Covering and Secret Sharing with Linear Codes

Cunsheng Ding and Jin Yuan

Department of Computer Science
The Hong Kong University of Science and Technology
Kowloon, Hong Kong, China
{cding,jyuan}@cs.ust.hk

Abstract. Secret sharing has been a subject of study for over twenty years, and has had a number of real-world applications. There are several approaches to the construction of secret sharing schemes. One of them is based on coding theory. In principle, every linear code can be used to construct secret sharing schemes. But determining the access structure is very hard as this requires the complete characterisation of the minimal codewords of the underlying linear code, which is a difficult problem. In this paper we present a sufficient condition under which we are able to determine all the minimal codewords of certain linear codes. The condition is derived using exponential sums. We then construct some linear codes whose covering structure can be determined, and use them to construct secret sharing schemes with interesting access structures.

1 Introduction

Secret sharing schemes were first introduced by Blakley [6] and Shamir [13] in 1979. Since then, many constructions have been proposed. The relationship between Shamir's secret sharing scheme and the Reed-Solomon codes was pointed out by McEliece and Sarwate in 1981 [11]. Later several authors have considered the construction of secret sharing schemes using linear error correcting codes. Massey utilised linear codes for secret sharing and pointed out the relationship between the access structure and the minimal codewords of the dual code of the underlying code [9,10]. Unfortunately, determining the minimal codewords is extremely hard for general linear codes. This was done only for a few classes of special linear codes.

Several authors have investigated the minimal codewords for certain codes and characterised the access structures of the secret sharing schemes based on their dual codes [1,12,2,3,14]. In this paper, we first characterise the minimal codewords of certain linear codes using exponential sums, and then construct some linear codes suitable for secret sharing. Finally we determine the access structure of the secret sharing schemes based on the duals of those linear codes. The access structures of the secret sharing schemes constructed in this paper are quite interesting.

C.S. Calude et al. (Eds.): DMTCS 2003, LNCS 2731, pp. 11–25, 2003.

2 A Link between Secret Sharing Schemes and Linear Codes

An $[n, k, d; q]$ code C is a linear subspace of F_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. For all the linear codes mentioned in this paper we always assume that no column vector of any generator matrix is the zero vector. There are several ways to use linear codes to construct secret sharing schemes [9,12]. One of them is the following.

In the secret sharing scheme constructed from C, the secret is an element of F_q, and $n-1$ parties $P_1, P_2, \cdots, P_{n-1}$ and a dealer are involved.

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

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

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

Note that $t_0 = \mathbf{u}\mathbf{g}_0 = s$. It is easily seen that a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the secret if and only if $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$.

So we have the following lemma [9].

Proposition 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 $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determine 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, $1 \leq i_2 < \ldots < i_m \leq n-1$ and $1 \leq m \leq n-1$.

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 called a *minimal access set* if they can recover the secret with their shares, any of its proper subgroups cannot do so. Here a proper subgroup has fewer members than this group. Due to 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.

Definition 1. *The* support *of a vector* $\mathbf{c} \in \mathsf{F}_q^n$ *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* $\mathbf{c}_1$*. A codeword* $\mathbf{c}$ *is called* normalised *if its first coordinator is 1. A* minimal codeword *is a normalised codeword that covers no other normalised codeword.*

If a nonzero codeword $\mathbf{c}$ *covers only its multiples, but no other nonzero codewords, then it is called a* minimal vector*. Hence a minimal codeword must be a minimal vector, but a minimal vector may not be a minimal codeword.*

From Proposition 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 $\mathsf{C}^{\perp}$. In this paper, we shall consider the secret sharing schemes obtained from the dual codes of some linear codes whose minimal codewords can be characterised.

3 The Access Structure of the Secret Sharing Schemes Based on Linear Codes

Proposition 2. *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. If each nonzero codeword of* C *is a minimal vector, 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 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 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.*

Proof. We first prove that the total number of minimal access sets is q^{k-1}. At the very beginning of this paper, we assumed that every column vector of any generator matrix is nonzero. Hence $\mathbf{g}_0 \neq 0$. Thus the inner product $\mathbf{u}\mathbf{g}_0$ takes on each element of F_q exactly q^{k-1} times when $\mathbf{u}$ ranges over all elements of F_q^k. Hence there are altogether $q^k - q^{k-1}$ codewords in C whose first coordinator is nonzero. Since each nonzero codeword is a minimal vector, a codeword covers another one if and only if they are multiples of each other. Hence the total number of minimal codewords is $(q^k - q^{k-1})/(q-1) = q^{k-1}$, which is the number of minimal access sets.

For any $1 \leq i \leq n-1$, if $\mathbf{g}_i = a\mathbf{g}_0$ for some $a \in \mathsf{F}_q^*$, then $\mathbf{u}\mathbf{g}_0 = 1$ implies that $\mathbf{u}\mathbf{g}_i = a \neq 0$. Thus Participant P_i is in every minimal access set. For any

$1 \leq i \leq n-1$, if $\mathbf{g}_0$ and $\mathbf{g}_i$ are linearly independent, $(\mathbf{u}\mathbf{g}_0, \mathbf{u}\mathbf{g}_i)$ takes on each element of F_q^2 q^{k-2} times when the vector $\mathbf{u}$ ranges over F_q^k. Hence

$$|\{\mathbf{u} : \mathbf{u}\mathbf{g}_0 \neq 0 \text{ and } \mathbf{u}\mathbf{g}_i \neq 0)\}| = (q-1)^2 q^{k-2}$$

and

$$|\{\mathbf{u} : \mathbf{u}\mathbf{g}_0 = 1 \text{ and } \mathbf{u}\mathbf{g}_i \neq 0)\}| = (q-1) q^{k-2},$$

which is the number of minimal access sets in which P_i is involved.

