LATTICES OF TYPE A_n, D_n, E_n AND CODES

RIKU HIGA
TOKYO UNIVERSITY OF SCIENCE

Abstract. This paper discusses a generalization of Construction A and its application to root lattices of type A_n, D_n, and E_n. While the classical Construction A provides a correspondence between binary codes and lattices, and its extension to cyclotomic fields relates p-ary codes to lattices over the ring of integers of $\mathbb{Q}(\zeta_p)$, we further extend this framework to a broader class of even root lattices. Specifically, for a given lattice Λ of type A_n, D_n, or E_n, we define a surjective mapping ρ_Λ from the dual lattice Λ^* to a finite ring R isomorphic to the quotient Λ^*/Λ. We then characterize the condition under which the resulting lattice Λ_C, constructed from an R-code C, becomes an even unimodular lattice. Our main theorem demonstrates that the even unimodularity of Λ_C is equivalent to specific weight conditions of the code C, such as being self-dual, Type II, or Type IV, depending on the type and dimension of the underlying root lattice. Furthermore, we apply our generalized Construction A to the algebraic lattices of type D_4 and E_6 previously realized by E. Bayer-Fluckiger (1999) [1] as fractional ideals of the cyclotomic fields $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\zeta_9)$, respectively. By doing so, we describe these structural lattices explicitly in terms of linear codes over finite rings. As an application, we show that the theta functions associated with these lattices can be expressed via the weight enumerators of the corresponding codes, proving that they form Hilbert modular forms of specific weights over totally real subfields.

1. Introduction

The interplay between coding theory and lattice theory has been a remarkably fertile area of research in number theory and algebraic combinatorics. A lattice is, by definition, a discrete subgroup of a real vector space, and its most fundamental example is the ring of rational integers $\mathbb{Z}$ inside the real number field $\mathbb{R}$. By scaling the standard inner product by a factor of two, the ring of rational integers can be naturally viewed as the root lattice of type A_1.

The classical connection between lattices and codes manifests as Construction A, which establishes a systematic correspondence between lattices of type A_1 and binary linear codes. This framework allows for the algebraic construction of even unimodular lattices from Type II codes. Crucially, the analytical properties of these constructed lattices are deeply mirrored by the combinatorial properties of the underlying codes: the theta functions of these lattices can be explicitly described by the weight enumerators of the corresponding binary codes. Since the theta functions of even unimodular lattices are classical modular forms, Construction A provides a beautiful bridge between coding theory and the theory of modular forms.

In 1985, van der Geer and Hirzebruch [6] generalized this relationship between the weight enumerators of binary codes and theta functions of lattices beyond the A_1 case. Their generalization is based on an elegant framework connecting p-ary codes (where p is an odd prime number) with lattices over the ring of integers of algebraic number fields. More precisely, let ζ_p be a primitive p-th root of unity, and consider the cyclotomic field $\mathbb{Q}(\zeta_p)$. It is a well-known fact that the cyclotomic field $\mathbb{Q}(\zeta_p)$ contains a root lattice of type A_{p-1} realized as a fractional ideal of its ring of integers. By exploiting the arithmetic of these cyclotomic fields and the structural correspondence between the A_{p-1} lattices and p-ary codes, van der Geer and Hirzebruch successfully constructed even unimodular lattices using purely algebraic data from codes. As in the classical A_1 case, the theta functions of the lattices arising from this cyclotomic Construction A are completely determined by the weight enumerators of the associated p-ary codes. Furthermore, because these lattices carry a natural module structure over the ring of integers of $\mathbb{Q}(\zeta_p)$, their associated theta functions give rise to multivariable modular forms—specifically, Hilbert modular forms over the totally real subfield of $\mathbb{Q}(\zeta_p)$ (cf. [6, Chapter 5]).

An underlying observation throughout these developments is that the even root lattices of type A (namely, A_1 and A_{p-1}) play a vital role both in the classical Construction A and its cyclotomic generalization. Therefore, it is highly natural to expect that this beautiful algebraic dictionary between codes and lattices can be extended to other families of root lattices.

