Cunsheng Ding | Arto Salomaa

Secret Sharing Schemes with Nice Access Structures

Turku Centre *for* Computer Science

TUCS Technical Report
No 702, August 2005

Secret Sharing Schemes with Nice Access Structures

Cunsheng Ding
Department of Computer Science
The Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong, China
cding@cs.ust.hk
Arto Salomaa
Turku Centre for Computer Science
Lemminkäisenkatu 14, 20520 Turku, Finland
asalomaa@it.utu.fi

TUCS Technical Report
No 702, August 2005

Abstract

Secret sharing schemes, introduced by Blakley and Shamir independently in 1979, have a number of applications in security systems. One approach to the construction of secret sharing schemes is based on coding theory. In principle, every linear code can be used to construct secret sharing schemes. But only well structured linear codes give secret sharing schemes with nice access structures in the sense that every pair of participants plays the same role in the secret sharing. In this paper, we construct a class of good linear codes, and use them to obtain a class of secret sharing schemes with nice access structures.

Keywords: secret sharing schemes, linear codes, access structures

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Introduction

Since the introduction of secret sharing schemes by Blakley [4] and Shamir [18] in 1979, many constructions have been proposed. Two related constructions of secret sharing schemes from linear codes were developed. A relationship between Shamir's secret sharing scheme and the Reed-Solomon codes was pointed out by McEliece and Sarwate in 1981 [13]. Later several authors have considered the construction of secret sharing schemes using linear error correcting codes [1, 6, 8, 11, 12, 15, 16]. Massey utilized linear codes for secret sharing and pointed out a relationship between the access structure and the minimal codewords of the dual code of the underlying code [11, 12].

Several authors have investigated the minimal codewords for certain codes and characterized the access structures of the secret sharing schemes based on their dual codes [17, 2, 3, 19]. It is known that only well designed codes yield secret sharing schemes with nice access structures.

In this paper, we first construct a class of linear codes suitable for secret sharing, and then determine the access structure of the secret sharing schemes based on the duals of those linear codes. The secret sharing schemes obtained have nice access structures in the sense that every pair of participants plays the same role in the secret sharing.

2 A construction of secret sharing schemes from linear codes

The *Hamming weight* of a vector in $\mathrm{GF}(q)^n$ is defined to be the total number of nonzero coordinates. An $[n, k, d; q]$ code C is a linear subspace of $\mathrm{GF}(q)^n$ with dimension k and minimum nonzero Hamming weight d. Let $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$ be a generator matrix of an $[n, k, d; q]$ code, i.e., the row vectors of G generate the linear subspace C. Throughout this paper we assume that no column vector of any generator matrix is the zero vector for all the linear codes.

There are several ways to use linear codes to construct secret sharing schemes. One of them is the following described by Massey [11].

In the secret sharing scheme based on C, the secret is an element of $\mathrm{GF}(q)$, which is called the secret space, and $n-1$ participants $P_1, P_2, \cdots, P_{n-1}$ and a dealer are involved. The dealer is a trusted person.

In order to compute the shares with respect to a secret s, the dealer chooses randomly a vector $\mathbf{u} = (u_0, \ldots, u_{k-1}) \in \mathrm{GF}(q)^k$ such that $s = \mathbf{u}\mathbf{g}_0$. There are altogether q^{k-1} such vectors $\mathbf{u} \in \mathrm{GF}(q)^k$. The dealer then treats $\mathbf{u}$ as an information vector and computes the corresponding codeword

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

and gives t_i to participant P_i as share for each $i \geq 1$.

Since $t_0 = \mathbf{u}\mathbf{g}_0 = s$, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$, $1 \leq i_1 < \ldots < i_m \leq n-1$ and $1 \leq m \leq n-1$, determines the secret if and only if $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$.

Hence we have the following lemma [11].

Lemma 1 *Let G be a generator matrix of an $[n, k; q]$ code C. In the secret sharing scheme based on C, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$, $1 \leq i_1 < \ldots < i_m \leq n-1$ and $1 \leq m \leq n-1$, determines the secret if and only if there is a*

codeword

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

in the dual code $\mathsf{C}^{\perp}$*, where* $c_{i_j} \neq 0$ *for at least one* j*.*

If there is a codeword of (1) in $\mathsf{C}^{\perp}$, then the vector $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$, say, $\mathbf{g}_0 = \sum_{j=1}^{m} x_j \mathbf{g}_{i_j}$. Then the secret s is recovered by computing $s = \sum_{j=1}^{m} x_j t_{i_j}$.

