Research article

Group codes over symmetric groups

Yanyan Gao$^{1, *}$ and Yangjiang Wei$^2$

$^1$ School of Mathematics and Physics, Nanjing Institute of Technology, Nanjing, 211167, China
$^2$ School of Mathematics and Statistics Sciences, Nanning Normal University, Nanning, 530023, China

* Correspondence: Email: gyy_318@163.com.

Abstract: Let $\mathbb{F}_q$ be a finite field of characteristic $q$ and $S_n$ a symmetric group of order $n!$. In this paper, group codes in the symmetric group algebras $\mathbb{F}_q S_n$ with $q > 3$ and $n = 3, 4$ are proposed. We compute the unique (linear and nonlinear) idempotents of $\mathbb{F}_q S_n$ corresponding to the characters of symmetric groups and use the results to characterize the minimum distances and dimensions of group codes. Furthermore, we construct MDS group codes and almost MDS group codes in $\mathbb{F}_q S_3$ and $\mathbb{F}_q S_4$.

Keywords: group codes; group algebra; minimum distance; symmetric group

Mathematics Subject Classification: 94B05

1. Introduction

Group codes, a class of important linear codes, play a vital role in error correction coding. A linear code $C$ is called a group code if it is just a one-sided (left or right) ideal in a group algebra $R[G]$, where $R$ is a commutative ring and $G$ is a finite group. If $G$ is abelian, then $C$ is an abelian code.

A brief survey on group codes of some recent results is provided as follows. Polcino Milies et al. [13] calculated the minimum distances and the dimensions of all cyclic codes of length $p^n$ over a finite field $\mathbb{F}_q$, when $p$ is an odd prime and $\mathbb{F}_q$ is a finite field with $q$ elements, assuming that $\bar{q}$ generates the group of invertible elements of the residue ring module $p^n$, denoted by $\mathbb{Z}_{p^n}$. Jitman et al. [11] gave a characterization and an enumeration of Euclidean self-dual and Euclidean self-orthogonal abelian codes in a principal ideal group algebra. Choosuwan et al. [5] gave the complete enumeration of self-dual abelian codes in nonprincipal ideal group algebras $\mathbb{F}_{2^k}[A \times \mathbb{Z}_2 \times \mathbb{Z}_2]$ with respect to both the Euclidean and Hermitian inner products, where $k$ and $s$ are positives and $A$ is an abelian group of odd order. In 2017, Boripan et al. [1] studied a family of abelian codes with complementary dual in a group algebra $\mathbb{F}_{p^v}[G]$ in the two cases of Euclidean and Hermitian inner products, where $p$ is a prime, $v$ is a positive integer, and $G$ is an arbitrary finite abelian group. Cao et al. [3, 4] proved that any left $D_{2n}$-code...
Then operator as follows: for elements of \( q \) with \( \text{gcd}(q, p) = 1 \). Brochero Martínez et al. [12] determined an explicit expression for the primitive idempotents of \( \mathbb{F}_q[G] \), where \( \mathbb{F}_q \) is a finite field, \( G \) is a finite cyclic group of order \( p^k \) and \( p \) is an odd prime with \( \text{gcd}(q, p) = 1 \). Based on the idea, Gao et al. [7] described and counted all linear complementary dual (LCD) codes and self-orthogonal codes in the generalized quaternion group algebras \( \mathbb{F}_q[Q_{4n}] \). It is a pity that the authors cannot give the parameters of group codes.

To address this issue, we can use the character label of corresponding groups to determine the idempotents of group algebras. Let \( S_n \) be a symmetric group of order \( n! \). In this paper, we propose group codes in symmetric group algebras \( \mathbb{F}_q S_n \) with \( q > 3 \) and \( n = 3, 4 \). We compute the unique (linear and nonlinear) idempotents of \( \mathbb{F}_q S_n \) corresponding to the characters of symmetric groups and use the results to characterize the minimum distances and dimensions of group codes. Furthermore, we construct MDS group codes and almost MDS group codes in \( \mathbb{F}_q S_3 \) and \( \mathbb{F}_q S_4 \).

The paper is organized as follows: Section 2 provides a review of some properties of group algebras and other preliminaries, while Section 3 investigates group codes in symmetric group algebras \( \mathbb{F}_q S_n \) with \( q > 3 \) and \( n = 3, 4 \), and obtains the parameters of all the above group codes.

2. Preliminaries

Let \( \mathbb{F}_q[G] \) be a group algebra, where \( \mathbb{F}_q \) is a finite field and \( G \) is a finite group. In fact, the group algebra \( \mathbb{F}_q[G] \) is a vector space over \( \mathbb{F}_q \) with basis \( G \), and it has scalar, additive, and multiplicative operator as follows: for \( c, a_g, b_g \in \mathbb{F}_q \) and \( g \in G \),

\[
ct(\sum_{g \in G} a_g g) = \sum_{g \in G} ca_g g,
\]

\[
\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,
\]

\[
(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g \in G} \sum_{u=v} a_u b_v g.
\]

Then \( \mathbb{F}_q[G] \) is an associative \( \mathbb{F}_q \)-algebra with the identity \( 1 = 1_{\mathbb{F}_q} 1_G \), where \( 1_{\mathbb{F}_q} \) and \( 1_G \) are the identity elements of \( \mathbb{F}_q \) and \( G \), respectively. Readers are referred to [14, 16] for more details on group ring or group algebra.

**Lemma 2.1.** (Maschke’s Theorem [14]) Let \( R \) be a ring and \( G \) be a group. Then the group ring \( R[G] \) is semisimple if and only if the following conditions hold.