In view of Proposition 2, it is an interesting problem to construct codes where each nonzero codeword is a minimal vector. Such a linear code gives a secret sharing scheme with the interesting access structure described in Proposition 2.

4 Characterisations of Minimal Codewords

4.1 Sufficient Condition from Weights

If the weights of a linear code are close enough to each other, then each nonzero codeword of the code is a minimal vector, as described by the following proposition.

Proposition 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 each nonzero codeword of C is a minimal vector.

Proof. Suppose $\mathbf{c}_1 = (u_0, u_1, \ldots, u_{n-1})$ covers $\mathbf{c}_2 = (v_0, v_1, \ldots, v_{n-1})$, and $\mathbf{c}_1$ is not a multiple of $\mathbf{c}_2$. Then

$$w_{min} \leq w(\mathbf{c}_2) \leq w(\mathbf{c}_1) \leq w_{max}$$

For any $t \in \mathsf{F}_q^*$, let $m_t = \#\{i : v_i \neq 0, u_i = tv_i\}$. By definition

$$\sum_{t \in \mathsf{F}_q^*} m_t = w_2.$$

Hence there exists some t such that $m_t \geq \frac{w_2}{q-1}$. For the codeword $\mathbf{c}_1 - t\mathbf{c}_2$,

$$w(\mathbf{c}_1 - t\mathbf{c}_2) \leq w_1 - \frac{w_2}{q-1} \leq w_{max} - \frac{w_{min}}{q-1} < \frac{q}{q-1} w_{min} - \frac{w_{min}}{q-1} = w_{min}$$

This means that the nonzero codeword $\mathbf{c}_1 - t\mathbf{c}_2$ has weight less than w_{min}, which is impossible. The conclusion then follows.

4.2 Sufficient and Necessary Condition Using Exponential Sums

Let p be an odd prime and let $q = p^k$. Throughout this paper, let χ denote the canonical additive character of F_q, i.e., $\chi(x) = \exp\left(i\frac{2\pi}{p}\mathsf{Tr}(x)\right)$. It is well known that each linear function from F_{p^k} to F_p can be written as a trace function. Hence for any $[n, k; p]$ linear code C with generator matrix G, there exists $g_1, g_2, \ldots g_n \in \mathsf{F}_{q^k}$ such that

$$\mathbf{c}_\alpha = (\mathsf{Tr}(g_1\alpha), \ldots, \mathsf{Tr}(g_n\alpha)) \tag{2}$$

Thus any linear code has a trace form of (2).

We now consider two nonzero codewords $\mathbf{c}_\alpha$ and $\mathbf{c}_\beta$, where $\beta/\alpha \notin \mathsf{F}_p$. If $\beta/\alpha \in \mathsf{F}_p$, then the two codewords would be multiples of each other. Let S_α be the number of coordinates in which $\mathbf{c}_\alpha$ takes on zero, and let $T_{\alpha,\beta}$ be the number of coordinates in which both $\mathbf{c}_\alpha$ and $\mathbf{c}_\beta$ take on zero.

By definition, $S_\alpha \geq T_{\alpha,\beta}$. Clearly, $\mathbf{c}_\alpha$ covers $\mathbf{c}_\beta$ if and only if $S_\alpha = T_{\alpha,\beta}$. Hence we have the following proposition.

Proposition 4. *$\forall\alpha \in \mathsf{F}_q^*, \mathbf{c}_\alpha$ is a minimal vector if and only if $\forall\beta \in \mathsf{F}_q^*$ with $\frac{\beta}{\alpha} \notin \mathsf{F}_p$, $S_\alpha > T_{\alpha,\beta}$.*

We would use this proposition to characterise the minimal vectors of the code C. To this end, we would compute the values of both S_α and $T_{\alpha,\beta}$. But this is extremely hard in general. Thus we would give tight bounds on them using known bounds on exponential sums.

By definition,

$$\begin{aligned} S_\alpha &= \#\{i : \mathsf{Tr}(g_i\alpha) = 0, 1 \leq i \leq n\} \\ &= \sum_{i=1}^{n}\sum_{c\in F_p}\frac{1}{p}\mathrm{e}^{i\frac{2\pi}{p}c\mathsf{Tr}(g_i\alpha)} \\ &= \frac{1}{p}\left(n + \sum_{c\in F_p^*}\sum_{i=1}^{n}\chi(cg_i\alpha)\right). \end{aligned} \tag{3}$$

