

ISOMORPHISM PROBLEMS FOR CONSTRUCTION A

TAKARA KONDO

1. INTRODUCTION

In [2], Lam and Shimakura proposed new methods for constructing a lattice. One of the constructions is called *Construction A*.

Let p be a prime and let C, D be self-orthogonal codes of length k over $\mathbb{F}_p$. In this article, we address the following problem:

$$L_A(C) \cong L_A(D) \iff C \cong D, \quad (1.1)$$

where $L_A(C)$ and $L_A(D)$ are Construction A by Lam-Shimakura ([2]).

Here, code equivalence between C and D means that there exists

$$f \in \langle s_i \mid 1 \leq i \leq k \rangle : S_k,$$

where s_i acts on $\mathbb{F}_p^k$ as -1 on the i -th coordinate and as 1 on the other coordinates, and each element of the symmetric group S_k induces a permutation of the coordinates. We call (1.1) isomorphism problems for Construction A.

In [1, 3], the problem (1.1) for the case $p = 2$ was proved. In this article, we prove (1.1) for the case $p = 3$.

2. PRELIMINARIES

2.1. Definition of Construction A. According to [2, Section 4], we introduce the definition of Construction A. Let

$$A_{n-1} = \{x = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \mid x_1 + x_2 + \dots + x_n = 0\}.$$

This is a standard realization of the root lattice A_{n-1} . Let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ be the canonical basis of $\mathbb{R}^n$ and let $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$ for $1 \leq i \leq n-1$. Note that $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ is a base of the root system of the root lattice A_{n-1} . We define the vectors ε'_i ($1 \leq i \leq n$) as follows:

$$\varepsilon'_i = -\frac{1}{n}(\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{i-1} - (n-1)\varepsilon_i + \varepsilon_{i+1} + \dots + \varepsilon_n).$$

Note that $\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_{n-1}$ is a basis of the dual lattice A_{n-1}^* and

$$A_{n-1}^*/A_{n-1} = \langle \varepsilon'_1 + A_{n-1} \rangle \cong \mathbb{Z}_n.$$

Moreover, by direct calculations, we have

$$(\varepsilon'_i, \varepsilon'_i) = \frac{n-1}{n} \text{ and } (\varepsilon'_i, \varepsilon'_j) = -\frac{1}{n} \text{ for } i \neq j.$$

Let p be a prime and let C be a self-orthogonal code of length k over $\mathbb{F}_p$. Then we can identify $C \subset \mathbb{Z}_p^k$ with a subset of $(A_{p-1}^*/A_{p-1})^k \cong \mathbb{Z}_p^k$. Let $\pi : (A_{p-1}^*)^k \rightarrow (A_{p-1}^*/A_{p-1})^k$ be the canonical map. Then *Construction A* $L_A(C)$ from C is defined as follows:

$$L_A(C) = \pi^{-1}(C).$$

3. A_n -FRAMES OF LATTICES

In this section, we define an A_n -frame of lattices.

Definition 3.1. Let L be a lattice. A finite subset F of L is called an A_n -frame of L if the following hold:

- (i) $F = F_1 \cup F_2 \cup \cdots \cup F_m$ (disjoint union) and $F_i \perp F_j$ if $i \neq j$.
- (ii) For each i , F_i forms a root system of type A_n .
- (iii) $\text{rank } L = mn$.

Let p be a prime and let C be a self-orthogonal code of length k over $\mathbb{F}_p$. Next, we consider A_{p-1} -frames of $L_A(C)$. Let R be k copies of the root lattice A_{p-1} . For a lattice L , the symbol $L(2)$ denotes the set of all roots of L . By the definition of $L_A(C)$, we have $R(2) \subset L_A(C)$. Hence, $R(2)$ is an A_{p-1} -frame of $L_A(C)$. $R(2)$ is called the *standard A_{p-1} -frame* of $L_A(C)$.

4. PROOF OF ISOMORPHISM PROBLEMS FOR CONSTRUCTION A

In this section, we prove (1.1) for the case $p = 3$. Let $R = A_2 \oplus A_2 \oplus A_2$ and let $\lambda \in R^*(2) \setminus R(2)$. Let $X_1 = \{\mathbf{0}, -\alpha_1, -\alpha_1 - \alpha_2\}$ and $X_2 = \{-2\alpha_1 - \alpha_2, -\alpha_1, -\alpha_1 - \alpha_2\}$, where α_1 and α_2 are simple roots of the root system $A_2(2)$ described in Section 2. By direct calculations, we see that λ is expressed as

$$\lambda = (c_1\varepsilon'_1 + x_1, c_2\varepsilon'_1 + x_2, c_3\varepsilon'_1 + x_3),$$

where $c_i \in \{1, 2\}$ and $x_i \in X_{c_i}$.

The following lemma is a characterization of the root lattice E_6 .

Lemma 4.1. *Let L be a lattice. Then the following conditions (i) and (ii) hold if and only if $L \cong E_6$.*

- (i) L is even and $\text{rank } L = 6$.
- (ii) $|L^*/L| = 3$ and $\#L(2) = 72$.

