Some punctured codes of several families of binary linear codes

Xiaoqiang Wang, Dabin Zheng[*], Cunsheng Ding

Abstract. Two general constructions of linear codes with functions over finite fields have been extensively studied in the literature. The first one is given by $\mathcal{C}(f) = \left\{ \mathrm{Tr}(af(x) + bx)_{x \in \mathbb{F}_{q^m}^*} : a, b \in \mathbb{F}_{q^m} \right\}$, where q is a prime power, $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$, Tr is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and $f(x)$ is a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$ with $f(0) = 0$. Almost bent functions, quadratic functions and some monomials on $\mathbb{F}_{2^m}$ were used in the first construction, and many families of binary linear codes with few weights were obtained in the literature. This paper studies some punctured codes of these binary codes. Several families of binary linear codes with few weights and new parameters are obtained in this paper. Several families of distance-optimal binary linear codes with new parameters are also produced in this paper.

Keywords. Boolean function, linear code, punctured code, distance-optimal code, weight distribution

2010 Mathematics Subject Classification. 94B05, 94B15

1 Introduction of motivations, objectives, and methodology

Let q be a prime power and n be a positive integer. An $[n, k, d]$ code $\mathcal{C}$ over the finite field $\mathbb{F}_q$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. The dual code, denoted by $\mathcal{C}^\perp$, of $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \left\{ \mathbf{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n : \sum_{i=0}^{n-1} x_i c_i = 0 \ \forall \ \mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C} \right\}.$$

The minimum distance of $\mathcal{C}^\perp$, denoted by $d^\perp$, is called the dual distance of $\mathcal{C}$. $\mathcal{C}$ is called a projective code if its dual distance is at least 3. An $[n, k, d]$ code over $\mathbb{F}_q$ is said to be *distance-optimal* (respectively, *dimension-optimal* and *length-optimal*) if there is no $[n, k, d' \geq d + 1]$ (respectively, $[n, k' \geq k + 1, d]$ and $[n' \leq n - 1, k, d]$) linear code over $\mathbb{F}_q$. An optimal code is a code that is length-optimal, or dimension-optimal, or distance-optimal, or meets a bound for linear codes. A

binary linear code $\mathcal{C}$ is called *self-complementary* if it contains the all-one vector. Let A_i denote the number of codewords with Hamming weight i in $\mathcal{C}$. The *weight enumerator* of $\mathcal{C}$ is defined by $1 + A_1 x + A_2 x^2 + \cdots + A_n x^n$. The *weight distribution* of $\mathcal{C}$ is defined by the sequence $(1, A_1, \cdots, A_n)$. If the number of nonzero A_i in the sequence $(A_1, \cdots, A_n)$ is t, then the code $\mathcal{C}$ is said to be a t-weight code. By the parameters of a code, we mean its length, dimension and minimum distance.

Coding theory has important applications in communications systems, data storage systems, consumer electronics, and cryptography. In addition, coding theory is closely related to many areas of mathematics, such as algebra, algebraic geometry, algebraic function fields, algebraic number theory, association schemes, combinatorics, finite fields, finite geometry, graph theory, and group theory. These are the major motivations of studying coding theory. Constructing linear codes with desired parameters and weight distributions has been an important task in the history of coding theory. Linear codes may be constructed directly with algebraic approaches, combinatorial approaches and other approaches. Alternatively, almost all linear codes over finite fields can be constructed from some known codes by the puncturing or shortening techniques.

Let $\mathcal{C}$ be an $[n, k, d]$ code over $\mathbb{F}_q$, and let T be a set of t coordinate positions in $\mathcal{C}$. We puncture $\mathcal{C}$ by deleting all the coordinates in T in each codeword of $\mathcal{C}$. The resulting code is still linear and has length $n - t$, where $t = |T|$. We denote the punctured code by $\mathcal{C}^T$. Let $\mathcal{C}(T)$ be the set of codewords which are 0 on T. Then $\mathcal{C}(T)$ is a subcode of $\mathcal{C}$. We now puncture $\mathcal{C}(T)$ on T, and obtain a linear code over $\mathbb{F}_q$ with length $n - t$, which is called a *shortened code* of $\mathcal{C}$, and is denoted by $\mathcal{C}_T$. The puncturing and shortening techniques are two very important tools for constructing new codes from old ones. It was shown that every projective linear code over $\mathbb{F}_q$ (i.e., the minimum distance of the dual code is at least 3) is a punctured code of a Simplex code over $\mathbb{F}_q$ and a shortened code of a Hamming code over $\mathbb{F}_q$ [37]. These facts justify the importance of the Simplex codes and the Hamming codes as well as the puncturing and shortening techniques. Note that the Simplex codes are optimal with respect to the Griesmer bound. Since every projective code is a punctured Simplex code, a punctured code of an optimal linear code may have good or bad parameters. To obtain a very good punctured code $\mathcal{C}^T$ from a good or optimal linear code $\mathcal{C}$, one has to choose a proper set T of coordinate positions in $\mathcal{C}$. This is the difficulty of using the puncturing technique to construct new linear codes with good parameters from old ones [37, 56]. In this paper, we will use the puncturing technique to construct new codes with interesting and new parameters from some old linear codes.

Linear codes with few weights have applications in secret sharing [1], strongly regular graphs [5], association schemes [4] and authentication codes [17]. In finite geometry, hyperovals in the projective geometry $\mathrm{PG}(2, 2^m)$ are the same as $[2^m + 2, 3, 2^m]$ MDS codes with two weights [13, Chapter 12], maximal arcs in $\mathrm{PG}(2, 2^m)$ are the same as a special type of two-weight codes [13, Chapter 12], and ovoids in $\mathrm{PG}(3, q)$ are the same as a special type of two-weight codes [13, Chapter 13]. Many families of linear codes have been used to construct combinatorial t-designs [13, Chapters 5–13]. These are some of the motivations of studying linear codes with few weights in the literature. In the past two decades, a lot of progress on the construction of linear codes with few weights has been made. The reader is referred to [11, 12, 16, 18, 24, 34, 38, 43, 44, 46, 47, 50–52, 54, 60] and the references therein for information. One of the objectives of this paper is to construct binary linear codes with few weights.

Functions and linear codes are closely connected. In the literature two general constructions of linear codes with functions over finite fields have been intensively investigated [12]. The first

construction is given by

$$\mathcal{C}(f) = \left\{ \mathrm{Tr}(af(x) + bx)_{x \in \mathbb{F}_{q^m}^*} \; : \; a, b \in \mathbb{F}_{q^m} \right\}, \tag{1}$$

where q is a prime power, $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$, Tr is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and $f(x)$ is a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$ with $f(0) = 0$. It is clear that $\mathcal{C}(f)$ is a linear code with length $q^m - 1$ and dimension at most $2m$. If $f(x)$ is a monomial, then $\mathcal{C}(f)$ is permutation-equivalent to a cyclic code [7]. This general construction has a long history and its importance is supported by Delsarte's Theorem [10]. The weight distribution of $\mathcal{C}(f)$ is closely related to the value distributions of certain exponential sums, and is difficult to settle in general. In order to determine the weight distribution of $\mathcal{C}(f)$, people usually choose $f(x)$ to be a special function such as a quadratic function, PN function, and APN function. Many good and optimal linear codes have been obtained with this construction. This is also a main method for constructing linear codes with few weights. The reader is referred to, for example, [7, 20, 26, 33, 39, 43, 51, 57] for information.

The second general construction of linear codes is described as follows [16, 53]. Let $D = \{d_1, d_2, \cdots, d_n\} \subset \mathbb{F}_{q^m}^*$ be a multiset. Define a linear code

$$\mathcal{C}_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \cdots, \mathrm{Tr}(xd_n)) : x \in \mathbb{F}_{q^m}\},$$

where q is a prime power, Tr is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. The code $\mathcal{C}_D$ over $\mathbb{F}_q$ has length n and dimension at most m, where D is called the defining set of $\mathcal{C}_D$. This construction is fundamental in the sense that every linear code over $\mathbb{F}_q$ can be expressed as $\mathcal{C}_D$ for some positive integer m and some subset D of $\mathbb{F}_{q^m}$ [23, 55]. It is known that this construction is equivalent to the generator matrix construction of linear codes. The code $\mathcal{C}_D$ may have good parameters if the defining set is properly chosen. With the second general construction, many good linear codes with few weights have been constructed [11, 15, 19, 24, 25, 34, 36, 38, 43, 50, 52]. With some variants of the second construction, interesting linear codes were obtained in [32, 34, 48].

By the definition of the second construction above, $\mathcal{C}_{\mathbb{F}_{q^m}^*}$ has parameters $[q^m - 1, m, (q-1)q^{m-1}]$ and weight enumerator $1 + (q^m - 1)z^{(q-1)q^{m-1}}$. If $D \subset \mathbb{F}_{q^m}^*$ does not contain repeated elements, let $\bar{D} = \mathbb{F}_{q^m}^* \setminus D$. In this case, we have $\mathcal{C}_D = (\mathcal{C}_{\mathbb{F}_{q^m}^*})^{\bar{D}}$, where the coordinate positions in $\mathcal{C}_{\mathbb{F}_{q^m}^*}$ are indexed by the elements in $\mathbb{F}_{q^m}^*$. This means that $\mathcal{C}_D$ is in fact a punctured code of the one-weight code $\mathcal{C}_{\mathbb{F}_{q^m}^*}$, which is a concatenation of $(q-1)$ Simplex codes over $\mathbb{F}_q$ with the same parameters. Hence, the second construction above is in fact a puncture construction, and every projective linear code over $\mathbb{F}_q$ is a punctured code of the one-weight code $\mathcal{C}_{\mathbb{F}_{q^m}^*}$.

Motivated by the power of the puncture technique and the first construction, in this paper we study some punctured codes of several families of binary linear codes $\mathcal{C}(f)$ from special functions on $\mathbb{F}_{2^m}$. Specifically, we will study the following punctured codes.

Let f be a function on $\mathbb{F}_{2^m}$ with $f(0) = 0$, and let $D = \{d_1, d_2, \cdots, d_n\} \subset \mathbb{F}_{2^m}^*$ that does not contain any repeated elements. Define $\bar{D} = \mathbb{F}_{2^m}^* \setminus D$. In this paper, we will study the punctured code

$$\mathcal{C}(f)^{\bar{D}} = \{\mathbf{c}(a, b) = (\mathrm{Tr}(af(d_1) + bd_1), \cdots, \mathrm{Tr}(af(d_n) + bd_n)) : a, b \in \mathbb{F}_{2^m}\}, \tag{2}$$

where Tr is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ and the binary code $\mathcal{C}(f)$ was defined in (1). We call the set D the *position set* of the code $\mathcal{C}(f)^{\bar{D}}$, as we index the coordinate positions of the code $\mathcal{C}(f)$ with the elements in $\mathbb{F}_{2^m}^*$. The dimension of $\mathcal{C}(f)^{\bar{D}}$ is at most $2m$. The two objectives of this paper

3

are to obtain binary linear codes $\mathcal{C}(f)^{\bar{D}}$ with new parameters and few weights and $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ with new and good parameters. To this end, we have to select f and the position set D carefully.

Concretely, we first choose the position set to be

$$D = \{x \in \mathbb{F}_{2^m}^* \ : \ \mathrm{Tr}(\lambda f(x)) = \nu\} \tag{3}$$

and determine the weight distributions of $\mathcal{C}(f)^{\bar{D}}$, where $\nu \in \{0,1\}$, $\lambda \in \mathbb{F}_{2^m}^*$ and $f(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. We show that $\mathcal{C}(f)^{\bar{D}}$ is a five-weight code if $\nu = 0$ and a self-complementary six-weight code if $\nu = 1$. Some of the codes $\mathcal{C}(f)^{\bar{D}}$ are optimal according to the tables of best codes known in [22]. The dual of $\mathcal{C}(f)^{\bar{D}}$ is distance-optimal with respect to the sphere packing bound if $\nu = 1$. We then present several classes of four-weight or six-weight linear codes by choosing $f(x)$ to be some special quadratic functions, and the position set to be the *support* of $\mathrm{Tr}(x)$, i.e.,

$$D = \{x \in \mathbb{F}_{2^m}^* \ : \ \mathrm{Tr}(x) = 1\}. \tag{4}$$

Several families of complementary binary linear codes are obtained. The parameters of the duals of $\mathcal{C}(f)^{\bar{D}}$ are also determined and almost all of them are distance-optimal with respect to the sphere packing bound. Finally, we present several classes of binary linear codes with three weights, or five weights or six weights by selecting the position sets to be some cyclotomic classes. Some of the codes and their duals are distance-optimal. The parameters of most of the codes presented in this paper are new.

The rest of this paper is organized as follows. Section 2 introduces some preliminaries. Section 3 investigates the weight distribution of the linear code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual, where $f(x)$ is an almost bent function, $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}(\lambda f(x)) = \nu\}$, $\nu \in \{0,1\}$ and $\lambda \in \mathbb{F}_{2^m}^*$. Section 4 determines the weight distribution of the linear code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual, where $f(x)$ is some special quadratic function and $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}(x) = 1\}$. Section 5 settles the weight distribution of the linear code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual, where D is a cyclotomic class and f is a monomial. Section 6 concludes this paper.

2 Preliminaries

In this section, we introduce some special functions on $\mathbb{F}_{2^m}$, some exponential sums and some basic results in coding theory, which will be used later in this paper.

2.1 Notation used starting from now on

Starting from now on, we assume $m \geq 4$ and adopt the following notation unless otherwise stated:

- $\mathbb{F}_{2^m}$ is the finite field with 2^m elements and γ is a primitive element of $\mathbb{F}_{2^m}$.

- $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$.

- $\mathrm{Tr}(\cdot)$ is the absolute trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

- $\mathrm{Tr}_u^v(\cdot)$ is the trace function from $\mathbb{F}_{2^v}$ to $\mathbb{F}_{2^u}$, where u, v are positive integers such that $u \mid v$.

- $v_2(\cdot)$ is the 2-adic order function with $v_2(0) = \infty$.

- $\text{wt}_H(\mathbf{c})$ denotes the Hamming weight of a vector $\mathbf{c}$.

- $d_H(\mathcal{C})$ denotes the minimum distance of a linear code $\mathcal{C}$.

2.2 AB and APN functions

Let $f(x)$ be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. The *Walsh transform* of $f(x)$ at $(a,b) \in \mathbb{F}_{2^m}^2$ is defined as

$$W_f(a,b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(af(x)+bx)}. \tag{5}$$

If $W_f(a,b) = 0$ or $\pm 2^{\frac{m+1}{2}}$ for any pair $(a,b) \in \mathbb{F}_{2^m}^2$ with $a \neq 0$, then $f(x)$ is called an *almost bent (AB) function*. Almost bent functions exist only for odd m. Define

$$\delta_f(a,b) = \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}} |\{x \in \mathbb{F}_{2^m} : f(x+a) + f(x) = b\}|,$$

then $f(x)$ is called an *almost perfect nonlinear (APN) function* if $\delta_f(a,b) = 2$.

