<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On the covering structures of two classes of linear codes from perfect nonlinear functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Li, Chao; Ling, San; Qu, Longjiang</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Li, C., Ling, S., &amp; 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.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2009</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/9845">http://hdl.handle.net/10220/9845</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 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: [<a href="http://dx.doi.org/10.1109/TIT.2008.2008145">http://dx.doi.org/10.1109/TIT.2008.2008145</a>].</td>
</tr>
</tbody>
</table>
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 $F_{q^n}$ 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 $F_{q^n}$ be a finite field of order $q^n$, where $q$ is an odd prime power and $n$ is a positive integer. A function $f : F_{q^n} \to F_{q^n}$ is called perfect nonlinear if $f(x + a) = f(x)$ is a permutation from $F_{q^n}$ to itself for every $a \in F_{q^n}$.

Up to now, all known explicit perfect nonlinear functions from $F_{q^n}$ 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) $\Pi_2(x) = x^{\frac{q^t + 1}{2}}$, where $q = 3$, $k$ is odd, and $gcd(m, k) = 1$ [7];

3) $\Pi_3(x) = x^{q^t - u x^{q^t} - u^2 x^{q^t}}$, where $q = 3$, $m$ is odd, and $u \in F_{q^n}^*$ [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, $\Pi_1(x) = x^{q^t + 1}$, $\Pi_2(x) = x^{\frac{q^t + 1}{2}}$, and $\Pi_3(x) = x^{q^t - u x^{q^t} - u^2 x^{q^t}}$ are said to be the first, second, and third perfect nonlinear functions, respectively, and all the known explicit perfect nonlinear functions from $F_{q^n}$ 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 $F_{q^n}$ to itself as follows [6].

Definition 2: Let $F_{q^n} = \{\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{q^n - 1}\}$ and $\gamma_0 = 0$, let $\Pi(x)$ be a perfect nonlinear function from $F_{q^n}$ to itself, and let $f_{a,b}(x) = tr(a \Pi(x) + bx)$ and $f_{a,b,c}(x) = tr(a \Pi(x) + bx + c)$ be two functions from $F_{q^n}$ to $F_{q^n}$, where $a, b, c \in F_{q^n}$ and $tr(\cdot)$ denotes the trace function from $F_{q^n}$ to $F_q$, i.e., $tr(x) = x + x^2 + x^3 + \cdots + x^{q^n - 1}$ for all $x \in F_{q^n}$. Let $C_{\Pi}$ and $C_{\Pi}$ be (linear) codes over $F_q$ defined as follows:

$C_{\Pi} = \{\langle f_{a,b}(\gamma_1), f_{a,b}(\gamma_2), \ldots, f_{a,b}(\gamma_{q^n - 1}) \rangle | a, b \in F_{q^n} \}$

and

$C_{\Pi} = \{\langle f_{a,b,c}(\gamma_0), f_{a,b,c}(\gamma_1), \ldots, f_{a,b,c}(\gamma_{q^n - 1}) \rangle | a, b, c \in F_{q^n} \}$.  

(1)

(2)

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

**Problem 1:** Determine the weight distributions of $C_{II}$ and $\tilde{C}_{II}$ 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 $C_{II}$ and $\tilde{C}_{II}$ for all known explicit perfect nonlinear functions $\Pi(x)$ from $F_{q^m}$ to itself, where $C_{II}$ and $\tilde{C}_{II}$ are the dual codes of $C_{II}$ and $\tilde{C}_{II}$, 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 $2q \geq q^2 + 1$ 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 $C_{II}$ 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 $C_{II}$, 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 $C_{II}$ 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 $\tilde{C}_{II}$.

In this paper, using a unified approach, we first determine the weight distributions of $C_{II}$ and $\tilde{C}_{II}$ 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 $\tilde{C}_{II}$, which was not known before;

2) a new unified approach to the determination of the weight distribution of $\tilde{C}_{II}$.

As for Problem 2, the paper [6] partly answered Problem 2. The authors determined the access structures of the secret sharing schemes based on $C_{II}$ 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 $\tilde{C}_{II}$ with $m \geq 2$ and $C_{II}$ 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 $C_{II}$ and $\tilde{C}_{II}$. Using the properties of the weights of codewords in $C_{II}$ and $\tilde{C}_{II}$, we characterize all the minimal codewords in these codes for all known explicit perfect 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 $C_{II}$ and $\tilde{C}_{II}$ 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 $C_{II}$ and $\tilde{C}_{II}$. In Section IV, all the minimal access sets of the secret sharing schemes based on $C_{II}$ and $\tilde{C}_{II}$ 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 $\{A_q, A_1, \ldots, A_n\}$, where $A_q$ denotes the number of codewords of weight $q$. The determination of the weight distribution of a code is often a hard problem.

The paper [6] pointed out that $C_{II}$ is a $[q^{m-1} + 2m; q]$-code and $\tilde{C}_{II}$ is a $[q^{m-1} + 2m + 1; q]$-code, and demonstrated that many codes $C_{II}$ and $\tilde{C}_{II}$ 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 $C_{II}$ is given as follows: all $A_i = 0$ except that

\[
\begin{align*}
A_0 &= 1 \\
A_{(q-1)q^{m-1} - q^{m-2}} &= \frac{1}{2}(q-1)(q^m - 1)
\left(q^{m-1} + q^{m-2}\right)
\end{align*}
\]

ii) if $m$ is even, the weight distribution of $C_{II}$ is given as follows: all $A_i = 0$ except that

\[
\begin{align*}
A_0 &= 1 \\
A_{(q-1)q^{m-1} - q^{m-2}} &= \frac{1}{2}(q-1)(q^m - 1)
\left(q^{m-1} + q^{m-2}\right)
\end{align*}
\]

**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 \( C_{II} \) is given as follows: all \( A_i = 0 \) except that
\[
\begin{align*}
A_0 &= 1 \\
A_{(q-1)q^m - 1 - q^{m-1}} &= \frac{1}{2}(q - 1)(q^{2m} - q^m) \\
A_{(q-1)q^m - 1} &= \frac{1}{2}(q - 1)(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 - q^{m-1}} &= \frac{1}{2}(q - 1)(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 + q^{m-1}} &= q - 1.
\end{align*}
\]

ii) If \( m \) is even, the weight distribution of \( C_{II} \) is given as follows: all \( A_i = 0 \) except that
\[
\begin{align*}
A_0 &= 1 \\
A_{(q-1)q^m - 1 - q^{m-2}} &= \frac{1}{2}(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 - q^{m-2}} &= \frac{1}{2}(q - 1)(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 - q^{m-2}} &= \frac{1}{2}(q - 1)(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 - q^{m-2}} &= \frac{1}{2}(q^{2m} - q^m) \\
A_{(q-1)q^m - 1 - q^{m-2}} &= q - 1.
\end{align*}
\]

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 \( C_{II} \) is a \([q^m - 1, 2m, (q - 1)(q^{m-1} - q^{m-2}) + q]\)-code and \( C_{II} \) is a \([q^m, 2m + 1, (q - 1)(q^{m-1} - q^{m-2})] + q\)-code.

