$. Assume that d is the smallest element of its cyclotomic coset.*

(a) *Let $d=2^i+2^j+1$. Then the function f is constantly c, $c\in\mathbf{F}_2$, if and only if $c=0$ and*

$$n=3\ell,\quad d=2^{2\ell}+2^\ell+1,\quad \text{and}\quad \delta+\delta^{2^\ell}+\delta^{2^{2\ell}}=0.$$

(b) *Let $d=2^i+1$. Then the function f is constantly c, $c\in\mathbf{F}_2$, if and only if $c=0$ and*

$$n=2\ell,\quad i=\ell\quad \text{and}\quad \delta\in\mathbf{F}_{2^\ell}.$$

Proof. Assume that $f(x)=c$ for all x. Then $c=0$ since $f(0)=0$. So the polynomial

$$T_1^n(\delta x^d)=\delta x^d+(\delta x^d)^2+\cdots+(\delta x^d)^{2^{n-1}}$$

is the null polynomial since it has degree less than 2^n. Hence the cyclotomic coset C_d has cardinality ℓ with $\ell<n$ and $n=k\ell$. Then $\{x^k : x\in\mathbf{F}_{2^n}\}\subset\mathbf{F}_{2^l}$ and we have

$$T_1^n(\delta x^d)=T_1^l(x^dT_l^n(\delta)).$$

To complete the proof we find the exponents d of binary weights 3 and 2 satisfying $2^ld\equiv d \pmod{2^n-1}$.

(a) $2^\ell(2^i+2^j+1)\equiv 2^i+2^j+1 \pmod{2^n-1}$ if and only if $n-i=i-j=j=\ell$. Thus $n=3\ell$, $i=2\ell$, and $j=\ell$. In this case, to have $T_1^n(\delta x^d)$ constantly zero it must also hold that $\delta+\delta^{2^\ell}+\delta^{2^{2\ell}}=0$.

(b) $2^\ell(2^i+1)=2^i+1$ if and only if $n-i=i=\ell$. Then $n=2\ell$ and, moreover, $\delta+\delta^{2^\ell}=0$. ∎

We will also need the following observation.

LEMMA 3.2. *Let $n=6j$ and $d=2^{4j}+2^{2j}+1$. Let f_λ be the function on $\mathbf{F}_{2^n}$ defined by $f_\lambda(x)=T_1^n(\lambda x^d)$, $\lambda\in\mathbf{F}_{2^n}$. Then, f_λ is the null function when $T_{2j}^{6j}(\lambda)=0$. Otherwise the weight of f_λ is equal to $2^{2j-1}(2^{4j}+2^{2j}+1)$. In particular, f_λ cannot be bent.*

Proof. Recall that the weight of f_λ, say $wt(f_\lambda)$, is the number of x such that $f_\lambda(x)=1$. Since $(2^{2j}-1)d=2^{6j}-1$, the image set of $x\mapsto x^d$ is equal to $\mathbf{F}_{2^{2j}}$ and every nonzero element from $\mathbf{F}_{2^{2j}}$ has $2^{4j}+2^{2j}+1$ many preimages. Using

$$T_1^{6j}(\lambda x^{2^{4j}+2^{2j}+1})=T_1^{2j}\left(T_{2j}^{6j}(\lambda)x^{2^{4j}+2^{2j}+1}\right)$$

it is clear that $wt(f_\lambda) = 0$ when λ satisfies $T_{2^j}^{6j}(\lambda) = 0$ (see also Lemma 3.1). Otherwise

$$wt(f_\lambda) = (2^{4j} + 2^{2j} + 1)\#\{\ y \in \mathbf{F}_{2^{2j}} \mid T_1^{2j}(T_{2^j}^{6j}(\lambda)y) = 1\ \},$$

where $\#B$ denotes the cardinality of a set B. So we get $wt(f_\lambda) = 2^{2j-1}d$. The weights 0 and $2^{2j-1}d$ both do not correspond to a weight of a bent function, completing the proof. □

THEOREM 3.3. *Let $n = 2t$ and $d = 2^i + 2^j + 1$, where d satisfies (3.1). Given $\lambda \in \mathbf{F}_{2^n}^*$, let us define*

$$f_\lambda \ :\ x \in \mathbf{F}_{2^n} \mapsto T_1^n(\lambda x^d).$$

Then f_λ can be represented in the form (2.1) exactly in one of the following cases:

(i) *The trivial case: $n = 6j$ and $d = 2^{4j} + 2^{2j} + 1$ with $\lambda + \lambda^{2^{2j}} + \lambda^{2^{4j}} = 0$—in this case f_λ is the null function;*
(ii) *$n = 6j$ and $d = 2^{2j} + 2^j + 1$ with $\lambda \in \mathbf{F}_{2^{3j}}$ satisfying $\lambda + \lambda^{2^j} + \lambda^{2^{2j}} = 0$;*
(iii) *$d = 2^t + 2^j + 1$ with $\lambda \in \mathbf{F}_{2^t}$.*

Proof. The function f_λ can be represented in the form (2.1) if and only if the sum of the summands in (3.2) and (3.3) is either constant or linear on y. Note that since $y \in \mathbf{F}_{2^t}$ we are interested in the behavior of $d \pmod{2^t - 1}$.

Let us consider (3.2). We want to determine d such that $c(y) = T_1^t(T_t^{2t}(\lambda)y^d)$ is of degree strictly less than 3. Because of the conditions on i, j, if $c(y)$ is not constantly zero, then i must be equal to t. We will consider the cases $i = t$ and $i \neq t$ separately.

