Secret-sharing with a class of ternary codes

Kohel, David R.; Ding, Cunsheng; Ling, San

2000

Ding, C., Kohel, D. R., & Ling, S. (2000). Secret-sharing with a class of ternary codes. Theoretical Computer Science, 246(1-2), 285-298.

https://hdl.handle.net/10356/96090

https://doi.org/10.1016/S0304-3975(00)00207-3

Secret-sharing with a class of ternary codes

Cunsheng Ding[a], David R Kohel[b], San Ling[c,*]

[a] *Department of Computer Science, National University of Singapore, Science Drive 2, Singapore 117543, Singapore*

[b] *School of Mathematics and Statistics, Carslaw Building, F7, University of Sydney, Sydney, NSW 2006, Australia*

[c] *Department of Mathematics, National University of Singapore, Science Drive 2, Singapore 117543, Singapore*

Abstract

Secret-sharing is an important topic of cryptography and has applications in information security. One approach to the construction of secret-sharing schemes is based on error-correcting codes. In this paper, we describe a secret-sharing scheme based on a class of ternary codes (Ding et al. IEEE Trans. Inform. Theory IT-46 (2000) 280–284). We determine the access structure and prove properties of the secret-sharing scheme.

Keywords: Group character codes; Secret sharing; Cryptography

1. Introduction

In a secret-sharing scheme, a dealer has a secret. The dealer gives each party in the scheme a share of the secret. Let $\mathbf{P}$ denote the set of parties involved in the secret-sharing. There is a set $\Gamma \subseteq 2^{\mathbf{P}}$ such that any subset of parties that is in Γ can determine the secret and no subset in $2^{\mathbf{P}} \backslash \Gamma$ can determine the secret. The set Γ is called the *access structure* of the secret-sharing scheme.

The first construction of secret-sharing schemes was done by Blakley [3] and Shamir [14]. Since then many other schemes have been proposed and studied. Two kinds of

* Corresponding author.

E-mail addresses: dingcs@comp.nus.edu.sg (C. Ding), kohel@maths.usyd.edu.au (D.R. Kohel), lings@math.nus.edu.sg (S. Ling).

approaches to the construction of secret-sharing schemes based on linear codes have been so far considered (see [9–12, 1, 4, 15]). The relations between secret-sharing and codes based on the Chinese Remainder Theorem are dealt with by Ding et al. in [6, Chapter 7].

The access structure of secret-sharing schemes based on error-correcting codes depends on the weight distribution of their dual codes. In fact, the determination of the access structure of those secret-sharing schemes requires more than the knowledge of the weight distribution. This makes it rather difficult to determine the access structure of secret-sharing schemes based on codes, as determining the weight distribution of codes is a very hard problem in general. Note that the weight distribution of only a few classes of codes is known. In principle, every error-correcting linear code can be used to construct secret-sharing scheme. The question is how to determine the access structure.

In this paper, we describe a secret-sharing scheme based on a class of ternary codes which is described and analyzed by Ding et al. [5]. We determine the access structure of the secret-sharing schemes and prove their properties. The access structure of this secret-sharing scheme is richer, compared with the schemes based on some two weight geometric codes [1]. We are able to determine the access structure of our secret-sharing scheme because the structure of the underlying error-correcting ternary codes is fully understood [5].

2. The general secret-sharing scheme based on codes

Recall that a code of length N over $GF(q)$ is a nonempty subset of $GF(q)^N$. An $[N,k;q]$ linear code is a k-dimensional subspace of $GF(q)^N$. The elements of a code are called *codewords*. The (*Hamming*) *weight* of a codeword $\mathbf{c}$, denoted $\mathrm{wt}(\mathbf{c})$, is the number of nonzero positions in $\mathbf{c}$. The *minimum distance* d of the code is the smallest (Hamming) distance between any two distinct codewords. Because of linearity, this is also the smallest weight of a nonzero codeword. Sometimes we include d in the notation and describe the code as an $[N,k,d;q]$ code. A generator matrix G of an $[N,k;q]$ code C is a $k \times N$ matrix over $GF(q)$ whose rows form a basis for C.

One approach to the construction of secret-sharing schemes based on linear codes is as follows. Choose an $[N,k;q]$ code C such that its dual code $C^{\perp}$ has no codeword of Hamming weight one. Let G be a generator matrix of C. Let $s \in GF(q)$ denote the secret, and $\mathbf{g}_0 = (g_{00}, g_{10}, \ldots, g_{k-1,0})^{\mathrm{T}}$ be the first column of the generator matrix G. Then the information vector $\mathbf{u} = (u_0, \ldots, u_{k-1})$ is chosen to be any vector of $GF(q)^k$ such that $s = \mathbf{u}\mathbf{g}_0 = \sum_{i=0}^{k-1} u_i g_{i0}$.

The codeword corresponding to this information vector $\mathbf{u}$ is

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

We give t_i to the party p_i as their share for each $i \geqslant 1$, and the first component $t_0 = s$ of the codeword $\mathbf{t}$ is the secret. So the number of parties involved in this secret-sharing scheme is $N-1$.

