A Construction of Secret Sharing Scheme

*Goh Y. L. and Denis C. K. Wong

Department of Mathematical and Actuarial Sciences,
University of Tunku Abdul Rahman,
Jalan Sungai Long, Bandar Sungai Long,
Cheras, 43000 Kajang, Selangor, Malaysia

E-mail: gohyl@utar.edu.my

*Corresponding author

ABSTRACT

In this paper, binary linear codes are used to construct the access structures of a secret sharing scheme. The relationship between the minimal codewords of a linear code and the minimal access structure are shown. Furthermore, we generalize the construction of secret sharing scheme by using semisimple group algebra codes. Finally, we study the access structures of a secret sharing scheme based on group algebra code defined by cyclic group of odd prime order over binary field.

Keywords: Secret sharing scheme, linear codes, group algebra codes

1. INTRODUCTION

To keep a secret efficiently and safely, Shamir, 1979 developed the concept of secret sharing scheme which is a rapidly developed field in cryptography. One of the well-known secret sharing scheme is constructed by Shamir, the \((n, k)\) —threshold secret sharing scheme over \(F_q\), which is defined as follows: A secret \(s \in F_q\) is split into \(n\) shares \(s_i \in F_q\) for \(i = 1, 2, \ldots, n\) in such a way that any \(k\) shares uniquely determine the secret but any \(k - 1\) or fewer shares provide no information about the secret. McEliece and Sarwate, 1981 improved the \((n, k)\) —threshold secret sharing scheme by introducing the following secret sharing scheme based on linear code: First, choose a \([n, k, n - k + 1]\) — linear MDS code \(C\) over \(F_q\). The secret is chosen as the first digit of a codeword \(v \in C\). The next \(k - 1\) digits are chosen uniformly at
random over $F_q$ and the codeword $v$ then computed. The $n - 1$ shares are all the digits in $v$ after the first digit. The threshold is $k$ because the digits in any $k$ positions of a codeword in an MDS code uniquely determine the full codeword, that is, any $k$ positions are an information set.

In a more general setting, a secret sharing scheme involved a dealer, denoted by $D$, who is responsible for selecting a secret $k$, and then computing the shares $s_i$ from the secret using some systematical algorithm. Other participants form a set $P$, who will share the secret. Furthermore, let $\tau \subseteq P$ where $\tau$ can determine the secret. $\tau$ is called the access structure and any subset of $\tau$ are called access sets. Recently, many researchers have constructed secret sharing scheme by using linear codes as the theory of algebraic coding theory have been systematically developed (Ashikhmin and Barg, 1998; Ding, Kohel and Ling, 2000; Li, Xue and Lai, 2010; Massey, 1993; Yuan and Ding, 2006).

Algebraic coding theory is important in modern digital communication; however noises might occur during the transmission of digital data across a communication channel. This may cause the received data to differ from the transmitted data. Therefore, error correcting and detecting codes are used in modern digital communication system. The study of group codes as an ideal in a group algebra $FG$ has been developed long time ago (Berman, 1967; Berman, 1989). In 1993, Massey has shown a nice relationship between the access structure and the minimal codewords of the dual code of the underlying code Massey, 1993.

In this paper, a method to construct secret sharing scheme is proposed by using group algebra codes defined over various groups. The paper is organized into four sections. Section 2 introduces the group algebra codes. In section 3, the implementation of secret sharing scheme via group algebra codes are discussed. Finally, some constructions and remarks are given in the last section.

2. SECRET SHARING SCHEME BASED ON LINEAR CODES

Before we start with the construction of secret sharing scheme, we first recall some well-known definitions from error correcting code. A $q$–ary$[n,k,d]$–linear code $C$ is a subspace of $F_q^n$ and a generator matrix of $C$ is a $k \times n$ matrix where all rows of $G$ form a basis for $C$. Any element of $C$ is called a codeword of $C$. 

