A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing

Kelan Ding and Cunsheng Ding

Abstract

In this paper, a class of two-weight and three-weight linear codes over $\mathrm{GF}(p)$ is constructed, and their application in secret sharing is investigated. Some of the linear codes obtained are optimal in the sense that they meet certain bounds on linear codes. These codes have applications also in authentication codes, association schemes, and strongly regular graphs, in addition to their applications in consumer electronics, communication and data storage systems.

Index Terms

Association schemes, authentication codes, linear codes, secret sharing schemes, strongly regular graphs.

I. INTRODUCTION

Throughout this paper, let p be an odd prime and let $q = p^m$ for some positive integer m. An $[n, k, d]$ code $\mathcal{C}$ over $\mathrm{GF}(p)$ is a k-dimensional subspace of $\mathrm{GF}(p)^n$ with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. The *weight distribution* $(1, A_1, \ldots, A_n)$ is an important research topic in coding theory, as it contains crucial information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \cdots, A_n)$ is equal to t.

Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathrm{GF}(q)$. Let Tr denote the trace function from $\mathrm{GF}(q)$ onto $\mathrm{GF}(p)$ throughout this paper. We define a linear code of length n over $\mathrm{GF}(p)$ by

$$\mathcal{C}_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathrm{GF}(q)\}, \tag{1}$$

and call D the *defining set* of this code $\mathcal{C}_D$.

This construction is generic in the sense that many classes of known codes could be produced by selecting the defining set $D \subseteq \mathrm{GF}(q)$. This construction technique was employed in [15] and [16] for obtaining linear codes with a few weights.

The objective of this paper is to construct a class of linear codes over $\mathrm{GF}(p)$ with two and three nonzero weights using this generic construction method, and investigate their application in secret sharing. Some of the linear codes obtained in this paper are optimal in the sense that they meet some bounds on linear codes. The linear codes with a few weights presented in this paper have applications also in authentication codes [17], association schemes [5], and strongly regular graphs [5], in addition to their applications in consumer electronics, communication and data storage systems.

K. Ding is with the State Key Laboratory of Information Security, the Institute of Information Engineering, The Chinese Academy of Sciences, Beijing, China. Email: dingkelan@iie.ac.cn

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. Email: cding@ust.hk

II. THE LINEAR CODES WITH TWO AND THREE WEIGHTS

We only describe the codes and introduce their parameters in this section. The proofs of their parameters will be given in Section III.

In this paper, the defining set D of the code $\mathcal{C}_D$ of (1) is given by

$$D = \{x \in \mathrm{GF}(q)^* : \mathrm{Tr}(x^2) = 0\}. \tag{2}$$

Theorem 1. *Let $m > 1$ be odd, and let D be defined in (2). Then the set $\mathcal{C}_D$ of (1) is a $[p^{m-1} - 1, m]$ code over $\mathrm{GF}(p)$ with the weight distribution in Table I, where $A_w = 0$ for all other weights w not listed in the table.*

TABLE I
THE WEIGHT DISTRIBUTION OF THE CODES OF THEOREM 1

Weight w	Multiplicity A_w
0	1
$(p-1)\left(p^{m-2} - p^{\frac{m-3}{2}}\right)$	$\frac{p-1}{2}\left(p^{m-1} + p^{\frac{m-1}{2}}\right)$
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)\left(p^{m-2} + p^{\frac{m-3}{2}}\right)$	$\frac{p-1}{2}\left(p^{m-1} - p^{\frac{m-1}{2}}\right)$

Example 1. *Let $(p,m) = (3,5)$. Then the code $\mathcal{C}_D$ has parameters $[80,5,48]$ and weight enumerator $1 + 90z^{48} + 80z^{54} + 72z^{60}$.*

Theorem 2. *Let $m \geq 2$ be even, and let D be defined in (2). Then the code $\mathcal{C}_D$ over $\mathrm{GF}(p)$ of (1) has parameters*

$$\left[p^{m-1} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)p^{\frac{m-2}{2}} - 1, m\right]$$

and the weight distribution in Table II, where $A_w = 0$ for all other weights w not listed in the table.

TABLE II
THE WEIGHT DISTRIBUTION OF THE CODES OF THEOREM 2

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

Example 2. *Let $(p,m) = (5,4)$. Then the code $\mathcal{C}_D$ has parameters $[104,4,80]$ and weight enumerator $1 + 520z^{80} + 104z^{100}$. The best linear code of length 104 and dimension 4 over $\mathrm{GF}(5)$ has minimum weight 81.*

It is observed that the weights in the code $\mathcal{C}_D$ have a common divisor $p-1$. This indicates that the code $\mathcal{C}_D$ may be punctured into a shorter one whose weight distribution can be easily derived from that of the original code $\mathcal{C}_D$. This is indeed true and can be done as follows.

Note that $\mathrm{Tr}(ax^2) = 0$ for all $a \in \mathrm{GF}(p)$ if $\mathrm{Tr}(x^2) = 0$. Hence, the set D of (2) can be expressed as

$$D = (\mathrm{GF}(p)^*)\bar{D} = \{ab : a \in \mathrm{GF}(p)^* \text{ and } b \in \bar{D}\}, \tag{3}$$

where $d_i/d_j \notin \mathrm{GF}(p)^*$ for every pair of distinct elements d_i and d_j in $\bar{D}$. Then the code $\mathcal{C}_{\bar{D}}$ is a punctured version of $\mathcal{C}_D$ whose parameters are given in the following two corollaries.

