Acta Math., 175 (1995), 123–150

Self-dual lattices of type A

by

XIAOPING XU(1)

The Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong

1. Introduction

The existence of an infinite-dimensional module for the Monster group (the largest finite simple sporadic group), satisfying a number of remarkable properties known collectively as "moonshine", was conjectured by McKay, Thompson, Conway and Norton (e.g., see [6]). Frenkel, Lepowsky and Meurman [13], [14] constructed an example of such a representation—the so-called "moonshine module"—as a certain special type of vertex operator algebra on which the Monster acts, and proved that the Monster is in fact the full automorphism group for this algebra.

One of key steps in the construction of the moonshine module is the construction of what Frenkel, Lepowsky and Meurman called "triality", which essentially consists of certain modules for a vertex operator algebra associated with an integral lattice constructed by gluing finite copies of the root lattice of type A_1. The main technique in the triality work involves using four kinds of vertex operator realizations of type $\hat{A}_1^{(1)}$.

We ask whether there exist other vertex operator algebras whose automorphism groups are finite. From the finite group point of view, we try to find more finite groups which have a moonshine representation analogous to that of the Monster. One of the initial steps in this direction is that we need to study self-dual lattices related to a finite number of any root lattices of type A.

In terms of the classification of simple vertex operator algebras (or related conformal field theories), one has to know more simple vertex operator algebras. One of the important ways to construct vertex operator algebras is the technique used by Frenkel, Lepowsky and Meurman [13], [14] in constructing the moonshine module, which could be called the "$\mathbf{Z}_2$-orbit fold technique" (also cf. [10]). A natural generalization of this technique is the "$\mathbf{Z}_n$-orbit fold technique" for any natural number $n\geqslant 2$. One of the best

---

(1) The results in this paper are extracted from the author's Ph.D. dissertation at Rutgers University, 1992.

ways of realizing this generalization is to invoke vertex operator algebras constructed from lattices related to finite copies of a root lattice of type A_{n-1}.

In this paper, we obtain two gluing techniques for constructing self-dual lattices by analyzing the constructions of self-dual lattices in [7], [8], [22] and refining the well-known gluing theory of Conway and Sloane (cf. §3, Chapter 4 of [9]). Using these techniques, we construct two families of self-dual lattices related to a finite number of any root lattices of type A, based on the ring structure of a root lattice of type A induced by the Coxeter element.

Let us recall some basic definitions. We denote the field of rational numbers by $\mathbf{Q}$ and the ring of integers by $\mathbf{Z}$. A (*rational*) *lattice* L is a free Abelian group (or free $\mathbf{Z}$-module) of finite rank with a $\mathbf{Q}$-valued symmetric $\mathbf{Z}$-bilinear form $\langle\cdot,\cdot\rangle$. The rank is sometimes called the *dimension* of the lattice. Let $L_{\mathbf{Q}}=\mathbf{Q}\otimes_{\mathbf{Z}}L$ and extend $\langle\cdot,\cdot\rangle$ to $L_{\mathbf{Q}}$ canonically. The *integral dual* L° of L is defined by

$$L^\circ=\{y\in L_{\mathbf{Q}}\mid\langle y,x\rangle\in\mathbf{Z}\text{ for all }x\in L\}. \tag{1.1}$$

The dual L° is also a lattice if $\langle\cdot,\cdot\rangle$ is nondegenerate. If L is a root lattice of type A, D or E, then L° is the weight lattice. A lattice L is called *integral* (*self-dual*) if $L\subset L^\circ$ ($L=L^\circ$).

Many of the known constructions of self-dual lattices involve "linear codes". In this paper, we need the following concepts of codes. Let n be a positive integer and let $\mathbf{Z}_n=\mathbf{Z}/(n)$. A *linear code of length* k over $\mathbf{Z}_n$ is a $\mathbf{Z}_n$-submodule of $\mathbf{Z}_n^k$. Let f be a symmetric $\mathbf{Z}_n$-bilinear form on $\mathbf{Z}_n^k$. The *dual code* of C is defined by

$$C_f^\perp=\{\alpha\in\mathbf{Z}_n^k\mid f(\alpha,\beta)=0\text{ for all }\beta\in C\}. \tag{1.2}$$

A code C is called *self-orthogonal* (*self-dual*) *relative to* f if $C\subset C_f^\perp$ ($C=C_f^\perp$). If f is a symmetric bilinear form associated with a matrix of the form

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix}, \tag{1.3}$$

then we also say that C is self-orthogonal (self-dual) *relative to* $\mathbf{d}=(d_1,\dots,d_n)$. When $\mathbf{d}=(1,\dots,1)$, we simply say that C is self-orthogonal (self-dual). A code over $\mathbf{Z}_2$ ($\mathbf{Z}_3$) is called a *binary* (*ternary*) code. An element of a code is called a *codeword.* The (*Hamming*) *weight* of a codeword is the number of its nonzero coordinates. A binary code is a *doubly even* code if the weights of its codewords are divisible by 4.