Furthermore, the $n \times (n - k)$ matrix where all columns of $H$ form a basis for $C^\perp$ is called the parity check matrix of $C$. The support of $v \in F_q^n$ is defined by the set $\{0 \leq i \leq n - 1, v_i \neq 0\}$, and say that $w_1 \in F_q^n$ cover $w_2 \in F_q^n$ provided $\text{supp}(w_2) \subseteq \text{supp}(w_1)$. An element $v \neq 0$ is minimal if it covers its scalar multiples. Furthermore, a codeword whose first component is 1 and only covers its scalar multiples is called a minimal codeword. Clearly, every minimal codeword is a minimal vector. In this section, we show a construction of secret sharing scheme by using the matrices $G$ and $H$. Massey, 1993 points out a nice relationship between a minimal codeword and a minimum access structure of a secret sharing scheme. Next, we will illustrate this relationship which is proposed by Massey.

**Construction 1:** Secret sharing scheme based on a $[7,4,3]$ – binary linear code.

Let $C$ be a $[7,4,3]$ – binary linear code with the following generator matrix

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

Note that $C$ is equivalent to the well-known binary Hamming code of length $7$. Any codeword $v$ in $C$ can be written uniquely in the form

\[v = (v_1, v_2, v_3, v_4, v_1 + v_3 + v_4, v_1 + v_2 + v_4, v_2 + v_3 + v_4),\]

where $(v_1, v_2, v_3, v_4) \in F_2^4$ is the corresponding message word. The parity check matrix of $C$ is

\[
\begin{bmatrix}
1 & 1 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

It is well known that $v' \in C$ if and only if $v'H = (0, 0, 0) \in F_2^3$. Suppose we let $v' = (a, b, c, d, e, f, g)$. Then, the condition $v'H = (0, 0, 0)$ produces the following system of equations:
\[ a + c + d + e = 0 \] \hspace{1cm} (1)  \\
\[ a + b + d + f = 0 \] \hspace{1cm} (2)  \\
\[ b + c + d + g = 0 \] \hspace{1cm} (3)

From equation (1), we have
\[ a = c + d + e. \] \hspace{1cm} (4)

From equation (2), we have
\[ a = b + d + f. \] \hspace{1cm} (5)

By adding equations (1) and (3), we obtain
\[ a = b + e + g. \] \hspace{1cm} (6)

Finally, by adding equations (2) and (3), we obtain
\[ a = c + f + g. \] \hspace{1cm} (7)

Next, we setup the correspondence between each digit in a codeword, and the secret with distributions to participants as shown in Table 1. From equations (4) to (7), we see that the access structure for the secret sharing scheme with the above correspondence based on \( C \) are \( \{ P_2, P_3, P_4 \}, \{ P_1, P_3, P_5 \}, \{ P_1, P_4, P_6 \} \) and \( \{ P_2, P_5, P_6 \} \). Now, we consider the \([7, 3, 4]\) – binary dual code \( C^\perp \) of \( C \) which has the following generator matrix
\[
\begin{bmatrix}
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}
\]

All codewords of \( C^\perp \) are listed in Table 2.

TABLE 1: Correspondence between digits in codeword, secret and participants

<table>
<thead>
<tr>
<th>Digit in codeword</th>
<th>Secret and participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v_1 )</td>
<td>Secret</td>
</tr>
<tr>
<td>( v_2 )</td>
<td>( P_1 )</td>
</tr>
<tr>
<td>( v_3 )</td>
<td>( P_2 )</td>
</tr>
<tr>
<td>( v_4 )</td>
<td>( P_3 )</td>
</tr>
<tr>
<td>( v_5 )</td>
<td>( P_4 )</td>
</tr>
<tr>
<td>( v_6 )</td>
<td>( P_5 )</td>
</tr>
<tr>
<td>( v_7 )</td>
<td>( P_6 )</td>
</tr>
</tbody>
</table>
A Construction of Secret Sharing Scheme

