On the covering structures of two classes of linear codes from perfect nonlinear functions

Li, Chao; Ling, San; Qu, Longjiang

2009

Li, C., Ling, S., & Qu, L. (2009). On the Covering Structures of Two Classes of Linear Codes From Perfect Nonlinear Functions. IEEE Transactions on Information Theory, 55(1), 70-82.

<https://hdl.handle.net/10356/96412>

<https://doi.org/10.1109/TIT.2008.2008145>

© 2009 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TIT.2008.2008145>].

Downloaded on 26 Apr 2023 21:02:54 SGT

On the Covering Structures of Two Classes of Linear Codes From Perfect Nonlinear Functions

Chao Li, San Ling, and Longjiang Qu

Abstract—In this paper, the weight distributions of two classes of linear codes based on all known explicit perfect nonlinear functions from F_{q^m} to itself are determined using a unified approach. All the minimal codewords of these codes are characterized according to their weights, which suggests that their covering structures are determined. Finally, all the minimal access sets of the secret sharing schemes based on their dual codes are obtained.

Index Terms—Access structures, covering structures, perfect nonlinear functions, weight distributions.

I. INTRODUCTION

SECRET sharing schemes were introduced by Blakley [4] and Shamir [20] in 1979, respectively. Since McEliece and Sarwate [18] pointed out the relationship between Shamir's secret sharing schemes and the Reed–Solomon codes in 1981, many constructions of secret sharing schemes based on linear codes have been proposed [13], [16], [17], [9], [6]. Among these constructions, Massey found the relationship between the access structures of the secret sharing schemes and the covering structures of the dual code of the underlying code [16], [17]. In fact, there exists a one-to-one correspondence between the set of minimal access sets and the set of minimal codewords of the dual codes whose first coordinate is 1 (see Section IV for precise definitions). The covering problem of a linear code refers to the determination of the set of all the minimal codewords in the linear code, which is called the covering structure of the linear code. Determining the covering structures is extremely hard for general linear codes. This was done only for a few classes of special linear codes. Ashikhmin and Barg [1], [2] presented some basic properties of the minimal codewords in general linear codes, obtained all the minimal codewords for some special codes including the Hamming codes and second-order

Reed–Muller codes, and they pointed out that there exist linear codes all of whose nonzero codewords are minimal. Yuan and Ding [22] characterized the minimal codewords of three kinds of linear codes, using exponential sums over finite fields, and constructed some linear codes all of whose nonzero codewords are minimal.

Definition 1: Let F_{q^m} be a finite field of order q^m , where q is an odd prime power and m is a positive integer. A function $f : F_{q^m} \rightarrow F_{q^m}$ is called perfect nonlinear if $f(x+a) - f(x)$ is a permutation from F_{q^m} to itself for every $a \in F_{q^m}^*$.

Up to now, all known explicit perfect nonlinear functions from F_{q^m} to itself are affine equivalent to one of the following functions [11], [21]:

- 1) $\Pi_1(x) = x^{q^t+1}$, where $t \geq 0$ is an integer and $\frac{m}{\gcd(m,t)}$ is odd [8];
- 2) $\Pi_2(x) = x^{\frac{3^k+1}{2}}$, where $q = 3$, k is odd, and $\gcd(m, k) = 1$ [7];
- 3) $\Pi_3(x) = x^{10} - ux^6 - u^2x^2$, where $q = 3$, m is odd, and $u \in F_{q^m}^*$ [10].

We note, however, that, strictly speaking, the above list is not complete, since every semifield of odd order can give a perfect nonlinear function [12]. In this paper, $\Pi_1(x) = x^{q^t+1}$, $\Pi_2(x) = x^{\frac{3^k+1}{2}}$, and $\Pi_3(x) = x^{10} - ux^6 - u^2x^2$ are said to be the first, second, and third perfect nonlinear functions, respectively, and all the known explicit perfect nonlinear functions from F_{q^m} to itself refer to these three families of functions. It is noted that $\Pi(x) = x^2$ is a first perfect nonlinear function with $t = 0$ and it is also a second perfect nonlinear function with $k = 1$.

Recently, Carlet, Ding, and Yuan constructed two classes of q -ary linear codes based on perfect nonlinear functions from F_{q^m} to itself as follows [6].

Definition 2: Let $F_{q^m} = \{\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_{q^m-1}\}$ and $\gamma_0 = 0$, let $\Pi(x)$ be a perfect nonlinear function from F_{q^m} to itself, and let $f_{a,b}(x) = \text{tr}(a\Pi(x) + bx)$ and $f_{a,b,c}(x) = \text{tr}(a\Pi(x) + bx + c)$ be two functions from F_{q^m} to F_q , where $a, b, c \in F_{q^m}$ and $\text{tr}(\cdot)$ denotes the trace function from F_{q^m} to F_q , i.e., $\text{tr}(x) = x + x^q + x^{q^2} + \dots + x^{q^{m-1}}$ for all $x \in F_{q^m}$. Let C_Π and $\bar{C}_\Pi$ be (linear) codes over F_q defined as follows:

$$C_\Pi = \{(f_{a,b}(\gamma_1), f_{a,b}(\gamma_2), \dots, f_{a,b}(\gamma_{q^m-1})) | a, b \in F_{q^m}\} \quad (1)$$

and

$$\bar{C}_\Pi = \{(f_{a,b,c}(\gamma_0), f_{a,b,c}(\gamma_1), \dots, f_{a,b,c}(\gamma_{q^m-1})) | a, b, c \in F_{q^m}\}. \quad (2)$$

Six open problems were proposed in [6], five of which are related to the weight distributions of the above codes and the access structures of the secret sharing schemes based on their

The work of S. Ling was supported in part by MOE-AcRF under research Grant T206B2204. This work was performed while C. Li was visiting the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University.

C. Li and L. Qu are with the Department of Mathematics and System Sciences, Science College, National University of Defence Technology, Changsha 410073, China and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: lichao_nudt@sina.com; ljqu_happy@hotmail.com).

S. Ling is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Singapore (e-mail: lingsan@ntu.edu.sg).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.2008145

dual codes. These can be summarized and generalized as the following two problems.

Problem 1: Determine the weight distributions of C_Π and $\bar{C}_\Pi$ based on all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself.

Problem 2: Determine the access structures of the secret sharing schemes based on $C_\Pi^\perp$ and $\bar{C}_\Pi^\perp$ for all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself, where $C_\Pi^\perp$ and $\bar{C}_\Pi^\perp$ are the dual codes of C_Π and $\bar{C}_\Pi$, respectively.

Remark: Open problems 2 and 3 in [6] are special cases of Problem 1 above. We also note that the conditions of open problems 4 and 6 are equivalent to that of open problem 5 in [6], since $2q \geq q^{\frac{m}{2}} + 1$ if and only if $m = 2$, when q is an odd prime power and $m \geq 2$. Therefore, open problems 5 and 6 in [6] are the special cases of Problem 2 above with $m = 2$, and open problem 4 in [6] for all known explicit perfect nonlinear functions can be regarded as special cases of Problem 2 above with $m = 2$.

For Problem 1, the known results are as follows.

- 1) The paper [21] partly answered Problem 1. The authors obtained the weight distributions of C_Π based on all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself, except for one open case, where q is an odd prime. However, as the authors of [21] said in their concluding remarks, since they did not see any possibility of a uniform treatment for determining the weight distributions of C_Π , they had to deal with the weight distributions of these linear codes separately.
- 2) Recently, [11] presented a uniform way to determine the weight distributions of C_Π for the first and second perfect nonlinear functions from F_{q^m} to itself by studying the value distributions of exponential sums over finite fields, where q is an odd prime.

There is no known work on the weight distribution of $\bar{C}_\Pi$.

In this paper, using a unified approach, we first determine the weight distributions of C_Π and $\bar{C}_\Pi$ based on all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself, where q is an odd prime power. The main contributions towards Problem 1 are as follows:

- 1) the determination of the weight distribution of $\bar{C}_\Pi$, which was not known before;
- 2) a new unified approach to the determination of the weight distribution of C_Π .

As for Problem 2, the paper [6] partly answered Problem 2. The authors determined the access structures of the secret sharing schemes based on $C_\Pi^\perp$ for all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself in the case $m \geq 3$, but they did not obtain the access structures of the secret sharing schemes based on $\bar{C}_\Pi^\perp$ with $m \geq 2$ and $C_\Pi^\perp$ with $m = 2$. The latter cases for three distinct explicit perfect nonlinear functions are regarded as three open problems in [6].

The main contributions of this paper to Problem 2 is the complete determination of the access structures of the secret sharing schemes based on both $C_\Pi^\perp$ and $\bar{C}_\Pi^\perp$. Using the properties of the weights of codewords in C_Π and $\bar{C}_\Pi$, we characterize all the minimal codewords in these codes for all known explicit per-

fect nonlinear functions $\Pi(x)$ from F_{q^m} to itself, which suggests that the covering structures of these codes are determined. This in turn leads to the determination of all the minimal access sets of the secret sharing schemes in question.

These results demonstrate that the two problems above are completely solved.

This paper is organized as follows. In Section II, we determine the weight distributions of C_Π and $\bar{C}_\Pi$ for all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself. In Section III, we characterize all the minimal codewords of C_Π and $\bar{C}_\Pi$. In Section IV, all the minimal access sets of the secret sharing schemes based on $C_\Pi^\perp$ and $\bar{C}_\Pi^\perp$ are obtained.

II. WEIGHT DISTRIBUTIONS OF TWO CLASSES OF LINEAR CODES FROM PERFECT NONLINEAR FUNCTIONS

A linear code of length n , dimension k , and minimum distance d over a finite field F_q is often denoted as an $[n, k, d; q]$ -code, or $[n, k; q]$ -code if d is either not known or needs not be reflected. The weight distribution of such a code refers to the set $\{A_0, A_1, \dots, A_n\}$, where A_i denotes the number of codewords of weight i . The determination of the weight distribution of a code is often a hard problem.

The paper [6] pointed out that C_Π is a $[q^m - 1, 2m; q]$ -code and $\bar{C}_\Pi$ is a $[q^m, 2m + 1; q]$ -code, and demonstrated that many codes C_Π and their dual codes $C_\Pi^\perp$ are optimal or among the best codes for such lengths and dimensions. The main results of this section are the following two theorems.