Similarly,

$$\begin{aligned} T_{\alpha,\beta} &= \#\{i : \mathsf{Tr}(g_i\alpha) = 0, \mathsf{Tr}(g_i\beta) = 0\} \\ &= \sum_{i=1}^{n}\left(\frac{1}{p}\sum_{u\in\mathsf{F}_p}e^{i\frac{2\pi}{p}u\mathsf{Tr}(g_i\alpha)}\right)\left(\frac{1}{p}\sum_{v\in\mathsf{F}_p}e^{i\frac{2\pi}{p}v\mathsf{Tr}(g_i\alpha)}\right) \\ &= \frac{1}{p^2}\left(n + \sum_{(u,v)\in\mathsf{F}_p^2\setminus\{(0,0)\}}\sum_{i=1}^{n}\chi(g_i(u\alpha + v\beta))\right). \end{aligned} \tag{4}$$

As can be seen from the expressions of S_α and $T_{\alpha,\beta}$, when c or u, v is fixed, the inner sum for both expressions is

$$\sum_{i=1}^{n}\chi(g_i a)$$

for some fixed a, where χ is the canonical additive character over F_q. However, most known bounds on exponential sums are summed over the whole F_q, and may not be used to give bounds on S_α and $T_{\alpha,\beta}$. However, if the set $G = \{g_1, \ldots g_n\}$ constitutes the range of some function defined over F_q, and each element in this range is taken on the same number of times by this function, we will be able to derive bounds for S_α and $T_{\alpha,\beta}$ using known bounds on exponential sums. This will become clear in later sections.

5 Bounds on Exponential Sums

In this section, we introduce the following bounds on exponential sums which will be needed later. Their proofs can be found in [8, Chapter 5].

Definition 2. *Let ψ be a multiplicative and χ an additive character of F_q. Then the* Gaussian sum *$G(\psi, \chi)$ is defined by*

$$G(\psi, \chi) = \sum_{c \in \mathsf{F}_q^*} \psi(c)\chi(c).$$

It is well known that if both ψ and χ are nontrivial, $|G(\psi, \chi)| = \sqrt{q}$.

Proposition 5. *Let F_q be a finite field with $q = p^s$, where p is an odd prime and $s \in \mathbf{N}$. Let η be the quadratic character of F_q and let χ be the canonical additive character of F_q. Then*

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

Proposition 6. *Let χ be a nontrivial additive character of F_q, $n \in \mathbf{N}$, and $d = \gcd(n, q-1)$. Then*

$$\left| \sum_{c \in \mathsf{F}_q} \chi(ac^n + b) \right| \leq (d-1)q^{1/2} \tag{6}$$

for any $a, b \in \mathsf{F}_q$ with $a \neq 0$.

Proposition 7. *Let χ be a nontrivial additive character of F_q with q odd, and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathsf{F}_q[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c \in \mathsf{F}_q} \chi(f(c)) = \chi(a_0 - {a_1}^2(4a_2)^{-1})\eta(a_2)G(\eta, \chi) \tag{7}$$

where η is the quadratic character of F_q.

Proposition 8. (Weil's Theorem) *Let $f \in \mathsf{F}_q[x]$ be of degree $n \geq 1$ with* $\gcd(n, q)$ $= 1$ *and let χ be a nontrivial additive character of F_q. Then*

$$\left| \sum_{c \in \mathsf{F}_q} \chi(f(c)) \right| \leq (n-1)q^{1/2} \tag{8}$$

6 Secret Sharing Schemes from Irreducible Cyclic Codes

6.1 The General Case

Definition 3. *Let p be a prime, and let $q = p^k$. Suppose $N|q-1$, and $nN = q-1$. If θ is a primitive n-th root of unity in F_q, then the set C of n-tuples*

$$\mathbf{c}(\xi) = (\mathsf{Tr}(\xi), \mathsf{Tr}(\xi\theta), \ldots, \mathsf{Tr}(\xi\theta^{n-1})), \xi \in \mathsf{F}_q$$

is an irreducible cyclic $[n, k_0]$ code over F_p, where k_0 divides k and $\mathsf{Tr}(\xi) = \xi + \xi^p + \ldots + \xi^{p^{k-1}}$ is the trace function from F_q to F_p.

For these codes we have $\{g_1, g_2, \ldots, g_n\} = \{1, \theta, \ldots, \theta^{n-1}\}$ in (2). We consider those irreducible cyclic codes where $k_0 = k$, and would determine their minimal vectors. To this end, we will give tight bounds on S_α and $T_{\alpha,\beta}$ for two nonzero codewords $\mathbf{c}_\alpha$ and $\mathbf{c}_\beta$, where $\alpha/\beta \notin \mathsf{F}_p$.

Bounds on S_α:

Using (3), we have

$$\begin{aligned}
S_\alpha &= \frac{1}{p}\left(n + \sum_{c\in\mathsf{F}_p^*} \frac{1}{N} \sum_{x\in\mathsf{F}_q^*} \chi(c\alpha x^N)\right) \\
&= \frac{1}{p}\left(n + \sum_{c\in\mathsf{F}_p^*} \frac{1}{N} \left(\sum_{x\in\mathsf{F}_q} \chi(c\alpha x^N) - 1\right)\right) \\
&= \frac{1}{Np}\left(q - p + \sum_{c\in F_p^*} \sum_{x\in F_q} \chi(c\alpha x^N)\right) \\
&= \frac{1}{Np}(q - p + A_\alpha)
\end{aligned}$$

where

$$A_\alpha = \sum_{c\in F_p^*} \sum_{x\in F_q} \chi(c\alpha x^N)$$

Applying the bound of (6) to A_α above, we have

$$|A_\alpha| \leq \sum_{c\in F_p^*} \left| \sum_{x\in F_q} \chi(c\alpha x^N) \right| \leq (p-1)(N-1)\sqrt{q}$$