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. A group of participants is referred to as a *minimal access set* if they can recover the secret with their shares, while any of its proper subgroups cannot do so. Here a proper subgroup has fewer members than the whole group. In view of these facts, we are only interested in the set of all minimal access sets. To determine this set, we need the notion of minimal codewords.

The *support* of a vector $\mathbf{c} \in \mathrm{GF}(q)^n$ is defined to be $\{0 \leq i \leq n-1 : c_i \neq 0\}$. A codeword $\mathbf{c}_2$ *covers* a codeword $\mathbf{c}_1$ if the support of $\mathbf{c}_2$ contains that of $\mathbf{c}_1$.

If a nonzero codeword $\mathbf{c}$ covers only its scalar multiples, but no other nonzero codewords, then it is called a *minimal codeword*.

¿From Lemma 1 and the discussions above, it is clear that there is a one-to-one correspondence between the set of minimal access sets and the set of minimal codewords of the dual code $\mathsf{C}^{\perp}$ whose first coordinate is 1. To determine the access structure of the secret sharing scheme, we need to determine only the set of minimal codewords whose first coordinate is 1, i.e., a subset of the set of all minimal codewords. However, in almost every case we should be able to determine the set of all minimal codewords as long as we can determine the set of minimal codewords whose first coordinate is 1. The *covering problem* of a linear code is to determine the set of all its minimal codewords.

It is clear that the shares for the participants depend on the selection of the generator matrix G of the code C. However, by Lemma 1 the selection of G does not affect the access structure of the secret sharing scheme. Therefore in the sequel we will call it the secret sharing scheme based on C, without mentioning the generator matrix used to compute the shares.

We say that a secret sharing scheme is *democratic of degree* t if every group of t participants is in the same number of minimal access sets, where $t \geq 1$.

3 The access structure of the secret sharing schemes based on the duals of the codes

Every linear code has the dual code. In Section 2, we described the secret sharing scheme based on a linear code C. Naturally, we have also the secret sharing scheme based on the dual code $\mathsf{C}^{\perp}$. In this and later sections, we consider only the secret sharing scheme based on the dual code of a given linear code. This should cause no confusion.

The following lemma describes properties of the minimal access sets of the secret sharing scheme based on $\mathsf{C}^{\perp}$ [7]. Note that the vectors $\mathbf{g}_i$ in this and later sections are not the same as those in Section 2.

Lemma 2 [7] *Let* C *be an* $[n, k; q]$ *code, and let* $G = [\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{n-1}]$ *be its generator matrix, where all* $\mathbf{g}_i$ *are nonzero. If each nonzero codeword of* C *is minimal, then in the secret sharing scheme based on* $\mathsf{C}^{\perp}$*, there are altogether* q^{k-1} *minimal access sets. In addition, we have the following:*

1. *If* $\mathbf{g}_i$ *is a scalar multiple of* $\mathbf{g}_0$, $1 \leq i \leq n-1$, *then participant* P_i *must be in every minimal access set. Such a participant is called a* dictatorial participant.

2. *If* $\mathbf{g}_i$ *is not a scalar multiple of* $\mathbf{g}_0$, $1 \leq i \leq n-1$, *then participant* P_i *must be in* $(q-1)q^{k-2}$ *out of* q^{k-1} *minimal access sets.*

In view of Lemma 2, it would be an interesting problem to construct codes whose nonzero codewords are all minimal. Such a linear code gives a secret sharing scheme with the interesting access structure described in Lemma 2.

If the weights of a linear code are close enough to each other, then all nonzero codewords of the code are minimal, as described below.

Lemma 3 (Ashikhmin-Barg [3]) *In an* $[n, k; q]$ *code* C, *let* w_{min} *and* w_{max} *be the minimum and maximum nonzero weights respectively. If*

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

then all nonzero codewords of C *are minimal.*

The Ashikhmin-Barg lemma is quite useful in determining the minimal codewords for special linear codes.