The primary objective of this paper is to generalize the framework of van der Geer and Hirzebruch to a much broader class of root lattices. Specifically, we focus on irreducible and even root lattices of type A_n, D_n, and E_n. We introduce a generalized version of Construction A for these root lattices by setting up a surjective mapping from their dual lattices to appropriate finite rings. We then characterize the conditions under which the lifted lattices become even unimodular in terms of specific code structures, such as Type II, Type IV, or self-dual.

Notation. In this paper, for every field extension K/k, the usual trace map $\mathrm{Tr}_{K/k} : K \to k$ and the usual norm map $N_{K/k} : K \to k$ are often abbreviated to Tr and N if there is no fear of confusion. For every field k and every positive integer n, $k^{\oplus n}$ denotes the direct sum of n copies of k.

As usual, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. We denote the complex conjugate on $\mathbb{C}$ by $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$. For every integer $n \neq 0$, set $\zeta_n := \exp(2\pi\sqrt{-1}/n) \in \mathbb{C}$. $\mathbb{H}$ denotes the upper half plane, that is $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$. A number field is an extension field F of the field $\mathbb{Q}$ such that the field extension $F/\mathbb{Q}$ has finite degree. For every number field F, $\mathbb{Z}_F$ denotes the ring of integers in F, that is, the subring of F consisting of the roots of the monic polynomials with coefficients in $\mathbb{Z}$. A finitely generated $\mathbb{Z}_F$-submodule of $\mathbb{Z}_F$ (resp. of F) is called an ideal of $\mathbb{Z}_F$ (resp. a fractional ideal of F).

2. Basic definitions

First, we recall some basic definitions. For details, see e.g. [6, Ch. 1], [5], [4].

Definition 2.1. Let Λ be a free $\mathbb{Z}$-module of rank n and $b : \Lambda \times \Lambda \to \mathbb{R}$ be a bilinear form.

(1) A pair $\Lambda = (\Lambda, b)$ is called a lattice if b is positive-definite and symmetric, that is, $b(x, x) > 0$ for every $x \in \Lambda \setminus \{0\}$ and $b(x, y) = b(y, x)$ for every $x, y \in \Lambda$. We often abbreviate (Λ, b) to Λ.
(2) A $\mathbb{Z}$-submodule Λ' of a lattice Λ is called a sublattice of Λ.
(3) A lattice Λ is called integral if $b(x, y) \in \mathbb{Z}$ for every $x, y \in \Lambda$.
(4) An integral lattice Λ is called even if $b(x, x) \in 2\mathbb{Z}$ for every $x \in \Lambda$, and odd otherwise.
(5) A lattice Λ is called of type A_n if Λ has a basis $(e_1, \dots, e_n)$ such that

$$b(e_i, e_j) = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } |j-i| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(6) A lattice Λ is called of type D_n $(n \geq 4)$ if Λ has a basis $(e_1, \ldots, e_n)$ such that

$$b(e_i, e_j) = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } (|j-i| = 1 \text{ and } \{i,j\} \neq \{n-1,n\}) \text{ or } \{i,j\} = \{n-2,n\}, \\ 0 & \text{otherwise.} \end{cases}$$

(7) A lattice Λ is called of type E_n $(n = 6, 7, 8)$

$$b(e_i, e_j) = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } (|j-i| = 1 \text{ and } \{i,j\} \neq \{n-1,n\}) \text{ or } \{i,j\} = \{n-3,n\}, \\ 0 & \text{otherwise.} \end{cases}$$

(8) For a lattice Λ of rank n, its dual lattice Λ^* is defined by

$$\Lambda^* := \left\{ x \in \mathbb{R}^{\oplus n} \;\middle|\; b(x,y) \in \mathbb{Z} \text{ for every } y \in \Lambda \right\},$$

where we extend b $\mathbb{R}$-bilinearly to $(\Lambda \otimes_{\mathbb{Z}} \mathbb{R}) \times (\Lambda \otimes_{\mathbb{Z}} \mathbb{R})$.