It is not hard to prove that in the secret-sharing scheme based on a generator matrix $G = [\mathbf{g}_0 \mathbf{g}_1, \ldots, \mathbf{g}_{N-1}]$ of an $[N, k; q]$ linear code such that $\mathbf{g}_0$ is a linear combination of the other $N-1$ columns $\mathbf{g}_1, \ldots, \mathbf{g}_{N-1}$, the secret t_0 is determined by the set of shares $\{t_{i_1}, \ldots, t_{i_m}\}$ if and only if $\mathbf{g}_0$ is a linear combination of the vectors $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$, where $1 \leqslant i_1 < \cdots < i_m \leqslant N-1$ and $m \leqslant N-1$.

Computing the secret is straightforward: solve the linear equation

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

to find x_j, and the secret is then given by

$$t_0 = \mathbf{u}\mathbf{g}_0 = \sum_{j=1}^{m} x_j \mathbf{u}\mathbf{g}_{i_j} = \sum_{j=1}^{m} x_j t_{i_j}.$$

Secret-sharing schemes based on this general approach were considered by Karnin et al. [7], and Massey [9, 10]. The approach of McEliece and Sarwate is different but closely related [11].

For secret-sharing schemes based on the Karnin–Green–Hellman approach, Massey introduced the concept of minimal codewords and characterized the resulting access structures [9, 10]. We state his characterization in the following lemma which will be needed in later sections.

Lemma 1. *Let G be a generator matrix of an $[N, k; q]$ code C whose dual code $C^{\perp}$ does not have any codeword of Hamming weight 1. In the secret-sharing scheme based on G, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the secret if and only if there is a codeword*

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

in the dual code $C^{\perp}$, where $c_{i_j} \neq 0$ for at least one j, $1 \leqslant i_1 < \cdots < i_m \leqslant N-1$ and $1 \leqslant m \leqslant N-1$.

Here we would point out that this lemma was incorrectly stated in [1, 12], but other results in the two references are still correct.

We also mention the fact that for secret-sharing schemes based on the above approach, a set of shares either determines the secret or gives no information about it, i.e., such schemes are *perfect*. This fact and Lemma 1 will be used to determine the access structure of our secret-sharing scheme later. The access structure of secret-sharing schemes based on error-correcting codes is closely related to the parameters of the codes. For details, we refer to [12].

3. The class of ternary codes

Note that $(GF(2)^n, +)$ is an additive Abelian group of exponent 2 and order $N = 2^n$, with $\mathbf{0}$ as the identity element. From now on we assume that $n \geqslant 2$. Let M denote the multiplicative group of characters from $GF(2)^n$ to $GF(3)^*$. The group M is isomorphic non-canonically to $GF(2)^n$ [13, Chapter 6]. In particular we have $|M| = |GF(2)^n| = N = 2^n$.

The set $GF(2)^n$ may be identified with the set of integers $\{i : 0 \leqslant i \leqslant 2^n - 1\}$: the element $(i_0, i_1, \ldots, i_{n-1})$ of $GF(2)^n$ is identified with $i = i_0 + i_1 2 + \cdots + i_{n-1} 2^{n-1}$, where each i_j is 0 or 1. We also say that $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i.

We define

$$f_i(y) = (-1)^{i_0 y_0 + i_1 y_1 + \cdots + i_{n-1} y_{n-1}}, \tag{1}$$

where $y = (y_0, y_1, \ldots, y_{n-1}) \in GF(2)^n$, and $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i. It is easy to check that, for all i with $0 \leqslant i \leqslant 2^n - 1$, this gives all the 2^n characters from $GF(2)^n$ to $GF(3)^*$ with f_0 as the trivial character, so $M = \{f_0, f_1, \ldots, f_{2^n-1}\}$. Since we identify i and y with their respective binary representation, we have $f_i(y) = f_y(i)$.

For any subset X of $GF(2)^n$, the group character code C_X over $GF(3)$ described by Ding et al. [5] is

$$C_X = \left\{ (c_0, c_1, \ldots, c_{N-1}) \in GF(3)^N : \sum_{i=0}^{N-1} c_i f_i(x) = 0 \text{ for all } x \in X \right\}.$$

Let $X = \{x_0, x_1, \ldots, x_{t-1}\}$ be a subset of $GF(2)^n$ and let X^c be the complement of X in $GF(2)^n$, indexed such that $GF(2)^n = \{x_0, x_1, \ldots, x_{N-1}\}$.

Proposition 2 (Ding et al. [5, Proposition 2 and Section 3]). *Let X be as above. For $0 \leqslant i \leqslant N - 1$, let $\mathbf{v}_i$ denote the vector*

$$(f_0(x_i), f_1(x_i), \ldots, f_{N-1}(x_i)).$$

Then the set $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{N-1}\}$ is linearly independent. In particular,

$$H = [f_{j-1}(x_{i-1})]_{1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant N}$$

has rank t and is a parity check matrix of C_X,

$$G = [f_{j-1}(x_{t-1+i})]_{1 \leqslant i \leqslant N-t,\ 1 \leqslant j \leqslant N}$$

has rank $N - t$ and is a generator matrix for C_X, so C_X is an $[N, N - t]$ linear code over $GF(3)$. Moreover, H is a generator matrix for C_{X^c} and $C_X \oplus C_{X^c} = GF(3)^N$.

