Advances in Mathematics of Communications
Vol. 22, 2026, pp. 132-146 (December 5, 2025)
doi:10.3934/amc.2026003

CONSTRUCTIONS OF BINARY QUANTUM CSS-T CODES FROM SOME SPECIAL FUNCTIONS

Bin Zheng✉ and Shixin Zhu✉*
School of Mathematics, Hefei University of Technology, Hefei 230601, China

(Communicated by Sihem Mesnager)

Abstract. Transversal T gates, which are seen as the most common non-Clifford gates, are an essential component of the universal set for fault tolerance. CSS-T codes are proposed to reduce the cost of implementing logical non-Clifford gates. So far, there have been limited studies on CSS-T codes. In this paper, we proposed new constructions of binary quantum CSS-T codes from four classes of special functions. Our constructions are based on a general construction of linear codes over the finite field $\mathbb{F}_2$, and we prove that such a pair of codes is actually a CSS-T pair under the given conditions. The resulting CSS-T codes are new compared with these codes in the literature.

1. **Introduction.** Quantum error-correcting codes play an important role in the realization of universal fault-tolerant quantum computation. Errors, which can be represented by the group of tensors of the Pauli matrices, cannot be avoided in quantum computers. Calderbank and Shor [7] and, independently, Steane [28], introduced a systematic method to construct quantum codes from binary classical error-correcting codes, which is known as the CSS construction. Afterward, CSS codes were extended to arbitrary finite fields [1, 19].

Universally, there are four quantum gates in quantum computation: the Hadamard gate H, the phase gate S, the controlled-NOT gate CX, and the transversal Toffoli gate T. The first three gates form a generating set of the Clifford group, while the transversal T gate is a non-Clifford gate. Generally speaking, the Clifford gates can be handled on a classical computer, but the implementation of a non-Clifford gate cannot. A transversal gate is a tensor product of single-qubit gates acting on the n physical qubits, and thus introduces no interaction between the physical qubits. Hence, transversal gates are the first choice for fault-tolerance, as they avert the spread of errors. In [26, 27], Rengaswamy et al. proposed an effective scheme, i.e., the CSS-T codes, to implement the operation on the transversal T gate. Indeed, CSS-T codes are a subfamily of CSS codes among non-degenerate stabilizer codes supporting the transversal T gate. The CSS codes are the optimal family.

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. A q-ary $[n, k]$ linear code is a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. Ding and Niederreiter [13]

2020 *Mathematics Subject Classification.* Primary: 94B05, 81P73; Secondary: 11T71.
Key words and phrases. Boolean functions, quantum error correcting codes, CSS-T codes, fault tolerance.
This paper is supported by the National Natural Science Foundation of China under Grant U21A20428 and Grant 12171134.
*Corresponding author: Shixin Zhu.

introduced a generic method to contruct linear codes with the given defining sets. Let $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_{q^m}^n$ and define

$$\mathcal{C}_D = \{\mathrm{Tr}_{q^m/q}(xd_1), \mathrm{Tr}_{q^m/q}(xd_2), \cdots, \mathrm{Tr}_{q^m/q}(xd_n) : x \in \mathbb{F}_{q^m}\}, \tag{1}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Then, the resulting code $\mathcal{C}_D$ is a linear code over $\mathbb{F}_q$ and the dimension of $\mathcal{C}_D$ is at most m. This construction is very significant, because every linear code over $\mathbb{F}_q$ can be expressed as $\mathcal{C}_D$ once the subset D of $\mathbb{F}_{q^m}$ is properly chosen [30]. It is known that this construction is equivalent to the generator matrix construction of linear codes. So far, many linear codes with good parameters have been constructed by employing this fundamental method (see [11, 14, 15, 13, 12, 16, 17, 29]). Let A_i denote the number of codewords with Hamming weight i in a linear code $\mathcal{C}$ of length n. The weight enumerator of the code $\mathcal{C}$ is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$

The sequence $(1, A_1, \cdots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. When the number of nonzero A_i is equal to t, then $\mathcal{C}$ is called a t-weight code. A linear code $\mathcal{C}$ is called nontrivial if $d(\mathcal{C}) \geq 2$ and $d(\mathcal{C}^\perp) \geq 2$, and trivial otherwise. In this paper, we consider only nontrivial linear codes, as trivial linear codes are not interesting for error correction.

1.1. **Recent related works.**

- In [26], the definition was given and an open question was raised: whether there exist families of CSS-T codes with non-vanishing rate and relative distance. Then, Berardini et al. [3] illustrated that the rate and relative distance cannot be simultaneously large.
- Andrade et al. [4] utilized Reed-Muller codes to construct binary CSS-T codes and studied their asymptotic properties. The authors also extended the initial definition to any finite field and constructed CSS-T codes from Hermitian curves.
- Camps-Moreno et al. [9] characterized binary CSS-T codes by using Schur square codes and used the characterization to show that CSS-T codes form a poset. The authors gave new conditions to guarantee that a pair of binary codes is a CSS-T pair. In [8], Camps-Moreno et al. constructed CSS-T code from sparse matrices. In [10], Camps-Moreno et al. studied binary triorthogonal codes and their relation to quantum CSS-T codes. This paper characterized the binary triorthogonal codes that are minimal or maximal with respect to the CSS-T poset.

1.2. **Our motivations and contributions.** Inspired by these works, it is natural to ask whether it is possible to yield CSS-T codes by utilizing new methodologies and obtain CSS-T codes with new parameters. For this aim, we will focus on the construction that was introduced by Ding and Niederreiter thereinbefore.

Up to now, there have been few studies on quantum CSS-T codes, and constructing binary CSS-T codes with new parameters is essential. In this paper, some special functions will be used to construct quantum CSS-T codes whose parameters are different from those of quantum CSS-T codes in the literature. An important condition on the constructions of CSS-T codes is that some punctured codes need be self-orthogonal. The weight distributions of the constructed linear codes are

completely determined by accurately calculating the exponential sum over the finite field. Then, we prove that the constructed linear codes are self-orthogonal. Therefore, we obtain some new CSS-T codes. The general construction of linear codes was introduced for the first time to construct CSS-T codes.

1.3. **Organization of this paper.** This paper is organized as follows: In Section 2, we recall some required concepts and results. In Section 3, we choose appropriate defining sets to contruct linear codes. Some special functions, including linear function $\mathrm{Tr}_2^{2^m}(x)$, two-to-one functions, bent functions, and almost-bent functions, are utilized to construct binary quantum CSS-T codes, whose parameters are new. In Section 4, we give a summary.