APN and AB functions have applications in coding theory, combinatorics, cryptography, finite geometry and sequence design. Many good linear codes over finite fields have been constructed with APN and AB functions [6, 11, 12, 33, 43]. AB functions and APN functions have the following relationship.

Lemma 2.1 *[3] Let $\mathbb{F}_{2^m}$ be a finite field with 2^m elements. If $f(x)$ is an almost bent function over $\mathbb{F}_{2^m}$, then $f(x)$ is an almost perfect nonlinear function over $\mathbb{F}_{2^m}$.*

The converse is not true for Lemma 2.1, as almost bent functions exist only for m being odd while almost perfect nonlinear functions exist for m being even too.

2.3 Quadratic functions

By identifying the finite field $\mathbb{F}_{2^m}$ with the m-dimensional vector space $\mathbb{F}_2^m$ over $\mathbb{F}_2$, a function f from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ can be viewed as an m-variable polynomial over $\mathbb{F}_2$. In the sequel, we fix a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and identify $x \in \mathbb{F}_{2^m}$ with a vector $(x_1, x_2, \cdots, x_m) \in \mathbb{F}_2^m$, a quadratic function over $\mathbb{F}_2$ is of the form:

$$Q(x_1, x_2, \cdots, x_m) = (x_1, x_2, \cdots, x_m) A (x_1, x_2, \cdots, x_m)^T,$$

where $A = (a_{ij})_{m \times m}$, $a_{ij} \in \mathbb{F}_2$, is an upper triangular matrix. The matrix $A + A^T$ is called an alternate matrix and its rank must be even [49]. By the theory of linear equations, the rank r of the matrix $A + A^T$ is equal to the codimension of the $\mathbb{F}_2$-linear subspace

$$V = \{x \in \mathbb{F}_{2^m} : Q(x+z) + Q(x) + Q(z) = 0 \text{ for all } z \in \mathbb{F}_{2^m}\}, \tag{6}$$

i.e. $r = m - \dim_{\mathbb{F}_2} V$. Let $G(x)$ be a linear polynomial over $\mathbb{F}_{2^m}$, then

$$\left(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(x)+G(x))}\right)^2 = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(x)+G(x))} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(y)+G(y))}$$

$$= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(x+y)+G(x+y)+Q(x)+G(x))}$$

$$= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(y)+G(y))} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(x+y)+Q(x)+Q(y))}$$

$$= 2^m \cdot \sum_{y\in V} (-1)^{\mathrm{Tr}(Q(y)+G(y))},$$

where V was defined in (6). It is easy to check that

$$\mathrm{Tr}\left(Q(x+y)+G(x+y)\right) = \mathrm{Tr}\left(Q(x)+G(x)\right) + \mathrm{Tr}\left(Q(y)+G(y)\right)$$

for any $x, y \in V$. Then

$$\left(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Q(x)+G(x))}\right)^2 = \begin{cases} 2^{m+r}, & \text{if } \mathrm{Tr}\left(Q(y)+G(y)\right) = 0 \text{ for all } y \in V, \\ 0, & \text{otherwise,} \end{cases} \tag{7}$$

where r is the rank of $Q(x)$ and $r = m - \dim_{\mathbb{F}_2} V$. The following are some well known results about quadratic forms, which will be needed in this paper.

Lemma 2.2 *[8, 9] Let m and k be non-negative integers with $v_2(m) \le v_2(k)$ and $a, b \in \mathbb{F}_{2^m}$ with $a \ne 0$. Let*

$$S(a,b) = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left(ax^{2^k+1}+bx\right)}, \tag{8}$$

then the possible values of $S(a,b)$ are in the set $\{0, \pm 2^{\frac{m+\ell}{2}}\}$, where $\ell = \gcd(m,k)$.

Lemma 2.3 *[8, 9] Let m and k be non-negative integers with $v_2(m) > v_2(k)$ and $a, b \in \mathbb{F}_{2^m}$ with $a \ne 0$. Let $S(a,b)$ be defined in (8). Then $S(a,b) = 0$ unless the equation $a^{2^k} x^{2^{2k}} + ax + b^{2^k} = 0$ is solvable. Let γ be a primitive element of $\mathbb{F}_{2^m}$. Let $\ell = \gcd(m,k)$. Assume $a^{2^k} x^{2^{2k}} + ax + b^{2^k} = 0$ is solvable. Then there are two possibilities as follows.*

(i) *If $a \ne \gamma^{s(2^\ell+1)}$ for any integer s, then the equation has a unique solution x_b for any $b \in \mathbb{F}_{2^m}$, and*

$$S(a,b) = (-1)^{\frac{m}{2\ell} - \mathrm{Tr}\left(ax_b^{2^k+1}\right)} 2^{\frac{m}{2}}.$$

(ii) *If $a = \gamma^{s(2^\ell+1)}$ for some integer s, then the equation is solvable if and only if $\mathrm{Tr}_{2\ell}^m(b\beta^{-s}) = 0$, where $\beta \in \mathbb{F}_{2^m}^*$ is the unique element satisfying $\beta^{\frac{2^k+1}{2^\ell+1}} = \gamma$. In such case,*

$$S(a,b) = -(-1)^{\frac{m}{2\ell} - \mathrm{Tr}\left(ax_b^{2^k+1}\right)} 2^{\frac{m}{2}+\ell},$$

where x_b is a solution to $a^{2^k} x^{2^{2k}} + ax + b^{2^k} = 0$.

6

Lemma 2.4 *[42] Let γ be a primitive element of $\mathbb{F}_{2^m}$. Assume that $m = 2sh$ and $\ell \mid (2^h + 1)$. Then*

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\gamma^i x^\ell)} = \begin{cases} (-1)^s 2^{\frac{m}{2}}, & \text{if } i \not\equiv 0 \pmod{\ell}, \\ (-1)^{s-1}(\ell - 1)2^{\frac{m}{2}}, & \text{if } i \equiv 0 \pmod{\ell}. \end{cases}$$

Lemma 2.5 *[40] Let $\ell = \gcd(\frac{m}{2}, k)$ and $\ell' = \gcd(\frac{m}{2} + k, 2k)$. Let*

$$S_1(a, b) = (-1)^{\mathrm{Tr}\left(ax^{2^k+1} + bx^{2^{\frac{m}{2}}+1}\right)}.$$

If $\ell' = 2\ell$ and (a, b) runs over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^{\frac{m}{2}}}$, then

$$S_1(a, b) = \begin{cases} 2^m, & \text{occuring } 1 \text{ time,} \\ -2^{\frac{m}{2}}, & \text{occuring } \frac{2^{3k}(2^{\frac{m}{2}}-1)(2^m - 2^{m-2k} - 2^{m-3k} + 2^{\frac{m}{2}} - 2^{\frac{m}{2}-k} + 1)}{(2^k+1)(2^{2k}-1)} \text{ times,} \\ 2^{\frac{m}{2}+k}, & \text{occuring } \frac{2^k(2^m-1)(2^m - 2^{m-\ell} + 2^{m-2\ell} + 1)}{(2^k+1)^2} \text{ times,} \\ -2^{\frac{m}{2}+2k}, & \text{occuring } \frac{(2^{\frac{m}{2}-\ell}-1)(2^m-1)}{(2^k+1)(2^{2k}-1)} \text{ times.} \end{cases}$$

2.4 Pless power moments and the sphere packing bound

To study the parameters of the duals of the punctured binary codes $\mathcal{C}(f)^{\bar{D}}$, we need the Pless power moments of linear codes. Let $\mathcal{C}$ be a binary $[n, k]$ code, and denote its dual by $\mathcal{C}^\perp$. Let A_i and $A_i^\perp$ be the number of codewords of weight i in $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively. The first five Pless power moments are the following [41, p. 131]:

$$\sum_{i=0}^{n} A_i = 2^k;$$

$$\sum_{i=0}^{n} i A_i = 2^{k-1}(n - A_1^\perp);$$

$$\sum_{i=0}^{n} i^2 A_i = 2^{k-2}[n(n+1) - 2nA_1^\perp + 2A_2^\perp];$$

$$\sum_{i=0}^{n} i^3 A_i = 2^{k-3}[n^2(n+3) - (3n^2 + 3n - 2)A_1^\perp + 6nA_2^\perp - 6A_3^\perp];$$

$$\sum_{i=0}^{n} i^4 A_i = 2^{k-4}[n(n+1)(n^2 + 5n - 2) - 4n(n^2 + 3n - 2)A_1^\perp + 4(3n^2 + 3n - 4)A_2^\perp - 24nA_3^\perp + 24A_4^\perp].$$

If $A_1^\perp = A_2^\perp = A_3^\perp = A_4^\perp = 0$, then the sixth Pless power moment becomes the following:

$$\sum_{i=0}^{n} i^5 A_i = 2^{k-5} \cdot n^5 + 5 \cdot 2^{k-4} \cdot n^4 + 15 \cdot 2^{k-5} \cdot n^3 - 5 \cdot 2^{k-4} \cdot n^2 - A_5^\perp \cdot 2^{k-5} \cdot 120.$$

We will need the following bound for binary linear codes later.

Lemma 2.6 (The sphere packing bound) *Let $\mathcal{C}$ be an $[n, k, d]$ binary code. Then*

$$2^n \geq 2^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}.$$

7

3 Some punctured codes of the binary codes from almost bent functions

Recall the code $\mathcal{C}(f)$ defined in (1). When $q = 2$ and $f(x) = x^{2^h+1}$ with $\gcd(h, m) = 1$ and m being odd, the parameters and weight distribution of the binary code $\mathcal{C}(f)$ were settled in [29, 30]. When $q = 2$, m is odd and $f(x)$ is an almost bent function on $\mathbb{F}_{2^m}$, the parameters and weight distribution of the binary code $\mathcal{C}(f)$ were settled in [6]. The binary code $\mathcal{C}(f)$ has parameters $[2^m - 1, 2m, 2^{m-1} - 2^{(m-1)/2}]$ and three nonzero weights [6]. Let $\mathcal{C}(f)^{\bar{D}}$ be the binary punctured code defined in (2) with position set D in (3), where $f(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. In this section, we investigate the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual. We first give the length of the linear code $\mathcal{C}(f)^{\bar{D}}$ in the following lemma.

Lemma 3.1 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (3), where $f(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. Then the length n of $\mathcal{C}(f)^{\bar{D}}$ is*

$$n = |D| = \begin{cases} 2^{m-1} - (-1)^\nu 2^{\frac{m-1}{2}} - 1 + \nu, & \text{if } W_f(\lambda, 0) = -2^{\frac{m+1}{2}}, \\ 2^{m-1} + (-1)^\nu 2^{\frac{m-1}{2}} - 1 + \nu, & \text{if } W_f(\lambda, 0) = 2^{\frac{m+1}{2}}, \\ 2^{m-1} - 1 + \nu, & \text{if } W_f(\lambda, 0) = 0, \end{cases}$$

where $W_f(\lambda, 0)$ was defined in (5) and $\nu \in \{0, 1\}$.

In order to apply the Pless power moments to determine the multiplicity of each Hamming weight of $\mathcal{C}(f)^{\bar{D}}$, we need to investigate the minimum Hamming distance of its dual.

Lemma 3.2 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (3), where $f(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. Then the dual distance is lower bounded by*

$$d_H\left(\left(\mathcal{C}(f)^{\bar{D}}\right)^\perp\right) \geq \begin{cases} 5, & \text{if } \nu = 0, \\ 6, & \text{if } \nu = 1. \end{cases}$$

Proof. It is easy to see $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) \geq 3$ from the definition of $\mathcal{C}(f)^{\bar{D}}$. Next, we show that $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) \neq 4$. The case of $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) \neq 3$ can be shown similarly, and we omit the details of the proof.

If $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) = 4$, then there are four pairwise-distinct elements x_1, x_2, x_3 and x_4 in $\mathbb{F}_{2^m}^*$ such that

$$\begin{cases} \mathrm{Tr}(\lambda f(x_1)) = \mathrm{Tr}(\lambda f(x_2)) = \mathrm{Tr}(\lambda f(x_3)) = \mathrm{Tr}(\lambda f(x_4)) = \nu, \\ a(x_1 + x_2 + x_3 + x_4) + b(f(x_1) + f(x_2) + f(x_3) + f(x_4)) = 0 \end{cases}$$

for any $a, b \in \mathbb{F}_{2^m}$. Then,

$$\begin{cases} \mathrm{Tr}(\lambda f(x_1)) = \mathrm{Tr}(\lambda f(x_2)) = \mathrm{Tr}(\lambda f(x_3)) = \mathrm{Tr}(\lambda f(x_4)) = \nu, \\ x_1 + x_2 + x_3 + x_4 = 0, \\ f(x_1) + f(x_2) + f(x_3) + f(x_4) = 0. \end{cases} \tag{9}$$

The second and third equations in (9) can be rewritten as

$$\begin{cases} x_1 + x_2 = \alpha \text{ and } x_3 + x_4 = \alpha, \\ f(x_1) + f(x_2) = \beta \text{ and } f(x_3) + f(x_4) = \beta, \end{cases}$$

where $\alpha, \beta \in \mathbb{F}_{2^m}$ with $\alpha \neq 0$. Hence, there are four different elements x_1, $x_1 + \alpha$, x_3 and $x_3 + \alpha$ satisfying the equation $f(x) + f(x + \alpha) = \beta$. This contradicts Lemma 2.1, as $f(x)$ is an almost perfect nonlinear function. Therefore, $d_H\left((\mathcal{C}(f)^{\bar{D}})^{\perp}\right) \geq 5$.

If $\nu = 1$ and $d_H\left((\mathcal{C}(f)^{\bar{D}})^{\perp}\right) = 5$, there are five pairwise-distinct elements x_1, x_2, x_3, x_4, x_5 in $\mathbb{F}_{2^m}^*$ such that $f(x_1) + f(x_2) + f(x_3) + f(x_4) + f(x_5) = 0$ by the definition of $\mathcal{C}(f)^{\bar{D}}$, then $\text{Tr}(\lambda(f(x_1) + f(x_2) + f(x_3) + f(x_4) + f(x_5))) = 0$, which is contradictory to $\text{Tr}(\lambda f(x_1)) = \text{Tr}(\lambda f(x_2)) = \text{Tr}(\lambda f(x_3)) = \text{Tr}(\lambda f(x_4)) = \text{Tr}(\lambda f(x_5)) = 1$. Hence,

$$d_H\left((\mathcal{C}(f)^{\bar{D}})^{\perp}\right) \geq \begin{cases} 5, & \text{if } \nu = 0, \\ 6, & \text{if } \nu = 1. \end{cases}$$

This completes the proof of this lemma. $\square$

We now give the weight distribution of the binary code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual as follows.

