Korean J. Math. **17** (2009), No. 4, pp. 487–493

AUTOMORPHISM GROUP OF THE TERNARY TETRACODE

Young Ho Park

Abstract. We study the group structure of the automorphism group of the ternary self-dual tetracode of length 4.

1. Introduction

Let R be a ring. A *linear code* of length n over R is a R-submodule of R^n. We define an inner product on R^n by $(x, y) = \sum_{i=1}^{n} x_i y_i$ where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. The *dual code* $C^\perp$ of a code C of length n is defined to be $C^\perp = \{y \in R^n \mid (y, x) = 0 \text{ for all } x \in C\}$. C is *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.

When considering code classification, a notion of equivalence is necessary. An $n \times n$ matrix with coefficients in R is said to be *monomial* if there is exactly one nonzero entry in each row and column. The set of all invertible monomial transformations is denoted by $\mathcal{M} = \mathcal{M}_n(R)$. A monomial matrix is called a *permutation matrix* if the only nonzero entry in each row and column is 1. Any monomial matrix M_n can be uniquely written as $M = PD$ or $M = DP$, where P is a permutation matrix and D is a diagonal matrix. A monomial matrix M acts on the elements $x \in R^n$ as $x \mapsto xM$ and hence on codes. Two codes C_1 and C_2 are *permutation equivalent* if there is a permutation matrix P such that $C_1 P = C_2$. There is a more general equivalence. Two codes C_1 and C_2 are *(monomially) equivalent* if there exists an invertible monomial matrix M such that $C_1 M = C_2$. Note that if C_1 and C_2 are monomially equivalent codes over $\mathbb{Z}_3$ and if C_1 is self-orthogonal, then so is C_2. The *automorphism group* of a code C of length n over R is the set of all

Received October 16, 2008. Revised November 29, 2008.
2000 Mathematics Subject Classification: 95A.
Key words and phrases: self-dual code, tetra code, automorphism group.

monomial transformations M such that $CM = C$:

$$\mathrm{Aut}(C) = \{M \in \mathcal{M} \mid CM = M\}$$

As described in [11], self-dual codes are an important class of linear codes, both theoretically and for practical reasons. Self-dual codes have received an enormous research effort. One of the most fundamental problem on self-dual codes is to classify them. See [2] for recent results. Such classification heavily relies on the knowledge of the so-called *mass formula*, i.e., counting formula for self-dual codes, and the sizes of automorphism groups. For example, the following mass formula for ternary codes of length n is well-known ([9, 10, 4]).

THEOREM 1.1. *There exists a ternary self-dual code of length n if and only if n is divisible by 4. In this case, the number of self-dual code of length n is given by*

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

Suppose that $C_1, \cdots, C_r$ are all inequivalent ternary self-dual codes of length n. Then

$$2\prod_{i=1}^{\frac{n}{2}-1}(3^i + 1) = \sum_{j=1}^{r}\frac{|\mathcal{M}_n(\mathbb{Z}_3)|}{|\mathrm{Aut}(C_i)|}. \tag{1}$$

Thus the classification comes down to constructing inequivalent self-dual codes $C_1, \cdots, C_r$ which meets the equality (1). See [7] for details.

Recently, codes over $\mathbb{Z}_m$ are studied in many places (see [8],[1], [6]). Classification of self-dual codes over these rings requires not just the size of automorphism groups of codes over the fields $\mathbb{Z}_p$ but also the knowledge of their subgroups. This will be exploited in the forthcoming papers. However, the automorphism group $\mathrm{Aut}(T)$ of the tetracode T is given incorrectly in [7] and [11], which motivated this article. The results of this article can be used in classifying ternary self-dual codes of length a multiple of 4 over the rings $\mathbb{Z}_{3m}$.