Let $d = 2^t + 2^j + 1$. Then the sum of terms in (3.2) and (3.3) becomes

$$g(y) = T_1^t\left(T_t^{2t}(\lambda)y^{2^j+2}\right) + T_1^t\left(T_t^{2t}(\lambda)(a^{2^t} + a)y^{2^j+1} + T_t^{2t}(\lambda a^{2^j})y^2\right).$$

Suppose that $\lambda \notin \mathbf{F}_{2^t}$. So the function g is of degree 2. Indeed, the integer $2^j + 1$ cannot be a power of 2 and it is not in the cyclotomic coset (modulo $2^t - 1$) of $2^j + 2$. We must have

$$T_1^t\left(T_t^{2t}(\lambda)(a^{2^t} + a)y^{2^j+1}\right) = 0, \tag{3.4}$$

for any $a \in W$, where $j < t$. By Lemma 3.1(b), (3.4) holds if and only if

$$t = 2\ell,\ j = \ell \ \text{ and } \ T_t^{2t}(\lambda)T_t^{2t}(a) \in \mathbf{F}_{2^\ell}.$$

But this last condition cannot hold for any $a \in W$, since the map $a \mapsto T_t^{2t}(a)$, from W to $\mathbf{F}_{2^t}$, is bijective. We conclude that we must have $T_t^{2t}(\lambda) = 0$. In this case, we get $g(y) = T_1^t(T_t^{2t}(\lambda a^{2^j})y^2)$, which proves case (iii).

Let $d = 2^i + 2^j + 1$ with $i \neq t$. Set $d' = d \pmod{2^t - 1}$, $0 < d' < 2^t - 1$. In this case $c(y)$ must be constantly zero, and thus applying Lemma 3.1(a), we get

$$t = 3k, \quad d' = 2^{2k} + 2^k + 1 \quad \text{and} \quad T_{3k}^{6k}(\lambda + \lambda^{2^k} + \lambda^{2^{2k}}) = T_k^{6k}(\lambda) = 0.$$

Hence there are two possibilities for d: either $d = d'$ or $d = 2^{4k} + 2^{2k} + 1$. Suppose $d = d'$. Then the sum in (3.3) is as follows:

$$\begin{aligned} &T_1^{3k}\left(T_{3k}^{6k}(\lambda a^{2^{2k}})y^{2^k+1} + T_{3k}^{6k}(\lambda a^{2^k})y^{2^{2k}(2^k+1)} + T_{3k}^{6k}(\lambda a)y^{2^k(2^k+1)}\right) \\ &\quad = T_1^{3k}\left(T_{3k}^{6k}((\lambda + \lambda^{2^k} + \lambda^{2^{2k}})a^{2^{2k}})y^{2^k+1}\right) \\ &\quad = T_1^{3k}\left((\lambda + \lambda^{2^k} + \lambda^{2^{2k}})T_{3k}^{6k}(a^{2^{2k}})y^{2^k+1}\right), \end{aligned}$$

where the last equality follows from previously obtained condition $T_k^{6k}(\lambda)=0$. Lemma 3.1(b), implies that $\lambda+\lambda^{2^k}+\lambda^{2^{2k}}=0$, which is possible only for $\lambda\in\mathbf{F}_{2^{3k}}$, because the polynomial $X+X^{2^k}+X^{2^{2k}}$ divides $X^{2^{3k}}+X$. Hence we have proved case (ii).

The last possibility is $d=2^{4k}+2^{2k}+1$. We apply Lemma 3.2. If f_λ is not the null function, then $\mathcal{F}(f_\lambda)=2^n-2^{2j}d$. Since $\mathcal{F}(f_\lambda)$ is not divisible by 2^{3j}, we deduce from Proposition 2.1 that f_λ cannot be represented in the form (2.1). Hence we obtain the trivial case (i). ∎

Further, we want to see when the decomposable cubic monomial functions are bent. We have seen that the exponent $d=2^{4j}+2^{2j}+1$ does not lead to a bent monomial function. The bent monomial functions with the exponent $2^{2j}+2^j+1$ are studied in [1], where the following result is proved.

THEOREM 3.4 (see [1]). *The monomial function $T_1^{6r}(\lambda' x^{2^{2r}+2^r+1})$ in $\mathbf{F}_{2^{6r}}$ is bent if and only if there are $\lambda\in\mathbf{F}_{2^{3r}}$ and $a\in\mathbf{F}_{2^{6r}}$ such that $T_r^{3r}(\lambda)=0$ and $\lambda'=\lambda a^{2^{2r}+2^r+1}$. Moreover, all these bent functions are from the Maiorana–McFarland class.*

By Theorem 3.3 only the exponents 2^t+2^j+1 may provide further examples of cubic monomial bent functions from $\mathcal{M}(\mathbf{F}_{2^t})$. The rest of this paper is devoted to the study of this exponent.

4. Exponent 2^t+2^j+1. In the study of the Walsh spectrum of the monomial functions with exponents 2^t+2^j+1, we may restrict ourselves to the elements λ from the subfield $\mathbf{F}_{2^t}$. This is a consequence of the following observation.

LEMMA 4.1. *Let b be such that $\gcd(b,2^t+1)=1$. Then, for any $\mu\in\mathbf{F}_{2^{2t}}$, there are $\lambda\in\mathbf{F}_{2^t}$ and $\delta\in\mathbf{F}_{2^{2t}}$ such that $\mu=\lambda\delta^b$. Consequently, the Walsh spectrum of the monomial function $T_1^{2t}(\mu x^b)$ is the same as the one of $T_1^{2t}(\lambda x^b)$.*

Proof. Let α be a primitive element of $\mathbf{F}_{2^{2t}}$. Since $\gcd(2^t-1,2^t+1)=1$, any element $\mu\in\mathbf{F}_{2^{2t}}^*$ can be expressed as follows:

$$\mu=\alpha^{\ell(2^t-1)}\alpha^{k(2^t+1)},\quad 0\le\ell\le 2^t,\quad 0\le\ell\le 2^t-2.$$