Theorem 1: Let $\Pi(x)$ be a known explicit perfect nonlinear function from F_{q^m} to itself, where q is an odd prime power and m is a positive integer greater than 1. Then:

- i) if m is odd, the weight distribution of C_Π is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{(q-1)q^{m-1}-q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^m-1) \left(q^{m-1} + q^{\frac{m-1}{2}} \right) \\ A_{(q-1)q^{m-1}} = (q^{m-1} + 1)(q^m - 1) \\ A_{(q-1)q^{m-1}+q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^m-1) \left(q^{m-1} - q^{\frac{m-1}{2}} \right); \end{cases} \quad (3)$$

- ii) if m is even, the weight distribution of C_Π is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})} = \frac{1}{2}(q^m-1) \left(q^{m-1} + (q-1)q^{\frac{m-2}{2}} \right) \\ A_{(q-1)q^{m-1}-q^{\frac{m-2}{2}}} = \frac{1}{2}(q-1)(q^m-1) \left(q^{m-1} + q^{\frac{m-2}{2}} \right) \\ A_{(q-1)q^{m-1}} = q^m - 1 \\ A_{(q-1)q^{m-1}+q^{\frac{m-2}{2}}} = \frac{1}{2}(q-1)(q^m-1) \left(q^{m-1} - q^{\frac{m-2}{2}} \right) \\ A_{(q-1)(q^{m-1}+q^{\frac{m-2}{2}})} = \frac{1}{2}(q^m-1) \left(q^{m-1} - (q-1)q^{\frac{m-2}{2}} \right). \end{cases} \quad (4)$$

Theorem 2: Let $\Pi(x)$ be a known explicit perfect nonlinear function from F_{q^m} to itself, where q is an odd prime power and m is a positive integer greater than 1. Then:

i) if m is odd, the weight distribution of $\bar{C}_\Pi$ is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{(q-1)q^{m-1}-q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^{2m}-q^m) \\ A_{(q-1)q^{m-1}} = (q^m+q)(q^m-1) \\ A_{(q-1)q^{m-1}+q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^{2m}-q^m) \\ A_{q^m} = q-1; \end{cases} \quad (5)$$

ii) if m is even, the weight distribution of $\bar{C}_\Pi$ is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})} = \frac{1}{2}(q^{2m}-q^m) \\ A_{(q-1)q^{m-1}-q^{\frac{m-2}{2}}} = \frac{1}{2}(q-1)(q^{2m}-q^m) \\ A_{(q-1)q^{m-1}} = q^{m+1}-q \\ A_{(q-1)q^{m-1}+q^{\frac{m-2}{2}}} = \frac{1}{2}(q-1)(q^{2m}-q^m) \\ A_{(q-1)(q^{m-1}+q^{\frac{m-2}{2}})} = \frac{1}{2}(q^{2m}-q^m) \\ A_{q^m} = q-1. \end{cases} \quad (6)$$

Theorems 1 and 2 answer Problem 1 in Section I, which suggests that open problems 2 and 3 in [6] are completely solved. Furthermore, we obtain the following.

Corollary 1: If m is an odd positive integer greater than 1, then C_Π is a $[q^m-1, 2m, (q-1)q^{m-1}-q^{\frac{m-1}{2}}; q]$ -code and $\bar{C}_\Pi$ is a $[q^m, 2m+1, (q-1)q^{m-1}-q^{\frac{m-1}{2}}; q]$ -code.

Corollary 2: If m is an even positive integer, then C_Π is a $[q^m-1, 2m, (q-1)(q^{m-1}-q^{\frac{m-2}{2}}); q]$ -code and $\bar{C}_\Pi$ is a $[q^m, 2m+1, (q-1)(q^{m-1}-q^{\frac{m-2}{2}}); q]$ -code.

A. Preliminaries

In order to prove Theorems 1 and 2, we need to introduce some concepts and results on quadratic forms and character sums over finite fields.

A quadratic form in n indeterminates over F_q is a homogenous polynomial of degree 2, or the zero polynomial in $F_q[x_1, x_2, \dots, x_n]$, where q is a prime power. When q is an odd prime power, every quadratic form $f(x_1, x_2, \dots, x_n)$ can be represented in the following form:

$$f(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j, (a_{ij} = a_{ji}, a_{ij} \in F_q).$$

We associate with $f(x_1, x_2, \dots, x_n)$ the $n \times n$ symmetric matrix A whose (i, j) entry is a_{ij} , which is called the matrix of $f(x_1, x_2, \dots, x_n)$. The determinant and rank of matrix A are called the determinant and rank of the quadratic form $f(x_1, x_2, \dots, x_n)$, and they are denoted by $\det(f)$ and $\text{rank}(f)$, respectively. If a quadratic form $f(x_1, x_2, \dots, x_n)$ is of rank n , we say that $f(x_1, x_2, \dots, x_n)$ is nondegenerate. Two quadratic forms $f(x_1, x_2, \dots, x_n)$ and $g(y_1, y_2, \dots, y_n)$ over F_q are called equivalent if $f(x_1, x_2, \dots, x_n)$ can be transformed into $g(y_1, y_2, \dots, y_n)$ by means of a nonsingular linear substitution of indeterminates $\underline{x} = P\underline{y}$, where $\underline{x} = (x_1, x_2, \dots, x_n)^T$, $\underline{y} = (y_1, y_2, \dots, y_n)^T$, P is a nonsingular matrix over F_q , and T is the transpose operation.

The quadratic character η of F_q is defined by

$$\eta(x) = \begin{cases} 0, & \text{if } x = 0 \\ 1, & \text{if } x \text{ is a nonzero square of } F_q \\ -1, & \text{if } x \text{ is a nonsquare of } F_q \end{cases}$$

and the canonical additive character χ of F_q is defined by $\chi(x) = \zeta_p^{\text{tr}(x)}$, where p is the characteristic of F_q , $\zeta_p = e^{\frac{2\pi i}{p}}$, and $\text{tr}(\cdot)$ is the absolute trace function from F_q to F_p .

Lemma 1 [15, Th. 6.21]: Let $f(x_1, x_2, \dots, x_n)$ be a quadratic form of rank r over F_q , where q is an odd prime power. Then, $f(x_1, x_2, \dots, x_n)$ is equivalent to a diagonal quadratic form $a_1 y_1^2 + a_2 y_2^2 + \dots + a_r y_r^2$, where $a_1, a_2, \dots, a_r$ are nonzero elements of F_q .

Lemma 2 [15, Th. 6.26 and 6.27]: Let m be a positive integer, let q be an odd prime power, let η be the quadratic character of F_q , and let $b \in F_q$. If $f(x_1, x_2, \dots, x_n)$ is a nondegenerate quadratic form over F_q , and Δ denotes the determinant of f , then the number of solutions in F_q^n of the equation $f(x_1, x_2, \dots, x_n) = b$ is given by

$$\begin{cases} q^{n-1} + q^{\frac{n-1}{2}} \eta((-1)^{\frac{n-1}{2}} b \Delta), & \text{when } n \text{ is odd} \\ q^{n-1} + v(b) q^{\frac{n-2}{2}} \eta((-1)^{\frac{n}{2}} \Delta), & \text{when } n \text{ is even} \end{cases}$$

where $v(\cdot)$ is defined by $v(b) = -1$ for $b \in F_q^*$ and $v(0) = q-1$.

Lemma 3 [15, Th. 5.15]: Let $q = p^m$, where p is an odd prime and m is a positive integer. Let $G(\eta, \chi)$ be the Gauss sum of the quadratic character η and the canonical additive character χ of F_q , i.e.,

$$G(\eta, \chi) = \sum_{c \in F_q^*} \eta(c) \chi(c).$$

Then, $\sum_{c \in F_q^*} \eta(c) = \sum_{c \in F_q} \chi(c) = 0$, and

$$G^2(\eta, \chi) = \begin{cases} q, & \text{if } p \equiv 1 \pmod{4} \\ -q, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Lemma 4 [15, Exercises 6.27 and 6.28]: Let η and χ be the quadratic character and the canonical additive character of F_q , respectively. Let $f(x_1, x_2, \dots, x_n)$ be a nondegenerate quadratic form over F_q . Then

$$\begin{aligned} & \sum_{c_1, c_2, \dots, c_n \in F_q} \chi(f(c_1, c_2, \dots, c_n)) \\ &= \begin{cases} q^{\frac{n-1}{2}} \eta((-1)^{\frac{n-1}{2}} \Delta) G(\eta, \chi), & \text{when } n \text{ is odd} \\ q^{\frac{n}{2}} \eta((-1)^{\frac{n}{2}} \Delta), & \text{when } n \text{ is even} \end{cases} \end{aligned}$$

where Δ denotes the determinant of f .

Lemma 5 comes from [11, p. 3037]. Although these results are proved only for the first perfect nonlinear functions, they are also true for the third perfect nonlinear functions.

Lemma 5: Let q be an odd prime power and let m be a positive integer greater than 1. Then, for every nonzero $a \in F_{q^m}$, $f_a(x) = \text{tr}(a\Pi(x))$ is a nondegenerate quadratic form of m indeterminates over F_q , where $\Pi(x) = \Pi_1(x)$ or $\Pi_3(x)$.

Let β be a primitive element of F_q , and denote

$$k_0 = \#\{x \in F_{q^m} \mid \text{tr}(a\Pi(x)) = 0\}$$

$$k_i = \#\{x \in F_{q^m} \mid \text{tr}(a\Pi(x)) = \beta^i\}, \quad i = 1, 2, \dots, q-1$$

where $\Pi(x)$ is a perfect nonlinear function from F_{q^m} to itself. Then, we call $(k_0, k_1, \dots, k_{q-1})$ the preimage distribution of $\text{tr}(a\Pi(x))$.

For every nonzero $a \in F_{q^m}$ and $\Pi(x) = \Pi_1(x)$ or $\Pi_3(x)$, let $\Delta_a = \det(\text{tr}(a\Pi(x)))$. Clearly, $\Delta_a \in F_q^*$. According to Lemma 2, the preimage distributions of $\text{tr}(a\Pi(x))$ take only two cases: one case holds for $\eta(\Delta_a) = 1$ and the other case holds for $\eta(\Delta_a) = -1$. It is easily verified that the preimage distributions of $\text{tr}(a\Pi(x))$ have the following properties:

- 1) when $\Pi(x) = \Pi_1(x)$, for all $a \in F_{q^m}^*$, the preimage distribution of $\text{tr}(a\Pi(x))$ is the same as that of $\text{tr}(ax^2)$;
- 2) when $\Pi(x) = x^2$, for all $a \in F_{q^m}^*$, the preimage distributions of $\text{tr}(ax^2)$ take only two cases: one case holds for all nonzero squares $a \in F_{q^m}$ and the other case holds for all nonsquares $a \in F_{q^m}$;
- 3) when $\Pi(x) = \Pi_3(x)$, for all $a \in F_{q^m}^*$, the preimage distributions of $\text{tr}(a\Pi(x))$ take only two cases: one case holds for $\text{tr}(a\Pi(x))$ if and only if the other case holds for $\text{tr}(-a\Pi(x))$.