Combining this with the formula for S_α above yields

$$\frac{1}{Np}(q - p - (p-1)(N-1)\sqrt{q}) \leq S_\alpha \leq \frac{1}{Np}(q - p + (p-1)(N-1)\sqrt{q})$$

Bounds on $T_{\alpha,\beta}$:

Using (4), we have

$$\begin{aligned}
T_{\alpha,\beta} &= \frac{1}{p^2}\left(n + \sum_{(u,v)\in \mathsf{F}_p^2\setminus\{(0,0)\}} \frac{1}{N}\sum_{x\in \mathsf{F}_q^*} \chi((u\alpha+v\beta)x^N)\right) \\
&= \frac{1}{p^2}\left(n + \frac{1}{N}\sum_{(u,v)\in \mathsf{F}_p^2\setminus\{(0,0)\}} \left(\sum_{x\in \mathsf{F}_q} \chi((u\alpha+v\beta)x^N) - 1\right)\right) \\
&= \frac{1}{Np^2}\left(-p^2 + q + \sum_{(u,v)\in \mathsf{F}_p^2\setminus\{(0,0)\}} \sum_{x\in F_q} \chi((u\alpha+v\beta)x^N)\right) \\
&= \frac{1}{Np^2}\left(q - p^2 + B_{\alpha,\beta}\right),
\end{aligned}$$

where

$$B_{\alpha,\beta} = \sum_{(u,v)\in \mathsf{F}_p^2\setminus\{(0,0)\}} \sum_{x\in F_q} \chi((u\alpha+v\beta)x^N)$$

Note that we assumed that both α and β are nonzero and that $\alpha/\beta \notin \mathsf{F}_p$. Hence for any pair $(u,v) \neq (0,0)$, $u\alpha + v\beta \neq 0$. Thus after applying the bound of (6), we have

$$\begin{aligned}
|B_{\alpha,\beta}| &\leq \sum_{(u,v)\in \mathsf{F}_p^2\setminus\{(0,0)\}} \left|\sum_{x\in F_q} \chi((u\alpha+v\beta)x^N)\right| \\
&\leq (p^2-1)(N-1)\sqrt{q}.
\end{aligned}$$

Combining this inequality and the formula for $T_{\alpha,\beta}$ above, we get

$$\frac{1}{Np^2}(q - p^2 - (p^2-1)(N-1)\sqrt{q}) \leq T_{\alpha,\beta} \leq \frac{1}{Np^2}(q - p^2 + (p^2-1)(N-1)\sqrt{q})$$

Proposition 9. *For the irreducible cyclic code* C *with parameters* $[n,k]$*, when*

$$N - 1 < \frac{\sqrt{q}}{2p+1},$$

each nonzero codeword of C *is a minimal vector.*

Proof. When the above inequality holds, $S_\alpha > T_{\alpha,\beta}$ is satisfied because of the bounds on S_α and $T_{\alpha,\beta}$ developed before. The conclusion then follows from Proposition 4.

Proposition 10. *Let* C *be the* $[n, k]$ *irreducible cyclic code, where* $N-1 < \frac{\sqrt{q}}{2p+1}$*. In the secret sharing scheme based on* $\mathsf{C}^{\perp}$*, the* $n-1$ *participants are divided into two subgroups. The first subgroup comprises of* $\gcd(n, p-1)-1$ dictatorial parties*, i.e., each of them must be in every minimal access set; the rest participants form the second subgroup, and each of them serves in* $(p-1)p^{k-2}$ *minimal access sets.*

Proof. Note that $\mathbf{g}_i$ is a multiple of $\mathbf{g}_0$ if and only if $\theta^i \in \mathsf{F}_p$. This is true if and only if $n|i(p-1)$, i.e.,

$$\frac{n}{\gcd(n,p-1)}|i\frac{p-1}{\gcd(n,p-1)},$$

so

$$\frac{n}{\gcd(n,p-1)}|i.$$

For $0 < i < n$, there are $\gcd(n, p-1) - 1$ $\mathbf{g}_i$'s which are multiples of $\mathbf{g}_0$. The conclusion then follows from Proposition 2.

6.2 The Semi-primitive Case

In Section 6.1 we showed that all nonzero codewords of the irreducible cyclic codes are minimal vectors under the condition that $N-1 < \frac{\sqrt{q}}{2p+1}$. In this case the secret sharing scheme based on the dual code has the interesting access structure, as described in Proposition 10. The condition $N-1 < \frac{\sqrt{q}}{2p+1}$ is derived using bounds on both S_α and $T_{\alpha,\beta}$. If we can compute one of them or both exactly, we could relax the condition $N-1 < \frac{\sqrt{q}}{2p+1}$. In this section, we show that this can be done for a special class of irreducible cyclic codes, i.e., *the semi-primitive irreducible cyclic codes.*

Definition 4. [5] *An irreducible cyclic* $[n, k]$ *code is said to be* semi-primitive *if* $n = (p^k - 1)/N$ *and there exists a divisor* j *of* $k/2$ *for which* $p^j \equiv -1 \pmod{N}$*.*

In the semi-primitive case, the code C has only two nonzero weights and its weight distribution is determined [4]. The weights and their distributions are closely related to cyclotomic numbers and Gaussian periods.