Since b and 2^t+1 are coprime, it holds that $\mu=\lambda\delta^b$ with $\lambda=\alpha^{k(2^t+1)}$ and $\delta^b=\alpha^{\ell(2^t-1)}$. ∎

The next proposition gives the explicit decomposition of the function

$$g_\lambda(x)=T_1^{2t}\left(\lambda x^{2^t+2^j+1}\right),\quad 0<j<t,\quad \lambda\in\mathbf{F}_{2^t}^*. \tag{4.1}$$

PROPOSITION 4.2. *Let $W\subset\mathbf{F}_{2^{2t}}$ be such that $\mathbf{F}_{2^{2t}}=\mathbf{F}_{2^t}\oplus W$. Then the function g_λ defined in (4.1) can be written as follows:*

$$g_\lambda(y,a)=T_1^t\left(y\pi(a)+h(a)\right),\quad y\in\mathbf{F}_{2^t},\quad a\in W,$$

where $\pi,h:W\to\mathbf{F}_{2^t}$ are given by

$$\pi(a)=\lambda^{2^{t-1}}(a+a^{2^t})^{2^{j-1}}+\lambda(a^{2^t}+a)^{2^j+1}$$

and

$$h(a)=\lambda a^{2^t+1}(a+a^{2^t})^{2^j}.$$

Proof. For any $y\in\mathbf{F}_{2^t}$ and $a\in W$, we compute

$$g_\lambda(y,a)=g_\lambda(y+a)=T_1^{2t}\left(\lambda(y+a)^d\right).$$

We have $T_1^{2t}(\lambda y^d) = 0$ since λ and y are in $\mathbf{F}_{2^t}$. The part which is (a priori) quadratic relative to y is

$$\begin{aligned} B &= T_1^{2t}\left(\lambda(y^{1+2^j}a + y^{2^j+1}a^{2^t} + y^2a^{2^j})\right) \\ &= T_1^{2t}\left(\lambda y^{2^j+1}(a^{2^t}+a) + \lambda y^2 a^{2^j}\right) \\ &= T_1^{2t}(\lambda y^2 a^{2^j}) = T_1^t(\lambda y^2(a+a^{2^t})^{2^j}), \end{aligned}$$

since $\lambda y^{2^j+1}(a^{2^t}+a) \in \mathbf{F}_{2^t}$. Further, we compute the part which is linear relative to y:

$$\begin{aligned} C &= T_1^{2t}\left(y(\lambda(a^{2^t+2^j}+a^{2^j+1}) + \lambda^{2^{t-j}}a^{2^{t-j}(2^t+1)})\right) \\ &= T_1^{2t}\left(y\lambda(a^{2^t+2^j}+a^{2^j+1})\right) \\ &= T_1^t\left(y\lambda(a^{2^t}+a)^{2^j+1}\right), \end{aligned}$$

since $\lambda^{2^{t-j}}a^{2^{t-j}(2^t+1)} \in \mathbf{F}_{2^t}$. Finally,

$$g_\lambda(y,a) = T_1^t\left(y(\lambda^{2^{t-1}}(a+a^{2^t})^{2^{j-1}} + \lambda(a^{2^t}+a)^{2^j+1})\right) + T_1^{2t}(\lambda a^d).$$

So, we have $g_\lambda(y,a) = T_1^t(y\pi(a) + h(a))$, where $\pi(a)$ is the coefficient of y above and

$$h(a) = \lambda T_t^{2t}(a^d) = \lambda a^{2^t+1}(a+a^{2^t})^{2^j},$$

since $d = 2^t + 2^j + 1$ and $2^t d \equiv 1 + 2^t + 2^{t+j}$. □

The obtained decomposition allows us to get some information on the Walsh spectrum of g_λ in general. By Proposition 2.1 we obtain

$$\mathcal{F}(g_\lambda + \varphi_u) = 2^t \sum_{a \in W_u} (-1)^{T_1^t(h(a)+T_t^{2t}(ua))}, \tag{4.2}$$

where $W_u = \{\ a \in W \mid \pi(a) = u + u^{2^t}\ \}$ and, by convention, the sum above is null if $W_u = \emptyset$. Note that

$$W_u = W_{u+\beta} \quad \text{for all } \beta \in \mathbf{F}_{2^t}.$$

Recall that g_λ is bent if and only if π is a permutation (see Corollary 2.2).

As a direct consequence of (4.2) we get a lower bound on the multiplicity of the value 0 in the Walsh spectrum of g_λ. This is because $W_u = \emptyset$ when $u + u^{2^t}$ is not in the image of π.

PROPOSITION 4.3. *Let I be the cardinality of the image of π in $\mathbf{F}_{2^t}$. Then*

$$\#\{\ v \in \mathbf{F}_{2^{2t}} \mid \mathcal{F}(g_\lambda + \varphi_v) = 0\ \} \geq 2^t(2^t - I).$$

Equation (4.2) gives also an upper bound on the magnitude of the value of Walsh transform at u in terms of the cardinality of W_u.

PROPOSITION 4.4. *For any u, $\mathcal{F}(g_\lambda + \varphi_u) \equiv 0 \pmod{2^t}$. Moreover,*

$$|\mathcal{F}(g_\lambda + \varphi_u)| \leq 2^t \times \#W_u.$$

As we have seen, the Walsh spectrum of g_λ could be determined as soon as we know the set W_u, which describes the preimages of the mapping $\pi : W \to \mathbf{F}_{2^t}$. Recall that

$$\pi(a) = \lambda^{2^{t-1}}(a + a^{2^t})^{2^{j-1}} + \lambda(a^{2^t} + a)^{2^j+1}.$$

Since the mapping $a \mapsto a + a^{2^t}$ is a permutation from W to $\mathbf{F}_{2^t}$, we have $\pi(a) = \pi'(a + a^t)$, where $\pi' : \mathbf{F}_{2^t} \to \mathbf{F}_{2^t}$ is given by

$$\pi'(y) = \lambda^{2^{t-1}} y^{2^{j-1}} + \lambda y^{2^j+1}, \quad y \in \mathbf{F}_{2^t}. \tag{4.3}$$

Hence our problem is linked with the one of determining the image of π' or, equivalently, of $(\pi')^2$.