(i) \( R \) is a semisimple ring.
By Lemma 2.1, it is easy to verify that \( \mathbb{F}_q[G] \) is semisimple if and only if \( G \) is a finite group and \( \text{char}(\mathbb{F}_q) \nmid |G| \). Let \( \mathbb{F}_q[G] \) be a semisimple group algebra. Then \( \mathbb{F}_q[G] \) can be decomposed into a direct sum \( \mathbb{F}_q[G] = \bigoplus_{i \in \Omega} \mathbb{F}_q[G]e_i \), where \( \mathbb{F}_q[G]e_i \) is the minimal ideal generated by the idempotent \( e_i \), \( i \in \Omega \) and \( \Omega \) is the index set (see [9]). If \( I \) is any ideal of \( \mathbb{F}_q[G] \), then \( I \) can be expressed as a direct sum of some minimal ideal \( \mathbb{F}_q[G]e_i \) of \( \mathbb{F}_q[G] \), i.e., \( I = \bigoplus_{i \in \Omega} \mathbb{F}_q[G]e_i \). Let \( I \) be an ideal generated by a subset \( \Omega_1 \) and \( \Lambda = \Omega \setminus \Omega_1 \). Then \( I = I_{\Lambda} \). (\( \alpha \in \mathbb{F}_q[G]\) \( \alpha e_j = 0 \) for all \( e_j \in \Lambda \)).

Suppose that \( \alpha = \sum_{g \in G} a_g g \in \mathbb{F}_q[G] \). Then \( \text{wt}(\alpha) = \|a_g : a_g \neq 0\| \) is called the Hamming weight of \( \alpha \) (\([19]\)). Let \( I_{\Lambda} \) be a group code in \( \mathbb{F}_q[G] \). Its length \( n \) is the order of \( G \) in group algebra \( \mathbb{F}_q[G] \). Its dimension \( k \) is the dimension of \( \text{I}_{\Lambda} \) as a subspace over \( \mathbb{F}_q \). Its minimal distance \( d \) is defined as \( d = \min \{\text{wt}(\alpha) : \alpha e_i = 0 \} \) for nonzero element \( \alpha \) and for all \( e_i \in \Lambda \). Thus the group code \( I_{\Lambda} \) is called an \( [n, k, d] \) code. Moreover, a linear \( [n, k, d] \) group code over \( \mathbb{F}_q \) with \( d = n - k + 1 \) is called a maximum distance separable (MDS) group code. And, a linear \( [n, k, d] \) group code over \( \mathbb{F}_q \) with \( d = n - k \) is called an almost MDS (AMDS) group code. MDS codes and AMDS codes are considered to be an attractive solution for information storage as they operate at the optimal storage versus reliability trade-off (see \([8, 15, 17, 18, 20, 21]\)).

Based on the following lemma, we can give the unique idempotents of \( \mathbb{F}_q[G] \).

**Lemma 2.2.** \([10]\) If \( \chi \) is a character of \( \mathbb{F}_qG \)-module, then the idempotents corresponding to the character \( \chi \) are given by

\[
e = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g.
\]

### 3. Group codes in \( \mathbb{F}_qS_n \)

#### 3.1. Group codes in \( \mathbb{F}_qS_3 \)

In the subsection, we will consider the group codes on \( S_3 \), where \( S_3 \) is a nonabelian group with the smallest order. Let

\[
S_3 = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle = \{1, a, a^2, b, ab, a^2b\}.
\]

It is well-known that \( S_3 \) is all the permutations on three elements 1,2,3. In this sense, set \( a = (123) \), \( b = (12) \), \( S_3 \) can be given by \( \{1\}, \{1\}, (123), (132), (12), (23), (13) \). For convenience, we denote \( g_i \) (\( 1 \leq i \leq 6 \)) as the \( i \)-th element of \( S_3 \) in the above two sets.

In addition, \( S_3 \) has three conjugacy classes as follows:

\[
C_1 = \{1\}, C_2 = \{b, ab, a^2b\}, C_3 = \{a, a^2\}.
\]

Since the commutator group of \( S_3 \) is \( S_3' = \{1, a, a^2\} \), we have \( |S_3/S_3'| = 2 \). As a consequence of this, the group \( S_3 \) has two linear characters \( \chi_1, \chi_2 \) and one nonlinear character \( \chi_3 \). The character table of \( S_3 \) is as follows (see Table 1).
Table 1. The character table of $S_3$.

<table>
<thead>
<tr>
<th>Characters</th>
<th>1</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

By Lemma 2.2, the unique idempotents of $\mathbb{F}_q S_3$ are given in the following theorem.

**Theorem 3.1.** There are three idempotents in $\mathbb{F}_q S_3$ as follows:

$$
e_1 = \frac{1}{6}[1 + \overline{C}_2 + \overline{C}_3],$$

$$
e_2 = \frac{1}{6}[1 - \overline{C}_2 + \overline{C}_3],$$

$$
f_1 = \frac{1}{6}[2 - \overline{C}_3],$$

where $\overline{C}_i = \sum_{g \in C_i} g, i = 2, 3.$

In order to construct the group codes of $\mathbb{F}_q S_3$, we need the product between idempotents $e_1, e_2, f_1$ and an arbitrary element of $\mathbb{F}_q S_3$. For any element $\alpha = \sum_{i=1}^{6} a_i g_i \in \mathbb{F}_q S_3$, where $a_i \in \mathbb{F}_q, i = 1, 2, \ldots, 6$, we have

$$\alpha e_1 = (\sum_{i=1}^{6} a_i)e_1.$$  \hfill (3.1)

$$\alpha e_2 = (\sum_{i=1}^{3} a_i - \sum_{i=4}^{6} a_i)e_2.$$  \hfill (3.2)

$$\alpha f_1 = \frac{1}{6}[(2a_1 - a_2 - a_3)g_1 + (-a_1 + 2a_2 - a_3)g_2 + (-a_1 - a_2 + 2a_3)g_3 + (2a_4 - a_5 - a_6)g_4 + (-a_4 + 2a_5 - a_6)g_5 + (-a_4 - a_5 + 2a_6)g_6].$$  \hfill (3.3)

The following theorems give us the parameters of group codes in $\mathbb{F}_q S_3$.