Next, let us use the following known examples to explain the development of our idea in this paper.

Construction 1 (cf. [14], [16], [22]). Let k be a positive even integer and let $V=\mathbf{Q}^k$, $L=\mathbf{Z}^k$. Define the symmetric $\mathbf{Z}$-bilinear form $\langle\cdot,\cdot\rangle$ on V by

$$\langle\alpha,\beta\rangle=\frac{1}{2}\sum_{j=1}^{k}\alpha_j\beta_j,\quad \alpha=(\alpha_j),\beta=(\beta_j)\in V. \tag{1.4}$$

Set

$$x_i=(0,\ldots,0,\overset{i}{1},0,\ldots,0)\quad \text{for } i=1,\ldots,k. \tag{1.5}$$

Then each $\mathbf{Z}2x_i$ is a copy of the root lattice of type A_1 with respect to $\langle\cdot,\cdot\rangle$. Define a section map $\eta\colon\mathbf{Z}_2\to\mathbf{Z}$ by $\eta(0)=0$, $\eta(1)=1$. For $\mathbf{c}=(c_j)\in\mathbf{Z}_2^k$, let

$$\Theta_{\mathbf{c}}=(\eta(c_1),\ldots,\eta(c_k)). \tag{1.6}$$

Let C be a doubly even self-dual binary code of length k (k must be divisible by 8 (e.g., cf. [9], [22])). Set

$$L_{2,A}[C]=\sum_{\mathbf{c}\in C}\mathbf{Z}\Theta_{\mathbf{c}}+2L. \tag{1.7}$$

Then the lattice $L_{2,A}[C]$ is a self-dual lattice, where 2 means the dual Coxeter number of A_1. Let

$$\begin{aligned}\tilde{L}_{2,A}[C]=\mathbf{Z}\big(\tfrac{1}{2}(1-4\varepsilon,1,\ldots,1)\big)+\sum_{\mathbf{c}\in C}\mathbf{Z}\Theta_{\mathbf{c}}\\ +\left\{2\alpha\,\middle|\,\alpha=(\alpha_j)\in L,\ \sum_{j=1}^{k}\alpha_j\equiv 0\ (\mathrm{mod}\ 2)\right\},\end{aligned} \tag{1.8}$$

where $\varepsilon=0,1$. Then $\tilde{L}_{2,A}[C]$ is also a self-dual lattice. We can see that the lattice $L_{2,A}[C]$ is obtained by gluing k copies of the root lattice of type A_1 with C as a "glue code". Moreover, the lattice $\tilde{L}_{2,A}[C]$ can be interpreted to be obtained by twisting the lattice $L_{2,A}[C]$.

Construction 2 (cf. [22]). Let k be a positive even integer again. Let $\mathbf{Q}_3^A=\mathbf{Q}(\omega_3)$ and $R_3^A=\mathbf{Z}[\omega_3]$ with $\omega_3=e^{2\pi i/3}$. The ring R_3^A is called the ring of *Eisenstein integers.* Set $V=(\mathbf{Q}_3^A)^k$, $L=(R_3^A)^k$ and define the positive definite Hermitian form $(\cdot,\cdot)_{3,A}$ and symmetric form $\langle\cdot,\cdot\rangle_{3,A}$ by

$$(\alpha,\beta)_{3,A}=\sum_{j=1}^{k}\alpha_j\bar{\beta}_j,\quad \alpha=(\alpha_j),\beta=(\beta_j)\in V;\quad \langle\cdot,\cdot\rangle_{3,A}=\tfrac{2}{3}\operatorname{Re}(\cdot,\cdot)_{3,A}. \tag{1.9}$$