Theorem 3.3 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (3), where $f(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. Then the following statements hold.*

(1) *If $\nu = 0$, then $\mathcal{C}(f)^{\bar{D}}$ is an $[n, 2m-1, \frac{n+1}{2} - 2^{\frac{m-3}{2}}]$ code with the weight distribution in Table 1, where n was given in Lemma 3.1. Its dual has parameters $[n, n-2m+1, 5]$.*

Table 1: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $\nu = 0$ in Theorem 3.3

Weight	Multiplicity
0	1
$\frac{n+1}{2}$	$2^{2m-1} - (n+1)^4 2^{-2m} + 5(n+1)^2 2^{-m-1} - 5(n+1)2^{m-2} + \frac{3}{2}n^2 + 2n - \frac{1}{2}$
$\frac{n+1}{2} \pm 2^{\frac{m-1}{2}}$	$\pm\frac{1}{6}\left((n+1)^3 2^{\frac{1-3m}{2}} - (3n+1)2^{\frac{m-1}{2}} - (n+1)2^{-\frac{m+1}{2}} + 2^{\frac{3m-3}{2}}\right) - \frac{1}{6}(n+1)^4 2^{-2m} + \frac{1}{6}(n+1)^2 2^{-m-1} - \frac{1}{6}(n+1)2^{m-2} + \frac{1}{4}n^2 + \frac{1}{3}n + \frac{1}{12}$
$\frac{n+1}{2} \pm 2^{\frac{m-3}{2}}$	$\pm\frac{1}{6}\left(-(n+1)^3 2^{\frac{3-3m}{2}} + (n+1)2^{\frac{5-m}{2}} + 2^{\frac{m+1}{2}} - 2^{\frac{3+3m}{2}} + 6n \cdot 2^{\frac{m-1}{2}}\right) + 2^{2-2m} \cdot n^2 + \frac{1}{3}(n^4 + 4n^3 + 4n + 1)2^{1-2m} - \frac{1}{3}(n+1)^2 2^{2-m} + \frac{1}{3}(n+1)2^{1+m} - n^2 - \frac{4}{3}n - \frac{1}{3}$

(2) *If $\nu = 1$, then $\mathcal{C}(f)^{\bar{D}}$ is an $[n, 2m, \frac{n}{2} - 2^{\frac{m-3}{2}}]$ code with the weight distribution in Table 2, where n was given in Lemma 3.1. Its dual has parameters $[n, n-2m, 6]$, and is distance-optimal with respect to the sphere packing bound.*

Table 2: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $\nu = 1$ in Theorem 3.3

Weight	Multiplicity
0	1
$\frac{n}{2}$	$2^{2m} - 5n \cdot 2^{m-1} + 5n^2 \cdot 2^{-m} - 2^{1-2m}n^4 + 3n^2 - 2n - 2$
$\frac{n}{2} \pm 2^{\frac{m-1}{2}}$	$-\frac{1}{3}n^4 2^{-2m} + \frac{1}{6}(2^{-m}n^2 + 3n^2 - 2^{m-1}n - 2n)$
$\frac{n}{2} \pm 2^{\frac{m-3}{2}}$	$\frac{4n}{3}(2^{-2m}n^3 - 2^{1-m}n - \frac{3n}{2} + 2^m + 1)$
n	1

Proof. It follows from (2) that the Hamming weight of the codeword $\mathbf{c}(a, b)$ in $\mathcal{C}(f)^{\bar{D}}$ is given by

$$\mathrm{wt_H}(\mathbf{c}(a,b)) = |D| - |\{x \in D : \mathrm{Tr}(af(x) + bx) = 0\}|$$

$$= \frac{|D|}{2} - \frac{1}{2}\sum_{x \in D}(-1)^{\mathrm{Tr}(af(x)+bx)}$$

$$= \frac{|D|}{2} - \frac{1}{2}\sum_{x \in \mathbb{F}_{2^m}\setminus\{0\}}\left(\frac{1}{2}\sum_{y \in \mathbb{F}_2}(-1)^{y(\mathrm{Tr}(\lambda f(x))-\nu)}\right)(-1)^{\mathrm{Tr}(af(x)+bx)}$$

$$= \frac{|D|}{2} - \frac{1}{4}\sum_{x \in \mathbb{F}_{2^m}}\left(\sum_{y \in \mathbb{F}_2}(-1)^{y(\mathrm{Tr}(\lambda f(x))-\nu)}\right)(-1)^{\mathrm{Tr}(af(x)+bx)} + \frac{1}{4}\sum_{y \in \mathbb{F}_2}(-1)^{y\nu}$$

$$= \frac{|D|}{2} - \frac{1}{4}\sum_{x \in \mathbb{F}_{2^m}}\left(1 + (-1)^{(\mathrm{Tr}(\lambda f(x))-\nu)}\right)(-1)^{\mathrm{Tr}(af(x)+bx)} + \frac{1}{4}\sum_{y \in \mathbb{F}_2}(-1)^{y\nu}$$

$$= \frac{|D|}{2} - \frac{1}{4}\sum_{x \in \mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(af(x)+bx)} - (-1)^{\nu}\sum_{x \in \mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}((\lambda+a)f(x)+bx)} + \frac{1}{4}\sum_{y \in \mathbb{F}_2}(-1)^{zy\nu}$$

$$= \frac{|D|}{2} - \frac{1}{4}W_f(a,b) - \frac{(-1)^{\nu}}{4}W_f(a+\lambda,b) + \frac{1}{4}\sum_{y \in \mathbb{F}_2}(-1)^{z_0\nu}, \tag{10}$$

where $W_f(a, b)$ was defined in (5). By the definition of almost bent functions, for any $(a, b) \in \mathbb{F}_{2^m}^2 \setminus \{(0, 0)\}$, we know that $W_f(a, b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$. So,

$$\frac{1}{4}\left(W_f(a,b) \pm W_f(a+\lambda,b)\right) \in \left\{0, \pm 2^{\frac{m-1}{2}}, \pm 2^{\frac{m-3}{2}}\right\} \tag{11}$$

for any $(a, b) \in \mathbb{F}_{2^m}^2 \setminus \{(0, 0), (\lambda, 0)\}$. In the following, we prove this theorem case by case.

Case 1: $\nu = 0$, i.e., $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}(\lambda f(x)) = 0\}$. By (10) and (11), when (a, b) runs over $\mathbb{F}_{2^m}^2 \setminus \{(0, 0), (\lambda, 0)\}$, the possible values of $\mathrm{wt_H}(\mathbf{c}(a, b))$ are

$$\frac{n+1}{2}, \frac{n+1}{2} \pm 2^{\frac{m-1}{2}}, \text{ and } \frac{n+1}{2} \pm 2^{\frac{m-3}{2}},$$

where n was given in Lemma 3.1. It is easy to see that $\mathrm{wt_H}(\mathbf{c}(a, b)) = 0$ if and only if $(a, b) = (0, 0)$ or $(a, b) = (\lambda, 0)$. So, the dimension of $\mathcal{C}(f)^{\bar{D}}$ is $2m - 1$.

10

Denote $w_1 = \frac{n+1}{2}$, $w_2 = \frac{n+1}{2} + 2^{\frac{m-1}{2}}$, $w_3 = \frac{n+1}{2} - 2^{\frac{m-1}{2}}$, $w_4 = \frac{n+1}{2} + 2^{\frac{m-3}{2}}$ and $w_5 = \frac{n+1}{2} - 2^{\frac{m-3}{2}}$.
Let A_{w_i} be the number of the codewords with weight w_i in $\mathcal{C}(f)^{\bar{D}}$. By Lemma 3.2, we know that $A_1^\perp = A_2^\perp = A_3^\perp = A_4^\perp = 0$. From the first five Pless power moments, we have the following system of equations:

$$
\begin{cases}
\sum_{i=1}^5 A_{w_i} = 2^{2m-1} - 1; \\
\sum_{i=1}^5 w_i A_{w_i} = 2^{2m-2} n; \\
\sum_{i=1}^5 w_i^2 A_{w_i} = 2^{2m-3} n(n+1); \\
\sum_{i=1}^5 w_i^3 A_{w_i} = 2^{2m-4} n^2(n+3); \\
\sum_{i=1}^5 w_i^4 A_{w_i} = 2^{2m-5} n(n+1)(n^2 + 5n - 2).
\end{cases}
$$

Solving this system of equations, we obtain the desired values of A_{w_1}, A_{w_2}, A_{w_3}, A_{w_4} and A_{w_5} in Table 1.

We now determine the parameters of the dual of $\mathcal{C}(f)^{\bar{D}}$. We consider only the case $n = 2^{m-1} - 1$, i.e., the value of $W_f(\lambda, 0)$ is zero. The other two cases can be shown similarly. Substituting the value of $n = 2^{m-1} - 1$ in Table 1, we obtain that $A_{w_1} = 3 \cdot 2^{2m-4} + 2^{m-3} - 1$, $A_{w_2} = 2^{2m-5} - 2^{\frac{3m-7}{2}} + 2^{\frac{m-5}{2}} - 2^{m-4}$, $A_{w_3} = 2^{2m-5} + 2^{\frac{3m-7}{2}} - 2^{\frac{m-5}{2}} - 2^{m-4}$, $A_{w_4} = 2^{2m-3} - 2^{\frac{3m-5}{2}}$ and $A_{w_5} = 2^{2m-3} + 2^{\frac{3m-5}{2}}$.
By Lemma 3.2, $A_1^\perp = A_2^\perp = A_3^\perp = A_4^\perp = 0$. Then from the sixth Pless power moment, we have

$$
\sum_{i=1}^5 w_i^5 A_{w_i} = 2^{2m-6} \cdot (2^{m-1} - 1)^5 + 5 \cdot 2^{2m-5} \cdot (2^{m-1} - 1)^4
$$

$$
+ 15 \cdot 2^{2m-6} \cdot (2^{m-1} - 1)^3 - 5 \cdot 2^{2m-5} \cdot (2^{m-1} - 1)^2 - A_5^\perp \cdot 2^{2m-6} \cdot 120.
$$

Solving this equation, we obtain $A_5^\perp = (11 \cdot 2^m + 2^{3m-4} - 13 \cdot 2^{2m-3} - 2^4)/120 \neq 0$. Hence, $(\mathcal{C}(f)^{\bar{D}})^\perp$ has parameters $[2^{m-1} - 1, 2^{m-1} - 2m, 5]$.

Case 2: $\nu = 1$, i.e., $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}(\lambda f(x)) = 1\}$. By (10) and (11), when (a, b) runs over $\mathbb{F}_{2^m}^2 \setminus \{(0, 0), (\lambda, 0)\}$, the possible values of $\mathrm{wt}_H(\mathbf{c}(a, b))$ are

$$
\frac{n}{2}, \quad \frac{n}{2} \pm 2^{\frac{m-1}{2}} \quad \text{and} \quad \frac{n}{2} \pm 2^{\frac{m-3}{2}},
$$

where n was given in Lemma 3.1. Moreover, $\mathrm{wt}_H(\mathbf{c}(a, b)) = 0$ if and only if $(a, b) = (0, 0)$ and $\mathrm{wt}_H(\mathbf{c}(a, b)) = n$ if $(a, b) = (\lambda, 0)$. So, the dimension of $\mathcal{C}(f)^{\bar{D}}$ is $2m$.
Denote $w_1 = 2^{m-2}$, $w_2 = 2^{m-2} + 2^{\frac{m-1}{2}}$, $w_3 = 2^{m-2} - 2^{\frac{m-1}{2}}$, $w_4 = 2^{m-2} + 2^{\frac{m-3}{2}}$ and $w_5 = 2^{m-2} - 2^{\frac{m-3}{2}}$. Let A_{w_i} be the number of the codewords with weight w_i in $\mathcal{C}(f)^{\bar{D}}$. From Lemma 3.2 we know that $A_1^\perp = A_2^\perp = A_3^\perp = A_4^\perp = 0$. Then the first five Pless power moments lead to the following system of equations:

$$
\begin{cases}
\sum_{i=1}^5 A_{w_i} = 2^{2m} - 2; \\
\sum_{i=1}^5 w_i A_{w_i} = 2^{2m-1} n - n; \\
\sum_{i=1}^5 w_i^2 A_{w_i} = 2^{2m-2} n(n+1) - n^2; \\
\sum_{i=1}^5 w_i^3 A_{w_i} = 2^{2m-3} n^2(n+3) - n^3; \\
\sum_{i=1}^5 w_i^4 A_{w_i} = 2^{2m-4} n(n+1)(n^2 + 5n - 2) - n^4.
\end{cases}
$$

Solving this system of equations, we obtain the desired values of A_{w_1}, A_{w_2}, A_{w_3}, A_{w_4} and A_{w_5} in Table 2.

11

We now determine the parameters of the dual of $\mathcal{C}(f)^{\bar{D}}$. We treat only the case $n = 2^{m-1}$ and the other two cases can be treated similarly. Substituting the value of $n = 2^{m-1}$ in Table 2, we obtain that $A_{w_1} = 3 \cdot 2^{2m-3} + 2^{m-2} - 2$, $A_{w_2} = A_{w_3} = 2^{2m-4} - 2^{m-3}$ and $A_{w_4} = A_{w_5} = 2^{2m-2}$. If $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) > 6$, then

$$\sum_{i=0}^{3} \binom{2^{m-1}}{i} = 1 + 2^{m-1} + 2^{m-2} \cdot (2^{m-1} - 1) + \frac{2^{m-2} \cdot (2^{m-1} - 1) \cdot (2^{m-1} - 2)}{3} > 2^{2m},$$

which contradicts the sphere packing bound. From Lemma 3.2, we then deduce that $d_H\left((\mathcal{C}(f)^{\bar{D}})^\perp\right) = 6$, and $(\mathcal{C}(f)^{\bar{D}})^\perp$ is distance-optimal with respect to the sphere packing bound. $\square$

Example 3.4 *Let $m = 7$ and $f(x)$ be an almost bent function from $\mathbb{F}_{2^7}$ to $\mathbb{F}_{2^7}$ with $W_f(1, 0) = 2^{\frac{7+1}{2}}$. Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 3.3.*

(1) If $\nu = 0$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[71, 13, 28]$ and its dual has parameters $[71, 58, 5]$.

(2) If $\nu = 1$ then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[56, 14, 20]$ and its dual has parameters $[56, 42, 6]$.

The four codes are optimal according to the tables of best codes known in [22].