**Theorem 3.2.** Let $e_1, e_2$ and $f_1$ be idempotents in $\mathbb{F}_q S_3$. Then

1. $I_{\{e_1\}}$ is a [6,5,2] group code;
2. $I_{\{e_2\}}$ is a [6,5,2] group code;
3. $I_{\{f_1\}}$ is a [6,2,3] group code.

**Proof.** (1) Clearly, $I_{\{e_1\}} = \{\alpha \in \mathbb{F}_q S_3 | \alpha e_1 = 0\}$. Firstly, we will give the dimension of group code $I_{\{e_1\}}$. For any $\alpha = \sum_{i=1}^{6} a_i g_i \in I_{\{e_1\}}$, we have $\alpha e_1 = 0$. By (3.1), we obtain $\sum_{i=1}^{6} a_i = 0$. Then dim($I_{\{e_1\}}$) = 5. Secondly, we will compute the minimal distance of group code $I_{\{e_1\}}$. For some $\alpha = kg_i, 1 \leq i \leq 6$, if $k \neq 0$, then $\alpha e_1 \neq 0$, i.e., $\alpha = kg_i \notin I_{\{e_1\}}$. So d($I_{\{e_1\}}$) $\geq$ 2. Set $\alpha = g_1 - g_2$. Since $\alpha e_1 = (g_1 - g_2)e_1 = 0$, we get $\alpha = g_1 - g_2 \in I_{\{e_1\}}$. Hence, d($I_{\{e_1\}}$) = 2.
Secondly, we will compute the minimal distance of group code \(I_{|e_2|}\). For any \(e = \sum a_i g_i \in I_{|e_2|}\), we have \(ae_2 = 0\). By (3.2), we obtain \(\sum a_i = 0\). Then \(\dim(I_{|e_2|}) = 5\).

Secondly, we will compute the minimal distance of group code \(I_{|e_2|}\). For some \(\alpha = k g_i, 1 \leq i \leq 6\), if \(k \neq 0\), then \(\alpha e_2 \neq 0\), i.e., \(\alpha = k g_i \notin I_{|e_2|}\). So \(d(I_{|e_2|}) \geq 2\). Set \(\alpha = g_1 + g_4\). Since \(\alpha e_2 = (g_1 + g_4)e_2 = 0\), we get \(\alpha = g_1 + g_4 \in I_{|e_2|}\). Hence, \(d(I_{|e_2|}) = 2\).

(3) Clearly, \(I_{|f_1|} = \{\alpha \in \mathbb{F}_q S_3 | \alpha e_1 = 0\}\). Firstly, we will give the dimension of group code \(I_{|f_1|}\). For any \(\alpha = \sum a_i g_i \in I_{|f_1|}\), we have \(\alpha f_1 = 0\). By (3.3), we obtain

\[
\begin{align*}
2a_1 - a_2 - a_3 &= 0 \\
-a_1 + 2a_2 - a_3 &= 0 \\
-a_1 - a_2 + 2a_3 &= 0 \\
2a_4 - a_5 - a_6 &= 0 \\
-a_4 + 2a_5 - a_6 &= 0 \\
-a_4 - a_5 + 2a_6 &= 0
\end{align*}
\]

Since the rank of the coefficient matrix of the above equation is 4, we know that \(\dim(I_{|f_1|}) = 2\).

Secondly, we will compute the minimal distance of group code \(I_{|f_1|}\). For some \(\alpha = k g_i + k_j g_j, 1 \leq i, j \leq 6\), if \(k_i, k_j \neq 0\), then \(\alpha f_1 \neq 0\), i.e., \(\alpha = k g_i + k_j g_j \notin I_{|f_1|}\). So \(d(I_{|f_1|}) \geq 3\). Set \(\alpha = g_1 + g_2 + g_3\). Since \(\alpha f_1 = (g_1 + g_2 + g_3)f_1 = 0\), we get \(\alpha = g_1 + g_2 + g_3 \in I_{|f_1|}\). Hence, \(d(I_{|f_1|}) = 3\).

This completes the proof. 

\[\square\]

**Theorem 3.3.** Let \(e_1, e_2\) and \(f_1\) be idempotents in \(\mathbb{F}_q S_3\). Then

(1) \(I_{|e_1| e_2}\) is a \([6,4,2]\) group code;

(2) \(I_{|e_1| f_1}\) is a \([6,1,6]\) group code;

(3) \(I_{|e_2| f_1}\) is a \([6,1,6]\) group code.

**Proof.** (1) Clearly, \(I_{|e_1| e_2|} = \{\alpha \in \mathbb{F}_q S_3 | \alpha e_1 = 0, \alpha e_2 = 0\}\). Firstly, we will give the dimension of group code \(I_{|e_1| e_2|}\). For any \(\alpha = \sum a_i g_i \in I_{|e_1| e_2|}\), we have \(\alpha e_1 = 0\) and \(\alpha e_2 = 0\). From (3.1) and (3.2), we obtain

\[
\begin{align*}
\frac{a_1 + a_2 + a_3 + a_4 + a_5 + a_6}{a_1 + a_2 + a_3 - a_4 - a_5 - a_6} &= 0
\end{align*}
\]

Since the rank of the coefficient matrix of the above equation is 2, we know that \(\dim(I_{|e_1| e_2|}) = 4\).

Secondly, we will compute the minimal distance of group code \(I_{|e_1| e_2|}\). For some \(\alpha = k g_i, 1 \leq i \leq 6\), if \(k \neq 0\), then \(\alpha e_1 \neq 0\), i.e., \(\alpha = k g_i \notin I_{|e_1| e_2|}\). So \(d(I_{|e_1| e_2|}) \geq 2\). Set \(\alpha = g_1 - g_3\). Since \(\alpha e_1 = (g_1 - g_3)e_1 = 0\) and \(\alpha e_2 = (g_1 - g_3)e_2 = 0\), we get \(\alpha = g_1 - g_3 \in I_{|e_1| e_2|}\). Hence, \(d(I_{|e_1| e_2|}) = 2\).