Based on the above properties of the preimage distributions of $\text{tr}(a\Pi(x))$, we can obtain the following.

Theorem 3: Let q be an odd prime power and let m be a positive integer greater than 1. Then, there are exactly $\frac{1}{2}(q^m - 1)$ nonzero $a \in F_{q^m}$ such that $\eta(\Delta_a) = 1$, and other $\frac{1}{2}(q^m - 1)$ nonzero $a \in F_{q^m}$ such that $\eta(\Delta_a) = -1$, where η is the quadratic character of F_q .

On the other hand, it is easily verified that $\text{tr}(a\Pi_2(x))$ is a homogenous polynomial of degree $k+1$ of m indeterminates over F_3 for every nonzero $a \in F_{3^m}$, where k is the parameter of the second perfect nonlinear function. Hence, it is a quadratic form over F_3 only when $k = 1$. However, for any $a, b \in F_{3^m}$, it is shown in [19] that the character sum

$$S(a, b) = \sum_{x \in F_{3^m}} \omega^{\text{tr}(a\Pi_2(x) + bx)}, \quad \text{where } \omega = e^{\frac{2\pi i}{3}}$$

is related to quadratic forms over F_3 , and the value distribution of $S(a, b)$ is given as follows, by using the theory of quadratic forms over finite fields.

Theorem 4 [19]:

- i) If m is odd, the value distribution of the character sums $\{S(a, b) \mid a, b \in F_{3^m}\}$ is given by

$$\begin{cases} \lambda_{3^m} = 1 \\ \lambda_0 = 3^m - 1 \\ \lambda_{i3^{\frac{m}{2}}} = \frac{1}{2}(3^m - 1)3^{m-1} \\ \lambda_{-i3^{\frac{m}{2}}} = \frac{1}{2}(3^m - 1)3^{m-1} \\ \lambda_{i3^{\frac{m}{2}}\omega} = \frac{1}{2}(3^m - 1)\left(3^{m-1} - 3^{\frac{m-1}{2}}\right) \\ \lambda_{-i3^{\frac{m}{2}}\omega} = \frac{1}{2}(3^m - 1)\left(3^{m-1} + 3^{\frac{m-1}{2}}\right) \\ \lambda_{i3^{\frac{m}{2}}\omega^2} = \frac{1}{2}(3^m - 1)\left(3^{m-1} + 3^{\frac{m-1}{2}}\right) \\ \lambda_{-i3^{\frac{m}{2}}\omega^2} = \frac{1}{2}(3^m - 1)\left(3^{m-1} - 3^{\frac{m-1}{2}}\right). \end{cases} \quad (7)$$

- ii) If m is even, the value distribution of the character sums $\{S(a, b) \mid a, b \in F_{3^m}\}$ is given by

$$\begin{cases} \lambda_{3^m} = 1 \\ \lambda_0 = 3^m - 1 \\ \lambda_{3^{\frac{m}{2}}} = \frac{1}{2}(3^m - 1)\left(3^{m-1} + 2 \cdot 3^{\frac{m-2}{2}}\right) \\ \lambda_{-3^{\frac{m}{2}}} = \frac{1}{2}(3^m - 1)\left(3^{m-1} - 2 \cdot 3^{\frac{m-2}{2}}\right) \\ \lambda_{3^{\frac{m}{2}}\omega} = \frac{1}{2}(3^m - 1)\left(3^{m-1} - 3^{\frac{m-2}{2}}\right) \\ \lambda_{-3^{\frac{m}{2}}\omega} = \frac{1}{2}(3^m - 1)\left(3^{m-1} + 3^{\frac{m-2}{2}}\right) \\ \lambda_{3^{\frac{m}{2}}\omega^2} = \frac{1}{2}(3^m - 1)\left(3^{m-1} - 3^{\frac{m-2}{2}}\right) \\ \lambda_{-3^{\frac{m}{2}}\omega^2} = \frac{1}{2}(3^m - 1)\left(3^{m-1} + 3^{\frac{m-2}{2}}\right) \end{cases} \quad (8)$$

where $\omega = e^{\frac{2\pi i}{3}}$, and λ_v denotes the frequency of value v of the character sums $S(a, b)$ as (a, b) ranges over all elements of $F_{3^m} \times F_{3^m}$.

B. Proof of Theorem 2

For any two codewords $c_{a,b,c}$ and $c_{a',b',c'}$ in $\bar{C}_\Pi$ defined by (2), where

$$c_{a,b,c} = (f_{a,b,c}(\gamma_0), f_{a,b,c}(\gamma_1), \dots, f_{a,b,c}(\gamma_{q^m-1}))$$

$$c_{a',b',c'} = (f_{a',b',c'}(\gamma_0), f_{a',b',c'}(\gamma_1), \dots, f_{a',b',c'}(\gamma_{q^m-1}))$$

it is easy to verify that $c_{a,b,c} = c_{a',b',c'}$ if and only if $a = a', b = b'$, and $\text{tr}(c) = \text{tr}(c')$. Then, $\bar{C}_\Pi$ can be expressed as follows:

$$\bar{C}_\Pi = \{(f_{a,b,c}(\gamma_0), \dots, f_{a,b,c}(\gamma_{q^m-1})) \mid a, b \in F_{q^m}, c \in \Omega\}$$

where $\Omega = \{t_0, t_1, \dots, t_{q-1}\}$ and $t_0, t_1, \dots, t_{q-1}$ are distinct elements of F_{q^m} such that $\text{tr}(t_0) = 0$ and $\text{tr}(t_i) = \beta^i, i = 1, 2, \dots, q-1$, β being the primitive element of F_q .

Let $w_H(a, b, c)$ be the Hamming weight of the codeword $c_{a,b,c}$ in $\bar{C}_\Pi$.

Case 1: $\Pi(x) = \Pi_1(x)$ or $\Pi_3(x)$.

When $a = 0$, it is easily seen that $w_H(0, 0, t_0) = 0$, $w_H(0, 0, c) = q^m$ for every $c \in \Omega \setminus \{t_0\}$, and $w_H(0, b, c) = (q-1)q^{m-1}$ for any $b \in F_{q^m}^*$ and $c \in \Omega$.

Next, we consider $w_H(a, b, c)$ in the case $a \neq 0$.

By Lemmas 5 and 1, there exists a nonsingular linear substitution $\underline{x} = P\underline{y}$ such that $\text{tr}(a\Pi(x))$ is equivalent to

$$a_1y_1^2 + a_2y_2^2 + \dots + a_my_m^2$$

where $a_1, a_2, \dots, a_m$ are nonzero elements of F_q , and $P \in F_q^{m \times m}$ is a nonsingular matrix. It is noted that $\eta(\Delta_a) = \eta(a_1a_2 \dots a_m)$, where Δ_a is the determinant of $\text{tr}(a\Pi(x))$ and η is the quadratic character of F_q . It follows that

$$\text{tr}(a\Pi(x) + bx) = a_1y_1^2 + a_2y_2^2 + \dots + a_my_m^2 + b_1y_1 + \dots + b_my_m$$

where $b_1, b_2, \dots, b_m \in F_q$. Note that there is a one-to-one correspondence between $b \in F_{q^m}$ and $(b_1, b_2, \dots, b_m) \in F_q^m$ such that $b = 0$ if and only if $(b_1, b_2, \dots, b_m) = 0$.

Let $z_1 = y_1 + \frac{b_1}{2a_1}, z_2 = y_2 + \frac{b_2}{2a_2}, \dots, z_m = y_m + \frac{b_m}{2a_m}$ and let $c_0 = -\sum_{i=1}^m \frac{b_i^2}{4a_i} \in F_q$. Then

$$\text{tr}(a\Pi(x) + bx) = a_1 z_1^2 + a_2 z_2^2 + \dots + a_m z_m^2 + c_0.$$

With χ the canonical additive character of F_q , $t = \text{tr}(c)$ and $d = t - \sum_{i=1}^m \frac{b_i^2}{4a_i} \in F_q$ (note that t ranges over all the elements of F_q as c ranges over all the elements of Ω), it follows that

$$\begin{aligned} w_H(a, b, c) &= q^m - \#\{x \in F_{q^m}, \text{tr}(a\Pi(x) + bx + c) = 0\} \\ &= q^m - \frac{1}{q} \sum_{s \in F_q} \sum_{x \in F_{q^m}} \chi(s(\text{tr}(a\Pi(x) + bx + c))) \\ &= (q-1)q^{m-1} - \frac{1}{q} \sum_{s \in F_q^*} \chi(st) \sum_{x \in F_{q^m}} \chi(s(\text{tr}(a\Pi(x) + bx))) \\ &= (q-1)q^{m-1} - \frac{1}{q} \sum_{s \in F_q^*} \chi(sd) \times \\ &\quad \times \sum_{z_1, z_2, \dots, z_m \in F_q} \chi(sa_1 z_1^2 + sa_2 z_2^2 + \dots + sa_m z_m^2). \end{aligned} \quad (9)$$

i) If m is odd, from Lemma 4, for any $s \in F_q^*$, we obtain

$$\begin{aligned} &\sum_{z_1, z_2, \dots, z_m \in F_q} \chi(sa_1 z_1^2 + sa_2 z_2^2 + \dots + sa_m z_m^2) \\ &= q^{\frac{m-1}{2}} \eta\left((-1)^{\frac{m-1}{2}} s^m a_1 a_2 \dots a_m\right) G(\eta, \chi) \\ &= q^{\frac{m-1}{2}} G(\eta, \chi) \eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta(s). \end{aligned} \quad (10)$$

It follows that

$$\begin{aligned} w_H(a, b, c) &= (q-1)q^{m-1} - q^{\frac{m-3}{2}} G(\eta, \chi) \\ &\quad \times \eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \sum_{s \in F_q^*} \chi(sd) \eta(s). \end{aligned} \quad (11)$$

If $d = 0$, then

$$\sum_{s \in F_q^*} \chi(sd) \eta(s) = \sum_{s \in F_q^*} \eta(s) = 0$$

which implies that $w_H(a, b, c) = (q-1)q^{m-1}$.