4 Group characters and bounds on character sums

In this section, we present some bounds on character sums which will be needed in the sequel. Consider the finite field GF(q), where $q = p^s, p$ is a prime, and s is a positive integer. The absolute trace function $\mathsf{Tr}_{q/p}$ from GF(q) to GF(p) is defined by

$$\mathsf{Tr}_{q/p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{s-1}}.$$

An *additive character* of GF(q) is a nonzero function χ from GF(q) to the set of 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

$$\chi_b(c) = e^{2\pi\sqrt{-1}\mathsf{Tr}_{q/p}(bc)/p} \quad \text{for all } c \in \mathrm{GF}(q) \tag{2}$$

defines an additive character of GF(q). When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of GF(q). The character χ_1 in (2) is called the *canonical additive character* of GF(q).

A *multiplicative character* of GF(q) is a nonzero function ψ from $\mathrm{GF}(q)^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for all pairs $(x, y) \in \mathrm{GF}(q)^* \times \mathrm{GF}(q)^*$. Let g be a fixed primitive element of GF(q). For each $j = 0, 1, \ldots, q-2$, the function ψ_j with

$$\psi_j(g^k) = e^{2\pi\sqrt{-1}jk/(q-1)} \quad \text{for } k = 0, 1, \ldots, q-2 \tag{3}$$

defines a multiplicative character of GF(q). When $j = 0$, $\psi_0(c) = 1$ for all $c \in \mathrm{GF}(q)^*$, and is called the *trivial multiplicative character* of GF(q).

Let q be odd and $j = (q-1)/2$ in (3). We then get a multiplicative character η such that $\eta(c) = 1$ if c is the square of an element and $\eta(c) = -1$ otherwise. This η is called the *quadratic character* of GF(q).

In this paper, we denote the canonical additive characters of GF(q) and GF(q^m) respectively by

$$\chi_1(x) = e^{2\pi\sqrt{-1}\mathrm{Tr}_{q/p}(x)/p},\ x \in \mathrm{GF}(q),$$
$$\chi_2(x) = e^{2\pi\sqrt{-1}\mathrm{Tr}_{q^m/p}(x)/p},\ x \in \mathrm{GF}(q^m);$$

and the quadratic characters of GF(q) and GF(q^m) respectively by η_1 and η_2.

Suppose α is a primitive element of GF(q^m). Then $\alpha' = \alpha^{(q^m-1)/(q-1)}$ is a primitive element of GF(q^m). We note that when q is odd, $(q^m-1)/(q-1) = \sum_{i=0}^{m-1} q^i$ is even if and only if m is even. Hence we have

$$\eta_2(x) = \begin{cases} 1 & \text{if } m \text{ is even,} \\ \eta_1(x) & \text{if } m \text{ is odd} \end{cases}$$

for all $x \in \mathrm{GF}(q)$.

Let ψ be a multiplicative and χ an additive character of GF(q). Then the *Gaussian sum* $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) = \sum_{c \in \mathrm{GF}(q)^*} \psi(c)\chi(c).$$

We have

$$G(\psi, \chi) = \begin{cases} q-1 & \text{for } \psi = \psi_0, \chi = \chi_0, \\ -1 & \text{for } \psi = \psi_0, \chi \neq \chi_0, \\ 0 & \text{for } \psi \neq \psi_0, \chi = \chi_0 \end{cases} \tag{4}$$

If $\psi \neq \psi_0$ and $\chi \neq \chi_0$, then $|G(\psi, \chi)| = q^{1/2}$. If $q = p^h$, where p is an odd prime and h is a positive integer, then

$$G(\eta, \chi_1) = \begin{cases} (-1)^{h-1} q^{1/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{h-1} (\sqrt{-1})^h q^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{5}$$

Let χ be a nontrivial additive character of GF(q) and let the polynomial $f \in \mathrm{GF}(q)[x]$ be of positive degree. Sums of the form $\sum_{c \in \mathrm{GF}(q)} \chi(f(c))$ are called *Weil sums*.

The following is referred to as Weil's bound [9].