(2) Clearly, \(I_{|e_1| f_1|} = \{\alpha \in \mathbb{F}_q S_3 | \alpha e_1 = 0, \alpha f_1 = 0\}\). Firstly, we will give the dimension of group code
\( I_{(e_i,f_i)} \). For any \( \alpha = \sum_{i=1}^{6} a_i g_i \in I_{(e_i,f_i)} \), we have \( \alpha e_1 = 0 \) and \( \alpha f_1 = 0 \). From (3.1) and (3.3), we obtain

\[
\begin{align*}
\alpha &= a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 0 \\
2a_1 - a_2 - a_3 &= 0 \\
-a_1 + 2a_2 - a_3 &= 0 \\
-a_1 - a_2 + 2a_3 &= 0 \\
2a_4 - a_5 - a_6 &= 0 \\
-a_4 + 2a_5 - a_6 &= 0 \\
-a_4 - a_5 + 2a_6 &= 0
\end{align*}
\]

Since the rank of the coefficient matrix of the above equations is 5, we know that \( \dim(I_{(e_i,f_i)}) = 1 \). Secondly, we will compute the minimal distance of group code \( I_{(e_i,f_i)} \). If we take \( \alpha = g_1 + g_2 + g_3 \), we have \( \alpha f_1 = 0 \) and \( \alpha e_1 \neq 0 \), i.e., \( \alpha = g_1 + g_2 + g_3 \notin I_{(e_i,f_i)} \). So \( d(I_{(e_i,f_i)}) \geq 3 \). Set \( \alpha = g_1 + g_2 + g_3 - g_4 - g_5 - g_6 \). Since \( \alpha e_1 = (g_1 + g_2 + g_3 - g_4 - g_5 - g_6) e_1 = 0 \) and \( \alpha e_2 = (g_1 + g_2 + g_3 - g_4 - g_5 - g_6) f_1 = 0 \), we get \( \alpha = g_1 + g_2 + g_3 - g_4 - g_5 - g_6 \notin I_{(e_i,f_i)} \). Hence, \( d(I_{(e_i,f_i)}) = 6 \).

(3) The result can be obtained by a similar proof of (2).

This completes the proof. \[ \square \]

We can get the following results based on Theorems 3.2 and 3.3.

**Remark 3.4.** Let \( e_1, e_2 \) and \( f_1 \) be idempotents in \( \mathbb{F}_q S_3 \).

1. \( I_{(e_i)} \) and \( I_{(e_i,f_i)} \), \( i = 1, 2 \) are MDS group codes;
2. \( I_{(e_i,f_i)} \) is an AMDS group codes.

### 3.2. Group codes in \( \mathbb{F}_q S_4 \)

In the subsection, we will consider the group codes on \( S_4 \), where \( S_4 \) is a nonabelian group of order 24. Let

\[
S_4 = \langle a, b : a^4 = b^2 = (ab)^4 = 1 \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b, ba, aba, a^2ba, a^3ba, ba^2, aba^2, a^2ba^2, a^3ba^2, ba^3, aba^3, a^2ba^3, a^3ba^3, ba^2b, aba^2b, a^2ba^2b, a^3ba^2b \}.
\]

It is well-known that \( S_4 \) is all the permutations on four elements 1, 2, 3, 4. In this sense, set \( a = (1234), b = (12) \), \( S_4 \) can be given by \( \{(1), (1234), (13)(24), (1432), (12), (234), (1324), (143), (134), (1243), (142), (23), (1423), (132), (34), (124), (243), (14), (123), (1342), (14)(23), (13), (12)(34), (24) \} \). For convenience, we denote \( g_i \) \( (1 \leq i \leq 24) \) as the \( i \)-th element of \( S_4 \) in the above two sets.

In addition, \( S_4 \) has five conjugacy classes as follows:

\[
\begin{align*}
C_1 &= \{(1)\}, \\
C_2 &= \{(12), (13), (14), (23), (24), (34)\}, \\
C_3 &= \{(12)(34), (13)(24), (14)(23)\}, \\
C_4 &= \{(123), (132), (234), (243), (124), (142), (134), (143)\}, \\
C_5 &= \{(1234), (1432), (1324), (1243), (1423), (1342)\}.
\end{align*}
\]
Since the commutator group of $S_4$ is $S_4' = A_4$, we have $|S_4/S_4'| = 2$. As a consequence of this, the group $S_4$ has two linear characters $\chi_1, \chi_2$ and three nonlinear characters $\chi_3, \chi_4, \chi_5$. The character table of $S_4$ is as follows (see Table 2).

**Table 2.** The character table of $S_4$.

<table>
<thead>
<tr>
<th>Characters</th>
<th>(1)</th>
<th>(12)</th>
<th>(12)(34)</th>
<th>(123)</th>
<th>(1234)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>3</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

By Lemma 2.2, the unique idempotents of $\mathbb{F}_qS_4$ are given in the following theorem.

**Theorem 3.5.** There are five idempotents in $\mathbb{F}_qS_4$ as follows:

\[
e_1 = \frac{1}{24} [1 + \overline{C}_2 + \overline{C}_3 + \overline{C}_4 + \overline{C}_5],
\]

\[
e_2 = \frac{1}{24} [1 - \overline{C}_2 + \overline{C}_3 + \overline{C}_4 - \overline{C}_5],
\]

\[
f_1 = \frac{1}{24} [2 + 2\overline{C}_3 - \overline{C}_4],
\]

\[
f_2 = \frac{1}{24} [3 + \overline{C}_2 - \overline{C}_3 - \overline{C}_5],
\]

\[
f_3 = \frac{1}{24} [3 - \overline{C}_2 - \overline{C}_3 + \overline{C}_5],
\]

where $\overline{C}_i = \sum_{g \in C_i} g, i = 2, 3, 4, 5$.