TABLE 2: Codewords in the $[7, 3, 4]$ – binary dual code

<table>
<thead>
<tr>
<th>$F_2^3$</th>
<th>$C^\perp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0000000</td>
</tr>
<tr>
<td>100</td>
<td>1011100</td>
</tr>
<tr>
<td>010</td>
<td>1101010</td>
</tr>
<tr>
<td>001</td>
<td>0110101</td>
</tr>
<tr>
<td>110</td>
<td>0110110</td>
</tr>
<tr>
<td>101</td>
<td>1100101</td>
</tr>
<tr>
<td>011</td>
<td>1010011</td>
</tr>
<tr>
<td>111</td>
<td>0001111</td>
</tr>
</tbody>
</table>

By inspecting through each codeword in $C^\perp$ and compare the access structures obtained above, we see that all possible access structures are corresponding to the minimal codeword in $C^\perp$ with a “1” in the first position as shown in Table 3.

TABLE 3: Correspondence between minimal codewords and access structure

<table>
<thead>
<tr>
<th>Minimal codewords in $C^\perp$</th>
<th>Access structure based on $C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1011100</td>
<td>${P_2, P_3, P_4}$</td>
</tr>
<tr>
<td>1101010</td>
<td>${P_1, P_3, P_5}$</td>
</tr>
<tr>
<td>1100101</td>
<td>${P_1, P_4, P_6}$</td>
</tr>
<tr>
<td>1010011</td>
<td>${P_2, P_5, P_6}$</td>
</tr>
</tbody>
</table>

**Construction 2**: Secret sharing scheme based on a binary $[9,5,3]$ – linear code.

Let consider the $[9,5,3]$ – binary code $C$ with the following generator matrix

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}
$$

The corresponding parity check matrix for $C$ is
All codewords in $C^{\perp}$ are listed in the Table 4. For all $v = (v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9) \in C$, if we setup the correspondence as shown in Table 5, it follows that the access structure of the secret sharing scheme based on $C$ are $A_1 = \{P_1, P_4, P_5\}$, $A_2 = \{P_1, P_3, P_6\}$, $A_3 = \{P_2, P_3, P_7\}$, $A_4 = \{P_2, P_4, P_8\}$, $A_5 = \{P_2, P_4, P_5, P_7\}$, $A_6 = \{P_2, P_3, P_5, P_6, P_8\}$, $A_7 = \{P_1, P_3, P_5, P_7, P_8\}$, and $A_8 = \{P_1, P_4, P_6, P_7, P_8\}$. Therefore, the minimal access structures are $A_1$, $A_2$, $A_3$ and $A_4$.

<table>
<thead>
<tr>
<th>$F^4_2$</th>
<th>$C^{\perp}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>000000000</td>
</tr>
<tr>
<td>1000</td>
<td>110011000</td>
</tr>
<tr>
<td>0100</td>
<td>110100100</td>
</tr>
<tr>
<td>0010</td>
<td>101100010</td>
</tr>
<tr>
<td>0001</td>
<td>101010001</td>
</tr>
<tr>
<td>1100</td>
<td>000111100</td>
</tr>
<tr>
<td>1010</td>
<td>011111010</td>
</tr>
<tr>
<td>1001</td>
<td>011001001</td>
</tr>
<tr>
<td>0110</td>
<td>011010110</td>
</tr>
<tr>
<td>0101</td>
<td>011110101</td>
</tr>
<tr>
<td>0011</td>
<td>000110011</td>
</tr>
<tr>
<td>1110</td>
<td>101011110</td>
</tr>
<tr>
<td>1101</td>
<td>101101101</td>
</tr>
<tr>
<td>1011</td>
<td>110101011</td>
</tr>
<tr>
<td>0111</td>
<td>110010111</td>
</tr>
<tr>
<td>1111</td>
<td>000011111</td>
</tr>
</tbody>
</table>
In general, let $A = \{P_{i_1}, P_{i_2}, \ldots, P_{i_m}\}$ be a minimal access set of the secret sharing scheme based on a $[n,k,d]$ – linear code $C$. Suppose the columns $g_{i_1}, \ldots, g_{i_m}$ of the generator matrix $G$ of $C$ are linear dependent. Then, we have $\sum_{k=1}^{m} \lambda_k g_{i_k} = 0$, where not all $\lambda_j$ are 0. Without loss of generality, we may assume $\lambda_1 \neq 0$. Thus, we have $g_{i_1} = \sum_{k=2}^{m} \frac{\lambda_k}{\lambda_1} g_{i_k}$.