**Corollary 2:** If \( m \) is an even positive integer, then \( C_{II} \) is a \([q^m - 1, 2m, (q - 1)(q^{m-1} - q^{m-2}) + q]\)-code and \( C_{II} \) is a \([q^m, 2m + 1, (q - 1)(q^{m-1} - q^{m-2}) + q]\)-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 homogeneous polynomial of degree 2, or the zero polynomial in \( F_q[x_1, x_2, \ldots, x_n] \), where \( q \) is a prime power. When \( q \) is an odd prime power, every quadratic form \( f(x_1, x_2, \ldots, x_n) \) can be represented in the following form:

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

We associate with \( f(x_1, x_2, \ldots, x_n) \) the \( n \times n \) symmetric matrix \( A \) whose \((i,j)\) entry is \( a_{ij} \), which is called the matrix of \( f(x_1, x_2, \ldots, x_n) \). The determinant and rank of matrix \( A \) are called the determinant and rank of the quadratic form \( f(x_1, x_2, \ldots, x_n) \), and they are denoted by \( \det(f) \) and \( \text{rank}(f) \), respectively. If a quadratic form \( f(x_1, x_2, \ldots, x_n) \) is of rank \( n \), we say that \( f(x_1, x_2, \ldots, x_n) \) is nondegenerate. Two quadratic forms \( f_1(x_1, x_2, \ldots, x_n) \) and \( g_1(y_1, y_2, \ldots, y_n) \) over \( F_q \) are called equivalent if \( f_1(x_1, x_2, \ldots, x_n) \) can be transformed into \( g_1(y_1, y_2, \ldots, y_n) \) by means of a nonsingular linear substitution of indeterminates \( \bar{y} = Py \), where \( \bar{y} = (x_1, x_2, \ldots, x_n)^T, y = (y_1, y_2, \ldots, y_n)^T, \ P \) is a nonsingular matrix over \( F_q \), and \( T \) is the transpose operation.

The quadratic character \( \eta \) of \( F_q \) is defined by
\[
\eta(x) = \begin{cases}
0, & \text{if } x = 0 \\
1, & \text{if } x \text{ is a nonzero square of } F_q \\
-1, & \text{if } x \text{ is a non-square of } F_q
\end{cases}
\]
and the canonical additive character \( \chi \) of \( F_q \) is defined by \( \chi(x) = \zeta_p^x, \) where \( p \) is the characteristic of \( F_q \), \( \zeta_p = e^{2\pi i/p} \), and \( \text{tr}(\cdot) \) is the absolute trace function from \( F_q \) to \( \mathbb{F}_p \).

**Lemma 1 [15, Th. 6.21]:** Let \( f(x_1, x_2, \ldots, x_n) \) be a quadratic form of rank \( r \) over \( F_q \), where \( q \) is an odd prime power. Then, \( f(x_1, x_2, \ldots, x_n) \) is equivalent to a diagonal quadratic form \( a_1 y_1^2 + a_2 y_2^2 + \cdots + a_r y_r^2 \), where \( a_1, a_2, \ldots, a_r \) 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 \( \eta \) be the quadratic character of \( F_q \), and let \( b \in F_q \). If \( f(x_1, x_2, \ldots, x_n) \) is a nondegenerate quadratic form over \( F_q \), and \( \Delta \) denotes the determinant of \( f \), then the number of solutions in \( F_q^n \) of the equation \( f(x_1, x_2, \ldots, x_n) = b \) is given by

\[
\begin{align*}
q^{n-1} + q^{\frac{n-2}{2}} \eta \left( (-1)^{\frac{n-2}{2}} b \Delta \right), & \quad \text{when } \eta \text{ is odd} \\
q^{n-1} + q \nu(b) q^{\frac{n-2}{2}} \eta \left( (-1)^{\frac{n-2}{2}} \Delta \right), & \quad \text{when } \eta \text{ is even}
\end{align*}
\]

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

**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 \( \eta \) and the canonical additive character \( \chi \) 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

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

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

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

where \( \Delta \) 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 \( \Pi(x) = \Pi_1(x) \).
Let $\beta$ be a primitive element of $F_q$, and denote
\[
\begin{align*}
  k_0 &= \# \{x \in F_q^m \mid \text{tr}(\alpha \Pi(x)) = 0\}, \\
  k_i &= \# \{x \in F_q^m \mid \text{tr}(\alpha \Pi(x)) = \beta^i, \quad i = 1, 2, \ldots, q-1\}
\end{align*}
\]
where $\Pi(x)$ is a perfect nonlinear function from $F_q^m$ to itself. Then, we call $(k_0, k_1, \ldots, k_{q-1})$ the preimage distribution of $\text{tr}(\alpha \Pi(x))$.

For every nonzero $a \in F_q^m$ and $\Pi(x) = \Pi_1(x)$ or $\Pi_2(x)$, let $\Delta_a = \det(\text{tr}(a \Pi(x)))$. Clearly, $\Delta_a \in F_q^m$. According to Lemma 2, the preimage distributions of $\text{tr}(\alpha \Pi(x))$ 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 $\text{tr}(\alpha \Pi(x))$ have the following properties:
1) when $\Pi(x) = \Pi_1(x)$, for all $a \in F_q^m$, the preimage distribution of $\text{tr}(\alpha \Pi(x))$ is the same as that of $\text{tr}(x^2)$;
2) when $\Pi(x) = x^2$, for all $a \in F_q^m$, the preimage distribution of $\text{tr}(x^2)$ take only two cases: one case holds for all nonzero squares $a \in F_q^m$ and the other case holds for all non-squares $a \in F_q^m$;
3) when $\Pi(x) = \Pi_2(x)$, for all $a \in F_q^m$, the preimage distribution of $\text{tr}(\alpha \Pi(x))$ take only two cases: one case holds for $\text{tr}(\alpha \Pi(x))$ if and only if the other case holds for $\text{tr}(\alpha \Pi(x))$.

Based on the above properties of the preimage distributions of $\text{tr}(\alpha \Pi(x))$, 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 $\Delta_a = \eta^{(1)}$, and other $\frac{1}{2}(q^m - 1)$ nonzero $a \in F_q^m$ such that $\Delta_a = \eta^{(-1)}$, where $\eta$ is the quadratic character of $F_q$.