2. **Preliminaries.** For a positive integer n, we write $[n] := \{1, \ldots, n\}$. Let T be a subset of $[n]$. By deleting all the coordinates in T in each codeword of $\mathcal{C}$, the resulting code is called a punctured code of $\mathcal{C}$ denoted by $\mathcal{C}^T$. We have that the length of $\mathcal{C}^T$ is $n-|T|$. Let $\mathcal{C}(T)$ be the set of codewords whose coordinates in T are zero. By puncturing $\mathcal{C}(T)$ on T, such code with length $n-|T|$ is called a shortened code of $\mathcal{C}$ and is denoted by $\mathcal{C}_T$. The punctured and shortened codes of $\mathcal{C}$ and $\mathcal{C}^\perp$ have the following relationship:

Lemma 2.1. *Let $\mathcal{C}$ be a $[n,k,d]$ linear code over $\mathbb{F}_q$ and $d^\perp$ the minimum distance of $\mathcal{C}^\perp$. Let T be any set of t coordinate positions. Then, $(\mathcal{C}^\perp)_T = (\mathcal{C}^T)^\perp$ and $(\mathcal{C}^\perp)^T = (\mathcal{C}_T)^\perp$.*

A q-ary linear code $\mathcal{C}$ with length n is even if all of its codewords have even weight. For a codeword $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$, the support of c is the set of coordinates that are nonzero and is denoted by $supp(c)$. The set of coordinates that are zero is denoted by $Z(c) = [n] \setminus supp(c)$. The Euclidean inner product on $\mathbb{F}_q^n$ is defined by $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_E = \sum_{i=1}^{n} x_i y_i$, where $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. For a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$, the code

$$\mathcal{C}^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle_E = 0, \text{ for all } \boldsymbol{y} \in \mathcal{C}\}$$

is referred to as its Euclidean dual code. Especially, $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

We say that a code $\mathcal{C}$ is divisible if all codewords have weights divisible by an integer $\Delta > 1$. The following lemma establishes the relationship between divisible codes and self-orthogonal codes.

Lemma 2.2. [18] *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. When $q = 2$, if every codeword of $\mathcal{C}$ has weight divisible by four, then $\mathcal{C}$ is self-orthogonal.*

2.1. **CSS-T codes.** Let's start by recalling some concepts related to quantum code. A q-ary quantum code Q of length n and size K is a K-dimensional subspace of a q^n-dimensional Hilbert space $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. Assume that $a, b \in \mathbb{F}_q$ and define the unitary linear operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ as

$$X(a)|x\rangle = |x + a\rangle \text{ and } Z(b)|x\rangle = \omega^{\mathrm{Tr}(bx)}|x\rangle,$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a primitive p-th root of unity, and Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. For $\mathbf{a} = (a_1, a_2, \ldots, a_n), \mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$, denote $X(\mathbf{a}) = X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{b}) = Z(b_1) \otimes Z(b_2) \otimes \cdots \otimes Z(b_n)$ by the tensor products of n error operators. The set $E_n = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ is an error basis on $\mathbb{C}^{q^n}$.

Then the set $G_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_q\}$ is the error group associated with E_n. A quantum code Q has minimum distance d if it can detect all errors in G_n of weight less than d. Define $k = \log_q K$ and we denote the quantum code Q by $[[n, k, d]]_q$ or $((n, K, d))_q$. For every orthogonal pair $|\mathbf{u}\rangle$, $|\mathbf{v}\rangle$ in Q with $\langle \mathbf{u}|\mathbf{v}\rangle = 0$ and every $\mathbf{e} \in G_n$ with $W_Q(\mathbf{e}) \leq d-1$, $|\mathbf{u}\rangle$ and $\mathbf{e}|\mathbf{v}\rangle$ are orthogonal, i.e., $\langle \mathbf{u}|\mathbf{e}|\mathbf{v}\rangle = 0$. For any $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$ in Q and any $\mathbf{e} \in G_n$ with $W_Q(\mathbf{e}) \leq d-1$, the quantum code Q is called pure if $\langle \mathbf{u}|\mathbf{e}|\mathbf{v}\rangle = 0$. A quantum code Q with dimension $K = 1$ is pure.

From the classical codes, we can obtain a family of quantum codes by the following CSS code construction.

Lemma 2.3. [6] *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ denote two classical codes over $\mathbb{F}_q$ with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, such that $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Then there exists an $[[n, k_1 - k_2, d]]_q$ quantum code, where $d = \min\{wt(\mathbf{c}) \mid \mathbf{c} \in (\mathcal{C}_1 \backslash \mathcal{C}_2) \cup (\mathcal{C}_2^{\perp} \backslash \mathcal{C}_1^{\perp})\}$ that is pure to $\min\{d_1, d_2^{\perp}\}$.*

Let $d^* := \min\{wt(\mathcal{C}_1), wt(\mathcal{C}_2^{\perp})\}$. If $d = d^*$, the corresponding quantum code is said to be nondegenerate, and it is called degenerate if $d > d^*$. Purity and nondegeneracy are equivalent notions in the case of stabilizer codes.

The CSS-T codes are a family of quantum stabilizer codes, and the definition of binary CSS-T codes was given initially in [26].

Definition 2.4. A pair $(\mathcal{C}_1, \mathcal{C}_2)$ of binary linear codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $\mathcal{C}_2 \subseteq \mathcal{C}_1$ and the following properties hold:

1) $\mathcal{C}_2$ is an even code, i.e., $w_H(x) \equiv 0 \bmod 2$ for all $x \in \mathcal{C}_2$, where $w_H(x)$ is the Hamming weight of x.
2) For each $x \in \mathcal{C}_2$, there exists a dimension $w_H(x)/2$ self-dual code in $\mathcal{C}_1^{\perp}$ that is supported on x, i.e., there exists $\mathcal{C}_x \subseteq \mathcal{C}_1^{\perp}$ s.t. $|\mathcal{C}_x| = 2^{w_H(x)/2}$, $\mathcal{C}_x \subseteq \mathcal{C}_x^{\perp}$, and $z \in \mathcal{C}_x \Rightarrow z \preceq x$, i.e., $\mathrm{supp}(z) \subseteq \mathrm{supp}(x)$, where $\mathcal{C}_1^{\perp}$ is the code dual to $\mathcal{C}_1$ and $\mathrm{supp}(x)$ is the support of x.

Their original binary definition was generalized to an arbitrary finite field in [3], and this definition is more understandable.

Definition 2.5. A pair $(\mathcal{C}_1, \mathcal{C}_2)$ of q-ary linear codes satisfying the following statements is called a CSS-T pair:

1) $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$, i.e., $\mathcal{C}_2 \subseteq \mathcal{C}_1$.
2) $\mathcal{C}_2$ is an even code.
3) For any $x \in \mathcal{C}_2$, the shortened code $(\mathcal{C}_1^{\perp})_{Z(x)}$ contains a self-dual code.

Lemma 2.6. [3] *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension $k \geq n/2$. If q is even, then $\mathcal{C}$ contains a self-dual code if and only if n is even and $\mathcal{C}^{\perp}$ is self-orthogonal, i.e., $\mathcal{C}^{\perp} \subseteq \mathcal{C}$.*

From Lemma 2.6, we can see that $\mathcal{C}^{\perp}$ is required to be self-orthogonal while $\mathcal{C}$ contains a self-dual code. Combining with Lemma 2.1, the following conclusion is obtained.

Lemma 2.7. [3] *Let $\mathcal{C}_2 \subseteq \mathcal{C}_1$ be q-ary linear codes with length n and let $\mathcal{C}_2$ be even. If q is even, then $(\mathcal{C}_1, \mathcal{C}_2)$ is a CSS-T pair if and only if for any $x \in \mathcal{C}_2$ we have that $\mathcal{C}_1^{Z(x)}$ is self-orthogonal.*

When there exists a CSS-T pair $(\mathcal{C}_1, \mathcal{C}_2)$ with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, this leads to a CSS-T code with parameters $[[n, k_1 - k_2, \geq d(\mathcal{C}_2^{\perp})]]$.

