Binary linear codes with few weights from two-to-one functions

Kangquan Li, Chunlei Li, *Member, IEEE*, Tor Helleseth, *Fellow, IEEE*, and Longjiang Qu

***Abstract*—In this paper, we apply two-to-one functions over $\mathbb{F}_{2^n}$ in two generic constructions of binary linear codes. We consider two-to-one functions in two forms: (1) generalized quadratic functions; and (2) $(x^{2^t}+x)^e$ with $\gcd(t,n) = \gcd(e,2^n-1) = 1$. Based on the study of the Walsh transforms of those functions or their variants, we present many classes of linear codes with few nonzero weights, including one weight, three weights, four weights, and five weights. The weight distributions of the proposed codes with one weight and with three weights are determined. In addition, we discuss the minimum distance of the dual of the constructed codes and show that some of them achieve the sphere packing bound. Moreover, examples show that some codes in this paper have best-known parameters.**

***Index Terms*—Binary linear codes, two-to-one functions, 3-weight linear codes, 1-weight linear codes**

I. Introduction

LET q be a power of a prime p, $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_q^*$ be its multiplicative group. An $[n,k,d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum (Hamming) distance d. It is sometimes said to be optimal (with respect to the Hamming bound) when its minimum distance d achieves the maximum possible value for given parameters n and k [1]. Given an $[n,k,d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$, its dual is an $[n,n-k]$ linear code defined by $\mathcal{C}^\perp = \left\{\mathbf{x}\in\mathbb{F}_q^n : \mathbf{x}\cdot\mathbf{c}=0, \forall \mathbf{c}\in\mathcal{C}\right\}$, where $\mathbf{x}\cdot\mathbf{c} = \sum_{i=1}^n x_i c_i$ is the Euclidean inner product. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined as $1+A_1z+A_2z^2+\cdots+A_nz^n$. The sequence $(1,A_1,A_2,\cdots,A_n)$ is called the weight distribution of $\mathcal{C}$. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1,A_2,\cdots,A_n)$ is equal to t. Linear t-weight codes with small values of t have found applications in secret sharing schemes [2, 3], authentication codes [4], association schemes [5], strongly regular graphs [6], etc. In particular, one-weight codes are closely connected to the theory of Steiner systems and designs [7].

Known linear codes with good properties are constructed largely by two generic approaches [2, 8, 9]. The first approach defines linear codes over $\mathbb{F}_q$ with a function f from $\mathbb{F}_{q^n}$ to itself by

$$\overline{\mathcal{C}}_f = \left\{(\mathrm{Tr}_n(ax+bf(x)))_{x\in\mathbb{F}_{q^n}} : a,\, b\in\mathbb{F}_{q^n}\right\}$$

or

$$\mathcal{C}_f = \left\{(\mathrm{Tr}_n(ax+bf(x)))_{x\in\mathbb{F}_{q^n}^*} : a,\, b\in\mathbb{F}_{q^n}\right\}$$

when $f(0)=0$, where n is a positive integer and $\mathrm{Tr}_n(\cdot)$ is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. This generic construction has a long history and pertains to Delsarte's Theorem [10]. It also provides a coding-theory characterisation of APN functions, almost bent functions, and bent functions [11], and of the cross-correlation between m-sequences and their d-decimations when $f(x)$ is a power function x^d [12]. The second generic construction, initiated by Ding and Niederreiter [8], defines a linear code of length ℓ over $\mathbb{F}_q$ with a subset $D=\{d_1,d_2,\cdots,d_\ell\}\subseteq\mathbb{F}_{q^n}$ as

$$\mathcal{C}_D = \{(\mathrm{Tr}_n(xd_1),\mathrm{Tr}_n(xd_2),\cdots,\mathrm{Tr}_n(xd_\ell)) : x\in\mathbb{F}_{q^n}\}.$$

When the defining set D is properly chosen, the code $\mathcal{C}_D$ can have good or optimal parameters. The above construction is generic in the sense that all linear codes could be produced by selecting proper defining sets D. Researchers have proposed new families of linear codes with few weights by considering defining sets derived from the support and image of certain functions over $\mathbb{F}_{q^n}$, see

Kangquan Li and Longjiang Qu are with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, 410073, China (e-mail: likangquan11@nudt.edu.cn; ljqu_happy@hotmail.com). Longjiang Qu is also with the State Key Laboratory of Cryptology, Beijing, 100878, China.

Chunlei Li and Tor Helleseth are with the Department of Informatics, University of Bergen, Bergen N-5020, Norway (e-mail: chunlei.li@uib.no, tor.helleseth@uib.no).

The work of Longjiang Qu was supported by the National Natural Science Foundation of China (NSFC) under Grant 61722213, 11531002, National Key R&D Program of China (No.2017YFB0802000), and the Open Foundation of State Key Laboratory of Cryptology. The work of Tor Helleseth and Chunlei Li was supported by the Research Council of Norway (No. 247742/O70 and No. 311646/O70). The work of Chunlei Li was also supported in part by the National Natural Science Foundation of China under Grant (No. 61771021). The work of Kangquan Li was supported by China Scholarship Council. Longjiang Qu is the corresponding author.

[9, 13–20]. Interested readers may refer to a recent survey by Li and Mesnager in [21] and references therein for good or optimal linear codes constructed from these two generic approaches.

Nonlinear functions over finite fields play important roles in cryptography, combinatorics and sequence design. In coding theory, they have been utilized in the above two constructions to derive a number of good or optimal linear codes. Very recently Mesnager and Qu in [22] made a systematic study of two-to-one functions over arbitrary finite fields, motivated by their close connection to special important primitives in symmetric cryptography. Later, Li et al. studied two-to-one functions over finite fields with characteristic 2 and proposed some two-to-one trinomials and quadrinomials [23].

Constructing linear codes from two-to-one functions, to the best of our knowledge, began in [13, 24] where o-monomials and APN functions are discussed in the context. In this paper we will conduct a more comprehensive study of two-to-one functions in constructing binary linear codes with few weights. Two forms of two-to-one functions from $\mathbb{F}_{2^n}$ to itself are considered. The first form is the generalized quadratic polynomial $f(x)$, for which there exists a positive integer e with $\gcd(e, 2^n-1) = 1$ such that $f(x^e)$ is a quadratic function over $\mathbb{F}_{2^n}$. The second form is the function $(x^{2^t}+x)^e$ with $\gcd(t, n) = \gcd(e, 2^n - 1) = 1$. Among the generalized quadratic polynomials, of particular interest are those with few possible ranks because they can produce linear codes with few weights. Hence some two-to-one functions in [23] and two newly constructed two-to-one polynomials are considered. As a result, we obtain many classes of 1-weight, 3-weight, 5-weight binary linear codes by the two generic constructions. For the second form $(x^{2^t} + x)^e$, we provide an interesting connection between the weight distribution of linear codes and the Walsh spectrum of the Boolean function $\mathrm{Tr}_n(x^e)$. The connection enables us to derive many classes of 3-weight, 4-weight and 5-weight binary linear codes from known works on sequence design and cryptographically strong functions. Moreover, with the help of the Pless power moments, the weight distributions of the proposed 1-weight and 3-weight linear codes are determined. We do not manage to determine the weight distribution of those 5-weight linear codes in this paper. In the end, based on experimental results, we propose some open problems for the weight distributions of the constructed linear codes.

The remainder of this paper is organized as follows. Section 2 introduces some basic foundations and auxiliary results. Section 3 first recalls some known two-to-one functions in [23] and then investigates the parameters of binary linear codes constructed from those two-to-one functions. In Section 4, we construct two new classes of two-to-one functions and propose 3-weight linear codes from them. In Section 5, we discuss the properties of linear codes from the two-to-one functions of the form $(x^{2^t}+x)^e$. Finally, Section 6 concludes our work in the paper.

II. Preliminaries

This section presents basic notation, definitions and auxiliary results for the subsequent sections. Throughout this paper, we will restrict our discussion to finite fields with characteristic 2.

Let n be a positive integer. For $m \mid n$, let $\mathrm{Tr}_m^n(\cdot)$ denote the relative trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^m}$, i.e., $\mathrm{Tr}_m^n(x) = x + x^{2^m} + \cdots + x^{2^{\left(\frac{n}{m}-1\right)m}}$ for any $x \in \mathbb{F}_{2^n}$. Particularly, when $m = 1$, we use $\mathrm{Tr}_n(\cdot)$ to denote the absolute trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$. For any set E, we denote by $\#E$ the cardinality of E. For any function f, $\mathrm{Im}(f)$ denotes the image set of f. The statement that f vanishes on a given set V means that $f(x) = 0$ for any $x \in V$.

A. Binary codes from two-to-one functions

Let f be a mapping from $\mathbb{F}_{2^n}$ to itself with $f(0) = 0$. Recall that the Walsh transform of f at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is given by

$$W_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bf(x))}. \tag{1}$$

Here we add the case that $b = 0$ in the definition for convenience. The multiset

$$\{* \ \ W_f(a, b) : a, b \in \mathbb{F}_{2^n} \ \ *\}$$

is called the Walsh spectrum of f.

In the first generic construction, the binary linear code from f is given by

$$\mathcal{C}_f = \left\{ \mathbf{c}_{a,b} = (\mathrm{Tr}_n(ax + bf(x)))_{x \in \mathbb{F}_{2^n}^*} : a, b \in \mathbb{F}_{2^n} \right\}. \tag{2}$$

Note that the restriction $f(0) = 0$ implies $\mathrm{Tr}_n(ax + bf(x)) = 0$ for any $a, b \in \mathbb{F}_{2^n}$ when $x = 0$. Hence the code $\mathcal{C}_f$ is commonly considered in the literature over the code $\overline{\mathcal{C}_f}$ in the first generic construction. It is clear that $\mathcal{C}_f$ in (2) has length $2^n - 1$ and dimension at most $2n$. For determining the dimension of $\mathcal{C}_f$, it suffices to compute the number of $a, b \in \mathbb{F}_{2^n}$ such that the function $\mathrm{Tr}_n(ax+bf(x))$ vanishes on $\mathbb{F}_{2^n}$ since the code is linear. Equivalently, the dimension of $\mathcal{C}_f$ is equal to $2n - d_{K_1}$,

where d_{K_1} is the dimension of the $\mathbb{F}_2$-vector space K_1 defined as

$$\{(a,b) \in \mathbb{F}_{2^n}^2 : \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bf(x))} = 2^n\}. \quad (3)$$

The Hamming weight of a codeword $\mathbf{c}_{a,b}$ in $\mathcal{C}_f$ is given by

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_{a,b}) &= \#\{x \in \mathbb{F}_{2^n}^* : \mathrm{Tr}_n(ax+bf(x)) = 1\} \\ &= 2^{n-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bf(x))} \\ &= 2^{n-1} - \frac{1}{2} W_f(a,b). \end{aligned} \quad (4)$$

Therefore, the weight distribution of $\mathcal{C}_f$ can be directly derived from the Walsh spectrum of f. Namely, if a value of $W_f(a,b)$ occurs X times in the Walsh spectrum of f, then there are $X/2^{d_{K_1}}$ codewords in $\mathcal{C}_f$ with Hamming weight $2^{n-1} - \frac{1}{2}W_f(a,b)$. In particular, when the Walsh transforms of f take only three nontrivial values ($\neq 2^n$) v_1, v_2, v_3 for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$, the value distribution of $W_f(a,b)$ can be calculated by solving the following equations derived from the first three power moment identities [25]:

$$\begin{cases} X_0 + X_1 + X_2 + X_3 = 2^{2n} \\ v_0 X_0 + v_1 X_1 + v_2 X_2 + v_3 X_3 = 2^{2n} \\ v_0^2 X_0 + v_1^2 X_1 + v_2^2 X_2 + v_3^2 X_3 = 2^{3n}, \end{cases} \quad (5)$$

where X_i is the occurrences of $W_f(a,b) = v_i$'s, $i = 0,1,2,3$ in the Walsh spectrum of f with $(X_0, v_0) = (2^{d_{K_1}}, 2^n)$. Then the weight distribution of $\mathcal{C}_f$ can be determined accordingly.

Carlet, Charpin and Zinoviev [11] pointed out that the dual code of $\mathcal{C}_f$ has minimum distance 5 if and only if $f(x)$ is an APN function.