(9) A lattice Λ is called unimodular if $\Lambda^* = \Lambda$.

Note that a lattice Λ is integral if and only if $\Lambda \subset \Lambda^*$.

We summarize the well-known structure theorem of Λ^*/Λ for Λ of type A_n, D_n, E_n as follows.

Lemma 2.2. *We have the following isomorphisms of $\mathbb{Z}$-modules:*

$$\Lambda^*/\Lambda \simeq \begin{cases} \mathbb{Z}/(n+1)\mathbb{Z} & \text{if } \Lambda \text{ is of type } A_n, \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & \text{if } \Lambda \text{ is of type } D_n \text{ for even } n, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } \Lambda \text{ is of type } D_n \text{ for odd } n, \\ \mathbb{Z}/(9-n)\mathbb{Z} & \text{if } \Lambda \text{ is of type } E_n. \end{cases}$$

Proof. See e.g. [6, the proof of (v)⇔(vi) in Proposition 1.5]. □

Let $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}$ be a ring of order four with $u^2 = 0$

Definition 2.3. Let $n \geq 2$ and $m \geq 1$ be integers.

(1) The number of coordinates in $x \in (\mathbb{Z}/n\mathbb{Z})^{\oplus m}$ that take the value i is denoted by $l_i(x)$.

(2) The Euclidean weight $\mathrm{wt_E}(x)$ of an element $x \in (\mathbb{Z}/n\mathbb{Z})^{\oplus m}$ is defined by

$$\mathrm{wt_E}(x) := (1^2)l_1(x) + \cdots + ((n-1)^2)l_{n-1}(x).$$

(3) The Lee composition of an element $x = (x_1, \ldots, x_m) \in (\mathbb{F}_2 + u\mathbb{F}_2)^{\oplus m}$ is defined as $(N_0(x), N_1(x), N_2(x))$ where N_0 is the number of $x_i = 0$, $N_2(x)$ is the number of $x_i = u$, and $N_1(x) = m - N_0(x) - N_2(x)$.

(4) The Lee weight $\mathrm{wt_L}(x)$ of an element $x \in (\mathbb{F}_2 + u\mathbb{F}_2)^{\oplus m}$ is defined as $N_1(x) + 2N_2(x)$.

(5) The Bachoc weight $\mathrm{wt_B}(x)$ of an element $x \in (\mathbb{F}_2 + u\mathbb{F}_2)^{\oplus m}$ is defined as $2N_1(x) + N_2(x)$.

Definition 2.4. Let $n \geq 2$ and $m \geq 1$ be integers and R be either $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{F}_2 + u\mathbb{F}_2$.

(1) A code C of length m over R (or an R-code C of length m) is a R-submodule of $R^{\oplus m}$.

(2) The elements of C are called codewords.

(3) The inner product of $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m)$ in $R^{\oplus m}$ is given by

$$x \cdot y := \sum_{i=1}^{m} x_i y_i \;.$$

(4) The dual code of a R-code C of length m is defined by

$$C^{\perp} := \{x \in R^{\oplus m} \mid x \cdot y = 0 \text{ for every } y \in C\}.$$

(5) An R-code C is called Euclidean self-dual if $C = C^{\perp}$
(6) A Euclidean self-dual code C over $\mathbb{Z}/n\mathbb{Z}$ is called Type II if $\mathrm{wt_E}(x) \in 2n\mathbb{Z}$ for every $x \in C$.
(7) A Euclidean self-dual code C over $\mathbb{F}_2 + u\mathbb{F}_2$ is called Type II if $\mathrm{wt_L}(x) \in 4\mathbb{Z}$ for every $x \in C$.
(8) A Euclidean self-dual code C over $\mathbb{F}_2 + u\mathbb{F}_2$ is called Type IV if $\mathrm{wt_H}(x) \in 2\mathbb{Z}$ for every $x \in C$.

Definition 2.5. Let F be a number field.

(1) F is called totally real if every field homomorphism $F \to \mathbb{C}$ has the image in $\mathbb{R}$.
(2) F is called CM (complex multiplication) if F has no field homomorphisms $F \to \mathbb{R}$ and F has a totally real subfield F^+ such that $[F : F^+] = 2$.