2.2. **Characters and exponential sums.** Let $q = p^r$ be a prime power p and m be a positive integer. The trace function $\mathrm{Tr}_{q^m/q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is defined by:

$$\mathrm{Tr}_{q^m/q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$

If q is a prime, the trace function $\mathrm{Tr}_{q^m/q}$ is called the absolute trace function and is denoted by Tr_m.

Let ζ_p be the primitive p-th root of unity. For any $a \in \mathbb{F}_q$, an additive character of $\mathbb{F}_q$ is defined by:

$$\chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)}, x \in \mathbb{F}_q.$$

In particular, we call χ_0 the trivial additive character and χ_1 the canonical additive character of $\mathbb{F}_q$. It is well-known that the additive characters satisfy the following orthogonal relation:

$$\sum_{x\in\mathbb{F}_q} \chi_a(x) = \begin{cases} q, & \text{for } a = 0, \\ 0, & \text{for } a \in \mathbb{F}_q^*. \end{cases}$$

2.3. **Pless power moments.** For a q-ary linear code $\mathcal{C}$ with parameters $[n, k, d]$, we analogously denote by $(1, A_1^\perp, \cdots, A_n^\perp)$ the weight distribution of the dual code $\mathcal{C}^\perp$. The Pless power moments state the relationship between the weight distribution $(1, A_1, \cdots, A_n)$ of $\mathcal{C}$ and the weight distribution $(1, A_1^\perp, \cdots, A_n^\perp)$ of $\mathcal{C}^\perp$. The first four Pless power moments are given as follows [18]:

$$\begin{aligned}
&\sum_{j=0}^{n} A_j = q^k, \\
&\sum_{j=0}^{n} jA_j = q^{k-1}(qn - n - A_1^\perp), \\
&\sum_{j=0}^{n} j^2A_j = q^{k-2}[(q-1)n(qn-n+1) - (2qn - q - 2n + 2)A_1^\perp + 2A_2^\perp], \\
&\sum_{j=0}^{n} j^3A_j = q^{k-3}[(q-1)n(q^2n^2 - 2qn^2 + 3qn - q + n^2 - 3n + 2) \\
&\qquad - (3q^2n^2 - 3q^2n - 6qn^2 + 12qn + q^2 - 6q + 3n^2 - 9n + 6)A_1^\perp \\
&\qquad + 6(qn - q - n + 2)A_2^\perp - 6A_3^\perp].
\end{aligned}$$

If $A_1^\perp = A_2^\perp = A_3^\perp = 0$, the fifth Pless power moment is the following:

$$\begin{aligned}
\sum_{j=0}^{n} j^4A_j = q^{k-4}[&(q-1)n(q^3n^3 - 3q^2n^3 + 6q^2n^2 - 4q^2n + q^2 + 3qn^3 - 12qn^2 \\
&+ 15qn - 6q - n^3 + 6n^2 - 11n + 6) + 24A_4^\perp].
\end{aligned}$$

3. **Constructions of binary CSS-T codes from some special functions.** In this section, we always assume that $q = 2$ and m, m_1 are positive integers with $m_1|m$. Let the defining set $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_{2^m}^n$. Define

$$\begin{aligned}
\mathcal{C}_1 &= \{(\mathrm{Tr}_{2^m/2}(ad_1), \mathrm{Tr}_{2^m/2}(ad_2), \cdots, \mathrm{Tr}_{2^m/2}(ad_n)) : a \in \mathbb{F}_{2^m}\}, \\
\mathcal{C}_2 &= \{(\mathrm{Tr}_{2^m/2}(bd_1), \mathrm{Tr}_{2^m/2}(bd_2), \cdots, \mathrm{Tr}_{2^m/2}(bd_n)) : b \in \mathbb{F}_{2^{m_1}}\}.
\end{aligned} \tag{2}$$

It is easily seen that $\mathcal{C}_1$ and $\mathcal{C}_2$ are binary linear codes and $\mathcal{C}_2 \subseteq \mathcal{C}_1$.

One well-known method for constructing linear codes is based on special functions and cryptographic functions over finite fields, which play a crucial role in symmetric cryptography. Cryptographic functions and linear codes are closely related and have led to fascinating results. Based on this, in this paper, cryptographic functions, including linear functions, two-to-one functions, bent functions, and almost-bent functions, have been employed to construct linear codes.

Let f be a Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $f(0) = 0$ and let the defining set D be the support of f, i.e., $D = \{d \in \mathbb{F}_{2^m} : f(d) = 1\}$. Note that for a Boolean function f with $f(0) = 1$, this causes the definition set D to include 0, and we have that the minimal distance of the dual code equals to 1.

For any $w \in \mathbb{F}_{2^m}$, the Walsh transform of f is defined by

$$\hat{f}(w) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+\mathrm{Tr}_{2^m/2}(wx)}.$$

It follows from the orthogonal relation of additive characters that the lengths of $\mathcal{C}_1$ and $\mathcal{C}_2$ are $n = |D| = 2^{-1} \sum_{s \in \mathbb{F}_2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{sf(d)-s} = 2^{m-1} - \frac{1}{2}\hat{f}(0)$.

For any $\mathbf{c}_2 \in \mathcal{C}_2$, by the orthogonal relation of additive characters, the codewords $\mathbf{c}_1^{(\mathbf{c}_2)}$ of the punctured code $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ have weight

$$\begin{aligned}
\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) &= \#\{d \in D : \mathrm{Tr}_{2^m/2}(bd) = 1, \mathrm{Tr}_{2^m/2}(ad) = 1\} \\
&= \frac{1}{4} \sum_{i=1}^{n} \Big(\sum_{u \in \mathbb{F}_2} (-1)^{u\mathrm{Tr}_{2^m/2}(ad_i)-u} \Big) \Big(\sum_{v \in \mathbb{F}_2} (-1)^{v\mathrm{Tr}_{2^m/2}(bd_i)-v} \Big) \\
&= \frac{1}{4} \sum_{i=1}^{n} \Big(1 - (-1)^{\mathrm{Tr}_{2^m/2}(ad_i)} \Big) \Big(1 - (-1)^{\mathrm{Tr}_{2^m/2}(bd_i)} \Big) \\
&= \frac{1}{4} \sum_{i=1}^{n} \Big(1 - (-1)^{\mathrm{Tr}_{2^m/2}(ad_i)} - (-1)^{\mathrm{Tr}_{2^m/2}(bd_i)} + (-1)^{\mathrm{Tr}_{2^m/2}((a+b)d_i)} \Big) \\
&= \frac{n}{4} - \frac{1}{4} \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}(ad_i)} - \frac{1}{4} \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}(bd_i)} \\
&\quad + \frac{1}{4} \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}((a+b)d_i)}.
\end{aligned}$$

Define an exponential sum by $S_D(x) = \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_2^{2^m}(xd_i)}$, then we have

$$\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) = \frac{n}{4} - \frac{1}{4} S_D(a) - \frac{1}{4} S_D(b) + \frac{1}{4} S_D(a+b), \tag{3}$$

where $a \in \mathbb{F}_{2^m}, b \in \mathbb{F}_{2^{m_1}}$.