2. Ternary tetracode

The tetracode is a ternary code T with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

It is easy to see that T is a self-dual code with 9 elements

$$T = \{0000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2210\}$$

and any self-dual code of length 4 is equivalent to T. The automorphism group $\mathrm{Aut}(T)$ will be denoted by G. The mass formula (1) with $n = 4$ gives

$$2 \times (3+1) = \sum_{j=1}^{r} \frac{2^4 \cdot (4!)}{|\mathrm{Aut}(C_i)|}. \tag{2}$$

Since there exists a unique inequivalent ternary code T of length 4, we have that

$$8 = \frac{2^4 \cdot (4!)}{|\mathrm{Aut}(T)|}$$

which gives that $G = \mathrm{Aut}(T)$ has order 48. See [5] for the classification of ternary self-dual codes of small length.

Theorem 2.1. *G can be generated by two elements*

$$\mathbf{b} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Proof. Note that the actions of $\mathbf{b}$ and $\mathbf{c}$ are given by

$$(a_1, a_2, a_3, a_4)\mathbf{b} = (a_2, a_3, a_4, -a_1), \quad (a_1, a_2, a_3, a_4)\mathbf{c} = (a_3, a_2, a_4, a_1)$$

and T is invariant under $\mathbf{b}$ and $\mathbf{c}$. It is easy to check that $\mathbf{b}^4 = -I_4$, $|\mathbf{b}| = 8$ and $|\mathbf{c}| = 3$. Therefore, the subgroup H generated by $\mathbf{b}$ and $\mathbf{c}$ contains at least 24 distinct elements $\mathbf{b}^i\mathbf{c}^j$ where $0 \le i \le 7$, $0 \le j \le 2$. Note that $(a_1, a_2, a_3, a_4)\mathbf{cb} = (a_2, a_4, a_1, -a_3)$ and that $\mathbf{b}^i\mathbf{c}^j$ acts on (a_1, a_2, a_3, a_4) by a permutation of coordinates and the sign changes. Only when $i = 1$ or 7, the action of $\mathbf{b}^i\mathbf{c}^j$ contains exactly one sign change. Now it is straightforward to check that $\mathbf{cb} \ne \mathbf{b}^i\mathbf{c}^j$ for $i = 1, 7$ and $j = 0, 1, 2$. Hence H contains more than 24 elements and thus $H = G$. □

We used Theorem 2.1 to identify all elements of G given in Table 1. We also computed the conjugacy classes of G given in Table 2.

Table 1. Elements of G

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}^{1}_{1}, \quad \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&0&0&-1\\0&-1&0&0\end{pmatrix}^{3}_{2}, \quad \begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&-1&0\\0&1&0&0\end{pmatrix}^{2}_{3}, \quad \begin{pmatrix}1&0&0&0\\0&0&0&-1\\0&1&0&0\\0&0&-1&0\end{pmatrix}^{3}_{4}$$

$$\begin{pmatrix}1&0&0&0\\0&0&-1&0\\0&-1&0&0\\0&0&0&-1\end{pmatrix}^{2}_{5}, \quad \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}^{2}_{6}, \quad \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}^{2}_{7}, \quad \begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\-1&0&0&0\end{pmatrix}^{8}_{8},$$

$$\begin{pmatrix}0&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&-1&0\end{pmatrix}^{8}_{9}, \quad \begin{pmatrix}0&1&0&0\\0&0&0&-1\\0&0&-1&0\\1&0&0&0\end{pmatrix}^{6}_{10}, \quad \begin{pmatrix}0&1&0&0\\0&0&-1&0\\-1&0&0&0\\0&0&0&1\end{pmatrix}^{3}_{11}, \quad \begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}^{4}_{12}$$

$$\begin{pmatrix}0&0&1&0\\1&0&0&0\\0&0&0&-1\\0&1&0&0\end{pmatrix}^{8}_{13} \quad \begin{pmatrix}0&0&1&0\\0&1&0&0\\0&0&0&1\\1&0&0&0\end{pmatrix}^{3}_{14} \quad \begin{pmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{pmatrix}^{4}_{15} \quad \begin{pmatrix}0&0&1&0\\0&0&0&-1\\0&-1&0&0\\-1&0&0&0\end{pmatrix}^{8}_{16}$$