If $d \neq 0$, then

$$\begin{aligned} \sum_{s \in F_q^*} \chi(sd) \eta(s) &= \sum_{s' \in F_q^*} \chi(s') \eta(d^{-1} s') \\ &= \eta(d) G(\eta, \chi) \end{aligned}$$

and noting that $G^2(\eta, \chi) = \pm q$ from Lemma 3, then

$$w_H(a, b, c) = (q-1)q^{m-1} \pm q^{\frac{m-1}{2}} \eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta(d).$$

Therefore, the following assertions hold for $a \neq 0$:

1) $w_H(a, b, c) = (q-1)q^{m-1}$ if and only if

$$t - \sum_{i=1}^m \frac{b_i^2}{4a_i} = 0; \quad (12)$$

2) $w_H(a, b, c) = (q-1)q^{m-1} + q^{\frac{m-1}{2}}$ if and only if

$$\begin{aligned} &\eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta\left(t - \sum_{i=1}^m \frac{b_i^2}{4a_i}\right) \\ &= \begin{cases} -1, & \text{if } p \equiv 1 \pmod{4} \\ 1, & \text{if } p \equiv 3 \pmod{4}; \end{cases} \end{aligned} \quad (13)$$

3) $w_H(a, b, c) = (q-1)q^{m-1} - q^{\frac{m-1}{2}}$ if and only if

$$\begin{aligned} &\eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta\left(t - \sum_{i=1}^m \frac{b_i^2}{4a_i}\right) \\ &= \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \end{aligned} \quad (14)$$

According to Theorem 3 and Lemma 2, the number of $(a, b, c) \in F_{q^m}^* \times F_{q^m} \times \Omega$ satisfying the conditions in (12) can be calculated as follows:

$$\begin{aligned} &(q^m - 1) \left(q^{m-1} + \sum_{t \in F_q^*} \left(q^{m-1} + q^{\frac{m-1}{2}} \eta\left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta(t) \right) \right) \\ &= (q^m - 1)(q^{m-1} + (q-1)q^{m-1}) = q^m(q^m - 1). \end{aligned}$$

Therefore, combining the two cases $a = 0$ and $a \neq 0$, we obtain

$$A_{(q-1)q^m} = (q^m - 1)q + q^m(q^m - 1) = (q^m + q)(q^m - 1). \quad (15)$$

In the case $p \equiv 1 \pmod{4}$, the number of $(a, b, c) \in F_{q^m}^* \times F_{q^m} \times \Omega$ satisfying the conditions in (13) can be calculated as follows:

$$\begin{aligned} &\frac{1}{2}(q-1)(q^m - 1) \left(q^{m-1} + \sum_{u \in F_q^*} \left(q^{m-1} + q^{\frac{m-1}{2}} \eta(u) \right) \right) \\ &= \frac{1}{2}(q-1)(q^{2m} - q^m) \end{aligned}$$

which implies that

$$A_{(q-1)q^{m-1} + q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^{2m} - q^m). \quad (16)$$

Similarly, we also obtain

$$A_{(q-1)q^{m-1} - q^{\frac{m-1}{2}}} = \frac{1}{2}(q-1)(q^{2m} - q^m). \quad (17)$$

In the case $p \equiv 3 \pmod{4}$, results similar to those of (16) and (17) can be obtained in a similar fashion. From (15)–(17) and noting that $A_0 = 1$, $A_{q^m} = q - 1$, (5) follows for odd m in the case $\Pi(x) = \Pi_1(x)$ or $\Pi_3(x)$.

ii) If m is even, from Lemma 4, for any $s \in F_q^*$, we obtain

$$\begin{aligned} & \sum_{z_1, z_2, \dots, z_m \in F_q} \chi(sa_1 z_1^2 + sa_2 z_2^2 + \dots + sa_m z_m^2) \\ &= q^{\frac{m}{2}} \eta((-1)^{\frac{m}{2}} s^m a_1 a_2 \dots a_m) \\ &= q^{\frac{m}{2}} \eta((-1)^{\frac{m}{2}} \Delta_a). \end{aligned}$$

From (9), we have

$$\begin{aligned} w_H(a, b, c) &= (q-1)q^{m-1} - q^{\frac{m-2}{2}} \eta((-1)^{\frac{m}{2}} \Delta_a) \sum_{s \in F_q^*} \chi(sd) \\ &= \begin{cases} (q-1)q^{m-1} - (q-1)q^{\frac{m-2}{2}} \eta((-1)^{\frac{m}{2}} \Delta_a), & \text{if } d=0 \\ (q-1)q^{m-1} + (q-1)q^{\frac{m-2}{2}} \eta((-1)^{\frac{m}{2}} \Delta_a), & \text{if } d \neq 0. \end{cases} \end{aligned} \quad (18)$$

Therefore, we obtain the following assertions for $a \neq 0$:

1) $w_H(a, b, c) = (q-1)(q^{m-1} - q^{\frac{m-2}{2}})$ if and only if

$$t - \sum_{i=1}^m \frac{b_i^2}{4a_i} = 0 \quad \text{and} \quad \eta((-1)^{\frac{m}{2}} \Delta_a) = 1; \quad (19)$$

2) $w_H(a, b, c) = (q-1)(q^{m-1} + q^{\frac{m-2}{2}})$ if and only if

$$t - \sum_{i=1}^m \frac{b_i^2}{4a_i} = 0 \quad \text{and} \quad \eta((-1)^{\frac{m}{2}} \Delta_a) = -1; \quad (20)$$

3) $w_H(a, b, c) = (q-1)q^{m-1} + q^{\frac{m-2}{2}}$ if and only if

$$t - \sum_{i=1}^m \frac{b_i^2}{4a_i} \neq 0 \quad \text{and} \quad \eta((-1)^{\frac{m}{2}} \Delta_a) = 1; \quad (21)$$

4) $w_H(a, b, c) = (q-1)q^{m-1} - q^{\frac{m-2}{2}}$ if and only if

$$t - \sum_{i=1}^m \frac{b_i^2}{4a_i} \neq 0 \quad \text{and} \quad \eta((-1)^{\frac{m}{2}} \Delta_a) = -1. \quad (22)$$

It is easily seen that

$$A_0 = 1 \quad A_{(q-1)q^{m-1}} = q^{m+1} - q \quad A_{q^m} = q - 1 \quad (23)$$

since these weights occur only in the case $a = 0$.

Noting that the number of $(a, b, c) \in F_q^* \times F_q^m \times \Omega$ satisfying the conditions in (19) is $\frac{1}{2}(q^m - 1)q^m$, then we have

$$A_{(q-1)(q^{m-1} - q^{\frac{m-2}{2}})} = \frac{1}{2}(q^{2m} - q^m). \quad (24)$$

Similarly, we also obtain

$$A_{(q-1)(q^{m-1} + q^{\frac{m-2}{2}})} = \frac{1}{2}(q^{2m} - q^m). \quad (25)$$

Hence, from (19), (21), and (24), we obtain

$$\begin{aligned} A_{(q-1)q^{m-1} + q^{\frac{m-2}{2}}} &= \frac{1}{2}(q^m - 1)q^{m+1} - \frac{1}{2}(q^{2m} - q^m) \end{aligned}$$

$$= \frac{1}{2}(q-1)(q^{2m} - q^m). \quad (26)$$

Likewise, from (20), (22), and (25), we obtain

$$A_{(q-1)q^{m-1} - q^{\frac{m-2}{2}}} = \frac{1}{2}(q-1)(q^{2m} - q^m). \quad (27)$$

Therefore, (6) readily follows from (23), (24), (25), (26), and (27) for even m in the case $\Pi(x) = \Pi_1(x)$ or $\Pi_3(x)$.

Case 2: $\Pi(x) = \Pi_2(x)$.

In this subcase, $q = 3$. Noting that the character sum

$$S(a, b) = \sum_{x \in F_{3^m}} \omega^{\text{tr}(a\Pi_2(x) + bx)}$$

satisfies $S(-a, -b) = \overline{S(a, b)}$ for any $a, b \in F_{3^m}$, where $\omega = e^{\frac{2\pi i}{3}}$ and $\overline{S(a, b)}$ denotes the complex conjugate of $S(a, b)$, it follows that

$$\begin{aligned} w_H(a, b, c) &= 3^m - \frac{1}{3} \sum_{s \in F_3} \sum_{x \in F_{3^m}} \omega^{\text{tr}(sa\Pi_2(x) + sbx + sc)} \\ &= 3^m - \frac{1}{3} \sum_{s \in F_3} \omega^{st} S(sa, sb) \\ &= 2 \cdot 3^{m-1} - \frac{1}{3} (\omega^t S(a, b) + \omega^{-t} S(-a, -b)) \\ &= 2 \cdot 3^{m-1} - \frac{2}{3} \text{Re}(\omega^t S(a, b)) \end{aligned}$$

where $t = \text{tr}(c)$ and $\text{Re}(\cdot)$ denotes the real part of a complex number.

In the following, we consider only the case of m odd. The case m even is similarly verified.

When m is odd, according to Theorem 4i), all the values of $S(a, b)$, where $a, b \in F_{3^m}$, are given as follows:

$$3^m, 0, \pm i3^{\frac{m}{2}}, \pm i3^{\frac{m}{2}}\omega, \pm i3^{\frac{m}{2}}\omega^2.$$

By direct calculations, when $S(a, b)$ takes on the following values:

$$3^m, 0, i3^{\frac{m}{2}}, -i3^{\frac{m}{2}}, i3^{\frac{m}{2}}\omega, -i3^{\frac{m}{2}}\omega, i3^{\frac{m}{2}}\omega^2, -i3^{\frac{m}{2}}\omega^2$$

the corresponding $w_H(a, b, c)$ with $t = \text{tr}(c) = 0$ takes on the following values:

$$\begin{aligned} & 0, 2 \cdot 3^{m-1}, 2 \cdot 3^{m-1}, 2 \cdot 3^{m-1}, 2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}}, \\ & 2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}, 2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}, 2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}}. \end{aligned}$$

Therefore, from (7), we obtain the frequencies of the above weights as follows in the case $t = 0$:

$$\begin{cases} A_0^{(0)} = 1 \\ A_{2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}}^{(0)} = (3^m - 1) \left(3^{m-1} + 3^{\frac{m-1}{2}} \right) \\ A_{2 \cdot 3^{m-1}}^{(0)} = (3^m - 1)(3^m - 1) \\ A_{2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}}}^{(0)} = (3^m - 1) \left(3^{m-1} - 3^{\frac{m-1}{2}} \right) \end{cases} \quad (28)$$

where, for $t = 0, 1, 2$, $A_w^{(t)}$ denotes the number of codewords $c_{a,b,c}$ of weight w with $t = \text{tr}(c)$.