Corollary 3. *Let $m > 1$ be odd, and let $\bar{D}$ be defined in (3). Then the set $\mathcal{C}_{\bar{D}}$ of (1) is a $[(p^{m-1} - 1)/(p - 1), m]$ code over $\mathrm{GF}(p)$ with the weight distribution in Table III, where $A_w = 0$ for all other weights w not listed in the table.*

TABLE III
THE WEIGHT DISTRIBUTION OF THE CODES OF COROLLARY 3

Weight w	Multiplicity A_w
0	1
$p^{m-2} - p^{\frac{m-3}{2}}$	$\frac{p-1}{2}\left(p^{m-1} + p^{\frac{m-1}{2}}\right)$
p^{m-2}	$p^{m-1} - 1$
$p^{m-2} + p^{\frac{m-3}{2}}$	$\frac{p-1}{2}\left(p^{m-1} - p^{\frac{m-1}{2}}\right)$

Example 3. *Let* $(p,m) = (3,5)$. *Then the code* $\mathcal{C}_{\bar{D}}$ *has parameters* $[40,5,24]$ *and weight enumerator* $1 + 90z^{24} + 80z^{27} + 72z^{30}$. *This code is optimal in the sense that any ternary code of length* 40 *and dimension* 5 *cannot have minimum distance* 25 *or more* [20].

Corollary 4. *Let* $m \geq 2$ *be even, and let* $\bar{D}$ *be defined in* (3). *Then the code* $\mathcal{C}_{\bar{D}}$ *over* $\mathrm{GF}(p)$ *of* (1) *has parameters*

$$\left[\frac{p^{m-1}-1}{p-1} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}} p^{\frac{m-2}{2}}, m\right]$$

and the weight distribution in Table IV, where $A_w = 0$ *for all other weights* w *not listed in the table.*

TABLE IV
THE WEIGHT DISTRIBUTION OF THE CODES OF COROLLARY 4

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

Example 4. *Let* $(p,m) = (5,4)$. *Then the code* $\mathcal{C}_{\bar{D}}$ *has parameters* $[26,4,20]$ *and weight enumerator* $1 + 520z^{20} + 104z^{25}$. *This code is optimal due to the Griesmer bound.*

III. THE PROOFS OF THE MAIN RESULTS

Our task of this section is to prove Theorems 1 and 2, while Corollaries 3 and 4 follow directly from Theorems 1 and 2, respectively.

A. Some auxiliary results

To prove Theorems 1 and 2, we need the help of a number of lemmas that are described and proved in the sequel. We start with group characters and Gauss sums.

An *additive character* of $\mathrm{GF}(q)$ is a nonzero function χ from $\mathrm{GF}(q)$ to the set of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x,y) \in \mathrm{GF}(q)^2$. For each $b \in \mathrm{GF}(q)$, the function

$$\chi_b(c) = \varepsilon_p^{\mathrm{Tr}(bc)} \quad \text{for all } c \in \mathrm{GF}(q) \tag{4}$$

defines an additive character of $\mathrm{GF}(q)$, where $\varepsilon_p = e^{2\pi\sqrt{-1}/p}$. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of $\mathrm{GF}(q)$. The character χ_1 in (4) is called the *canonical additive character* of $\mathrm{GF}(q)$. It is known that every additive character of $\mathrm{GF}(q)$ can be written as $\chi_b(x) = \chi_1(bx)$ [24, Theorem 5.7].

Since the multiplicative group $\mathrm{GF}(q)^*$ is cyclic, all the characters of the multiplicative group $\mathrm{GF}(q)^*$ are given by

$$\psi_j(\alpha^k) = e^{2\pi\sqrt{-1}jk/(q-1)}, \quad k = 0, 1, \cdots, q-2,$$

where $0 \leq j \leq q-2$ and α is a generator of $GF(q)^*$. These ψ_j are called *multiplicative characters* of $GF(q)$, and form a group of order $q-1$ with identity element ψ_0. The character $\psi_{(q-1)/2}$ is called the *quadratic character* of $GF(q)$, and is denoted by η in this paper. We extend this quadratic character by letting $\eta(0) = 0$.

The Gauss sum $G(\eta, \chi_1)$ over $GF(q)$ is defined by

$$G(\eta, \chi_1) = \sum_{c \in GF(q)^*} \eta(c)\chi_1(c) = \sum_{c \in GF(q)} \eta(c)\chi_1(c) \tag{5}$$

and the Gauss sum $G(\bar{\eta}, \bar{\chi}_1)$ over $GF(p)$ is defined by

$$G(\bar{\eta}, \bar{\chi}_1) = \sum_{c \in GF(p)^*} \bar{\eta}(c)\bar{\chi}_1(c) = \sum_{c \in GF(p)} \bar{\eta}(c)\bar{\chi}_1(c), \tag{6}$$

where $\bar{\eta}$ and $\bar{\chi}_1$ are the quadratic and canonical additive characters of $GF(p)$, respectively.

The following lemma is proved in [24, Theorem 5.15].

Lemma 5. *With the symbols and notation above, we have*

$$G(\eta, \chi_1) = (-1)^{m-1}\sqrt{-1}^{(\frac{p-1}{2})^2 m}\sqrt{q}$$

and

$$G(\bar{\eta}, \bar{\chi}_1) = \sqrt{-1}^{(\frac{p-1}{2})^2}\sqrt{p}.$$

We will need the following lemma [24, Theorem 5.33].

Lemma 6. *Let χ be a nontrivial additive character of $GF(q)$ with q odd, and let $f(x) = a_2 x^2 + a_1 x + a_0 \in GF(q)[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c \in GF(q)} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta, \chi).$$

The conclusion of the following lemma is straightforward. For completeness, we provide a proof below.