PROBLEM 1. *Let $\lambda \in \mathbf{F}_{2^t}$. For any $\tau \in \mathbf{F}_{2^t}$, compute the number of $y \in \mathbf{F}_{2^t}$ such that*

$$\lambda^2 y^{2(2^j+1)} + \lambda y^{2^j} + \tau = 0.$$

This problem can be easily solved for $\tau = 0$, which yields information on $\mathcal{F}(g_\lambda + \varphi_u)$ for $u \in \mathbf{F}_{2^t}$ as in subsection 4.1 shown. Subsection 4.2 is devoted to the characterization of λ and j such that the equation of Problem 1 has exactly one solution.

4.1. The case $u \in \mathbf{F}_{2^t}$. Let $u \in \mathbf{F}_{2^t}$. Then $W_u = \{\, a \in W \mid \pi(a) = 0 \,\}$ and $W_u = W_{u'}$ for all $u' \in \mathbf{F}_{2^t}$. Clearly, $\pi'(0) = 0$, where π' is given by (4.3). For nonzero y, it holds that

$$\pi'(y) = 0 \quad \Leftrightarrow \quad y^{2^{j-1}+1} = \lambda^{2^{t-1}-1} \quad \Leftrightarrow \quad y^{2^j+2} = \frac{1}{\lambda}.$$

Thus, for any $u \in \mathbf{F}_{2^t}$,

$$W_u = \left\{ a \in W \mid a = 0 \text{ or } (a + a^{2^t})^{2^j+2} = \frac{1}{\lambda} \right\}. \tag{4.4}$$

LEMMA 4.5. *Let $u \in \mathbf{F}_{2^t}$. Then the constant term of g_λ, given by*

$$h(a) = \lambda a^{2^t+1}(a + a^{2^t})^{2^j},$$

satisfies $T_1^t(h(a)) = 1$ for any nonzero $a \in W_u$.

Proof. Note that $h(0) = 0$ and assume now that $a \neq 0$. Using (4.4), we have $(a + a^{2^t})^{2^j+2} = \lambda^{-1}$. By replacing $(a + a^{2^t})^{2^j}$ in $h(a)$, we get

$$h(a) = \lambda a^{2^t+1}\lambda^{-1}(a + a^{2^t})^{-2} = \frac{a^{2^t+1}}{(a + a^{2^t})^2}.$$

The elements a and a^{2^t} are the solutions in $\mathbf{F}_{2^{2t}}$ of the equation

$$x^2 + (a + a^{2^t})x + a^{2^t+1} = 0,$$

while they do not belong to $\mathbf{F}_{2^t}$. This implies that the polynomial $X^2 + (a + a^{2^t})X + a^{2^t+1} \in \mathbf{F}_{2^t}[X]$ is irreducible over $\mathbf{F}_{2^t}$. Hence

$$T_1^t\left(\frac{a^{2^t+1}}{(a + a^{2^t})^2}\right) = T_1^t(h(a)) = 1. \qquad \square$$

Now we can describe the values $\mathcal{F}(g_\lambda + \varphi_u)$ for $u \in \mathbf{F}_{2^t}$ more precisely. Notably, we compute the weight of each function g_λ.

PROPOSITION 4.6. *Let $u \in \mathbf{F}_{2^t}$ and W_u be given by (4.4). Set $s = \gcd(2^{j-1}+1, 2^t-1)$. Then we have the following:*

(i) *If $s = 1$ (i.e., $t/\gcd(j-1,t)$ odd) then $\#W_u = 2$ and*

$$\mathcal{F}(g_\lambda + \varphi_u) = \begin{cases} 0 & \text{if } T_1^t(u(a+a^{2^t})) = 0, \\ 2^{t+1} & \text{if } T_1^t(u(a+a^{2^t})) = 1, \end{cases}$$

where a is the unique element of W_u different from 0. Note that each value above occurs 2^{t-1} times. In particular, $\mathcal{F}(g_\lambda) = 0$.

(ii) *Set $S_s = \{u^s | u \in \mathbf{F}_{2^t}\}$. For $s > 1$ we have that*
- *if $\lambda \notin S_s$, then $\mathcal{F}(g_\lambda + \varphi_u) = 2^t$ for any u.*
- *if $\lambda \in S_s$, then $|\mathcal{F}(g_\lambda + \varphi_u)| \le (s+1)2^t$. In particular, $\mathcal{F}(g_\lambda) = (1-s)2^t$.*

Consequently, if g_λ is bent then $s > 1$ and $\lambda \notin S_s$.

Proof. According to (4.4), we get from (4.2) and Lemma 4.5 that

$$\begin{aligned} \mathcal{F}(g_\lambda + \varphi_u) &= 2^t \sum_{a \in W_u} (-1)^{T_1^t(h(a)+u(a+a^{2^t}))} \\ &= 2^t - 2^t \sum_{a \in W_u, a \neq 0} (-1)^{T_1^t(u(a+a^{2^t}))}. \end{aligned}$$

(i) When $s = 1$ then W_u contains only 0 and a unique a such that $(a+a^{2^t})^{2^j+2} = \lambda^{-1}$. Consequently, $\mathcal{F}(g_\lambda + \varphi_u) = 0$ or 2^{t+1} depending on whether $T_1^t(u(a + a^{2^t})) = 0$ or 1. Since u runs through $\mathbf{F}_{2^t}$, each such case occurs 2^{t-1} times. In particular, for $u = 0$, we get $\mathcal{F}(g_\lambda) = 0$.