On the other hand, it is easily verified that $\text{tr}(\alpha \Pi_2(x))$ is a homogenous polynomial of degree $k+1$ of $m$ indeterminates over $F_3$ for every nonzero $a \in F_q^m$, 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 $a, b \in F_3$, it is shown in [19] that the character sum
\[
S(a, b) = \sum_{x \in F_3^m} \omega^{\text{tr}(\alpha \Pi_2(x)) + b \cdot c}, \quad \text{where } \omega = e^{2\pi i q}
\]
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 $\{S(a, b) \mid a, b \in F_q^m\}$ is given by
\[
\begin{align*}
  &\lambda_{3^m} = 1, \\
  &\lambda_0 = 3^m - 1, \\
  &\lambda_{3^{m-1}} = \frac{1}{2}(3^m - 1)3^{m-1}, \\
  &\lambda_{-3^{m-1}} = \frac{1}{2}(3^m - 1)3^{m-1}, \\
  &\lambda_{3^{m-2} \omega} = \frac{1}{2}(3^m - 1)(3^{m-1} - \frac{3^{m-1}}{2}), \\
  &\lambda_{-3^{m-2} \omega} = \frac{1}{2}(3^m - 1)(3^{m-1} + \frac{3^{m-1}}{2}), \\
  &\lambda_{3^{m-2} \omega^2} = \frac{1}{2}(3^m - 1)(3^{m-1} - \frac{3^{m-1}}{2}), \\
  &\lambda_{-3^{m-2} \omega^2} = \frac{1}{2}(3^m - 1)(3^{m-1} + \frac{3^{m-1}}{2}).
\end{align*}
\]

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
\[
\begin{align*}
  &\lambda_{3^m} = 1, \\
  &\lambda_0 = 3^m - 1, \\
  &\lambda_{3^{m-1}} = \frac{1}{2}(3^m - 1)(3^{m-1} + 2 \cdot \frac{3^{m-2}}{2}), \\
  &\lambda_{-3^{m-1}} = \frac{1}{2}(3^m - 1)(3^{m-1} - 2 \cdot \frac{3^{m-2}}{2}), \\
  &\lambda_{3^{m-2} \omega} = \frac{1}{2}(3^m - 1)(3^{m-1} - \frac{3^{m-2}}{2}), \\
  &\lambda_{-3^{m-2} \omega} = \frac{1}{2}(3^m - 1)(3^{m-1} + \frac{3^{m-2}}{2}), \\
  &\lambda_{3^{m-2} \omega^2} = \frac{1}{2}(3^m - 1)(3^{m-1} - \frac{3^{m-2}}{2}), \\
  &\lambda_{-3^{m-2} \omega^2} = \frac{1}{2}(3^m - 1)(3^{m-1} + \frac{3^{m-2}}{2}).
\end{align*}
\]

where $\omega = e^{2\pi i q}$, and $\lambda_v$ 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 $c_{d, d', c'}$ in $C_{II}$ defined by (2), where
\[
\begin{align*}
  &c_{a, b, c} = (f_0, f_1, \ldots, f_m, c), \quad f_a, f_b, f_c \in \mathbb{F}_q^m, \\
  &c_{d, d', c'} = (f_{a'}, f_{b'}, f_{c'}), \quad f_{a'}, f_{b'}, f_{c'} \in \mathbb{F}_q^{m-1},
\end{align*}
\]
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, $C_{II}$ can be expressed as follows:
\[
C_{II} = \{(f_a, f_b, f_c) \mid f_a, f_b, f_c \in \mathbb{F}_q^m, \forall c \in \Omega\}
\]
where $\Omega = \{t_0, t_1, \ldots, t_{q-1}\}$ and $t_0, t_1, \ldots, t_{q-1}$ are distinct elements of $F_3^m$ such that $\text{tr}(t_0) = 0$ and $\text{tr}(t_i) = \beta^i$ for $i = 1, 2, \ldots, q - 1$, $\beta$ 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 $C_{II}$.

**Case 1:** $\Pi(x) = \Pi_1(x)$ or $\Pi_2(x)$.

When $a = 0$, it is easily seen that $w_H(0, b, c) = 0, w_H(0, 0, c) = q^m$ for every $c \in \Omega \{t_0\}$, and $w_H(0, b, c) = (q - 1)^2$ 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 $x = F_H y$ such that $\text{tr}(\alpha \Pi(x))$ is equivalent to
\[
a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2
\]
where $a_1, a_2, \ldots, a_m$ are nonzero elements of $F_q$, and $P \in F_q^{m \times m}$ is a nonsingular matrix. It is noted that $\eta(\Delta_a) = \eta(a_1 a_2 \cdots a_m)$, where $\Delta_a$ is the determinant of $\text{tr}(\alpha \Pi(x))$ and $\eta$ is the quadratic character of $F_q$. Then, it follows that
\[
\text{tr}(\alpha \Pi(x) + kx) = a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2 + b_1 y_1 + \cdots + b_m y_m
\]
where $b_1, b_2, \ldots, b_m \in F_q$. Note that there is a one-to-one correspondence between $b \in F_q^m$ and $(b_1, b_2, \ldots, b_m) \in F_q^m$ such that $b = 0$ if and only if $(b_1, b_2, \ldots, b_m) = 0$. 
Let $z_1 = y_1 + \frac{b_1}{2a_1}, z_2 = y_2 + \frac{b_2}{2a_2}, \ldots, z_m = y_m + \frac{b_m}{2a_m}$ and let $c_0 = -\sum_{i=1}^{m} \frac{b_i}{2a_i} \in F_q$. Then
\[
\text{tr}(aI(x) + bx) = a_1z_1^2 + a_2z_2^2 + \cdots + a_mz_m^2 + c_0.
\]
With $\chi$ the canonical additive character of $F_q$, $t = \text{tr}(c)$ and $d = t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \in F_q$ (note that $t$ ranges over all the elements of $F_q$ as $c$ ranges over all the elements of $\Omega$), it follows that
\[
w_H(a, b, c) = q^m - \frac{1}{q} \sum_{x \in F_q^m} \sum_{s \in F_q^m} \chi(s(\text{tr}(aI(x) + bx + c))) = (q-1)q^{m-1} - \frac{1}{q} \sum_{s \in F_q^m} \chi(s t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \delta_i(s)) = (q-1)q^{m-1} - \frac{1}{q} \sum_{s \in F_q^m} \chi(s t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \delta_i(s)).
\]