In the second construction, let $D(f) = \{f(x) : x \in \mathbb{F}_{2^n}\} \backslash \{0\} = \{d_1, d_2, \ldots, d_\ell\}$ and define the binary linear code $\mathcal{C}_{D(f)}$ as

$$\{\mathbf{c}_b = (\mathrm{Tr}_n(bd_1), \ldots, \mathrm{Tr}_n(bd_\ell)) : b \in \mathbb{F}_{2^n}\}. \quad (6)$$

It is clear that the code $\mathcal{C}_{D(f)}$ has length $\ell = \#D(f)$ and dimension at most n. Furthermore, in order to determine the dimension of $\mathcal{C}_{D(f)}$, we need to compute the number of $b \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_n(bf(x)) = 0$ for any $x \in \mathbb{F}_{2^n}$ since the code is linear. Equivalently, the dimension of $\mathcal{C}_{D(f)}$ is equal to $n - d_{K_2}$, where d_{K_2} is the dimension of the $\mathbb{F}_2$-vector space K_2 defined as

$$\{b \in \mathbb{F}_{2^n} : \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bf(x))} = 2^n\}. \quad (7)$$

For any $b \in \mathbb{F}_{2^n}$, the Hamming weight of a codeword $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ is given by

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_b) &= \#\{1 \le i \le \ell : \mathrm{Tr}_n(bd_i) = 1\} \\ &= \frac{1}{2}\left(\#D(f) - \sum_{d \in D(f)} (-1)^{\mathrm{Tr}_n(bd)}\right). \end{aligned}$$

According to the above formula, the weight distribution of the linear code $\mathcal{C}_{D(f)}$ is essentially the value distribution of a partial exponential sum, which is generally intractable if f is not properly chosen.

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be two-to-one over $\mathbb{F}_{2^n}$ if $\#f^{-1}(a) = 2$ for any $a \in \mathrm{Im}(f)$. For a two-to-one function $f(x)$ over $\mathbb{F}_{2^n}$ with $f(0) = 0$, the linear code $\mathcal{C}_{D(f)}$ has length $\#D(f) = 2^{n-1} - 1$ and the Hamming weight of its codeword is given by

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_b) &= \frac{1}{2}\left(\#D(f) - \frac{1}{2}\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bf(x))} + 1\right) \\ &= 2^{n-2} - \frac{1}{4}\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bf(x))}. \end{aligned} \quad (8)$$

From (7) and (8), one sees that the dimension and the weight distribution of $\mathcal{C}_{D(f)}$ heavily depend on the value of

$$W_f(0,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bf(x))}, \quad b \in \mathbb{F}_{2^n}. \quad (9)$$

For simplicity, we will write $W_f(0,b)$ as $W_f(b)$. In particular, if $W_f(b)$ takes only three nontrivial values ($\neq 2^n$) v_1, v_2 and v_3 for $b \in \mathbb{F}_{2^n}^*$, then the code $\mathcal{C}_{D(f)}$ has three nonzero weights, namely, $\mathrm{w}_i = 2^{n-2} - v_i/4$ for $i = 1,2,3$. Note that the dual of $\mathcal{C}_{D(f)}$ has Hamming weight no less than 3 as shown in Theorem 1. Denote by A_i the number of codewords with weight w_i in $\mathcal{C}_{D(f)}$. The first three Pless power moments [1, Th. 7.3.1] lead to the following system of equations:

$$\begin{cases} A_1 + A_2 + A_3 = 2^n - 1 \\ \mathrm{w}_1 A_1 + \mathrm{w}_2 A_2 + \mathrm{w}_3 A_3 = \ell 2^{n-1} \\ \mathrm{w}_1^2 A_1 + \mathrm{w}_2^2 A_2 + \mathrm{w}_3^2 A_3 = \ell(\ell+1)2^{n-2}, \end{cases} \quad (10)$$

where $\ell = 2^{n-1} - 1$. Therefore, the weight distribution of $\mathcal{C}_{D(f)}$ can be determined from the above system of equations when it is shown to have only three nonzero weights.

The above discussion shows that for a two-to-one mapping f, the parameters of the linear codes $\mathcal{C}_f$ in (2) and $\mathcal{C}_{D(f)}$ in (6) depend on the investigation of the Walsh transform of f. Ding in [13, 24] had a similar observation. Here we provide the discussion for self-completeness. In

addition, it is clear that the number of nonzero weights in $\mathcal{C}_{D(f)}$ is no more than that of $\mathcal{C}_f$. Therefore, we will focus on the two-to-one functions of which the Walsh transforms have few different values.

At the end of this subsection, we consider the parameters of the dual codes of $\mathcal{C}_{D(f)}$ in (6).

Theorem 1. *Let f be a two-to-one mapping over $\mathbb{F}_{2^n}$ with $f(0)=0$ and $\mathcal{C}_{D(f)}$ be defined as in (6). Let $\mathcal{C}_{D(f)}^{\perp}$ be the dual code of $\mathcal{C}_{D(f)}$ and d_{K_2} be defined as in (7). Then $\mathcal{C}_{D(f)}^{\perp}$ is a $\left[2^{n-1}-1, 2^{n-1}-1-n+d_{K_2}\right]$ binary code with the minimum distance $d_{D(f)}^{\perp}$ satisfying $3 \le d_{D(f)}^{\perp} \le 4$. Particularly, when $d_{K_2}=1$, the equality of the sphere packing bound can be achieved. Moreover, $d_{D(f)}^{\perp}=3$ if and only if there exist three distinct elements $x_1, x_2, x_3 \in \mathbb{F}_{2^n}^*$ such that $f(x_i) \neq f(x_j)$ for $1 \le i < j \le 3$ and $f(x_1)+f(x_2)+f(x_3)=0$.*

Proof. According to the above discussion, the linear code $\mathcal{C}_{D(f)}$ has length $2^{n-1}-1$ and dimension $n-d_{K_2}$. Then length and dimension of $\mathcal{C}_{D(f)}^{\perp}$ can be trivially determined by definition. Thus it suffices to consider the minimum distance.

It is clear that $d_{D(f)}^{\perp} \neq 1$. By definition $d_{D(f)}^{\perp}=2$ implies there exist two distinct elements $d_1, d_2 \in \mathrm{Im}(f)$ satisfying $d_1+d_2=0$, which is a contradiction. Thus $d_{D(f)}^{\perp} \ge 3$. In addition, suppose $d_{D(f)}^{\perp} \ge 5$, then we have

$$\sum_{i=0}^{2} \binom{2^{n-1}-1}{i} (2-1)^i = 2^{2n-3} - 2^{n-2} + 1 > 2^{n-d_{K_2}},$$

which contradicts the sphere packing bound. Thus $3 \le d_{D(f)}^{\perp} \le 4$. Particularly, when $d_{K_2}=1$, the equality of the sphere packing bound can be achieved, namely,

$$\sum_{i=0}^{1} \binom{2^{n-1}-1}{i} (2-1)^i = 2^{n-1} = 2^{n-d_{K_2}}.$$

Moreover, by definition $d_{D(f)}^{\perp}=3$ if and only if there are three distinct elements $d_1, d_2, d_3 \in \mathrm{Im}(f)$ such that $d_1+d_2+d_3=0$, i.e., there exist three distinct elements $x_1, x_2, x_3 \in \mathbb{F}_{2^n}^*$ such that $f(x_i) \neq f(x_j)$ for $1 \le i < j \le 3$ and $f(x_1)+f(x_2)+f(x_3)=0$. □

We need to recall some useful results on the Walsh transforms of quadratic functions.

B. Quadratic functions and Walsh transforms

Let Q be a quadratic function from $\mathbb{F}_{2^n}$ to itself, i.e., it has algebraic degree 2, and let $\varphi(x)=\mathrm{Tr}_n(Q(x))$. For the associated bilinear mapping $B_\varphi(x,y)=\varphi(x+y)+\varphi(x)+\varphi(y)$, its kernel V_φ is given by

$$\{y \in \mathbb{F}_{2^n} : B_\varphi(x,y)=0 \text{ for } \forall x \in \mathbb{F}_{2^n}\}.$$

The rank of φ is defined by $\mathrm{Rank}(\varphi)=n-\dim_{\mathbb{F}_2}(V_\varphi)$. Observe that

$$\begin{aligned}
&\left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(x))}\right)^2 \\
=& \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(x))} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(y))} \\
=& \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(x+y)+Q(y))} \\
=& \sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(y))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(x+y)+Q(x)+Q(y))} \\
=& 2^n \sum_{y\in V_\varphi} (-1)^{\mathrm{Tr}_n(Q(y))}.
\end{aligned}$$

By the definition of the kernel V_φ, it is readily seen that $\varphi(y)=\mathrm{Tr}_n(Q(y))$ is linear over V_φ. Then one has

$$\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\varphi(x)} = \begin{cases} \pm 2^{\frac{n+d}{2}}, & \text{if } \varphi \text{ vanishes on } V_\varphi, \\ 0, & \text{otherwise,} \end{cases} \tag{11}$$

where d is the dimension of V_φ over $\mathbb{F}_2$.

For a quadratic function f from $\mathbb{F}_{2^n}$ to itself, define

$$\varphi_{a,b}(x)=\mathrm{Tr}_n(ax+bf(x))$$

and

$$\varphi_b(x)=\mathrm{Tr}_n(bf(x)).$$

The bilinear mapping of $\varphi_{a,b}(x)$ is the same as that of $\varphi_b(x)$ for any nonzero b in $\mathbb{F}_{2^n}$. Therefore, the Walsh transform of f at (a,b) can be given, similar to (11), as below:

$$\begin{aligned} W_f(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\varphi_{a,b}(x)} \\ &= \begin{cases} \pm 2^{\frac{n+d_b}{2}}, & \text{if } \varphi_{a,b} \text{ vanishes on } V_{\varphi_b}, \\ 0, & \text{otherwise,} \end{cases} \end{aligned} \tag{12}$$

where d_b is the dimension of the kernel V_{φ_b} of the bilinear mapping φ_b over $\mathbb{F}_2$.

In Sections 3 and 4, we will discuss the properties of linear codes defined as in (2) and (6) from generalized quadratic functions. The Walsh transform of quadratic functions f in (12) will be heavily used in the discussion.

C. Factorization of low-degree polynomials

The following lemma describes the factorization of a cubic polynomial over $\mathbb{F}_{2^n}$. If f factors over $\mathbb{F}_{2^n}$ as a product of three linear factors we write $f=(1,1,1)$, if f factors as a product of a linear factor and an irreducible quadratic factor we write $f=(1,2)$ and finally if f is irreducible over $\mathbb{F}_{2^n}$ we write $f=(3)$.

Lemma 1. *[26] Let $f(x) = x^3 + ax + b \in \mathbb{F}_{2^n}[x]$ and $b \neq 0$. Let t_1, t_2 denote the solutions of $t^2 + bt + a^3 = 0$. Then the factorizations of $f(x)$ over $\mathbb{F}_{2^n}$ are characterized as follows:*

(1) $f = (1,1,1)$ if and only if $\mathrm{Tr}_n\left(a^3/b^2\right) = \mathrm{Tr}_n(1)$, t_1, t_2 are cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd);

(2) $f = (1,2)$ if and only if $\mathrm{Tr}_n\left(a^3/b^2\right) \neq \mathrm{Tr}_n(1)$;

(3) $f = (3)$ if and only if $\mathrm{Tr}_n\left(a^3/b^2\right) = \mathrm{Tr}_n(1)$, t_1, t_2 are not cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd).

Lemma 2. *[26] Let $f(x) = x^3 + ax + b \in \mathbb{F}_{2^n}[x]$ and $b \neq 0$. Let t be one solution of $t^2 + bt + a^3 = 0$ and ϵ be one solution of $x^3 = t$. Then $r = \epsilon + \frac{a}{\epsilon}$ is a solution of $f(x) = 0$.*

Lemma 3. *[27] Let $f(x) = x^4 + a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{F}_{2^n}$ and $a_0a_1 \neq 0$. Let $f_1(y) = y^3 + a_2y + a_1$ and r_1, r_2, r_3 denote roots of $f_1(y) = 0$ when they exist in $\mathbb{F}_{2^n}$. Set $w_i = a_0\frac{r_i^2}{a_1^2}$. Then $f = (1,1,2)$ if and only if $f_1 = (1,2)$ and $\mathrm{Tr}_n(w_1) = 0$.*

III. Binary linear codes from known two-to-one trinomials and quadrinomials

In this section, we will propose several binary codes with few weights, which are constructed from known two-to-one functions. We first recall some two-to-one functions recently obtained in [23].