Then each $R_3^A(1-\omega_3)x_i$ is a copy of the root lattice of type A_2 for $i=1,\dots,k$. In the above notations, the subindex "3" means the dual Coxeter number of A_2. Again we define a section map $\eta:\mathbf{Z}_3\to\mathbf{Z}$ by $\eta(0)=0$, $\eta(1)=1$, $\eta(2)=2$. For $\mathbf{c}=(c_j)\in\mathbf{Z}_3^k$, set

$$\Theta_{\mathbf{c}}=(\eta(c_1),\dots,\eta(c_k)). \tag{1.10}$$

Let $\mathcal{C}$ be a self-dual ternary code of length k. Set

$$L_{3,A}[\mathcal{C}]=\sum_{\mathbf{c}\in\mathcal{C}}\mathbf{Z}\Theta_{\mathbf{c}}+(1-\omega_3)L. \tag{1.11}$$

Then $L_{3,A}[\mathcal{C}]$ is a self-dual lattice with respect to $\langle\cdot,\cdot\rangle_{3,A}$. The lattice $L_{3,A}[\mathcal{C}]$ can be viewed as being obtained by gluing k copies of the root lattice of type A_2 with $\mathcal{C}$ as a glue code.

The following construction seems only known for the ternary Golay code $\mathcal{G}_{12}$ (of length 12) (e.g., cf. [9], [22]). Let $k=12$. Any $\alpha\in L$ can be written uniquely as $\alpha=(\lambda_{1,0}+\lambda_{1,1}\omega_3,\dots,\lambda_{12,0}+\lambda_{12,1}\omega_3)$, where $\lambda_{j,i}\in\mathbf{Z}$. We define

$$T(\alpha)=\sum_{j=1}^{12}(\lambda_{j,0}+\lambda_{j,1}). \tag{1.12}$$

Then

$$\begin{aligned}\tilde{L}_{3,A}[\mathcal{G}_{12}]=\mathbf{Z}\left(\frac{1}{1-\omega_3}(\omega_3-3,\omega_3,\dots,\omega_3)\right)+\sum_{\mathbf{c}\in\mathcal{G}_{12}}\mathbf{Z}\Theta_{\mathbf{c}}\\ +\{(1-\omega_3)\alpha\mid\alpha\in L,\ T(\alpha)\equiv 0\pmod 3\}\end{aligned} \tag{1.13}$$

is a copy of the Leech lattice with respect to $\langle\cdot,\cdot\rangle_{3,A}$. The lattice $\tilde{L}_{3,A}[\mathcal{G}_{12}]$ can be interpreted as being obtained by twisting $L_{3,A}[\mathcal{G}_{12}]$.

We first analyze these constructions and the constructions of self-dual lattices in [7], [8], and find certain common characteristics. Then we generalize the above constructions of $L_{2,A}[\mathcal{C}]$ and $L_{3,A}[\mathcal{C}]$ to a construction technique which we call an "untwisted gluing technique". By this technique, we construct a large family of self-dual lattices by gluing a finite number of root lattices (not necessarily the same) of type A with certain relatively self-dual codes over $\mathbf{Z}_n$ (n not necessarily prime) as glue codes. We call these lattices *untwisted self-dual lattices of type A*. Similarly, we generalize the constructions of $\tilde{L}_{2,A}[\mathcal{C}]$ and $\tilde{L}_{3,A}[\mathcal{G}_{12}]$ to a construction technique which we call a "twisted gluing technique". This technique results from modifying the untwisted technique in the same way that one twists $L_{2,A}[\mathcal{C}]$ and $L_{3,A}[\mathcal{G}_{12}]$ into $\tilde{L}_{2,A}[\mathcal{C}]$ and $\tilde{L}_{3,A}[\mathcal{G}_{12}]$. By this technique, we get another large family of self-dual lattices, which we call "twisted self-dual lattices of type A", by twisting the untwisted ones. Our techniques can be viewed as refinements of the gluing theory of Conway and Sloane (cf. §3, Chapter 4 of [9]). Certain lattices in our two families of type-A lattices are known (e.g., see [2], [7], [8]).

By [19], the lattices $L_{3,A}[\mathcal{C}]$ and $\tilde{L}_{3,A}[\mathcal{G}_{12}]$ are "complex self-dual lattices". We prove that the untwisted self-dual lattices of type A obtained by gluing finite copies of the same root lattice and the corresponding twisted lattices with $(1,...,1)$ in the glue codes possess certain properties of complex self-dual lattices (see Theorems 5.12 and 5.14). The Coxeter element of the root lattice acts on these lattices as a fixed-point-free lattice automorphism. In fact, if the root lattice is of type A_{p-1} with p prime, then these lattices are complex self-dual lattices (cf. [12], [22]). In general cases of the root lattice, we call these lattices *self-dual complex lattices of type A*.