Lemma 4 *Let $f \in \mathrm{GF}(q)[x]$ be of degree $m \geq 1$ with $\gcd(m, q) = 1$ and let χ be a nontrivial additive character of* GF(q). *Then*

$$\left| \sum_{c \in \mathrm{GF}(q)} \chi(f(c)) \right| \leq (m-1)q^{1/2}.$$

The following is useful in the sequel [9].

Lemma 5 *Let χ be a nontrivial additive character of* GF(q) *with q odd, and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathrm{GF}(q)[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c \in \mathrm{GF}(q)} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta, \chi). \tag{6}$$

5 The class of trace codes

Let $p \geq 5$ be a prime, m a positive integer, and $q = p^s$ for some positive integer s. For any $a, b, c \in \mathrm{GF}(q^m)$, define

$$f_{a,b,c}(x) = \mathsf{Tr}_{q^m/q}(ax^3 + bx^2 + cx),$$

which is a function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$.

We now define a linear code over $\mathrm{GF}(q)$ as

$$\mathsf{C}_{q,m} = \{\mathbf{c}_{a,b,c} = (f_{a,b,c}(\gamma_1), \cdots, f_{a,b,c}(\gamma_{q^m-1})) : a, b, c \in \mathrm{GF}(q^m)\}, \tag{7}$$

where $\gamma_1, \cdots, \gamma_{q^m-1}$ are all the nonzero elements of $\mathrm{GF}(p^m)$ arranged in some order.

Our task in this section is to study the code $\mathsf{C}_{q,m}$ and its dual. We shall determine the dimension and some weights of the code, and derive tight lower and upper bounds on the the minimum distance of the code.

Theorem 1 *Let $p \geq 5$. Then the code $\mathsf{C}_{q,m}$ of (7) has parameters $[q^m - 1, 3m, d; q]$ with*

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

Furthermore, we have the following conclusions.

1. *If m is even, then*

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

and the code $\mathsf{C}_{q,m}$ has codewords of the following weights:

$$(q-1)q^{m-1} \pm (q-1)q^{(m-2)/2}, (q-1)q^{m-1} \pm q^{(m-2)/2}, (q-1)q^{m-1}.$$

2. *If m is odd, then*

$$(q-1)\left(q^{m-1} - 2q^{(m-2)/2}\right) \leq d \leq (q-1)q^{m-1} - q^{(m-1)/2}$$

and the code $\mathsf{C}_{q,m}$ has codewords of the following weights:

$$(q-1)q^{m-1} \pm q^{(m-1)/2}, (q-1)q^{m-1}.$$

Proof. For any $a, b, c \in \mathrm{GF}(q^m)$, define

$$N_{a,b,c} = |\{x : f_{a,b,c}(x) = 0, x \in \mathrm{GF}(q^m)\}|.$$

Then the Hamming weight of the codeword $\mathbf{c}_{a,b,c}$ is equal to $q^m - N_{a,b,c}$.

By (4), we have

$$\begin{aligned}
qN_{a,b,c} &= \sum_{x \in \mathrm{GF}(q^m)} \sum_{y \in \mathrm{GF}(q)} \chi_1[y f_{a,b,c}(x)] \\
&= q^m + \sum_{y \in \mathrm{GF}(q)^*} \sum_{x \in \mathrm{GF}(q^m)} \chi_1[y f_{a,b,c}(x)] \\
&= q^m + \sum_{y \in \mathrm{GF}(q)^*} \sum_{x \in \mathrm{GF}(q^m)} \chi_1[\mathsf{Tr}_{q^m/q}(yax^3 + ybx^2 + ycx)] \\
&= q^m + \sum_{y \in \mathrm{GF}(q)^*} \sum_{x \in \mathrm{GF}(q^m)} \chi_2[yax^3 + ybx^2 + ycx]. \qquad (8)
\end{aligned}$$

If $a \neq 0$, it would be hard to derive a formula for $N_{a,b,c}$. In this case, we shall develop tight lower and upper bounds on $N_{a,b,c}$. If $a = 0$ but $b \neq 0$, we are able to give formulas for $N_{a,b,c}$.