When $D = \{d \in \mathbb{F}_{2^m} : f(d) = 1\}$, then

$$\begin{aligned}
S_D(x) &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}(xd_i)} \\
&= \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(xd)} \sum_{s \in \mathbb{F}_2} (-1)^{sf(d)-s} \\
&= \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(xd)} - \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{f(d)+\mathrm{Tr}_{2^m/2}(xd)}
\end{aligned}$$

$$= \begin{cases} 2^{m-1} - \frac{1}{2}\hat{f}(0), & \text{for } x = 0, \\ -\frac{1}{2}\hat{f}(x), & \text{for } x \neq 0. \end{cases}$$

It follows that

$$\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) = \begin{cases} \frac{n}{2} + \frac{1}{8}\hat{f}(a) + \frac{1}{8}\hat{f}(b), & \text{if} \quad a = b \neq 0, \\ \frac{n}{4} + \frac{1}{8}\hat{f}(a) + \frac{1}{8}\hat{f}(b) - \frac{1}{8}\hat{f}(a+b), & \text{if} \quad a \neq 0,\ b \neq 0,\ a+b \neq 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

3.1. **Binary CSS-T codes from linear functions.** In this subsection, let $f(x) = \mathrm{Tr}_{2^m/2}(x)$ and $D = \{d \in \mathbb{F}_{2^m} : \mathrm{Tr}_{2^m/2}(d) = 1\}$, then

$$S_D(x) = \frac{1}{2}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(dx)} - \frac{1}{2}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}((x+1)d)}.$$

Thus it follows that

$$S_D(x) = \begin{cases} 2^{m-1}, & \text{for } x = 0, \\ -2^{m-1}, & \text{for } x = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Lemma 3.1. *Let $m \geq 5$ be a positive integer and $f(x) = \mathrm{Tr}_{2^m/2}(x)$. Then the code $\mathcal{C}_1$ in Eq. (2) is a two-weight binary code with parameters $[2^{m-1}, m, 2^{m-2}]$, and its weight enumerator is $1 + z^{2^{m-1}} + (2^m - 2)z^{2^{m-2}}$.*

Proof. The codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in Eq. (2) have length

$$n = \frac{1}{2}\sum_{d\in\mathbb{F}_{2^m}}\sum_{u\in\mathbb{F}_2} (-1)^{u(\mathrm{Tr}_{2^m/2}(d)-1)} = 2^{m-1} - \frac{1}{2}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(d)} = 2^{m-1}.$$

For any codeword $\mathbf{c}_1 = (\mathrm{Tr}_{2^m/2}(ad_1), \mathrm{Tr}_{2^m/2}(ad_2), \cdots, \mathrm{Tr}_{2^m/2}(ad_n))$ with $a \in \mathbb{F}_{2^m}$, by the orthogonal relation of additive characters, its Hamming weight is

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_1) =& \#\{d \in D : \mathrm{Tr}_{2^m/2}(ad) = 1\} \\ =& \#\{d \in \mathbb{F}_{2^m} : \mathrm{Tr}_{2^m/2}(ad) = 1, \mathrm{Tr}_{2^m/2}(d) = 1\} \\ =& \frac{1}{4}\sum_{d\in\mathbb{F}_{2^m}}\sum_{u\in\mathbb{F}_2} (-1)^{u(\mathrm{Tr}_{2^m/2}(ad)-1)} \sum_{v\in\mathbb{F}_2} (-1)^{v(\mathrm{Tr}_{2^m/2}(d)-1)} \\ =& \frac{1}{4}\sum_{d\in\mathbb{F}_{2^m}} (1 - (-1)^{\mathrm{Tr}_{2^m/2}(ad)})(1 - (-1)^{\mathrm{Tr}_{2^m/2}(d)}) \\ =& 2^{m-2} - \frac{1}{4}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(ad)} - \frac{1}{4}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(d)} \\ & + \frac{1}{4}\sum_{d\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}((a+1)d)} \\ =& \begin{cases} 0, & \text{for } a = 0, \\ 2^{m-1}, & \text{for } a = 1, \\ 2^{m-2}, & \text{for } a \neq 0 \text{ and } a \neq 1. \end{cases} \end{aligned}$$

Then the desired results are obtained. □

Theorem 3.2. *Let $m \geq 4$ be a positive integer with $m_1 | m$ and $f(x) = \mathrm{Tr}_{2^m/2}(x)$. Then there exists a nondegenerate CSS-T code with parameters $[[2^{m-1}, m - m_1, d \geq 2]]$.*

Proof. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be defined as Eq. (2). Clearly, we have that $\mathcal{C}_2 \subseteq \mathcal{C}_1$ and $\mathcal{C}_2$ is an even code. If $d(\mathcal{C}_2^{\perp}) = 1$, it means that there exists $d_i \in D$ such that $\mathrm{Tr}_{2^m/2}(bd_i) = 0$ for any $b \in \mathbb{F}_{2^{m_1}}$. Since $\mathrm{Tr}_{2^m/2}(bd_i) = \mathrm{Tr}_{2^{m_1}/2}(b\mathrm{Tr}_{2^m/2^{m_1}}(d_i)) = 0$ for any $b \in \mathbb{F}_{2^{m_1}}$, it follows that $\mathrm{Tr}_{2^m/2}(d_i) = \mathrm{Tr}_{2^{m_1}/2}(\mathrm{Tr}_{2^m/2^{m_1}}(d_i)) = 0$, i.e., $\mathrm{Tr}_{2^m/2}(d_i) = 0$. This leads to a contradiction. Thus the code $\mathcal{C}_2$ has parameters $[2^{m-1}, m_1]$ with $d(\mathcal{C}_2^{\perp}) \geq 2$. It is easy to see that there exists $\mathbf{c} \in \mathcal{C}_2^{\perp} \backslash \mathcal{C}_1^{\perp}$ such that $d(\mathcal{C}_2^{\perp}) = \mathrm{wt}(\mathbf{c})$.

For any $\mathbf{c}_2 \in \mathcal{C}_2$, the codewords $\mathbf{c}_1^{(\mathbf{c}_2)}$ of the punctured code $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ have weight

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) &= \frac{n}{4} - \frac{1}{4}S_D(a) - \frac{1}{4}S_D(b) + \frac{1}{4}S_D(a+b) \\ &= \begin{cases} 0, & \text{for } a = 0 \text{ or } b = 0, \\ 2^{m-1}, & \text{for } a = b = 1, \\ 2^{m-2}, & \text{otherwise.} \end{cases}\end{aligned}$$

When $m \geq 4$, we have $4|\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$. It follows from Lemma 2.2 that $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ is self-orthogonal. This completes the proof. □

Corollary 3.3. *Let $m \geq 4$ be a positive integer and $f(x) = \mathrm{Tr}_2^{2^m}(x)$. Then we have the following:*

1) *If $m_1 = 1$, then there exists a binary CSS-T code with parameters $[[2^{m-1}, m-1, \geq 2]]$.*
2) *If $m_1 = m$, then there exists a binary CSS-T code with parameters $[[2^{m-1}, 0, \geq 4]]$.*

Proof. For 1), when $m_1 = 1$, we prove that $d(\mathcal{C}_2^{\perp}) = 2$. Actually, in this case, the code $\mathcal{C}_2$ has two codewords, i.e., $\mathcal{C}_2 = \{(0, 0, \cdots, 0), (1, 1, \cdots, 1)\}$. Clearly, we have $d(\mathcal{C}_2^{\perp}) = 2$. From Theorem 3.2, the desired conclusion then follows.