The self-dual type-A complex lattices that we construct in this paper are proved, in another work [26], to have very nice properties with respect to their central extensions. In [27], we find more twisted vertex operator realizations of the basic representations of $A_n^{(1)}$ by means of the ring structure of a root lattice of type A used in this paper. We construct in [28] an analogue of "vertex operator triality" for each self-orthogonal ternary code containing $(1,...,1)$. This would be a key step in constructing what we will call "ternary moonshine vertex operator algebras", which will be analogues of the moonshine module (cf. [13], [14]) in terms of the vertex operator structures.

The structure of this paper is as follows:

In §2, we present the untwisted technique for self-dual lattices and a decomposability theorem. In §3, the twisted gluing technique is given. We present the construction of untwisted type-A lattices in §4. In §5, the twisted construction of type-A lattices is given. Finally, in §6, we find out all the "basic homogeneous twist parameters of type A" appearing in the twisted construction.

2. The untwisted gluing technique

The definition of a (rational) lattice and some related definitions are the same as in the introduction. Now we give the other definitions that we will use.

Definition 2.1. The lattice L is said to be *decomposable* if $L=L_1\oplus L_2$ as a $\mathbf{Z}$-module and $\langle\cdot,\cdot\rangle=\langle\cdot,\cdot\rangle_1\oplus\langle\cdot,\cdot\rangle_2$, where $\langle\cdot,\cdot\rangle_i$ is a symmetric $\mathbf{Z}$-bilinear form of L_i.

Let L_1 and L_2 be lattices with associated $\mathbf{Z}$-bilinear forms $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$, respectively. The lattices L_1 and L_2 are said to be *isomorphic* if there exists a $\mathbf{Z}$-module isomorphism $\tau\colon L_1\to L_2$ such that

$$\langle\tau(\xi),\tau(\xi')\rangle_2=\langle\xi,\xi'\rangle_1 \quad \text{for all } \xi,\xi'\in L_1. \tag{2.1}$$

Such a τ is called a *lattice isomorphism*, and it is called a *lattice automorphism* if $L_1=L_2$. We use the notation $\mathrm{Aut}(L)$ to denote the group of all (lattice) automorphisms of a lattice L.

Remark 2.2. In the rest of our paper, the extension of $\langle\cdot,\cdot\rangle$ to $L_{\mathbf{Q}}$ for a lattice L is always taken for granted.

Let m, n be integers. We use g.c.d.$\{m,n\}$ to denote the "greatest common divisor of m and n" and l.c.m.$\{m,n\}$ to denote the "least common multiple of m and n". The same notations are also used for more integers. Throughout this paper, we use the index notation $\Omega(k)=\{1,\ldots,k\}$ for any positive integer k. We also take $\Omega(0)=\varnothing$.

Our untwisted gluing technique is based on the following concept.

Definition 2.3. Let L be an integral lattice with associated $\mathbf{Z}$-bilinear form $\langle\cdot,\cdot\rangle$. Suppose that there exist a set $\{x_i,\zeta_j,\xi_j\mid i\in\Omega(s),\, j\in\Omega(t)\}$ of vectors of L° such that:

(1)

$$L^\circ/L=\bigoplus_{i=1}^{s}\langle x_i+L\rangle\oplus\bigoplus_{j=1}^{t}[\langle\zeta_j+L\rangle\oplus\langle\xi_j+L\rangle] \tag{2.2}$$

as Abelian groups, where each $\langle x_i+L\rangle$ is a cyclic group of order n_i, and $\langle\zeta_j+L\rangle$, $\langle\xi_j+L\rangle$ are cyclic groups of order m_j for each j;

(2)

$$\langle x_i,x_i\rangle\equiv\frac{\beta_i}{n_i},\quad \langle\zeta_j,\xi_j\rangle\equiv\frac{1}{m_j}\quad (\mathrm{mod}\ \mathbf{Z}),\quad i\in\Omega(s),\ j\in\Omega(t), \tag{2.3}$$

where $\beta_i\in\mathbf{Z}$, g.c.d.$\{\beta_i,n_i\}=1$, and

$$\langle\zeta,\zeta'\rangle\in\mathbf{Z}\quad \text{for any other pair } \zeta,\zeta'\in\{x_i,\zeta_j,\xi_j\}. \tag{2.4}$$