We first consider the case that $a \neq 0$. In this case, by Lemma 4 and (8) we have

$$\begin{aligned} |qN_{a,b,c} - q^m| &= \left| \sum_{y \in \mathrm{GF}(q)^*} \sum_{x \in \mathrm{GF}(q^m)} \chi_2[yax^3 + ybx^2 + ycx] \right| \\ &\leq \sum_{y \in \mathrm{GF}(q)^*} \left| \sum_{x \in \mathrm{GF}(q^m)} \chi_2[yax^3 + ybx^2 + ycx] \right| \\ &\leq 2(q-1)q^{m/2}. \end{aligned} \tag{9}$$

Now we consider the case that $a = 0$ but $b \neq 0$. Similarly, by Lemma 4 and (8) we have

$$\begin{aligned} |qN_{0,b,c} - q^m| &= \left| \sum_{y \in \mathrm{GF}(q)^*} \sum_{x \in \mathrm{GF}(q^m)} \chi_2[ybx^2 + ycx] \right| \\ &\leq \sum_{y \in \mathrm{GF}(q)^*} \left| \sum_{x \in \mathrm{GF}(q^m)} \chi_2[ybx^2 + ycx] \right| \\ &\leq (q-1)q^{m/2}. \end{aligned} \tag{10}$$

Finally, we consider the case that $a = 0$, $b = 0$, but $c \neq 0$. In this case we have clearly

$$N_{0,0,c} = q^{m-1}. \tag{11}$$

Combining (9), (10), and (11), we obtain

$$q^{m-1} - 2(q-1)q^{(m-2)/2} \leq N_{a,b,c} \leq q^{m-1} + 2(q-1)q^{(m-2)/2} \tag{12}$$

if $(a, b, c) \neq (0, 0, 0)$. Hence the Hamming weight $\mathrm{HW}(\mathbf{c}_{a,b,c})$ of any nonzero codeword $\mathbf{c}_{a,b,c}$ satisfies that

$$(q-1)\left(q^{m-1} - 2q^{(m-2)/2}\right) \leq \mathrm{HW}(\mathbf{c}_{a,b,c}) \leq (q-1)\left(q^{m-1} + 2q^{(m-2)/2}\right). \tag{13}$$

This proves the lower bound on the minimum distance of the code.

Now it is time to derive the upper bounds on the minimum distance and determine some weights in the code. We consider the codewords $\mathbf{c}_{a,b,c}$ with $a = 0$, $b \in \mathrm{GF}(q)^*$, and $c \in \mathrm{GF}(q)$. Note that

$$f_{0,b,c}(x) = \mathsf{Tr}_{q^m/q}(bz^2) - \mathsf{Tr}_{q^m/q}(c^2/4b),$$

where $z = x + c/2b$. In this case, we have

$$N_{0,b,c} = |\{z \in \mathrm{GF}(q^m) : \mathsf{Tr}_{q^m/q}(bz^2) = \mathsf{Tr}_{q^m/q}(c^2/4b)\}|. \tag{14}$$