Similarly, by direct calculations, the weights and their frequencies in the cases $t = 1$ and $t = 2$ are the same, and they are given as follows:

$$\begin{cases} A_{3^m}^{(t)} = 1 \\ A_{2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}}^{(t)} = \frac{1}{2}(3^m - 1) \left(2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}} \right) \\ A_{2 \cdot 3^{m-1}}^{(t)} = (3^m - 1)(3^{m-1} + 1) \\ A_{2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}}}^{(t)} = \frac{1}{2}(3^m - 1) \left(2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}} \right) \end{cases} \quad (29)$$

where $t = 1$ or 2 .

By adding up the frequencies of the corresponding weights for $t = 0, 1, 2$, we obtain the results of (5) with $q = 3$. $\square$

Remark: Since the weight distribution of C_Π is the same as that of the code $\{c_{a,b,c} \in \tilde{C}_\Pi | a, b \in F_{q^m}, c = t_0\}$. If we only consider the case $t = \text{tr}(t_0) = 0$ in the proof of Theorem 2, we can obtain Theorem 1.

From the proof of Theorems 1 and 2, we have the following two facts.

Corollary 3: When m is even, for the first or third perfect nonlinear function $\Pi(x)$, let $c_{a,b}$ be a nonzero codeword of C_Π . Then, $c_{a,b}$ is of weight $q^m - q^{m-1}$ if and only if $a = 0$ and $b \neq 0$.

Corollary 4: When m is even, for the first or third perfect nonlinear function $\Pi(x)$, let $c_{a,b,c}$ be a nonzero codeword of $\tilde{C}_\Pi$. Then, $c_{a,b,c}$ is of weight $q^m - q^{m-1}$ if and only if $a = 0$, $b \neq 0$ and $c \in \Omega$, and $c_{a,b,c}$ is of weight q^m if and only if $a = b = 0$ and $c \in \Omega \setminus \{t_0\}$.

III. COVERING STRUCTURES OF TWO CLASSES OF LINEAR CODES FROM PERFECT NONLINEAR FUNCTIONS

We begin with the following definitions.

Definition 3: Let $\underline{c} = (c_0, c_1, \dots, c_{n-1})$ be a vector of F_q^n . The support of $\underline{c}$, denoted by $\text{Supp}(\underline{c})$, is defined to be the set $\{i | 0 \leq i \leq n-1, c_i \neq 0\}$. For any two vectors $\underline{c}, \underline{c}' \in F_q^n$, $\underline{c}$ covers $\underline{c}'$ if the support of $\underline{c}$ contains that of $\underline{c}'$.

Definition 4: In a linear code C , a nonzero codeword is called a minimal codeword if it covers only its multiples but no other nonzero codewords.

In this section, we characterize all the minimal codewords of C_Π and $\tilde{C}_\Pi$ for all known explicit perfect nonlinear functions $\Pi(x)$ from F_{q^m} to itself, which suggests the covering structures of these codes are determined. The main results of this section are as follows.

Theorem 5 (Covering structure of C_Π): Let q be an odd prime power and let m be a positive integer greater than 1. If $\Pi(x)$ is a known explicit perfect nonlinear function from F_{q^m} to itself, then the covering structure of C_Π is given as follows:

- i) if $m \geq 3$, all the nonzero codewords of C_Π are minimal;
- ii) if $m = 2$ and $q = 3$, the codewords of weights 4 and 5 are minimal, and the other codewords are not minimal;

- iii) if $m = 2$ and $q > 3$, the codewords of weights $q^2 - 2q + 1$, $q^2 - q - 1$, and $q^2 - q + 1$ are minimal, and the other codewords are not minimal.

Theorem 6 (Covering structure of $\tilde{C}_\Pi$): Let q be an odd prime power and let m be a positive integer greater than 1. If $\Pi(x)$ is a known explicit perfect nonlinear function from F_{q^m} to itself, then the covering structure of $\tilde{C}_\Pi$ is given as follows:

- i) if $m \geq 3$, all the nonzero codewords, except the codewords of weight q^m , are minimal, and the codewords of weight q^m are not minimal;
- ii) if $m = 2$ and $q = 3$, the codewords of weights 4 and 5 are minimal, and the other codewords are not minimal;
- iii) if $m = 2$ and $q > 3$, the codewords of weights $q^2 - 2q + 1$, $q^2 - q - 1$, and $q^2 - q + 1$ are minimal, and the other codewords are not minimal.

A. Some Auxiliary Results

The following three lemmas are very useful in determining the covering structures of C_Π and $\tilde{C}_\Pi$.

Lemma 6 [1]: Let C be an $[n, k, d; q]$ -code. Then, the weight of every minimal codeword must be less than or equal to $n - k + 1$, and every codeword whose weight is less than or equal to $\frac{qd-q+1}{q-1}$ must be a minimal codeword.

Lemma 7: Let C_Π be defined by (1) with $\Pi(x) = x^2$, $m = 2$, and $q > 3$. If $c_{a,b} \in C_\Pi$ is of weight $q^2 - q + 1$ and not a minimal codeword, then $a, b \neq 0$ and $\text{tr}(\frac{b^2}{a}) = 0$.

Proof: Since $m = 2$, from (4), all the nonzero weights of C_Π are

$$\{q^2 - 2q + 1, q^2 - q - 1, q^2 - q, q^2 - q + 1, q^2 - 1\}.$$

If $c_{a,b}$ is a codeword of weight $q^2 - q + 1$ in C_Π , then $a \neq 0$ from Corollary 3. According to (19) and (20) with $t = 0$, we obtain $b \neq 0$. Let

$$\begin{aligned} S &= \{x | x \in F_{q^2}^*, \text{tr}(ax^2 + bx) = 0\} \\ T &= \{x | x \in F_{q^2}^*, (ax^2 + bx)^{q-1} = -1\}. \end{aligned}$$

Clearly, $|S| = (q^2 - 1) - (q^2 - q + 1) = q - 2$.

Note that $\text{tr}(ax^2 + bx) = 0$ if and only if

$$ax^2 + bx = 0 \quad \text{or} \quad (ax^2 + bx)^{q-1} = -1.$$

Hence, $T \subseteq S$ and $|T| = |S| - 1 = q - 3 \geq 2$, as q is an odd prime power greater than 3.

If $c_{a,b}$ is not a minimal codeword of C_Π , then there exists a nonzero codeword $c_{a',b'} \in C_\Pi$ such that $c_{a,b}$ covers $c_{a',b'}$ and $(a', b') \neq k(a, b)$ for any $k \in F_q^*$. Clearly, $(a', b') \neq (0, 0)$. Let $t = a'b - ab'$, then $t \neq 0$. Otherwise, if $t = 0$, then $\frac{a'}{a} = \frac{b'}{b} = u \in F_{q^2}$. Since $c_{a,b}$ covers $c_{a',b'}$ and $|T| \geq 2$, there exists $y \in F_{q^2}^*$ such that

$$(ay^2 + by)^{q-1} = (a'y^2 + b'y)^{q-1} = -1.$$

Note that

$$\begin{aligned} -1 &= (a'y^2 + b'y)^{q-1} = (uay^2 + uby)^{q-1} \\ &= u^{q-1}(ay^2 + by)^{q-1} = -u^{q-1}. \end{aligned}$$

Therefore, $u^{q-1} = 1$. It follows that $u \in F_q^*$, which is a contradiction to $(a', b') \neq k(a, b)$ for any $k \in F_q^*$. Hence, $t \neq 0$.

For any $z \in T$, we have $-\frac{b}{a} - z \in T$, since

$$\begin{aligned} \left(a \left(-\frac{b}{a} - z \right)^2 + b \left(-\frac{b}{a} - z \right) \right)^{q-1} &= (az^2 + bz)^{q-1} \\ &= -1. \end{aligned}$$

Noting that $T \subseteq S$ and $c_{a,b}$ covers $c_{a',b'}$, we obtain

$$\text{tr}(a'z^2 + b'z) = \text{tr} \left(a' \left(-\frac{b}{a} - z \right)^2 + b' \left(-\frac{b}{a} - z \right) \right) = 0$$

which implies that

$$\text{tr} \left(\frac{2tz}{a} + \frac{bt}{a^2} \right) = 0. \quad (30)$$

It is easily verified that $-\frac{b}{a} \in S$, then we have

$$0 = \text{tr} \left(a' \left(-\frac{b}{a} \right)^2 + b' \left(-\frac{b}{a} \right) \right) = \text{tr} \left(\frac{bt}{a^2} \right). \quad (31)$$

From (30) and (31), we obtain that $\text{tr}(\frac{tz}{a}) = 0$ for every $z \in T$, which implies that $z^q = -(\frac{t}{a})^{1-q}z$. Substitute z^q by $-(\frac{t}{a})^{1-q}z$ in the following equation:

$$0 = \text{tr}(az^2 + bz) = az^2 + bz + a^q z^{2q} + b^q z^q$$

and then reformulate it as

$$\left(a + a^q \left(\frac{t}{a} \right)^{2-2q} \right) z^2 + \left(b - b^q \left(\frac{t}{a} \right)^{1-q} \right) z = 0.$$

Noting that $z \neq 0$, it follows that:

$$\left(a + a^q \left(\frac{t}{a} \right)^{2-2q} \right) z + \left(b - b^q \left(\frac{t}{a} \right)^{1-q} \right) = 0$$

for every $z \in T$. This shows that the linear equation

$$\left(a + a^q \left(\frac{t}{a} \right)^{2-2q} \right) x + \left(b - b^q \left(\frac{t}{a} \right)^{1-q} \right) = 0$$

has at least $|T| \geq 2$ solutions. Hence

$$a + a^q \left(\frac{t}{a} \right)^{2-2q} = b - b^q \left(\frac{t}{a} \right)^{1-q} = 0. \quad (32)$$

Since $c_{a,b}$ covers $c_{a',b'}$, we similarly obtain

$$a' + (a')^q \left(\frac{t}{a} \right)^{2-2q} = b' - (b')^q \left(\frac{t}{a} \right)^{1-q} = 0. \quad (33)$$

From (32) and (33), we obtain that $(a')^{q-1} = a^{q-1}$ if $a' \neq 0$ and $(b')^{q-1} = b^{q-1}$ if $b' \neq 0$. Now we can prove $\text{tr}(\frac{b^2}{a}) = 0$ by distinguishing the following three cases.

Case 1: If $a' = 0$, then $b' \neq 0$. Hence, $t = -ab'$ and $(b')^{q-1} = b^{q-1}$, which implies that there exists $k \in F_q^*$ such that $b' = kb$. Therefore, we obtain from (31) that

$$0 = \text{tr} \left(\frac{bt}{a^2} \right) = \text{tr} \left(-k \frac{b^2}{a} \right) = -k \text{tr} \left(\frac{b^2}{a} \right).$$

It follows that $\text{tr}(\frac{b^2}{a}) = 0$.