If F is a CM number field, then F/F^+ is a Galois extension whose Galois group $\mathrm{Gal}(F/F^+)$ is generated by the complex conjugate.

Lemma 2.6. *Suppose that F is a totally real or CM number field. Then the bilinear form*

$$\mathrm{Tr} = \mathrm{Tr}_F : F \times F \to \mathbb{Q}; (x, y) \mapsto \mathrm{Tr}_{F/\mathbb{Q}}(x\bar{y})$$

is positive-definite and symmetric. In particular, for every $\mathbb{Z}$-submodule Λ of F, the pair $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ is a lattice.

Proof. The only non-trivial statement is the symmetry of Tr for a CM number field F, which we can check as follows:

$$\mathrm{Tr}_{F/\mathbb{Q}}(y\bar{x}) = \mathrm{Tr}_{F^+/\mathbb{Q}}(\mathrm{Tr}_{F/F^+}(y\bar{x})) = \mathrm{Tr}_{F^+/\mathbb{Q}}(y\bar{x}+x\bar{y}) = \mathrm{Tr}_{F^+/\mathbb{Q}}(\mathrm{Tr}_{F/F^+}(x\bar{y})) = \mathrm{Tr}_{F/\mathbb{Q}}(x\bar{y}).$$

□

Let K be a totally real number field of degree $r = [K : \mathbb{Q}]$. Let $\sigma_1, \dots, \sigma_r$ be the distinct embeddings of K into $\mathbb{R}$ with $\sigma_1 = \mathrm{id}$. We consider an n-dimensional vector space V over K equipped with a totally positive definite scalar product $\langle\ ,\ \rangle_K$. This means that $\langle\ ,\ \rangle_K : V \times V \to K$ is a symmetric bilinear form, and $\sigma_j(\langle v, v\rangle_K) > 0$ for all $1 \le j \le r$ and all $v \in V \setminus \{0\}$.

Definition 2.7. Let Λ be a finitely generated sub $\mathbb{Z}_K$-module of V which contains a K-basis of V. A pair $(\Lambda, \langle\ ,\ \rangle_K)$ is called a $\mathbb{Z}_K$-lattice in V.

For a $\mathbb{Z}_K$-lattice $(\Lambda, \langle\ ,\ \rangle_K)$, $\big(\Lambda, \mathrm{Tr}_{K/\mathbb{Q}}(\langle\ ,\ \rangle_K)\big)$ is a lattice.

Definition 2.8. The theta function $\theta_\Lambda(z)$ of a $\mathbb{Z}_K$-lattice $(\Lambda, \langle\ ,\ \rangle_K)$ is defined for $z = (z_1, \dots, z_r) \in \mathbb{H}^{\oplus r}$ by

$$\theta_\Lambda(z) := \sum_{x\in\Lambda} \exp(\pi\sqrt{-1}\,\mathrm{Tr}_{K/\mathbb{Q}}(\langle x, x\rangle_K z)),$$

where $\mathrm{Tr}_{K/\mathbb{Q}}(\langle x, x\rangle_K z) := \sum_{l=1}^{r} \sigma_l(\langle x, x\rangle_K) z_l$.

Proposition 2.9 ([6, Theorem 5.8])**.** *If a $\mathbb{Z}_K$-lattice $(\Lambda, \langle\ ,\ \rangle_K)$ of rank n is even unimodular as a lattice, the theta function θ_Λ is a Hilbert modular form of weight $n/2$ for $\mathrm{SL}_2(\mathbb{Z}_K)$, which means*

$$\theta_\Lambda\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = N_{K/\mathbb{Q}}(\gamma z + \delta)^{n/2} \cdot \theta_\Lambda(z) \quad \text{for all } \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_K).$$

3. Lattices of type A_n, D_n, E_n and codes

In this section, we generalize Construction A to a correspondence between lattices of type A_n, D_n, E_n and codes.