$$\begin{pmatrix}0&0&1&0\\0&-1&0&0\\1&0&0&0\\0&0&0&1\end{pmatrix}^{2}_{17} \quad \begin{pmatrix}0&0&1&0\\-1&0&0&0\\0&1&0&0\\0&0&0&-1\end{pmatrix}^{6}_{18} \quad \begin{pmatrix}0&0&0&1\\1&0&0&0\\0&0&-1&0\\0&-1&0&0\end{pmatrix}^{6}_{19} \quad \begin{pmatrix}0&0&0&1\\0&1&0&0\\1&0&0&0\\0&0&1&0\end{pmatrix}^{3}_{20}$$

$$\begin{pmatrix}0&0&0&1\\0&0&1&0\\-1&0&0&0\\0&1&0&0\end{pmatrix}^{8}_{21} \quad \begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{pmatrix}^{4}_{22} \quad \begin{pmatrix}0&0&0&1\\0&-1&0&0\\0&0&1&0\\1&0&0&0\end{pmatrix}^{2}_{23} \quad \begin{pmatrix}0&0&0&1\\-1&0&0&0\\0&-1&0&0\\0&0&-1&0\end{pmatrix}^{8}_{24}$$

$$\begin{pmatrix}0&0&0&-1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}^{8}_{25} \quad \begin{pmatrix}0&0&0&-1\\0&1&0&0\\0&0&-1&0\\-1&0&0&0\end{pmatrix}^{2}_{26} \quad \begin{pmatrix}0&0&0&-1\\0&0&1&0\\0&-1&0&0\\1&0&0&0\end{pmatrix}^{4}_{27} \quad \begin{pmatrix}0&0&0&-1\\0&0&-1&0\\1&0&0&0\\0&-1&0&0\end{pmatrix}^{8}_{28}$$

$$\begin{pmatrix}0&0&0&-1\\0&-1&0&0\\-1&0&0&0\\0&0&-1&0\end{pmatrix}^{6}_{29} \quad \begin{pmatrix}0&0&0&-1\\-1&0&0&0\\0&0&1&0\\0&1&0&0\end{pmatrix}^{3}_{30} \quad \begin{pmatrix}0&0&-1&0\\1&0&0&0\\0&-1&0&0\\0&0&0&1\end{pmatrix}^{3}_{31} \quad \begin{pmatrix}0&0&-1&0\\0&1&0&0\\-1&0&0&0\\0&0&0&-1\end{pmatrix}^{2}_{32}$$

$$\begin{pmatrix}0&0&-1&0\\0&0&0&1\\0&1&0&0\\1&0&0&0\end{pmatrix}^{8}_{33} \quad \begin{pmatrix}0&0&-1&0\\0&0&0&-1\\1&0&0&0\\0&1&0&0\end{pmatrix}^{4}_{34} \quad \begin{pmatrix}0&0&-1&0\\0&-1&0&0\\0&0&0&-1\\-1&0&0&0\end{pmatrix}^{6}_{35} \quad \begin{pmatrix}0&0&-1&0\\-1&0&0&0\\0&0&0&1\\0&-1&0&0\end{pmatrix}^{8}_{36}$$

$$\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}^{4}_{37} \quad \begin{pmatrix}0&-1&0&0\\0&0&1&0\\1&0&0&0\\0&0&0&-1\end{pmatrix}^{6}_{38} \quad \begin{pmatrix}0&-1&0&0\\0&0&0&1\\0&0&1&0\\-1&0&0&0\end{pmatrix}^{3}_{39} \quad \begin{pmatrix}0&-1&0&0\\0&0&0&-1\\-1&0&0&0\\0&0&1&0\end{pmatrix}^{8}_{40}$$

$$\begin{pmatrix}0&-1&0&0\\0&0&-1&0\\0&0&0&-1\\1&0&0&0\end{pmatrix}^{8}_{41} \quad \begin{pmatrix}0&-1&0&0\\-1&0&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}^{2}_{42} \quad \begin{pmatrix}-1&0&0&0\\0&1&0&0\\0&0&0&-1\\0&0&-1&0\end{pmatrix}^{2}_{43} \quad \begin{pmatrix}-1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}^{2}_{44}$$

$$\begin{pmatrix}-1&0&0&0\\0&0&0&1\\0&-1&0&0\\0&0&1&0\end{pmatrix}^{6}_{45} \quad \begin{pmatrix}-1&0&0&0\\0&0&0&-1\\0&0&1&0\\0&-1&0&0\end{pmatrix}^{2}_{46} \quad \begin{pmatrix}-1&0&0&0\\0&0&-1&0\\0&0&0&1\\0&1&0&0\end{pmatrix}^{6}_{47} \quad \begin{pmatrix}-1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{pmatrix}^{2}_{48}$$

Notation: A^i_j indicates that the matrix A will be denoted by g_j or sometimes simply by j and the order of g_j is i.