Case 2: If $b' = 0$, then $a' \neq 0$. Hence, $t = a'b$ and $(a')^{q-1} = a^{q-1}$, which implies that there exists $k \in F_q^*$ such that $a' = ka$. Therefore, we obtain from (31) that

$$0 = \text{tr} \left(\frac{bt}{a^2} \right) = \text{tr} \left(k \frac{b^2}{a} \right) = k \text{tr} \left(\frac{b^2}{a} \right).$$

It follows again that $\text{tr}(\frac{b^2}{a}) = 0$.

Case 3: If $a' \neq 0$ and $b' \neq 0$, then $(a')^{q-1} = a^{q-1}$ and $(b')^{q-1} = b^{q-1}$, which implies that there exist $k_1, k_2 \in F_q^*$ such that $a' = k_1 a$, $b' = k_2 b$, and $k_1 \neq k_2$. Therefore, we obtain from (31) that

$$\begin{aligned} 0 &= \text{tr} \left(\frac{bt}{a^2} \right) = \text{tr} \left((k_1 - k_2) \frac{b^2}{a} \right) \\ &= (k_1 - k_2) \text{tr} \left(\frac{b^2}{a} \right). \end{aligned}$$

It follows once again that $\text{tr}(\frac{b^2}{a}) = 0$. $\square$

Lemma 8: Let $\bar{C}_\Pi$ be defined by (2) with $\Pi(x) = x^2$, $m = 2$, and $q > 3$. Then, the codewords of weight $q^2 - q + 1$ cannot cover the nonzero codewords of the form $c_{0,u,v}$ in $\bar{C}_\Pi$.

Proof: Since $m = 2$, from (6), all the nonzero weights of $\bar{C}_\Pi$ are

$$\{q^2 - 2q + 1, q^2 - q - 1, q^2 - q, q^2 - q + 1, q^2 - 1, q^2\}.$$

Let $c_{a,b,c}$ be a codeword of weight $q^2 - q + 1$ in $\bar{C}_\Pi$. Then, $a \neq 0$ from Corollary 4. Note that the following equation holds when $a \neq 0$:

$$ax^2 + bx + c = a \left(x + \frac{b}{2a} \right)^2 + \frac{4ac - b^2}{4a}.$$

If $\text{tr}(\frac{4ac - b^2}{4a}) = 0$, then $\text{tr}(ax^2 + bx + c) = \text{tr}(az^2)$, where $z = x + \frac{b}{2a}$. Hence, from (19) and (20), we obtain $w_H(c_{a,b,c}) = q^2 - 2q + 1$ or $q^2 - q$, which is a contradiction. Therefore

$$\text{tr} \left(\frac{4ac - b^2}{4a} \right) \neq 0. \quad (34)$$

Let $S = \{x | x \in F_{q^2}, \text{tr}(ax^2 + bx + c) = 0\}$. Then, $|S| = q^2 - (q^2 - q + 1) = q - 1$ and $-\frac{b}{2a} \notin S$.

It is easily seen that $c_{a,b,c}$ cannot cover any nonzero codeword of the form $c_{0,0,v}$ in $\bar{C}_\Pi$. Now we prove that $c_{a,b,c}$ cannot cover any nonzero codeword of the form $c_{0,u,v}$, where $u \in F_{q^2}^*$. Supposing the contrary that $c_{a,b,c}$ covers some $c_{0,u,v}$, where $u \in F_{q^2}^*$ and $v \in \Omega$, we let

$$S_{u,v} = \{x | x \in F_{q^2}, \text{tr}(ux + v) = 0\}$$

and for every $y \in S$, let

$$T_y = \{z | z \in F_{q^2}^*, y + z \in S\}.$$

Since $c_{a,b,c}$ covers $c_{0,u,v}$, we have $S \subseteq S_{u,v}$, and $|T_y| = q-2 \geq 3$, since q is an odd prime power greater than 3.

For any $y \in S$ and any $z \in T_y$, we have $y, y+z \in S_{u,v}$ since $S \subseteq S_{u,v}$. Hence

$$\text{tr}(uz) = 0 \quad (35)$$

which implies that

$$(uz)^{q-1} = -1 \quad (36)$$

since $u, z \in F_{q^2}^*$. It follows that

$$z^q = -u^{1-q}z. \quad (37)$$

On the other hand, since $y, y+z \in S$, we have

$$\text{tr}(ay^2 + by + c) = \text{tr}(a(y+z)^2 + b(y+z) + c) = 0.$$

This implies that $\text{tr}(z(az + 2ay + b)) = 0$, which is equivalent to

$$az + 2ay + b = 0 \quad \text{or} \quad (z(az + 2ay + b))^{q-1} = -1. \quad (38)$$

Note that for any $y \in S$, there is at most one $z \in T_y$ such that $az + 2ay + b = 0$. Therefore, combining (36) and (38), there are at least $|T_y| - 1 = q - 3 \geq 2$ elements z of T_y such that

$$(z(az + 2ay + b))^{q-1} = (uz)^{q-1}.$$

It follows that $(\frac{az+2ay+b}{u})^{q-1} = 1$, which is equivalent to

$$\frac{a^q z^q + (2ay + b)^q}{u^q} = \frac{az + 2ay + b}{u}. \quad (39)$$

Substituting (37) into (39), we obtain

$$(au^{q-1} + a^q u^{1-q})z + u^{q-1}(2ay + b) - (2ay + b)^q = 0. \quad (40)$$

If $au^{q-1} + a^q u^{1-q} \neq 0$, then the following linear equation:

$$(au^{q-1} + a^q u^{1-q})x + u^{q-1}(2ay + b) - (2ay + b)^q = 0$$

has at least $|T_y| - 1 = q - 3 \geq 2$ solutions, which is a contradiction. Therefore

$$au^{q-1} + a^q u^{1-q} = 0 \quad \text{and} \quad u^{q-1}(2ay + b) - (2ay + b)^q = 0.$$

It follows that $(\frac{2ay+b}{u})^{q-1} = 1$ since $-\frac{b}{2a} \notin S$ implies $2ay + b \neq 0$. Hence, $\frac{2ay+b}{u} \in F_q^*$. Since $|S| = q - 1$, we obtain

$$S = \left\{ y | y = \frac{ku - b}{2a}, k \in F_q^* \right\}.$$

Taking $y = \frac{u-b}{2a} \in S$, then $z = \frac{u}{2a} \in T_y$ since $y + z = \frac{2u-b}{2a} \in S$.

It follows from (35) that

$$\text{tr}\left(\frac{u^2}{a}\right) = \text{tr}\left(2u\left(\frac{u}{2a}\right)\right) = 2\text{tr}(uz) = 0. \quad (41)$$

Noting that $y = \frac{u-b}{2a} \in S$, we have

$$\begin{aligned} 0 &= \text{tr}(ay^2 + by + c) \\ &= \text{tr}\left(a\left(y + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a}\right) \\ &= \text{tr}\left(\frac{u^2}{4a}\right) + \text{tr}\left(\frac{4ac - b^2}{4a}\right). \end{aligned} \quad (42)$$

From (41) and (42), we obtain that $\text{tr}(\frac{4ac-b^2}{4a}) = 0$, which is contrary to (34). Therefore, $c_{a,b,c}$ cannot cover any codeword of the form $c_{0,u,v}$, where $u \in F_{q^2}^*$. $\square$

B. Determining the Covering Structure of C_Π

Using Lemmas 6 and 7, we can now prove Theorem 5.

i) When m is odd, C_Π is a $[q^m - 1, 2m, (q-1)q^{m-1} - q^{\frac{m-1}{2}}; q]$ -code from Corollary 1. In this subcase

$$\frac{qd - q + 1}{q - 1} = \frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

It is easily verified that the following inequality is true for odd $m \geq 3$:

$$(q-1)q^{m-1} + q^{\frac{m-1}{2}} \leq \frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

It follows from Theorem 1 that each of the nonzero weights in C_Π in the case of m odd is less than or equal to

$$\frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

Hence, from Lemma 6, i) is true for odd $m \geq 3$.

When m is even, C_Π is a $[q^m - 1, 2m, (q-1)(q^{m-1} - q^{\frac{m-2}{2}}); q]$ -code from Corollary 2. In this subcase

$$\frac{qd - q + 1}{q - 1} = q^m - q^{\frac{m}{2}} - 1.$$

It is easily verified that the following inequality is true for even $m > 3$:

$$(q-1)\left(q^{m-1} + q^{\frac{m-2}{2}}\right) \leq q^m - q^{\frac{m}{2}} - 1.$$

It follows from Theorem 1 that each of the nonzero weights in C_Π in the case of m even is less than or equal to $q^m - q^{\frac{m}{2}} - 1$. Hence, from Lemma 6, i) is also true for even $m > 3$.

ii) If $m = 2$ and $q = 3$, C_Π is an $[8, 4, 4; 3]$ -code from Corollary 2, and all the nonzero weights of C_Π are 4, 5, 6, 7, 8 from (4). In this subcase

$$\begin{aligned} n - k + 1 &= 8 - 4 + 1 \\ &= 5, \frac{qd - q + 1}{q - 1} = \frac{3 \times 4 - 3 + 1}{2} = 5. \end{aligned}$$

From Lemma 6, the codewords of weights 4 and 5 are minimal, while the codewords of weights 6, 7, and 8 are not minimal.

- iii) If $m = 2$ and $q > 3$, C_{Π} is a $[q^2 - 1, 4, q^2 - 2q + 1; q]$ -code from Corollary 2, and all the nonzero weights of C_{Π} are given from (4) as follows:

$$\{q^2 - 2q + 1, q^2 - q - 1, q^2 - q, q^2 - q + 1, q^2 - 1\}.$$

In this subcase

$$\begin{aligned} n - k + 1 &= q^2 - 1 - 4 + 1 = q^2 - 4 \\ \frac{qd - q + 1}{q - 1} &= \frac{q(q^2 - 2q + 1) - q + 1}{q - 1} = q^2 - q - 1. \end{aligned}$$

From Lemma 6, the codewords of weights $q^2 - 2q + 1$ and $q^2 - q - 1$ are minimal, while the codewords of weights $q^2 - 1$ are not minimal.

In the following, we discuss the minimality of the codewords of weights $q^2 - q$ and $q^2 - q + 1$ in C_{Π} . Since $m = 2$ and $q > 3$, the only known explicit perfect nonlinear function is $\Pi(x) = x^2$.