Therefore, the participants $\{P_{i_2}, \ldots, P_{i_m}\}$ can learn the share of $P_{i_1}$ by combining their shares and hence they can recover the secret which is a contradiction. Hence, we known that the columns $g_{i_1}, \ldots, g_{i_m}$ of $G$ are linear independent.

Conversely, if $c = (1, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$ is a minimal codeword, it follows that all rows $g_0, g_{i_1}, \ldots, g_{i_m}$ of $G$ are linear dependent. Thus, the set of participants $\{P_{i_1}, \ldots, P_{i_m}\}$ can recover the secret. If any proper subset of this can recover the secret, then there exists a nonzero codeword which $c$ properly covers. This contradicts the minimality of $c$. Therefore, $\{P_{i_1}, \ldots, P_{i_m}\}$ is a minimal access set.

**TABLE 5: Correspondence between digits in codeword, secret and participants**

<table>
<thead>
<tr>
<th>Digit in codeword</th>
<th>Secret and participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_1$</td>
<td>Secret</td>
</tr>
<tr>
<td>$v_2$</td>
<td>$P_1$</td>
</tr>
<tr>
<td>$v_3$</td>
<td>$P_2$</td>
</tr>
<tr>
<td>$v_4$</td>
<td>$P_3$</td>
</tr>
<tr>
<td>$v_5$</td>
<td>$P_4$</td>
</tr>
<tr>
<td>$v_6$</td>
<td>$P_5$</td>
</tr>
<tr>
<td>$v_7$</td>
<td>$P_6$</td>
</tr>
<tr>
<td>$v_8$</td>
<td>$P_7$</td>
</tr>
<tr>
<td>$v_9$</td>
<td>$P_8$</td>
</tr>
</tbody>
</table>

Then, there exist a codeword $a = (1,0,\ldots,0,a_{i_1},0,\ldots,0,a_{i_m},0,\ldots,0) \in C^\perp$. This must be truth if not then will contradict the fact that the rows of the parity check matrix $H$ of $C$ are also linearly independent. If $a_{i_j} = 0$ for some $j \in \{1,\ldots,m\}$, it follows that $\{P_{i_1}, \ldots, P_{i_{j-1}}, P_{i_{j+1}}, \ldots, P_{i_m}\}$ can recover the secret which contradict the minimality of the access structure $A$. Thus, the set of participants $\{P_{i_1}, \ldots, P_{i_m}\}$ can recover the secret. If any proper subset of this can recover the secret, then there exists a nonzero codeword which $c$ properly covers. This contradicts the minimality of $c$. Therefore, $\{P_{i_2}, \ldots, P_{i_m}\}$ is a minimal access set. Thus, we have the following proposition.
Proposition 1. The minimal access structures of a secret sharing scheme based on a \([n, k, d]\) – linear code \(C\) is the set of all minimal codewords \(v\) of the dual code \(C^\perp\) of \(C\), where \(v\) has a “1” in the first coordinate.

3. SECRET SHARING SCHEME BASED ON GROUP ALGEBRA CODES

Motivated by the construction described in the previous section, we next proposed a secret sharing scheme based on group algebra code.