Remark 3.5 *In [36], the authors proposed the following open problem (Problem 4.4): Let $\lambda \in \mathbb{F}_{2^s}^*$, F be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^s}$ and D be the support of $\mathrm{Tr}_1^s(\lambda F(x))$. Define a linear code $\mathcal{C}'(F)^{\bar{D}}$ over $\mathbb{F}_2$ by*

$$\mathcal{C}'(F)^{\bar{D}} = \{(\mathrm{Tr}_1^m(xh) + \mathrm{Tr}_1^s(yF(h)))_{h \in D} : x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^s}\}.$$

Determining the weight distributions of the linear codes if F is a vectorial bent function with $m \neq 2s$ or an almost bent function but not the Gold type. Clearly, if F is an almost bent function, then $s = m$. Table 2 in Theorem 3.3 has given the weight distribution of $\mathcal{C}'(F)^{\bar{D}}$ for F being an almost bent function.

The following is a list of known almost bent monomials $f(x) = x^d$ on $\mathbb{F}_{2^m}$ for an odd m:

- $d = 2^h + 1$, where $\gcd(m, h) = 1$ is odd [21];

- $d = 2^{2h} - 2^h + 1$, where $h \geq 2$ and $\gcd(m, h) = 1$ is odd [31];

- $d = 2^{\frac{m-1}{2}} + 3$, where m is odd [31];

- $d = 2^{\frac{m-1}{2}} + 2^{\frac{m-1}{4}} - 1$, where $m \equiv 1 \pmod 4$ [26, 27];

- $d = 2^{\frac{m-1}{2}} + 2^{\frac{3m-1}{4}} - 1$, where $m \equiv 3 \pmod 4$ [26, 27].

All almost bent monomials $f(x) = x^d$ for d in the list above are permutation polynomials on $\mathbb{F}_{2^m}$. Hence, the length of $\mathcal{C}(f)^{\bar{D}}$ is $n = 2^{m-1} - 1$ if $\nu = 0$ and $n = 2^{m-1}$ if $\nu = 1$, respectively. Substituting the value of n into Theorem 3.3, we obtain the following results.

Corollary 3.6 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (3). If $f(x) = x^d$ for some integer d in the list above, then the following statements hold.*

12

Table 3: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $\nu = 0$ in Corollary 3.6

Weight	Multiplicity
0	1
2^{m-2}	$3 \cdot 2^{2m-4} + 2^{m-3} - 1$
$2^{m-2} \pm 2^{\frac{m-1}{2}}$	$2^{2m-5} \mp 2^{\frac{3m-7}{2}} \pm 2^{\frac{m-5}{2}} - 2^{m-4}$
$2^{m-2} \pm 2^{\frac{m-3}{2}}$	$2^{2m-3} \mp 2^{\frac{3m-5}{2}}$

(1) If $\nu = 0$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1} - 1, 2m - 1, 2^{m-2} - 2^{\frac{m-3}{2}}]$ code with the weight distribution in Table 3. Its dual has parameters $[2^{m-1} - 1, 2^{m-1} - 2m, 5]$.

(2) If $\nu = 1$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, 2m, 2^{m-2} - 2^{\frac{m-3}{2}}]$ code with the weight distribution in Table 4. Its dual has parameters $[2^{m-1}, 2^{m-1} - 2m, 6]$, and is distance-optimal with respect to the sphere packing bound.

Table 4: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $\nu = 1$ in Corollary 3.6

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

Example 3.7 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Corollary 3.6.*

(1) *If $m = 7$, $\nu = 0$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[63, 13, 24]$ and its dual has parameters $[63, 50, 5]$.*

(2) *If $m = 7$, $\nu = 1$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[64, 14, 24]$ and its dual has parameters $[64, 50, 6]$.*

The four codes are optimal according to the tables of best codes known in [22].

4 Some punctured codes of binary linear codes from quadratic functions

Let $\mathcal{C}(f)^{\bar{D}}$ be the binary punctured code defined in (2) with the position set D in (4). It is clear that the length of $\mathcal{C}(f)^{\bar{D}}$ is equal to 2^{m-1}, as $|D| = |\{x \in \mathbb{F}_{2^m}^* : \text{Tr}_1^m(x) = 1\}| = 2^{m-1}$. As shown in (10), the Hamming weight of each codeword in this case can be expressed as

$$\text{wt}_{\text{H}}(\mathbf{c}(a, b)) = 2^{m-2} - \frac{1}{4}\left(W_f(a, b) - W_f(a, b + 1)\right), \tag{12}$$

13

where $W_f(a,b)$ was given in (5). In this section, we investigate the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ with the position set D in (4), where f is a quadratic function in the list below and the parameters of its dual.

- $f(x) = x^{2^k+1}$, where k is an integer with $1 \le k \le m-1$;

- $f(x) = x^{t_1} + x^{t_2}$, where $3 \mid m$, $m \ge 9$ and $t_1, t_2 \in \{2^{\frac{m}{3}}+1, 2^{\frac{2m}{3}}+1, 2^{\frac{2m}{3}}+2^{\frac{m}{3}}\}$ with $t_1 \ne t_2$;

- $f(x) = \mathrm{Tr}_k^m(x^{2^k+1})$, where m, k are positive integers such that $k \mid m$.

When $f(x) = x^{2^k+1}$, the parameters and weight distribution of the binary code $\mathcal{C}(f)$ were settled in [29, 30]. In this section we will investigate the punctured code $\mathcal{C}(f)^{\bar{D}}$ with a different position set $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}_1^m(x) = 1\}$. It is open if the binary code $\mathcal{C}(f)$ was studied in the literature or not when f is one of the other two quadratic functions in the list above.

4.1 The case that $f(x) = x^{2^k+1}$

In this subsection, we study the punctured code $\mathcal{C}(f)^{\bar{D}}$ in (2) and determine its weight distribution, where $f(x) = x^{2^k+1}$ and $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}_1^m(x) = 1\}$. When $k = 0$, $f(x) = x^2$. In this case, it can be proved that the punctured code $\mathcal{C}(f)^{\bar{D}}$ is permutation-equivalent to the first-order Reed-Muller code. In the following, we investigate the linear code $\mathcal{C}(f)^{\bar{D}}$ for $f(x) = x^{2^k+1}$ with $1 \le k < m$. We start with the following two lemmas.

Lemma 4.1 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (4). Let $A_i^{\perp}$ denote the number of codewords with weight i in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$. If $f(x) = x^{2^k+1}$ with $1 \le k < m$, then*

$$A_1^{\perp} = A_2^{\perp} = A_3^{\perp} = A_5^{\perp} = 0 \text{ and } A_4^{\perp} = \frac{2^{m-1} \cdot (2^{m-2}-1) \cdot (2^{\ell}-2)}{4!},$$

where $\ell = \gcd(k, m)$.

Proof. From the definition of the linear code $\mathcal{C}(f)^{\bar{D}}$, we know that $A_i^{\perp}$ is equal to the number of sets $\{x_1, x_2, \cdots, x_i\}$ with i pairwise-distinct nonzero elements in $\mathbb{F}_{2^m}$ such that

$$\begin{cases} \mathrm{Tr}(x_1) = \mathrm{Tr}(x_2) = \cdots = \mathrm{Tr}(x_i) = 1, \\ x_1 + x_2 + \cdots + x_i = 0, \\ x_1^{2^k+1} + x_2^{2^k+1} + \cdots + x_i^{2^k+1} = 0. \end{cases}$$

It is clear that $A_1^{\perp} = A_2^{\perp} = 0$. From the first and second equations, we see that $A_i^{\perp} = 0$ if i is odd. Hence, $A_3^{\perp} = A_5^{\perp} = 0$. In the following, we determine the value of $A_4^{\perp}$, which is equal to the number of sets $\{x_1, x_2, x_3, x_4\}$ with 4 pairwise-distinct nonzero elements in $\mathbb{F}_{2^m}$ such that

$$\begin{cases} \mathrm{Tr}(x_1) = \mathrm{Tr}(x_2) = \mathrm{Tr}(x_3) = \mathrm{Tr}(x_4) = 1, \\ x_1 + x_2 + x_3 + x_4 = 0, \\ x_1^{2^k+1} + x_2^{2^k+1} + x_3^{2^k+1} + x_4^{2^k+1} = 0. \end{cases} \tag{13}$$

14

Assume that $x_1 = \mu$, $x_2 = \mu + \beta$, $x_3 = \gamma$ and $x_4 = \gamma + \beta$, where $\mu \neq 0, \beta, \gamma, \gamma + \beta$, and $\gamma \neq 0, \beta$, and $\beta \neq 0$. From (13) we know that $A_4^{\perp}$ is equal to the number of the sets of the form $\{\mu, \mu + \beta, \gamma, \gamma + \beta\}$ such that

$$\mu^{2^k+1} + (\mu + \beta)^{2^k+1} = \gamma^{2^k+1} + (\gamma + \beta)^{2^k+1}, \ \mathrm{Tr}(\mu) = \mathrm{Tr}(\gamma) = 1 \text{ and } \mathrm{Tr}(\beta) = 0,$$

i.e.,

$$(\mu + \gamma)^{2^k-1} = \beta^{2^k-1}, \ \mathrm{Tr}(\mu) = \mathrm{Tr}(\gamma) = 1 \text{ and } \mathrm{Tr}(\beta) = 0.$$

It is clear that $(\mu + \gamma)^{2^k-1} = \beta^{2^k-1}$ if and only if there is a $\delta \in \mathbb{F}_{2^\ell}$ such that $\mu + \gamma = \delta\beta$ as $\gcd(2^m - 1, 2^k - 1) = 2^\ell - 1$. Then $A_4^{\perp}$ is equal to the number of the sets of the form $\{\mu, \mu + \beta, \mu + \delta\beta, \mu + \beta(\delta+1)\}$ such that $\mathrm{Tr}(\mu) = 1$ and $\mathrm{Tr}(\beta) = \mathrm{Tr}(\delta\beta) = 0$, where $\delta \in \mathbb{F}_{2^\ell} \backslash \{0, 1\}$, $\mu \neq 0, \beta, \delta\beta, \beta(\delta + 1)$ and $\beta \neq 0$. Hence,

$$A_4^{\perp} = \frac{1}{8 \cdot 4!} \sum_{z_0 \in \mathbb{F}_2} \sum_{\mu \in \mathbb{F}_{2^m}^* \backslash \{\beta, \delta\beta, \beta(\delta+1)\}} (-1)^{z_0(\mathrm{Tr}(\mu)-1)} \sum_{z_1 \in \mathbb{F}_2} \sum_{\beta \in \mathbb{F}_{2^m}^*} (-1)^{z_1 \mathrm{Tr}(\beta)} \sum_{z_2 \in \mathbb{F}_2} \sum_{\delta \in \mathbb{F}_{2^\ell}^* \backslash \{1\}} (-1)^{z_2 \mathrm{Tr}(\delta\beta)}$$

$$= \frac{2^{m-3}}{4!} \sum_{z_1 \in \mathbb{F}_2} \sum_{\beta \in \mathbb{F}_{2^m}^*} (-1)^{z_1 \mathrm{Tr}(\beta)} \sum_{z_2 \in \mathbb{F}_2} \sum_{\delta \in \mathbb{F}_{2^\ell}^* \backslash \{1\}} (-1)^{z_2 \mathrm{Tr}(\delta\beta)}$$

$$= \frac{2^{m-3}}{4!} \sum_{z_1 \in \mathbb{F}_2} \sum_{z_2 \in \mathbb{F}_2} \sum_{\beta \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^\ell}^* \backslash \{1\}} (-1)^{\mathrm{Tr}((z_1 + z_2\gamma)\beta)}$$

$$= \frac{2^{m-3}}{4!} \left(\sum_{z_1 \in \mathbb{F}_2} \sum_{z_2 \in \mathbb{F}_2} \sum_{\beta \in \mathbb{F}_{2^m}} \sum_{\gamma \in \mathbb{F}_{2^\ell}^* \backslash \{1\}} (-1)^{\mathrm{Tr}((z_1 + z_2\gamma)\beta)} - 2^2 \cdot (2^\ell - 2) \right)$$

$$= \frac{2^{m-3}}{4!} \left(2^m \cdot (2^\ell - 2) - 2^2 \cdot (2^\ell - 2) \right) = \frac{2^{m-1} \cdot (2^{m-2} - 1) \cdot (2^\ell - 2)}{4!}.$$

The desired conclusion then follows. $\square$

Theorem 4.2 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (3). Let k be a positive integer with $k < m$ and $\ell = \gcd(k, m)$. If $f(x) = x^{2^k+1}$, then the following statements hold.*

(1) *If $v_2(m) \leq v_2(k)$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, 2m, 2^{m-2} - 2^{\frac{m+\ell-4}{2}}]$ code with the weight distribution in Table 5. If $\ell \geq 2$, then its dual has parameters $[2^{m-1}, 2^{m-1} - 2m, 4]$. If $\ell = 1$, then its dual has parameters $[2^{m-1}, 2^{m-1} - 2m, 6]$, and is distance-optimal with respect to the sphere packing bound.*

(2) *If $v_2(m) > v_2(k)$ and $\gcd(m, k) = 1$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, 2m, 2^{m-2} - 2^{\frac{m}{2}}]$ code with the weight distribution in Table 6. Its dual has parameters $[2^{m-1}, 2^{m-1} - 2m, 6]$, and is distance-optimal with respect to the sphere packing bound.*

(3) *If $k = \frac{m}{2}$ and $m \geq 4$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, \frac{3m}{2}, 2^{m-2} - 2^{\frac{m-2}{2}}]$ code with the weight distribution in Table 7. Its dual has parameters $[2^{m-1}, 2^{m-1} - \frac{3m}{2}, 4]$, and is distance-optimal with respect to the sphere packing bound.*

Table 5: The weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.2

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

Table 6: The weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.2

Weight	Multiplicity
0	1
2^{m-2}	$17 \cdot 2^{2m-5} + 3 \cdot 2^{m-3} - 2$
$2^{m-2} \pm 2^{\frac{m}{2}}$	$\frac{1}{3}\left(2^{2m-6} - 2^{m-4}\right)$
$2^{m-2} \pm 2^{\frac{m-2}{2}}$	$\frac{1}{6}\left(11 \cdot 2^{2m-3} - 2^m\right)$
2^{m-1}	1

Proof. We prove the desired conclusions for Cases (1) and (3) only. The conclusions in Case (2) can be proved in a similar way. If $a = 0$, it is easy to see that

$$\mathrm{wt_H}\left(\mathbf{c}(a,b)\right) = 2^{m-2} - \frac{1}{4}\left(W_f(0,b) - W_f(0,b+1)\right) = \begin{cases} 0, & \text{if } b = 0, \\ 2^{m-1}, & \text{if } b = 1, \\ 2^{m-2}, & \text{if } b \neq 0,\ 1. \end{cases}$$