First, the codewords of weight $q^2 - q$ in C_{Π} are not minimal. Indeed, let $c_{a,b}$ be a codeword of weight $q^2 - q$ in C_{Π} . Then, $a = 0$ and $b \neq 0$ from Corollary 3. Set $a' = \alpha^{\frac{q+1}{2}} b^2$, where α is a primitive element of F_{q^2} . Clearly, $a' \neq 0$. For every $x \in F_{q^2}^*$, if $\text{tr}(bx) = 0$, then $bx + (bx)^q = 0$, which implies $(bx)^{q-1} = -1$ since $b, x \in F_{q^2}^*$. Hence

$$\begin{aligned} \text{tr}(a'x^2 + bx) &= a'x^2 + (a'x^2)^q \\ &= (a'x^2)(1 + (a'x^2)^{q-1}) \\ &= (a'x^2) \left(1 + \alpha^{\frac{q^2-1}{2}} (bx)^{2(q-1)} \right) \\ &= (a'x^2)(1 - 1) = 0. \end{aligned}$$

This demonstrates that $c_{0,b}$ covers $c_{a',b}$, and $c_{0,b}$ is not a multiple of $c_{a',b}$ since $a' \neq 0$. Therefore, the codewords of weight $q^2 - q$ are not minimal.

Finally, the codewords of weight $q^2 - q + 1$ in C_{Π} are minimal. Indeed, if $c_{a,b}$ is of weight $q^2 - q + 1$ and not a minimal codeword of C_{Π} , then $a, b \neq 0$ and $\text{tr}(\frac{b^2}{a}) = 0$ from Lemma 7. This implies $a^{q-1} = -b^{2(q-1)}$. Hence, for any $x \in F_{q^2}^*$, if $\text{tr}(bx) = 0$, we have $(bx)^{q-1} = -1$ since $b, x \in F_{q^2}^*$. Therefore

$$\begin{aligned} \text{tr}(ax^2 + bx) &= \text{tr}(ax^2) = ax^2(1 + (ax^2)^{q-1}) \\ &= ax^2(1 - (bx)^{2(q-1)}) = ax^2(1 - 1) = 0. \end{aligned}$$

This shows that the codeword $c_{0,b}$ covers the codeword $c_{a,b}$. It follows that the weight of $c_{a,b}$ is less than or equal to that of $c_{0,b}$. However, from Corollary 3, the weight of $c_{0,b}$ is $q^2 - q$. Hence, $q^2 - q + 1 \leq q^2 - q$, which is false. Therefore, $c_{a,b}$ must be a minimal codeword. $\square$

C. Determining the Covering Structure of $\bar{C}_{\Pi}$

Using Lemmas 6 and 8, we can now prove Theorem 6.

- i) When m is odd, $\bar{C}_{\Pi}$ is a $[q^m, 2m + 1, (q - 1)q^{m-1} - q^{\frac{m-1}{2}}; q]$ -code from Corollary 1. In this subcase

$$n - k + 1 = q^m - (2m + 1) + 1 = q^m - 2m$$

$$\frac{qd - q + 1}{q - 1} = \frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

As in the proof of Theorem 5i)

$$(q - 1)q^{m-1} + q^{\frac{m-1}{2}} \leq \frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

It follows from Theorem 2 that each of the nonzero weights, except q^m , in $\bar{C}_{\Pi}$ in the case of m odd is less than or equal to

$$\frac{q^{m+1} - q^m - q^{\frac{m+1}{2}} - q + 1}{q - 1}.$$

Note that $q^m > q^m - 2m$, from Lemma 6, i) is true for odd $m \geq 3$.

When m is even, $\bar{C}_{\Pi}$ is a $[q^m, 2m + 1, (q - 1)(q^{m-1} - q^{\frac{m-2}{2}}); q]$ -code from Corollary 2. In this subcase

$$\begin{aligned} n - k + 1 &= q^m - (2m + 1) + 1 = q^m - 2m \\ \frac{qd - q + 1}{q - 1} &= q^m - q^{\frac{m}{2}} - 1. \end{aligned}$$

As in the proof of Theorem 5i)

$$(q - 1) \left(q^{m-1} + q^{\frac{m-2}{2}} \right) \leq q^m - q^{\frac{m}{2}} - 1.$$

It follows from Theorem 2 that each of the nonzero weights, except q^m , in $\bar{C}_{\Pi}$ in the case of m even is less than or equal to $q^m - q^{\frac{m}{2}} - 1$. Note that $q^m > q^m - 2m$, from Lemma 6, i) is also true for even $m \geq 3$.

- ii) If $m = 2$ and $q = 3$, $\bar{C}_{\Pi}$ is a $[9, 5, 4; 3]$ -code from Corollary 2, and all the nonzero weights of $\bar{C}_{\Pi}$ are 4, 5, 6, 7, 8, and 9 from (6). In this subcase

$$\begin{aligned} n - k + 1 &= 9 - 5 + 1 = 5 \\ \frac{qd - q + 1}{q - 1} &= \frac{3 \times 4 - 3 + 1}{2} = 5. \end{aligned}$$

From Lemma 6, the codewords of weights 4 and 5 are minimal, while the codewords of weights 6, 7, 8, and 9 are not minimal.

- iii) If $m = 2$ and $q > 3$, $\bar{C}_{\Pi}$ is a $[q^2, 5, q^2 - 2q + 1; q]$ -code from Corollary 2, and all the nonzero weights of $\bar{C}_{\Pi}$ are given from (6) as follows:

$$\{q^2 - 2q + 1, q^2 - q - 1, q^2 - q, q^2 - q + 1, q^2 - 1, q^2\}.$$

In this subcase

$$\begin{aligned} n - k + 1 &= q^2 - 5 + 1 = q^2 - 4 \\ \frac{qd - q + 1}{q - 1} &= \frac{q(q^2 - 2q + 1) - q + 1}{q - 1} \\ &= q^2 - q - 1. \end{aligned}$$

From Lemma 6, the codewords of weights $q^2 - 2q + 1$ and $q^2 - q - 1$ are minimal, while the codewords of weights q^2 and $q^2 - 1$ are not minimal.

In the following, we consider the minimality of the codewords of weights $q^2 - q$ and $q^2 - q + 1$ in $\bar{C}_\Pi$. As in the proof of Theorem 5iii), we only need to consider the case $\Pi(x) = x^2$.

First, the codewords of weight $q^2 - q$ in $\bar{C}_\Pi$ are not minimal. Indeed, if $c_{a,b,c}$ is a codeword of weight $q^2 - q$ in $\bar{C}_\Pi$, then $a = 0$ and $b \neq 0$ from Corollary 4. Set $a' = \alpha^{\frac{q+1}{2}}$, where α is a primitive element of F_{q^2} . Clearly, $a' \neq 0$. For every $x \in F_{q^2}$, if $\text{tr}(bx + c) = 0$, then

$$(bx + c)^2 = (bx + c)^{2q}.$$

Hence

$$\text{tr}(a'(bx + c)^2) = 0$$

since $a'^q = -a'$.

It follows that $c_{0,b,c}$ covers $c_{a'b^2, 2a'bc, a'^2c^2}$. Note that $c_{0,b,c}$ is not a multiple of $c_{a'b^2, 2a'bc, a'^2c^2}$ since $a'b^2 \neq 0$; the codewords of weight $q^2 - q$ are, therefore, not minimal.

Finally, the codewords of weight $q^2 - q + 1$ in $\bar{C}_\Pi$ are minimal. Indeed, if $c_{a,b,c}$ is a codeword of weight $q^2 - q + 1$ in $\bar{C}_\Pi$, we let

$$S = \{x | x \in F_{q^2}, \text{tr}(ax^2 + bx + c) = 0\}.$$

Recall that $|S| = q - 1 > 2$, since q is an odd prime power greater than 3.

If $c_{a,b,c}$ is not a minimal codeword of $\bar{C}_\Pi$, then there exists $c_{a',b',c'} \in \bar{C}_\Pi$ such that $c_{a,b,c}$ covers $c_{a',b',c'}$ and $c_{a',b',c'} \neq kc_{a,b,c}$, where $k \in F_q^*$. Hence, $a, a' \neq 0$ from Corollary 4 and Lemma 8. Set $t = ab - ab'$, then $t = 0$. Otherwise, for any $y \in S$

$$\text{tr}(a(-\frac{b}{a} - y)^2 + b(-\frac{b}{a} - y) + c) = \text{tr}(ay^2 + by + c) = 0$$

which implies that $-\frac{b}{a} - y \in S$. Note that $c_{a,b,c}$ covers $c_{a',b',c'}$, and we have

$$\begin{aligned} & \text{tr}(a'y^2 + b'y + c') \\ &= \text{tr}(a'(-\frac{b}{a} - y)^2 + b'(-\frac{b}{a} - y) + c') \\ &= 0. \end{aligned} \quad (43)$$

It follows that $\text{tr}(\frac{2t}{a}y + \frac{bt}{a^2}) = 0$ for every $y \in S$. Hence, $c_{a,b,c}$ covers $c_{0, \frac{2t}{a}, \frac{bt}{a^2}}$ and $\frac{2t}{a} \neq 0$, which is contrary to Lemma 8.

Therefore, $t = ab - ab' = 0$. Let $\frac{a'}{a} = w$, then $w \in F_{q^2}^*$ since $a, a' \neq 0$ and $b' = wb$ since $t = 0$. We now proceed to prove $w \in F_q^*$. Since $c_{a,b,c}$ covers $c_{a',b',c'}$ and $y \in S$, the following equalities follow:

$$\begin{aligned} 0 &= \text{tr}(ay^2 + by + c) \\ &= (ay^2 + by + c)^q + (ay^2 + by + c) \end{aligned} \quad (44)$$

and

$$\begin{aligned} 0 &= \text{tr}(a'y^2 + b'y + c') \\ &= \text{tr}(w(ay^2 + by + c) + (c' - wc)) \\ &= \text{tr}(w(ay^2 + by + c)) + \text{tr}(c' - wc) \\ &= w^q(ay^2 + by + c)^q \\ &\quad + w(ay^2 + by + c) + \text{tr}(c' - wc). \end{aligned} \quad (45)$$

From (44) and (45), we obtain that $(w - w^q)(ay^2 + by + c) + \text{tr}(c' - wc) = 0$ for every $y \in S$. It follows that the quadratic

equation $(w - w^q)(ax^2 + bx + c) + \text{tr}(c' - wc) = 0$ has at least $|S| = q - 1 > 2$ solutions $y \in S$. Then, we must have $w - w^q = 0$ and $\text{tr}(c' - wc) = 0$. This means $w \in F_q^*$ and $c_{a',b',c'} = wc_{a,b,c}$, which is a contradiction. Therefore, $c_{a,b,c}$ must be a minimal codeword in the linear code $\bar{C}_\Pi$. $\square$

IV. ACCESS STRUCTURES OF THE SECRET SHARING SCHEMES BASED ON TWO CLASSES OF LINEAR CODES

There are several ways to construct secret sharing schemes by using linear codes. One of them is the following scheme proposed by Massey [16], [17].