Definition 5. *Let* q *be a power of a prime* p*,* $Nn = q - 1$*. Let* g *be a primitive element of* F_q*. For all* $0 \le i < N$*, the* Gaussian periods of order N over F_q *are defined to be*

$$\eta_i = \sum_{t=0}^{n-1} e^{i\frac{2\pi}{p}\mathsf{Tr}(g^{Nt+i})}$$

Lemma 1. [4] *Let* q *be a power of a prime* p*, and* $N|q-1$*,* $N \ge 3$*. If* -1 *is a power of* p *mod* N*, then* $q = r^2$ *for an integer* r *with* $r = 1 \bmod N$*, and one Gaussian period takes on* η_c*, and all other* $N-1$ *Gaussian periods take on* η*, where* $\eta = \frac{r-1}{N}$ *and* $\eta_c = \eta - r$*.*

By definition in the semi-primitive case there is a divisor j of $\frac{k}{2}$ such that $N|p^j+1$. Thus $-1 = p^j \bmod N$ and the condition of Lemma 1 is satisfied. Hence the N Gaussian periods take on only two different values.

If $\frac{k}{2j}$ is odd, then $N|p^j+1|p^{\frac{k}{2}}+1 = \sqrt{q}+1$. $r = -\sqrt{q}$. $\eta_c = \frac{(N-1)\sqrt{q}-1}{N}$ for some c, and $\eta_j = \frac{-\sqrt{q}-1}{N}$ for all $j \neq c$.

If $\frac{k}{2j}$ is even, then $N|p^j+1|p^{2j}-1|p^{\frac{k}{2}}-1 = \sqrt{q}-1$. $r = \sqrt{q}$. $\eta_c = \frac{-(N-1)\sqrt{q}-1}{N}$ for some c, and $\eta_j = \frac{\sqrt{q}-1}{N}$ for all $j \neq c$.

For any $\gamma \in \mathsf{F}_q^*$, if $\gamma = g^{Nt+i}$, $0 \le t < n$, $0 \le i < N$, by abuse of notation, we define $\eta_\gamma = \eta_i$, then it's easily seen $\sum_{x \in F_q} \chi(\gamma x^N) = N\eta_\gamma + 1$.

Let S_α, $T_{\alpha,\beta}$, A_α and $B_{\alpha,\beta}$ be defined the same as in Section 6.1. Note that $S_\alpha > T_{\alpha,\beta}$ is equivalent to $B_{\alpha,\beta} - pA_\alpha < (p-1)q$.

We have

$$\begin{aligned} B_{\alpha,\beta} - pA_\alpha &= \sum_{(u,v)\in \mathsf{F}_q^2 \setminus \{(0,0)\}} (N\eta_{u\alpha+v\beta}+1) - p\sum_{c\in \mathsf{F}_p^*} (N\eta_{c\alpha}+1) \\ &= p-1+N\sum_{i=0}^{p-1}\sum_{j=1}^{p-1} \eta_{j(\beta+i\alpha)} - N(p-1)\sum_{k=1}^{p-1} \eta_{k\alpha} \end{aligned}$$

Because the Gaussian periods are two-valued,

$$B_{\alpha,\beta} - pA_\alpha \le \begin{cases} (p-1)(pN\sqrt{q}-\sqrt{q}), & \text{if } \frac{k}{2j} \text{ is odd} \\ (p-1)((p-1)N\sqrt{q}+\sqrt{q}), & \text{if } \frac{k}{2j} \text{ is even.} \end{cases} \tag{9}$$

Proposition 11. *If*

$$N < \frac{\sqrt{q}+1}{p},$$

all nonzero codewords of the semi-primitive cyclic code C *are minimal vectors. In the secret sharing scheme based on* $\mathsf{C}^\perp$, *the* $n-1$ *participants are divided into two subgroups. The first subgroup comprises of* $\gcd(n, p-1) - 1$ dictatorial parties, *i.e., each of them must be in every minimal access set; the rest participants form the second subgroup, and each of them serves in* $(p-1)p^{k-2}$ *minimal access sets.*

Proof. On easily verifies if $N < \frac{\sqrt{q}+1}{p}$, the upper bounds (9) on $B_{\alpha,\beta} - pA_\alpha$ in both cases is less than $(p-1)q$, so $S_\alpha > T_{\alpha,\beta}$ for any $\alpha \in \mathsf{F}_q^*$. The rest follows from Proposition 2.

7 Secret Sharing Schemes from Quadratic Form Codes

Let p be an odd prime, $q = p^m$. Let $a_1 \in \mathsf{F}_q^*$. Consider $f(x) = x^2 + a_1 x$ defined over F_q. It is easily seen that

1. $f(y) = f(-a_1 - y)$ for any y;
2. $f(0) = f(-a_1) = 0$;

3. $y = -a_1 - y$ and $f(y) = -\frac{a_1^2}{4}$ when $y = -\frac{a_1}{2}$.