In order to construct the group codes of $\mathbb{F}_qS_4$, we need the product between idempotents $e_1, e_2, f_1, f_2, f_3$ and an arbitrary element of $\mathbb{F}_qS_4$. For any element $\alpha = \sum_{i=1}^{24} a_i g_i \in \mathbb{F}_qS_4$, where $a_i \in \mathbb{F}_q, i = 1, 2, \ldots, 24$, we have

\[
\alpha e_1 = \left( \sum_{i=1}^{24} a_i \right) e_1, \tag{3.4}
\]

\[
\alpha e_2 = \left( (a_1 + a_3 + a_6 + a_8 + a_9 + a_{11} + a_{14} + a_{17} + a_{19} + a_{21} + a_{23}) - (a_2 + a_4 + a_5 + a_7 + a_{10} + a_{12} + a_{13} + a_{15} + a_{18} + a_{20} + a_{22} + a_{24}) \right) e_2, \tag{3.5}
\]

\[
\alpha f_1 = \frac{1}{24} [2(a_1 + 2a_3 + 2a_{21} + 2a_{23} - a_6 - a_8 - a_9 - a_{11} - a_{14} - a_{16} - a_{17} - a_{19}) + (2a_2 + 2a_4 + 2a_{22} + 2a_{24} - a_5 - a_{10} - 2a_{12} - a_{13} - a_{15} - a_{18} - a_{20}) + (2a_5 + 2a_7 + 2a_{13} + 2a_{15} - a_2 - a_4 - a_{10} - a_{12} - a_{18} - a_{20} - a_{22} - a_{24}) + (2a_6 + 2a_8 + 2a_{14} + 2a_{16} - a_1 - a_3 - a_9 - a_{11} - a_{17} -...
\]

AIMS Mathematics  Volume 8, Issue 9, 19842–19856.
Theorem 3.6. Let $e_i, i = 1, 2$ and $f_j, j = 1, 2, 3$ be idempotents in $\mathbb{F}_q S_4$. Then

(1) $I_{e_i}$ is a $\{24, 23, 2\}$ group code, for $i = 1, 2$;

AIMS Mathematics

Volume 8, Issue 9, 19842–19856.
(2) $I_{(f_1)}$ is a $[24,20,2]$ group code;

(3) $I_{(f_j)}$ is a $[24,15,4]$ group code, for $j = 2, 3$.

Proof. (1) Clearly, $I_{(e_i)} = \{ \alpha \in \mathbb{F}_q S_4 | \alpha e_i = 0 \}$, for $i = 1, 2$. Firstly, we will give the dimension of group code $I_{(e_i)}$, $i = 1, 2$. For any $\alpha = \sum_{i=1}^{24} a_i g_i \in I_{(e_i)}$, we have $\alpha e_i = 0$. By (3.4), we obtain the following equation:

$$
\sum_{i=1}^{24} a_i = 0. \quad (3.6)
$$

By (3.5), we obtain the following equation:

$$
(a_1 + a_3 + a_6 + a_9 + a_{11} + a_{14} + a_{17} + a_{19} + a_{21} + a_{23})
- (a_2 + a_4 + a_7 + a_{10} + a_{12} + a_{13} + a_{15} + a_{18} + a_{20} + a_{22} + a_{24}) = 0. \quad (3.7)
$$

Then, for $i = 1, 2$, we have $\dim(I_{(e_i)}) = 5$. Secondly, we will compute the minimal distance of group code $I_{(e_i)}$. For some $\alpha = kg_i$, $1 \leq i \leq 24$, if $k \neq 0$, then $\alpha e_i \neq 0$, i.e., $\alpha = kg_i \notin I_{(e_i)}$. So $d(I_{(e_i)}) \geq 2$. Set $\alpha = g_1 - g_3$. Since $\alpha e_i = (g_1 - g_3)e_i = 0$, we get $\alpha = g_1 - g_3 \in I_{(e_i)}$. Hence, $d(I_{(e_i)}) = 2$.

(2) Clearly, $I_{(f_1)} = \{ \alpha \in \mathbb{F}_q S_4 | \alpha f_1 = 0 \}$. Firstly, we will give the dimension of group code $I_{(f_1)}$. For any $\alpha = \sum_{i=1}^{24} a_i g_i \in I_{(f_1)}$, we have $\alpha f_1 = 0$. Then, we obtain the following equations:

$$
2a_1 + 2a_3 + 2a_{21} + 2a_{23} - a_6 - a_8 - a_9 - a_{11} - a_{14} - a_{16} - a_{17} - a_{19} = 0. \quad (3.8)
$$

$$
2a_2 + 2a_4 + 2a_{22} + 2a_{24} - a_5 - a_7 - a_{10} - a_{12} - a_{13} - a_{15} - a_{18} - a_{20} = 0. \quad (3.9)
$$

$$
2a_5 + 2a_7 + 2a_{13} + 2a_{15} - a_2 - a_4 - a_{10} - a_{12} - a_{18} - a_{20} - a_{22} - a_{24} = 0. \quad (3.10)
$$

$$
2a_6 + 2a_8 + 2a_{14} + 2a_{16} - a_1 - a_3 - a_9 - a_{11} - a_{17} - a_{19} - a_{21} - a_{23} = 0. \quad (3.11)
$$

$$
2a_9 + 2a_{11} + 2a_{17} + 2a_{19} - a_1 - a_3 - a_9 - a_{16} - a_{18} - a_{21} - a_{23} = 0. \quad (3.12)
$$

$$
2a_{10} + 2a_{12} + 2a_{18} + 2a_{20} - a_2 - a_4 - a_5 - a_7 - a_{13} - a_{15} - a_{22} - a_{24} = 0. \quad (3.13)
$$

Since the rank of the coefficient matrix of the above equations is 4, we know that $\dim(I_{(f_1)}) = 20$. Secondly, we will compute the minimal distance of group code $I_{(f_1)}$. For some $\alpha = kg_i$, $1 \leq i \leq 24$, if $k \neq 0$, then $\alpha f_1 \neq 0$, i.e., $\alpha = kg_i \notin I_{(f_1)}$. So $d(I_{(f_1)}) \geq 2$. Set $\alpha = g_2 - g_4$. Since $\alpha f_1 = (g_2 - g_4)f_1 = 0$, we get $\alpha = g_2 - g_4 \in I_{(f_1)}$. Hence, $d(I_{(f_1)}) = 2$.