Definition. The Hamming weight of a vector $\mathbf{a}$ of $GF(2)^n$, denoted $\mathrm{wt}(\mathbf{a})$, is defined to be the number of its nonzero coordinates. For $-1 \leqslant r \leqslant n$, let $X(r, n) = \{\mathbf{a} \in GF(2)^n :$

Table 1
The weight distribution in $C_3(1,\ n)$

Range of m $0 \leqslant m \leqslant n$	Weight	Frequency	Codeword type $1 \leqslant i_k \leqslant n$
$m \equiv 0 \pmod 3$	$2^n - 2^{n-m}\frac{2^m + (-1)^{m/3}2}{3}$	$\binom{n}{m}2^m$	$\sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$
$m \equiv 0 \pmod 3$	$2^n - 2^{n-m}\frac{2^m - (-1)^{m/3}}{3}$	$\binom{n}{m}2^{m+1}$	$a\mathbf{v}_0 + \sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$
$m \equiv 1 \pmod 3$	$2^n - 2^{n-m}\frac{2^m - (-1)^{(m-1)/3}2}{3}$	$\binom{n}{m}2^m$	$\sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$
$m \equiv 1 \pmod 3$	$2^n - 2^{n-m}\frac{2^m + (-1)^{(m-1)/3}}{3}$	$\binom{n}{m}2^{m+1}$	$a\mathbf{v}_0 + \sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$
$m \equiv 2 \pmod 3$	$2^n - 2^{n-m}\frac{2^m + (-1)^{(m-2)/3}2}{3}$	$\binom{n}{m}2^m$	$\sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$
$m \equiv 2 \pmod 3$	$2^n - 2^{n-m}\frac{2^m - (-1)^{(m-2)/3}}{3}$	$\binom{n}{m}2^{m+1}$	$a\mathbf{v}_0 + \sum_{k=1}^{m} a_k \mathbf{v}_{i_k}$

$\mathrm{wt}(\mathbf{a}) > r\}$, and let $C_3(r,n)$ denote the code $C_{X(r,n)}$ over $GF(3)$. For a word $\mathbf{c} = (c_0, \ldots, c_{2^n-1})$ in $GF(3)^{2^n}$, let the support of $\mathbf{c}$ be defined as

$$\mathrm{Supp}(\mathbf{c}) = \{i : 0 \leqslant i < 2^n, \text{ and } c_i \neq 0\}.$$

By convention we define the minimum distance of the zero code to be ∞.

Proposition 3 (Ding et al. [5]). *The following properties of the codes $C_3(r,n)$ are known*:
(A) *$C_3(r,n)$ is a $[2^n, \sum_{j=0}^{r}\binom{n}{j}, 2^{n-r}]$ ternary code.*
(B) *The minimum nonzero weight codewords generate $C_3(r,n)$.*
(C) *The dual code $C_3(r,n)^{\perp}$ is equivalent to $C_3(n-r-1,n)$.*

In the sequel we define $\mathbf{v}_0 = (1,1,\ldots,1) \in GF(3)^n$ and

$$\mathbf{v}_i = (f_0(\mathbf{e}_i), f_1(\mathbf{e}_i), \ldots, f_{N-1}(\mathbf{e}_i))$$

for all $1 \leqslant i \leqslant n$, where $\mathbf{e}_i$ is the vector of $GF(2)^n$ whose ith coordinate is 1 and other coordinates are all zero.

Proposition 4 (Ding et al. [5]). *The weight distribution in the code $C_3(1,n)$ is given in Table* 1, *where all the a and a_i are nonzero elements of $GF(3)$.*

Proposition 5. *For any integer $1 \leqslant m \leqslant n$, in the code $C_3(1,n)$ there are $\binom{n+1}{m}2^m$ codewords of the form $\sum_{j=0}^{m-1} a_j \mathbf{v}_{i_j}$ which have the same Hamming weight*

$$w(m) := 2^n - 2^{n-m}\frac{2^m + (-1)^{(m+2r)/3}2}{3}, \tag{2}$$

where all $a_j \in GF(3)^*$, $r = m \bmod 3$ is the unique remainder with $0 \leqslant r \leqslant 2$, and $0 \leqslant i_0 < i_1 < \cdots < i_{m-1} \leqslant n$.

The n weights $w(m)$ in (2) are pairwise distinct and satisfy

$$w(2) < w(4) < w(6) < \cdots < w(2\lfloor n/2 \rfloor) < w(2\lfloor (n-1)/2 \rfloor + 1)$$
$$< w(2\lfloor (n-1)/2 \rfloor - 1) < \cdots < w(5) < w(3) < w(1).$$

Proof. We first prove that all the $\binom{n+1}{m}2^m$ codewords of the form $\sum_{j=0}^{m-1} a_j \mathbf{v}_{i_j}$ have the same weight. We prove this in three cases.