For 2), when $m_1 = m$, we have $\mathcal{C}_1 = \mathcal{C}_2$. Next, we prove that $d(\mathcal{C}_1^{\perp}) = d(\mathcal{C}_2^{\perp}) = 4$. Define $w_1 = 2^{m-1}, w_2 = 2^{m-2}$, then $A_{w_1} = 1, A_{w_2} = 2^m - 2$. From the weight distribution of $\mathcal{C}_1$ and the Pless power moments, we give the following system of equations:

$$\begin{cases} w_1 A_{w_1} + w_2 A_{w_2} &= 2^{m-1}(n - A_1^{\perp}), \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} &= 2^{m-2}[n(n+1) - 2nA_1^{\perp} + 2A_2^{\perp}], \\ w_1^3 A_{w_1} + w_2^3 A_{w_2} &= 2^{m-3}[n^3 + 3n^2 - (3n^2 + 3n - 2)A_1^{\perp} + 6nA_2^{\perp} - 6A_3^{\perp}] \\ w_1^4 A_{w_1} + w_2^4 A_{w_2} &= 2^{m-4}[n^4 + 6n^3 + 3n^2 - 2n - 4n(n^2 + 3n - 2)A_1^{\perp} \\ & \quad +4(3n^2 + 3n - 4)A_2^{\perp} - 24nA_3^{\perp} + 24A_4^{\perp}]. \end{cases}$$

By solving the above system of equations, we have $A_1^{\perp} = A_2^{\perp} = A_3^{\perp} = 0, A_4^{\perp} = \frac{2^{3m-6} - 3 \cdot 2^{2m-5} + 2^{m-3}}{3} > 0$, which means that $d(\mathcal{C}_2^{\perp}) = 4$. From Theorem 3.2, the desired conclusion then follows. □

Example 1. We give some examples of Corollary 3.3 in the following:

- If $m = 4$ and $m_1 = 1$, then there exists a binary CSS-T code with parameters $[[8, 3, \geq 2]]$.
- If $m = m_1 = 4$, then there exists a binary CSS-T code with parameters $[[8, 0, \geq 4]]$.
- If $m = 5, m_1 = 1$, then there exists a binary CSS-T code with parameters $[[16, 4, \geq 2]]$.

- If $m = m_1 = 5$, then there exists a binary CSS-T code with parameters $[[16, 0, \geq 4]]$.

Remark 3.4. A 0-dimensional quantum code with length n has parameters $[[n, 0, d]]$. Such a quantum code represents a single quantum state capable of correcting any $(d-1)/2$ errors. In practice, 0-dimensional quantum codes can be useful, for example, in testing whether certain storage locations for qubits are decohering faster than they should.

3.2. **Binary CSS-T codes from two-to-one functions.** Let f be a mapping from $\mathbb{F}_{2^r}$ to itself, where r is a positive integer. For any $a \in \mathbb{F}_{2^r}$, the mapping f is said to be a two-to-one mapping if the number of the solutions of the equation $f(x) = a$ is equal to 0 or 2. Some known two-to-one functions over $\mathbb{F}_{2^r}$ are listed in Table 1.

TABLE 1. Some known two-to-one functions over $\mathbb{F}_{2^r}$

Functions	Conditions	Ref.
$f(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x$	m odd, $r = 2m$, $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$, $\alpha \in \mathbb{F}_{2^r}$, $\alpha^{2^m-1} = w$	[22]
$f(x) = x^{2^r-2^m} + x^{2^r-2^m-1} + \alpha x$	$m \in \mathbb{N}$, $r = 2m$, $\alpha \in \mathbb{F}_{2^r}$, $\alpha^{2^m} + \alpha + 1 = 0$	[23]
$f(x) = (x^2 + x + \delta)^{2^m+1} + x$	m even, $r = 2m$, $\delta \in \mathbb{F}_{2^r}$, $\mathrm{Tr}_{2^r/2}(\delta) = 1$	[31]
$f(x) = (x^2 + x + \delta)^{2^{2m-2}+2^{m-2}} + x$	m even, $r = 2m$, $\delta \in \mathbb{F}_{2^r}$, $\mathrm{Tr}_{2^r/2}(\delta) = 1$	[31]
$f(x) = (x^2 + x + \delta)^{2^{2m-1}+2^{m-1}} + x$	m even, $r = 2m$, $\delta \in \mathbb{F}_{2^r}$, $\mathrm{Tr}_{2^r/2}(\delta) = 1$	[31]
$f(x) = (x^{2^m} + x + \delta)^{2^i+1} + cx$	$m, i \in \mathbb{N}$, $r = 2m$, $\gcd(m, i) = 1$, $\delta \in \mathbb{F}_{2^r}$, $c \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_{2^r/2^m}(\delta^2 + c^{2^{m-i}}\delta) \neq 0$	[31]
$f(x) = (x^{2^m} + x + \delta)^{2^m+2^i+1} + cx$	$m, i \in \mathbb{N}$, $r = 2m$, $\gcd(m, i) = 1$, $\delta \in \mathbb{F}_{2^r}$, $c \in \mathbb{F}_{2^m}$, $\mathrm{Tr}_{2^r/2^m}(\delta)^{2^i+2} + \mathrm{Tr}_{2^r/2^m}(\delta) \neq 0$	[31]
$f(x) = (x^{2^m}+x+\delta)^{2^{2m-2}+2^m-2^{m-2}}+wx$	$m \in \mathbb{N}$, $r = 2m$, $\delta \in \mathbb{F}_{2^r} \backslash \mathbb{F}_{2^m}$, $c \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_{2^r/2}(\frac{1}{c} + 1) \neq 0$	[31]
$f(x) = x^{\frac{2^{r-1}+2^m-1}{3}} + x^{2^m} + wx$	m odd, $r = 2m$, $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$	[23]
$f(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^{m+1}+2} + x^{2^{m+1}+1} + x^2 + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^{m+2}+4} + x^{2^{m+1}+2} + x^2 + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^r-2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^r-2} + x^{2^r-2^{m+1}} + x^{2^{m+1}-1} + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^r-2}+x^{2^r-2^{m+1}}+x^{2^r-2^{m+1}-2}+x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^r-2} + x^{2^{r-1}+1} + x^{2^{r-1}-2} + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^r-2} + x^{2^r-4} + x^3 + x$	$m \in \mathbb{N}$, $r = 2m + 1$	[23]
$f(x) = x^{2^{2m}+1} + x^{2^{m+1}} + x^{2^m+1} + x$	$m \in \mathbb{N}$, $m \not\equiv 1 \pmod 3$, $r = 3m$	[23]
$f(x) = x^{2^{2m}+2^m} + x^{2^{2m}+1} + x^{2^m+1} + x$	m odd, $r = 3m$	[23]
$f(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$	m odd, $r = 3m$	[21]
$f(x) = \mathrm{Tr}_{2^r/2^m}(x^{2^m+1}) + x$	$m \in \mathbb{N}$, k odd, $r = km$	[21]

Let f be a two-to-one function over $\mathbb{F}_{2^r}$. Let the defining set $D := \{f(d), d \in \mathbb{F}_{2^r}\} \setminus \{0\} = \{d_1, d_2, \cdots, d_n\}$. Then the length of $\mathcal{C}_D$ is $n = |D| = 2^{r-1} - 1$.