Lemma 7. *If $m \geq 2$ is even, then $\eta(y) = 1$ for each $y \in GF(p)^*$. If m is odd, then $\eta(y) = \bar{\eta}(y)$ for each $y \in GF(p)$.*

Proof: Let α be a generator of $GF(q)^*$. Notice that every $y \in GF(p)^*$ can be expressed as $\alpha^{\frac{q-1}{p-1}j}$, where $0 \leq j \leq p-2$. We have

$$\frac{q-1}{p-1} \bmod 2 = m \bmod 2.$$

Hence, every element $y \in GF(p)^*$ is a square in $GF(q)$ when m is an even positive integer, and $\eta(y) = \bar{\eta}(y)$ for each $y \in GF(p)$ when m is odd. This completes the proof. ∎

Below we prove a few more auxiliary results before proving the main results of this paper.

Lemma 8. *We have the following equality:*

$$\sum_{y \in GF(p)^*} \sum_{x \in GF(q)} \varepsilon_p^{y\text{Tr}(x^2)} = \begin{cases} 0 & \text{if } m \text{ odd,} \\ (-1)^{m-1}(-1)^{(\frac{p-1}{2})^2\frac{m}{2}}(p-1)\sqrt{q} & \text{if } m \text{ even.} \end{cases}$$

Proof: By Lemma 6, we have

$$\sum_{y \in GF(p)^*} \sum_{x \in GF(q)} \varepsilon_p^{y\text{Tr}(x^2)} = G(\eta, \chi_1) \sum_{y \in GF(p)^*} \eta(y).$$

Using Lemma 7, we obtain

$$\sum_{y\in \mathrm{GF}(p)^*} \eta(y) = \begin{cases} 0 & \text{if } m \text{ odd}, \\ p-1 & \text{if } m \text{ even}. \end{cases}$$

The desired conclusion then follows. ∎

The next lemma will be employed later.

Lemma 9. *For each $a \in \mathrm{GF}(p)$, let*

$$n_a = |\{x \in \mathrm{GF}(q) : \mathrm{Tr}(x^2) = a\}|.$$

Then

$$n_a = \begin{cases} p^{m-1} & \text{if } m \text{ odd and } a = 0, \\ p^{m-1} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)p^{\frac{m-2}{2}} & \text{if } m \text{ even and } a = 0, \\ p^{m-1} - \bar{\eta}(a)(-1)^{\frac{p-1}{2}}(-1)^{(\frac{p-1}{2})^2(\frac{m+1}{2})}p^{\frac{m-1}{2}} & \text{if } m \text{ odd and } a \neq 0, \\ p^{m-1} + (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}p^{\frac{m-2}{2}} & \text{if } m \text{ even and } a \neq 0. \end{cases}$$

Proof: It follows from Lemma 6 that

$$
\begin{aligned}
n_a &= \frac{1}{p} \sum_{x \in \mathrm{GF}(q)} \sum_{y \in \mathrm{GF}(p)} \varepsilon_p^{y(\mathrm{Tr}(x^2)-a)} \\
&= p^{m-1} + \frac{1}{p} \sum_{y \in \mathrm{GF}(p)^*} \varepsilon_p^{ya} \sum_{x \in \mathrm{GF}(q)} \varepsilon_p^{\mathrm{Tr}(yx^2)} \\
&= p^{m-1} + \frac{1}{p} G(\eta, \chi_1) \sum_{y \in \mathrm{GF}(p)^*} \varepsilon_p^{ya} \eta(y) \\
&= \begin{cases} p^{m-1} + \frac{1}{p} G(\eta, \chi_1) \sum_{y \in \mathrm{GF}(p)^*} \eta(y) & \text{if } a = 0 \\ p^{m-1} + \frac{1}{p}\eta(a) G(\eta, \chi_1) \sum_{z \in \mathrm{GF}(p)^*} \varepsilon_p^z \eta(z) & \text{if } a \neq 0 \end{cases} \\
&= \begin{cases} p^{m-1} & \text{if } m \text{ odd and } a = 0, \\ p^{m-1} + \frac{p-1}{p} G(\eta, \chi_1) & \text{if } m \text{ even and } a = 0, \\ p^{m-1} + \frac{\bar{\eta}(a)}{p} G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1) & \text{if } m \text{ odd and } a \neq 0, \\ p^{m-1} - \frac{1}{p} G(\eta, \chi_1) & \text{if } m \text{ even and } a \neq 0, \end{cases}
\end{aligned}
$$

where the first equality follows from the fact that $\sum_{y \in \mathrm{GF}(p)} \bar{\chi}_1(yz) = 0$ for every $z \in \mathrm{GF}(p)^*$. The desired conclusion then follows from Lemma 5. ∎

The following result will play an important role in proving the main results of this paper.