\[
(9)
\]
i) If $m$ is odd, from Lemma 4, for any $s \in F_q^*$, we obtain
\[
\sum_{s_1, s_2, \ldots, s_m \in F_q^*} \chi(s_1z_1^2 + s_2z_2^2 + \cdots + s_mz_m^2) = q^{\frac{m-1}{2}} \eta \left( (-1)^{\frac{m-1}{2}} s^m a_1a_2 \cdots a_m \right) G(\eta, \chi) = q^{\frac{m-1}{2}} G(\eta, \chi) \eta \left( (-1)^{\frac{m-1}{2}} \Delta_a \right) \eta(s).
\]

\[
(10)
\]
It follows that
\[
w_H(a, b, c) = (q-1)q^{m-1} - q^{\frac{m-1}{2}} G(\eta, \chi) \times \eta \left( (-1)^{\frac{m-1}{2}} \Delta_a \right) \sum_{s \in F_q^m} \chi(s) \eta(s).
\]

\[
(11)
\]
If $d = 0$, then
\[
\sum_{s \in F_q^m} \chi(s) \eta(s) = \sum_{s \in F_q^m} \eta(s) = 0
\]
which implies that $w_H(a, b, c) = (q-1)q^{m-1}$.
If $d \neq 0$, then
\[
\sum_{s \in F_q^m} \chi(s) \eta(s) = \sum_{s' \in F_q^m} \chi(s') \eta(d^{-1} s') = \eta(d) G(\eta, \chi)
\]
and noting that $G(\eta, \chi) = \pm q$ 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
\[
t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \delta_i = 0;
\]

2) $w_H(a, b, c) = (q-1)q^{m-1} + q^{\frac{m-1}{2}}$ if and only if
\[
\eta \left( (-1)^{\frac{m-1}{2}} \Delta_a \right) \eta \left( t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \delta_i \right) = \begin{cases} -1, & \text{if } p \equiv 1 \mod 4; \\ 1, & \text{if } p \equiv 3 \mod 4. \end{cases}
\]

3) $w_H(a, b, c) = (q-1)q^{m-1} - q^{\frac{m-1}{2}}$ if and only if
\[
\eta \left( (-1)^{\frac{m-1}{2}} \Delta_a \right) \eta \left( t - \sum_{i=1}^{m} \frac{b_i}{2a_i} \delta_i \right) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4; \\ -1, & \text{if } p \equiv 3 \mod 4. \end{cases}
\]

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:
\[
(q-1) \left( q^{m-1} + \sum_{t \in F_q^m} \left( q^{m-1} + q^{\frac{m-1}{2}} \eta \left((-1)^{\frac{m-1}{2}} \Delta_a\right) \eta(t) \right) \right) = (q-1)(q^{m-1} + (q-1)q^{m-1}) = q^m(q^m - 1).
\]

Therefore, combining the two cases $a = 0$ and $a \neq 0$, we obtain
\[
A_{(q-1)q^m} = (q-1)q + q^m(q^m - 1) = (q^m + q)(q^m - 1).
\]

In the case $p \equiv 1 \mod 4$, 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:
\[
\frac{1}{2} (q-1)(q^m-1) \left( q^{m-1} + \sum_{t \in F_q^m} \left( q^{m-1} + q^{\frac{m-1}{2}} \eta(t) \right) \right) = \frac{1}{2} (q-1)(q^{2m} - q^m)
\]
which implies that
\[
A_{(q-1)q^{m-1} + q^{\frac{m-1}{2}}} = \frac{1}{2} (q-1)(q^{2m} - q^m).
\]

Similarly, we also obtain
\[
A_{(q-1)q^{m-1} - q^{\frac{m-1}{2}}} = \frac{1}{2} (q-1)(q^{2m} - q^m).
\]

In the case $p \equiv 3 \mod 4$, 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 $\Pi_2(x)$. 


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

\[
\sum_{z_1, z_2, \ldots, z_m \in F_q} \chi(s_1 z_1^2 + s_2 z_2^2 + \cdots + s_m z_m^2) = q^{m/2} \eta((-1)^{m/2} a_1 z_1 \cdots z_m).
\]

From (9), we have

\[
w_H(a, b, c) = (q-1)q^{m-1} - q^{m-2} \eta((-1)^{m/2} \Delta_a) \sum_{s \in F_q^m} \chi(sd) = \begin{cases} 
(q-1)q^{m-1} - (q-1)q^{m-2} \eta((-1)^{m/2} \Delta_a), & \text{if } d \neq 0; \\
(q-1)q^{m-1} + (q-1)q^{m-2} \eta((-1)^{m/2} \Delta_a), & \text{if } d \neq 0.
\end{cases}
\] (26)

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

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

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

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

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

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

\[
t - \sum_{i=1}^{m} b_i^2 a_i = 0 \quad \text{and} \quad \eta((-1)^{m/2} \Delta_a) = -1;
\] (21)

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

\[
t - \sum_{i=1}^{m} b_i^2 a_i = 0 \quad \text{and} \quad \eta((-1)^{m/2} \Delta_a) = -1.
\] (22)

It is easily seen that

\[
A_0 = 1 \quad A_{(q-1)} = q^{m+1} - q \quad A_q = q - 1
\]

since these weights occur only in the case \( a = 0 \).

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

\[
A_{(q-1)}(q^{m-1} - q^{m-2}) = \frac{1}{2}(q^{2m} - q^m),
\] (23)

Similarly, we also obtain

\[
A_{(q-1)}(q^{m-1} + q^{m-2}) = \frac{1}{2}(q^{2m} - q^m).
\] (24)

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

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

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

\[
A_{(q-1)}(q^{m-1} - q^{m-2}) = \frac{1}{2}(q^{m} - 1)(q^{2m} - q^m).
\] (26)

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

\[
S(a, b) = \sum_{x \in F_q^m} \omega^{\text{tr}(a \Pi_2(x) + bx)}
\]

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

\[
w_H(a, b, c) = 3^m - 3 \sum_{a \in F_q^m} \sum_{b \in F_q} \omega^{\text{tr}(a \Pi_2(x) + bx + \gamma c)}
\]

\[
= 3^m - 3 \sum_{a \in F_q^m} \omega^{\text{tr}(S(a, b))}
\]

\[
= 2 \cdot 3^{m-1} - \frac{1}{3}(\omega^t S(a, b) + \omega^{-t} S(-a, -b))
\]

\[
= 2 \cdot 3^{m-1} - \frac{1}{3} \text{Re}(\omega^t S(a, b))
\]

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 4(i), all the values of \( S(a, b) \), where \( a, b \in F_q^m \), are given as follows:

\[
3^m, 0, \pm i3^m, \pm i3^m \omega, \pm i3^m \omega^2, -i3^m \omega^2.
\]