Then we call $\mathcal{S}=(L;\langle\cdot,\cdot\rangle;x_i;\zeta_j;\xi_j;i\in\Omega(s),j\in\Omega(t))$ a *U-shell* of self-dual lattices. A shell $\mathcal{S}$ is called *type* I (*type* II) if $t=0$ ($s=0$). Moreover, x_i are called *untwisted glue vectors of type* I, and ζ_j,ξ_j are called *untwisted glue vectors of type* II. Two shells are called equivalent if the underlying lattices are isomorphic.

Remark 2.4. (a) If m_j is odd for some $j\in\Omega(t)$, the pair ζ_j,ξ_j can be changed into glue vectors of type I as follows: Choose $\alpha\in\mathbf{Z}$ such that $2\alpha\equiv 1$ (mod m_j). Set

$$x_j^*=\alpha(\zeta_j+\xi_j),\quad x_j^\dagger=\alpha(\zeta_j-\xi_j). \tag{2.5}$$

Then we have

$$\langle x_j^*,x_j^\dagger\rangle\equiv 0,\quad \langle x_j^*,x_j^*\rangle\equiv-\langle x_j^\dagger,x_j^\dagger\rangle\equiv\frac{\alpha}{m_j}\quad (\mathrm{mod}\ \mathbf{Z}). \tag{2.6}$$

Changing $\zeta_j \to x_j^*$, $\xi_j \to x_j^\dagger$ in $\mathcal{S}$, we get an equivalent shell because $\zeta_j \equiv x_j^* + x_j^\dagger$, $\xi_j \equiv x_j^* - x_j^\dagger$ (mod L).

(b) If $\mathcal{S}$ only satisfies (2.2) and (2) in Definition 2.3, then we can make $\mathcal{S}$ to be a U-shell through the replacement of L by $L + \sum_{i=1}^{s} \mathbf{Z} n_i x_i + \sum_{j=1}^{t} [\mathbf{Z} m_j \zeta_j + \mathbf{Z} m_j \xi_j]$.

Our untwisted gluing technique has two steps.

Step 1. *Combining a finite number of U-shells into a larger U-shell.*

Let $\{(L_l; \langle \cdot, \cdot \rangle_l; x_{li}; \zeta_{lj}; \xi_{lj}; i \in \Omega(s_l), j \in \Omega(t_l)) \mid l \in \Omega(k)\}$ be a family of k U-shells of self-dual lattices. We define

$$L = \bigoplus_{l=1}^{k} L_l \quad \text{as } \mathbf{Z}\text{-modules}, \quad \langle \cdot, \cdot \rangle = \bigoplus_{l=1}^{k} \langle \cdot, \cdot \rangle_l \quad \text{on } L \times L. \tag{2.7}$$

Then we have

$$L_{\mathbf{Q}} = \bigoplus_{l=1}^{k} L_{l\mathbf{Q}}, \quad L^\circ = \bigoplus_{l=1}^{k} L_l^\circ. \tag{2.8}$$

We identify L_l with $L_l \oplus \bigoplus_{l' \neq l} 0^{(l')}$, where $0^{(l')}$ is the zero vector of $L_{l'}$. Thus, we have the following new larger U-shell of self-dual lattices:

$$(L; \langle \cdot, \cdot \rangle; x_{li}; \zeta_{lj}; \xi_{lj}; l \in \Omega(k), i \in \Omega(s_l), j \in \Omega(t_l)). \tag{2.9}$$

Step 2. *Gluing a given U-shell into a self-dual lattice.*

Let $\mathcal{S}$ be a U-shell of self-dual lattices, and let other notations be the same as in Definition 2.3. Set

$$M = \text{l.c.m.}\{n_i, m_j \mid i \in \Omega(s), j \in \Omega(t)\} \tag{2.10}$$

and

$$\varepsilon_i = \frac{M}{n_i}, \quad d_i = \beta_i \varepsilon_i, \quad \gamma_j = \frac{M}{m_j}, \quad \text{for } i \in \Omega(s),\ j \in \Omega(t). \tag{2.11}$$