Lemma 10. *Let $b \in \mathrm{GF}(q)^*$. Then*

$$\sum_{y \in \mathrm{GF}(p)^*} \sum_{z \in \mathrm{GF}(p)^*} \sum_{x \in \mathrm{GF}(q)} \varepsilon_p^{\mathrm{Tr}(yx^2 + bzx)}$$

$$= \begin{cases} 0 & \text{if } m \text{ odd and } \mathrm{Tr}(b^2) = 0, \\ -\bar{\eta}(\mathrm{Tr}(b^2))(-1)^{(\frac{p-1}{2})^2(\frac{m+1}{2})}(p-1)p^{\frac{m+1}{2}} & \text{if } m \text{ odd and } \mathrm{Tr}(b^2) \neq 0, \\ -(-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)^2 p^{\frac{m}{2}} & \text{if } m \text{ even and } \mathrm{Tr}(b^2) = 0, \\ (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)p^{\frac{m}{2}} & \text{if } m \text{ even and } \mathrm{Tr}(b^2) \neq 0. \end{cases}$$

Proof: It follows from Lemmas 6 and 7 that

$$\sum_{y\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\sum_{x\in\mathrm{GF}(q)}\varepsilon_p^{\mathrm{Tr}(yx^2+bzx)}$$

$$= G(\eta,\chi_1)\sum_{y\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\chi_1\left(-\frac{b^2z^2}{4y}\right)\eta(y)$$

$$= G(\eta,\chi_1)\sum_{y_1\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\chi_1\left(-b^2z^2y_1\right)\eta\left(\frac{1}{4y_1}\right)$$

$$= G(\eta,\chi_1)\sum_{y_1\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\chi_1\left(-b^2z^2y_1\right)\eta\left(\frac{y_1}{(2y_1)^2}\right)$$

$$= G(\eta,\chi_1)\sum_{y\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\chi_1\left(-b^2z^2y\right)\eta(y)$$

$$= G(\eta,\chi_1)\sum_{y\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\varepsilon_p^{-z^2\mathrm{Tr}(b^2)y}\eta(y)$$

$$= \begin{cases} G(\eta,\chi_1)\sum_{z\in\mathrm{GF}(p)^*}\sum_{y\in\mathrm{GF}(p)^*}\eta(y) & \text{if }\mathrm{Tr}(b^2)=0 \\ G(\eta,\chi_1)\sum_{z\in\mathrm{GF}(p)^*}\sum_{y\in\mathrm{GF}(p)^*}\varepsilon_p^{-z^2\mathrm{Tr}(b^2)y}\eta(-z^2\mathrm{Tr}(b^2)y)\eta(-\mathrm{Tr}(b^2)) & \text{if }\mathrm{Tr}(b^2)\neq 0 \end{cases}$$

$$= \begin{cases} G(\eta,\chi_1)(p-1)\sum_{y\in\mathrm{GF}(p)^*}\eta(y) & \text{if }\mathrm{Tr}(b^2)=0 \\ G(\eta,\chi_1)\eta(-\mathrm{Tr}(b^2))(p-1)\sum_{y\in\mathrm{GF}(p)^*}\varepsilon_p^y\eta(y) & \text{if }\mathrm{Tr}(b^2)\neq 0 \end{cases}$$

$$= \begin{cases} 0 & \text{if }m\text{ odd and }\mathrm{Tr}(b^2)=0, \\ G(\eta,\chi_1)G(\bar\eta,\bar\chi_1)\eta(-\mathrm{Tr}(b^2))(p-1) & \text{if }m\text{ odd and }\mathrm{Tr}(b^2)\neq 0, \\ G(\eta,\chi_1)(p-1)^2 & \text{if }m\text{ even and }\mathrm{Tr}(b^2)=0, \\ -G(\eta,\chi_1)(p-1) & \text{if }m\text{ even and }\mathrm{Tr}(b^2)\neq 0. \end{cases}$$

The desired conclusions then follow from Lemmas 5 and 7. ∎

The last auxiliary result we need is the following.

Lemma 11. *For any $b\in\mathrm{GF}(q)^*$ and any $a\in\mathrm{GF}(p)$, let*

$$N(b) = |\{x\in\mathrm{GF}(q) : \mathrm{Tr}(x^2)=0 \text{ and } \mathrm{Tr}(bx)=0\}|.$$

Then

$$N(b) = \begin{cases} p^{m-2} & \text{if m odd and }\mathrm{Tr}(b^2)=0, \\ p^{m-2}-\bar\eta(\mathrm{Tr}(b^2))(-1)^{\left(\frac{p-1}{2}\right)^2\left(\frac{m+1}{2}\right)}(p-1)p^{\frac{m-3}{2}} & \text{if m odd and }\mathrm{Tr}(b^2)\neq 0, \\ p^{m-2}-(-1)^{\left(\frac{p-1}{2}\right)^2\frac{m}{2}}(p-1)p^{\frac{m-2}{2}} & \text{if m even and }\mathrm{Tr}(b^2)=0, \\ p^{m-2} & \text{if m even and }\mathrm{Tr}(b^2)\neq 0. \end{cases}$$

Proof: By definition, we have

$$N(b) = p^{-2}\sum_{x\in\mathrm{GF}(q)}\left(\sum_{y\in\mathrm{GF}(p)}\varepsilon_p^{y\mathrm{Tr}(x^2)}\right)\left(\sum_{z\in\mathrm{GF}(p)}\varepsilon_p^{z\mathrm{Tr}(bx)}\right)$$

$$= p^{-2}\sum_{z\in\mathrm{GF}(p)^*}\sum_{x\in\mathrm{GF}(q)}\varepsilon_p^{\mathrm{Tr}(bzx)}+p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\sum_{x\in\mathrm{GF}(q)}\varepsilon_p^{\mathrm{Tr}(yx^2)}+$$

$$p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\sum_{z\in\mathrm{GF}(p)^*}\sum_{x\in\mathrm{GF}(q)}\varepsilon_p^{\mathrm{Tr}(yx^2+bzx)}+p^{m-2}.$$

Note that

$$\sum_{z \in \mathrm{GF}(p)^*} \sum_{x \in \mathrm{GF}(q)} \varepsilon_p^{\mathrm{Tr}(bzx)} = 0.$$