Lemma 4. *[23] Let $n = 2m$ with m being an odd positive integer and $\omega \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$. Then the function $f(x) = x^{\frac{2^{n-1}+2^m-1}{3}} + x^{2^m} + \omega x$ is two-to-one over $\mathbb{F}_{2^n}$.*

Lemma 5. *[23] Let $n = 2m+1$. Then the following quadrinomials are all two-to-one over $\mathbb{F}_{2^n}$:*

(1) $f(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$;

(2) $f(x) = x^{2^{m+1}+2} + x^{2^{m+1}+1} + x^2 + x$;

(3) $f(x) = x^{2^{m+2}+4} + x^{2^{m+1}+2} + x^2 + x$;

(4) $f(x) = x^{2^n-2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$.

Lemma 6. *[23] Let $n = 3m$. Then the following quadrinomials are two-to-one over $\mathbb{F}_{2^n}$:*

(1) $f(x) = x^{2^{2m}+1} + x^{2^{m+1}} + x^{2^m+1} + x$ with $m \not\equiv 1 \pmod 3$;

(2) $f(x) = x^{2^{2m}+2^m} + x^{2^{2m}+1} + x^{2^m+1} + x$.

Below we shall investigate the parameters of the constructed linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$. According to different forms of n in Lemmas 4 - 6, we divide them into three subsections.

A. The case $n = 2m$

The following binary linear code is derived from the two-to-one polynomial in Lemma 4.

TABLE I
The weight distribution of the codes $\mathcal{C}_f$ in Theorem 2

Weight	Multiplicity
0	1
$2^{n-1} - 2^m$	$2^{4m-3} + 2^{3m-2} - 2^{2m-3} - 2^{m-2}$
2^{n-1}	$3 \cdot 2^{4m-2} + 2^{2m-2} - 1$
$2^{n-1} + 2^m$	$2^{4m-3} + 2^{m-2} - 2^{3m-2} - 2^{2m-3}$

TABLE II
The weight distribution of the codes $\mathcal{C}_{D(f)}$ in Theorem 2

Weight	Multiplicity
0	1
$2^{n-2} - 2^{m-1}$	$2^{n-3} + 2^{m-2}$
2^{n-2}	$3 \cdot 2^{n-2} - 1$
$2^{n-2} + 2^{m-1}$	$2^{n-3} - 2^{m-2}$

Theorem 2. *Let $f(x) = x^{\frac{2^{n-1}+2^m-1}{3}} + x^{2^m} + \omega x \in \mathbb{F}_{2^n}[x]$ with $n = 2m$, where $m > 1$ is odd and $\omega \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in (2) and (6), respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n - 1, 2n]$ binary linear code with weight distribution in Table I.

(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1} - 1, n\right]$ binary linear code with weight distribution in Table II.

Proof. We first compute the Walsh transforms $W_f(a,b)$ and $W_f(b)$ defined as in (9), for any $a, b \in \mathbb{F}_{2^n}$. It is obvious that $W_f(a,b) = 2^n$ when $a = b = 0$. Below we consider the cases where $(a,b) \neq (0,0)$.

Let $f_1(x) = f(x^{2^{m+2}+2}) = x + x^{2^{m+1}+4} + \omega x^{2^{m+2}+2}$ and $Q(x) = ax^{2^{m+2}+2} + bf_1(x) = bx + bx^{2^{m+1}+4} + (b\omega + a)x^{2^{m+2}+2}$. Since $\gcd\left(2^{m+2}+2, 2^n-1\right) = 1$, which is clear by the Euclidean algorithm, the Walsh transform

$$\begin{aligned} W_f(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n\left(ax^{2^{m+2}+2}+bf\left(x^{2^{m+2}+2}\right)\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(Q(x))}. \end{aligned}$$

Note that the bilinear form of $\varphi_{a,b}(x) = \mathrm{Tr}_n(Q(x))$ is given by

$$\begin{aligned} B_{\varphi_{a,b}}(x,y) =& \varphi_{a,b}(x+y) + \varphi_{a,b}(x) + \varphi_{a,b}(y) \\ =& \mathrm{Tr}_n\Big(by^4x^{2^{m+1}} + (b\omega+a)y^2x^{2^{m+2}} + \\ & by^{2^{m+1}}x^4 + (b\omega+a)y^{2^{m+2}}x^2\Big) \\ =& \mathrm{Tr}_n\left(L_{a,b}(y)x^{2^{m+2}}\right) \end{aligned}$$

with

$$L_{a,b}(y) = \Delta^2y^8 + \Delta^{2^m}y^2 \text{ and } \Delta = b^{2^m}\omega^2 + b + a^{2^m}.$$

Let $\ker(L_{a,b}) = \{y \in \mathbb{F}_{2^n} : L_{a,b}(y) = 0\}$. From (11), we have

$$W_f(a,b) = \begin{cases} \pm 2^{\frac{n+2}{2}}, & \text{if } \varphi_{a,b} \text{ vanishes on } \ker(L_{a,b}), \\ 0, & \text{otherwise.} \end{cases}$$

Now we discuss the values of $\varphi_{a,b}(x)$ where $x \in \ker(L_{a,b})$. When $\Delta = 0$, we have $L_{a,b}(y) = 0$ for any $y \in \mathbb{F}_{2^n}$. When $\Delta \neq 0$, by computation we have

$$\ker(L_{a,b}) = \left\{0,\ y_0,\ y_0\omega,\ y_0\omega^2\right\},$$

where $y_0 = \Delta^{\frac{2^{m-1}-1}{3}}$. Moreover,

$$\begin{aligned} \varphi_{a,b}(y_0) &= \mathrm{Tr}_n\left(by_0 + by_0^{2^{m+1}+4} + (a+\omega b)y_0^{2^{m+2}+2}\right) \\ &= \mathrm{Tr}_n\left(by_0 + \left(b + a^{2^m} + \omega^2 b^{2^m}\right) y_0^{2^{m+1}+4}\right) \\ &= \mathrm{Tr}_n\left(by_0 + \Delta^{\frac{2^n-1}{3}}\right). \end{aligned}$$

Similarly, we have

$$\varphi_{a,b}(y_0\omega) = \mathrm{Tr}_n\left(\omega b y_0 + \omega^2 \Delta^{\frac{2^n-1}{3}}\right).$$

and

$$\varphi_{a,b}(y_0\omega^2) = \varphi_{a,b}(y_0) + \varphi_{a,b}(y_0\omega).$$

In the following, we assume $a = 0$ and will show that there exist some (not all) b's $\in \mathbb{F}_{2^n}$ such that $\varphi_{0,b}$ vanishes on $\ker(L_{0,b})$, which implies

$$W_f(b) \in \left\{0, \pm 2^{\frac{n+2}{2}}\right\}.$$

It is well-known that for any elements $b \in \mathbb{F}_{2^n}$, there exist unique $b_1, b_2 \in \mathbb{F}_{2^m}$ such that $b = b_1 + b_2\omega$ since m is odd. Plugging $b = b_1 + b_2\omega$ into the expression of Δ, we get

$$\Delta = b^{2^m}\omega^2 + b = (b_1 + b_2\omega^2)\omega^2 + b_1 + b_2\omega = b_1\omega$$

and

$$y_0 = \Delta^{\frac{2^{m-1}-1}{3}} = (b_1\omega)^{\frac{2^{m-1}-1}{3}}.$$

Furthermore, we have

$$\varphi_{0,b}(y_0) = \mathrm{Tr}_n((b_1 + b_2\omega)(b_1\omega)^{\frac{2^{m-1}-1}{3}} + b_1^{\frac{2^n-1}{3}}\omega^{\frac{2^n-1}{3}})$$

and

$$\varphi_{0,b}(y_0\omega) = \mathrm{Tr}_n((b_1 + b_2\omega)(b_1\omega)^{\frac{2^{m-1}-1}{3}}\omega + b_1^{\frac{2^n-1}{3}}\omega^{\frac{2^n+5}{3}}).$$

It suffices to show that there exist some (not all) $b_1, b_2 \in \mathbb{F}_{2^m}$ such that $\varphi_{0,b}(y_0) = \varphi_{0,b}(y_0\omega) = 0$. Next, we only prove the case $m \equiv 0 \pmod 3$. The proofs of the other two cases are similar.

When $m \equiv 0 \pmod 3$, since m is odd, we can assume that $m = 3(2l+1)$ with some integer l. Then $2^{m-1} - 1 = 2^{6l+2} - 1 = 4 \times 8^{2l} - 1$ and thus $2^{m-1} - 1 \equiv 3 \pmod 9$, i.e., $\frac{2^{m-1}-1}{3} \equiv 1 \pmod 3$. Similarly, we have $\frac{2^n-1}{3} \equiv 0 \pmod 3$. Plugging these congruence equations into the expressions of $\varphi_{0,b}(y_0)$ and $\varphi_{0,b}(y_0\omega)$, we get

$$\begin{aligned} \varphi_{0,b}(y_0) &= \mathrm{Tr}_n\left(b_1^{\frac{2^{m-1}+2}{3}}\omega + b_1^{\frac{2^{m-1}-1}{3}}b_2\omega^2 + b_1^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_m\left(b_1^{\frac{2^{m-1}+2}{3}} + b_1^{\frac{2^{m-1}-1}{3}}b_2\right), \end{aligned}$$

and

$$\begin{aligned} \varphi_{0,b}(y_0\omega) &= \mathrm{Tr}_n\left(b_1^{\frac{2^{m-1}+2}{3}}\omega^2 + b_1^{\frac{2^{m-1}-1}{3}}b_2 + b_1^{\frac{2^n-1}{3}}\omega^2\right) \\ &= \mathrm{Tr}_m\left(b_1^{\frac{2^{m-1}+2}{3}} + b_1^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_m\left(b_1^{\frac{2^{m-1}+2}{3}}\right) + 1. \end{aligned}$$

Since $\gcd\left(\frac{2^{m-1}+2}{3}, 2^m - 1\right) = 1$, $p(b_1) = b_1^{\frac{2^{m-1}+2}{3}}$ permutes $\mathbb{F}_{2^m}$ and then there must exist some $b_1 \in \mathbb{F}_{2^m}$ such that $\varphi_{0,b}(y_0\omega) = 0$. Moreover, it is clear that $p(b_2) = b_1^{\frac{2^{m-1}+2}{3}} + b_1^{\frac{2^{m-1}-1}{3}}b_2$ permutes $\mathbb{F}_{2^m}$ for any $b_1 \in \mathbb{F}_{2^m}^*$. Thus for any $b_1 \in \mathbb{F}_{2^m}$ satisfying $\varphi_{0,b}(y_0\omega) = 0$, there exist some $b_2 \in \mathbb{F}_{2^m}$ such that $\varphi_{0,b}(y_0) = 0$ or 1. In other words, there exist some (not all) $b_1, b_2 \in \mathbb{F}_{2^m}$ such that $\varphi_{0,b}$ vanishes on $\ker(L_{0,b})$.

Therefore, we have $W_f(b) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ and obviously, $W_f(a,b) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for $(a,b) \neq (0,0)$.

With the analysis of possible values of $W_f(a,b)$ and $W_f(b)$, we are now ready to determine the parameters of $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ in the following.

(1) For the linear code $\mathcal{C}_f$, since $W_f(a,b) = 2^n$ if and only if $a = b = 0$, it follows from (3) that the dimension is $2n$. Moreover, for any $a, b \in \mathbb{F}_{2^n}$, $W_f(a,b) \in \left\{0, 2^n, \pm 2^{\frac{n+2}{2}}\right\}$. Let

$$v_1 = -2^{\frac{n+2}{2}}, \quad v_2 = 0, \quad v_3 = 2^{\frac{n+2}{2}}.$$

According to (5), we can obtain the occurrences of $W_f(a,b) = v_i$'s, $i = 1,2,3$ in the Walsh spectrum of f and then the desired weight distribution of $\mathcal{C}_f$ in Table I follows directly from (4).