Case 1: $m \equiv 0 \pmod 3$. In this case, we have $m-1 \equiv 2 \pmod 3$. If $\mathbf{v}_0$ appears in the sum $\sum_{j=0}^{m-1} a_j \mathbf{v}_{i_j}$, according to the last row of Table 1 this codeword has weight

$$2^n - 2^{n-(m-1)} \frac{2^{(m-1)} - (-1)^{(m-3)/3}}{3}$$
$$= 2^n - 2^{n-m} \frac{2^m - (-1)^{(m-3)/3} 2}{3}$$
$$= 2^n - 2^{n-m} \frac{2^m + (-1)^{m/3} 2}{3}.$$

If $\mathbf{v}_0$ is not involved, according to the first row of Table 1 this codeword has weight

$$2^n - 2^{n-m} \frac{2^m + (-1)^{m/3} 2}{3},$$

which is the same. This proves the conclusion for Case 1.

Case 2: $m \equiv 1 \pmod 3$. The proof is similar to that of Case 1, except that rows 2 and 3 of Table 1 are used instead.

Case 3: $m \equiv 2 \pmod 3$. The proof is similar to that of Case 1, except that rows 4 and 5 of Table 1 are used instead.

It is straightforward to get

$$w(2j+2) = w(2j) + 2^{n-(2j+1)},$$
$$w(2j+1) = w(2j-1) - 2^{n-2j}.$$

We now prove that

$$w(2\lfloor n/2 \rfloor) + 2 = w(2\lfloor (n-1)/2 \rfloor + 1). \tag{3}$$

Assume that $n = 2j$ is even. Then

$$w(2\lfloor n/2 \rfloor) = 2^n - \frac{2^n + 2}{3}$$

and

$$w(2\lfloor (n-1)/2 \rfloor + 1) = 2^n - \frac{2^n - 4}{3}.$$

So (3) is true when n is even. We can similarly prove that it is also true when n is odd. The inequalities then follow. □

Proposition 5 gives not only the weight distribution of $C_3(1, n)$, but also the information which codewords have the weights. It also shows an interesting pattern in the weight distribution.

4. Our secret-sharing scheme

4.1. Splitting a big secret into a string of small ones

In our secret-sharing scheme, the secret to be shared could be a positive integer or an element of $GF(3^m)$. Any positive integer s has the 3-adic expansion

$$s = s_0 + s_1 3 + s_2 3^2 + \cdots + s_j 3^j,$$

where each $s_i \in \{0, 1, 2\}$ for all $0 \leqslant i \leqslant j$ and $s_j \neq 0$. In this case, sharing the secret s becomes sharing each s_i one by one.

If the secret s is an element of $GF(3^m)$ for some positive integer m, it can be represented as

$$s = s_0 + s_1 \alpha + s_2 \alpha^2 + \cdots + s_{m-1} \alpha^{m-1},$$

where $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ is a basis of $GF(3^m)$ over $GF(3)$, and s_i is again an element of $GF(3)$. In this case, sharing s becomes sharing each s_i one by one.

4.2. Sharing small secrets

As we split a big secret into a string of smaller ones, we assume that the secret s is an element of $GF(3) = \{0, 1, 2\}$. This secret is shared among $2^n - 1$ parties. We use the code $C_3(1, n)^\perp$ to establish our secret-sharing scheme, and we use the approach described in Section 2. By Proposition 3 $C_3(1, n)$ and $C_3(1, n)^\perp$ are $[2^n, n + 1, 2^{n-1}]$ and $[2^n, 2^n - n - 1, 4]$ ternary codes, respectively.

Let G be a generator matrix of $C_3(1, n)^\perp$. Let $s \in GF(3)$ denote the secret, and $\mathbf{g}_0 = (g_{00}, g_{10}, \ldots, g_{2^n-n-2,0})^{\mathrm{T}}$ be the first column of the generator matrix G. Then the information vector $\mathbf{u} = (u_0, \ldots, u_{2^n-n-2})$ is chosen to be any vector of $GF(3)^{2^n-n-1}$ such that $s = \mathbf{u}\mathbf{g}_0 = \sum_{i=0}^{2^n-n-2} u_i g_{i0}$.

The codeword corresponding to this information vector $\mathbf{u}$ is

$$\mathbf{t} = (t_0, t_1, \ldots, t_{2^n-1}) = \mathbf{u}G.$$

We give t_i to party p_i as his share, and the first component $t_0 = s$ of the codeword $\mathbf{t}$ is the secret. This explains how to compute the shares. Recovering the secret s can be done by solving linear equations, as described in Section 2.

The following property of the code $C_3(1, n)$ is useful in understanding the access structure of our secret-sharing schemes.