In the secret sharing scheme based on C , where C is an $[n, k, d; q]$ -code, the secret s is an element of F_q , which is called the secret space. There are a dealer P_0 and $n - 1$ parties $P_1, P_2, \dots, P_{n-1}$ in the secret sharing scheme. Let $G = (g_0, g_1, \dots, g_{n-1})$ be a generator matrix of C such that $g_i \neq 0$ for $0 \leq i \leq n - 1$. Then, the secret sharing scheme can be described as follows.

Step 1) The dealer P_0 chooses randomly a vector $\underline{u} = (u_0, u_1, \dots, u_{k-1}) \in F_q^k$ such that $s = \underline{u}g_0$.

Step 2) The dealer P_0 treats $\underline{u}$ as an information vector and computes the corresponding codeword $\underline{t} = \underline{u}G = (t_0, t_1, \dots, t_{n-1})$, then he sends t_i to party P_i as the share for every $i (1 \leq i \leq n - 1)$.

Step 3) The secret s is recovered as follows: the set of shares $\{t_{i_1}, t_{i_2}, \dots, t_{i_m}\}$ can determine the secret s if and only if g_0 is a linear combination of $\{g_{i_1}, g_{i_2}, \dots, g_{i_m}\}$, where $1 \leq i_1 < i_2 < \dots < i_m \leq n - 1$.

Clearly, if a group of participants can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret. The set $\{i_1, i_2, \dots, i_m\}$ is said to be a minimal access set if it can recover the secret s but none of its proper subsets can do so. The access structure of the secret sharing scheme refers to the set of all minimal access sets.

The following lemma from [16] presents the relationship between the minimal access sets of the secret sharing scheme based on C and the minimal codewords of the dual code $C^\perp$.

Lemma 9 [16]: Let C be an $[n, k, d; q]$ -code. Then, the set $\{i_1, i_2, \dots, i_m\} \subseteq \{1, 2, \dots, n - 1\}$ such that $i_1 < i_2 < \dots < i_m$ is a minimal access set in the secret sharing scheme based on C if and only if there exists a minimal codeword $\underline{c} = (c_0, c_1, \dots, c_{n-1}) \in C^\perp$ such that $\text{Supp}(\underline{c}) = \{0, i_1, i_2, \dots, i_m\}$ and $c_0 = 1$.

If $\underline{c}$ is a nonzero codeword, whose first coordinate is 1, in a linear code, and the support of the codeword $\underline{c}$ is $\text{Supp}(\underline{c}) = \{0, i_1, i_2, \dots, i_m\}$ such that $1 \leq i_1 < i_2 < \dots < i_m \leq n - 1$, we call the set $\{i_1, i_2, \dots, i_m\}$ the access support of the codeword $\underline{c}$.

In the following, we consider the secret sharing schemes based on $C_\Pi^\perp$ and $\bar{C}_\Pi^\perp$. From Lemma 9 and Theorems 5 and 6, we readily obtain the following.

Theorem 7: Let q be an odd prime power and let m be a positive integer greater than 1. If $\Pi(x)$ is a known explicit perfect

nonlinear function from F_{q^m} to itself, then the access structure of the secret sharing scheme based on $C_{\Pi}^{\perp}$ is given as follows:

- i) if $m \geq 3$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in C_{Π} with first coordinate 1;
- ii) if $m = 2$ and $q = 3$, the set of minimal access sets is equal to the set of access supports of the codewords in C_{Π} with first coordinate 1 and of weights 4 and 5;
- iii) if $m = 2$ and $q > 3$, the set of minimal access sets is equal to the set of access supports of the codewords in C_{Π} with first coordinate 1 and of weights $q^2 - 2q + 1, q^2 - q - 1$ and $q^2 - q + 1$.

Theorem 8: Let q be an odd prime power and let m be a positive integer greater than 1. If $\Pi(x)$ is a known explicit perfect nonlinear function from F_{q^m} to itself, then the access structure of the secret sharing scheme based on $\bar{C}_{\Pi}^{\perp}$ is given as follows:

- i) if $m \geq 3$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $\bar{C}_{\Pi}$ with first coordinate 1 except for the codeword $(1, 1, \dots, 1)$;
- ii) if $m = 2$ and $q = 3$, the set of minimal access sets is equal to the set of access supports of the codewords in $\bar{C}_{\Pi}$ with first coordinate 1 and of weights 4 and 5;
- iii) if $m = 2$ and $q > 3$, the set of minimal access sets is equal to the set of access supports of the codewords in $\bar{C}_{\Pi}$ with first coordinate 1 and of weights $q^2 - 2q + 1, q^2 - q - 1$ and $q^2 - q + 1$.

Theorems 7 and 8 answer Problem 2 in Section I, thus suggesting that open problems 4, 5, and 6 in [6] and open problem 2 in [22] are solved.

Example 1: Let C_{Π} be the $[8, 4, 4; 3]$ -code from the perfect nonlinear function $\Pi(x) = x^{\frac{3k+1}{2}}$ where $(q, m, k) = (3, 2, 1)$. Then, from Theorem 1ii), the weight enumerator of C_{Π} is

$$1 + 20x^4 + 32x^5 + 8x^6 + 16x^7 + 4x^8.$$

According to Theorem 5ii), there are $20 + 32 = 52$ minimal codewords in C_{Π} . Of these minimal codewords, the following codewords are of first coordinate 1:

$$\begin{aligned} &[1, 1, 0, 0, 2, 0, 0, 2], [1, 0, 2, 0, 1, 0, 2, 0], [1, 2, 2, 0, 0, 1, 0, 0], \\ &[1, 0, 0, 1, 2, 2, 0, 0], [1, 0, 0, 2, 0, 0, 2, 1], [1, 0, 0, 0, 1, 1, 1, 2], \\ &[1, 2, 0, 0, 0, 2, 2, 2], [1, 0, 1, 0, 1, 2, 0, 1], [1, 2, 1, 0, 0, 0, 1, 1], \\ &[1, 1, 0, 1, 0, 1, 2, 0], [1, 2, 0, 1, 1, 0, 1, 0], [1, 1, 2, 1, 0, 0, 0, 1], \\ &[1, 0, 1, 2, 0, 1, 1, 0], [1, 1, 1, 2, 1, 0, 0, 0], [1, 0, 2, 2, 0, 2, 0, 2]. \end{aligned}$$

Therefore, from Theorem 7ii), all the minimal access sets in the secret sharing scheme based on $C_{\Pi}^{\perp}$ are

$$\begin{aligned} &\{1, 4, 7\}, \{2, 4, 6\}, \{1, 2, 5\}, \{3, 4, 5\}, \{3, 6, 7\}, \{4, 5, 6, 7\}, \\ &\{1, 5, 6, 7\}, \{2, 4, 5, 7\}, \{1, 2, 6, 7\}, \{1, 3, 5, 6\}, \{1, 3, 4, 6\}, \\ &\{1, 2, 3, 7\}, \{2, 3, 5, 6\}, \{1, 2, 3, 4\}, \{2, 3, 5, 7\}. \end{aligned}$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees and the Associate Editor for invaluable suggestions that have helped to improve the organization of this paper and the exposition.

REFERENCES

- [1] A. Ashikhmin, A. Barg, G. Cohen, and L. Huguët, "Variations on minimal codewords in linear codes," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1995, vol. 948, pp. 96–105.
- [2] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 2010–2017, Sep. 1998.
- [3] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 65–76.
- [4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Comput. Conf.*, New York, 1979, pp. 313–317.
- [5] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2, pp. 205–244, 2004.
- [6] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, Jun. 2005.
- [7] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes Cryptogr.*, vol. 10, pp. 167–184, 1997.
- [8] P. Dembowski and T. G. Ostrom, "Planes of order n^2 ," *Math. Z.*, vol. 193, pp. 239–258, 1968.
- [9] C. Ding, D. Kohel, and S. Ling, "Secret sharing with a class of ternary codes," *Theo. Comput. Sci.*, vol. 246, pp. 285–298, 2000.
- [10] C. Ding and J. Yuan, "A family of skew Hadamard difference sets," *J. Comb. Theory*, ser. A, vol. 113, pp. 1526–1535, 2006.
- [11] K. Feng and J. Luo, "Value distributions of exponential sums from perfect nonlinear functions and their applications," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3035–3041, Sep. 2007.
- [12] W. Kantor, "Finite semifields, in: Finite geometries, groups and computation," in *Proc. Conf. at Pingree Park*, Berlin, Germany, 2006, pp. 103–114.
- [13] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
- [14] C. Li, Q. Li, and S. Ling, "Properties and applications of preimage distributions of perfect nonlinear functions," *IEEE Trans. Inf. Theory*, accepted for publication.
- [15] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.
- [16] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Workshop Inf. Theory*, Molle, Sweden, 1993, pp. 276–279.
- [17] J. L. Massey, "Some applications of coding theory," *Cryptography, codes and Ciphers: Cryptography and Coding IV*, pp. 33–47, 1995.
- [18] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Commun. ACM*, vol. 24, pp. 583–584, 1981.
- [19] G. J. Ness, T. Helleseht, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2241–2247, May 2006.
- [20] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.
- [21] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 712–717, Feb. 2006.
- [22] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, Jan. 2006.

Chao Li received the B.A. degree in mathematics from the University of Information Engineering of China, Zhengzhou, China, in 1987, the M.S. degree in mathematics from the University of Science and Technology of China, Hefei, China, in 1990, and the Ph.D. degree in engineering from the National University of Defense Technology of China, Changsha, China, in 2002.

Since December 2001, he has been a Professor with the Department of Mathematics and System Science, National University of Defense Technology, Changsha, China. His research fields include coding theory, cryptography, and sequences.

San Ling received the B.A. and M.A. degrees in mathematics from the University of Cambridge, Cambridge, U.K., in 1985 and 1989, respectively, and the Ph.D. degree in mathematics from the University of California, Berkeley, in 1990.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography, and sequences.

Longjiang Qu received the B.A. and Ph.D. degrees in mathematics from the National University of Defense Technology, Changsha, China, in 2002 and 2007, respectively.

He is now a Lecturer with the Department of Mathematics and System Science, National University of Defense Technology of China. His research fields include cryptography and coding theory.