For a function g defined from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$, the Walsh transform of g at $(u,v) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$ is defined by

$$\widehat{W}_g(u,v) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(ug(x)+vx)}.$$

Note that $S_D(x) = \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}(xd_i)} = \frac{1}{2} \sum_{d \in \mathbb{F}_{2^r}} (-1)^{\mathrm{Tr}_{2^m/2}(xf(d))} - 1 = \frac{1}{2}\widehat{W}_f(x,0) - 1$, then

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) &= \frac{n}{4} - \frac{1}{4}S_D(a) - \frac{1}{4}S_D(b) + \frac{1}{4}S_D(a+b) \\ &= 2^{r-3} - \frac{1}{8}\widehat{W}_f(a,0) - \frac{1}{8}\widehat{W}_f(b,0) + \frac{1}{8}\widehat{W}_f(a+b,0). \end{aligned} \tag{6}$$

Theorem 3.5. *Let $r = 2m$, $m_1 | r$ and $f(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x \in \mathbb{F}_{2^r}[x]$, where $m \geq 5$ is odd, and $\alpha \in \mathbb{F}_{2^r}$ such that $\alpha^{2^m-1} = w$ with $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$. Then there exists a CSS-T code with parameters $[[2^{r-1}-1, r-m_1, d \geq d(\mathcal{C}_2^{\perp})]]$.*

Proof. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be defined as Eq. (2). By the proof of Theorem 2 in [25], we have that $\mathcal{C}_1$ is a binary linear code with parameters $[2^{r-1}-1, r, 2^{r-2}-2^{m-1}]$, and its weight distribution is given in Table 2. By the definitions of $\mathcal{C}_1$ and $\mathcal{C}_2$, it is easy to see that $\mathcal{C}_2 \subseteq \mathcal{C}_1$ and $\mathcal{C}_2$ is an even code. The code $\mathcal{C}_2$ has parameters $[2^{r-1}-1, m_1]$.

TABLE 2. The weight distribution of the codes

Weight w	Multiplicity A_w
0	1
$2^{r-2} - 2^{m-1}$	$2^{r-3} + 2^{m-2}$
2^{r-2}	$3 \cdot 2^{r-2} - 1$
$2^{r-2} + 2^{m-1}$	$2^{r-3} - 2^{m-2}$

By the proof of Theorem 2 in [25], $\widehat{W}_f(x,0) = 2^r$ if and only if $x = 0$; if $x \in \mathbb{F}_{2^m} \backslash \{0\}$, then $\widehat{W}_f(x,0) = 0$; for any $x \in \mathbb{F}_{2^r} \backslash \mathbb{F}_{2^m}$, we have $\widehat{W}_f(x,0) \in \{0, \pm 2^{m+1}\}$. When $m \geq 5$, we have $4 | \mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$ by Eq. (6). It follows from Lemma 2.2 that $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ is self-orthogonal. Then the desired conclusion is obtained. □

Corollary 3.6. *Let $r = 2m$, $m_1 | r$ and $f(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x \in \mathbb{F}_{2^r}[x]$, where $m \geq 5$ is odd, and $\alpha \in \mathbb{F}_{2^r}$ such that $\alpha^{2^m-1} = w$ with $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$. If $m_1 = m$, then there exists a binary CSS-T code with parameters $[[2^{r-1}-1, 0, \geq 3]]$.*

Proof. When $m_1 = m$, we have $\mathcal{C}_1 = \mathcal{C}_2$. Next, we prove that $d(\mathcal{C}_1^{\perp}) = d(\mathcal{C}_2^{\perp}) = 3$. Clearly, we have $d(\mathcal{C}_2^{\perp}) \neq 1$. If $d(\mathcal{C}_2^{\perp}) = 2$, there exist two distinct elements $d_i, d_j \in \mathbb{F}_{2^m}^*$ such that $\mathrm{Tr}_{2^m/2}(ad_i) + \mathrm{Tr}_{2^m/2}(ad_j) = 0$ for any $a \in \mathbb{F}_{2^m}$. Then $\mathrm{Tr}_{2^m/2}(a(d_i + d_j)) = 0$ for any $a \in \mathbb{F}_{2^m}$ and it follows that $d_i + d_j = 0$, which leads to a contradiction. From Theorem 3.5, the desired conclusion then follows. □

3.3. **Binary CSS-T codes from bent functions.** A function f from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is called bent if $\hat{f}(w) = \pm 2^{m/2}$ for any $w \in \mathbb{F}_{2^m}$ and bent functions exist only for even m. Let f be bent and the defining set $D = \{d \in \mathbb{F}_{2^m} : f(d) = 1\}$, then the length is $2^{m-1} \pm 2^{(m-2)/2}$.

Lemma 3.7. [11] *Let f be a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $f(0) = 0$, where $m \geq 4$ and is even. Then the code $\mathcal{C}_1$ in Eq. (2) is a $[n, m, (n - 2^{(m-2)/2})/2]$ two-weight binary code with the weight distribution in Table 3, where $n = 2^{m-1} \pm 2^{(m-2)/2}$.*

TABLE 3. The weight distribution of the codes in Lemma 3.7

Weight w	Multiplicity A_w
0	1
$\frac{n}{2} - 2^{\frac{m-4}{2}}$	$\frac{2^m - 1 - n2^{-\frac{m-2}{2}}}{2}$
$\frac{n}{2} + 2^{\frac{m-4}{2}}$	$\frac{2^m - 1 + n2^{-\frac{m-2}{2}}}{2}$

Theorem 3.8. *Let $m \geq 10$ be even and m_1 be an even divisor of m. Suppose that f is a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $f(0) = 0$. Then there exists a CSS-T code with parameters $[[n, m - m_1, d \geq d(\mathcal{C}_2^{\perp})]]$, where $n = 2^{m-1} \pm 2^{(m-2)/2}$.*

Proof. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be defined as Eq. (2). It is obvious that $\mathcal{C}_2 \subseteq \mathcal{C}_1$ and $\mathcal{C}_1$ is an even code. Since $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$, it follows that $\mathcal{C}_2$ is also an even code, and $\mathcal{C}_2$ has length n and dimension m_1.