(2) For the linear code $\mathcal{C}_{D(f)}$, since $W_f(b) = 2^n$ if and only if $b = 0$, it follows from (7) that the dimension of $\mathcal{C}_{D(f)}$ is n. Note that for any $b \in \mathbb{F}_{2^n}$, $W_f(b) \in \left\{0, 2^n, \pm 2^{\frac{n+2}{2}}\right\}$. By (8), the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy

$$\mathrm{wt}(\mathbf{c}_b) \in \left\{2^{n-2}, 0, 2^{n-2} - 2^{\frac{n-2}{2}}, 2^{n-2} + 2^{\frac{n-2}{2}}\right\}.$$

TABLE III
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_{D(f)}$ IN THEOREM 3

Weight	Multiplicity
0	1
$2^{n-2}-2^{m-1}$	$2^{n-2}+2^{m-1}$
2^{n-2}	$2^{n-1}-1$
$2^{n-2}+2^{m-1}$	$2^{n-2}-2^{m-1}$

Denote

$$\mathrm{w}_1 = 2^{n-2} - 2^{\frac{n-2}{2}},\ \mathrm{w}_2 = 2^{n-2},\ \mathrm{w}_3 = 2^{n-2} + 2^{\frac{n-2}{2}}.$$

The desired weight distribution of $\mathcal{C}_{D(f)}$ in Table II can be easily obtained by solving (10) accordingly. □

Example 1. *Take $m = 3$. In Theorem 2 the code $\mathcal{C}_f$ is a $[63, 12, 24]$ binary linear code with weight enumerator $1 + 630z^{24} + 3087z^{32} + 378z^{36}$ and the code $C_{D(f)}$ is a $[31, 6, 12]$ binary linear code with weight enumerator $1 + 10z^{12} + 47z^{16} + 6z^{20}$. They are consistent with the weight distributions in Tables I and II. According to the code table [28], the linear code $\mathcal{C}_f$ has the best-known parameters.*

B. The case $n = 2m + 1$

From the four classes of two-to-one functions in Lemma 5, this subsection presents five classes of 3-weight linear codes, two classes of 1-weight linear codes and one class of linear codes with at most five weights.

Theorem 3. *Let $n = 2m + 1$ and $f(x) = x^{2^n-2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in (2) and (6), respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n - 1, 2n]$ binary linear code with at most five weights.

(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1} - 1, n\right]$ binary linear code with weight distribution in Table III.

Proof. Since $\gcd(2^m + 1, 2^n - 1) = 1$, we have that $W_f(a, b)$ equals

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n\left(ax^{2^m+1}+bf(x^{2^m+1})\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n\left((a^2+b+b^2)x^{2^{m+1}+2}+bx^{2^{m+1}+1}+bx^{2^m+2}\right)} \\
&\triangleq \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\varphi_{a,b}(x)}.
\end{aligned}$$

Similar to the proof of Theorem 2 and by (12), we have $W_f(0, 0) = 0$ and for $(a, b) \neq (0, 0)$,

$$W_f(a,b) = \begin{cases} \pm 2^{\frac{n+d_{a,b}}{2}}, & \text{if } \varphi_{a,b} \text{ vanishes on } \ker(L_{a,b}), \\ 0, & \text{otherwise,} \end{cases}$$

where $d_{a,b}$ is the dimension of $\ker(L_{a,b})$ and

$$\begin{aligned}
L_{a,b}(y) =& b^4y^8 + \left(b^{2^{m+2}} + b^4 + b^2 + a^4\right) y^4 + \\
&\left(b^{2^{m+2}} + b^{2^{m+1}} + b^2 + a^{2^{m+2}}\right) y^2 + b^{2^{m+1}} y.
\end{aligned}$$

From the expression of $L_{a,b}$, it is obvious that $d_{a,b} \leq 3$. Moreover, since $n + d_{a,b}$ must be even and n is odd, $d_{a,b} \in \{1, 3\}$. Hence the Walsh transform

$$W_f(a, b) \in \left\{2^n,\ 0,\ \pm 2^{\frac{n+1}{2}},\ \pm 2^{\frac{n+3}{2}}\right\}.$$

Next, we will show that the Walsh transform $W_f(b) = 0$ when $d_{0,b} = 3$. Namely, there exists some $y_0 \in \ker(L_{0,b})$ such that $\varphi_{0,b}(y_0) = 1$. In this case, we have

$$\begin{aligned}
L_{0,b}(y) \quad = \quad & b^4y^8 + \left(b^{2^{m+2}} + b^4 + b^2\right) y^4 + \\
& \left(b^{2^{m+2}} + b^{2^{m+1}} + b^2\right) y^2 + b^{2^{m+1}} y.
\end{aligned}$$

Denote

$$\varphi_{0,b}(y) = \mathrm{Tr}_n\left(b(y^{2^{m+1}+2} + y^{2^{m+1}+1} + y^{2^m+2} + y^{2^m+1})\right).$$

Let $z = y^2 + y$. Then we have

$$\begin{aligned}
L_{0,b} \quad &= \quad b^4z^4 + b^2z^2 + b^{2^{m+2}}z^2 + b^{2^{m+1}}z \\
&= \quad (b^2z^2 + b^{2^{m+1}}z)^2 + b^2z^2 + b^{2^{m+1}}z.
\end{aligned}$$

If $d_{0,b} = 3$, i.e., the number of solutions of $L_{0,b} = 0$ equals 8, then the equation

$$(b^2z^2 + b^{2^{m+1}}z)^2 + b^2z^2 + b^{2^{m+1}}z = 0 \qquad (13)$$

has 4 solutions in $\mathbb{F}_{2^n}$ since y and $y + 1$ correspond to the same $z = y^2 + y$. Clearly, from (13), we have $b^2z^2 + b^{2^{m+1}}z = 0$ or $b^2z^2 + b^{2^{m+1}}z = 1$. From $b^2z^2 + b^{2^{m+1}}z = 0$, we get two solutions $z_0 = 0$ and $z_1 = b^{2^{m+1}-2}$ in $\mathbb{F}_{2^n}$. Similarly, we also obtain two solutions $z = z_2, z_3$ from $b^2z^2 + b^{2^{m+1}}z = 1$. Thus if $d_{0,b} = 3$, $y^2 + y = z_i$ for $i = 0, 1, 2, 3$ exactly has two solutions in $\mathbb{F}_{2^n}$. Namely, $\mathrm{Tr}_n(z_i) = 0$ for $i = 0, 1, 2, 3$. Particularly, $\mathrm{Tr}_n(z_1) = \mathrm{Tr}_n(b^{2^{m+1}-2}) = 0$. Therefore, there exists some element $y_0 \in \mathbb{F}_{2^n}$ such that $b^{2^{m+1}-2} = y_0^2 + y_0$, i.e., $b = \frac{1}{(y_0^2+y_0)^{2^{m+1}}}$. Note that such y_0 belongs to $\ker(L_{0,b})$ and is what we need. Indeed,

$$\begin{aligned}
\varphi_b(y_0) =& \mathrm{Tr}_n\left(b(y_0^{2^{m+1}+2} + y_0^{2^{m+1}+1} + y_0^{2^m+2} + y_0^{2^m+1})\right) \\
=& \mathrm{Tr}_n\left(\frac{y_0^{2^{m+1}+2} + y_0^{2^{m+1}+1} + y_0^{2^m+2} + y_0^{2^m+1}}{(y_0^2+y_0)^{2^m+1}}\right) \\
=& \mathrm{Tr}_n(1) = 1.
\end{aligned}$$

Hence, $W_f(b) = 0$ when the dimension of $\ker(L_{0,b})$ is 3.

Next, we consider the parameters of $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$, respectively.

TABLE IV
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_{D(f)}$ IN THEOREM 4

Weight	Multiplicity
0	1
$2^{n-1}-2^m$	$2^{4m}+2^{3m}-2^{2m-1}-2^{m-1}$
2^{n-1}	$2^{4m+1}+2^{2m}-1$
$2^{n-1}+2^m$	$2^{4m}+2^{m-1}-2^{3m}-2^{2m-1}$

TABLE V
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_f$ IN THEOREM 5

Weight	Multiplicity
0	1
$2^{n-1}-2^m$	$2^{4m-1}+2^{3m-1}-2^{2m-1}-2^{m-1}$
2^{n-1}	$2^{4m}+2^{2m}-1$
$2^{n-1}+2^m$	$2^{4m-1}+2^{m-1}-2^{3m-1}-2^{2m-1}$

(1) For the linear code $\mathcal{C}_f$, since $W_f(a,b)=2^n$ if and only if $(a,b)=(0,0)$, the dimension is $2n$ from (3). Moreover, the possible Hamming weights of codewords in $\mathcal{C}_f$ are given by

$$\mathrm{wt}(\mathbf{c}_{a,b}) \in \left\{0, 2^{n-1}, 2^{n-1}\pm 2^{\frac{n-1}{2}}, 2^{n-1}\pm 2^{\frac{n+1}{2}}\right\}.$$

(2) For the linear code $\mathcal{C}_{D(f)}$, $W_f(b)=2^n$ if and only if $b=0$, which means that the dimension of $\mathcal{C}_{D(f)}$ is n according to (7). Since for any $b\in\mathbb{F}_{2^n}$, $W_f(b)\in\left\{2^n, 0, \pm 2^{\frac{n+1}{2}}\right\}$, by (8), the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy

$$\mathrm{wt}(\mathbf{c}_b) \in \left\{2^{n-2}, 0, 2^{n-2}-2^{\frac{n-3}{2}}, 2^{n-2}+2^{\frac{n-3}{2}}\right\}.$$

Then the desired weight distribution of $\mathcal{C}_{D(f)}$ can be obtained by solving (10) accordingly. □

The linear codes in the following two theorems are from quadratic two-to-one quadrinomials. These proofs can be easily obtained from (12) and thus we omit them here.

Theorem 4. *Let $n=2m+1$ and $f(x)=x^{2^{m+1}+2}+x^{2^{m+1}}+x^2+x$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in* (2) *and* (6)*, respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n-1, 2n]$ binary linear code with weight distribution in Table IV.
(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1}-1, n\right]$ binary linear code with weight distribution in Table III.

Theorem 5. *Let $n=2m+1$ and $f(x)=x^{2^{m+1}+2}+x^{2^{m+1}+1}+x^2+x$ or $f(x)=x^{2^{m+2}+4}+x^{2^{m+1}+2}+x^2+x$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in* (2) *and* (6)*, respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n-1, 2n-1]$ binary linear code with weight distribution in Table V.

TABLE VI
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_f$ IN THEOREM 6

Weight	Multiplicity
0	1
$2^{n-1}-2^{2m-1}$	$2^{4m-1}+2^{3m-1}-2^{2m-1}-2^{m-1}$
2^{n-1}	$2^{5m}+2^{2m}-2^{4m}-1$
$2^{n-1}+2^{2m-1}$	$2^{4m-1}+2^{m-1}-2^{3m-1}-2^{2m-1}$

(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1}-1, n-1\right]$ binary linear code with weight enumerator $1+(2^{n-1}-1)z^{2^{n-2}}$.

Example 2. *When $m=3$, the code $\mathcal{C}_f$ in Theorem 4 is a $[127, 14, 56]$ binary linear code with weight enumerator*

$$1+4572z^{56}+8255z^{64}+3556z^{72}.$$

Referring to the code table [28], the linear code is optimal.

Example 3. *When $m=3$, the code $\mathcal{C}_f$ in Theorem 5 is a $[127, 13, 56]$ binary linear code with weight enumerator*

$$1+2268z^{56}+4159z^{64}+1764z^{72}.$$

Referring to the code table [28], the linear code $\mathcal{C}_f$ has the best-known parameter. When $m=3$, the code $\mathcal{C}_{D(f)}$ in Theorem 5 is a $[63, 6, 32]$ binary linear code with weight enumerator $1+63z^{32}$. Referring to the code table [28], the linear code $\mathcal{C}_{D(f)}$ is optimal.

C. The case $n=3m$

In this subsection, we consider binary linear codes from the first two-to-one polynomial in Lemma 6. The second one will be generalized in Section 4 and the corresponding linear code will be discussed later.

Theorem 6. *Let $n=3m$ with $m\equiv 0 \pmod 3$ and $f(x)=x^{2^{2m}+1}+x^{2^{m+1}}+x^{2^m+1}+x$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in* (2) *and* (6)*, respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n-1, 5m]$ binary linear code with weight distribution in Table VI.
(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1}-1, n-1\right]$ binary linear code with weight enumerator $1+(2^{n-1}-1)z^{2^{n-2}}$.