(ii) Now assume that $s > 1$. If $\lambda \notin S_s$, then $W_u = \{0\}$, implying $\mathcal{F}(g_\lambda + \varphi_u) = 2^t$ for any u.

Denote by G_s the subgroup of $\mathbf{F}_{2^t}^*$ of order s. If $\lambda \in S_s$, then

$$W_u = \{0\} \cup \{\ a \in W \mid a + a^{2^t} \in yG_s \ \text{ with } \ y^{2^j+2} = \lambda^{-1}\ \}$$

(where $y \in \mathbf{F}_{2^t}$). Using Proposition 4.4, we conclude that $|\mathcal{F}(g_\lambda + \varphi_u)| \le (s+1)2^t$ when $\lambda \in S_s$. Finally, observe that for $u = 0$, we get $\mathcal{F}(g_\lambda) = (1-s)2^t$. ∎

4.2. The bent functions. In this section we find all j and $\mu \in \mathbf{F}_{2^{2t}}$ defining bent monomial functions $x \mapsto T_1^{2t}(\mu x^{2^t+2^j+1})$. Remember that this is equivalent to describing those $\lambda \in \mathbf{F}_{2^t}$ for which π', defined in (4.3), is a permutation. Consider

$$\begin{aligned} (\pi'(y))^2 &= \lambda y^{2^j} + \lambda^2 y^{2^{j+1}+2} \\ &= \lambda(y + \lambda^{2^{t-j}} y^{2^{t-j}(2^{j+1}+2)})^{2^j} \\ &= \lambda(y + \lambda^{2^{t-j}} y^{2^{t-j+1}+2})^{2^j} \\ &= \lambda^2(\lambda^{-2^{t-j}} y + y^{2^{t-j+1}+2})^{2^j}. \end{aligned}$$

Thus, the function g_λ is bent if and only if the mapping $\rho : \mathbf{F}_{2^t} \to \mathbf{F}_{2^t}$, given by

$$\rho(y) = y^{2^{t-j+1}+2} + \nu y,$$

where $\nu = \lambda^{-2^{t-j}}$, is a permutation. All such permutation polynomials are characterized in Theorem 5.1 of the next section. In particular, Theorem 5.1 implies the following proposition.

PROPOSITION 4.7. *Let* $g_\lambda = T_1^{2t}(\lambda x^{2^t+2^j+1})$, $0 < j < t$, $\lambda \in \mathbf{F}_{2^t}^*$. *Then,* g_λ *can be bent only if* $t = 2r$, r *odd, and* $j = r + 1$.

In [10] it is shown that the exponent $2^{2r} + 2^{r+1} + 1$ in $\mathbf{F}_{2^{4r}}$, r odd, yields a bent function if λ is chosen to be β^5, where β is the root of the polynomial $X^4 + X + 1$. Theorem 5.1 allows us to extend this result.

THEOREM 4.8. *Let* $\omega \in \mathbf{F}_4 \setminus \mathbf{F}_2$. *The monomial function* $T_1^{4r}(\mu x^{2^{2r}+2^{r+1}+1})$ *on* $\mathbf{F}_{2^{4r}}$ *is bent for some* $\mu \in \mathbf{F}_{2^{4r}}$ *if and only if* r *is odd and there are* $\lambda \in \omega\mathbf{F}_{2^r}$ *and* $a \in \mathbf{F}_{2^{4r}}$ *such that* $\mu = \lambda a^{2^{2r}+2^{r+1}+1}$.

5. On some binomial quadratic permutations in $\mathbf{F}_{2^t}$. In this section we describe all permutation polynomials of type

$$X^{2^k+2} + \nu X$$

in a finite field of characteristics 2. More precisely, we will prove the next theorem.

THEOREM 5.1. *Let* $0 \le k \le t - 1$ *and* $\nu \neq 0$. *Then the polynomial*

$$\rho(X) = X^{2^k+2} + \nu X \quad \textit{in } \mathbf{F}_{2^t}[X]$$

is a permutation polynomial of $\mathbf{F}_{2^t}$ *if and only if* t *is even and*

- *either* $k = 1$ *and* ν *is not a third power in* $\mathbf{F}_{2^t}$, *or*
- $t = 2r$, $r \ge 3$ *with* r *odd,* $k = r$, *and* $\nu \in \omega\mathbf{F}_{2^r}$, *where* $\omega \in \mathbf{F}_{2^2} \setminus \mathbf{F}_2$.

We will use some well-known facts about the quadratic monomial Boolean functions. Our main reference is [11, pp. 175–189]; we give only the idea of a proof of Proposition 5.2. The interested reader may see [8, 10] for these proofs and [5, 8] for some other properties of the quadratic monomial functions.

PROPOSITION 5.2. *Let* $\gcd(t, i) = s$ *and* $F : \mathbf{F}_{2^t} \to \mathbf{F}_{2^t}$ *be given by* $F(x) = x^{2^i+1}$. *Let* f_μ, $\mu \in \mathbf{F}_{2^t}^*$, *be the Boolean function defined by* $f_\mu(x) = T_1^t(\mu F(x))$. *Then the following properties hold:*

(a) *The function* F *is bijective if and only if* t/s *is odd.*
(b) *If* t/s *is odd, then the Walsh transform of the Boolean function* f_μ *takes the values* $\{0, \pm 2^{\frac{t+s}{2}}\}$. *In particular,* f_μ *is never bent.*
(c) *Assume that* t/s *is even. The function* f_μ *is bent if and only if* μ *is not a* $(2^i + 1)$*th power in* $\mathbf{F}_{2^t}$. *Otherwise, its Walsh transform takes the values* $\{0, \pm 2^{\frac{t+2s}{2}}\}$.