Define $g_\gamma(x) = \mathsf{Tr}_{q^m/q}(\gamma x^2)$ and

$$U_v(\gamma) = |\{x \in \mathrm{GF}(q^m) : g_\gamma(x) = v\}|.$$

Then we have

$$
\begin{aligned}
& qU_v(\gamma) \\
&= \sum_{x\in \mathrm{GF}(q^m)} \sum_{y\in \mathrm{GF}(q)} \chi_1[y(g_\gamma(x)-v)] \\
&= q^m + \sum_{y\in \mathrm{GF}(q)^*} \sum_{x\in \mathrm{GF}(q^m)} \chi_1[y(g_\gamma(x)-v)] \\
&= q^m + \sum_{y\in \mathrm{GF}(q)^*} \sum_{x\in \mathrm{GF}(q^m)} \chi_1[\mathsf{Tr}_{q^m/q}(\gamma y x^2 - vy)] \\
&= q^m + \sum_{y\in \mathrm{GF}(q)^*} \sum_{x\in \mathrm{GF}(q^m)} \chi_2[\gamma y x^2 - vy] \\
&= q^m + G(\eta_2,\chi_2) \sum_{y\in \mathrm{GF}(q)^*} \chi_2[-vy]\eta_2[\gamma y] \\
&= \begin{cases} q^m + G(\eta_2,\chi_2)\eta_2(\gamma)\sum_{y\in \mathrm{GF}(q)^*}\eta_2[y] & v=0 \\ q^m + G(\eta_2,\chi_2)\eta_2(-v\gamma)\sum_{z\in \mathrm{GF}(q)^*}\chi_2[z]\eta_2[z] & v\neq 0 \end{cases} \\
&= \begin{cases} q^m + (q-1)\eta_2(\gamma)G(\eta_2,\chi_2) & v=0, m \text{ even} \\ q^m & v=0, m \text{ odd} \\ q^m + \eta_2(-v\gamma)G(\eta_2,\chi_2)\sum_{z\in \mathrm{GF}(q)^*}\chi_2[z] & v\neq 0, m \text{ even} \\ q^m + \eta_2(-v\gamma)G(\eta_2,\chi_2)G(\eta_1,\chi_1) & v\neq 0, m \text{ odd} \end{cases} \qquad (15) \\
&= \begin{cases} q^m - (q-1)q^{m/2}\eta_2(\gamma) & v=0, m \text{ even}, p\equiv 1 \pmod 4 \\ q^m + (-1)^{ms/2+1}(q-1)q^{m/2}\eta_2(\gamma) & v=0, m \text{ even}, p\equiv 3 \pmod 4 \\ q^m & v=0, m \text{ odd} \\ q^m + q^{m/2}\eta_2(\gamma)\eta_2(-v) & v\neq 0, m \text{ even}, p\equiv 1 \pmod 4 \\ q^m - (-1)^{ms/2}q^{m/2}\eta_2(\gamma)\eta_2(-v) & v\neq 0, m \text{ even}, p\equiv 3 \pmod 4 \\ q^m + q^{(m+1)/2}\eta_2(\gamma)\eta_2(-v) & v\neq 0, m \text{ odd}, p\equiv 1 \pmod 4 \\ q^m + (-1)^{(m+1)s/2}q^{(m+1)/2}\eta_2(\gamma)\eta_2(-v) & v\neq 0, m \text{ odd}, p\equiv 3 \pmod 4 \end{cases}
\end{aligned}
$$

Note that $\mathbf{c}_{0,0,c}$ has Hamming weight $(q-1)q^{m-1}$ for any $c\in \mathrm{GF}(q^m)^*$.

Clearly, $\eta_2(\gamma)$ takes on both ± 1 when γ ranges over $\mathrm{GF}(q^m)^*$. It then follows from (15) that when m is even $U_v(\gamma)$ takes on all the values

$$q^{m-1} \pm (q-1)q^{(m-2)/2}, q^{m-1} \pm q^{(m-2)/2}.$$

Hence in this case, by (14) $\mathsf{C}_{q,m}$ has codewords of the following weights:

$$(q-1)q^{m-1} \pm (q-1)q^{(m-2)/2}, (q-1)q^{m-1} \pm q^{(m-2)/2}, (q-1)q^{m-1}.$$

The conclusions for the case that m is odd follow similarly from (14) and (15).

We now prove that the dimension of the code is $3m$. For any two pairs (a_1,b_1,c_1) and (a_2,b_2,c_2), if $\mathbf{c}_{a_1,b_1,c_1} = \mathbf{c}_{a_2,b_2,c_2}$, then we have

$$(a_1-a_2)x^3 + (b_1-b_2)x^2 + (c_1-c_2)x = 0$$

for all $x\in \mathrm{GF}(q^m)$. It then follows from $p\geq 5$ that $(a_1,b_1,c_1) = (a_2,b_2,c_2)$. Hence C has q^{3m} distinct codewords, and thus dimension $3m$.

This completes the proof of this theorem.

Theorem 2 *The dual code $\mathsf{C}_{q,m}^{\perp}$ has parameters $[q^m-1, q^m-3m-1, 4; q]$.*

Proof. Let $d^\perp$ denote the minimum distance of $\mathsf{C}_{q,m}^\perp$. Clearly, $d^\perp \neq 1$. We first prove that $d^\perp \neq 2$. Let x_1 and x_2 be two distinct nonzero elements of $\mathrm{GF}(q^m)$. Suppose that there is a $u \in \mathrm{GF}(q)^*$ such that

$$\mathsf{Tr}_{q^m/q}(ax_1^3 + bx_1^2 + cx_1) = u\mathsf{Tr}_{q^m/q}(ax_2^3 + bx_2^2 + cx_2)$$

for all $(a, b, c) \in \mathrm{GF}(q^m)^3$. Then we have

$$x_1 = ux_2,\ x_1^2 = ux_2^2,\ x_1^3 = ux_2^3.$$

It follows that $u = 1$ and hence $x_1 = x_2$. This is contrary to the assumption that x_1 and x_2 are distinct. This proves that $d^\perp \neq 2$.