Proof. We shall compute the value $W_f(a,b)$ for any $a,b\in\mathbb{F}_{2^n}$. Clearly, $W_f(0,0)=2^n$ and

$$\begin{aligned} W_f(a,1) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n\left(ax+x^{2^{2m}+1}+x^{2^{m+1}}+x^{2^m+1}+x\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax)}, \end{aligned}$$

which equals 2^n if $a = 0$ and 0 otherwise. Moreover, if $b \in \mathbb{F}_{2^m}\backslash\mathbb{F}_2$, then

$$W_f(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n\left(\left(a^{2^{m+1}}+b+b^2\right)x^{2^{m+1}}\right)},$$

which equals 2^n if $a^{2^{m+1}} + b + b^2 = 0$ and 0 otherwise. Next, we assume $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. For $(a,b) \neq (0,0)$, let $\varphi_{a,b}(x) = \mathrm{Tr}_n(ax + bf(x))$ and $\varphi_b(x) = \mathrm{Tr}_n(bf(x))$. According to (12), a routine calculation gives

$$W_f(a,b) = \begin{cases} \pm 2^{2m}, & \text{if } \varphi_{a,b} \text{ vanishes on } \ker(L_b), \\ 0, & \text{otherwise,} \end{cases}$$

where $L_b(y) = (b + b^{2^m})y + (b^{2^m} + b^{2^{2m}})y^{2^{2m}}$ and

$$\ker(L_b) = \left\{(b^{2^m} + b^{2^{2m}})\eta : \eta \in \mathbb{F}_{2^m}\right\}.$$

For any $x = (b^{2^m} + b^{2^{2m}})\eta \in \ker(L_b)$ with $\eta \in \mathbb{F}_{2^m}$,

$$\varphi_{a,b}(x) = \mathrm{Tr}_n\left(U_{a,b}\eta^2\right) = \mathrm{Tr}_m\left(\mathrm{Tr}_m^n(U_{a,b})\eta^2\right).$$

where

$$\begin{aligned} U_{a,b} &= a^2(b+b^{2^m})^{2^{m+1}} + (b+b^{2^m})^{2^{2m}+2^m+1} \\ &\quad +(b+b^{2^m})^{2^{2m+1}}(b^{2^{m+1}}+b). \end{aligned}$$

Obviously, $\mathrm{Tr}_n(ax + bf(x)) = 0$ if and only if

$$a^2 = (b+b^{2^m})^{2^{2m}-2^m+1}+(b+b^{2^m})^{2^{2m+1}-2^{m+1}}(b^{2^{m+1}}+b).$$

Thus for any $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$,

$$W_f(a,b) \in \left\{0, \pm 2^{2m}\right\}.$$

As for $W_f(b)$, we need the following claim which will be shown at the end of the proof.

Claim. For any $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, $\mathrm{Tr}_m^n(U_b) \neq 0$, where $U_b = U_{0,b}$.

According to the above claim, it is clear that $W_f(b) = 0$ for any $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$.

Next, we consider the parameters of $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$, respectively.

(1) For the linear code $\mathcal{C}_f$, since $W_f(a,b) = 2^n$ if and only if $b \in \mathbb{F}_{2^m}$ and $a^{2^{m+1}} + b + b^2 = 0$, by (3), the dimension of $K_1 = \{a, b \in \mathbb{F}_{2^n} : W_f(a,b) = 2^n\}$ is m and thus the dimension of $\mathcal{C}_f$ is $2n - m = 5m$. Moreover, for any $a, b \in \mathbb{F}_{2^n}$, $W_f(a,b) \in \left\{0, 2^n, \pm 2^{2m}\right\}$. Let

$$v_1 = -2^{2m}, \quad v_2 = 0, \quad v_3 = 2^{2m}.$$

By computing (5), we can get the occurrences of $W_f(a,b) = v_i$'s, $i = 1,2,3$ in the Walsh spectrum of f and then by (4), the desired weight distribution of $\mathcal{C}_f$ can be obtained.

(2) For the linear code $\mathcal{C}_{D(f)}$, since there are two b's (0 and 1) such that $W_f(b) = 2^n$ and $(2^n - 2)$ b's such that $W_f(b) = 0$, by (7), the dimension of $\mathcal{C}_{D(f)}$ equals $n - 1$. Moreover, by (8), we know that the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy $\mathrm{wt}(\mathbf{c}_b) \in \{0, 2^{n-2}\}$. Furthermore, the stated weight enumerator follows.

Finally, we prove the claim, i.e., for any $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, $\mathrm{Tr}_m^n(U_b) \neq 0$. A direct computation yields

$$\begin{aligned} \mathrm{Tr}_m^n(U_b) =& b^3 + b^{3\cdot 2^m} + b^{3\cdot 2^{2m}} + b^{2^{2m+1}+2^m} \\ &+ b^{2^{2m}+2} + b^{2^{m+1}+1}. \end{aligned} \tag{14}$$

For any $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, define

$$\begin{cases} b + b^{2^m} + b^{2^{2m}} = \alpha \\ b^{2^m+1} + b^{2^{2m}+1} + b^{2^{2m}+2^m} = \beta \\ b^{2^{2m}+2^m+1} = \gamma \end{cases}$$

and $g(x) = x^3 + \alpha x^2 + \beta x + \gamma \in \mathbb{F}_{2^m}[x]$. Then it is clear that $g(x) = (x+b)\left(x + b^{2^m}\right)\left(x + b^{2^{2m}}\right)$ and $g(x)$ is irreducible on $\mathbb{F}_{2^m}$. Let $u = b^{2^{2m+1}+2^m} + b^{2^{2m}+2} + b^{2^{m+1}+1}$ and $v = b^{2^{2m+1}+1} + b^{2^m+2} + b^{2^{m+1}+2^{2m}}$. Then we have

$$\begin{aligned} u + v &= \left(b + b^{2^m}\right)\left(b + b^{2^{2m}}\right)\left(b^{2^m} + b^{2^{2m}}\right) \\ &= (\alpha + b)\left(\alpha + b^{2^m}\right)\left(\alpha + b^{2^{2m}}\right) \\ &= g(\alpha) = \alpha\beta + \gamma. \end{aligned}$$

In addition, from the expanded form of $\left(b + b^{2^m} + b^{2^{2m}}\right)^3$, we know that

$$b^3 + b^{3\cdot 2^m} + b^{3\cdot 2^{2m}} = \alpha^3 + u + v = \alpha^3 + \alpha\beta + \gamma.$$

Moreover, since $b, b^{2^m}, b^{2^{2m}}$ are the roots of $g(x)$ in $\mathbb{F}_{2^n}$, $\frac{1}{b}, \frac{1}{b^{2^m}}, \frac{1}{b^{2^{2m}}}$ are the roots of

$$g'(x) = \frac{1}{\gamma}x^3 g\left(\frac{1}{x}\right) = x^3 + \frac{\beta}{\gamma}x^2 + \frac{\alpha}{\gamma}x + \frac{1}{\gamma}.$$

in $\mathbb{F}_{2^n}$. Similarly, we have

$$\frac{1}{b^3} + \frac{1}{b^{3\cdot 2^m}} + \frac{1}{b^{3\cdot 2^{2m}}} = \frac{\beta^3}{\gamma^3} + \frac{\alpha\beta}{\gamma^2} + \frac{1}{\gamma} = \frac{\beta^3 + \alpha\beta\gamma + \gamma^2}{\gamma^3}.$$

Furthermore,

$$\begin{aligned} uv &= \gamma^2 + \gamma(b^3 + b^{3\cdot 2^m} + b^{3\cdot 2^{2m}})b^{3\cdot(2^m+1)} \\ &\quad + b^{3\cdot\left(2^{2m}+2^m\right)} + b^{3\cdot\left(2^{2m}+1\right)} \\ &= \gamma^2 + \gamma(\alpha^3 + \alpha\beta + \gamma) + \gamma^3\left(\frac{1}{b^3} + \frac{1}{b^{3\cdot 2^m}} + \frac{1}{b^{3\cdot 2^{2m}}}\right) \\ &= \alpha^3\gamma + \alpha\beta\gamma + \beta^3 + \alpha\beta\gamma + \gamma^2 \\ &= \alpha^3\gamma + \beta^3 + \gamma^2. \end{aligned}$$

Now we go back to the expression of $\mathrm{Tr}_m^n(U_b)$, i.e., (14). If $\mathrm{Tr}_m^n(U_b)=0$, we have

$$u = b^3 + b^{3\cdot 2^m} + b^{3\cdot 2^{2m}} = \alpha^3 + \alpha\beta + \gamma$$

and then $v = \alpha\beta + \gamma + u = \alpha^3$. Thus $uv = \alpha^6 + \alpha^4\beta + \alpha^3\gamma = \alpha^3\gamma + \beta^3 + \gamma^2$, namely,

$$\alpha^6 + \alpha^4\beta + \beta^3 + \gamma^2 = 0. \tag{15}$$

Next, we show that under (15), $g(x) = 0$ has three solutions in $\mathbb{F}_{2^m}$, which is in contradiction with the irreduciblity of $g(x)$. Firstly, using $x+\alpha$ to replace x in $g(x)=0$ and simplifying it, we obtain

$$x^3 + (\alpha^2+\beta)x + \alpha\beta + \gamma = 0. \tag{16}$$

Moreover,

$$\begin{aligned}\mathrm{Tr}_m\left(\frac{(\alpha^2+\beta)^3}{(\alpha\beta+\gamma)^2}\right) &= \mathrm{Tr}_m\left(\frac{\alpha^6+\beta^3+\alpha^4\beta+\alpha^2\beta^2}{(\alpha\beta+\gamma)^2}\right)\\ &= \mathrm{Tr}_m(1),\end{aligned}$$

where the last equality is derived from (15). Furthermore, it is easy to get that the equation

$$t^2 + (\alpha\beta+\gamma)t + (\alpha^2+\beta)^3 = 0$$

has a solution $t_1 = (\alpha\beta+\gamma)\omega$, where $\omega^3=1$. Since $m \equiv 0 \pmod 3$, ω is a cube in $\mathbb{F}_{2^m}$ (m even), $\mathbb{F}_{2^{2m}}$ (m odd). In addition, $\alpha\beta+\gamma = \sqrt{(\alpha^2+\beta)^3}$ is also a cube in $\mathbb{F}_{2^m}$. Thus according to Lemma 1, (16) has three solutions in $\mathbb{F}_{2^m}$, which is a contradiction, and thus $\mathrm{Tr}_m^n(U_b) \neq 0$. □

IV. Binary linear codes from new two-to-one polynomials

In this section, we construct two new classes of two-to-one functions, of which the first one is a generalization of (2) in Lemma 6. Then we also obtain some binary linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ from these two new two-to-one functions .

A. Two new classes of two-to-one functions

Theorem 7. *Let $n = km$ with k, m odd and $f(x) = \mathrm{Tr}_m^n\left(x^{2^m+1}\right) + x$. Then $f(x)$ is two-to-one over $\mathbb{F}_{2^n}$.*

Proof. According to the definition of two-to-one functions, it suffices to prove that for any $a \in \mathbb{F}_{2^n}$, $\#f^{-1}(a) \in \{0,2\}$. Namely, for any $a \in \mathbb{F}_{2^n}$, $f(x+a)+f(a)=0$ has exactly two solutions in $\mathbb{F}_{2^n}$. By simplifying the equation, we have

$$\mathrm{Tr}_m^n\left(x^{2^m+1} + ax^{2^m} + a^{2^m}x\right) = x. \tag{17}$$

This implies $x \in \mathbb{F}_{2^m}$, and then (17) becomes $x^2+x=0$, which has exactly two solutions $x=0,1$. □

Theorem 8. *Let $n = 3m$ with m odd and $f(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$. Then $f(x)$ is two-to-one over $\mathbb{F}_{2^n}$.*

Proof. It suffices to prove that for any $a \in \mathbb{F}_{2^n}$, the equation $f(x+a)+f(a)=0$, i.e.,

$$\begin{aligned}&x^{2^{2m+1}+1} + ax^{2^{2m+1}} + x^{2^{m+1}+1} + ax^{2^{m+1}} + x^4 +\\ &x^3 + ax^2 + \left(a^{2^{2m+1}} + a^{2^{m+1}} + a^2\right)x = 0,\end{aligned} \tag{18}$$

has exactly two solutions in $\mathbb{F}_{2^n}$. In fact, since $x=0$ is clearly a solution of (18), we shall only show that (18) has at most two solutions in $\mathbb{F}_{2^n}$.