Let

$$G = \mathrm{Range}(f) \setminus \left\{-\frac{a_1^2}{4}, 0\right\}.$$

Let $n = \frac{q-3}{2}$, then $|G| = n$. Write $G = \{g_1, g_2, \ldots, g_n\}$. We do not care about the order here.

We define a linear code C as

$$\mathsf{C} = \{\mathbf{c}_\alpha = (\mathsf{Tr}(\alpha g_1), \mathsf{Tr}(\alpha g_2), \ldots, \mathsf{Tr}(\alpha g_n)) : \alpha \in \mathsf{F}_q\}$$

where $\mathsf{Tr}(x)$ is the trace function from F_q to F_p.

Lemma 2. *C is an $[n, m; p]$ code.*

Proof. First, there are m elements in G which are linearly independent over F_p. This is because $|G| = \frac{q-3}{2} > p^{m-1} - 1$, which is the size of an $(m-1)$-dimensional space over F_p excluding the zero element. Second, let $\{b_1, b_2, \ldots, b_m\}$ be a basis of F_q over F_p, we prove $\mathbf{c}_{b_1}, \mathbf{c}_{b_2}, \ldots, \mathbf{c}_{b_m}$ are linearly independent over F_p. W.l.o.g. suppose $g_1, g_2, \ldots, g_m$ are linearly independent over F_p. We only need to prove the matrix

$$\begin{pmatrix} \mathsf{Tr}(b_1 g_1) & \mathsf{Tr}(b_1 g_2) & \ldots \mathsf{Tr}(b_1 g_m) \\ \mathsf{Tr}(b_2 g_1) & \mathsf{Tr}(b_2 g_2) & \ldots \mathsf{Tr}(b_2 g_m) \\ & & \ldots \\ \mathsf{Tr}(b_m g_1) & \mathsf{Tr}(b_m g_2) & \ldots \mathsf{Tr}(b_m g_m) \end{pmatrix}$$

is nonsingular. Suppose there is a linear dependency among the column vectors, i.e., there exist $c_1, c_2, \ldots, c_m \in \mathsf{F}_p$ s.t. for $1 \leq i \leq m$, $c_1 \mathsf{Tr}(b_i g_1) + c_2 \mathsf{Tr}(b_i g_2) + \ldots c_m \mathsf{Tr}(b_i g_m)$=0, i.e., $\mathsf{Tr}(b_i(\sum_{j=1}^m c_j g_j)) = 0$. So $\sum_{j=1}^m c_j g_j = 0$. We get $c_1 = c_2 = \ldots = c_m = 0$. So C has dimension m. This completes the proof of this lemma.

Now we investigate the weights of C. Note for any $a \in \mathsf{F}_q^*$, by (3)

$$\begin{aligned} \sum_{i=1}^n \chi(g_i a) &= \frac{1}{2} \sum_{x \in F_q \setminus \{-a_1/2, 0, -a_1\}} \chi(f(x)a) \\ &= \frac{1}{2} \left(\sum_{x \in F_q} \chi(ax^2 + aa_1 x)) - \chi\left(-\frac{{a_1}^2}{4} a\right) - 2 \right) \\ &= \frac{1}{2} \left(\chi\big(- (aa_1)^2 (4a)^{-1}\big) \eta(a) G(\eta, \chi) - \chi\left(-\frac{a_1^2}{4} a\right)\right) - 1 \\ &= \frac{1}{2} \chi\left(-\frac{a{a_1}^2}{4}\right) (\eta(a) G(\eta, \chi) - 1) - 1 \end{aligned} \qquad (10)$$

Let

$$C_a = \sum_{s \in F_p^*} \sum_{i=1}^n \chi(g_i s a)$$

then by (3)

$$w(\mathbf{c}_\alpha) = n - S_\alpha = n - \frac{1}{p}(n + C_\alpha) = \frac{p-1}{p}\frac{q-3}{2} - \frac{1}{p}C_\alpha \tag{11}$$

To determine the weight of $\mathbf{c}_\alpha$, we need to compute C_α. In this paper we determine C_α and the weights of the code C only for the case m being even.

Note that $\chi(-\alpha a_1^2/4) = 1$ if $\mathsf{Tr}(-\alpha a_1^2/4) = 0$ and $\chi(-\alpha a_1^2/4) \neq 1$ otherwise. We have

$$\sum_{s \in \mathsf{F}_p^*} \chi\left(-\frac{\alpha a_1^2}{4}\right)^s = \begin{cases} p-1, & \text{if } \mathsf{Tr}(-\alpha a_1^2/4) = 0 \\ -1, & \text{if } \mathsf{Tr}(-\alpha a_1^2/4) \neq 0 \end{cases}$$

We have also

$$\begin{aligned} C_\alpha &= \sum_{s \in \mathsf{F}_p^*} \left(\frac{1}{2}\chi\left(-\frac{\alpha s a_1^2}{4}\right)[\eta(\alpha s)G(\eta,\chi) - 1] - 1\right) \\ &= \frac{1}{2}\sum_{s \in \mathsf{F}_p^*} \chi\left(-\frac{\alpha s a_1^2}{4}\right)[\eta(\alpha s)G(\eta,\chi) - 1] - (p-1) \\ &= \frac{1}{2}\sum_{s \in \mathsf{F}_p^*} \chi\left(-\frac{\alpha a_1^2}{4}\right)^s [\eta(\alpha s)G(\eta,\chi) - 1] - (p-1). \end{aligned}$$