If $a \neq 0$ and $v_2(m) \leq v_2(k)$, then Lemma 2.2 shows that $W_f(a,b) \in \{0, \pm 2^{\frac{m+\ell}{2}}\}$. Consequently, in this case we have $W_f(a,b) - W_f(a,b+1) \in \{0, \pm 2^{\frac{m+\ell}{2}}, \pm 2^{\frac{m+\ell+2}{2}}\}$. From (12) we see that the set of possible nonzero weights of $\mathcal{C}(f)^{\bar{D}}$ is $\{2^{m-1}, 2^{m-2}, 2^{m-2} \pm 2^{\frac{m+\ell-2}{2}}, 2^{m-2} \pm 2^{\frac{m+\ell-4}{2}}\}$ and $\mathcal{C}(f)^{\bar{D}}$ has dimension $2m$. Set $w_1 = 2^{m-1}, w_2 = 2^{m-2}, w_3 = 2^{m-2} + 2^{\frac{m+\ell-2}{2}}, w_4 = 2^{m-2} - 2^{\frac{m+\ell-2}{2}}, w_5 = 2^{m-2} + 2^{\frac{m+\ell-4}{2}}$ and $w_6 = 2^{m-2} - 2^{\frac{m+\ell-4}{2}}$. It is known that $A_{w_1} = 1$. From Lemma 4.1 and the first five Pless power moments we have

$$\begin{cases} \sum_{i=2}^{6} A_{w_i} = 2^{2m} - 2; \\ \sum_{i=2}^{6} w_i A_{w_i} = 2^{m-1}(2^{2m-1} - 1); \\ \sum_{i=2}^{6} w_i^2 A_{w_i} = 2^{2m-2}(2^{2m-2} + 2^{m-1} - 1); \\ \sum_{i=2}^{6} w_i^3 A_{w_i} = 2^{3m-3}(2^{2m-2} + 3 \cdot 2^{m-1} - 1); \\ \sum_{i=2}^{6} w_i^4 A_{w_i} = 2^{3m-5}\left((2^{m-1} + 1)(2^{2m-2} + 5 \cdot 2^{m-1} - 2) - (2^{m-2} - 1)(2^{\ell} - 1)\right) - 2^{4(m-1)}. \end{cases} \tag{14}$$

Solving the linear equations in (14), we get the desired values of A_{w_i} in Table 5. If $\ell > 1$, by Lemma 4.1, $A_4^{\perp} > 0$. Consequently, the dual distance of the code equals 4. If $\ell = 1$, by Lemma 4.1, $A_4^{\perp} = 0$. Since all weights in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ are even, the minimum distance of $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is at least 6. By the

Table 7: The weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.2

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

sphere packing bound, the minimum distance of $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ cannot be 8 or more. Consequently, the minimum distance of $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is equal to 6. This completes the proof of the conclusions in Case (1).

Next, we prove the conclusions for Case (3). Assume that $k = \frac{m}{2}$ and $f(x) = x^{2^{m/2}+1}$, then

$$
\begin{aligned}
W_f^2(a,b) &= \sum_{x_0 \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(ax_0^{2^{m/2}+1}+bx_0)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(ax^{2^{m/2}+1}+bx)} \\
&= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a(x+y)^{2^{m/2}+1}+b(x+y)+ax^{2^{m/2}+1}+bx)} \\
&= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a(y^{2^{m/2}+1}+xy^{2^{m/2}}+x^{2^{m/2}}y)+by)} \\
&= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(ay^{2^{m/2}+1}+by)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a(xy^{2^{m/2}}+x^{2^{m/2}}y))} \quad (15) \\
&= 2^m \sum_{\substack{y \in \mathbb{F}_{2^m} \\ (a+a^{2^{m/2}})y = 0}} (-1)^{\mathrm{Tr}(ay^{2^{m/2}+1}+by)} \\
&= \begin{cases} 2^m W_f(a,b), & \text{if } a \in \mathbb{F}_{2^{\frac{m}{2}}}, \\ 2^m, & \text{otherwise.} \end{cases}
\end{aligned}
$$

If $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, then $\mathrm{Tr}(ay^{2^{m/2}+1}) = 0$ and the possible values of $W_f(a,b)$ are as follows:

$$
W_f(a,b) = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(ay^{2^{m/2}+1}+by)} = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(by)} = \begin{cases} 2^m, & \text{if } b = 0, \\ 0, & \text{otherwise.} \end{cases}
$$

Hence,

$$
W_f(a,b) = \begin{cases} 2^m, & \text{if } a \in \mathbb{F}_{2^{\frac{m}{2}}} \text{ and } b = 0, \\ 0, & \text{if } a \in \mathbb{F}_{2^{\frac{m}{2}}} \text{ and } b \neq 0, \\ \pm 2^{\frac{m}{2}}, & \text{otherwise.} \end{cases}
$$

When (a,b) runs through $\mathbb{F}_{2^m}^2$, we know that $W_f(a,b) - W_f(a,b+1) \in \{0, \pm 2^{\frac{m+2}{2}}, \pm 2^m\}$ and the value 2^m occurs $2^{\frac{m}{2}}$ times. Then $\mathrm{wt_H}(\mathbf{c}(a,b)) \in \{0, 2^{m-2} \pm 2^{\frac{m-2}{2}}, 2^{m-1}\}$ and $\mathrm{wt_H}(\mathbf{c}(a,b)) = 0$ occurs $2^{\frac{m}{2}}$ times by (15). So, $\mathcal{C}(f)^{\bar{D}}$ has dimension $\frac{3m}{2}$ and we obtain the weight distribution in Table 7

17

from the first three Pless power moments. From the sphere packing bound and Lemma 4.1, the desired conclusions on $\mathcal{C}(f)^{\bar{D}}$ then follow. In this case, $\ell = m/2 > 1$. It then follows from Lemma 4.1, $A_4^{\perp} > 0$. Consequently, the dual distance of the code equals 4. $\square$

Example 4.3 Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 4.2.

(1) Let $m = 5$, $k = 1$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[16, 10, 4]$ and its dual has parameters $[16, 6, 6]$.

(2) Let $m = 8$, $k = 4$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[128, 12, 56]$ and its dual has parameters $[128, 116, 4]$.

All the four codes are optimal according to the tables of best codes known in [22].

4.2 The case that $f(x) = x^{t_1} + x^{t_2}$

In this subsection, we investigate the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual for $f(x) = x^{t_1} + x^{t_2}$, where $3 \mid m$, $m \geq 9$ and $t_1, t_2 \in \{2^{\frac{m}{3}} + 1, 2^{\frac{2m}{3}} + 1, 2^{\frac{2m}{3}} + 2^{\frac{m}{3}}\}$ with $t_1 \neq t_2$. We first determine all possible Hamming weights in $\mathcal{C}(f)^{\bar{D}}$.

Lemma 4.4 Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (2) with the position set D in (4). Let $3 \mid m$, $m \geq 9$ and $f(x) = x^{t_1} + x^{t_2}$, where $t_1, t_2 \in \{2^{\frac{m}{3}} + 1, 2^{\frac{2m}{3}} + 1, 2^{\frac{2m}{3}} + 2^{\frac{m}{3}}\}$ with $t_1 \neq t_2$. Then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, \frac{5m}{3}]$ code with nonzero weights in the set $\{2^{m-2}, 2^{m-1}, 2^{m-2} \pm 2^{\frac{2m}{3} - 1}\}$.

Proof. We prove the conclusions only for the case $t_1 = 2^{\frac{2m}{3}} + 1$ and $t_2 = 2^{\frac{2m}{3}} + 2^{\frac{m}{3}}$. The conclusions in the other two cases can be similarly proved. In this case, we have

$$W_f(a, b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(a(x^{2^{2m/3}+1} + x^{2^{2m/3}+2^{m/3}}) + bx)}.$$

If $a \in \mathbb{F}_{2^{\frac{m}{3}}}$, then $a + a^{2^{m/3}} = 0$ and $a + a^{2^{2m/3}} = 0$. In this case,

$$W_f(a, b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(bx)} = \begin{cases} 2^m, & \text{if } b = 0, \\ 0, & \text{if } b \neq 0. \end{cases}$$

Hence, when (a, b) runs over $\mathbb{F}_{2^{\frac{m}{3}}} \times \mathbb{F}_{2^m}$, we obtain

$$W_f(a, b) - W_f(a, b+1) = \begin{cases} 0, & \text{occuring } 2^{2m} - 2^{\frac{m}{3}+1} \text{ times,} \\ 2^m, & \text{occuring } 2^{\frac{m}{3}} \text{ times,} \\ -2^m, & \text{occuring } 2^{\frac{m}{3}} \text{ times.} \end{cases} \tag{16}$$

If $a \in \mathbb{F}_{2^m} \setminus \mathbb{F}_{2^{\frac{m}{3}}}$, similar to the calculations in (15), we have

$$W_f^2(a, b) = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(a(y^{2^{2m/3}+1} + y^{2^{2m/3}+2^{m/3}}) + by)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}((ay^{2^{m/3}} + a^{2^{m/3}}y + a^{2^{2m/3}}y^{2^{m/3}} + ay)x^{2^{2m/3}})}$$

$$= 2^m \sum_{\substack{y \in \mathbb{F}_{2^m} \\ (a + a^{2^{2m/3}})y^{2^{m/3}} + (a^{2^{m/3}} + a)y = 0}} (-1)^{\text{Tr}(a(y^{2^{2m/3}+1} + y^{2^{2m/3}+2^{m/3}}) + by)}.$$

18

Let $L_a(y) = (a + a^{2^{2m/3}})y^{2^{m/3}} + (a^{2^{m/3}} + a)y$, then

$$\mathrm{Ker}(L_a(y)) = \{\, y \in \mathbb{F}_{2^m} \mid L_a(y) = 0 \,\} = \left\{ (a^{2^{2m/3}} + a)z : \ z \in \mathbb{F}_{2^{\frac{m}{3}}} \right\}.$$

From (7) we get

$$W_f^2(a,b) = \begin{cases} 2^{\frac{4m}{3}}, & \text{if } \mathrm{Tr}\left(a(y^{2^{2m/3}+1} + y^{2^{2m/3}+2^{m/3}}) + by\right) = 0 \text{ for all } y \in \mathrm{Ker}(L_a(y)), \\ 0, & \text{otherwise.} \end{cases}$$

If $\mathrm{Tr}\left(a(y^{2^{2m/3}+1} + y^{2^{2m/3}+2^{m/3}}) + by\right) = 0$ for all $y \in \mathrm{Ker}(L_a(y))$, then

$$\mathrm{Tr}\left(a(y^{2^{2m/3}+1} + y^{2^{2m/3}+2^{m/3}}) + (b+1)y\right) = \mathrm{Tr}(y) = \mathrm{Tr}_1^{\frac{m}{3}}\left(\mathrm{Tr}_{\frac{m}{3}}^m((a^{2^{2m/3}} + a)t)\right) = 0$$

because $t \in \mathbb{F}_{2^{\frac{m}{3}}}$. Hence, $W_f(a,b) - W_f(a,b+1) \in \left\{0, \pm 2^{\frac{2m}{3}+1}\right\}$ for $a \in \mathbb{F}_{2^m} \backslash \mathbb{F}_{2^{\frac{m}{3}}}$. Combining this with (16), when (a,b) runs through $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have

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

and each of the values $\pm 2^m$ occurs $2^{\frac{m}{3}}$ times. Then from (12) we know that $\mathrm{wt}_H(\mathbf{c}(a,b)) = 0$ and $\mathrm{wt}_H(\mathbf{c}(a,b)) = 2^{m-1}$ both occur $2^{\frac{m}{3}}$ times and the nonzero weights in $\mathcal{C}(f)^{\bar{D}}$ belong to the set $\{2^{m-2}, 2^{m-1}, 2^{m-2} \pm 2^{\frac{2m}{3}-1}\}$. It then follows that $\mathcal{C}(f)^{\bar{D}}$ is degenerate and has dimension $\frac{5m}{3}$. This completes the proof. $\square$

Theorem 4.5 *Follow the notation and conditions introduced in Lemma 4.4. Then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, \frac{5m}{3}, 2^{m-2} - 2^{\frac{2m}{3}-1}]$ code with the weight distribution in Table 8. Its dual has parameters $[2^{m-1}, 2^{m-1} - \frac{5m}{3}, 4]$, and is distance-optimal with respect to the sphere packing bound.*

Table 8: The weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.5

Weight	Multiplicity
0	1
2^{m-2}	$2^{\frac{5m}{3}} - 2^{\frac{4m}{3}-1} + 2^{\frac{2m}{3}-1} - 2$
$2^{m-2} \pm 2^{\frac{2m}{3}-1}$	$2^{\frac{4m}{3}-2} - 2^{\frac{2m}{3}-2}$
2^{m-1}	1

Proof. From Lemma 4.4, we conclude that the dimension of $\mathcal{C}(f)^{\bar{D}}$ is $\frac{5m}{3}$, the possible weights in $\mathcal{C}(f)^{\bar{D}}$ are given in the set $\{0, 2^{m-1}, 2^{m-2}, 2^{m-2} \pm 2^{\frac{2m}{3}-1}\}$ and the weight 2^{m-1} occurs 1 time.

Denote $w_1 = 2^{m-2}$, $w_2 = 2^{m-2} - 2^{\frac{2m}{3}-1}$ and $w_3 = 2^{m-2} + 2^{\frac{2m}{3}-1}$. Let A_{w_i} be the number of the codewords with weight w_i in $\mathcal{C}(f)^{\bar{D}}$. Note that the all-one vector is a codeword of $\mathcal{C}(f)^{\bar{D}}$. It then follows that all codewords in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ have even weights. It is easily seen that the minimum weight

19

in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ cannot be 2. Consequently, the minimum weight in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is at least 4. From the first three Pless power moments, we have

$$\begin{cases} \sum_{i=1}^{3} A_{w_i} = 2^{\frac{5m}{3}} - 2; \\ \sum_{i=1}^{3} w_i A_{w_i} = 2^{\frac{8m}{3}-2} - 2^{m-1}; \\ \sum_{i=1}^{3} w_i^2 A_{w_i} = 2^{\frac{8m}{3}-2}(2^{m-1}+1) - 2^{2m-2}. \end{cases}$$

Solving this system of equations, we obtain $A_{w_1} = 2^{\frac{5m}{3}} - 2^{\frac{4m}{3}-1} + 2^{\frac{2m}{3}-1} - 2$, $A_{w_2} = A_{w_3} = 2^{\frac{4m}{3}-2} - 2^{\frac{2m}{3}-2}$.