Let $y = x^{2^m}$, $z = y^{2^m}$, $b = a^{2^m}$ and $c = b^{2^m}$. Then (18) becomes

$$\begin{aligned}&xz^2 + xy^2 + x^3 + x^4 + a(x^2+y^2+z^2)\\ &\quad +(a^2+b^2+c^2)x = 0.\end{aligned} \tag{19}$$

Raising (19) to the 2^m-th power and the 2^{2m}-th power, we get

$$\begin{aligned}&yx^2 + yz^2 + y^3 + y^4 + b(x^2+y^2+z^2)\\ &\quad +(a^2+b^2+c^2)y = 0\end{aligned} \tag{20}$$

and

$$\begin{aligned}&zy^2 + zx^2 + z^3 + z^4 + c(x^2+y^2+z^2)\\ &\quad +(a^2+b^2+c^2)z = 0,\end{aligned} \tag{21}$$

respectively. Let $t = x+y+z$ and $s = a+b+c$. Computing the summation of (19), (20) and (21), we obtain

$$t^4 + t^3 + st^2 + s^2t = 0.$$

Thus $t=0$ or $t^3+t^2+st+s^2=0$.

If $t=0$, plugging it into (19), we have $x^4+sx=0$ and thus $x=0$ or $x^3=s$. It is clear that $x=0$ is a solution of (18). If $x^3 = s = a+b+c \in \mathbb{F}_{2^m}$, then $x = s^{\frac{1}{3}} \in \mathbb{F}_{2^m}$ and $y = z = x \in \mathbb{F}_{2^m}$. Thus $x = x+y+z = t = 0$.

If $t^3+t^2+st+s^2=0$, using (t_1+1) to replace t, we get

$$t_1^3 + (s+1)t_1 + s^2 + s = 0. \tag{22}$$

Since

$$\mathrm{Tr}_m\left(\frac{(s+1)^3}{(s^2+s)^2}\right) = \mathrm{Tr}_m\left(\frac{1}{s} + \frac{1}{s^2}\right) = 0 \neq \mathrm{Tr}_m(1),$$

(22) has exactly one solution in $\mathbb{F}_{2^m}$ according to Lemma 1. Moreover, we can get the expression of the unique solution by Lemma 2. For the equation $u^2 + (s^2+s)u + (s+1)^3 = 0$, we have

$$\left(\frac{u}{s^2+s}\right)^2 + \frac{u}{s^2+s} = \frac{1}{s} + \frac{1}{s^2}$$

and thus $u = s + 1$ is a solution and $\epsilon = (s+1)^{\frac{1}{3}}$ is a solution of $x^3 = u$ since $\gcd(3, 2^m - 1) = 1$. Furthermore, $r = \epsilon + \frac{a}{\epsilon} = (s+1)^{\frac{1}{3}} + (s+1)^{\frac{2}{3}}$ is a solution of (22) and thus

$$\bar{t} = r + 1 = \epsilon + \epsilon^2 + 1,$$

where $\epsilon = (s+1)^{\frac{1}{3}}$, is the unique solution of $t^3 + t^2 + st + s^2 = 0$. Namely, $x+y+z$ equals a constant. Plugging $x + y + z = \bar{t}$ into (19), we get

$$x^4 + (s^2 + \bar{t}^2)x + a\bar{t}^2 = 0. \tag{23}$$

Next, using Lemma 3, we will prove that the above equation has two solutions in $\mathbb{F}_{2^n}$. However, we will also show that the two solutions can not satisfy $x + y + z = \bar{t}$ at the same time and thus (19) has at most one solution in this case. Together with the zero solution, (19) has at most two solutions in $\mathbb{F}_{2^n}$ and thus $f(x)$ is two-to-one.

Recall that $\epsilon^3 = s+1$ and $\bar{t} = \epsilon+\epsilon^2+1$. Since $s^2+\bar{t}^2 = \epsilon^6+\epsilon^4+\epsilon^2$, if $s^2+\bar{t}^2 = 0$, then $\epsilon = 0$ clearly ($\epsilon^2+\epsilon+1 \neq 0$ due to m odd). Moreover, $s = \epsilon^3+1 = 1$ and $t = 1$. Thus if $s = 1$ and $t = 1$, (23) becomes $x^4 = a$, which has exactly one solution in $\mathbb{F}_{2^n}$. In the following, we assume that $s^2 + \bar{t}^2 \neq 0$. Let $f_1(r) = r^3 + (s^2 + \bar{t}^2)$. Then it is clear that $f_1 = (1, 2)$, which means that f_1 can factor as a product of a linear factor and an irreducible quadratic factor. Moreover,

$$r_1 = (s^2 + \bar{t}^2)^{\frac{1}{3}} = (s^2 + \epsilon^2 + \epsilon^4 + 1)^{\frac{1}{3}} = (\epsilon^2 + \epsilon^4 + \epsilon^6)^{\frac{1}{3}}$$

is the unique solution of $f_1(r) = 0$. Set $w_1 = a\bar{t}^2 \frac{r_1^2}{(s^2+\bar{t}^2)^2}$. In addition,

$$\begin{aligned}
\mathrm{Tr}_n(w_1) &= \mathrm{Tr}_n\left(\frac{a(\epsilon+\epsilon^2+1)^2}{(\epsilon^2+\epsilon^4+\epsilon^6)^{\frac{4}{3}}}\right) \\
&= \mathrm{Tr}_m\left(\mathrm{Tr}_m^n\left(\frac{a\bar{t}^2}{(\epsilon^2+\epsilon^4+\epsilon^6)^{\frac{4}{3}}}\right)\right) \\
&= \mathrm{Tr}_m\left(\frac{s\bar{t}^2}{(\epsilon^2+\epsilon^4+\epsilon^6)^{\frac{4}{3}}}\right) \\
&= \mathrm{Tr}_m\left(\frac{(\epsilon^2+\epsilon+1)^{\frac{4}{3}}}{\epsilon^{\frac{8}{3}}} + \frac{(\epsilon^2+\epsilon+1)^{\frac{1}{3}}}{\epsilon^{\frac{2}{3}}}\right) = 0.
\end{aligned}$$

Thus according to Lemma 3, (23) has exactly two solutions in $\mathbb{F}_{2^n}$, denoted by x_1, x_2. Next, we show that the two solutions cannot satisfy $x + y + z = \bar{t}$ at the same time. Clearly, there exist some $\alpha, \beta \in \mathbb{F}_{2^n}$ such that (23) becomes

$$\left(x^2 + \alpha x + \beta\right)\left(x^2 + \alpha x + \alpha^2 + \beta\right) = 0$$

and by comparing the coefficient of x, we know that $\alpha^3 = (s^2+\bar{t}^2) \neq 0$. In addition, by the Vieta theorem, $x_1+x_2 = \alpha \neq 0$. Thus the two solutions cannot satisfy $x+y+z = \bar{t}$ at the same time. □

TABLE VII
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_f$ IN THEOREM 9

Weight	Multiplicity
0	1
$2^{n-1} - 2^{\frac{n+m-1}{2}}$	$2^{n-1} + 2^{\frac{n+m}{2}-1} - 2^{n-m-1} - 2^{\frac{n-m}{2}-1}$
2^{n-1}	$2^{n+m} + 2^{n-m} - 2^n - 1$
$2^{n-1} + 2^{\frac{n+m-1}{2}}$	$2^{\frac{n-m}{2}-1} + 2^{n-1} - 2^{\frac{n+m}{2}-1} - 2^{n-m-1}$

TABLE VIII
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_{D(f)}$ IN THEOREM 9

Weight	Multiplicity
0	1
$2^{n-2} - 2^{\frac{n+m-4}{2}}$	$2^{n-m-1} + 2^{\frac{n-m-2}{2}}$
2^{n-2}	$2^n - 2^{n-m} - 1$
$2^{n-2} + 2^{\frac{n+m-4}{2}}$	$2^{n-m-1} - 2^{\frac{n-m-2}{2}}$

TABLE IX
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_{D(f)}$ IN THEOREM 10

Weight	Multiplicity
0	1
$2^{n-2} - 2^{\frac{n+2m-3}{2}}$	$2^{m-2} + 2^{\frac{m-3}{2}}$
2^{n-2}	$2^n - 2^{m-1} - 1$
$2^{n-2} + 2^{\frac{n+2m-3}{2}}$	$2^{m-2} - 2^{\frac{m-3}{2}}$

B. Binary linear codes from these new two-to-one functions

Theorem 9. *Let $n = km$ with k, m odd and $f(x) = \mathrm{Tr}_m^n\left(x^{2^m+1}\right) + x$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in* (2) *and* (6)*, respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n - 1, n + m]$ binary linear code with weight distribution in Table VII.
(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1} - 1, n\right]$ binary linear code with weight distribution in Table VIII

Proof. The two-to-one function in this theorem is quadratic and the proof is similarly obtained by the Walsh spectrum of f, whose computation is not difficult. We omit it here. □

Theorem 10. *Let $n = 3m$ with m odd and $f(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$. Define two linear codes $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$ as in* (2) *and* (6)*, respectively. Then,*

(1) $\mathcal{C}_f$ is a $[2^n - 1, 2n]$ binary linear code with 5 weights. Moreover, the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_f$

satisfy

$$\mathrm{wt}(\mathbf{c}_b) \in \Big\{2^{n-1}-2^{\frac{n+2m-1}{2}}, 2^{n-1}+2^{\frac{n+2m-1}{2}}, 2^{n-1}-2^{\frac{n+m-2}{2}}, 2^{n-1}+2^{\frac{n+m-2}{2}}, 2^{n-1}, 0\Big\}.$$

(2) $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1}-1, n\right]$ binary linear code with weight distribution in Table IX.

Proof. First of all, we shall determine the value $W_f(a,b)$. It is clear that when $(a,b)=(0,0)$, $W_f(a,b)=2^n$. Since f is quadratic, according to (12) and by computing, we have

$$W_f(a,b)=\begin{cases}\pm 2^{\frac{n+d_b}{2}}, & \text{if } \varphi_{a,b}\text{vanishes on } \ker(L_b),\\ 0, & \text{otherwise,}\end{cases}$$

where $\varphi_{a,b}(x)=\mathrm{Tr}_n(ax+bf(x))$,

$$L_b(y)=b^2y^{2^{2m+2}}+b^{2^{2m}}y^{2^{2m}}+b^2y^{2^{m+2}}+b^{2^m}y^{2^m}+b^2y^4+by$$

and d_b is the dimension of $\ker(L_b)$.

Next, we consider the equation $L_b(y)=0$, i.e., $b^2\mathrm{Tr}_m^n(y)^4=\mathrm{Tr}_m^n(by)$. Since $\mathrm{Tr}_m^n(y), \mathrm{Tr}_m^n(by)\in\mathbb{F}_{2^m}$, we have $b\in\mathbb{F}_{2^m}^*$ or $\mathrm{Tr}_m^n(y)=\mathrm{Tr}_m^n(by)=0$.

Case 1: If $b\in\mathbb{F}_{2^m}^*$, then the equation $L_b(y)=0$ becomes $\mathrm{Tr}_m^n(y)=0$ or $\sqrt[3]{b^{-1}}$. Thus in this case, the number of solutions of $L_b(y)$ is 2^{2m+1}. Namely, $d_b=2m+1$. In the following, we show that there exist some $b\in\mathbb{F}_{2^m}^*$ such that the restriction of $\mathrm{Tr}_n(bf(x))$ on $\ker(L_b)=\left\{y\in\mathbb{F}_{2^n}:\mathrm{Tr}_m^n(y)=0 \text{ or } \sqrt[3]{b^{-1}}\right\}$ is the all-zero mapping or not, i.e., $W_f(b)\in\left\{0,\pm 2^{\frac{n+2m+1}{2}}\right\}$ for $b\in\mathbb{F}_{2^m}^*$. On one hand, if $\mathrm{Tr}_m^n(y)=0$,

$$\begin{aligned}\mathrm{Tr}_n(bf(y)) &= \mathrm{Tr}_n\left(b\left(y\mathrm{Tr}_m^n(y)^2+y^4\right)\right)\\ &= \mathrm{Tr}_n(by^4)=\mathrm{Tr}_m\left(b\mathrm{Tr}_m^n\left(y^4\right)\right)=0.\end{aligned}$$

On the other hand, if $\mathrm{Tr}_m^n(y)=\sqrt[3]{b^{-1}}$,

$$\begin{aligned}\mathrm{Tr}_n(bf(y)) &= \mathrm{Tr}_n\left(b(y\mathrm{Tr}_m^n(y)^2+y^4)\right)\\ &= \mathrm{Tr}_m\left(\mathrm{Tr}_m^n\left(by\mathrm{Tr}_m^n(y)^2\right)+\mathrm{Tr}_m^n(by^4)\right)\\ &= \mathrm{Tr}_m\left(b\mathrm{Tr}_m^n(y)^3+b\mathrm{Tr}_m^n(y)^4\right)\\ &= \mathrm{Tr}_m(1+\mathrm{Tr}_m^n(y))=1+\mathrm{Tr}_m\left(\sqrt[3]{b^{-1}}\right).\end{aligned}$$

Then $\mathrm{Tr}_n(bf(y))=0$ if and only if $\mathrm{Tr}_m\left(\sqrt[3]{b^{-1}}\right)=1$ and thus the restriction of $\mathrm{Tr}_n(b(f(x)))$ on $\ker(L_b)$ is the all-zero mapping if and only if $\mathrm{Tr}_m\left(\sqrt[3]{b^{-1}}\right)=1$. Therefore $W_f(b)\in\left\{0,\pm 2^{\frac{n+2m+1}{2}}\right\}$ and then clearly $W_f(a,b)\in\left\{0,\pm 2^{\frac{n+2m+1}{2}}\right\}$ in this case.