3.1. **Construction A.** Let C be a binary code. We consider the map $\rho_2^{\oplus m} : \left(\frac{1}{\sqrt{2}}\mathbb{Z}\right)^{\oplus m} \ni \frac{1}{\sqrt{2}}(x_i) \mapsto (x_i \mod 2) \in (\mathbb{Z}/2\mathbb{Z})^{\oplus m}$. We set $\Lambda_C = (\rho_2^{\oplus m})^{-1}(C)$. Then $(\Lambda_C, \ \cdot\ )$ is a lattice, where $\cdot$ denotes the standard Euclidean inner product. Moreover, $(\Lambda_C, \ \cdot\ )$ is even unimodular if and only if C is Type II (e.g., see [6, Proposition 1.3]).

3.2. **Generalization of Construction A by van der Geer and Hirzebruch.** We introduce a generalization of Construction A developed by van der Geer and Hirzebruch, which establishes a correspondence between the ring of integers in a cyclotomic field and p-ary codes (for details, see [6, Ch. 5]) Let p be an odd prime number and $\zeta_p = \exp(2\pi\sqrt{-1}/p)$. We consider the cyclotomic field $\mathbb{Q}(\zeta_p)$ and the map

$$\begin{array}{cccc} \rho_p^{\oplus m}: & \left(\frac{1}{(1-\zeta_p)^{\frac{p-1}{2}}}\mathbb{Z}_{\mathbb{Q}(\zeta_p)}\right)^{\oplus m} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{\oplus m} \\ & \cup & & \cup \\ & \frac{1}{(1-\zeta_p)\cdots(1-\zeta_p^{(p-1)/2})}\left(\sum_{j=0}^{p-2} x_{ij}\zeta_p^j\right) & \longmapsto & \left(\left(\sum_{j=0}^{p-2} x_{ij}\right) \bmod p\right). \end{array}$$

For a p-ary code C, let $\Lambda_C = (\rho_p^{\oplus m})^{-1}(C)$. Then the pair $\left(\Lambda_C, \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\ \cdot\bar{\ })\right)$ is a lattice. $\left(\Lambda_C, \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\ \cdot\bar{\ })\right)$ is even unimodular if and only if C is self-dual. Moreover, Λ_C is a $\mathbb{Z}_{\mathbb{Q}(\zeta_p)}$-module. Let $F = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $V = F^{\oplus m}$. For $x, y \in V$, we define a totally positive definite scalar product $\langle\ ,\ \rangle_K$ by $\langle x, y\rangle_K = \mathrm{Tr}_{F/K}(x \cdot \overline{y})$. Then $(\Lambda_C, \langle\ ,\ \rangle_K)$ is a $\mathbb{Z}_K$-lattice and the theta function θ_{Λ_C} is a Hilbert modular form of weight m for $\mathrm{SL}_2(\mathbb{Z}_K)$ if C is self-dual.

Let $\Lambda = \frac{1-\zeta_p}{(1-\zeta_p)^{\frac{p-1}{2}}}\mathbb{Z}_{\mathbb{Q}(\zeta_p)}$. Then $(\Lambda, \langle\ ,\ \rangle_K)$ is a $\mathbb{Z}_K$-lattice and

$$\left(\Lambda, \mathrm{Tr}_{F/\mathbb{Q}}(\ \cdot\bar{\ })\right)^* = \left(\frac{1}{(1-\zeta_p)^{\frac{p-1}{2}}}\mathbb{Z}_{\mathbb{Q}(\zeta_p)}, \mathrm{Tr}_{F/\mathbb{Q}}(\ \cdot\bar{\ })\right).$$

For $a \in \Lambda^*/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} = \{0, \ldots, p-1\}$, we define

$$\theta_a := \theta_{a+\Lambda}(z) = \sum_{x \in a+\Lambda} \exp\left((\pi\sqrt{-1})\,\mathrm{Tr}_{K/\mathbb{Q}}(\langle x, x\rangle_K z)\right).$$

The Lee weight enumerator of a code C of length m over $\mathbb{Z}/p\mathbb{Z}$ is the polynomial

$$W_C\left(X_0, X_1, \ldots, X_{(p-1)/2}\right) := \sum_{c \in C} \prod_{i=1}^{(p-1)/2} X_i^{l_i(c)+l_{p-i}(c)}$$

Since $\theta_a = \theta_{-a}$, we have the following proposition.