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

\[
3^m, 0, i3^m, -i3^m, i3^m \omega, -i3^m \omega, i3^m \omega^2, -i3^m \omega^2
\]

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

\[
0, 2 \cdot 3^m - 2 \cdot 3^m - 2 \cdot 3^m, 2 \cdot 3^m - 2 \cdot 3^m - 2 \cdot 3^m, 2 \cdot 3^m - 2 \cdot 3^m - 2 \cdot 3^m.
\]

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

\[
\begin{align*}
A_0^{(0)} &= 1 \\
A_0^{(0)}(3^m, -1) &= (3^m - 1)(3^m - 3^m) \\
A_0^{(2)}(3^m, -1) &= (3^m - 1)(3^m - 3^m) \\
A_0^{(2)}(3^m, -1) &= (3^m - 1)(3^m - 3^m)
\end{align*}
\] (28)

where, for \( t = 0, 1, 2 \), \( A_0^{(t)} \) 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:

\[
\begin{align*}
A(t)_{2^{m-1}} &= 1 \\
A(t)_{2^{m-1}+\frac{m-1}{2}} &= \frac{1}{2}(3^m - 1)
\left(2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}\right) \\
A(t)_{2^{m-1}+\frac{m+1}{2}} &= \frac{1}{2}(3^m - 1)
\left(2 \cdot 3^{m-1} + 3^\frac{m+1}{2}\right)
\end{align*}
\]  

(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 \( C_{11} \) is the same as that of the code \( \{c_{ab} \in \tilde{C}_{11} | a, b \in \mathbb{F}_{q^m}, c = t_0\} \). 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 \( c_{ab} \) be a nonzero codeword of \( \tilde{C}_{11} \). Then, \( c_{ab} \) 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 \( c_{ab} \) be a nonzero codeword of \( \tilde{C}_{11} \). Then, \( c_{ab} \) is of weight \( q^m - q^m - 1 \) if and only if \( a = 0 \), \( b \neq 0 \) and \( c \in \Omega \), and \( c_{ab} \) 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 \( \mathcal{C} = \{c_0, c_1, \ldots, c_n\} \) be a vector of \( \mathbb{F}_{q}^n \). The support of \( \mathcal{C} \), denoted by \( \text{Supp}(\mathcal{C}) \), is defined to be the set \( \{i|0 \leq i \leq n - 1, c_i \neq 0\} \). For any two vectors \( \mathcal{C}, \mathcal{C}' \in \mathbb{F}_{q}^n \), \( \mathcal{C} \) covers \( \mathcal{C}' \) if the support of \( \mathcal{C} \) contains that of \( \mathcal{C}' \).

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 \( C_{11} \) and \( \tilde{C}_{11} \) for all known explicit perfect nonlinear functions \( \Pi(x) \) from \( \mathbb{F}_{q^m} \) 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 \( C_{11} \)) 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 \( \mathbb{F}_{q^m} \) to itself, then the covering structure of \( \tilde{C}_{11} \) is given as follows:

i) if \( m \geq 3 \), all the nonzero codewords of \( C_{11} \) 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 \( q^2 - 2q + 1, q^2 - q - 1, q^2 - 1 \) are minimal, and the other codewords are not minimal.

Theorem 6 (Covering structure of \( \tilde{C}_{11} \)) 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 \( \mathbb{F}_{q^m} \) to itself, then the covering structure of \( \tilde{C}_{11} \) 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 \( q^2 - 2q + 1, q^2 - q - 1, q^2 - q + 1 \) 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 \( C_{11} \) and \( \tilde{C}_{11} \).

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 \( \frac{2n - q + 1}{q - 1} \) must be a minimal codeword.

Lemma 7: Let \( C_{11} \) be defined by (1) with \( \Pi(x) = x^2, m = 2 \), and \( q > 3 \). If \( c_{ab} \in C_{11} \) is of weight \( q^2 - q + 1 \) and not a minimal codeword, then \( a, b \neq 0 \) and \( t(\frac{t^2}{a}) = 0 \).

Proof: Since \( m = 2 \), from (4), all the nonzero weights of \( C_{11} \) are

\[ q^2 - 2q + 1, q^2 - q - 1, q^2 - q - 1, q^2 - q + 1, q^2 - 1. \]

If \( c_{ab} \) is a codeword of weight \( q^2 - q + 1 \) in \( C_{11} \), then \( a \neq 0 \) from Corollary 3. According to (19) and (20) with \( t = 0 \), we obtain \( b \neq 0 \). Let

\[ S = \{x|x \in \mathbb{F}_{q^2}, \text{tr}(ax^2 + bx) = 0\} \]

\[ T = \{x|x \in \mathbb{F}_{q^2}, (ax^2 + bx)^{q-1} = -1\}. \]

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 \( c_{ab} \) is not a minimal codeword of \( C_{11} \), then there exists a nonzero codeword \( c_{a'b'} \in \tilde{C}_{11} \) such that \( c_{ab} \) covers \( c_{a'b'} \) and \( (a', b') \neq (k(a, b)) \) for any \( k \in \mathbb{F}_{q}^* \). Clearly, \( (a', b') \neq (0, 0) \).

Let \( t = a'b' - ab' \), then \( t \neq 0 \). Otherwise, if \( t = 0 \), then \( \frac{a'}{b'} = \frac{b'}{a'} = u \in \mathbb{F}_{q^2}^* \). Since \( c_{ab} \) covers \( c_{a'b'} \) and \( |T| \geq 2 \), there exists \( y \in \mathbb{F}_{q^2}^* \) such that

\[ (a'y^2 + by)^{q-1} = (a'y^2 + b'y)^{q-1} = -1. \]
Note that

\[-1 = (a' \cdot y^2 + b' \cdot y)^{q-1} = (u_1 y^2 + u_2 y)^{q-1} = u_1^{q-1} (a y^2 + b y)^{q-1} = -u_1^{q-1}.
\]

Therefore, \( u_1^{q-1} = 1 \). 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 \(-b/a - z \in T\), since

\[
\left( a \left( -\frac{b}{a} - z \right)^2 + b \left( -\frac{b}{a} - z \right) \right)^{q-1} = (az^2 + bz)^{q-1} = -1.
\]

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

\[
\text{tr}(a' z^2 + b' z) = \text{tr}\left( a' \left( b/a - z \right)^2 + b' \left( -b/a - z \right) \right) = 0
\]

which implies that

\[
\text{tr}\left( \frac{2t}{a} + \frac{bt}{a^2} \right) = 0, \tag{30}
\]