Case 2: If $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, then

$$\ker(L_b)=\left\{y: y\in\mathbb{F}_{2^n} \text{ and } \mathrm{Tr}_m^n(y)=\mathrm{Tr}_m^n(by)=0\right\}.$$

For any $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, define

$$\begin{cases}b+b^{2^m}+b^{2^{2m}}=\alpha\\ b^{2^m+1}+b^{2^{2m}+1}+b^{2^{2m}+2^m}=\beta\\ b^{2^{2m}+2^m+1}=\gamma\end{cases}$$

and $g(x)=x^3+\alpha x^2+\beta x+\gamma\in\mathbb{F}_{2^m}[x]$. Then it is clear that $g(x)=(x+b)\left(x+b^{2^m}\right)\left(x+b^{2^{2m}}\right)$ and $g(x)$ is irreducible on $\mathbb{F}_{2^m}$. Since $g(x+\alpha)=x^3+(\alpha^2+\beta)x+\alpha\beta+\gamma$ is also irreducible, we have $\alpha^2+\beta\neq 0$ and $\alpha\beta+\gamma\neq 0$. In addition, for any fixed $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, it is well-known that for any $y\in\mathbb{F}_{2^n}$, there exist unique $y_0,y_1,y_2\in\mathbb{F}_{2^m}$ such that $y=y_0+y_1b+y_2b^2$. Then $\mathrm{Tr}_m^n(y)=y_0+y_1\alpha+y_2\alpha^2=0$ and

$$\begin{aligned}\mathrm{Tr}_m^n(by) &= \mathrm{Tr}_m^n\left(y_0b+y_1b^2+y_2b^3\right)\\ &= \mathrm{Tr}_m^n\left((y_1+y_2\alpha)b^2+(y_0+y_2\beta)b+y_2\gamma\right)\\ &= \alpha y_0+\alpha^2y_1+\left(\gamma+\alpha\beta+\alpha^3\right)y_2\\ &= 0.\end{aligned}$$

Plugging $y_0=y_1\alpha+y_2\alpha^2$ into the above equation and simplifying it, we obtain $(\gamma+\alpha\beta)y_2=0$ and then $y_2=0$ since $\gamma+\alpha\beta\neq 0$. Thus

$$\ker(L_b)=\left\{(\alpha+b)\eta:\eta\in\mathbb{F}_{2^m}\right\}.$$

Clearly, in this case, the dimension of $\ker(L_b)$ is m. Moreover, for $x\in\ker(L_b)$,

$$\begin{aligned}&\mathrm{Tr}_n(ax+bf(x))\\ =\ &\mathrm{Tr}_n\left(b(x\mathrm{Tr}_m^n(x)^2+x^4)+ax\right)=\mathrm{Tr}_n((b+a^4)x^4)\\ =\ &\mathrm{Tr}_n\left((b+a^4)(\alpha+b)^4\eta^4\right)\\ =\ &\mathrm{Tr}_m\left(\mathrm{Tr}_m^n\left((b+a^4)(\alpha+b)^4\right)\eta^4\right).\end{aligned}$$

Obviously, if $a^4=b$, the restriction of $\mathrm{Tr}_n(ax+bf(x))$ on $\ker(L_b)$ is the all-zero mapping and thus $W_f(a,b)=\pm 2^{\frac{n+m}{2}}$.

Moreover, if $a=0$, then we have $\mathrm{Tr}_n(bf(x))=\mathrm{Tr}_m\left(\mathrm{Tr}_m^n\left(b(\alpha+b)^4\right)\eta^4\right)=\mathrm{Tr}_m\left(U_b\eta^4\right)$, where

$$U_b=\mathrm{Tr}_m^n(b(\alpha^4+b^4))=\alpha^5+b^5+b^{5\cdot 2^m}+b^{5\cdot 2^{2m}}.$$

In the following, we will show that $U_b\neq 0$ for any $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. If there exists some $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ such that $U_b=0$, then by simplifying it, we get

$$(b+b^{2^m})(b+b^{2^{2m}})(b^{2^m}+b^{2^{2m}})\left(\alpha^2+\beta\right)=0,$$

which is impossible since $b\notin\mathbb{F}_{2^m}$ and $\alpha^2+\beta\neq 0$. Thus for any $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, $U_b\neq 0$ and then the restriction of $\mathrm{Tr}_n(bf(x))$ on $\ker(L_b)$ cannot be the all-zero mapping. Thus $W_f(b)=0$.

In conclusion, for any $a, b \in \mathbb{F}_{2^n}$,

$$W_f(a,b) \in \left\{0, 2^n, \pm 2^{\frac{n+2m+1}{2}}, \pm 2^{\frac{n+m}{2}}\right\}.$$

However, for any $b \in \mathbb{F}_{2^n}$,

$$W_f(b) \in \left\{0, 2^n, \pm 2^{\frac{n+2m+1}{2}}\right\}.$$

Next, we consider the parameters of $\mathcal{C}_f$ and $\mathcal{C}_{D(f)}$, respectively.

(1) For the linear code $\mathcal{C}_f$, since $W_f(a,b) = 2^n$ if and only if $(a,b) = (0,0)$, by (3), the dimension of $\mathcal{C}_f$ is $2n$. Moreover, since for any $a, b \in \mathbb{F}_{2^n}$, $W_f(a,b) \in \left\{0, 2^n, \pm 2^{\frac{n+2m+1}{2}}, \pm 2^{\frac{n+m}{2}}\right\}$, by (4), the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_f$ satisfy

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_b) \in \Big\{&2^{n-1} - 2^{\frac{n+2m-1}{2}}, 2^{n-1} + 2^{\frac{n+2m-1}{2}},\\ &2^{n-1} - 2^{\frac{n+m-2}{2}}, 2^{n-1} + 2^{\frac{n+m-2}{2}}, 2^{n-1}, 0\Big\}.\end{aligned}$$

(2) For the linear code $\mathcal{C}_{D(f)}$, $W_f(b) = 2^n$ if and only if $b = 0$, which means that the dimension of $\mathcal{C}_{D(f)}$ is n according to (7). Since for any $b \in \mathbb{F}_{2^n}$, $W_f(b) \in \left\{0, 2^n, \pm 2^{\frac{n+2m+1}{2}}\right\}$, by (8), the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy

$$\mathrm{wt}(\mathbf{c}_b) \in \left\{2^{n-2}, 0, 2^{n-2} - 2^{\frac{n+2m-3}{2}}, 2^{n-2} + 2^{\frac{n+2m-3}{2}}\right\}.$$

In the following, we determine the weight distribution of $\mathcal{C}_{D(f)}$. Define

$$\mathrm{w}_1 = 2^{n-2} - 2^{\frac{n+2m-3}{2}},\ \mathrm{w}_2 = 2^{n-2},\ \mathrm{w}_3 = 2^{n-2} + 2^{\frac{n+2m-3}{2}}.$$

Then solving (10) gives the desired weight distribution. □

Remark 1. In Theorems 5 - 6, the linear codes $\mathcal{C}_{D(f)}$ has the same parameters as the shortened Hadamard codes, which are locally decodable codes that provide a way to recover parts of the original message with high probability, while only looking at a small fraction of the received word. This property gives rise to applications in the computational complexity theory and in the CDMA communication system. The dual codes of $\mathcal{C}_{D(f)}$ are the binary Hamming codes with parameters $[2^{n-1} - 1, 2^{n-1} - n, 3]$.

Remark 2. In [21] there are several other classes of two-to-one quadratic polynomials. The experimental results show that we can obtain 3-weight or 5-weight binary linear codes as well from generalized quadratic polynomials. Due to the similarities of the parameters of those codes and the proofs, we choose some representatives of them that are more difficult and omitted the others in this paper. In addition, the linear code $\mathcal{C}_f$ in Theorem 3 appears to be a 3-weight code by numerical results. Nevertheless, we did not manage to prove it by the techniques used in this paper. We cordially invite interested readers to determine the weight distribution of the linear codes $\mathcal{C}_f$ in Theorem 3 and Theorem 10.

Problem 1. *Determine the weight distributions of the linear codes $\mathcal{C}_f$ in Theorem 3 and Theorem 10.*

According to the experimental results, we also have the following open problem.

Problem 2. *Let $n = 2m + 1$ and $f(x) = x^{3 \cdot 2^{m+1}} + x^{2^{m+2}+1} + x^{2^{m+1}+1} + x$. Prove that $f(x)$ is two-to-one over $\mathbb{F}_{2^n}$. Moreover, when $m \geq 4$, show that the linear code $\mathcal{C}_{D(f)}$ has the parameters $\left[2^{n-1} - 1, n, 2^{n-1} - 2^{\frac{n-1}{2}}\right]$ and the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy*

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_b) \in \Big\{&2^{n-2} - 2^{\frac{n-3}{2}}, 2^{n-2} + 2^{\frac{n-3}{2}},\\ &2^{n-2} - 2^{\frac{n-1}{2}}, 2^{n-2} + 2^{\frac{n-1}{2}}, 2^{n-2}, 0\Big\}.\end{aligned}$$

Determine the weight distribution of the linear code $\mathcal{C}_{D(f)}$.

V. Binary linear codes from $(x^{2^t} + x)^e$

The function $(x^{2^t} + x)^e$ with $\gcd(t, n) = \gcd(e, 2^n - 1) = 1$ is a two-to-one function from $\mathbb{F}_{2^n}$ to itself. In this section, we construct binary linear codes from two-to-one functions of this form.

Recall that given a two-to-one function f, the parameters of the linear codes $\mathcal{C}_{D(f)}$ in (6) depend on the investigation of the value $W_f(b)$. We first present an interesting relation on $W_f(b)$ for $f(x) = (x^{2^t} + x)^e$ and the Walsh transform of $\mathrm{Tr}_n(x^e)$. Indeed, we consider the relation for functions of a general form $f(x) = P(\psi(x))$, where P is a permutation polynomial over $\mathbb{F}_{2^n}$ and $\psi(x)$ is two-to-one with $\mathrm{Im}(\psi) = \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(y) = 0\}$.