For any $\mathbf{c}_2 \in \mathcal{C}_2$, the codewords $\mathbf{c}_1^{(\mathbf{c}_2)}$ of the punctured code $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ have weight $\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$ in Eq. (4). When f is a bent function and $m \geq 10$, we have $4|\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$. It follows from Lemma 2.2 that $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ is self-orthogonal. Similar to Theorem 3.2, the lower bound of the minimum distance can be proved. The desired conclusion is obtained. □

Corollary 3.9. *Let $m \geq 10$ be even and f is a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $f(0) = 0$. If $m_1 = m$, then there exists a binary CSS-T code with parameters $[[n, 0, \geq 3]]$, where $n = 2^{m-1} \pm 2^{(m-2)/2}$.*

Proof. When $m_1 = m$, we have $\mathcal{C}_1 = \mathcal{C}_2$. Next, we prove that $d(\mathcal{C}_2^{\perp}) \geq 3$. Clearly, we have $d(\mathcal{C}_2^{\perp}) \neq 1$. If $d(\mathcal{C}_2^{\perp}) = 2$, there are two distinct elements $d_i, d_j \in \mathbb{F}_{2^m}^*$ such that $\mathrm{Tr}_{2^m/2}(ad_i) + \mathrm{Tr}_{2^m/2}(ad_j) = 0$ for any $a \in \mathbb{F}_{2^m}$. Then $\mathrm{Tr}_{2^m/2}(a(d_i + d_j)) = 0$ for any $a \in \mathbb{F}_{2^m}$ and it follows that $d_i + d_j = 0$, which leads to a contradiction. The desired conclusion then follows from Theorem 3.8. □

3.4. **Binary CSS-T codes from almost-bent functions.** A function g from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is called almost-bent if $\widehat{W}(u, v) \in \{0, \pm 2^{(m+1)/2}\}$ for every pair $(u, v) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$, and almost-bent functions exist only for odd m. Let g be an almost-bent function, and define $f = \mathrm{Tr}_{2^m/2}(g)$. As before, let the defining set be $D = \{d \in \mathbb{F}_{2^m} : f(d) = 1\} = \{d \in \mathbb{F}_{2^m} : \mathrm{Tr}_{2^m/2}(g(d)) = 1\}$. Then

$$\begin{aligned} n &= \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} \sum_{u \in \mathbb{F}_2} (-1)^{u\mathrm{Tr}_{2^m/2}(g(d)) - u} \\ &= 2^{m-1} - \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(g(d))} \end{aligned}$$

$$= 2^{m-1} - \frac{1}{2}\widehat{W}_g(1,0).$$

Thus it follows that

$$n = \begin{cases} 2^{m-1} - 2^{(m-1)/2}, & \text{if } \widehat{W}_g(1,0) = 2^{(m+1)/2}, \\ 2^{m-1} + 2^{(m-1)/2}, & \text{if } \widehat{W}_g(1,0) = -2^{(m+1)/2}, \\ 2^{m-1}, & \text{if } \widehat{W}_g(1,0) = 0. \end{cases} \tag{7}$$

Note that

$$\begin{aligned} S_D(x) &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}_{2^m/2}(xd_i)} \\ &= \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(xd)} \sum_{s \in \mathbb{F}_2} (-1)^{s\mathrm{Tr}_{2^m/2}(g(d))-s} \\ &= \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(xd)} - \frac{1}{2} \sum_{d \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(g(d)+xd)} \\ &= \begin{cases} 2^{m-1} - \frac{1}{2}\widehat{W}_g(1,0), & \text{for } x = 0, \\ -\frac{1}{2}\widehat{W}_g(1,x), & \text{for } x \neq 0. \end{cases} \end{aligned}$$

It follows from Eq. (3) that

$$\begin{aligned} &\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)}) \\ &= \begin{cases} \frac{n}{2} + \frac{1}{8}\widehat{W}_g(1,a) + \frac{1}{8}\widehat{W}_g(1,b), & \text{if } a = b \neq 0, \\ \frac{n}{4} + \frac{1}{8}\widehat{W}_g(1,a) + \frac{1}{8}\widehat{W}_g(1,b) - \frac{1}{8}\widehat{W}_g(1,a+b), & \text{if } a \neq 0,\ b \neq 0,\ a+b \neq 0, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{8}$$

Lemma 3.10. [11] *Let f be an almost-bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$, where m is odd. Then the code $\mathcal{C}_1$ in Eq. (2) is a $[n, m, (n - 2^{(m-1)/2})/2]$ three-weight binary code with the weight distribution in Table 3, where n is given in Eq. (7).*

TABLE 4. The weight distribution of the codes in Lemma 3.10

Weight w	Multiplicity A_w
0	1
$\frac{n-2^{\frac{m-1}{2}}}{2}$	$n(2^m - n)2^{-m} - n2^{-(m+1)/2}$
$\frac{n}{2}$	$2^m - 1 - n(2^m - n)2^{-(m-1)}$
$\frac{n+2^{\frac{m-1}{2}}}{2}$	$n(2^m - n)2^{-m} + n2^{-(m+1)/2}$

Theorem 3.11. *Let $m \geq 9$ be odd and m_1 be a positive divisor of m. Suppose that f is an almost-bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ with $\mathrm{Tr}_{2^m/2}(g(0)) = 0$. Then there exists a CSS-T code with parameters $[[n, m - m_1, d \geq d(\mathcal{C}_2^{\perp})]]$, where n is given in Eq. (7).*

Proof. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be defined as Eq. (2). It is obvious that $\mathcal{C}_1$ is an even code and $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Since $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$, it follows that $\mathcal{C}_2$ is also an even code, and $\mathcal{C}_2$ has length n and dimension m_1.

For any $\mathbf{c}_2 \in \mathcal{C}_2$, the codewords $\mathbf{c}_1^{(\mathbf{c}_2)}$ of the punctured code $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ have weight $\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$ in Eq. (8). When f is an almost-bent function and $m \geq 9$, we have $4|\mathrm{wt}(\mathbf{c}_1^{(\mathbf{c}_2)})$. Similar to Theorem 3.2, the lower bound of the minimum distance can be proved. It follows from Lemma 2.2 that $\mathcal{C}_1^{Z(\mathbf{c}_2)}$ is self-orthogonal. The desired conclusion is obtained. □

Corollary 3.12. *Let $m \geq 9$ be odd and f is an almost-bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ with $\mathrm{Tr}_2^{2^m}(g(0)) = 0$. If $m_1 = m$, then there exists a binary CSS-T code with parameters $[[n, 0, \geq 3]]$, where n is given in Eq. (7).*

Proof. When $m_1 = m$, we have $\mathcal{C}_1 = \mathcal{C}_2$. Next, we prove that $d(\mathcal{C}_2^{\perp}) \geq 3$. Clearly, we have $d(\mathcal{C}_2^{\perp}) \neq 1$. If $d(\mathcal{C}_2^{\perp}) = 2$, there exist two distinct elements $d_i, d_j \in \mathbb{F}_{2^m}^*$ such that $\mathrm{Tr}_{2^m/2}(ad_i) + \mathrm{Tr}_{2^m/2}(ad_j) = 0$ for any $a \in \mathbb{F}_{2^m}$. Then $\mathrm{Tr}_{2^m/2}(a(d_i + d_j)) = 0$ for any $a \in \mathbb{F}_{2^m}$ and it follows that $d_i + d_j = 0$, which leads to a contradiction. From Theorem 3.11, the desired conclusion then follows. □

Remark 3.13. (Comparisons of CSS-T codes) In [9], the authors used cyclotomic cosets to characterize CSS-T pairs from cyclic codes and extended cyclic codes. In this paper, many specific examples were given, and the lengths of the codes are 2^m or $2^m - 1$ with $5 \leq m \leq 10$. Our examples in Example 1 show that we get some codes with smaller lengths than the results in [9]. Besides, the codes in Theorem 3.8 have lengths $n = 2^{m-1} \pm 2^{(m-2)/2}$ with m even, and the codes in Theorem 3.11 have lengths $n = 2^{m-1} \pm 2^{(m-1)/2}$ or $n = 2^{m-1}$ with m odd. Compared with the results in [9], the resulting CSS-T codes derived from our novel construction are different from theirs.