TABLE 2. Conjugacy classes of G

Class	Elements	$\lvert Ci\rvert$	$\lvert g\rvert$ $(g \in Ci)$
$C1$	1	1	1
$C2$	2,4,11,14,20,30,31,39	8	3
$C3$	3,5,6,7,17,23,26,32,42,43,44,46	12	2
$C4$	8,13,24,28,33,40	6	8
$C5$	9,16,21,25,36,41	6	8
$C6$	10,18,19,29,35,38,45,47	8	6
$C7$	12,15,22,27,34,37	6	4
$C8$	48	1	2

3. Group Structure of G

Table 1 gives the class equation for G:

$$48 = 1 + 1 + 6 + 6 + 6 + 8 + 8 + 12. \tag{3}$$

THEOREM 3.1. *The center of G is $\{I_4, -I_4\}$*

Proof. This follows from the table of conjugacy classes. □

LEMMA 3.2. [3] *Suppose H is a p-subgroup of any group G. Then*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Take any subgroup H of order 8 of G. By the previous lemma

$$[N_G(H) : H] \equiv 0 \pmod{2}.$$

Since the possibilities for $|N_G(H)|$ are $8, 16$, or 24, this implies that $|N_G(H)| = 16$. This gives the following theorem.

THEOREM 3.3. *Let H be any subgroup of order 8. Then any normalizer of H has order 16, and hence it is a Sylow 2-subgroup of G.*

The number N_2 of Sylow 2-subgroups satisfies $N_2 \equiv 1 \pmod{2}$, $N_2 \mid 3$ so that the possibilities are $N_2 = 1, 3$. Using Theorem 3.3, we can obtain three Sylow 2-subgroups as follows.

$$P_1 = N_G(\langle 8\rangle) = \{1, 3, 8, 12, 15, 17, 22, 24, 25, 27, 32, 34, 37, 41, 46, 48\},$$
$$P_2 = N_G(\langle 13\rangle) = \{1, 5, 9, 12, 13, 15, 22, 23, 26, 27, 34, 36, 37, 40, 44, 48\},$$
$$P_3 = N_G(\langle 28\rangle) = \{1, 6, 7, 12, 15, 16, 21, 22, 27, 28, 33, 34, 37, 42, 43, 48\}.$$

Since there are 8 elements of order 3, we see that Sylow 3-subgroups are the following four subgroups:

$$Q_1 = \{1, 2, 4\}, \qquad Q_2 = \{1, 11, 31\},$$
$$Q_3 = \{1, 14, 20\}, \qquad Q_4 = \{1, 30, 39\}.$$

We summarize the results about Sylow subgroups.

Theorem 3.4. *G has four Sylow 3-subgroups of order 3 and three Sylow 2-subgroups of order 16. Thus no Sylow subgroups are normal.*

Let

$$\mathbf{i} = g_{22} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \qquad \mathbf{j} = g_{34} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$
$$\mathbf{c} = g_{20} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \mathbf{d} = g_{46} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

We have the following relations about these elements.