Proposition 6 (Ding et al. [5]). *The supports of all the minimum weight codewords of $C_3(1,n)$ form a $1-(2^n,2^{n-1},n(n+1)/2)$ design. The $2n(n+1)$ minimum weight codewords are*

$$a\mathbf{v}_i + b\mathbf{v}_j, \quad 0 \leqslant i < j \leqslant n, \quad a,b \in GF(3)^*.$$

In some applications, a party may modify his share of the secret in order to cheat. We call such a party a *cheater*. In some cases, it would be good if a secret sharing scheme could detect and correct some false shares.

Theorem 7. *The access structure of this secret-sharing scheme is given by*

$$\Gamma = \{Q \subseteq \{1,2,\ldots,2^n-1\} \mid Q \text{ contains an element of } \Pi\},$$

where

$$\Pi = \{\mathrm{Supp}(\mathbf{c}) \cap \{1,\ldots,2^n-1\} \mid \mathbf{c} = (c_0,\ldots,c_{2^n-1}) \in C_3(1,n),\ c_0 \neq 0\}.$$

The number of parties involved in this scheme is 2^n-1. The access structure has the following properties:

(A) *Any group of less than $2^{n-1}-1$ parties cannot recover the secret. Thus, more than half of the parties are needed to recover the secret.*

(B) *There are $n(n+1)/2$ groups of $2^{n-1}-1$ parties that can recover the secret. They are* $\mathrm{Supp}(\mathbf{v}_i+\mathbf{v}_j) \cap \{1,2,\ldots,2^n-1\}$, *where $0 \leqslant i < j \leqslant n$.*

(C) *It is perfect, i.e., a group of shares either determine the secret or gives no information about the secret.*

(D) *When all the parties come together, one cheater can be found.*

Proof. Note that the subscripts of our codewords range from 0 to 2^n-1. The access structure of this secret-sharing scheme follows from Lemma 1. By Proposition 3, the minimum weight of $C_3(1,n)$ is 2^{n-1}. The conclusion of Part (A) then follows from Lemma 1.

We now prove Part (B). By Proposition 5, there are $\binom{n+1}{2}$ 4 minimum-weight codewords, which are $a\mathbf{v}_i + b\mathbf{v}_j$, where $a,b \in GF(3)^*$. It is easily seen that two minimum-weight codewords have the same support if and only if one is a multiple of the other, so the $\binom{n+1}{2}$ 2 minimum-weight codewords $\mathbf{v}_i + b\mathbf{v}_j$ have different supports, where b ranges over $\{1,2\}$. But the first coordinate of the codewords $\mathbf{v}_i + 2\mathbf{v}_j$ is zero. Hence the $\binom{n+1}{2}$ minimum-weight codewords $\mathbf{v}_i + \mathbf{v}_j$ give the different groups of $2^{n-1}-1$ participants that can recover the secret.

The conclusion of Part (C) is true for all such secret-sharing schemes based on linear codes [10].

Note that the code $C_3(1,n)^\perp$ has minimum weight 4. Deleting the first coordinate of this code gives a code with minimum weight 3 or 4. Hence, it can detect and correct one error. Thus, the conclusion of (D) follows. □

5. An example of the secret-sharing schemes

In this section, we describe an example of our secret-sharing scheme described in Section 4, specifically, the case $n=3$. This is a secret-sharing scheme involving seven parties.

The code $C_3(1,3)$ is a [8, 4, 4] ternary code with generator matrix

$$\begin{bmatrix} 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \end{bmatrix}.$$

Its dual code $C_3(1,3)^{\perp}$ is a $[8,4,4]$ ternary code with generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}.$$

Let $s \in GF(3)$ be the secret. Choose any vector $(u_1,u_2,u_3,u_4) \in GF(3)^4$ such that $u_1+u_2+u_3+u_4=s$. There are 27 such vectors. The shares $t_1,t_2,\ldots,t_7$ for the parties $p_1,p_2,\ldots,p_7$ are computed as follows:

$$(t_1,t_2,\ldots,t_7)=(u_1,u_2,u_3,u_4)\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}.$$

If $\{t_{j_1},t_{j_2},\ldots,t_{j_m}\}$ can be used to recover the secret s, then solve the following equation:

$$(1,1,1,1)^{\mathrm{T}}=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}(x_1,x_2,\ldots,x_7)^{\mathrm{T}}.$$

The secret s is then given by

$$s=\sum_{e=1}^{7} x_e t_{j_e}.$$

All the codewords of $C_3(1,3)$ tell us that a group of parties $\{p_{j_1},p_{j_2},\ldots,p_{j_e}\}$ can recover the secret if and only if the set $\{j_1,j_2,\ldots,j_e\}$ contains one of the following

sets:

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

Note that each of the parties p_1, p_2, p_3 and p_7 appears 5 times in the above 11 subsets and each of the rest appears 6 times. Thus, each party has more or less the same importance in this secret-sharing scheme.

By Proposition 6, the supports of all the minimum-weight codewords form a 1-design. But the example above shows that the $n(n+1)/2$ groups of $2^{n-1}-1$ parties, obtained from the minimum codewords of $C_3(1,n)$, do not form a 1-design in general.