(3) Clearly, $I_{(f_j)} = \{ \alpha \in \mathbb{F}_q S_4 | \alpha f_i = 0 \}$, $i = 2, 3$. Firstly, we will give the dimension of group code $I_{(f_j)}$. For any $\alpha = \sum_{i=1}^{24} a_i g_i \in I_{(f_j)}$, we have $\alpha f_2 = 0$. Then, we obtain a corresponding system of equations:

$$
3a_1 + a_5 + a_{12} + a_{15} + a_{18} + a_{22} + a_{24} - a_3 - a_{21}
- a_{23} - a_2 - a_4 - a_7 - a_{10} - a_{13} - a_{20} = 0. \quad (3.14)
$$
\begin{align*}
3a_2 + a_6 + a_9 + a_{16} + a_{19} + a_{21} + a_{23} - a_4 - a_{22} = 0. \\
-a_{24} - a_1 - a_3 - a_8 - a_{11} - a_{14} - a_{17} = 0. \\
3a_3 + a_7 + a_{10} + a_{13} + a_{20} + a_{22} + a_{24} - a_1 - a_{21} = 0. \\
-a_{23} - a_2 - a_4 - a_5 - a_{12} - a_{15} - a_{18} = 0. \\
3a_4 + a_8 + a_{11} + a_{14} + a_{17} + a_{21} + a_{23} - a_2 - a_{22} = 0. \\
-a_{24} - a_1 - a_3 - a_6 - a_9 - a_{16} - a_{19} = 0. \\
3a_5 + a_1 + a_{11} + a_{14} + a_{16} + a_{19} + a_{23} - a_7 - a_{13} = 0. \\
-a_{15} - a_2 - a_6 - a_8 - a_9 - a_{17} - a_{21} = 0. \\
3a_6 + a_2 + a_{12} + a_{13} + a_{15} + a_{20} + a_{24} - a_8 - a_{14} = 0. \\
-a_{16} - a_3 - a_5 - a_7 - a_{10} - a_{18} - a_{22} = 0. \\
3a_7 + a_3 + a_9 + a_{14} + a_{16} + a_{17} + a_{21} - a_5 - a_{13} = 0. \\
-a_{15} - a_1 - a_6 - a_8 - a_{11} - a_{19} - a_{23} = 0. \\
3a_8 + a_4 + a_{10} + a_{13} + a_{15} + a_{18} + a_{22} - a_6 - a_{14} = 0. \\
-a_{16} - a_2 - a_5 - a_7 - a_{12} - a_{20} - a_{24} = 0. \\
3a_9 + a_4 + a_7 + a_{10} + a_{12} + a_{13} + a_{24} = 0. \\
-a_{22} + a_4 + a_5 + a_{10} + a_{12} + a_{13} + a_{24} = 0. \\
3a_{10} + a_3 + a_8 + a_{16} + a_{17} + a_{19} + a_{23} - a_{12} - a_{18} = 0. \\
-a_{20} - a_1 - a_6 - a_9 - a_{11} - a_{14} - a_{21} = 0. \\
3a_{11} - a_4 - a_5 - a_9 - a_{13} - a_{17} - a_{18} - a_{19} - a_{20} = 0. \\
-a_{24} + a_2 + a_7 + a_{10} + a_{12} + a_{15} + a_{22} = 0. \\
3a_{12} - a_1 - a_6 - a_{10} - a_{14} - a_{17} - a_{18} - a_{19} - a_{20} = 0. \\
-a_{21} + a_3 + a_8 + a_9 + a_{11} + a_{16} + a_{23} = 0. \\
3a_{13} + a_3 + a_6 + a_8 + a_{11} + a_{19} + a_{21} - a_5 - a_7 = 0. \\
-a_{15} - a_1 - a_9 - a_{14} - a_{16} - a_{17} - a_{23} = 0. \\
3a_{14} + a_4 + a_5 + a_7 + a_{12} + a_{20} + a_{22} - a_6 - a_8 = 0. \\
-a_{16} - a_2 - a_{10} - a_{13} - a_{15} - a_{18} - a_{24} = 0.
\end{align*}
3a_{15} + a_{1} + a_{6} + a_{8} + a_{9} + a_{17} + a_{23} - a_{5} - a_{7} - a_{13} - a_{3} - a_{11} - a_{14} - a_{16} - a_{19} - a_{21} = 0. \quad (3.28)

3a_{16} + a_{2} + a_{5} + a_{7} + a_{10} + a_{18} + a_{24} - a_{6} - a_{8} - a_{14} - a_{2} - a_{5} - a_{13} - a_{15} - a_{20} - a_{22} = 0. \quad (3.29)

3a_{17} + a_{4} + a_{7} + a_{10} + a_{12} + a_{15} + a_{24} - a_{9} - a_{11} - a_{19} - a_{2} - a_{5} - a_{13} - a_{18} - a_{20} - a_{22} = 0. \quad (3.30)

3a_{18} + a_{1} + a_{8} + a_{9} + a_{11} + a_{16} + a_{21} - a_{10} - a_{12} - a_{20} - a_{3} - a_{6} - a_{14} - a_{17} - a_{19} - a_{23} = 0. \quad (3.31)

3a_{19} + a_{2} + a_{5} + a_{10} + a_{12} + a_{1} + a_{13} + a_{22} - a_{9} - a_{11} - a_{17} - a_{4} - a_{7} - a_{15} - a_{18} - a_{20} - a_{24} = 0. \quad (3.32)

3a_{20} + a_{3} + a_{6} + a_{9} + a_{11} + a_{14} + a_{23} - a_{10} - a_{12} - a_{18} - a_{1} - a_{8} - a_{16} - a_{17} - a_{19} - a_{21} = 0. \quad (3.33)