Let \(F_q\) denote a finite field with \(q\) elements such that \(q\) is a prime. Given a finite group \(G\) of order \(n\), the group algebra \(F_q G\) is a vector space over \(F_q\), with basis \(G\) and so, is isomorphic to \(F_q^n\) as a vector space. The group algebra \(F_q G\) of \(G\) with coefficients in \(F_q\) is the set of all formal sums \(\sum a_g g\) where \(a_g \in F_q\). Addition and multiplication in \(F_q G\) are defined as \(\sum a_g g + \sum b_g g = \sum_{g \in G} (a_g + b_g) g\) and \(\left(\sum a_g g\right)\left(\sum h \in G b_h h\right) = \sum_{h \in G} \sum_{g \in G} (a_g b_h) g h\), respectively. A group algebra code is defined as an ideal of the group algebra \(F_q G\). In particular, if \(G\) is a cyclic group then the ideal in \(F_q G\) is a cyclic code, and if \(G\) is an abelian group then the ideal in \(F_q G\) is an abelian code.

It is well-known that if \(q \nmid n\), it follows from Maschke’s Theorem (Theorem 1.9 in Berman, 1967) that the group algebra \(F_q G\) is semisimple and hence \(F_q G\) is a direct sum of minimal ideals, \(F_q G = I_1 \oplus I_2 \oplus \cdots \oplus I_s\), where \(I_j = F_q G e_j\) is the principal ideal of \(F_q G\) generated by \(e_j\) where \(e_j\) is an idempotent in \(F_q G\) for \(j = 1, 2, \cdots, s\). Let \(M = \{e_j\}_{j=1}^s\) be the set of all pairwise orthogonal idempotents. Every ideal \(I\) of \(F_q G\) is a direct sum \(I = I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_t}\), where \(t \leq s\). Now, write \(F_q G = I \oplus J\), where \(J = I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_{s-t}}\) is the direct sum of minimal ideals such that \(I_{i_l} \neq I_{i_m}\) for all \(1 \leq l \leq t\) and \(1 \leq m \leq s - t\). Using these observations, we see that

\[
I = I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_t}
= \{e_{i_k} | k = 1, 2, \cdots, t\}
= \{u \in F_q G | u e_{i_h} = 0, \text{ for all } h = 1, 2, \cdots, s - t\}.
\]

There are some nice properties for the idempotent \(e_{i_u}\) for \(u = 1, 2, \cdots, s\). In general, an element \(e \in F_q G\) is an idempotent if \(e^2 = e\).
Furthermore, two idempotents $e_1$ and $e_2$ are orthogonal provided $e_1 e_2 = e_2 e_1 = 0$. A direct computation can show that if $e$ is an idempotent, it follows that $1 - e$ is an idempotent orthogonal to $e$. Furthermore, if $e_1$ and $e_2$ are orthogonal, it follows that $e_1 + e_2$ is an idempotent.

To construct a secret sharing scheme via group algebra codes, we proposed the following algorithms. First, to construct the secret $k$ and the corresponding shares, we proceed as follows:

**Algorithm 1:**
Choose a finite group $G$ and a finite field $F_q$ satisfying the condition that $\gcd(|G|, q) = 1$. Construct all idempotents of $F_q G$. Hence, choose a set of idempotents to construct the following group algebra code

$$I = \{ u \in F_q [G] | ue_{ih} = 0, \text{for all } h = 1,2,\ldots, s - t \}.$$  

The dealer $D$ chooses a codeword $u \in I$ and write $u$ in terms of group algebra element $u = \sum_{g \in G} a_g g$. Take the secret $k$ as $a = a_e$, where $e$ is the identity element of $G$ and the remaining $|G| - 1$ coefficients $a_g$, for all $g \neq e$, in $u = \sum_{g \in G} a_g g$ are uniformly distributed to the set of participants $P = \{ p_1, p_2, \ldots, p_{|G|-1} \}$.

Next, to recover the secret from a subset of participants and hence obtain the access structure, we used the following algorithm.