6. The minimum access structure

Let Γ be the access structure of a secret-sharing scheme. An element B of Γ is called a *minimum access group* if no element of Γ is a proper subset of B. The set of all minimum access groups is called the *minimum access structure*, denoted $\underline{\Gamma}$, of this secret-sharing scheme. In other words, $\underline{\Gamma}$ is a subset of Γ such that

(1) a group of parties can determine the secret if and only if it contains an element of $\underline{\Gamma}$ as a subset;
(2) no element of $\underline{\Gamma}$ contains another element of $\underline{\Gamma}$.

For example, (4) gives the minimum access structure of the secret-sharing scheme described in Section 5.

The minimum access structure of a secret-sharing scheme is interesting in the following senses:

(1) It gives all the information about the access structure of the secret-sharing scheme, and the information it contains has no redundancy.
(2) It shows the role of each party in the secret sharing. The determination of the minimum access structure is in general a hard problem.

For our secret-sharing scheme based on the ternary code $C_3(1,n)^{\perp}$, the determination of the minimum access structure is related to the weight distribution of the second-order code $C_3(2,n)$.

We now prove a property of minimum access groups.

Theorem 8. *Any minimum access group of our secret-sharing scheme based on* $C_3(1,n)^{\perp}$ *must contain* $w(m)-1$ *parties for some* m *with* $1 \leqslant m \leqslant n$, *where* $w(m)$ *is defined as in Proposition 5.*

Proof. By Theorem 7 and the definition of minimum access groups, for any minimum access group B we have $B \in \Pi$, where

$$\Pi = \{\mathrm{Supp}(\mathbf{c}) \cap \{1, \ldots, 2^n - 1\} \mid \mathbf{c} = (c_0, \ldots, c_{2^n-1}) \in C_3(1, n),\ c_0 \neq 0\}.$$

The conclusion then follows from Proposition 5. □

We say that a codeword $\mathbf{a}$ covers another codeword $\mathbf{b}$ if $\mathrm{Supp}(\mathbf{a})$ contains $\mathrm{Supp}(\mathbf{b})$. By Theorem 8, to find the minimum access structure of our secret sharing scheme, we need only to look at the supports of the codewords of $C_3(1, n)$. Hence, for our secret-sharing scheme based on $C_3(1, n)^{\perp}$, the determination of the minimum access structure becomes the problem of finding the set W of codewords in $C_3(1, n)$ such that
(1) every codeword in $C_3(1, n)$ covers a codeword in W;
(2) if one codeword in W covers another one in W, they must have the same support.
The following lemma is easily proved.

Lemma 9. *A codeword* $\mathbf{a}$ *covers another codeword* $\mathbf{b}$ *if and only if* $\mathrm{wt}(\mathbf{a} \otimes \mathbf{b}) = \mathrm{wt}(\mathbf{b})$, *where* $\mathbf{a} \otimes \mathbf{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$, $\mathbf{a} = (a_1, \ldots, a_n)$ *and* $\mathbf{b} = (b_1, \ldots, b_n)$.

Let $\mathbf{a}$ and $\mathbf{b}$ be two codewords of $C_3(1, n)$. By definition both can be expressed as

$$\mathbf{a} = \sum_{l=1}^{t_a} a_{i_l} \mathbf{v}_{i_l}, \quad \text{where } a_{i_l} \in GF(3)^*,$$

$$\mathbf{b} = \sum_{h=1}^{t_b} b_{j_h} \mathbf{v}_{j_h}, \quad \text{where } b_{j_h} \in GF(3)^*,$$

where $0 \leqslant i_1 < \cdots < i_{t_a} \leqslant n$, $0 \leqslant j_1 < \cdots < j_{t_b} \leqslant n$, and the $\mathbf{v}_i$ are defined as before. Hence

$$\mathbf{a} \otimes \mathbf{b} = \sum_{l=1}^{t_a} \sum_{h=1}^{t_b} a_{i_l} b_{j_h} \mathbf{v}_{i_l} \otimes \mathbf{v}_{j_h}.$$

By the definition of $C_3(2, n)$, $\mathbf{a} \otimes \mathbf{b}$ is a codeword of $C_3(2, n)$. Therefore, as long as we can determine the weights of the codewords of $C_3(2, n)$, we are able to determine the set W and hence the minimum access structure of our secret-sharing scheme.

Open Problem. Determine the weight distribution of the code $C_3(2, n)$.

As mentioned above, the determination of the minimum access structure of our secret sharing-scheme is not easy. However, we are able to determine some members of the minimum access structure, as shown below.

We first determine the distinct supports of the codewords $\sum_{j=0}^{3} a_j \mathbf{v}_{i_j}$.

Proposition 10. *Let*

$$\mathbf{x} = \sum_{k=0}^{3} a_k \mathbf{v}_{i_k} \quad \text{and} \quad \mathbf{y} = \sum_{k=0}^{3} b_k \mathbf{v}_{j_k}$$

be two codewords of $C_3(1, n)$, *where* $0 \leqslant i_k \leqslant n$, $0 \leqslant j_k \leqslant n$ $(0 \leqslant k \leqslant 3)$, *and* a_i, $b_i \in GF(3)^*$. *Then* $\mathbf{x}$ *covers* $\mathbf{y}$ *if and only if* $\mathbf{x}$ *is a multiple of* $\mathbf{y}$.