3a_{21} + a_{2} + a_{4} + a_{7} + a_{12} + a_{13} + a_{18} - a_{1} - a_{3} - a_{23} - a_{5} - a_{10} - a_{15} - a_{20} - a_{22} - a_{24} = 0. \quad (3.34)

3a_{22} + a_{1} + a_{3} + a_{8} + a_{9} + a_{14} + a_{19} - a_{2} - a_{4} - a_{24} - a_{6} - a_{11} - a_{16} - a_{17} - a_{21} - a_{23} = 0. \quad (3.35)

3a_{23} + a_{2} + a_{4} + a_{10} + a_{14} + a_{20} - a_{1} - a_{3} - a_{21} - a_{7} - a_{12} - a_{13} - a_{18} - a_{22} - a_{24} = 0. \quad (3.36)

3a_{24} + a_{1} + a_{3} + a_{6} + a_{11} + a_{16} + a_{17} - a_{2} - a_{4} - a_{22} - a_{8} - a_{9} - a_{14} - a_{19} - a_{21} - a_{23} = 0. \quad (3.37)

Since the rank of the coefficient matrix of the above equations is 9, we know that \( \dim(I_{(f)}) = 15 \). Secondly, we will compute the minimal distance of group code \( I_{(f)} \). For some \( \alpha = kg_{i}, 1 \leq i \leq 24 \), if \( k \neq 0 \), then \( \alpha f_{2} \neq 0 \), i.e., \( \alpha = kg_{i} \notin I_{(f)} \). Though the coefficients of \( f_{2} \), it is not difficult to find that \( \alpha f_{2} \neq 0 \) for \( \text{wt}(\alpha) \leq 3 \). So \( d(I_{(f)}) \geq 4 \). Set \( \alpha = g_{1} + g_{2} + g_{3} + g_{4} \). Since \( \alpha f_{1} = (g_{1} + g_{2} + g_{3} + g_{4})f_{1} = 0 \), we get \( \alpha = g_{1} + g_{2} + g_{3} + g_{4} \notin I_{(f)} \). Hence, \( d(I_{(f)}) = 4 \). We can compute the parameters of group code \( I_{(f)} \) by the similarly method (for \( d(I_{(f)}) = 4 \), take \( \alpha = -g_{1} + g_{2} - g_{3} + g_{4} \)).

This completes the proof. \( \square \)
Theorem 3.7. Let $e_i, i = 1, 2$ and $f_j, j = 1, 2, 3$ be idempotents in $\mathbb{F}_q S_4$. Then

1. $I_{\{e_i, e_2\}}$ is a $[24,22,2]$ group code;
2. $I_{\{e_i, f_j\}}$ is a $[24,17,2]$ group code, for $i = 1, 2$;
3. $I_{\{e_i, f_j\}}$ is a $[24,14,8]$ group code, for $i = 1, 2, j = 2, 3$;
4. $I_{\{f_i, f_j\}}$ is a $[24,11,8]$ group code, for $j = 2, 3$;
5. $I_{\{f_i, f_j\}}$ is a $[24,6,8]$ group code.

Proof. (1) Clearly, $I_{\{e_i, e_2\}} = \{\alpha \in \mathbb{F}_q S_4 | a e_1 = 0$ and $a e_2 = 0\}$. Firstly, we will give the dimension of group code $I_{\{e_i, e_2\}}$. For any $\alpha = \sum_{i=1}^{24} a_i g_i \in I_{\{e_i, e_2\}}$, we have $a e_1 = 0$ and $a e_2 = 0$. From (3.4) and (3.5), we obtain the following system of equations:

\[
\begin{align*}
\sum_{i=1}^{24} a_i &= 0 \\
(a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} + a_{11} + a_{12} + a_{13} + a_{14} + a_{15} + a_{16} + a_{17} + a_{18} + a_{19} + a_{20} + a_{21} + a_{22} + a_{23}) &= 0 \\
-(a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} + a_{11} + a_{12} + a_{13} + a_{14} + a_{15} + a_{16} + a_{17} + a_{18} + a_{19} + a_{20} + a_{21} + a_{22} + a_{23}) &= 0
\end{align*}
\]

Then, we have $\dim(I_{\{e_i, e_2\}}) = 22$. Secondly, we will compute the minimal distance of group code $I_{\{e_i, e_2\}}$. For some $\alpha = k g_i, 1 \leq i \leq 24$, if $k \neq 0$, then $a e_i \neq 0$, i.e., $\alpha = k g_i \notin I_{\{e_i, e_2\}}$. So $d(I_{\{e_i, e_2\}}) \geq 2$. Set $\alpha = g_1 - g_3$. Since $a e_i = (g_1 - g_3) e_i = 0$, for $i = 1, 2$, we get $\alpha = g_1 - g_3 \in I_{\{e_i, e_2\}}$. Hence, $d(I_{\{e_i, e_2\}}) = 2$.

(2) Let $I_{\{e_i, f_j\}}, i = 1, 2$ be the set of elements of the form $\alpha = \sum_{i=1}^{24} a_i g_i$ which the coefficients of $\alpha$ satisfy Eqs (3.6) and (3.8)–(3.13) for $i = 1$, while Eqs (3.7)–(3.13) for $i = 2$. Obviously, it does not contain any element with weight 1 of $I_{\{e_i, f_j\}}, i = 1, 2$. Also, set $\alpha = g_1 - g_3$, then $\alpha \in I_{\{e_i, f_j\}}, i = 1, 2$. Hence, $d(I_{\{e_i, f_j\}}) = 2, i = 1, 2$. Moreover, the dimension of $I_{\{e_i, f_j\}}, i = 1, 2$ is 17. Therefore, $I_{\{e_i, f_j\}}, i = 1, 2$ is a $[24,17,24]$ group code.