The desired conclusions then follow from Lemmas 8 and 10. ∎

B. The proof of Theorems 1 and 2

It follows from Lemma 9 that the length n of the code $\mathcal{C}_D$ is given by

$$n = |D| = n_0 - 1 = \begin{cases} p^{m-1} - 1 & \text{if } m \text{ odd}, \\ p^{m-1} - 1 - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)p^{\frac{m-2}{2}} & \text{if } m \text{ even}. \end{cases}$$

For each $b \in \mathrm{GF}(q)^*$, define

$$\mathbf{c}_b = (\mathrm{Tr}(bd_1), \mathrm{Tr}(bd_2), \ldots, \mathrm{Tr}(bd_n)), \tag{7}$$

where $d_1, d_2, \ldots, d_n$ are the elements of D. The Hamming weight $\mathrm{wt}(\mathbf{c}_b)$ of $\mathbf{c}_b$ is $n_0 - N(b)$, where n_0 and $N(b)$ were defined before.

When m is odd, it follows from Lemmas 9 and 11 that

$$\mathrm{wt}(\mathbf{c}_b) = n_0 - N(b) = \begin{cases} (p-1)p^{m-2} & \text{if } \mathrm{Tr}(b^2) = 0, \\ (p-1)\left(p^{m-2} + \bar{\eta}(\mathrm{Tr}(b^2))(-1)^{(\frac{p-1}{2})^2(\frac{m+1}{2})}p^{\frac{m-3}{2}}\right) & \text{if } \mathrm{Tr}(b^2) \neq 0. \end{cases}$$

The desired conclusions of Theorem 1 then follow from Lemma 9 and the fact that $\mathrm{wt}(\mathbf{c}_b) > 0$ for each $b \in \mathrm{GF}(q)^*$.

When m is even, it follows from Lemmas 9 and 11 that

$$\mathrm{wt}(\mathbf{c}_b) = n_0 - N(b) = \begin{cases} (p-1)p^{m-2} & \text{if } \mathrm{Tr}(b^2) = 0, \\ (p-1)\left(p^{m-2} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}p^{\frac{m-2}{2}}\right) & \text{if } \mathrm{Tr}(b^2) \neq 0. \end{cases}$$

The desired conclusions of Theorem 2 then follow from Lemma 9 and the fact that $\mathrm{wt}(\mathbf{c}_b) > 0$ for each $b \in \mathrm{GF}(q)^*$.

IV. A GENERALIZATION OF THE CONSTRUCTION

Let f be a function from a finite abelian group $(A, +)$ to a finite abelian group $(B, +)$. A robust measure of nonlinearity of f is defined by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \frac{|\{x \in A : f(x+a) - f(x) = b\}|}{|A|}.$$

The smaller the value of P_f, the higher the corresponding nonlinearity of f.

It is easily seen that $P_f \geq \frac{1}{|B|}$ [7]. A function $f : A \to B$ has *perfect nonlinearity* if $P_f = \frac{1}{|B|}$. A perfect nonlinear function from a finite abelian group to a finite abelian group of the same order is called a *planar function* in finite geometry. Planar functions were introduced by Dembowski and Ostrom in 1968 for the construction of affine planes [12]. We refer to Carlet and Ding [7] for a survey of highly nonlinear functions, Coulter and Matthews [10] and Ding and Yuan [19] for information about planar functions.

Some known planar functions from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ are the following [7], [10]:

- $f(x) = x^2$.
- $f(x) = x^{p^k+1}$, where $m/\gcd(m,k)$ is odd (Dembowski and Ostrom [12]).
- $f(x) = x^{\frac{3^k+1}{2}}$, where $p = 3$, k is odd, and $\gcd(m,k) = 1$ (Coulter and Matthews [10]).

- $f_u(x) = x^{10} - ux^6 - u^2x^2$, where $p = 3$ and m is odd (Coulter and Matthews [10] for the case $u = -1$, Ding and Yuan [19] for the general case).

Note that planar functions over $\mathrm{GF}(p^m)$ exist for any pair (p, m) with p being an odd prime number.

The construction of the linear code $\mathcal{C}_D$ of this paper can be generalized as follows. Let f be a planar function from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ such that

- $f(0) = 0$;
- $f(x) = f(-x)$ for all $x \in \mathrm{GF}(q)$; and
- $f(ax) = a^h f(x)$ for all $a \in \mathrm{GF}(p)$ and $x \in \mathrm{GF}(q)$, where h is some constant.

Then the set

$$D_f := \{x \in \mathrm{GF}(q)^* : \mathrm{Tr}(f(x)) = 0\} \subset \mathrm{GF}(q)$$

defines a linear code $\mathcal{C}_{D_f}$ over $\mathrm{GF}(p)$. The code $\mathcal{C}_{D_f}$ may have the same parameters as the code $\mathcal{C}_D$ of this paper. Magma confirms that this is true for all the four classes of planar functions listed above. But it is open whether $\mathcal{C}_{D_f}$ and $\mathcal{C}_D$ have the same parameters and weight distribution for any planar function f satisfying the three conditions above. It would be nice if this open problem can be settled.

We remark that this construction of linear codes with planar functions here is different from the one in [8], as the lengths and dimensions of the codes in the two constructions are different.

V. APPLICATIONS OF THE LINEAR CODES IN SECRET SHARING SCHEMES

In this section, we describe and analyse the secret sharing schemes from some of the codes presented in this paper.