**Algorithm 2:**
Let $\tau \subseteq P$ and $\tau = \{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\}$ such that $1 \leq k \leq |G| - 1$. Form the group algebra element $w = \sum_{j=1}^{k} a_{g_{ij}} g_{ij}$. Next, $w \in I$ if and only if $we_{ih} = 0$, for all $h = 1,2,\ldots, s - t$. Form a homogeneous system of $s - t$ equations with $k$ unknowns in which the access structure can be determined from these equations. Upon solving, we can recover the coefficients $a_{g_{ij}}$ for all $j = 1,2,\ldots, k$ and hence the secret $a$.

**Example 1.** To illustrate the above algorithms, we first choose a finite group said the dihedral group of order 6, $D_6 = \langle r, s | r^3 = s^2 = 1, rs = sr^2 \rangle$. To ensure the semisimplicity of $F[D_6]$, we choose $F = \mathbb{R}$. By constructing the
character table of $D_6$, we can obtain all the three idempotents of $F[D_6]$ which are listed as follows:

\[ e_1 = \frac{1}{6}((r) + (r)s), \]
\[ e_2 = \frac{1}{6}((r) - (r)s), \]
\[ e_3 = \frac{1}{3}(1 - (r)). \]

Next, we construct the following group algebra code:

\[ I = \{ u \in \mathbb{R}[D_6] | ue_1 = ue_2 = 0 \}. \]

Any $u \in I$ can be written in the form $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$. Hence,

\[ u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s \in I \]

if and only if
\[ \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 = 0 \]
and
\[ \lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6 = 0. \]

The dealer $D$ chooses $u = 2 - \frac{1}{3}r - \frac{5}{3}r^2 \in I$. Take the secret $k = 2$ and distribute $-\frac{1}{3}$ to $P_1$ (corresponds to the term $r$) and $-\frac{5}{3}$ to $P_2$ (corresponds to the term $r^2$). To recover the secret $k$, the participants $P_1$ and $P_2$ together will form the group algebra element $w = k - \frac{1}{3}r - \frac{5}{3}r^2$. Hence, $w \in I$ if and only if $k - \frac{1}{3} - \frac{5}{3} = 0$, that is, $k = 2$.

Next, we give a detail treatment on constructing secret sharing scheme based on group algebra codes defined by cyclic group of order $p$ over binary field. Our intention is to obtain information regarding the access structure of the constructed secret sharing scheme. We follow the approach used by Ding and Ling, 2000, whereby the authors constructed secret sharing scheme based on BIBD (Balanced Incomplete Block Design). We start with the following simple results.

**Lemma 1.** Let $G = \langle g \mid g^p = 1 \rangle$ be a cyclic group of order $p$, where $p$ is an odd prime. Then, $1 + g + g^2 + \cdots + g^{p-1} = 0$ holds in $F_2[G]$. 

---

*Malaysian Journal of Mathematical Sciences*
Proof. The result is follows directly from the fact that \((g + 1)(\sum_{i=0}^{p-1} g^i) = g^p - 1 = 0\) and \(g + 1 \neq 0\).

Q.E.D.

Lemma 2. Let \(I = \{0\} \cup \prod_{h=1}^{p} A_h\),

where \(A_h = \left\{(g^i + g^j)(\sum_{t=1}^{h} g^{K_t}) | K_t \in \{0,1,2,...,p-1\}\right\} \). Then,

(i) All elements in \(A_h\) are distinct for \(h = 1,2,...,p\).