Proposition 3.1 ([6, Theorem 5.3])**.**

$$\theta_{\Lambda_C} = W_C\left(\theta_0, \theta_1, \ldots, \theta_{(p-1)/2}\right).$$

3.3. **Extending the generalization of Construction A.** We discuss further extensions of Construction A. The lattice $\left(\frac{1}{\sqrt{2}}\mathbb{Z}, \ \cdot\ \right)$ is the dual lattice of a lattice of type A_1 and the lattice $\left(\frac{1}{(1-\zeta_p)^{\frac{p-1}{2}}}\mathbb{Z}_{\mathbb{Q}(\zeta_p)}, \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\ \cdot\bar{\ })\right)$ is the dual lattice of a lattice of type A_{p-1}. Since $\Lambda^*/\Lambda \simeq \mathbb{Z}/(n+1)\mathbb{Z}$ for a lattice Λ of type A_n, we can view the maps $\rho_2^{\oplus m}$ and $\rho_p^{\oplus m}$ as being induced by the natural projection from Λ^* to Λ^*/Λ. This observation suggests that these constructions can be naturally extended to other even root lattices, such as those of type A_n, D_n, or E_n. The following theorem is the main result in this study.

Theorem 3.2 ([7, Theorem 1.1]). *Let n and m be positive integers, Λ be a lattice of type A_n, D_n or E_n, and C be an R-code of length m, where*

$$R = \begin{cases} \mathbb{Z}/(n+1)\mathbb{Z} & \text{if } \Lambda \text{ is a lattice of type } A_n, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } \Lambda \text{ is a lattice of type } D_n \text{ for odd } n, \\ \mathbb{F}_2 + u\mathbb{F}_2 & \text{if } \Lambda \text{ is a lattice of type } D_n \text{ for even } n, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } \Lambda \text{ is a lattice of type } E_6, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } \Lambda \text{ is a lattice of type } E_7. \end{cases}$$

There exists a mapping $\rho_\Lambda^{\oplus m} : (\Lambda^*)^{\oplus m} \to R^{\oplus m}$ such that

$$\Lambda_C (= (\rho_\Lambda^{\oplus m})^{-1}(C)) \text{ is even unimodular} \Leftrightarrow$$

$$\begin{cases} C \text{ is Type II} & \text{if } \Lambda \text{ is a lattice of type } A_n \text{ for odd } n, \\ C \text{ is self-dual} & \text{if } \Lambda \text{ is a lattice of type } A_n \text{ for even } n, \\ C \text{ is Type II} & \text{if } \Lambda \text{ is a lattice of type } D_n \text{ for odd } n, \\ C \text{ is Type II} & \text{if } \Lambda \text{ is a lattice of type } D_n \text{ in the case } n \in 2\mathbb{Z} \text{ and } n \notin 4\mathbb{Z}, \\ C \text{ is Type IV} & \text{if } \Lambda \text{ is a lattice of type } D_n \text{ in the case } n \in 4\mathbb{Z}, \\ C \text{ is self-dual} & \text{if } \Lambda \text{ is a lattice of type } E_6, \\ C \text{ is Type II} & \text{if } \Lambda \text{ is a lattice of type } E_7. \end{cases}$$

4. Applications to Hilbert Modular Forms

Based on Theorem 3.2, the following questions naturally arise when extending the results of van der Geer and Hirzebruch.