A. Secret sharing schemes

A secret sharing scheme consists of

- a dealer, and a group $\mathcal{P} = \{P_1, P_2, \cdots, P_\ell\}$ of ℓ participants;
- a secret space $\mathcal{S}$;
- ℓ share spaces $\mathcal{S}_1, \mathcal{S}_2, \cdots, \mathcal{S}_\ell$;
- a share computing procedure; and
- a secret recovering procedure.

The dealer will choose a secret s from the secret space $\mathcal{S}$, and will employ the sharing computing procedure to compute a share of the secret s for each participant P_i, and then give the share to P_i. The share computed for P_i belongs to the share space $\mathcal{S}_i$. When a subset of the participants comes together with their shares, they may be able to recover the secret s from their shares with the secret recovering procedure. The secret s and the sharing computing function are known only to the dealer, while the secret recovering procedure is known to all the participants.

By an *access set* we mean a group of participants who can determine the secret from their shares. The *access structure* of a secret sharing scheme is defined to be the set of all access sets. A *minimal access set* is a group of participants who can recover the secret with their shares, but any of its proper subgroups cannot do so. A secret sharing scheme is said to have the *monotone access structure*, if any superset of any access set is also an access set. In a secret sharing scheme with the monotone access structure, the access structure is totally characterized by its minimal access sets by definition. In this section, we deal with secret sharing schemes only with the monotone access structure.

Secret sharing schemes have applications in banking systems, cryptographic protocols, electronic voting systems, and the control of nuclear weapons. In 1979, Shamir and Blakley documented the first secret sharing schemes in the literature [4], [27].

B. The covering problem of linear codes

In order to describe the secret sharing scheme of a linear code, we need to introduce the covering problem of linear codes.

The *support* of a vector $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathrm{GF}(p)^n$ is defined as

$$\{0 \leq i \leq n-1 : c_i \neq 0\}.$$

We say that a vector $\mathbf{x}$ covers a vector $\mathbf{y}$ if the support of $\mathbf{x}$ contains that of $\mathbf{y}$ as a proper subset.

A *minimal codeword* of a linear code C is a nonzero codeword that does not cover any other nonzero codeword of C. The *covering problem* of a linear code is to determine all the minimal codewords of C. This is a very hard problem in general, but can be solved for certain types of linear codes.

C. A construction of secret sharing schemes from linear codes

Any linear code over $\mathrm{GF}(p)$ can be employed to construct secret sharing schemes [1], [8], [25], [28]. Given a linear code C over $\mathrm{GF}(p)$ with parameters $[n,k,d]$ and generator matrix $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$, we use $d^\perp$ and $H = [\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-1}]$ to denote the minimum distance and the generator matrix of its dual code $C^\perp$.

In the secret sharing scheme based on C, the secret space and the share spaces all are $\mathrm{GF}(p)$, and the participants are denoted by $P_1, P_2, \cdots, P_{n-1}$. To compute shares for all the participants, The dealer chooses randomly a vector $\mathbf{u} = (u_0, \ldots, u_{n-k-1})$ such that $s = \mathbf{u}\mathbf{h}_0$, which is the inner product of the two vectors. The dealer then treats $\mathbf{u}$ as an information vector and computes the corresponding codeword

$$\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) = \mathbf{u}H.$$

He then gives t_i to party P_i as his/her share for each $i \geq 1$.

The secret recovering procedure is the following. Note that $t_0 = \mathbf{u}\mathbf{h}_0 = s$. A set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the secret s iff $\mathbf{h}_0$ is a linear combination of $\mathbf{h}_{i_1}, \ldots, \mathbf{h}_{i_m}$. Suppose that

$$\mathbf{h}_0 = \sum_{j=1}^{m} x_j \mathbf{h}_{i_j}.$$

Then the secret s is recovered by computing

$$s = \sum_{j=1}^{m} x_j t_{i_j}.$$

Equivalently, we look for codewords $\mathbf{c}$ of the code C with the shape

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$$

Hence, the minimal access sets of the secret sharing scheme based on $C^\perp$ correspond to the minimal codewords in C having 1 as their leftmost component. The other nonzero components correspond to the participants in the minimal access set. For example, if $(1, 2, 0, 0, 2)$ is a codeword of C, then $\{P_1, P_4\}$ is a minimal access set. To obtain the access structure of the secret sharing scheme based on $C^\perp$, we need to determine all minimal codewords of C.

Note that the access structure of the secret sharing scheme based on $C^\perp$ is independent of the choice of the generator matrix H of $C^\perp$. We therefore say that the secret sharing scheme is based on $C^\perp$ without mentioning the matrix H. We would remind the reader that a linear code gives a pair of secret sharing schemes. One is based on C and the other is based on $C^\perp$. Below we consider only the latter due to symmetry.

The access structure of the secret sharing scheme based on a linear code is very complex in general, but can be determined in certain special cases. The following theorem is proved in [18], [30].

Theorem 12. *Let C be an $[n,k,d]$ code over $\mathrm{GF}(p)$, and let $G = [\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{n-1}]$ be its generator matrix. Let $d^\perp$ denote the minimum distance of its dual code $C^\perp$. If each nonzero codeword of C is minimal, then in the secret sharing scheme based on $C^\perp$, the total number of participants is $n-1$, and there are altogether p^{k-1} minimal access sets.*

- *When $d^\perp = 2$, the access structure is as follows.*
  If $\mathbf{g}_i$ is a multiple of $\mathbf{g}_0$, $1 \le i \le n-1$, then participant P_i must be in every minimal access set.
  If $\mathbf{g}_i$ is not a multiple of $\mathbf{g}_0$, $1 \le i \le n-1$, then participant P_i must be in $(p-1)p^{k-2}$ out of p^{k-1} minimal access sets.
- *When $d^\perp \ge 3$, for any fixed $1 \le t \le \min\{k-1, d^\perp - 2\}$ every group of t participants is involved in $(p-1)^t p^{k-(t+1)}$ out of p^{k-1} minimal access sets.*

When the conditions of Theorem 12 are satisfied, the secret sharing scheme based on the dual code $C^\perp$ is interesting. In the case that $d^\perp = 2$, some participants must be in every minimal access sets, and thus are dictators. Such a secret sharing scheme may be required in certain applications. In the case that $d^\perp \ge 3$, each participant plays the same role as he/she is involved in the same number of minimal access sets. Such a secret sharing scheme is said to be *democratic*, and may be needed in some other application scenarios.