Proof. The function F is bijective if and only if $\gcd(2^i + 1, 2^t - 1) = 1$ which is equivalent to $s = \gcd(2i, t)$, i.e., t/s odd.

Set $S = \{y^{2^i+1} | y \in \mathbf{F}_{2^t}\}$. The function f_μ is bent if and only if t/s is even and $\mu \notin S$ (see [10, Thm. 2]). Otherwise the Walsh spectrum of f_μ is the same as that of the function $x \mapsto T_1^t(x^{2^i+1})$. The Walsh transform of this quadratic function takes the values

$$\begin{array}{ll} \{0, \pm 2^{\frac{t+s}{2}}\} & \text{if } t/s \text{ is odd,} \\ \{0, \pm 2^{\frac{t+2s}{2}}\} & \text{if } t/s \text{ is even and } \mu \in S. \end{array}$$

(see [11, Thm. 11.13]). ∎

Further, we need also the following property of the Walsh transform of quadratic Boolean functions.

PROPOSITION 5.3. *Let* $\gcd(t, i) = s$, t/s *be odd. Let* f *be the Boolean function on* $\mathbf{F}_{2^t}$ *defined by* $f(x) = T_1^t(x^{2^i+1} + \beta x)$. *Then* f *is balanced if and only if* $T_s^t(\beta) \neq 1$.

Proof. Note that $T_s^t(1) = 1$ since $t = su$ with odd u. Such a function f is balanced if and only if there is $a \in \mathbf{F}_{2^t}^*$ such that the derivative of f with respect to a constantly equals 1, that is,

$$h_a(x) = f(x) + f(x+a) = 1 \quad \text{for all } x$$

(see a proof in [4, Prop. II-5]). We compute the derivative of f with respect to a:

$$h_a(x) = T_1^t(ax^{2^i} + a^{2^i}x + a^{2^i+1} + \beta a) = T_1^t\left(x(a^{2^{t-i}} + a^{2^i}) + a(a^{2^i} + \beta)\right).$$

Then h_a is constant if and only if $a^{2^{2i}} = a$, i.e., $a \in \mathbf{F}_{2^s}^*$. In this case,

$$h_a(x) = T_1^t(a + \beta a) = T_1^s\left(aT_s^t(1+\beta)\right) = T_1^s\left(a(1 + T_s^t(\beta))\right).$$

So, there is $a \in \mathbf{F}_{2^s}^*$ such that $h_a = 1$ if and only if $T_s^t(\beta) \neq 1$. ∎

Now we are going to prove Theorem 5.1 by means of the two following lemmas.

LEMMA 5.4. *Let $\nu \in \mathbf{F}_{2^t}$ and $\rho : \mathbf{F}_{2^t} \to \mathbf{F}_{2^t}$ be given by the polynomial*

$$\rho(X) = X^{2^k+2} + \nu X, \quad 2 \le k \le t-1. \tag{5.1}$$

Take $c = \gcd(t, k-1)$. Then ρ is a permutation polynomial of $\mathbf{F}_{2^t}$ if and only if

$$\frac{t}{c} \text{ is odd} \quad \text{and} \quad T_c^t(\gamma^{2^k+1}\nu) \neq 1 \quad \text{for every } \gamma \in \mathbf{F}_{2^t}.$$

In this case, t is even, $\frac{t}{\gcd(t,k)}$ is even, and k is odd.

Proof. It is well known that a mapping $g : \mathbf{F}_{2^t} \to \mathbf{F}_{2^t}$ is bijective if and only if

$$\sum_{x \in \mathbf{F}_{2^t}} (-1)^{T_1^t(\beta g(x))} = 0$$

for any $\beta \in \mathbf{F}_{2^t}^*$. Consider the sum

$$S = \sum_{x \in \mathbf{F}_{2^t}} (-1)^{T_1^t(\beta x^{2^k+2} + \beta\nu x)} = \sum_{x \in \mathbf{F}_{2^t}} (-1)^{T_1^t(\beta^{2^{n-1}} x^{2^{k-1}+1} + \beta\nu x)}.$$

Suppose t/c is even; then by Proposition 5.2(c), there is a β such that the function $x \mapsto T_1^t(\beta^{2^{n-1}} x^{2^{k-1}+1})$ is bent. Clearly, $S \neq 0$ for such a β. Hence ρ defines a permutation only if t/c is odd.

We assume that t/c is odd, i.e., by Proposition 5.2(a), the mapping $x \mapsto x^{2^{k-1}+1}$ is a permutation on $\mathbf{F}_{2^t}$. Then $\beta^{2^{n-1}} = \gamma^{2^{k-1}+1}$ for some $\gamma \in \mathbf{F}_{2^t}$ and

$$\begin{aligned} S &= \sum_{x \in \mathbf{F}_{2^t}} (-1)^{T_1^t((\gamma x)^{2^{k-1}+1} + \gamma^{2^k+2}\nu x)} \\ &= \sum_{z \in \mathbf{F}_{2^t}} (-1)^{T_1^t(z^{2^{k-1}+1} + \gamma^{2^k+1}\nu z)}, \end{aligned}$$

where $z = \gamma x$. Hence, we are interested in $\nu \in \mathbf{F}_{2^t}$ satisfying

$$\sum_{z \in \mathbf{F}_{2^t}} (-1)^{T(z^{2^{k-1}+1} + \gamma^{2^k+1}\nu z)} = 0 \quad \text{for every } \gamma \in \mathbf{F}_{2^t}. \tag{5.2}$$

By Proposition 5.3, condition (5.2) is satisfied if and only if

$$T_c^t(\gamma^{2^k+1}\nu) \neq 1 \quad \text{for every } \gamma \in \mathbf{F}_{2^t}. \tag{5.3}$$

Let $s = \gcd(t,k)$. If (5.3) holds, then t/s must be even because otherwise $x \mapsto x^{2^k+1}$ would be a permutation. Hence t must be even. Further, $k-1$ must be even when t/c is odd. ∎

Now we are going to prove that condition (5.3) is generally impossible.