Proposition 1. *Let $f(x) = P(\psi(x))$, where P is a permutation polynomial over $\mathbb{F}_{2^n}$ and $\psi(x)$ is two-to-one with $\mathrm{Im}(\psi) = \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(y) = 0\}$. Then for any $b \in \mathbb{F}_{2^n}^*$,*

$$W_f(b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bP(x)+x)}.$$

Proof. Let $T_0 = \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(y) = 0\}$. Take an element $a \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_n(a) = 1$. Then $T_1 := \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(y) = 1\} = \{a + y : y \in T_0\}$. For any $b \in \mathbb{F}_{2^n}^*$, the fact $\sum_{y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bP(y))} = 0$ implies

$$\begin{aligned}\sum_{y \in T_0} (-1)^{\mathrm{Tr}_n(bP(y))} &= -\sum_{y \in T_1} (-1)^{\mathrm{Tr}_n(bP(y))}\\ &= \sum_{y \in T_0} (-1)^{\mathrm{Tr}_n(bP(y+a)+a)}.\end{aligned}$$

TABLE X
KNOWN ALMOST BENT POWER FUNCTIONS x^e OVER $\mathbb{F}_{2^n}$, n ODD

Functions	e	Conditions	References
Gold	2^i+1	$\gcd(i,n)=1$	[30, 31]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	[32]
Welch	2^m+3	$n=2m+1$	[33, 34]
Niho-1	$2^m+2^{\frac{m}{2}}-1$	$n=2m+1$, m even	[34]
Niho-2	$2^m+2^{\frac{3m+1}{2}}-1$	$n=2m+1$, m odd	[34]

Thus,

$$\begin{aligned}W_f(b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bP(\psi(x)))} = 2\sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y))}\\ &= \sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y))} + \sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y+a)+a)}\\ &= \sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y)+y)} + \sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y+a)+y+a)}\\ &= \sum_{y\in T_0} (-1)^{\mathrm{Tr}_n(bP(y)+y)} + \sum_{y\in T_1} (-1)^{\mathrm{Tr}_n(bP(y)+y)}\\ &= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bP(y)+y)}.\end{aligned}$$

□

Remark 3. It is well-known that given an integer e with $\gcd(e, 2^n-1)=1$, the calculations of the weight distribution of $\mathcal{C}_f$ with $f(x)=x^e$, the Walsh spectrum of x^e, the cross-correlation distribution of m-sequences, and their e-decimated sequences are equivalent. The relation has provided a great amount of interesting results which originated from cryptography, coding theory, and sequence design. Proposition 1 exhibits a similar relation, which indicates the equivalence between the computation of the weight distribution of $C_{D(f)}$ for $f(x)=\left(x^{2^t}+x\right)^e$ and the Walsh spectrum of $\mathrm{Tr}_n(x^e)$. In other words, any power function x^e, $\gcd(e,2^n-1)=1$, with t-valued Walsh spectrum can be employed to construct linear codes $\mathcal{C}_{D(f)}$ with t nonzero weights.

Recently Li and Zeng in [29] surveyed the exponents e that allow for 3-valued, 4-valued, 5-valued Walsh spectra of x^e. All the exponents e listed in [29] with $\gcd(e,2^n-1)=1$ can be employed to generate binary linear codes $C_{D(f)}$ with few weights.

For simplicity, we let $\psi(x)=x^{2^t}+x$ with $\gcd(t,n)=1$ and only provide the result from almost bent monomials over $\mathbb{F}_{2^n}$ with n odd, which has three-valued Walsh spectrum $\left\{0,\pm 2^{\frac{n+1}{2}}\right\}$ [35]. The known almost bent exponents e is listed in Table X. From Proposition 1, we have the following theorem on the linear codes $\mathcal{C}_{D(f)}$.

TABLE XI
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_{D(f)}$ IN THEOREM 11

Weight	Multiplicity
0	1
$2^{n-2}-2^{m-1}$	$2^{n-2}+2^{m-1}$
2^{n-2}	$2^{n-1}-1$
$2^{n-2}+2^{m-1}$	$2^{n-2}-2^{m-1}$

Theorem 11. *Let $n=2m+1$, $f(x)=(x^{2^t}+x)^e$ with $\gcd(t,n)=1$ and e being one of the almost bent exponents in Table X. Let $\mathcal{C}_{D(f)}$ is defined as in* (6)*. Then $\mathcal{C}_{D(f)}$ is a $\left[2^{n-1}-1,n\right]$ binary linear code with weight distribution in Table XI.*

Proof. From Proposition 1 and the almost bent property of x^e, we know that for $b\in\mathbb{F}_{2^n}^*$,

$$W_f(b)\in\left\{0,\pm 2^{\frac{n+1}{2}}\right\}.$$

Moreover, it is clear that $W_f(b)=2^n$ if and only if $b=0$, which means that the dimension of $\mathcal{C}_{D(f)}$ is n according to (7). Furthermore, by (8), the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_{D(f)}$ satisfy

$$\mathrm{wt}(\mathbf{c}_b)\in\left\{2^{n-2},0,2^{n-2}-2^{\frac{n-3}{2}},2^{n-2}+2^{\frac{n-3}{2}}\right\}.$$

Finally, define

$$\mathrm{w}_1=2^{n-2}-2^{\frac{n-3}{2}},\quad \mathrm{w}_2=2^{n-2},\quad \mathrm{w}_3=2^{n-2}+2^{\frac{n-3}{2}}.$$

Then solving (10) gives the desired weight distribution. □

As for the linear codes $\mathcal{C}_f$ defined as in (2), it seems hard to compute the Walsh transform $W_f(a,b)$ for any $a,b\in\mathbb{F}_{2^n}$. However, for the Gold function, we manage to determine its possible values. The proof is also easily obtained by the Walsh spectrum of the Gold function and thus we omit it here.

Theorem 12. *Let $n=2m+1$ and i be a positive integer with $\gcd(i,n)=1$. Let $f(x)=\left(x^{2^t}+x\right)^{2^i+1}$ with $\gcd(t,n)=1$. Define the linear code $\mathcal{C}_f$ as in* (2)*. Then, $\mathcal{C}_f$ is a $[2^n-1,2n]$ binary code with five weights. Moreover, the weights of the codewords $\mathbf{c}_b$ in $\mathcal{C}_f$ satisfy*

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_b)\in\Big\{&2^{n-1}-2^{\frac{n-1}{2}},2^{n-1}+2^{\frac{n-1}{2}},\\ &2^{n-1}-2^{\frac{n+1}{2}},2^{n-1}+2^{\frac{n+1}{2}},2^{n-1},0\Big\}.\end{aligned}$$

Moreover, according to the experimental results, we have the following open problem.

Problem 3. *Let $n = 2m + 1$ and e be the almost bent exponents as given in Table X. Let $f(x) = (x^{2^t} + x)^e$ with $\gcd(t, n) = 1$. Define the linear codes $\mathcal{C}_f$ as in* (2)*. Prove that the parameters of the linear codes $\mathcal{C}_f$ are the same as that in Theorem 12. Determine the weight distributions of the linear codes $\mathcal{C}_f$.*

VI. Conclusion

Known good linear codes are constructed primarily by two generic approaches. In this paper, we studied binary linear codes produced from two-to-one functions by the two generic approaches. We considered the relations between the Hamming weights of codewords in the constructed codes and the Walsh transforms of the corresponding two-to-one functions, and particularly studied two-to-one functions with few-valued Walsh transforms. As a result, a large number of new binary codes with few weights were presented and the weight distributions of some of the obtained codes are determined based on power moment identities.

Acknowledgment

The authors would like to thank deeply the Associate Editors Prof. Claude Carlet, and the anonymous referees for their valuable comments and suggestions that highly improved both the technical and the editorial qualities of this paper, especially the proof of Theorem 2.

References

[1] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge university press, 2003.

[2] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2089–2102, 2005.

[3] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 206–212, 2005.

[4] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," *Theoretical computer science*, vol. 330, no. 1, pp. 81–99, 2005.

[5] A. Calderbank and J. Goethals, "Three-weight codes and association schemes," *Philips J. Res*, vol. 39, no. 4-5, pp. 143–152, 1984.

[6] R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bulletin of the London Mathematical Society*, vol. 18, no. 2, pp. 97–122, 1986.

[7] C. Ding, *Designs From Linear Codes*. World Scientific Publishing Company, 2018.

[8] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3," *IEEE Transactions on information theory*, vol. 53, no. 6, pp. 2274–2277, 2007.

[9] C. Ding, "A construction of binary linear codes from boolean functions," *Discrete Mathematics*, vol. 339, no. 9, pp. 2288 – 2303, 2016.

[10] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes (Corresp.)," *IEEE Transactions on Information Theory*, vol. 21, no. 5, pp. 575–576, 1975.

[11] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.

[12] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 613–627, 2006.

[13] C. Ding, "Linear codes from some 2-designs," *IEEE Transactions on information theory*, vol. 61, no. 6, pp. 3265–3275, 2015.

[14] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 5835–5842, 2015.

[15] Z. Heng, Q. Yue, and C. Li, "Three classes of linear codes with two or three weights," *Discrete Mathematics*, vol. 339, no. 11, pp. 2832–2847, 2016.

[16] Z. Zhou, N. Li, C. Fan, and T. Helleseth, "Linear codes with two or three weights from quadratic bent functions," *Designs, Codes and Cryptography*, vol. 81, no. 2, pp. 283–295, 2016.

[17] C. Tang, N. Li, Y. Qi, Z. Zhou, and T. Helleseth, "Linear codes with two or three weights from weakly regular bent functions," *IEEE Transactions on Information Theory*, vol. 62, no. 3, pp. 1166–1176, 2016.

[18] S. Mesnager, "Linear codes with few weights from weakly regular bent functions based on a generic construction," *Cryptography and Communications*, vol. 9, no. 1, pp. 71–84, 2017.

[19] S. Mesnager and A. Sınak, "Several classes of minimal linear codes with few weights from weakly regular plateaued functions," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2296–2310, 2019.

[20] Y. Wu, N. Li, and X. Zeng, "Linear codes with few weights from cyclotomic classes and weakly regular bent functions," *Designs, Codes and Cryptography*, pp. 1–18, 2020.

[21] N. Li and S. Mesnager, "Recent results and prob-

lems on constructions of linear codes from cryptographic functions," *Cryptography and Communications*, vol. 12, no. 5, pp. 965–986, 2020.

[22] S. Mesnager and L. Qu, "On two-to-one mappings over finite fields," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 7884–7895, 2019.

[23] K. Li, S. Mesnager, and L. Qu, "Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$," *IEEE Transactions on Information Theory*, 10.1109/TIT.2021.3057094, 2021.

[24] C. Ding, "A construction of binary linear codes from Boolean functions," *Discrete mathematics*, vol. 339, no. 9, pp. 2288–2303, 2016.

[25] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[26] K. S. Williams, "Note on cubics over $\mathrm{GF}(2^n)$ and $\mathrm{GF}(3^n)$," *Journal of Number Theory*, vol. 7, no. 4, pp. 361–365, 1975.

[27] P. A. Leonard and K. S. Williams, "Quartics over $\mathrm{GF}(2^n)$," *Proceedings of the American Mathematical Society*, pp. 347–350, 1972.

[28] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2020-06-16.

[29] N. Li and X. Zeng, "A survey on the applications of niho exponents," *Cryptography and Communications*, vol. 11, no. 3, pp. 509–548, may 2018.

[30] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)," *IEEE transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[31] K. Nyberg, "Differentially uniform mappings for cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 55–64.

[32] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes," *Information and Control*, vol. 18, no. 4, pp. 369–394, 1971.

[33] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 4–8, 2000.

[34] H. D. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences," *Finite Fields and Their Applications*, vol. 7, no. 2, pp. 253–286, 2001.

[35] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1994, pp. 356–365.

Kangquan Li is currently a Ph.D. student with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China. His research interests are cryptography and coding theory.

Chunlei Li (Member, IEEE) received the Ph.D. degree from the University of Bergen, Norway in 2014. He was a postdoc at the University of Stavanger, Norway, during 2015-2017, and a researcher at the University of Bergen during 2017-2018. Since 2018, he has been an associate professor with the Department of Informatics, University of Bergen. His research interests include sequence design, coding theory and crpytography. He was the program co-chair of the workshops Mathematical Methods for Cryptography, 2017, Sequences and Their Applications, 2020, and severed as a program committee member of several workshops including WAIFI18, SETA18, IWSDA19 and IWSDA21.

Tor Helleseth (Fellow, IEEE) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973 to 1980, he was a Research Assistant with the Department of Mathematics, University of Bergen. From 1981 to 1984, he was with the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor with the Department of Informatics, University of Bergen. During the academic years of 1977 to 1978 and 1992 to 1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and from 1979 to 1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology. In 2004, he was also elected as a member of Det Norske Videnskaps-Akademi. He was the Program Chairman of Eurocrypt'93 and of the Information Theory Workshop, Longyearbyen, Norway, in 1997. He was the Program Co-Chairman of SETA04, Seoul, South Korea, of SETA06, Beijing, China, of SETA18, Hong Kong, China, and of SETA20, Saint-Petersburg, Russia. He was also the Program Co-Chairman of the IEEE Information Theory Workshop, Solstrand, Norway, in 2007. From 2007 to 2009, he served on the Board of Governors of the IEEE Information Theory Society. He served as an Associate Editor for coding theory for the IEEE Transactions on Information Theory from 1991 to 1993. In 1997, he was elected as a Fellow of the IEEE for his contributions to coding theory and cryptography.

Longjiang Qu received his B.A. degree in 2002 and Ph.D. degree in 2007 in mathematics from the National University of Defense Technology, Changsha, China. He is now a Professor with the College of Liberal Arts and Sciences, National University of Defense Technology of China. His research interests are cryptography and coding theory.