Then we prove that $d^\perp \neq 3$. Suppose $\mathsf{C}^\perp$ has a codeword of Hamming weight 3. Then there are three pairwise distinct elements x_1, x_2, x_3 of $\mathrm{GF}(q^m)^*$ and two elements u and v of $\mathrm{GF}(q)^*$ such that

$$\begin{cases} x_1 + ux_2 + vx_3 = 0, \\ x_1^2 + ux_2^2 + vx_3^2 = 0, \\ x_1^3 + ux_2^3 + vx_3^3 = 0. \end{cases} \tag{16}$$

Set $x = x_2/x_1$ and $y = x_3/x_1$. Then (16) becomes

$$\begin{cases} 1 + ux + vy = 0, \\ 1 + ux^2 + vy^2 = 0, \\ 1 + ux^3 + vy^3 = 0. \end{cases} \tag{17}$$

The first two equations of (16) give

$$u = \frac{y-1}{x(x-y)}, \quad v = \frac{x-1}{y(y-x)}.$$

Substituting the u and v in the last equation of (16) yields

$$(x-1)(y-1) = 0.$$

Hence $x = 1$ or $y = 1$. This is contrary to the fact that x_1, x_2 and x_3 are pairwise distinct. Thus $\mathsf{C}_{q,m}^\perp$ has no codeword of Hamming weight 3.

Now we prove that $d^\perp = 4$. It suffices to prove that $\mathsf{C}_{q,m}^\perp$ has a codeword of Hamming weight 4. Since $q \geq 5$, we can select three pairwise distinct elements x, y, z in $\mathrm{GF}(q) \setminus \{0, 1\}$. Define

$$\begin{aligned} u &= -\frac{(y-1)(z-1)}{x(x-y)(z-x)} \in \mathrm{GF}(q), \\ v &= -\frac{(x-1)(z-1)}{y(x-y)(z-y)} \in \mathrm{GF}(q), \\ w &= -\frac{(x-1)(y-1)}{z(y-z)(z-x)} \in \mathrm{GF}(q). \end{aligned}$$

It is easily checked that (u, v, w) is a solution to the following set of equations:

$$\begin{cases} 1 + ux + vy + wz = 0, \\ 1 + ux^2 + vy^2 + wz^2 = 0, \\ 1 + ux^3 + vy^3 + wz^2 = 0. \end{cases}$$

Assume that

$$\gamma_{i_1} = 1, \gamma_{i_2} = u, \gamma_{i_3} = v, \gamma_{i_4} = w.$$

Then the i_1th, i_2th, i_3th and i_4th columns of the code $\mathsf{C}_{p,m}$ are linearly dependent (with coefficients 1, u, v and w). Thus $\mathsf{C}_{q,m}^{\perp}$ must have a codeword of Hamming weight 4. This completes the proof.

In general, the codes $\mathsf{C}_{p,m}$ are very good. To justify this, we now give two examples of the codes. When $(q,m) = (5,2)$, the code $\mathsf{C}_{5,2}$ has parameters $[24, 6, 12; 5]$ with weight distribution

$$1 + 104x^{12} + 1404x^{16} + 1536x^{17} + 3024x^{18} + 1824x^{19}$$

$$+3624x^{20} + 2496x^{21} + 960x^{22} + 576x^{23} + 76x^{24}.$$

The dual code $\mathsf{C}_{5,2}^{\perp}$ has parameters $[24, 18, 4; 5]$.

When $(q,m) = (5,3)$, the code $\mathsf{C}_{5,3}$ has parameters $[124, 9, 90; 5]$ with weight distribution

$$1 + 147560x^{90} + 468720x^{95} + 930124x^{100} + 362080x^{105} + 44640x^{110}.$$

This code is the best code known with these parameters.