If m is even, let g be a primitive element of F_q, then F_p^* is generated by $g^{\frac{p^m-1}{p-1}}$. Because $\frac{p^m-1}{p-1}$ is even, all elements of F_p^* are squares in F_q. It then follows from the formula above that

$$C_\alpha = \begin{cases} \frac{1}{2}\big(\eta(\alpha)G(\eta,\chi) - 1\big)(p-1) - (p-1), & \mathsf{Tr}(-\frac{\alpha {a_1}^2}{4}) = 0 \\ \frac{1}{2}\big(\eta(\alpha)G(\eta,\chi) - 1\big)(-1) - (p-1), & \mathsf{Tr}(-\frac{\alpha {a_1}^2}{4}) \neq 0 \end{cases}$$

By (5), C_α can take four possible values, and from (11) the code has four possible nonzero weights:

$$\begin{aligned} w_1 &= \frac{1}{2p}(p-1)(q - \sqrt{q}) \\ w_2 &= \frac{1}{2p}(\sqrt{q}+1)(p\sqrt{q} - p - \sqrt{q}) \\ w_3 &= \frac{1}{2p}(\sqrt{q}-1)(p\sqrt{q} + p - \sqrt{q}) \\ w_4 &= \frac{1}{2p}(p-1)(q + \sqrt{q}) \end{aligned}$$

When $p \geq 3$ and $m \geq 4$ is even, because $\frac{w_{min}}{w_{max}} = \frac{w_1}{w_4} = \frac{q-\sqrt{q}}{q+\sqrt{q}} > \frac{p-1}{p}$ always holds, each nonzero codeword is a minimal vector.

Proposition 12. *For all $p \geq 3$ and $m \geq 4$ even, each nonzero codeword of the quadratic form code C is a minimal vector. In the secret sharing scheme based on $\mathsf{C}^\perp$, the number of dictatorial parties is at most $p-2$. Each of the other parties is in $(p-1)p^{m-2}$ minimal access sets.*

Proof. The first half follows from the calculation above. The number of dictatorial parties is at most $p-2$ because the elements $g_1, g_2, \ldots, g_n$ are all distinct, and $\#\{g_1 a : a \in \mathsf{F}_p^*\} = p-1$. The remaining conclusion follows from Proposition 2.

8 Secret Sharing Schemes from Another Class of Codes

8.1 A Generalisation of a Class of Linear Codes

Ding and Wang described a class of linear codes for the construction of authentication codes [7]. Here we present a generalisation of their construction.

Let p be an odd prime, $q = p^m$, $d < \sqrt{q}$, and $\gcd(d, q) = 1$. We consider the linear code C over F_p defined by

$$\mathsf{C} = \left\{ \mathbf{c}_f = \left(\mathsf{Tr}(f(1)), \mathsf{Tr}(f(\alpha)), \ldots, \mathsf{Tr}(f(\alpha^{p^m-2})) \right) : f(x) \in \mathsf{F}_q^{(d)}[x] \right\}$$

where α is a primitive element of F_q, and

$$\mathsf{F}_q^{(d)}[x] = \{ f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_d x^d \in \mathsf{F}_q[x], c_i = 0 \text{ for all } p|i. \}$$

Lemma 3. C *is a* $\left[p^m - 1, md - m \left\lfloor \frac{d}{p} \right\rfloor ; p \right]$ *code.*

Proof. In the set $\{c_0, c_1, \ldots, c_d\}$, $\left\lfloor \frac{d}{p} \right\rfloor + 1$ of them are fixed as zero, all the others can take on every value of $\mathsf{F}_q = \mathsf{F}_{p^m}$. So the size of $\mathsf{F}_q^{(d)}[x]$ is $p^{m(d - \lfloor \frac{d}{p} \rfloor)}$. Next we prove $\mathbf{c}_{f_1} \neq \mathbf{c}_{f_2}$ for any two distinct polynomials $f_1, f_2 \in \mathsf{F}_q^{(d)}[x]$. Otherwise, $\mathsf{Tr}(f_1(x)) = \mathsf{Tr}(f_2(x))$ for all $x \in \mathsf{F}_q^*$. Let $g = f_1 - f_2$, then $\sum_{c \in \mathsf{F}_q} \chi(g(c)) = q$. On the other hand, by assumption $\deg(g) < \sqrt{q}$ and $\gcd(\deg(g), q) = 1$. By Weil's bound (8),

$$q = \sum_{c \in \mathsf{F}_q} \chi(g(c)) \leq (\deg(g) - 1)\sqrt{q} \leq (\sqrt{q} - 1)\sqrt{q},$$

which is impossible. So C has $p^{m(d - \lfloor \frac{d}{p} \rfloor)}$ distinct codewords. Thus its dimension is $m \left(d - \left\lfloor \frac{d}{p} \right\rfloor \right)$. This completes the proof of this lemma.