Question 4.1. *Let K be a totally real number field.*

1. *Does there exist a $\mathbb{Z}_K$-lattice that is isomorphic to type A_n, D_n, or E_n as a lattice?*
2. *In particular, for a totally real or CM field F of degree n, can a fractional ideal Λ of F become a lattice $(\Lambda, Tr_{F/\mathbb{Q}})$ of type A_n, D_n, or E_n?*

Table 1. Known realizations of root lattices as fractional ideals

Lattice	Number field	Fractional ideal	Reference
A_{p-1}	$\mathbb{Q}(\zeta_p)$	$\mathfrak{P}_p^{-(p-3)/2}$	[3]
D_4	$\mathbb{Q}(\zeta_8)$	$\mathfrak{P}_2^{-3}$	[1]
E_6	$\mathbb{Q}(\zeta_9)$	$\mathfrak{P}_3^{-4}$	[1]
E_8	$\mathbb{Q}(\zeta_{20})$	$\mathfrak{P}_2\mathfrak{P}_5^{-3}$	[1]

Here, $\mathfrak{P}_q$ denotes a prime ideal lying above q in each number field.

Previous studies related to Question 4.1 (2) are summarized in Table 1. In this section, we apply Theorem 3.2 to the lattices of type D_4 and E_6 obtained from these existing constructions.

4.1. **Lattice of type E_6 as a fractional ideal of $\mathbb{Q}(\zeta_9)$.** Let $F = \mathbb{Q}(\zeta_9)$, $K = \mathbb{Q}(\zeta_9+\zeta_9^{-1})$ and $\Lambda = \frac{1}{(1-\zeta_9)^4}\mathbb{Z}_F$. Let C be a $\mathbb{Z}/3\mathbb{Z}$-code of length m. It is known from [1] that the pair $(\Lambda, \mathrm{Tr}_{F/\mathbb{Q}}(x\overline{y}))$ forms a lattice of type E_6.

By Theorem 3.2, there exists a mapping $\rho_\Lambda^{\oplus m} : (\Lambda^*)^{\oplus m} \to (\mathbb{Z}/3\mathbb{Z})^{\oplus m}$ such that the lifted lattice $\Lambda_C := (\rho_\Lambda^{\oplus m})^{-1}(C)$, equipped with the trace form $\mathrm{Tr}_{F/\mathbb{Q}}(x \cdot \overline{y})$, is even unimodular if and only if C is self-dual.

Here, we define a totally positive definite scalar product on $F^{\oplus n}$ by

$$\langle x, y\rangle_K := \mathrm{Tr}_{F/K}(x \cdot \overline{y}).$$

For each class $a \in \Lambda^*/\Lambda \simeq \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, we define the component theta function for $z \in \mathbb{H}^{\oplus 3}$ by

$$\theta_a(z) := \theta_{a+\Lambda}(z) = \sum_{x \in a+\Lambda} \exp\left(\pi\sqrt{-1}\,\mathrm{Tr}_{K/\mathbb{Q}}(\langle x, x\rangle_K z)\right).$$

Since $a^2 = (-a)^2$ for $a \in \mathbb{Z}/3\mathbb{Z}$, we have $\theta_1 = \theta_2$. Because $(\Lambda_C, \langle\cdot,\cdot\rangle_K)$ carries the structure of a $\mathbb{Z}_K$-lattice, its associated total theta function θ_{Λ_C} is a Hilbert modular form of weight m for $\mathrm{SL}_2(\mathbb{Z}_K)$ whenever C is self-dual. Furthermore, this theta function can be explicitly evaluated using the code's structural invariants:

Theorem 4.2. *Let C be a $\mathbb{Z}/3\mathbb{Z}$-code of length m, and let $W_C(X_0, X_1)$ be its Lee weight enumerator. Then we have*

$$\theta_{\Lambda_C} = W_C(\theta_0, \theta_1).$$

4.2. **Lattice of type D_4 as a fractional ideal of $\mathbb{Q}(\zeta_8)$.** Let $F = \mathbb{Q}(\zeta_8)$, $K = \mathbb{Q}(\zeta_8+\zeta_8^{-1})$ and $\Lambda = \frac{1}{(1-\zeta_8)^3}\mathbb{Z}_F$. Let C be a $\mathbb{F}_2 + u\mathbb{F}_2$-code of length m. It is known from [1] that the pair $(\Lambda, \mathrm{Tr}_{F/\mathbb{Q}}(x\overline{y}))$ forms a lattice of type D_4.