Proof. First we note that, if $\mathbf{x}$ is a multiple of $\mathbf{y}$, then clearly $\mathbf{x}$ covers $\mathbf{y}$. Conversely, assuming $\mathbf{x}$ covers $\mathbf{y}$, we prove that $\mathbf{x}$ is a multiple of $\mathbf{y}$ in several steps.

Step 1: *If* $\mathbf{x}$ *covers* $\mathbf{y}$, *then* $\{i_0, i_1, i_2, i_3\} = \{j_0, j_1, j_2, j_3\}$.

By Proposition 5, we have

$$w(2) < w(4) < w(6) < w(8) < w(7) < w(5) < w(3) < 2^n \tag{5}$$

and that $\mathbf{x}$ and $\mathbf{y}$ have the same weight. Suppose that $\mathbf{x}$ covers $\mathbf{y}$. Then $\mathrm{wt}(\mathbf{x}) \geqslant \mathrm{wt}(\mathbf{x}+\mathbf{y})$ and $\mathrm{wt}(\mathbf{x}) \geqslant \mathrm{wt}(\mathbf{x}-\mathbf{y})$. It follows that $|\{i_0, i_1, i_2, i_3\} \cap \{j_0, j_1, j_2, j_3\}| \geqslant 2$. Without loss of generality, we assume that $i_2 = j_2$ and $i_3 = j_3$. Note that one of $\mathbf{x} \pm \mathbf{y}$ has at least the term $\mathbf{v}_{i_2}$ or $\mathbf{v}_{i_3}$. By (5) we have $|\{i_0, i_1\} \cap \{j_0, j_1\}| \geqslant 1$. Without loss of generality, we assume that $i_1 = j_1$. Whence, we have

$$\mathbf{x} = a_0 \mathbf{v}_{i_0} + a_1 \mathbf{v}_{i_1} + a_2 \mathbf{v}_{i_2} + a_3 \mathbf{v}_{i_3},$$

$$\mathbf{y} = b_0 \mathbf{v}_{j_0} + b_1 \mathbf{v}_{i_1} + b_2 \mathbf{v}_{i_2} + b_3 \mathbf{v}_{i_3}.$$

If $i_0 \neq j_0$, then one of the following two statements must be true:

(i) one of $\mathbf{x} + \mathbf{y}$ and $\mathbf{x} - \mathbf{y}$ has exactly three terms among $\mathbf{v}_{i_0}, \mathbf{v}_{j_0}, \mathbf{v}_{i_1}, \mathbf{v}_{i_2}$ and $\mathbf{v}_{i_3}$ (and the other has four terms); or

(ii) one of $\mathbf{x} + \mathbf{y}$ and $\mathbf{x} - \mathbf{y}$ has exactly five terms among $\mathbf{v}_{i_0}, \mathbf{v}_{j_0}, \mathbf{v}_{i_1}, \mathbf{v}_{i_2}$ and $\mathbf{v}_{i_3}$ (and the other has two terms).

By (5) the weight of either $\mathbf{x} + \mathbf{y}$ or $\mathbf{x} - \mathbf{y}$ is greater than that of $\mathbf{x}$, which is a contradiction. This completes Step 1.

Step 2: *Assume* $i_k = j_k$ *for* $0 \leqslant k \leqslant 3$ *and define* $\mathbf{a} = (a_0, a_1, a_2, a_3)$ *and* $\mathbf{b} = (b_0, b_1, b_2, b_3)$. *Then* $\mathrm{wt}(\mathbf{a} \pm \mathbf{b})$ *equals one of the numbers* 0, 2, *and* 4.

If $\mathrm{wt}(\mathbf{a}+\mathbf{b}) = 1$ (resp. $\mathrm{wt}(\mathbf{a}-\mathbf{b}) = 1$), then $\mathrm{wt}(\mathbf{a}-\mathbf{b}) = 3$ (resp. $\mathrm{wt}(\mathbf{a}+\mathbf{b}) = 3$). Since $w(1) > w(3) > w(4)$, the conclusion then follows.

Step 3: *In fact*, $\mathrm{wt}(\mathbf{a} \pm \mathbf{b})$ *cannot be* 2.

Suppose, on the contrary, that $\mathrm{wt}(\mathbf{a} \pm \mathbf{b}) = 2$. By Proposition 5, $\mathbf{x}$ and $\mathbf{y}$ have the same weight $2^{n-1} + 2^{n-3}$. Since $\mathbf{x}$ covers $\mathbf{y}$, they should have the same support.

That $\mathbf{x}$ and $\mathbf{y}$ have the same support means that every (z_0, z_1, z_2, z_3) in the space $(GF(3)^*)^4$ is a solution of the equation $a_0 z_0 + a_1 z_1 + a_2 z_2 + a_3 z_3 = 0$ if and only if it is a solution of $-a_0 z_0 - a_1 z_1 + a_2 z_2 + a_3 z_3 = 0$. However, this is not true. Hence, $\mathbf{x}$ cannot cover $\mathbf{y}$, which is a contradiction.