Now we give bounds on the weights in C. Let S_f denote the number of zeroes of the codeword $\mathbf{c}_f$. Because $\mathsf{Tr}(f(0)) = 0$,

$$\begin{aligned} S_f &= \# \{ x \in \mathsf{F}_q : \mathsf{Tr}(f(x)) = 0 \} - 1 \\ &= \sum_{x \in \mathsf{F}_q} \sum_{c \in \mathsf{F}_p} \frac{1}{p} e^{i \frac{2\pi}{p} (c \mathsf{Tr}(f(x)))} - 1 \\ &= \frac{1}{p} \left(q + \sum_{c \in \mathsf{F}_p^*} \sum_{x \in \mathsf{F}_q} \chi(c f(x)) \right) - 1 \end{aligned}$$

Using (8),

$$\frac{q-(p-1)(d-1)\sqrt{q}}{p} - 1 \leq S_f \leq \frac{q+(p-1)(d-1)\sqrt{q}}{p} - 1$$

Thus

$$q - \frac{q+(p-1)(d-1)\sqrt{q}}{p} \leq w_{min} \leq w_{max} \leq q - \frac{q-(p-1)(d-1)\sqrt{q}}{p}$$

Proposition 13. *When*

$$d - 1 < \frac{\sqrt{q}}{2p-1}$$

each nonzero codeword is a minimal vector. In addition, the secret sharing scheme based on $\mathsf{C}^{\perp}$ *is democratic, i.e., every participant is involved in* $(p-1)p^{md-m\lfloor \frac{d}{p} \rfloor -2}$ *minimal access sets.*

Proof. It's easily verified when $d-1 < \frac{\sqrt{q}}{2p-1}$, $\frac{w_{min}}{w_{max}} > \frac{p-1}{p}$, so the first assertion follows. To prove the scheme is democratic, we only need to prove that there does not exist $\beta \in \mathsf{F}_q^*$, $\beta \neq 1$, s.t. for any possible f, $\mathsf{Tr}(f(1)) = 0$ iff $\mathsf{Tr}(f(\beta)) = 0$. Suppose such a β exists. $\forall u \in \mathsf{F}_q^*$, let $g_u(x) = ux - ux^2 \in \mathsf{F}_q^{(d)}[x]$. Then as u ranges over F_q^*, $\mathsf{Tr}(g_u(1)) = \mathsf{Tr}(0) = 0$ always holds, but $\mathsf{Tr}(g_u(\beta)) = 0$ cannot be always true since $g_u(\beta) = u(\beta - \beta^2)$ ranges over F_q^*. So there is no such β. The conclusion then follows from Proposition 2.

Remark 1. In the construction of Ding and Wang, functions of the form $\mathsf{Tr}(ax + bx^N)$ are used to construct the linear code and its corresponding authentication code.

9 Conclusion and Remarks

We characterised the minimal vectors in linear codes, and described several classes of codes in which each nonzero codeword is a minimal vector. We then determined the access structure of the secret sharing scheme based on their duals. As described before, the access structures of these secret sharing schemes are quite interesting.

Our characterisations of the minimal vectors of linear codes are generic. However, it involves the computation of incomplete character sums. This is a hard problem in general, but can be done in certain cases. We shall work on this in a future work.

Acknowledgements

This work was supported by a grant (Project No. HKUST6179/01E) from the Research Grants Council of the Hong Kong Special Administration Region, China.

References

1. R.J. Anderson, C. Ding, T. Helleseth, and T. Kløve, How to build robust shared control systems, Designs, Codes and Cryptography **15** (1998), pp. 111–124.
2. A. Ashikhmin, A. Barg, G. Cohen, and L. Huguet, Variations on minimal codewords in linear codes, Proc. AAECC, 1995, pp. 96–105.
3. A. Ashikhmin and A. Barg, Minimal vectors in linear codes, IEEE Trans. Inf. Theory **44(5)** (1998), pp. 2010–2017.
4. L.D. Baumert and W.H. Mills Uniform cyclotomy, Journal of Number Theory **14** (1982), pp. 67-82.
5. L.D. Baumert and R.J. McEliece, Weights of irreducible cyclic codes, Information and Control **20(2)** (1972), pp. 158–175.
6. G.R. Blakley, Safeguarding cryptographic keys, Proc. NCC AFIPS, 1979, pp. 313–317.
7. C. Ding and X. Wang, A coding theory construction of new Cartesian authentication codes, preprint, 2003.
8. R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.
9. J.L. Massey, Minimal codewords and secret sharing, Proc. 6th Joint Swedish-Russian Workshop on Information Theory, August 22-27, 1993, pp. 276–279.
10. J.L. Massey, Some applications of coding theory in cryptography, Codes and Ciphers: Cryptography and Coding IV, Formara Ltd, Esses, England, 1995, pp. 33–47.
11. R.J. McEliece and D.V. Sarwate, On sharing secrets and Reed-Solomon codes, Comm. ACM **24** (1981), pp. 583–584.
12. A. Renvall and C. Ding, The access structure of some secret-sharing schemes, Information Security and Privacy, Lecture Notes in Computer Science, vol. 1172, pp. 67–78, 1996, Springer-Verlag.
13. A. Shamir, How to share a secret, Comm. ACM **22** (1979), pp. 612–613.
14. J. Yuan and C. Ding, Secret sharing schemes from two-weight codes, The Bose Centenary Symposium on Discrete Mathematics and Applications, Kolkata, Dec 2002.