LEMMA 5.5. *Let $t = 2r$, $1 \leq k \leq r$, and $c = \gcd(t, k-1)$, where k is odd. Assume that there exists an element $\lambda \in \mathbf{F}_{2^t}^*$ satisfying*

$$T_c^t(\gamma^{2^k+1}\lambda) \neq 1 \quad \textit{for every } \gamma \in \mathbf{F}_{2^t}.$$

Then $k = r$ and $c = 2$. In particular, r is odd.

Proof. Note that c is even, by hypothesis, and thus $c \geq 2$. Denote by N the number of $x \in \mathbf{F}_{2^t}$ satisfying

$$T_c^t(x^{2^k+1}\lambda) = 1.$$

We have

$$\begin{aligned}
&\sum_{x\in\mathbf{F}_{2^t}} \sum_{a\in\mathbf{F}_{2^t}} (-1)^{T_1^t(a(T_c^t(x^{2^k+1}\lambda)+1))} \\
&= 2^t \times \#\{\ x \in \mathbf{F}_{2^t} \mid T_c^t(x^{2^k+1}\lambda) = 1\ \} \\
&= 2^t N.
\end{aligned}$$

Hence we can use the results on the Walsh transform of quadratic monomial functions to bound N. Our goal is to show that $N \geq 1$, except for the case $k = r$. Setting $b = T_c^t(a)$, the above sum can be modified to

$$\begin{aligned}
N &= \frac{1}{2^t} \sum_{b\in\mathbf{F}_{2^c}} 2^{t-c}(-1)^{T_1^c(b)} \sum_{x\in\mathbf{F}_{2^t}} (-1)^{T_1^c(b(T_c^t(x^{2^k+1}\lambda)))} \\
&= \frac{1}{2^c} \sum_{b\in\mathbf{F}_{2^c}} (-1)^{T_1^c(b)} \sum_{x\in\mathbf{F}_{2^t}} (-1)^{T_1^t(b\lambda x^{2^k+1})} \\
&= \frac{1}{2^c} \left(2^t + \sum_{b\in\mathbf{F}_{2^c}^*} (-1)^{T_1^c(b)} \sum_{x\in\mathbf{F}_{2^t}} (-1)^{T_1^t(b\lambda x^{2^k+1})} \right).
\end{aligned}$$

Let $s = \gcd(t,k)$. Since t/s is even, we have, by Proposition 5.2,

$$\mathcal{F}(h) = \sum_{x\in\mathbf{F}_{2^t}} (-1)^{T_1^t(b\lambda x^{2^k+1})} \in \{0, \pm 2^{r+s}, \pm 2^r\}.$$

Thus,

$$N = \frac{1}{2^c} \left(2^t + \sum_{b\in\mathbf{F}_{2^c}^*} (-1)^{T_1^c(b)}\ \epsilon_b \right),$$

where $\epsilon_b \in \{0, \pm 2^r, \pm 2^{r+s}\}$. In particular,

$$N > \frac{1}{2^c}\left(2^t - 2^c 2^{r+s}\right) = 2^{t-c} - 2^{r+s} = 2^r(2^{r-c} - 2^s). \tag{5.4}$$

Let us prove that $r - c \geq s$ unless $k = r$. Recall that $c = \gcd(2r, k-1)$ is even. Moreover, s is odd, $c < k \leq r$, and, clearly, $\gcd(s, c) = 1$.

First, note that $r - c \geq s$ for $s = 1$, since $r - c \geq 1$. So we assume that $s \geq 3$. Set $c = 2c'$ so that $r = sc'v$ for some c' and some $v \geq 1$. So we have

$$r - c = sc'v - 2c' = c'(sv - 2).$$

If $v > 1$, then for any c',

$$r - c = c'(sv - 2) = c'(s + (s(v-1) - 2)) \geq s.$$

If $v = 1$, then $r = c's$ and we want to check when $c'(s-2) \geq s$. Setting $s = 2 + \tau$ with τ odd, it holds if and only if $c'\tau \geq \tau + 2$. This last inequality is satisfied unless $c' = 1$ or $c' = 2$ and $\tau = 1$.

In the case where $c' = 2$ and $\tau = 1$, we have $r = 6$ and $s = 3$ so that $k = 3$, since $s = \gcd(r, k)$. Further, $c = 4$ and we get $k > c$, a contradiction.

Finally, it appears that $r - c \geq s$ unless $c' = 1$ and $v = 1$, the case where $r = s = k$. According to (5.4), we conclude that $N \geq 1$ unless $k = r$. In this case, we have $k = r = s$, which implies that r is odd and $c = 2$, completing the proof. ∎

Now we are able to prove our main theorem.

Proof of Theorem 5.1. We are now able to determine which polynomials of type

$$\rho(X) = X^{2^k+2} + \nu X, \qquad \rho \in \mathbf{F}_{2^t}[X],$$

with $0 \leq k \leq t-1$, are permutations of $\mathbf{F}_{2^t}$. If $k = 0$, then $\rho(X) = X^3 + \nu X$. So ρ cannot be a permutation, since it has two roots in $\mathbf{F}_{2^t}$. For $k = 1$, we get

$$\rho(X) = X^4 + \nu X = X(X^3 + \nu),$$

which is a linearized polynomial. Thus, it is a permutation polynomial if and only if it has only one root, i.e., ν is never equal to x^3 when x runs through $\mathbf{F}_{2^t}^*$.