Combining Steps 1–3, we have proved the proposition. □

Proposition 11. *Let*

$$\mathbf{x} = \sum_{k=0}^{3} a_k \mathbf{v}_{i_k} \quad \text{and} \quad \mathbf{y} = \sum_{k=0}^{1} b_k \mathbf{v}_{j_k}$$

be two codewords of $C_3(1, n)$, *where* $0 \leqslant i_k \leqslant n$ $(0 \leqslant k \leqslant 3)$, $0 \leqslant j_k \leqslant n$ $(k = 0, 1)$, *and* $a_i,\ b_i \in GF(3)^*$. *Then* $\mathbf{x}$ *cannot cover* $\mathbf{y}$.

Proof. We prove the following two statements:

(i) If $\mathbf{x}$ covers $\mathbf{y}$, then $\{j_0, j_1\} \subset \{i_0, i_1, i_2, i_3\}$. Suppose that $j_0 = i_0$ and $j_1 = i_1$, then $(b_0, b_1) = \pm (a_0, a_1)$.

(ii) Let $\mathbf{x} = \sum_{l=0}^{3} a_l \mathbf{v}_{i_l}$ and $\mathbf{y} = \pm (a_0 \mathbf{v}_{i_0} + a_1 \mathbf{v}_{i_1})$, where $a_l \neq 0$. Then $\mathbf{x}$ cannot cover $\mathbf{y}$.

The proof of (i) is similar to that of Step 1 of Proposition 10, while that of (ii) is similar to that of Step 3 of Proposition 10, except that we now compare $\mathbf{x}$ and $\mathbf{x} \pm \mathbf{y}$. □

Combining Theorem 7, Propositions 10 and 11, we obtain the following conclusion.

Theorem 12. *The minimum access structure* $\underline{\Gamma}$ *of our secret sharing scheme based on* $C_3(1, n)^{\perp}$ *contains the supports* (*in* $\{1, \ldots, 2^n - 1\}$) *of all the codewords*

$$\mathbf{x} = \sum_{k=0}^{3} a_k \mathbf{v}_{i_k}$$

with $\sum_{k=0}^{3} a_k = 1$, *where* $0 \leqslant i_0 < i_1 < i_2 < i_3 \leqslant n$, *and the minimum codewords of the form*

$$\mathbf{y} = \sum_{k=0}^{1} \mathbf{v}_{j_k},$$

where $0 \leqslant j_0 < j_1 \leqslant n$.

Acknowledgements

The authors thank the referee for helpful comments and suggestions that improved the presentation of this paper.

References

[1] R.J. Anderson, C. Ding, T. Helleseth, T. Kløve, How to build robust shared control systems, Designs Codes Cryptogr. 15 (1998) 111–124.

[2] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge University Press, Cambridge, 1992.

[3] G.R. Blakley, Safeguarding cryptographic keys, Proc. NCC AFIPS (1979) 313–317.

[4] E.F. Brickell, Some ideal secret sharing schemes, in: Advances in Cryptology – Eurocrypt'89, Lecture Notes in Computer Science, vol. 434, Springer, Heidelberg, 1990, pp. 468–475.
[5] C. Ding, D.R. Kohel, S. Ling, Elementary 2-group character codes, IEEE Trans Inform. Theory IT-46 (2000) 280–284.
[6] C. Ding, D. Pei, A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography, World Scientific, Singapore, 1996.
[7] E.D. Karnin, J.W. Green, M. Hellman, On secret sharing systems, IEEE Trans Inform. Theory IT-29 (1983) 644–654.
[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1978.
[9] J.L. Massey, Minimal codewords and secret sharing, Proc. 6th Joint Swedish–Russian Workshop on Information Theory, Mölle, Sweden, August 22–27, 1993, pp. 276–279.
[10] J.L. Massey, Some applications of coding theory in cryptography, in: P.G. Farrell (Ed.), Codes and Ciphers: Cryptography and Coding IV, Formara Ltd, Esses, England, 1995, pp. 33–47.
[11] R.J. McEliece, D.V. Sarwate, On sharing secrets and Reed–Solomon codes, Comm. ACM 24 (1981) 583–584.
[12] A. Renvall, C. Ding, The access structure of some secret sharing schemes, in: J. Pieprzyk, J. Seberry (Eds.), Information Security and Privacy, Lecture Notes in Computer Science, vol. 1172, Springer, Heidelberg, 1996, pp. 67–78.
[13] J.-P. Serre, A Course in Arithmetic, Graduate Texts in Mathematics, vol. 7, Springer, New York, 1973.
[14] A. Shamir, How to share a secret, Comm. ACM 22 (1979) 612–613.
[15] M. van Dijk, A linear construction of perfect secret sharing schemes, in: A. De Santis (Ed.), Advances in Cryptology – Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer, Heidelberg, 1995, pp. 23–34.