(4) $\mathbf{i}^2 = \mathbf{j}^2 = -I, \quad \mathbf{ji} = \mathbf{i}^3\mathbf{j},$

(5) $\mathbf{c}^3 = I, \quad \mathbf{ci} = \mathbf{jc}, \quad \mathbf{cj} = \mathbf{ijc}$

(6) $\mathbf{d}^2 = I, \quad \mathbf{di} = \mathbf{ijd}, \quad \mathbf{dj} = \mathbf{i}^2\mathbf{jd}, \quad \mathbf{dc} = \mathbf{ijc}^2\mathbf{d}$

The equation (4) shows that the subgroup

$$K = \langle \mathbf{i}, \mathbf{j} \rangle = \{\mathbf{i}^i\mathbf{j}^j \mid 0 \le i \le 3,\ 0 \le j \le 1\}$$

is isomorphic to the quaternion group of order 8. It turns out that

$$K = C1 \cup C8 \cup C7$$

and hence K is a normal subgroup of G. The equation (5) shows that the set

(7) $N = \{\mathbf{i}^i\mathbf{j}^j\mathbf{c}^c \mid 0 \le i \le 3,\ 0 \le j \le 1, 0 \le c \le 2\}$

is closed and hence a subgroup of G of order 24, which must be normal.

Theorem 3.5. *N is the unique subgroup of order 24 and*

$$N = C1 \cup C8 \cup C2 \cup C6 \cup C7.$$

Proof. A normal subgroup is a union of conjugacy classes including $C1$. The only way to get a normal subgroup N' of order 24 is by the summation $24 = 1 + 1 + 6 + 8 + 8$. Thus N' is a union of $N_1 = C1 \cup C8 \cup C2 \cup C6$ and one of $C4$, $C5$ or $C7$. We find that $g_{48}g_{40} = g_9 \in (C8)(C4) \cap C5$ and $g_{48}g_{41} = g_8 \in (C8)(C5) \cap C4$. These mean that

$N_1 \cup C4$ and $N_1 \cup C5$ are not closed, and hence not a subgroup. Therefore, N' must be $N_1 \cup C7$ and it is the unique subgroup of order 24, namely $N' = N$. □

In [7] and [11], it is incorrectly given that $G = 2.S_4$, where S_4 is the symmetric group of 4 letters. To see this, just notice that the center of N is $\{g_1, g_{48}\}$, while S_4 has the trivial center.

Finally we give a convenient presentation of G by generators and relations. Note that $\mathbf{d} \in C3$ so that $\mathbf{d} \notin N$. Thus $G = N \cup N\mathbf{d}$. This together with the equation (7) gives the following theorem.

THEOREM 3.6. *Let* $\mathbf{i}, \mathbf{j}, \mathbf{c}, \mathbf{d}$ *as above equations (4),(5) and (6). Then*

$$G = \{\mathbf{i}^i \mathbf{j}^j \mathbf{c}^c \mathbf{d}^d \mid 0 \leq i \leq 4,\ 0 \leq j \leq 1,\ 0 \leq c \leq 2,\ 0 \leq d \leq 1\}.$$

References

[1] J. Balmaceda, R. Betty and F. Nemenzo, *Mass formula for self-dual codes over* $\mathbb{Z}_{p^2}$, Discrete Math, Vol 308, 2008, 2984–3002

[2] W. C Huffman, *On the classification and enumeration of self-dual codes*, Finite fields and their appl., Vol. 11, 451–490, 2005

[3] Hungerford, *Algebra*, Springer-Verlag, New York, 1974,

[4] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[5] C. L. Mallows, V. Pless and N. J. A Sloane, *Self-dual codes over GF(3)*, Siam J. Appl. Math., Vol 31, 1976.

[6] K. Nagata, F. Nemenzo and H. Wada, *The number of self-dual codes over* $\mathbb{Z}_{p^3}$, Des. Codes Cryptogr., Vol 50, 2009, 291–303

[7] G. Nebe, E. Rains, and N.J.A. Sloane, *Self-dual codes and Invariant Theory*, Springer, Berlin, 2006

[8] Y. H. Park, *Modular independence and generator matrices for codes over* $\mathbb{Z}_m$, Des. Codes Cryptogr, Vol 50, 2009, 147–162.

[9] V. Pless, *The number of isotropic subspaces in a finite geometry*, Rend Cl. Scienze fisiche, Vol 39, 1965, 418–421.

[10] V. Pless, *On the uniqueness of the Golay codes*, J. Comb. Theory, Vol 5, 1968, 215–228

[11] E. Rains and N. J. A. Sloane, *Self-dual codes*, in the Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, 1998, 177-294.

Department of Mathematics
Kangwon National University
E-mail: yhpark@kangwon.ac.kr