It is easily verified that \(-b/a \in S\), then we have

\[
0 = \text{tr}\left( a' \left( b/a - z \right)^2 + b' \left( -b/a - z \right) \right) = \text{tr}\left( \frac{bt}{a^2} \right). \tag{31}
\]

From (30) and (31), we obtain that \( \text{tr}(\frac{2t}{a}) = 0 \) for every \( z \in T \), which implies that \( z^2 = -\frac{1}{a} t z \). Substitute \( z' \) by \(-\frac{1}{a} t z\) in the following equation:

\[
0 = \text{tr}(az^2 + bz) = az^2 + bz + a^2 z'^2 + b^2 z'^4
\]

and then reformulate it as

\[
\left( a + a^2 \left( \frac{t}{a} \right)^{-2q} \right) z'^2 + \left( b - b^2 \left( \frac{t}{a} \right)^{-1-q} \right) z = 0.
\]

Noting that \( z \neq 0 \), it follows that:

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

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

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

has at least \([T] \geq 2\) solutions. Hence

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

Since \( c_{a,b} \) covers \( c_{a', b'} \), we similarly obtain

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

From (32) and (33), we obtain that \((a')^{-q} = a^{-q-1}\) if \(a' \neq 0\) and \((b')^{-q} = b^{-q-1}\) if \(b' \neq 0\). Now we can prove \( \text{tr}(\frac{t}{a}) = 0 \) by distinguishing the following three cases.

**Case 1:** If \(a' = 0\), then \(b' \neq 0\). Hence, \( t = -b' \) 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

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

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

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

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 \( a' = k_1 a \) and \( b' = k_2 b \). Then, \( k_1 \neq k_2 \). Therefore, we obtain from (31) that

\[
0 = \text{tr}\left( \frac{bt}{a^2} \right) = \text{tr}\left( (k_1 - k_2) \frac{b^2}{a} \right).
\]

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

**Lemma 8:** Let \( \tilde{C}_{12} \) 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 \( c_{a,b,c} \) in \( \tilde{C}_{12} \).

**Proof:** Since \( m = 2 \), from (6), all the nonzero weights of \( \tilde{C}_{12} \) are:

\[
\{q^2 - 2q + 1, q^2 - q - 1, q^2 - q - 1, q^2 - q - 1, q^2 - 1, q^2 \}.
\]

Let \( c_{a,b,c} \) be a codeword of weight \( q^2 - q + 1 \) in \( \tilde{C}_{12} \). Then, \( a \neq 0 \) from Corollary 4. Note that the following equation holds when \( a \neq 0 \):

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

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 \( q^2 - q - 1 \), which is a contradiction. Therefore

\[
\text{tr}(\frac{4ac - b^2}{4a}) \neq 0, \tag{34}
\]

Let \( S = \{ x \in F_q \mid \text{tr}(ax^2 + bx + c) = 0 \} \). 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 \( c_{a,b,c} \) in \( \tilde{C}_{12} \). Now we prove that \( c_{a,b,c} \) cannot cover any nonzero codeword of the form \( c_{a,b,c} \) where \( u \in F_q^* \). Supposing the contrary that \( c_{a,b,c} \) covers some \( c_{a,b,c} \) where \( u \in F_q^* \) and \( v \in \Omega \), we let

\[
S_{u,v} = \{ x \in F_q | \text{tr}(ux + v) = 0 \}
\]
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 \( C_{a,b,c} \), we have \( S \subseteq S_{a,b,c} \) and \( |T_y| = q^{a-2} \geq 3 \), since \( q \) is an odd prime power greater than 3.

For any \( y \in S \) and any \( z \in T_y \), we have \( y, y + z \in S_{a,b,c} \), since \( S \subseteq S_{a,b,c} \). 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
\[
z^{q/2} = -u^{1-1}z \quad (37)
\]
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 \( \text{tr}(z(ax + 2ay + b)) = 0 \), which is equivalent to
\[
a2z + 2ay + b = 0 \quad \text{or} \quad (az + 2ay + b)^{q-1} = -1. \quad (38)
\]
Note that for any \( y \in S \), there is at most one \( z \in T_y \) such that \( a2z + 2ay + b = 0 \). Therefore, combining (36) and (38), there are at least \( |T_y| - 1 = q - 3 \geq 2 \) elements \( z \) of \( T_y \) such that
\[
(z(ax + 2ay + b))^{q-1} = (uz)^{q-1}.
\]
It follows that \( \frac{(ax + 2ay + b)^{q-1} - 1}{q} = az + 2ay + b \), which is equivalent to
\[
\frac{a(z^{q/2} + (2ay + b)^{q-1}}{q} = \frac{az + 2ay + b}{q} \quad (39).
\]
Substituting (37) into (39), we obtain
\[
(ax^{q-1} + a^{q-1}y)z + u^{q-1}(2ay + b) - (2ay + b)^q = 0. \quad (40)
\]
If \( ax^{q-1} + a^{q-1}y \neq 0 \), then the following linear equation:
\[
(ax^{q-1} + a^{q-1}y)x + u^{q-1}(2ay + b) - (2ay + b)^q = 0
\]
has at least \( |T_y| - 1 = q - 3 \geq 2 \) solutions, which is a contradiction. Therefore
\[
ax^{q-1} + a^{q-1}y = 0 \quad \text{and} \quad u^{q-1}(2ay + b) - (2ay + b)^q = 0.
\]
It follows that \( 2ay + b \neq 0 \) since \( b_{2a} \notin S \) implies \( 2ay + b \neq 0 \). Hence, \( 2ay + b \in F_{q^2}^* \). Since \( |S| = q - 1 \), we obtain
\[
S = \left\{ y | y = \frac{k}{2a}, k \in F_{q^2}^* \right\}.
\]
Taking \( y = \frac{u}{2a} \in S \), then \( z = \frac{u}{2a} \in T_y \) since \( y + z = \frac{u}{2a} + \frac{u}{2a} \in S \).

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 \( y = \frac{u^2}{2a} \in S \), we have
\[
0 = \text{tr}(ay^2 + by + c) = \text{tr} \left( a \left( y + \frac{b}{2a} \right)^2 + \frac{4ac - b^2}{4a} \right) = \text{tr} \left( \frac{u^2}{4a} + \frac{4ac - b^2}{4a} \right). \quad (42)
\]
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 \( c_{a,b,c} \), where \( u \in F_{q^2}^* \).

\[\square\]

**B. Determining the Covering Structure of \( C_{11} \)**

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

i) When \( m \) is odd, \( C_{11} \) is a \([q^{m-1} - 1, 2m, (q - 1)q^{m-1} - q^{m-2}; q] \)-code from Corollary 1. In this subcase
\[
\frac{qd - q + 1}{q - 1} = \frac{q^{m+1} - q^m - q^{m-1} - q + 1}{q - 1}.
\]
It is easily verified that the following inequality is true for odd \( m \geq 3 \):
\[
(q - 1)q^{m-1} + q^{m-1} \leq \frac{q^{m+1} - q^m - q^{m-1} - q + 1}{q - 1}.
\]
It follows from Theorem 1 that each of the nonzero weights in \( C_{11} \) in the case of \( m \) odd is less than or equal to
\[
\frac{q^{m+1} - q^m - q^{m-1} - q + 1}{q - 1}.
\]
Hence, from Lemma 6, i) is true for odd \( m \geq 3 \).