6 The access structure of the secret sharing schemes based on the dual codes

Theorem 3 *If $m \geq 4$ and $p \geq 5$, then all nonzero codewords of $\mathsf{C}_{p,m}$ are minimal. Furthermore, in the secret sharing scheme based on $\mathsf{C}_{p,m}^{\perp}$ every participant is in $(q-1)q^{3m-2}$ out of q^{3m-1} minimal access sets.*

Proof. If $m \geq 4$ and $p \geq 5$, by Theorem 1 we have

$$\frac{w_{min}}{w_{max}} \geq \frac{(q-1)(q^{m-1} - 2q^{(m-2)/2})}{(q-1)(q^{m-1} + 2q^{(m-2)/2})} > \frac{q-1}{q}.$$

It then follows from Lemma 3 that all nonzero codewords of $\mathsf{C}_{p,m}$ are minimal. The second conclusion then follows from Theorem 2 and Lemma 2.

With the help of Theorem 17 in [5], we can prove that in the secret sharing scheme based on $\mathsf{C}_{p,m}^{\perp}$, every group of two participants is involved in the same number of minimal access sets. Hence the access structure is democratic of degree 2.

Acknowledgement. Cunsheng Ding was supported by the Research Grants Council of the Hong Kong Special Administrative Region, Project Number HKUST6183/04E.

References

[1] Anderson, R. J., Ding, C., Helleseth, T., Kløve, T.: How to build robust shared control systems, *Designs, Codes and Cryptography,* **15**, 1998, 111–124.

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

[3] Ashikhmin, A., Barg, A.: Minimal vectors in linear codes, *IEEE Trans. Information Theory,* **44**(5), 1998, 2010–2017.

[4] Blakley, G. R.: Safeguarding cryptographic keys, *Proc. NCC AFIPS,* 1979, 313–317.

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

[6] Ding, C., Kohel, D., Ling, S.: Secret sharing with a class of ternary codes, *Theoretical Computer Science*, **246**, 2000, 285–298.

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

[8] Karnin, E. D., Greene, J. W., Hellman, M. E.: On secret sharing systems, *IEEE Trans. Information Theory,* **29**, 1983, 35–41.

[9] Lidl, L., Niederreiter, H.: *Finite Fields,* Cambridge University Press, 1997.

[10] Macwilliams, F. J., Sloane, N. J. A.: *The Theory of Error Correcting Codes,* North-Holland, Amsterdam, 1978.

[11] Massey, J. L.: Minimal codewords and secret sharing, *Proc. 6th Joint Swedish-Russian Workshop on Information Theory,* August 22-27, 1993, 276–279.

[12] Massey, J. L.: Some applications of coding theory, *Cryptography, Codes and Ciphers: Cryptography and Coding IV,* Formara Ltd, Esses, England, 1995, 33–47.

[13] McEliece, R. J., Sarwate, D. V.: On sharing secrets and Reed-Solomon codes, *Comm. ACM*, **24**, 1981, 583–584.

[14] Moreno, C., Moreno, O.: Exponential sums and Goppa Codes, *Proc. of the American Mathematical Society,* **111**, 1991, 523–531.

[15] Okada, K., Kurosawa, K.: MDS secret sharing scheme secure against cheaters, *IEEE Trans. Inform. Theory*, **46**(3), 2000, 1078–1081.

[16] Pieprzyk, J., Zhang, X. M.: Ideal Threshold Schemes from MDS Codes, *Information Security and Cryptology - Proc. of ICISC 2002,* LNCS 2587, Springer Verlag, Berlin, 2003, 269–279.

[17] Renvall, A., Ding, C.: The access structure of some secret-sharing schemes, *Information Security and Privacy,* LNCS 1172, Springer-Verlag, Berlin, 1996, 67–78.

[18] Shamir, A.: How to share a secret, *Comm. ACM,* **22**, 1979, 612–613.

[19] Yuan, J., Ding, C.: Secret sharing schemes from two-weight codes, *Discrete Mathematics*, to appear.

Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
- Institute of Information Systems Sciences

ISBN 952-12-1586-0
ISSN 1239-1891