A question now is how to construct a linear code whose nonzero codewords all are minimal. The following lemma provides a guideline in this direction [2], [3].

Lemma 13. *Every nonzero codeword of a linear code C over $\mathrm{GF}(p)$ is minimal, provided that*

$$\frac{w_{min}}{w_{max}} > \frac{p-1}{p},$$

where w_{max} and w_{min} denote the maximum and minimum nonzero weights in C, respectively.

D. The secret sharing schemes from the codes of this paper

In this subsection, we consider the secret sharing schemes based on the dual codes $C_D^\perp$ and $C_{\bar{D}}^\perp$ of the codes C_D and $C_{\bar{D}}$ presented in this paper.

For the code C_D of Theorem 1 and the code $C_{\bar{D}}$ of Corollary 3, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{p^{m-2} - p^{\frac{m-3}{2}}}{p^{m-2} + p^{\frac{m-3}{2}}} > \frac{p-1}{p}$$

if $m \ge 5$.

Let $m \equiv 0 \pmod 4$ or $m \equiv 0 \pmod 2$ and $p \equiv 1 \pmod 4$. Then for the code C_D of Theorem 2 and the code $C_{\bar{D}}$ of Corollary 4, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{p^{m-2} - p^{\frac{m-2}{2}}}{p^{m-2}} > \frac{p-1}{p}$$

if $m \ge 4$.

Let $m \equiv 2 \pmod 4$ and $p \equiv 1 \pmod 4$. Then for the code C_D of Theorem 2 and the code $C_{\bar{D}}$ of Corollary 4, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{p^{m-2}}{p^{m-2} + p^{\frac{m-2}{2}}} > \frac{p-1}{p}$$

if $m \ge 6$.

It then follows from Lemma 13 that all the nonzero codewords of C_D and $C_{\bar{D}}$ are minimal if $m \ge 6$. Hence, the secret sharing schemes based on the dual codes $C_D^\perp$ and $C_{\bar{D}}^\perp$ have the nice access structures described in Theorem 12.

As an example, we describe the access structure of the secret sharing scheme based on the dual code $\mathcal{C}_{\bar{D}}^{\perp}$ of the code $\mathcal{C}_{\bar{D}}$ of Corollary 3 as follows.

Corollary 14. *Let $m \geq 5$. In the secret sharing scheme based on the dual code $\mathcal{C}_{\bar{D}}^{\perp}$ of the code $\mathcal{C}_{\bar{D}}$ of Corollary 3, the total number of participants is p^{m-2}, and the total number of minimal access sets is p^{m-1}. Every participant is a member of exactly $(p-1)p^{m-2}$ minimal access sets.*

Proof: As proved above, every nonzero codeword of $\mathcal{C}_{\bar{D}}$ is minimal as $m \geq 5$. It can be easily proved that $d^{\perp} \geq 3$. The desired conclusions then follow from Theorem 12. ∎

As an example of Corollary 14, we have the following.

Example 5. *Let $m = 5$ and $p = 5$. In the secret sharing scheme based on the dual code $\mathcal{C}_{\bar{D}}^{\perp}$ of the code $\mathcal{C}_{\bar{D}}$ of Corollary 3, the total number of participants is 125, and the total number of minimal access sets is 625. Every participant is a member of exactly 500 minimal access sets.*

In the secret sharing scheme of Example 5, the secret space is GF(5), which is too small. However, it can still be employed for sharing a secret of any size. This is done as follows. One can have GF(5^h) as the extended secret space, where h could be as large as one wants (e.g., $h = 60$). Then any secret can be encoded as a sequence

$$s = s_1 s_2 \ldots s_h$$

using an encoding scheme, where each $s_i \in \text{GF}(5)$. Then the secret s can be shared by the 125 participants symbol by symbol with the secret sharing scheme of Example 5. Hence, the share for each participant will be a sequence of elements of GF(5) with length h. When a group of participants come together with their shares, the elements s_i in the secret s will be recovered one by one using the corresponding elements in their shares.

Finally, we mention that the secret sharing scheme based on the dual code $\mathcal{C}_{\bar{D}}^{\perp}$ of the code $\mathcal{C}_{\bar{D}}$ of Corollary 4 has a similar access structure as the one described in Corollary 14. For the linear codes of Theorems 1 and 2, their dual codes have minimum distance 2. Hence, the secret sharing scheme based on the dual code $\mathcal{C}_{\bar{D}}^{\perp}$ of the code $\mathcal{C}_{\bar{D}}$ in Theorems 1 and 2 have dictators in the whole group of participants. Their access structure is given in the first case of Theorem 12.

VI. CONCLUDING REMARKS

Calderbank and Kantor surveyed two-weight codes in [6]. There is a recent survey on three-weight cyclic codes [14]. Some interesting two-weight and three-weight codes were presented in [5], [11], [9], [21], [22], [23], [26], [29], and [31]. The length of the two-weight and three-weight codes in the literature usually divides $p^m - 1$, while that of the codes presented in this paper does not have this property. We did not find the parameters of the two-weight and three-weight codes of this paper in the literature.