By Theorem 3.2, there exists a mapping $\rho_\Lambda^{\oplus m} : (\Lambda^*)^{\oplus m} \to (\mathbb{F}_2 + u\mathbb{F}_2)^{\oplus m}$ such that the lifted lattice $\Lambda_C := (\rho_\Lambda^{\oplus m})^{-1}(C)$, equipped with the trace form $\mathrm{Tr}_{F/\mathbb{Q}}(x \cdot \overline{y})$, is even unimodular if and only if C is Type IV.

Here, we define a totally positive definite scalar product on $F^{\oplus n}$ by

$$\langle x, y\rangle_K := \mathrm{Tr}_{F/K}(x \cdot \overline{y}).$$

For each class $a \in \Lambda^*/\Lambda \simeq \mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}$, we define the component theta function for $z \in \mathbb{H}^{\oplus 2}$ by

$$\theta_a(z) := \theta_{a+\Lambda}(z) = \sum_{x \in a+\Lambda} \exp\left(\pi\sqrt{-1}\,\mathrm{Tr}_{K/\mathbb{Q}}(\langle x, x\rangle_K z)\right).$$

Since $1^2 = (1+u)^2$, we have $\theta_1 = \theta_{1+u}$. Because $(\Lambda_C, \langle\cdot,\cdot\rangle_K)$ carries the structure of a $\mathbb{Z}_K$-lattice, its associated total theta function θ_{Λ_C} is a Hilbert modular form of weight m for $\mathrm{SL}_2(\mathbb{Z}_K)$ whenever C is Type IV.

The Lee weight enumerator of a code C of length m over $\mathbb{F}_2 + u\mathbb{F}_2$ is the polynomial

$$W_C(X_0, X_1, X_2) := \sum_{x \in C} X_0^{N_0(x)} X_1^{N_1(x)} X_2^{N_2(x)}.$$

The theta function θ_{Λ_C} can be explicitly evaluated using the code's structural invariants:

Theorem 4.3. *Let C be a $\mathbb{F}_2 + u\mathbb{F}_2$-code of length m. Then we have*

$$\theta_{\Lambda_C} = W_C(\theta_0, \theta_1, \theta u).$$

References

[1] Eva Bayer-Flückiger, *Lattices and number fields* (1999), 69–84. MR1718137

[2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1988. With contributions by E. Bannai, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR920369

[3] Maurice Craig, *Automorphisms of prime cyclotomic lattices*, preprint.

[4] Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, Akihiro Munemasa, and Patrick Solé, *Type IV self-dual codes over rings*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2345–2360. MR1725122

[5] Steven T. Dougherty, Thomas A. Gulliver, and Masaaki Harada, *Type II self-dual codes over finite rings and even unimodular lattices*, J. Algebraic Combin. **9** (1999), no. 3, 233–250. MR1695075

[6] Wolfgang Ebeling, *Lattices and codes*, 3rd ed., Advanced Lectures in Mathematics, Springer Spektrum, Wiesbaden. A course partially based on lectures by Friedrich Hirzebruch. MR2977354

[7] Riku Higa, *Lattices of type A_n, D_n, E_n and codes*, 2025, https://arxiv.org/abs/2502.19753.

[8] Riku Higa and Yoshinosuke Hirakawa, *Galois trace forms of type A_n, D_n, E_n for odd n*, J. Number Theory **275** (2025), 196–213. MR4878849

[9] Gabriele Nebe and Neil Sloane, *Lattices: The brandt-intrau-schiemann table of odd ternary quadratic forms.* `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_1.html`.
[10] Vladimir L. Popov and Yuri G. Zarhin, *Root lattices in number fields*, Bull. Math. Sci. **11** (2021), no. 3, Paper No. 2050021, 22. MR4354460
[11] Jean-Pierre Serre, *Topics in Galois theory*, Second, Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008. With notes by Henri Darmon. MR2363329

(Riku Higa) Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641, Yamazaki, Noda, Chiba, Japan
Email address: 6123702@ed.tus.ac.jp, 6121510@ed.tus.ac.jp