When \( m \) is even, \( C_{11} \) is a \([q^{m-1} - 1, 2m, (q - 1)(q^{m-1} - q^{m-2}); q] \)-code from Corollary 2. In this subcase
\[
\frac{qd - q + 1}{q - 1} = \frac{q^m - q^{m-1} - 1}{q - 1}.
\]
It is easily verified that the following inequality is true for even \( m \geq 3 \):
\[
(q - 1) \left( q^{m-1} + q^{m-2} \right) \leq q^m - q^{m-1} - 1.
\]
It follows from Theorem 1 that each of the nonzero weights in \( C_{11} \) in the case of \( m \) even is less than or equal to \( q^m - q^{m-1} - 1 \). Hence, from Lemma 6, i) is also true for even \( m > 3 \).

ii) If \( m = 2 \) and \( q = 3 \), \( C_{11} \) is an \([8, 4, 4; 3] \)-code from Corollary 2, and all the nonzero weights of \( C_{11} \) are 4, 5, 6, 7, 8 from (4). In this subcase
\[
n - k + 1 = 8 - 4 + 1 = 5 \quad \frac{qd - q + 1}{q - 1} = \frac{3 	imes 4 - 3 + 1}{2} = 5.
\]
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 \( q > 3 \), \( C_{II} \) is a \([q^2-1,1,q^2-2q+1;q]\)-code from Corollary 2, and all the nonzero weights of \( C_{II} \) 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

\[
\frac{n-k+1}{q-1} = \frac{q(q^2-2q+1) - q+1}{q-1} = q^2 - q - 1.
\]

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

In the following, we discuss the minimality of the codewords of weights \( q^2-q \) and \( q^2-q+1 \) in \( C_{II} \). 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 \( C_{II} \) are not minimal. Indeed, let \( c_{a,b} \) be a codeword of weight \( q^2-q \) in \( C_{II} \). Then, \( a = 0 \) and \( b \neq 0 \) from Corollary 3. Set \( a = \alpha + \beta \bar{b}^2 \), where \( \alpha \) is a primitive element of \( F_q \). Clearly, \( a' \neq 0 \). For every \( x \in F_q^m \), if \( \text{tr}(bx) = 0 \), then \( bx = (bx)^q = 0 \), which implies \( \text{tr}(bx)^{q-1} = -1 \) since \( b, x \in F_q^m \). Hence

\[
\text{tr}(a'x^2 + bx) = (a'x^2 + (a'x^2)^q) = (a'x^2)\left(1 + \alpha^2x^{2q} - 1\right) = (a'x^2)(1-1) = 0.
\]

This demonstrates that \( c_{a,b} \) covers \( c_{a',b'} \), and \( c_{a,b} \) 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 \( C_{II} \) are minimal. Indeed, if \( c_{a,b} \) is of weight \( q^2-q+1 \) and not a minimal codeword of \( C_{II} \), then \( a, b \neq 0 \) and \( \text{tr}(\frac{b}{a}) = 0 \) from Lemma 7. This implies \( a^{q-1} = -1 \). Hence, for any \( x \in F_q^m \), if \( \text{tr}(bx) = 0 \), we have \( (bx)^{q-1} = -1 \) since \( b, x \in F_q^m \). Therefore

\[
\text{tr}(ax^2 + bx) = \text{tr}(ax^2) = ax^2(1 + (ax^2)^{q-1}) = ax^2(1 - (ax^2)^{q-1}) = ax^2 = 0.
\]

This shows that the codeword \( c_{a,b} \) covers the codeword \( c_{a,b} \). It follows that the weight of \( c_{a,b} \) is less than or equal to that of \( c_{a,b} \). However, from Corollary 3, the weight of \( c_{a,b} \) 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.

C. Determining the Covering Structure of \( \tilde{C}_{II} \)

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

i) When \( m \) is odd, \( \tilde{C}_{II} \) is a \([q^m,2m+1,(q-1)q^{m-1} - q^{\frac{m-3}{2}};q]\)-code from Corollary 1. In this subcase

\[
\frac{n-k+1}{q-1} = \frac{q^m - q^m - q^{m+1} - q + 1}{q-1}.
\]

As in the proof of Theorem 5i)

\[
(q-1)q^{m+1} - q^m - q^{m+1} - q + 1.
\]

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

\[
\frac{q^{m+1} - q^m - q^{m+1} - q + 1}{q-1}.
\]

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

When \( m \) is even, \( \tilde{C}_{II} \) is a \([q^m,2m+1,(q-1)(q^{m-1} - q^{\frac{m-3}{2}});q]\)-code from Corollary 2. In this subcase

\[
\frac{n-k+1}{q-1} = \frac{q^m - q^{m+1}}{q-1}.
\]

As in the proof of Theorem 5i)

\[
(q-1)\left(q^{m+1} - q^{\frac{m-3}{2}}\right) \leq q^m - q^{\frac{m-1}{2}} - 1.
\]

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

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

\[
\frac{n-k+1}{q-1} = \frac{9 - 5 + 1}{3} = 5.
\]

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

\[
\{q^2-2q+1, q^2-q-1, q^2-q, q^2-q+1, q^2-1, q^2-4\}.
\]

In this subcase

\[
\frac{n-k+1}{q-1} = \frac{q^2 - 5 + 1}{3} = q^2 - 4.
\]

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 \(C_{11}\). As in the proof of Theorem 5(ii), we only need to consider the case \(\Pi(x) = x^2\).

First, the codewords of weight \(q^2-q\) in \(C_{11}\) are not minimal. Indeed, if \(c_{ab,bc}\) is a codeword of weight \(q^2-q\) in \(C_{11}\), then \(a = 0\) and \(b \neq 0\) from Corollary 4. Set \(a' = \alpha b^2\), where \(\alpha\) is a primitive element of \(F_q^\ast\). Clearly, \(a' \neq 0\). For every \(x \in F_q^\ast\), 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 \(c_{0,ab,bc}\) covers \(c_{a'b^2,bc,a'c^2}\). Note that \(c_{0,ab,bc}\) is not a multiple of \(c_{a'b^2,bc,a'c^2}\) since \(ab^2 \neq 0\); the codewords of weight \(q^2-q\) are, therefore, not minimal.