We now consider the minimum distance of $(\mathcal{C}(f)^{\bar{D}})^{\perp}$. We have already proved that

$$d_H\left((\mathcal{C}(f)^{\bar{D}})^{\perp}\right) \geq 4.$$

If there exists a $[2^{m-1}, 2^{m-1} - \frac{5m}{3}]$ binary code with Hamming distance at least 5, then

$$\sum_{i=0}^{2} \binom{2^{m-1}}{i} = 1 + 2^{m-1} + 2^{m-2} \cdot (2^{m-1} - 1) > 2^{\frac{5m}{3}},$$

which contradicts the sphere packing bound. Hence, $d_H\left((\mathcal{C}(f)^{\bar{D}})^{\perp}\right) = 4$ and $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is distance-optimal to the sphere packing bound. $\square$

Example 4.6 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 4.5. Let $m = 9$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[256, 15, 96]$ and its dual has parameters $[256, 241, 4]$.*

We settled the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.5, but do not know if the corresponding code $\mathcal{C}(f)$ was studied in the literature or not.

4.3 The case that $f(x) = \mathrm{Tr}_k^m(x^{2^k+1})$

In this subsection, we study the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual for $f(x) = \mathrm{Tr}_k^m(x^{2^k+1})$, where k divides m. It is easy to see that $f(x) = 0$ if $k = \frac{m}{2}$. In the following, we just consider the case that $k \notin \{m, \frac{m}{2}\}$. We begin with the following lemma.

Lemma 4.7 *Let $\mathcal{C}(f)^{\bar{D}}$ be the punctured code defined in (2) with the position set D in (4). Let $f(x) = \mathrm{Tr}_k^m(x^{2^k+1})$, where k divides m and $k \notin \{m, \frac{m}{2}\}$. Let $t = 2^{\frac{m+2k-2}{2}}$ if $v_2(m) > v_2(k)+1$, and $t = 2^{\frac{m+2k-4}{2}}$ if $v_2(m) = v_2(k)+1$, and $t = 2^{\frac{m+k-4}{2}}$ if $v_2(m) = v_2(k)$. Then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, k+m]$ code whose nonzero weights are in the set $\{2^{m-2}, 2^{m-1}, 2^{m-2} \pm t\}$.*

Proof. We prove the conclusions only for the case $v_2(m) > v_2(k)+1$. The conclusions for the other two cases can be similarly proved. We first determine the possible values of $W_f(a,b)$ for $(a,b) \in \mathbb{F}_{2^m}^2$, where $W_f(a,b)$ was defined in (5). Note that $\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1})) = \mathrm{Tr}(\mathrm{Tr}_k^m(a)x^{2^k+1})$. If $\mathrm{Tr}_k^m(a) = 0$, then

$$W_f(a,b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(bx)} = \begin{cases} 2^m, & \text{if } b = 0, \\ 0, & \text{if } b \neq 0. \end{cases}$$

20

Let $L = \{a \in \mathbb{F}_{2^m} : \mathrm{Tr}_k^m(a) = 0\}$, then $|L| = 2^{m-k}$. Hence, when (a, b) runs over $L \times \mathbb{F}_{2^m}$, we have

$$W_f(a, b) - W_f(a, b + 1) = \begin{cases} 0, & \text{occuring } 2^{m+k} - 2^{m-k+1} \text{ times,} \\ 2^m, & \text{occuring } 2^{m-k} \text{ times,} \\ -2^m, & \text{occuring } 2^{m-k} \text{ times.} \end{cases} \tag{17}$$

If $\mathrm{Tr}_k^m(a) \neq 0$, similar to the discussions in (15), we have

$$W_f^2(a, b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1})+bx)} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a\mathrm{Tr}_k^m(xy^{2^k}+x^{2^k}y))}$$

$$= 2^m \sum_{\substack{x \in \mathbb{F}_{2^m} \\ x + x^{2^{2k}} = 0}} (-1)^{\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1})+bx)}$$

$$= 2^m \cdot \sum_{x \in \mathbb{F}_{2^{2k}}} (-1)^{\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1})+bx)},$$

as $v_2(m) > v_2(k) + 1$. Then by (7) we obtain

$$W_f^2(a, b) = \begin{cases} 2^{m+2k}, & \text{if } \mathrm{Tr}\left(a\mathrm{Tr}_k^m(x^{2^k+1}) + bx\right) = 0 \text{ for all } x \in \mathbb{F}_{2^{2k}}, \\ 0, & \text{otherwise.} \end{cases}$$

Clearly, if $\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1}) + bx) = 0$ for all $x \in \mathbb{F}_{2^{2k}}$, then $\mathrm{Tr}(a\mathrm{Tr}_k^m(x^{2^k+1}) + (b+1)x) = \mathrm{Tr}(x) = \frac{m}{2k}\mathrm{Tr}_1^{2k}(x)$. Hence, $W_f(a, b) - W_f(a, b + 1) \in \{0, \pm 2^{\frac{m+2k+2}{2}}\}$ for $\mathrm{Tr}_k^m(a) \neq 0$. Combining this with (17), when (a, b) runs through $\mathbb{F}_{2^m}^2$, we have

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

and each of the values $\pm 2^m$ occurs 2^{m-k} times. Then $\mathrm{wt}_H(\mathbf{c}(a, b)) = 0$ and $\mathrm{wt}_H(\mathbf{c}(a, b)) = 2^{m-1}$ both occur 2^{m-k} times and every nonzero weight in $\mathcal{C}(f)^{\bar{D}}$ belongs to the set $\{2^{m-2}, 2^{m-1}, 2^{m-2} \pm 2^{\frac{m+2k-2}{2}}\}$ by (12) . Hence, $\mathcal{C}(f)^{\bar{D}}$ is degenerate and has dimension $m + k$. This completes the proof. $\square$

Using Lemma 4.7 and similar discussions in the proof of Theorem 4.2, one can prove the following theorem.

Theorem 4.8 *Follow the notation and conditions introduced in Lemma 4.7. Then $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{m-1}, m + k, 2^{m-2} - t]$ code with the weight distribution in Table 9. Its dual has parameters $[2^{m-1}, 2^{m-1} - m - k, 4]$, and is distance-optimal with respect to the sphere packing bound.*

Example 4.9 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 4.8. Let $m = 5$ and $k = 1$. Then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[16, 6, 6]$ and its dual has parameters $[16, 10, 4]$. Both codes are optimal according to the tables of best codes known in [22].*

We settled the parameters and weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.8, but do not know if the corresponding code $\mathcal{C}(f)$ was studied in the literature or not.

Table 9: The weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 4.8

Weight	Multiplicity
0	1
2^{m-2}	$2^{m+k} - 2 + 2^{2m-3} \cdot (1 - 2^k)/t^2$
$2^{m-2} \pm t$	$2^{2m-4} \cdot (2^k - 1)/t^2$
2^{m-1}	1

5 Some punctured codes of binary linear codes from cyclotomic classes

In this section, we settle the weight distribution of the punctured code $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual, where the position set D is a cyclotomic class and $f(x) = x^d$ for some integer d. Let γ be a primitive element of $\mathbb{F}_{2^m}$ and let t be a positive integer dividing $2^m - 1$. Let $D = \langle \gamma^t \rangle$, which is the subgroup of $\mathbb{F}_{2^m}^*$ generated by γ^t. The multiplicative cosets of D are called the cyclotomic classes of order t in $\mathbb{F}_{2^m}^*$. Recall that the binary punctured code is

$$\mathcal{C}(f)^{\bar{D}} = \{\mathbf{c}(a,b) = (\text{Tr}(ax^d + bx))_{x \in D} : a, b \in \mathbb{F}_{2^m}\} \tag{18}$$

if $f(x) = x^d$. Since $|D| = \frac{2^m - 1}{t}$, the length n of $\mathcal{C}(f)^{\bar{D}}$ is $\frac{2^m - 1}{t}$. It is easily seen that the Hamming weight of the codeword $\mathbf{c}(a,b)$ is given by

$$\text{wt}_{\text{H}}(\mathbf{c}(a,b)) = n - \left| \left\{ x \in D : \ \text{Tr}\left(ax^d + bx\right) = 0 \right\} \right| = \frac{1}{2}\left(n - \sum_{x \in D}(-1)^{\text{Tr}(ax^d + bx)}\right). \tag{19}$$

To determine the weight distribution of $\mathcal{C}(f)^{\bar{D}}$, we need to determine the value distribution of

$$T(a,b) = \sum_{x \in D}(-1)^{\text{Tr}(ax^d + bx)} \tag{20}$$

for (a,b) running through $\mathbb{F}_{2^m}^2$. In the following, we propose several classes of linear codes with few weights by choosing proper d and t.

5.1 The case that $d = \frac{2^m - 1}{3}$ and $\text{lcm}(3, t) \,|\, (2^{\frac{m}{2}} + 1)$

In this subsection, we always assume that $v_2(m) = 1$, $d = \frac{2^m - 1}{3}$ and t is a positive integer satisfying $\text{lcm}(3, t) \,|\, (2^{\frac{m}{2}} + 1)$. If $3 \,|\, t$, then $x^{\frac{2^m - 1}{3}} = 1$ for any $x \in D$. From (20) we have

$$T(a,b) = \sum_{x \in D}(-1)^{\text{Tr}(a + bx)}. \tag{21}$$

If $3 \nmid t$, then

$$T(a,b) = \sum_{x \in \langle \gamma^{3t} \rangle} (-1)^{\mathrm{Tr}(a+bx)} + \sum_{x \in \langle \gamma^{3t} \rangle} (-1)^{\mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}+b\gamma^t x)} + \sum_{x \in \langle \gamma^{3t} \rangle} (-1)^{\mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}+b\gamma^{2t} x)}$$

$$= \frac{1}{3t} \left(\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(a+bx^{3t})} + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}+b\gamma^t x^{3t})} + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}+b\gamma^{2t} x^{3t})} \right)$$

$$= \frac{1}{3t} \left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a+bx^{3t})} + \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}+b\gamma^t x^{3t})} + \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}+b\gamma^{2t} x^{3t})} \right)$$

$$- \frac{1}{3t} \left((-1)^{\mathrm{Tr}(a)} + (-1)^{\mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}})} + (-1)^{\mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}})} \right).$$

$$(22)$$

In order to obtain the possible values of $T(a,b)$ for $3 \nmid t$, we need the following lemma.

Lemma 5.1 *Let N be the number of zeros in the sequence* $\left(\mathrm{Tr}(a), \ \mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}), \ \mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}) \right)$. *When a runs over $\mathbb{F}_{2^m}$, we have*

$$N = \begin{cases} 3, & \text{occuring } 2^{m-2} \text{ times}, \\ 1, & \text{occuring } 3 \cdot 2^{m-2} \text{ times}. \end{cases}$$

Proof. Obviously, the possible values of N are 0, 1, 2 or 3. Let N_i denote the number of times that $N = i$ when a runs over $\mathbb{F}_{2^m}$, where $i \in \{0,1,2,3\}$. Then

$$N_3 = \frac{1}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_0 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(y_1 a)} \sum_{y_1 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(y_1 a\gamma^{\frac{2^m-1}{3}})} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(y_2 a\gamma^{\frac{2(2^m-1)}{3}})}$$

$$= \frac{1}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_0 \in \mathbb{F}_2} \sum_{y_1 \in \mathbb{F}_2} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}\left(a(y_0+y_1\gamma^{\frac{2^m-1}{3}}+y_2\gamma^{\frac{2(2^m-1)}{3}}) \right)}.$$

Note that $y_0 + y_1\gamma^{\frac{2^m-1}{3}} + y_2\gamma^{\frac{2(2^m-1)}{3}} = 0$ if and only if $y_0 = y_1 = y_2 = 0$ or $y_0 = y_1 = y_2 = 1$. Then

$$N_3 = \frac{1}{2^3} (2^m + 2^m) = 2^{m-2}.$$

Due to symmetry, we have

$$N_2 = \frac{3}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_0 \in \mathbb{F}_2} (-1)^{y_0(\mathrm{Tr}(a)-1)} \sum_{y_1 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(y_1 a\gamma^{\frac{2^m-1}{3}})} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(y_2 a\gamma^{\frac{2(2^m-1)}{3}})}$$

$$= \frac{3}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_1 \in \mathbb{F}_2} \sum_{y_0 \in \mathbb{F}_2} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}(a(y_0+y_1\gamma^{\frac{2^m-1}{3}}+y_2\gamma^{\frac{2(2^m-1)}{3}})-y_0)}$$

$$= \frac{3}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_1 \in \mathbb{F}_2} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}\left(a(y_1\gamma^{\frac{2^m-1}{3}}+y_2\gamma^{\frac{2(2^m-1)}{3}}) \right)} -$$

$$\frac{3}{2^3} \sum_{a \in \mathbb{F}_{2^m}} \sum_{y_1 \in \mathbb{F}_2} \sum_{y_2 \in \mathbb{F}_2} (-1)^{\mathrm{Tr}\left(a(1+y_1\gamma^{\frac{2^m-1}{3}}+y_2\gamma^{\frac{2(2^m-1)}{3}}) \right)}.$$

23

Note that $y_1\gamma^{\frac{2^m-1}{3}} + y_2\gamma^{\frac{2(2^m-1)}{3}} = 0$ if and only if $y_1 = y_2 = 0$, and $1 + y_1\gamma^{\frac{2^m-1}{3}} + y_2\gamma^{\frac{2(2^m-1)}{3}} = 0$ if and only if $y_1 = y_2 = 1$. Then

$$N_2 = \frac{1}{2^3}\left(2^m - 2^m\right) = 0.$$

Similarly, we can prove that $N_1 = 3 \cdot 2^{m-2}$ and $N_0 = 0$. $\square$

Theorem 5.2 Let $v_2(m) = 1$, $d = \frac{2^m-1}{3}$ and t be a positive integer satisfying $lcm(3,t) \,|\, (2^{\frac{m}{2}}+1)$. Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (18) and $D = \langle\gamma^t\rangle$. If $t \neq 2^{\frac{m}{2}}+1$, then the following statements hold.

(1) If $3\,|\,t$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[\frac{2^m-1}{t}, m+1]$ code with the weight distribution in Table 10. Its dual has parameters $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - m - 1, 4]$, and is distance-optimal with respect to the sphere packing bound.

Table 10: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $3\,|\,t$ in Theorem 5.2

Weight	Multiplicity
0	1
$\frac{1}{2t}\left(2^m - 2 - 2^{\frac{m}{2}}\right)$	$\frac{(t-1)(2^m-1)}{t}$
$\frac{1}{2t}\left(2^m + 2^{\frac{m}{2}}\right)$	$\frac{(t-1)(2^m-1)}{t}$
$\frac{1}{2t}\left(2^m - 2 + (t-1)2^{\frac{m}{2}}\right)$	$\frac{(2^m-1)}{t}$
$\frac{1}{2t}\left(2^m - (t-1)2^{\frac{m}{2}}\right)$	$\frac{(2^m-1)}{t}$
$\frac{2^m-1}{t}$	1

(2) If $3 \nmid t$, then $\mathcal{C}(f)^{\bar{D}}$ is a $[\frac{2^m-1}{t}, m+2]$ code with the weight distribution in Table 11. Its dual has parameters $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - m - 2, 3]$.