(ii) For all \(1 \leq h < w \leq p\), \(A_h \cap A_w = \{\}.\)

Proof. For part (i), the proof is by using mathematical induction on the integer \(h \geq 1\). We show the case for \(h = 1\), for the inductive step the proof is follows exactly the same way. When \(h = 1\), we have \(A_1 = \left\{(g^i + g^j)g^{K_1} | K_1 \in \{0,1,2,...,p-1\}\right\} \). Assume \((g^i + g^j)g^{K_1} = (g^i + g^j)g^{K_2}\) for distinct integers \(K_1\) and \(K_2\). Thus, upon cancellation, we obtained \(K_1 = K_2\) which is a contradiction. For part (ii), assume there exists an element \(x \in A_h \cap A_w\). Hence, we have \(\sum_{t=1}^{h} g^{K_t} = \sum_{t=1}^{w} g^{K_t}\) for \(1 \leq h < w \leq p\). Upon cancellation, we obtain \(\sum_{j=h+1}^{w} g^{K_j} = 0\) and so \(g^{K_{h+1}}(1 + g + g^2 + \cdots + g^{K_w-K_{h+1}}) = 0\) which contradicts Lemma 1. Therefore, the result follows directly.

Q.E.D.

Theorem 1. Consider \(I\) in Lemma 2. Then,

(i) \(I = (g^i + g^j)\) for all \(1 \leq i < j \leq p\).

(ii) \(|I| = 2^{p-1}\).

(iii) For all \(v \in I\), \(wt(v)\) is even.

(iv) \(I\) is a \([p,p-1,2]\) - MDS code.

Proof. Part (i) is directly follows from the definition of principal ideal generated by the group algebra element \(g^i + g^j\). For part (ii), we note that \(|A_h| = \binom{p}{h}\) for \(h = 1,2,...,p\). Hence, \(|I| = \frac{\sum_{h=0}^{p} \binom{p}{h}}{2} = 2^{p-1}\). For part (iii), we prove by contradiction by assuming that there exists an element in \(I\) with odd weight which is impossible. The linearity of \(I\) follows from the property of ideal. The parameters of the code \(I\) in part (iv) follows immediately from parts (i) to (iii).

Q.E.D.
Remark. From Theorem 1, we deduce that the secret sharing scheme based on \( I \) is for sharing secrets among \( p - 1 \) participants. There are \( p \) possible access structures. Each access structure consists of \( 2^i \) participants for \( 1 \leq i \leq p - 1 \) and each participants is a member of exactly 2 access structures.

Example 2. Let \( p = 5 \).
Consider \( I = (g^2 + g^3) = \{(g^2 + g^3) \sum_{i=0}^{4} a_i g^i \mid a_i \in F_2\} = \{(a_2 + a_3) + (a_3 + a_4)g + (a_0 + a_4)g^2 + (a_0 + a_1)g^3 + (a_1 + a_2)g^4 \mid a_i \in F_2\} \).

Suppose the dealer chooses the codeword \( u = 1 + g^2 + g^3 + g^4 \). So the secret is 1, and the dealer distribute 0 to \( P_1 \), 1 to \( P_2 \), 1 to \( P_3 \) and 1 to \( P_4 \). Assume that the participants \( P_1 \) and \( P_2 \) wanted to compute the secret. Then, both participants will form the equations \( a_3 + a_4 = 0 \) and \( a_0 + a_4 = 1 \). However, by solving these two equations, both participants cannot compute the secret \( a_2 + a_3 \). Next, assume that the participants \( P_1, P_2 \) and \( P_4 \) wanted to compute the secret. Then, the equations \( a_3 + a_4 = 0 \), \( a_0 + a_4 = 1 \) and \( a_1 + a_2 = 0 \) are formed, in which case this system of homogeneous equations is solvable but do not have unique solution. We conclude that the secret can be recovered; however, it may not be a valid secret.

4. CONCLUSION

The two algorithms proposed here are depended heavily on the group algebra codes, in which the idempotents used to generate the codes play an equally important role in determining the minimal access structure of a constructed secret sharing scheme. Our future investigation is to use the group algebra codes obtained in Denis. and Ang, 2013a; 2013b together with algorithms 1 and 2 proposed here to obtain a nice relationship between minimal codewords and minimal access structures.

REFERENCES