The two-weight codes $\mathcal{C}_D$ of this paper give automatically strongly regular graphs having new parameters with the connection described in [6], and the three-weight codes $\mathcal{C}_D$ of this paper may yield association schemes having new parameters with the framework introduced in [5]. The linear codes of this paper can be employed to construct authentication codes having new parameters via the framework in [13], [17]. For this application, we need to know not only the weight distribution of the linear codes, but also the distribution of each element of GF(p) in each codeword of the linear code. This is called the *complete weight distribution* of a code. Another advantage of the linear codes in this paper is that their complete weight distribution can be settled with the help of Gaussian sums. In the literature the complete weight distribution of only a few classes of linear codes is known.

Compared with other two-weight and three-weight codes, the construction method of the codes in this paper is very simple and is defined by the simple function $\text{Tr}(x^2)$. This makes the analysis of the linear codes much easier.

ACKNOWLEDGEMENTS

REFERENCES

[1] R. Anderson, C. Ding, T. Helleseth and T. Kløve, "How to build robust shared control systems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp 111–124, 1998.

[2] A. Ashikhmin, A. Barg, G. Cohen and L. Huguet, "Variations on minimal codewords in linear codes, in *Proc. of AAECC 1995,* pp. 96–105, LNCS 948, Springer-Verlag, 1995.

[3] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Trans. Inform. Theory,* vol. 44, no. 5, pp. 2010–2017, 1998.

[4] G. R. Blakley, "Safeguarding cryptographic keys", in: *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317, 1979.

[5] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.*, vol. 39, pp. 143–152, 1984.

[6] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.*, vol. 18, pp. 97–122, 1986.

[7] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity,* vol. 20, no. 2, pp. 205–244, 2004.

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

[9] S.-T. Choi, J.-Y. Kim, J.-S. No and H. Chung, "Weight distribution of some cyclic codes," in: *Proc. of the 2012 International Symposium on Information Theory*, pp. 2911–2913, IEEE Press, 2012.

[10] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Designs, Codes and Cryptography,* vol. 10, pp. 167–184, 1997.

[11] B. Courteau and J. Wolfmann, "On triple-sum-sets and two or three weight codes," *Discrete Mathematics*, vol. 50, pp. 179–191, 1984.

[12] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2," *Math. Z.*, vol. 193, pp. 239–258, 1968.

[13] C. Ding, T. Helleseth, T. Kløve and X. Wang, "A general construction of authentication codes," *IEEE Trans. Inform. Theory,* vol. 53, no. 6, pp. 2229–2235, 2007.

[14] C. Ding, C. Li, N. Li and Z. Zhou, "Three-weight cyclic codes and their weight distributions," Preprint, 2014.

[15] C. Ding, J. Luo and H. Niederreiter, "Two weight codes punctured from irreducible cyclic codes," in: *Proc. of the First International Workshop on Coding Theory and Cryptography*, pp. 119–124. Singapore, World Scientific, 2008.

[16] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3", *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2274–2277, 2007.

[17] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," *Theoretical Computer Science*, vol. 330, pp. 81–99, 2005.

[18] C. Ding and J. Yuan, "Covering and secret sharing with linear codes," in: *Discrete Mathematics and Theoretical Computer Science,* pp. 11–25, LNCS 2731, Springer Verlag, 2003.

[19] C. Ding and J. Yuan, "A family of skew Paley-Hadamard difference sets," *J. of Combinatorial Theory A*, vol. 113, no. 7, pp. 1219–1592, 2006.

[20] M. van Eupen, "Some new results for ternary linear codes of dimension 5 and 6, *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 2048–2051, 1995.

[21] K. Feng and J. Luo, "Value distribution of exponential sums from perfect nonlinear functions and their applications," *IEEE Trans. Inform. Theory*, vol. 53, no. 9, pp. 3035–3041, 2007.

[22] C. Li, Q. Yue and F. Li, "Weight distributions of cyclic codes with respect to pairwise coprime order elements," *Finite Fields and Their Applications,* vol. 28, pp. 94–114, 2014.

[23] C. Li, Q. Yue and F. Li, "Hamming weights of the duals of cyclic codes with two zeros," *IEEE Trans. Inform. Theory,* vol. 60, no. 7, pp. 3895–3902, 2014.

[24] R. Lidl and H. Niederreiter, *Finite Fields,* Cambridge: Cambridge University Press, 1997.

[25] J. L. Massey, "Minimal codewords and secret sharing," in: *Proc. 6th Joint Swedish-Russian Workshop on Information Theory,* pp. 276–279, 1993.

[26] A. Rao and N. Pinnawala,"A family of two-weight irreducible cyclic codes," *IEEE Trans. Inform. Theory,* vol. 56, no. 6, pp. 2568–2570, 2010.

[27] A. Shamir, "How to share a secret," *Comm. ACM,* vol. 22, no. 11, pp. 612–613, 1979.

[28] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inform. Theory,* vol. 52, no. 1, pp. 206–212, 2006.

[29] Y. Xia, X. Zeng and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = (p^n + 1)/(p + 1) + (p^n - 1)/2$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, pp. 329–342, 2010.

[30] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 1, pp. 206–212, 2006.

[31] Z. Zhou and C. Ding, "A class of three-weight cyclic codes," *Finite Fields Appl.*, vol. 25, pp. 79–93, 2014.