Finally, the codewords of weight \(q^2-q+1\) in \(C_{11}\) are minimal. Indeed, if \(c_{a,ab,bc}\) is a codeword of weight \(q^2-q+1\) in \(C_{11}\), we let
\[
S = \{x \in F_q^\ast \mid \text{tr}(ax^2 + bx + c) = 0\}.
\]
Recall that \(|S| = q - 1 > 2\), since \(q\) is an odd prime power greater than 3.

If \(c_{a,ab,bc}\) is not a minimal codeword of \(C_{11}\), then there exists \(c_{a'b',b',c'} \in C_{11}\) such that \(c_{a,ab,bc}\) covers \(c_{a'b',b',c'}\) and \(c_{a'b',b',c'} \neq kc_{a,ab,bc}\), where \(k \in F_q^\ast\). Hence, \(a, a' \neq 0\) from Corollary 4 and Lemma 8. Set \(t = b - ab'\), then \(t = 0\). Otherwise, for any \(y \in S\),
\[
\text{tr}(a(b - y)^2 + b(-y - y) + c) = \text{tr}(ay^2 + by + c) = 0
\]
which implies that \(-b/a \in S\). Note that \(c_{a,ab,bc}\) covers \(c_{a'b',b',c'}\), and we have
\[
\begin{align*}
\text{tr}(a'(y/b - y)^2 + b'(b/a - y) + c') &= \text{tr}(a'(b/a - y)^2 + b'(-b/a - y) + c') \\
&= 0.
\end{align*}
\]
(43)

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

Therefore, \(t = b - ab' = 0\). Let \(\frac{a}{a'} = w\), then \(w \in F_q^\ast\) since \(a, a' \neq 0\) and \(b' = ub\) since \(t = 0\). We now proceed to prove that \(w \in F_q^\ast\). Since \(c_{a,ab,bc}\) covers \(c_{a'b',b',c'}\) and \(y \in S\), the following equalities follow:
\[
0 = \text{tr}(ay^2 + by + c)
= (ay^2 + by + c)^q + (ay^2 + by + c)
\]
and
\[
0 = \text{tr}(a'y^2 + b'y + c')
= \text{tr}(awy^2 + bwy + c) + (c' - wc))
= \text{tr}(awy^2 + bwy + c) + \text{tr}(c' - wc)
= w^q(ay^2 + by + c)^q
+ w^q(ay^2 + by + c) + \text{tr}(c' - wc).
\]
(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 \(w \in F_q^\ast\) 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 \(C_{11}\). 

\[\Box\]

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 \(C_{11}\), where \(C\) is an \([n, k, d; q]\)-code, the secret \(s\) is an element of \(F_q^\ast\), which is called the secret space. There are a dealer \(P_0\) and \(n - 1\) parties \(P_1, P_2, \ldots, P_{n-1}\) in the secret sharing scheme. Let \(G = (g_0, g_1, \ldots, g_{n-1})\) 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 \(y = (u_0, u_1, \ldots, u_{n-1}) \in F_q^n\) such that \(s = yg_0\).

Step 2) The dealer \(P_0\) treats \(y\) as an information vector and computes the corresponding codeword \(yG = (u_0, u_1, \ldots, u_{n-1})\), then he sends \(u_i\) 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 \(\{u_i, u_{i+1}, \ldots, u_{i+m}\}\) can determine the secret \(s\) if and only if there exists a minimal combination of \(\{g_i, g_{i+1}, \ldots, g_{i+m}\}\), where \(1 \leq i < i_2 < \cdots < i_m \leq n - 1\).

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 \(\{i_1, i_2, \ldots, i_m\}\) 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 assess 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 \(\{i_1, i_2, \ldots, i_m\} \subseteq \{1, 2, \ldots, n - 1\}\) such that \(i_1 < i_2 < \cdots < i_m\) is a minimal access set in the secret sharing scheme based on \(C\) if and only if there exists a minimal codeword \(c = (c_0, c_1, \ldots, c_{n-1}) \in C^\perp\) such that \(\text{Supp}(c) = \{i_1, i_2, \ldots, i_m\}\) and \(c_0 = 1\).

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

In the following, we consider the secret sharing schemes based on \(C_{11}\) and \(C_{11}^\perp\). 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 $F_{qm}$ to itself, then the access structure of the secret sharing scheme based on $C^\perp_{11}$ 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 $C^\perp_{11}$ 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 $C^\perp_{11}$ 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 $C^\perp_{11}$ 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 $F_{qm}$ to itself, then the access structure of the secret sharing scheme based on $C^\perp_{11}$ 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 $C^\perp_{11}$ with first coordinate 1 except for the codeword $(1,1,\ldots,1)$;

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 $C^\perp_{11}$ 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 $C^\perp_{11}$ 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 $C^\perp_{11}$ be the $[8,4,3]$-code from the perfect nonlinear function $\Pi(x) = x^{\frac{3^4 - 1}{2}}$ where $(q,m,k) = (3,2,1)$. Then, from Theorem 1(ii), the weight enumerator of $C^\perp_{11}$ is

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

According to Theorem 5(ii), there are $20 + 32 = 52$ minimal codewords in $C^\perp_{11}$. Of these minimal codewords, the following codewords are of first coordinate 1:

$$[1,0,0,0,0,0,0,0], [1,0,2,0,1,0,2,0], [1,2,2,0,0,1,0,0], [1,0,0,1,2,2,0,0], [1,0,0,0,2,0,1,2], [1,0,0,0,0,0,0,1,1,1,1,2], [1,2,0,0,0,2,2,2], [1,0,1,0,1,0,2,0], [1,2,0,1,0,0,1,1,1], [1,1,1,0,1,0,1,0,0,1,0,1], [1,2,0,1,0,1,0,0,1,0,1], [1,0,0,1,2,0,1,1,0,0,0,0,1], [1,2,0,2,0,2,0,0,2].$$

Therefore, from Theorem 7(ii), all the minimal access sets in the secret sharing scheme based on $C^\perp_{11}$ are:

$$[1,4,7], [2,4,6], [1,2,5], [3,4,5], [3,6,7], [4,5,6,7], [1,5,6,7], [2,4,5,7], [1,2,6,7], [1,3,5,6], [1,3,4,6], [1,2,3,7], [2,3,5,6], [1,2,3,4], [1,2,3,5].$$

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


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.

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.