We now assume that $k > 1$. According to Lemmas 5.4 and 5.5, we know that ρ is a permutation only when $t = 2r$, with r odd, $k = r$, and $c = \gcd(2r, r-1) = 2$. Moreover, those ν such that ρ is a permutation are the elements of $\mathbf{F}_{2^t}^*$ which satisfy

$$T_2^{2r}(\gamma^{2^r+1}\nu) \neq 1 \quad \text{for every} \quad \gamma \in \mathbf{F}_{2^{2r}}. \tag{5.5}$$

Note that $\{\gamma^{2^r+1} | \gamma \in \mathbf{F}_{2^{2r}}\} = \mathbf{F}_{2^r}$, and therefore (5.5) is equivalent to

$$T_2^{2r}(\delta\nu) \neq 1 \quad \text{for every} \quad \delta \in \mathbf{F}_{2^r}. \tag{5.6}$$

It remains to describe the set of suitable ν. Consider the map $\ell_\nu : \mathbf{F}_{2^r} \to \mathbf{F}_{2^2}$ defined by $\ell_\nu(z) = T_2^{2r}(\nu z)$. Note that ℓ_ν is $\mathbf{F}_2$-linear and

$$\ell_\nu(z) = \nu z + \cdots + (\nu z)^{2^{r-1}} + \nu^{2^{r+1}} z^2 + \cdots + \nu^{2^{2(r-1)}} z^{2^{r-2}}.$$

So ℓ_ν cannot be constant.

Moreover, if also (5.6) holds, then

$$\{\ell_\nu(z)|z \in \mathbf{F}_{2^r}\} = \{0, \omega\}, \quad \text{where } \omega \in \mathbf{F}_{2^2} \setminus \mathbf{F}_2. \tag{5.7}$$

Assume that ℓ_ν satisfies (5.7) for such ω. We consider now the map $\ell_{\nu\omega^2}$. Since $\ell_{\nu\omega^2}(z) = \omega^2\ell_\nu(z)$, we have

$$\{\ell_{\nu\omega^2}(z)|z \in \mathbf{F}_{2^r}\} = \{0, 1\}. \tag{5.8}$$

From (5.8) it follows that $T_1^2(\ell_{\nu\omega^2}(z)) = 0$ for every $z \in \mathbf{F}_{2^r}$. Observe, that

$$T_1^2(\ell_{\nu\omega^2}(z)) = T_1^2(T_2^{2r}(\nu\omega^2 z)) = T_1^{2r}(\nu\omega^2 z) = T_1^r(T_r^{2r}(\nu\omega^2)z).$$

But the function $z \mapsto T_1^r(T_r^{2r}(\nu\omega^2)z)$ is constantly zero if and only if $T_r^{2r}(\nu\omega^2)$ is zero, which is equivalent to $\nu\omega^2 \in \mathbf{F}_{2^r}$. To complete the proof, note that for any $\nu = \omega u$, with $u \in \mathbf{F}_{2^r}$, we have

$$\ell_{\nu\omega}(z) = \omega\ell_1(uz) = \omega T_1^r(uz),$$

implying (5.7). □

Remark 1. Note that we have proved the following: There are $2(2^r - 1)$ permutations of $\mathbf{F}_{2^{2r}}$ with polynomial form $X^{2^r+2} + \nu X$. These correspond to

$$\nu \in (\omega\mathbf{F}_{2^r}^*) \cup \left(\omega^2\mathbf{F}_{2^r}^*\right)$$

with notation $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$.

6. Conclusion. As one may see from the list of known monomial bent functions in the introduction, the quadratic monomial bent functions are easily characterized. The complete classification of the cubic monomial bent functions $T_1^{2t}(\lambda x^{2^i+2^j+1})$ seems to be a difficult problem. In this paper all bent exponents $2^t + 2^j + 1$ are found. Further, it is shown that all cubic monomial bent functions from the Maiorana–McFarland family to the subfield are known. All known bent exponents (computer search for $n \leq 24$, exhaustive search for $n \leq 20$) are covered by the examples in the introduction. However, the following question remains open.

Open Problem 1. *Are there cubic monomial bent functions besides those listed in the introduction of this paper?*

Acknowledgments. The authors thank Anne Canteaut for many helpful discussions along this work. They wish also to thank Gregor Leander for his valuable comments.

REFERENCES

[1] A. Canteaut, P. Charpin, and G. Kyureghyan, *A new class of monomial bent functions*, in Proceedings of the 2006 IEEE International Symposium on Information Theory (ISIT 06, Seattle), IEEE Press, Piscataway, NJ, 2006, pp. 903–906.

[2] A. Canteaut, P. Charpin, and G. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Appl., 14 (2008), pp. 221–241.

[3] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, *Finding nonnormal bent functions*, Discrete Appl. Math., 154 (2006), pp. 202–218.

[4] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, *On cryptographic properties of the cosets of $R(1, m)$*, IEEE Trans. Inform. Theory, 47 (2001), pp. 1494–1513.

[5] P. Charpin, C. Tavernier, and E. Pasalic, *On bent and semi-bent quadratic Boolean functions*, IEEE Trans. Inform. Theory, 51 (2005), pp. 4287–4298.

[6] J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph.D. dissertation, University of Maryland, College Park, MD, 1974.
[7] J. F. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl., 10 (2004), pp. 342–389.
[8] G. M. Kyureghyan, *Crooked maps in* $\mathbf{F}_{2^n}$, Finite Fields Appl., 13 (2007), pp. 713–726.
[9] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36 (1990), pp. 686–692.
[10] N. G. Leander, *Monomial bent functions*, IEEE Trans. Inform. Theory, 52 (2006), pp. 738–743.
[11] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer, Boston, 1987.
[12] R. L. McFarland, *A family of noncyclic difference sets*, J. Combin. Theory Ser. A, 15 (1973), pp. 1–10.