(3) Let $I_{\{e_i, f_j\}}, i = 1, 2$ be the set of elements of the form $\alpha = \sum_{i=1}^{24} a_i g_i$ which the coefficients of $\alpha$ satisfy Eqs (3.6) and (3.14)–(3.37) for $i = 1$, while Eqs (3.7) and (3.14)–(3.37) for $i = 2$. Obviously, it does not contain any element with weight $\leq 4$ of $I_{\{e_i, f_j\}}, i = 1, 2$. Also, set $\alpha = g_1 + g_2 + g_3 + g_4 - g_5 - g_6 - g_7 - g_8$, then $\alpha \in I_{\{e_i, f_j\}}, i = 1, 2$. Hence, $d(I_{\{e_i, f_j\}}) = 8, i = 1, 2$. Moreover, the dimension of $I_{\{e_i, f_j\}}, i = 1, 2$ is 14. Therefore, $I_{\{e_i, f_j\}}, i = 1, 2$ is a $[8,14,24]$ group code. In addition, we can obtain the parameters of $I_{\{e_i, f_j\}}, i = 1, 2$ by a similar proof.

(4) Let $I_{\{f_i, f_j\}}$ be the set of elements of the form $\alpha = \sum_{i=1}^{24} a_i g_i$ which the coefficients of $\alpha$ satisfy Eqs (3.8)–(3.37). Obviously, it does not contain any element with weight $\leq 4$ of $I_{\{f_i, f_j\}}$. Also, set $\alpha = g_1 + g_2 + g_3 + g_4 - g_5 - g_6 - g_7 - g_8$, then $\alpha \in I_{\{f_i, f_j\}}$. Hence, $d(I_{\{f_i, f_j\}}) = 8$. Moreover, the dimension of $I_{\{f_i, f_j\}}$ is 11. Therefore, $I_{\{f_i, f_j\}}$ is a $[24,11,8]$ group code. In addition, we can obtain the parameters of $I_{\{f_i, f_j\}}$ by a similar proof.

(5) Let $I_{\{f_i, f_j\}}$ be the set of elements of the form $\alpha = \sum_{i=1}^{24} a_i g_i$, with the coefficients of $\alpha$ satisfy the corresponding equations. Obviously, it does not contain any element with weight $\leq 4$ of $I_{\{f_i, f_j\}}$. Also, set $\alpha = g_1 + g_2 + g_3 + g_4 - g_5 - g_6 - g_7 - g_8$, then $\alpha \in I_{\{f_i, f_j\}}$. Hence, $d(I_{\{f_i, f_j\}}) = 8$. Moreover, the dimension of $I_{\{f_i, f_j\}}$ is 6. Therefore, $I_{\{f_i, f_j\}}$ is a $[6,8,24]$ group code.

This completes the proof. □

We summarize the following results about the group codes of $\mathbb{F}_q S_4$. In fact, these results can be proved by using similar techniques with rigorous derivation that we have used in the previous results.
in this section.

**Theorem 3.8.** Let \( e_i, i = 1, 2 \) and \( f_j, j = 1, 2, 3 \) be idempotents in \( \mathbb{F}_qS_4 \). Then

1. \( I_{\{e_1, e_2, f_1\}} \) is a \([24, 18, 2]\) group code;
2. \( I_{\{e_1, e_2, f_j\}} \) is a \([24, 13, 8]\) group code, for \( j = 2, 3 \);
3. \( I_{\{e_i, f_i, f_j\}} \) is a \([24, 10, 8]\) group code, for \( i = 1, 2, j = 2, 3 \);
4. \( I_{\{e_i, f_1, f_2\}} \) is a \([24, 5, 8]\) group code, for \( i = 1, 2 \);
5. \( I_{\{f_1, f_2, f_3\}} \) is a \([24, 2, 8]\) group code, for \( i = 1, 2 \).

**Theorem 3.9.** Let \( e_i, i = 1, 2 \) and \( f_j, j = 1, 2, 3 \) be idempotents in \( \mathbb{F}_qS_4 \). Then

1. \( I_{\{e_i, f_1, f_2, f_3\}} \) is a \([24, 1, 8]\) group code, for \( i = 1, 2 \);
2. \( I_{\{e_1, e_2, f_1, f_j\}} \) is a \([24, 9, 8]\) group code, for \( j = 2, 3 \);
3. \( I_{\{e_1, f_1, f_2, f_3\}} \) is a \([24, 4, 8]\) group code.

We can obtain the following results based on Theorems 3.6–3.9.

**Remark 3.10.** Let \( e_i, i = 1, 2 \) and \( f_j, j = 1, 2, 3 \) be idempotents in \( \mathbb{F}_qS_4 \).

1. \( I_{\{e_i\}}, i = 1, 2 \), and \( I_{\{e_1, e_2\}} \) are MDS group codes.
2. There are no AMDS group codes in \( \mathbb{F}_qS_4 \).

**4. Conclusions**

The main contributions of this paper are the following:

- The unique (linear and nonlinear) idempotents of \( \mathbb{F}_qS_3 \) and \( \mathbb{F}_qS_4 \) were described (see Theorems 3.1 and 3.6).
- The minimum distances and dimensions of \( \mathbb{F}_qS_3 \) and \( \mathbb{F}_qS_4 \) were characterized (see Theorems 3.2–3.3 and 3.6–3.9).
- The MDS group codes and almost MDS group codes in \( \mathbb{F}_qS_3 \) and \( \mathbb{F}_qS_4 \) were constructed (see Remarks 3.4 and 3.10).

**Use of AI tools declaration**

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

**Acknowledgments**

The authors are very grateful to the reviewers and the Associate Editor for their valuable comments and suggestions to improve the quality of this paper.

The paper is supported by National Natural Science Foundation of China (Nos. 11961050, 12101277), Fundation of Nanjing Institute of Technology (No. CKJB202007), the Guangxi Natural Science Foundation (No. 2020GXNSFAA159053).

**Conflict of interest**

The authors declare that there is no conflict of interest regarding the publication of this paper.
References


3. Y. Cao, Y. Cao, F. Fu, Concatenated structure of left dihedral codes, *Finite Fields Appl.*, **38** (2016), 93–115. https://doi.org/10.1016/jffa.2016.01.001


© 2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)