Table 11: Weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ for $3 \nmid t$ in Theorem 5.2

Weight	Multiplicity
0	1
$\frac{2^m-1}{2t} - \frac{1}{2t}\left((t-1)2^{\frac{m}{2}} - 1\right)$	$\frac{2^m-1}{t}$
$\frac{2^m-1}{2t} + \frac{1}{6t}\left((3t-1)2^{\frac{m}{2}} - 1\right)$	$\frac{2^{m+1}-2}{t}$
$\frac{1}{2t}\left(2^m + 2^{\frac{m}{2}}\right)$	$\frac{(t-1)(2^m-1)}{t}$
$\frac{2^m-1}{2t} - \frac{1}{6t}\left(2^{\frac{m}{2}} + 1\right)$	$\frac{3(t-1)(2^m-1)}{t}$
$\frac{2^m-1}{2t} - \frac{1}{6t}\left((3t+1)2^{\frac{m}{2}} + 1\right)$	$\frac{2^m-1}{t}$
$\frac{2(2^m-1)}{3t}$	3

Proof. We prove this theorem case by case as follows.

Case 1: $3 \mid t$. From (21) we have

$$T(a,b) = (-1)^{\mathrm{Tr}(a)} \sum_{x \in E} (-1)^{\mathrm{Tr}(bx)} = \frac{1}{t}(-1)^{\mathrm{Tr}(a)} \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(bx^t)}$$

$$= \frac{1}{t}(-1)^{\mathrm{Tr}(a)} - \frac{1}{t}(-1)^{\mathrm{Tr}(a)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(bx^t)}.$$

If $b = 0$, it is clear that

$$T(a,0) = \begin{cases} \frac{(1-2^m)}{t}, & \text{if } \mathrm{Tr}(a) = 0, \\ \frac{(2^m-1)}{t}, & \text{if } \mathrm{Tr}(a) = 1. \end{cases} \tag{23}$$

If $b \neq 0$, then b can be written as $b = \gamma^i$, where γ is a primitive element of $\mathbb{F}_{2^m}$ and $1 \leq i \leq 2^m - 1$. From Lemma 2.4 we have

$$T(a, \gamma^i) = \begin{cases} \frac{1}{t}(-1)^{\mathrm{Tr}(a)} - \frac{1}{t}(-1)^{\mathrm{Tr}(a)}(-1)^s 2^{\frac{m}{2}}, & \text{if } i \not\equiv 0 \pmod{t}, \\ \frac{1}{t}(-1)^{\mathrm{Tr}(a)} - \frac{1}{t}(-1)^{\mathrm{Tr}(a)}(-1)^{s-1}(t-1)2^{\frac{m}{2}}, & \text{if } i \equiv 0 \pmod{t}, \end{cases} \tag{24}$$

as t is a positive integer such that $\mathrm{lcm}(3,t) \mid (2^{m/2} + 1)$. Hence, when (a,b) runs over $\mathbb{F}_{2^m}^2$, by (23) and (24), the value distribution of $T(a,b)$ is given as follows:

$$T(a,b) = \begin{cases} \frac{(1-2^m)}{t}, & \text{occuring } 2^{m-1} \text{ times}, \\ \frac{(2^m-1)}{t}, & \text{occuring } 2^{m-1} \text{ times}, \\ \frac{1}{t}\left(2^{\frac{m}{2}}+1\right), & \text{occuring } \frac{2^{m-1}(t-1)(2^m-1)}{t} \text{ times}, \\ -\frac{1}{t}\left(2^{\frac{m}{2}}+1\right), & \text{occuring } \frac{2^{m-1}(t-1)(2^m-1)}{t} \text{ times}, \\ \frac{1}{t} - \frac{1}{t}(t-1)2^{\frac{m}{2}}, & \text{occuring } \frac{2^{m-1}(2^m-1)}{t} \text{ times}, \\ -\frac{1}{t} + \frac{1}{t}(t-1)2^{\frac{m}{2}}, & \text{occuring } \frac{2^{m-1}(2^m-1)}{t} \text{ times}. \end{cases} \tag{25}$$

From (19) and (25), we know that the Hamming weight 0 occurs 2^{m-1} times when (a,b) runs through $\mathbb{F}_{2^m}^2$. Hence, in this case, $\mathcal{C}(f)^{\bar{D}}$ is degenerate and has dimension $m + 1$. Dividing each frequency by 2^{m-1} in (25), we get the weight distribution in Table 10 from (19). From the first five Pless power moments and the weight distribution of $\mathcal{C}(f)^{\bar{D}}$, we deduce that the dual of $\mathcal{C}(f)^{\bar{D}}$ is a $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - m - 1, 4]$ code. If there exists a $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - m - 1]$ binary code with Hamming distance at least 5, then we have

$$\sum_{i=0}^{2} \binom{\frac{2^m-1}{t}}{i} = 1 + \frac{2^m-1}{t} + \frac{2^m-1}{2t} \cdot (\frac{2^m-1}{t} - 1) > 2^{m+1}$$

as $t \neq 2^{\frac{m}{2}} + 1$, which is contrary to the sphere packing bound. Hence, the dual code $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is distance-optimal with respect to the sphere packing bound.

Case 2: $3 \nmid t$. From (22) we have

$$T(a,b) = \frac{1}{3t}\left((-1)^{\mathrm{Tr}(a)}\left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(bx^{3t})} - 1\right) + (-1)^{\mathrm{Tr}(a\gamma^{\frac{t(2^m-1)}{3}})}\left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(b\gamma^t x^{3t})} - 1\right)\right.$$

$$\left. + (-1)^{\mathrm{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}})}\left(\sum_{x \in \mathbb{F}_{2^m}} (-1)^{(b\gamma^{2t} x^{3t})} - 1\right)\right).$$

25

If $b = 0$, it is clear that

$$T(a,0) = \frac{2^m - 1}{3t}\left((-1)^{\text{Tr}(a)} + (-1)^{\text{Tr}(a\gamma^{\frac{t(2^m-1)}{3}})} + (-1)^{\text{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}})}\right).$$

From Lemma 5.1 we have

$$T(a,0) = \begin{cases} \frac{(2^m-1)}{t}, & \text{occuring } 2^{m-2} \text{ times}, \\ -\frac{(2^m-1)}{3t}, & \text{occuring } 3 \cdot 2^{m-2} \text{ times}. \end{cases} \tag{26}$$

If $b \neq 0$, then b can be written as $b = \gamma^i$, where γ is a primitive element of $\mathbb{F}_{2^m}$ and $1 \le i \le 2^m - 1$. From Lemma 2.4 we have

$$T(a,\gamma^i) = \begin{cases} \frac{1}{3t} + \frac{1}{3t}\sum_{x\in\mathbb{F}_{2^m}}\left((-1)^{\text{Tr}(\gamma^i x^{3t})} - (-1)^{\text{Tr}(\gamma^{i+t}x^{3t})} - (-1)^{\text{Tr}(\gamma^{i+2t}x^{3t})}\right), \\ \qquad\qquad \text{if } \text{Tr}(a) = 0, \text{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}) = 1 \text{ and } \text{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}) = 1, \\ \frac{1}{3t} + \frac{1}{3t}\sum_{x\in\mathbb{F}_{2^m}}\left(-(-1)^{\text{Tr}(\gamma^i x^{3t})} + (-1)^{\text{Tr}(\gamma^{i+t}x^{3t})} - (-1)^{\text{Tr}(\gamma^{i+2t}x^{3t})}\right), \\ \qquad\qquad \text{if } \text{Tr}(a) = 1, \text{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}) = 0 \text{ and } \text{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}) = 1, \\ \frac{1}{3t} + \frac{1}{3t}\sum_{x\in\mathbb{F}_{2^m}}\left(-(-1)^{-\text{Tr}(\gamma^i x^{3t})} - (-1)^{\text{Tr}(\gamma^{i+t}x^{3t})} + (-1)^{\text{Tr}(\gamma^{i+2t}x^{3t})}\right), \\ \qquad\qquad \text{if } \text{Tr}(a) = 1, \text{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}) = 1 \text{ and } \text{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}) = 0, \\ -\frac{1}{t} + \frac{1}{3t}\sum_{x\in\mathbb{F}_{2^m}}\left((-1)^{\text{Tr}(\gamma^i x^{3t})} + (-1)^{\text{Tr}(\gamma^{i+t}x^{3t})} + (-1)^{\text{Tr}(\gamma^{i+2t}x^{3t})}\right), \\ \qquad\qquad \text{if } \text{Tr}(a) = \text{Tr}(a\gamma^{\frac{t(2^m-1)}{3}}) = \text{Tr}(a\gamma^{\frac{2t(2^m-1)}{3}}) = 0. \end{cases} \tag{27}$$

Clearly, one of $3t \mid i$, $3t \mid (i+t)$ and $3t \mid (i+2t)$ holds if and only if $t \mid i$ for any positive integer t and $1 \le i \le 2^m - 1$. Otherwise, $3t \nmid i$, $3t \nmid (i+t)$ and $3t \nmid (i+2t)$. Then combining Lemma 2.4, (26) and (27), it is not hard to see that when (a,b) runs over $\mathbb{F}_{2^m}^2$, the value distribution of $T(a,b)$ is given as follows:

$$T(a,b) = \begin{cases} \frac{(2^m-1)}{t}, & \text{occuring } 2^{m-2} \text{ times}, \\ -\frac{(2^m-1)}{3t}, & \text{occuring } 3 \cdot 2^{m-2} \text{ times}, \\ -\frac{1}{t} + \frac{1}{t}\left((t-1)2^{\frac{m}{2}}\right), & \text{occuring } \frac{(2^m-1)2^{m-2}}{t} \text{ times}, \\ \frac{1}{3t}\left(1 - 3\cdot2^{\frac{m}{2}}\right), & \text{occuring } \frac{(t-1)(2^m-1)2^{m-2}}{t} \text{ times}, \\ \frac{1}{3t}\left(1 - (3t-1)2^{\frac{m}{2}}\right), & \text{occuring } \frac{(2^m-1)2^{m-1}}{t} \text{ times}, \\ \frac{1}{3t}\left(2^{\frac{m}{2}} + 1\right), & \text{occuring } \frac{3(t-1)(2^m-1)2^{m-2}}{t} \text{ times}, \\ \frac{1}{3t}\left((3t+1)2^{\frac{m}{2}} + 1\right), & \text{occuring } \frac{(2^m-1)2^{m-2}}{t} \text{ times}. \end{cases} \tag{28}$$

By a similar analysis to Case 1, we obtain the weight distribution of $\mathcal{C}(f)^{\bar{D}}$ and the parameters of its dual. This completes the proof. $\square$

Example 5.3 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 5.2. Let $m = 6$ and $t = 3$, then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[21, 7, 8]$ and its dual has parameters $[21, 14, 4]$. The two codes are optimal according to the tables of best codes known in [22].*

Remark 5.4 If $t = 2^{\frac{m}{2}} + 1$, it is easy to check that $\mathcal{C}(f)^{\bar{D}}$ is a $[2^{\frac{m}{2}} - 1, \frac{m}{2} + 1, 2^{\frac{m}{2}-1} - 1]$ code with the weight enumerator

$$1 + (2^{\frac{m}{2}} - 1)(x^{2^{\frac{m}{2}-1}-1} + x^{2^{\frac{m}{2}-1}}) + x^{2^{\frac{m}{2}}-1},$$

which is optimal with respect to the Griesmer bound. Its dual has parameters $[2^{\frac{m}{2}} - 1, \frac{m}{2} + 1, 4]$, which is distance-optimal with respect to the sphere packing bound. By the Assmus-Mattson theorem [2], the code $\mathcal{C}(f)^{\bar{D}}$ and its dual support 2-designs [13, Chapter 4]. The reader is informed that in the special case $t = 2^{\frac{m}{2}} + 1$, the code $\mathcal{C}(f)^{\bar{D}}$ is permutation-equivalent to a singly punctured code of the first-order Reed-Muller code [37].

5.2 The case that $d(2^k + 1) \equiv 2^{\frac{m}{2}} + 1 \pmod{2^m - 1}$ and $t = 2^k + 1$

In this subsection, we always assume that m is even, $d(2^k + 1) \equiv 2^{\frac{m}{2}} + 1 \pmod{2^m - 1}$ and $t = 2^k + 1$. From (20) it follows that

$$
\begin{aligned}
T(a, b) &= \sum_{x \in D}(-1)^{\mathrm{Tr}(ax^d + bx)} = \frac{1}{2^k + 1}\sum_{x \in \mathbb{F}_{2^m}^*}(-1)^{\mathrm{Tr}(ax^{2^{m/2}+1}+bx^{2^k+1})} \\
&= \frac{1}{2^k + 1}\sum_{x \in \mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(ax^{2^{m/2}+1}+bx^{2^k+1})} - \frac{1}{2^k + 1}.
\end{aligned}
\tag{29}
$$

If $k = \frac{m}{2}$, by Lemma 2.4, (19) and (29), $\mathcal{C}(f)^{\bar{D}}$ is a one-weight code with parameters $[2^{\frac{m}{2}}-1, \frac{m}{2}, 2^{\frac{m}{2}-1}]$, and is permutation-equivalent to a Simplex code. In the following, we determine the parameters and the weight distribution of $\mathcal{C}(f)^{\bar{D}}$ and the parameters of the dual code $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ for $k \neq \frac{m}{2}$.

Theorem 5.5 Let d satisfy the condition $d(2^k + 1) \equiv 2^{\frac{m}{2}} + 1 \pmod{2^m - 1}$. Let $t = 2^k + 1$ and $k \neq \frac{m}{2}$. Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code defined in (18). Then $\mathcal{C}(f)^{\bar{D}}$ is a $[\frac{2^m-1}{t}, \frac{3m}{2}, \frac{2^{m-1}-2^{\frac{m}{2}+k-1}}{t}]$ code with the weight distribution in Table 12. If $k > 1$, its dual has parameters $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - \frac{3m}{2}, 3]$. If $k = 1$ and $m \neq 6$, its dual has parameters $[\frac{2^m-1}{t}, \frac{2^m-1}{t} - \frac{3m}{2}, 4]$, and is distance-optimal with respect to the sphere packing bound. If $k = 1$ and $m = 6$, its dual has parameters $[21, 12, 5]$, and is optimal according to the tables of best codes known in [22].