4. Conclusion.

In this paper, we employ four classes of functions, namely the linear function $\mathrm{Tr}_{2^m/2}(x)$, two-to-one functions, bent functions, and almost-bent functions, to construct binary quantum CSS-T codes. We prove that the weight distributions of some punctured codes over $\mathbb{F}_2$ are divided by four, and the punctured codes are self-orthogonal. Naturally, a CSS-T pair is derived from the defining-set construction. It is worth noting that the resulting codes are new in the sense that its parameters are different from all known ones. As future work, it would be an interesting and challenging problem to obtain more CSS-T codes over an arbitrary finite field.

Universal quantum computation requires the implementation of a logical non-Clifford gate. We note that this specific code family, i.e., CSS-T codes, arises when the T gate is applied transversally. Error correcting code will only be able to transversally implement a finite set of gates, and a gate outside this set is required to achieve universality [2]. The one non-transversal T gate contributes to the fault-tolerant threshold. The CSS-T codes can avoid the commonly used but costly distillation techniques [5, 20].

Acknowledgments. The authors sincerely thank the editors and the referees for their valuable comments and helpful suggestions, which helped to improve the presentation of the manuscript.

REFERENCES

[1] A. Ashikhmin and E. Knill, Nonbinary quantum stablizer codes, *IEEE Trans. Inf. Theory*, **47** (2001), 3065-3072.

[2] A. Barenco, C. H. Bennett, R. Cleve, et al., Elementary gates for quantum computation, *Phys. Rev. A*, **52** (1995), 3457–3467.
[3] E. Berardini, A. Caminata and A. Ravagnani, Structure of CSS and CSS-T quantum codes, *Des. Codes Cryptogr.*, **92** (2024), 2801-2823.
[4] J. Bolkema, E. Andrade, T. Dexter, H. Eggers, V. L. Fisher, L. Szramowski and F. Manganiello, CSS-T codes from Reed-Muller codes, *IEEE J. Select. Areas Inf. Theory*, **6** (2025), 199-204.
[5] S. Bravyi1 and J. Haah, Magic-state distillation with low overhead, *Phys. Rev. A*, **86** (2012), 052329.
[6] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory*, **44** (1998), 1369-1387.
[7] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A*, **54** (1996), 1098-1105.
[8] E. Camps-Moreno, H. H. López, G. L. Matthews and E. McMillon, Toward Quantum CSS-T codes from sparse matrices, *Proceedings of the 2024 IEEE International Symposium on Information Theory Workshops (ISIT-W)*, Athens, Greece, 2024, 1-6.
[9] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José and I. Soprunov, An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance, *Quantum Inf. Process.*, **23** (2024), Paper No. 230, 24 pp.
[10] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José and I. Soprunov, Binary triorthogonal and CSS-T Codes for quantum error correction, *Proceedings of the 2024 60th Annual Allerton Conference on Communication, Control, and Computing*, Urbana, IL, USA, 2024, 1-6.
[11] C. Ding, Linear codes from some 2-designs, *IEEE Trans. Inf. Theory*, **60** (2015), 3265-3275.
[12] C. Ding, C. Li, N. Li and Z. Zhou, Three-weight cyclic codes and their weight distributions, *Discrete Math.*, **339** (2016), 415-427.
[13] C. Ding and H. Niederreiter, Cyclotomic linear codes of order 3, *IEEE Trans. Inf. Theory*, **53** (2007), 2274-2277.
[14] K. Ding and C. Ding, Binary linear codes with three weights, *IEEE Commun. Lett.*, **18** (2014), 1879-1882.
[15] K. Ding and C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Trans. Inf. Theory*, **61** (2015), 5835-5842.
[16] Z. Heng, D. Li, J. Du and F. Chen, A family of projective two-weight linear codes, *Des. Codes Cryptogr.*, **89** (2021), 1993-2007.
[17] Z. Heng, W. Wang and Y. Wang, Projective binary linear codes from special Boolean functions, *Appl. Algebr. Eng. Comm. Comput.*, **32** (2021), 521-552.
[18] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
[19] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, Nonbinary stablizer codes over finite fields, *IEEE. Trans. Inform. Theory*, **52** (2006), 4892-4914.
[20] A. Krishna and J. P. Tillich, Towards low overhead magic state distillation, *Phys. Rev. Lett.*, **123** (2019), 070507.
[21] K. Li, C. Li, T. Helleseth and L. Qu, Binary linear codes with few weights from two-to-one functions, *IEEE Trans. Inf. Theory*, **67** (2021), 4263-4275.
[22] K. Li, S. Mesnager and L. Qu, Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$, *Proceedings of the 9th International Workshop on Signal Design and its Applications in Communications (IWSDA)*, Dongguan, China, 2019.
[23] K. Li, S. Mesnager and L. Qu, Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$, *IEEE Trans. Inf. Theory,* **67** (2021), 3486-3496.
[24] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
[25] S. Mesnager, L. Qian, X. Cao and M. Yuan, Several families of binary minimal linear codes from two-to-one functions, *IEEE Trans. Inf. Theory*, **69** (2023), 3285-3301.
[26] N. Rengaswamy, R. Calderbank, M. Newman and H. D. Pfister, Classical coding problem from transversal T-gates, *Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, USA, (2020), 1891-1896.
[27] N. Rengaswamy, R. Calderbank, M. Newman and H. D. Pfister, On optimality of CSS codes for transversal T, *IEEE J. Select. Areas Inf. Theory*, **1** (2020), 499-514.
[28] A. Steane, Multiple-particle interference and quantum error correction, *Proc. R. Soc. Lond. Ser. A*, **452** (1996), 2551-2577.

[29] C. Tang, N. Li, Y. Qi, Z. Zhou and T. Helleseth, Linear codes with two or three weights from weakly regular bent functions, *IEEE Trans. Inf. Theory*, **62** (2016), 1166-1176.
[30] C. Xiang, It is indeed a fundamental construction of all linear codes, preprint, 2016, arXiv:1610.06355.
[31] M. Yuan, D. Zheng and Y.-P. Wang, Two-to-one mappings and involutions without fixed points over $\mathbb{F}_{2^n}$, *Finite Fields Appl.*, **76** (2021), 101913, 23 pp.

Received October 2024; 1st revision February 2025; final revision November 2025; early access December 2025.