Proof. Clearly, if $L \cong E_6$, then the conditions (i) and (ii) hold. Conversely, we suppose that the conditions (i) and (ii) hold. Since L is even, $L(2)$ forms a simply laced root system. Since $\text{rank } L = 6$, the all possibilities of $L(2)$ are the following:

$$A_6, D_6, E_6, A_5 \oplus A_1, D_5 \oplus A_1, D_4 \oplus A_2, A_4 \oplus A_2, A_4 \oplus A_1^2, D_4 \oplus A_1^2, A_3^2, A_3 \oplus A_2 \oplus A_1, A_3 \oplus A_1^3, A_3^2, A_2^2 \oplus A_1^2, A_2 \oplus A_1^4, A_1^6.$$

Since $\#L(2) = 72$, $L(2)$ forms a root system of type E_6 . Since $|L^*/L| = 3$, we have $|L/\langle L(2) \rangle| = 1$, that is, $L = \langle L(2) \rangle \cong E_6$. $\square$

By the above lemma, we have the following proposition.

Proposition 4.2. *Let $\lambda \in R^*(2) \setminus R(2)$. Then we have $\mathbb{Z}\lambda + R \cong E_6$ as lattices.*

Proof. Let $L_\lambda = \mathbb{Z}\lambda + R$. We prove that L_λ satisfies the conditions (i) and (ii) in Lemma 4.1. By the definition of L_λ , we have $\text{rank } L_\lambda = 6$. Moreover, since the squared norm of λ is two, L_λ is even. Since $|L_\lambda/R| = 3$ and $|R^*/R| = 3^3$, we have $|L_\lambda^*/L_\lambda| = 3$.

Finally, we prove that $\#L_\lambda(2) = 72$. Let $\lambda \equiv (c_1\varepsilon'_1, c_2\varepsilon'_1, c_3\varepsilon'_1) \pmod R$, where $c_i \in \{1, 2\}$. For each coordinate and each c_i , we can choose vectors $c_i\varepsilon'_1 + x_i$ having the squared norm $2/3$, where $x_i \in X_{c_i}$. Since $\#X_i = 3$ for $i = 1, 2$ and $L_\lambda = R \cup (\lambda + R) \cup (-\lambda + R)$ (disjoint union), we have

$$\#L_\lambda(2) = \#R(2) + \#(\lambda + R)(2) + \#(-\lambda + R)(2) = 18 + 27 + 27 = 72.$$

Hence, by Lemma 4.1, we have $L_\lambda \cong E_6$. $\square$

Let $\mathcal{L}_{E_6} = \{L \mid L \text{ is a sublattice of } R^* \text{ such that } R \subset L \text{ and } L \cong E_6\}$. By the definition of $\mathcal{L}_{E_6}$, we have the following proposition:

Proposition 4.3. *If $L \in \mathcal{L}_{E_6}$, then there exists $\lambda \in R^*(2) \setminus R(2)$ such that $L = \mathbb{Z}\lambda + R$.*

The automorphism group $\text{Aut}(R)$ of the lattice R acts on $R^*(2) \setminus R(2)$. Next, we prove the transitivity of the action by $\text{Aut}(R)$.

Proposition 4.4. *$\text{Aut}(R)$ acts transitively on $R^*(2) \setminus R(2)$.*

Proof. Recall that

$$R^*(2) \setminus R(2) = \{(c_1\varepsilon'_1 + x_1, c_2\varepsilon'_1 + x_2, c_3\varepsilon'_1 + x_3) \mid c_i \in \{1, 2\}, x_i \in X_{c_i}\},$$

where $X_1 = \{0, -\alpha_1, -\alpha_1 - \alpha_2\}$ and $X_2 = \{-2\alpha_1 - \alpha_2, -\alpha_1, -\alpha_1 - \alpha_2\}$. Let r_x be the reflection induced by a vector x and let $\sigma : A_2 \rightarrow A_2$ be the map defined by $\alpha_1 \mapsto \alpha_2$ and $\alpha_2 \mapsto \alpha_1$. Let $X'_1 = \varepsilon'_1 + X_1$ and $X'_2 = 2\varepsilon'_1 + X_2$. Then we can identify the group $\langle r_{\alpha_1}, r_{\alpha_2} \rangle$ with the symmetric groups of X'_1 and we have $\sigma(X'_2) = X'_1$. Since $r_{\alpha_1}, r_{\alpha_2}, \sigma \in \text{Aut}(A_2)$, we have the desired result. $\square$

By Propositions 4.3 and 4.4, we have the following proposition:

Proposition 4.5. *$\text{Aut}(R)$ acts transitively on $\mathcal{L}_{E_6}$.*

Let $\lambda_0 = (\varepsilon'_1, \varepsilon'_1, \varepsilon'_1) \in R^*(2) \setminus R(2)$ and let $L \in \mathcal{L}_{E_6}$. Then $\text{Aut}(L)$ acts on the set of all A_2 -frames of L . The following proposition describes the transitivity of the action.