Table 12: Weight distribution of $\mathcal{C}(f)^{\bar{D}}$ in Theorem 5.5

Weight	Multiplicity
0	1
$\frac{2^{m-1}+2^{\frac{m}{2}-1}}{t}$	$\frac{2^{3k}(2^{\frac{m}{2}}-1)(2^m-2^{m-2k}-2^{m-3k}+2^{\frac{m}{2}}-2^{\frac{m}{2}-k}+1)}{t^2(2^k-1)}$
$\frac{2^{m-1}-2^{\frac{m}{2}+k-1}}{t}$	$\frac{2^k(2^m-1)(2^{\frac{m}{2}}+2^{\frac{m}{2}-k}+2^{\frac{m}{2}-2k}+1)}{t^2}$
$\frac{2^{m-1}+2^{\frac{m}{2}+2k-1}}{t}$	$\frac{(2^{\frac{m}{2}-k}-1)(2^m-1)}{t^2(2^k-1)}$

Proof. It is clear that $\mathrm{Tr}\left(ax^{2^{m/2}+1}\right) = \mathrm{Tr}_1^{\frac{m}{2}}\left((a + a^{2^{m/2}})x^{2^{m/2}+1}\right)$ and $a + a^{2^{m/2}} \in \mathbb{F}_{2^{\frac{m}{2}}}$ for any $a \in \mathbb{F}_{2^m}$. Obviously, $a + a^{2^{m/2}}$ runs through $\mathbb{F}_{2^{\frac{m}{2}}}$ with multiplicity $2^{\frac{m}{2}}$ when a runs through $\mathbb{F}_{2^m}$.

Let
$$K = \left\{ x \in \mathbb{F}_{2^m} : x + x^{2^{m/2}} \right\}.$$

Then $\mathbf{c}(a,b) = \mathbf{c}(a,b+\delta)$ for any $\delta \in K$. Since $t \mid (2^m - 1)$ and $t = 2^k + 1$, it is easy to prove that there exists a positive integer ℓ such that $\ell(2^k + 1) \equiv 2^{\frac{m}{2}} + 1 \pmod{2^m - 1}$ if and only if $v_2(k) = v_2(\frac{m}{2})$ and $k \mid \frac{m}{2}$. From Lemma 2.5, (19) and (29), the desired weight distribution of $\mathcal{C}(f)^{\bar{D}}$ follows.

Let $A_i^{\perp}$ be the number of the codewords with weight i in $(\mathcal{C}(f)^{\bar{D}})^{\perp}$. By the first four Pless power moments, we get that $A_1^{\perp} = A_2^{\perp} = 0$ and

$$A_3^{\perp} = \frac{1}{48(2^k + 1)^5(2^{2k} - 1)}\left((2^{7k} + 2^{6k+1} + 6 \cdot 2^{2k} + 4 \cdot 2^{3k} + 7 \cdot 2^k + 2 - 3 \cdot 2^{5k} - 10 \cdot 2^{4k} - 9 \cdot 2^{3k}) \cdot 2^{\frac{3m}{2}}\right.$$
$$\left. + (3 \cdot 2^{5k} + 10 \cdot 2^{4k} + 5 \cdot 2^{3k} - 6 \cdot 2^{2k} - 7 \cdot 2^k - 2) \cdot 2^{\frac{5m}{2}}\right).$$

We can check that $A_3 = 0$ if $k = 1$ and $A_3 \neq 0$ if $k > 1$. If $k = 1$, by the fifth Pless power moment, we obtain that

$$A_4^{\perp} = \frac{1}{6^4}(2^{4m} + 70 \cdot 2^{\frac{5m}{2}} - 6 \cdot 2^{\frac{7m}{2}} - 25 \cdot 2^{3m}) + \frac{2^{2m}}{54} - \frac{2^{\frac{3m}{2}+2}}{81}.$$

It is easy to check that $A_4^{\perp} = 0$ if and only if $m = 6$. Similarly to the proof of Theorem 5.2, we can show that $(\mathcal{C}(f)^{\bar{D}})^{\perp}$ is distance-optimal with respect to the sphere packing bound if $k = 1$ and $m \neq 6$. By the sixth Pless power moment, we obtain $A_5^{\perp} \neq 0$. This completes the proof. $\square$

Example 5.6 *Let $\mathcal{C}(f)^{\bar{D}}$ be the linear code in Theorem 5.5. Let $m = 10$ and $k = 1$. Then $\mathcal{C}(f)^{\bar{D}}$ has parameters $[341, 15, 160]$. Its dual has parameters $[341, 326, 4]$ and is distance-optimal with respect to the sphere packing bound.*

We settled the parameters and weight distribution of the code $\mathcal{C}(f)^{\bar{D}}$ in Theorem 5.5, but do not know if the corresponding code $\mathcal{C}(f)$ was studied in the literature or not.

6 Summary and concluding remarks

The main contributions of this paper are the following:

1. We obtained several classes of binary punctured codes with three weights, or four weights, or five weights, or six weights, and determined their weight distributions (see Theorem 3.3, Corollary 3.6, Theorem 4.2, Theorem 4.5, Theorem 4.8, Theorem 5.2 and Theorem 5.5).

2. We presented several classes of self-complementary linear codes. Almost all of their duals are distance-optimal with respect to the sphere packing bound (see Theorem 3.3, Corollary 3.6, Theorem 4.2, Theorem 4.5, Theorem 4.8, Theorem 5.2 and Theorem 5.5).

3. We got some distance-optimal codes with specific parameters (see Example 3.4, Example 3.7, Example 4.3, Example 4.9 and Example 5.3).

A constructed binary linear code $\mathcal{C}$ is new if one of the following happens:

- No binary linear code with the same parameters was documented in the literature.

- Some binary linear codes with the same parameters as $\mathcal{C}$ were documented in the literature, but their weight distributions are different from the weight distribution of $\mathcal{C}$.

- Some binary linear codes with the same parameters and weight distribution as those of $\mathcal{C}$ were documented in the literature, but they are not permutation-equivalent to $\mathcal{C}$.

Except the class of codes in Remark 5.4, every other class of binary codes presented in this paper would be new, as we have not found a class of binary codes with the same parameters and weight distributions in the literature as those codes documented in this paper.

Starting from Section 2, we restricted our discussions on finite fields with characteristic 2. The position sets were constructed from some trace functions and cyclotomic classes. It would be interesting to extend some of the results in this paper to the case that $q \geq 3$.

Finally, we make some comments on the puncturing and shortening techniques. As mentioned in the introductory section, every projective linear code over $\mathbb{F}_q$ is a punctured Simplex code over $\mathbb{F}_q$ and a shortened code of a Hamming code over $\mathbb{F}_q$. However, it is in general very hard to determine the parameters of punctured codes of Simplex codes and shortened codes of Hamming codes [37, 56]. Hence, we still need to study punctured and shortened codes of other families of linear codes. For a given linear code $\mathcal{C}$ and a set T of coordinate positions in $\mathcal{C}$, it may be possible to determine the parameters of the punctured code $\mathcal{C}^T$ when $|T|$ is small, but it is very hard to do so in general if $|T|$ is large [45].

References

[1] R. Anderson, C. Ding, T. Helleseth, T. Kløve, How to build robust shared control systems, Des. Codes Cryptogr. 15 (1998) 111-124.

[2] E. F. Assmus Jr., H. F. Mattson Jr., New 5-designs, J. Combin. Theory 6(2) (1969) 122–151.

[3] L. Budaghyan, C. Carlet, A. Pott, New classes of almost Bent and almost perfect nonlinear polynomials, IEEE Trans. Inf. Theory 52(3) (2006) 1141–1152.

[4] A. R. Calderbank, J. M. Goethals, Three-weight codes and association schemes, Philips J .Res. 39 (1984) 143–152.

[5] A. R. Calderbank, W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97–122.

[6] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (1998) 125–156.

[7] C. Carlet, C. Ding, J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, IEEE Trans. Inf. Theory (51)(6) (2005) 2089–2102.

[8] R. S. Coulter, Further evaluations of Weil sums, Acta Arith. 86 (1998) 217–226.

[9] R. S. Coulter, The number of rational points of a class of Artin-Schreier curves, Finite Fields Appl. 8 (2002) 397–413.

[10] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, IEEE Trans. Inf. Theory 21(5) (1975) 575–576.

[11] C. Ding, Linear codes from some 2-designs, IEEE Trans. Inf. Theory 61 (2015) 3265–3275.

[12] C. Ding, A construction of binary linear codes from Boolean functions, Discrete Math. 339 (2016) 2288–2303.

[13] C. Ding, Designs from Linear Codes, World Scientific, Singapore, 2018.

[14] C. Ding, Z. Heng, The subfield codes of ovoid codes, IEEE Trans. Inf. Theory 65(8) (2019) 4715–4729.

[15] C. Ding, C. Li, N. Li, Z. Zhou, Three-weight cyclic codes and their weight distributions, Discrete Math. 339 (2016) 415–427.

[16] C. Ding, H. Niederreiter, Cyclotomic linear codes of order 3, IEEE Trans. Inf. Theory 53(6) (2007) 2274–2277.

[17] C. Ding, X. Wang, A coding theory construction of new systematic authentication codes, Theor. Comput. Sci. 330(1) (2005) 81–99.

[18] K. Ding, C. Ding, Binary linear codes with three weights, IEEE Commun. Lett. 18(11) (2014) 1879–1882.

[19] K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, IEEE Trans. Inf. Theory 61(11) (2015) 5835–5842.

[20] K. Feng, J. Luo, Value distribution of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inf. Theory 53(9) (2007) 3035–3041.

[21] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation function, IEEE Trans. Inf. Theory 14(1) (1968) 154–156.

[22] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de.

[23] Z. Heng, W. Wang, Y. Wang, Projective binary linear codes from special Boolean functions, Appl. Algebra Eng. Commun. Comput., https://doi.org/10.1007/s00200-019-00412-z.

[24] Z. Heng, Q. Yue, A class of binary linear codes with at most three weights, IEEE Commun. Lett. 19 (9) (2015) 1488–1491.

[25] Z. Heng, Q. Yue, C. Li, Three classes of linear codes with two or three weights, Discrete Math. 339 (2016) 2832–2847.

[26] H. D. L. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary msequences, Finite Fields Appl. 7 (2001) 253–286.

[27] X. D. Hou, A note on the proof of Niho's conjecture, SIAM J. Discrete Math. 18(2) (2004) 313–319.

[28] W. Huffman, V. Pless, Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, 2010.

[29] T. Kasami, Weight distribution formula for some class of cyclic codes, University of Illinois, Urbana, Rept. R-265, April 1966.

[30] T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem codes, University of Illinois, Urbana, Rept. R-317, August 1966.

[31] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary RM codes, Information and Control 18 (1971) 369–394.

[32] C. Li, S. Bae, S. Yang, Some two-weight and three-weight linear codes, Math. of Comm. 13(1) (2019) 195–211.

[33] C. Li, N. Li, T. Helleseth, C. Ding, The weight distribution of several classes of cyclic codes from APN monomials, IEEE Trans. Inf. Theory 60(8) (2014) 4710–4721.

[34] C. Li, Q. Yue, F. Fu, A construction of several classes of two-weight and three-weight linear codes, Appl. Algebra Eng. Commun. Comput. 28 (2017) 11–30.

[35] F. Li, Q. Wang, D. Lin, A class of three-weight and five-weight linear codes, Discrete Appl. Math. 241 (2018) 25–38.

[36] N. Li, S. Mesnager, Recent results and problems on constructions of linear codes from crypto-graphic functions, Cryptogr. Commun. 12 (2020) 965–986.

[37] Y. Liu, C. Ding, C. Tang, Shortened linear codes over finite fields, arXiv:2007.05901 [cs.IT].

[38] G. Luo, X. Cao, S. Xu, J. Mi, Binary linear codes with two or three weights from niho exponents, Cryptogr. Commun. 10 (2018) 301–318.

[39] J. Luo, K. Feng, On the weight distributions of two classes of cyclic codes, IEEE Trans. Inf. Theory 54(12) (2008) 5332–5344.

[40] J. Luo, Y. Tang, H. Wang, Cyclic codes and sequences: the generalized Kasami case, IEEE Trans. Inf. Theory 56 (5) (2010) 2130–2142.

[41] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, Amsterdam, 1997.

[42] J. M. Marko, A note on evaluations of some exponential sums, Acta Arith. 93 (2000) 117–119.

[43] S. Mesnager, Linear codes from functions, in *Concise Encyclopedia of Coding Theory*, W. C. Huffman, J.-L. Kim, P. Slolé (Eds.), pp. 463–526, CRC Press, New York, 2021.

[44] P. Tan, Z. Zhou, D. Tang, T. Helleseth, The weight distribution of a class of two-weight linear codes derived from Kloosterman sums, Cryptogr. Commun. 10 (2018) 291–299.

[45] C. Tang, C. Ding, M. Xiong, Codes, differentially δ-uniform functions and t-designs, IEEE Trans. Inf. Theory 66(6) (2020) 3691–3703.

[46] C. Tang, N. Li, Y. Qi, Z. Zhou, T. Helleseth, Linear codes with two or three weights from weakly regular bent functions, IEEE Trans. Inf. Theory 62(3) (2016) 1166–1176.

[47] C. Tang, Y. Qi, D. Huang, Two-weight and three-weight linear codes from square functions, IEEE Commun. Lett. 20(1) (2015) 29–32.

[48] D. Tang, C. Carlet, Z. Zhou, Binary linear codes from vectorial boolean functions and their weight distribution, Discrete Math. 340(12) (2017) 3055–3072.

[49] Z. Wan, Lectures on Finite Fields and Galois Rings, World Scientific, Singapore, 2003.

[50] Q. Wang, K. Ding, R. Xue, Binary linear codes with two weights, IEEE Commun. Lett. 19(7) (2015) 1097–1100.

[51] X. Wang, D. Zheng, L. Hu, X. Zeng, The weight distributions of two classes of binary codes, Finite Fields Appl. 34 (2015) 192–207.

[52] X. Wang, D. Zheng, H. Liu, Several classes of linear codes and their weight distributions, Appl. Algebra Eng. Commun. Comput. 30 (2019) 75–92.

[53] J. Wolfmann, Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, Discrete Math. 13(2) (1975) 185—211.

[54] Y. Xia, C. Li, Three-weight ternary linear codes from a family of power functions, Finite Fields Appl. 46 (2017) 17–37.

[55] C. Xiang, It is indeed a fundamental construction of all linear codes, arXiv:1610.06355.

[56] C. Xiang, C. Tang, C. Ding, Shortened linear codes from APN and PN functions, arXiv:2007.05923 [cs.IT].

[57] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory 52(2) (2006) 712–717.

[58] Z. Zhou, C. Ding, Seven classes of three-weight cyclic codes, IEEE Trans. Inf. Theory 61(10) (2013) 4120–4126.

[59] Z. Zhou, C. Ding, A class of three-weight cyclic codes, Finite Fields Appl. 25 (2014) 79–93.

[60] Z. Zhou, N. Li, C. Fan, T. Helleseth, Linear codes with two or three weights from quadratic bent functions, Des. Codes Cryptogr. 81 (2015) 1–13.