Proposition 4.6. *$\text{Aut}(L)$ acts transitively on the set of all A_2 -frames of L*

Proof. By Proposition 4.3, if $L \in \mathcal{L}_{E_6}$, then there exists $\lambda \in R^*(2) \setminus R(2)$ such that $L = \mathbb{Z}\lambda + R$. Let $F_0 = R(2)$ and let F be an A_2 -frame of L . We prove that there exists $\sigma \in \text{Aut}(L)$ such that $\sigma(F) = F_0$. To prove this, we use induction on $\#(F \cap F_0)$. Let $f \in F \setminus F_0$. Since $f \in R^*(2) \setminus R(2)$, by Proposition 4.4, we may assume that $f = \lambda_0$. Let $F = F_1 \perp F_2 \perp F_3$ and $\lambda_0 \in F_1$. The symbols α_1^i and α_2^i denote the simple roots α_1 and α_2 of i -th A_2 , respectively. Since $(\lambda_0, \alpha_1^i) = 1, (\lambda_0, \alpha_2^i) = 0$ for $i = 1, 2, 3$ and since F_1 forms a root system of type A_2 , we see that there exists $i \in \{1, 2, 3\}$ such that

$$F_1 \cap R(2) = \{\pm\lambda_0, \pm\alpha_1^i, \pm(\lambda_0 - \alpha_1^i)\}, \{\pm\lambda_0, \pm(\alpha_1^i + \alpha_2^i), \pm(\lambda_0 - \alpha_1^i - \alpha_2^i)\}.$$

By considering the reflection $r_{\alpha_2^i} \in \text{Aut}(L)$, we may assume that

$$F_1 \cap R(2) = \{\pm\lambda_0, \pm\alpha_1^i, \pm(\lambda_0 - \alpha_1^i)\}.$$

Since $F_k \perp F_l$ if $k \neq l$ and since F_k forms a root system of type A_2 for each k , we see that $F_2 \cap R(2) \subset \{\pm\alpha_2^{i_1}\}$ for $i_1 \in \{1, 2, 3\} \setminus \{i\}$ and $F_3 \cap R(2) \subset \{\pm\alpha_2^{i_2}\}$ for $i_2 \in \{1, 2, 3\} \setminus \{i, i_1\}$. By direct calculations, we see that $\alpha_1^i, \alpha_2^{i_1}$, and $\alpha_2^{i_2}$ are fixed points of the reflection $r_{\lambda_0 - \alpha_1^i - \alpha_2^{i_2}} \in \text{Aut}(L)$, where $i_1 \in \{1, 2, 3\} \setminus \{i\}$ and $i_2 \in \{1, 2, 3\} \setminus \{i, i_1\}$. Moreover, since $r_{\lambda_0 - \alpha_1^i - \alpha_2^{i_2}}(\lambda_0) = \alpha_1^i + \alpha_2^{i_2}$, we see that

$$\#(r_{\lambda_0 - \alpha_1^i - \alpha_2^{i_2}}(F) \cap F_0) > \#(F \cap F_0).$$

Hence, by the induction hypothesis, we have the desired result. $\square$

By Proposition 4.6, we have the following proposition:

Proposition 4.7. *Let C be a self-orthogonal code over $\mathbb{F}_3$. Then $\text{Aut}(L_A(C))$ acts transitively on the set of all A_2 -frames of $L_A(C)$.*

Let C and D be self-orthogonal codes of same length over $\mathbb{F}_3$. If $L_A(C) \cong L_A(D)$ as lattices, then there exists isomorphism $\varphi : L_A(C) \rightarrow L_A(D)$. Then $\varphi(F_0)$ is an A_2 -frame of $L_A(D)$, where F_0 is the standard A_2 -frame of $L_A(C)$. By Proposition 4.7, there exists $\sigma \in \text{Aut}(L_A(C))$ such that $\sigma(\varphi(F_0))$ is the standard A_2 -frame of $L_A(D)$. Hence we have the desired code equivalence between C and D . Therefore, we have the following proposition:

Proposition 4.8. *Let C and D be self-orthogonal codes of same length over $\mathbb{F}_3$. Then the following holds:*

$$L_A(C) \cong L_A(D) \iff C \cong D.$$

Acknowledgments. This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

REFERENCES

- [1] M. Kitazume, T. Kondo, and I. Miyamoto, Even lattices and doubly even codes. *J. Math. Soc. Japan* **43** (1991), no. 1, 67–87.
- [2] C.H. Lam and H. Shimakura, Extra automorphisms of cyclic orbifolds of lattice vertex operator algebras, *Jornal of pure and Applied Algebra* **228** (2024), Article no. 107454.
- [3] H. Shimakura, On isomorphism problems for vertex operator algebras associated with even lattices, *Proc. Amer. Math. Soc.* **140** (2012), 3333–3348.

(T. Kondo) GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, HIROSAKI UNIVERSITY, HIROSAKI 036-8561, JAPAN

Email address: h23ms107@hirosaki-u.ac.jp