Furthermore, we set

$$\mathbf{d} = (d_1, \ldots, d_s), \quad \gamma = (\gamma_1, \ldots, \gamma_t), \tag{2.12}$$

and define $f(\cdot, \cdot)$ to be the symmetric $\mathbf{Z}_M$-bilinear form on $\mathbf{Z}_M^{s+2t}$ associated with the symmetric matrix

$$B_f = \begin{pmatrix} B_{\mathbf{d}} & & \\ & & B_\gamma \\ & B_\gamma & \end{pmatrix}, \tag{2.13}$$

where for any $\alpha = (\alpha_1, \ldots, \alpha_l) \in \mathbf{Z}_M^l$,

$$B_\alpha = \begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_l \end{pmatrix}. \tag{2.14}$$

Here we use empty positions to denote the entries 0.

For any $\mathbf{c}\in\mathbf{Z}_M^{s+2t}$, we write $\mathbf{c}=(\mathbf{c}^{\mathrm{I}},\mathbf{c}^{\mathrm{II}},\mathbf{c}^{\mathrm{III}})$, where

$$\mathbf{c}^{\mathrm{I}}=(c_1^{\mathrm{I}},\dots,c_s^{\mathrm{I}})\in\mathbf{Z}_M^s;\quad \mathbf{c}^p=(c_1^p,\dots,c_t^p)\in\mathbf{Z}_M^t,\quad p=\mathrm{II},\mathrm{III}. \tag{2.15}$$

We define the $\eta_M\colon\mathbf{Z}_M\to\mathbf{Z}$ by $\eta_M(N)=l$ with $0\leqslant l<M$ if $N\equiv l \pmod{M}$ for any $N\in\mathbf{Z}_M$. We now define

$$x_{\mathbf{c}^{\mathrm{I}}}=\sum_{i=1}^{s}\eta_M(c_i^{\mathrm{I}})x_i,\quad \zeta_{\mathbf{c}^{\mathrm{II}}}=\sum_{j=1}^{t}\eta_M(c_j^{\mathrm{II}})\zeta_j,\quad \xi_{\mathbf{c}^{\mathrm{III}}}=\sum_{j=1}^{t}\eta_M(c_j^{\mathrm{III}})\xi_j \tag{2.16}$$

and

$$\Theta_{\mathbf{c}}=x_{\mathbf{c}^{\mathrm{I}}}+\zeta_{\mathbf{c}^{\mathrm{II}}}+\xi_{\mathbf{c}^{\mathrm{III}}}. \tag{2.17}$$

Let C be a code of length $s+2t$ over $\mathbf{Z}_M$. We define

$$L(C)=\sum_{\mathbf{c}\in C}\mathbf{Z}\Theta_{\mathbf{c}}+L. \tag{2.18}$$

In addition, we set

$$\mathbf{n}=(n_1,\dots,n_s),\quad \mathbf{m}=(m_1,\dots,m_t) \tag{2.19}$$

and

$$\begin{aligned}\mathcal{R}[\mathbf{n},\mathbf{m}]=\{&(n_1c_1^{\mathrm{I}},\dots,n_sc_s^{\mathrm{I}},m_1c_1^{\mathrm{II}},\dots,m_tc_t^{\mathrm{II}},m_1c_1^{\mathrm{III}},\dots,m_tc_t^{\mathrm{III}})\mid\\ &\mathbf{c}=(\mathbf{c}^{\mathrm{I}},\mathbf{c}^{\mathrm{II}},\mathbf{c}^{\mathrm{III}})\in\mathbf{Z}_M^{s+2t}\}.\end{aligned} \tag{2.20}$$

One can easily verify that $\mathcal{R}[\mathbf{n},\mathbf{m}]$ is the radical of f in $\mathbf{Z}_M^{s+2t}$. Therefore, $\mathcal{R}[\mathbf{n},\mathbf{m}]\subset C'$ for any self-dual code C' over $\mathbf{Z}_M$ relative to f.

The following is one of the main theorems in this paper.

THEOREM 2.5. *The lattice $L(C)$ is integral if and only if C is self-orthogonal relative to f. Moreover, if C is self-dual relative to f, then $L(C)$ is self-dual. Conversely if $C\supset\mathcal{R}[\mathbf{n},\mathbf{m}]$ and $L(C)$ is self-dual, then C is self-dual.*

Proof. The key point is the following formula: for any $\mathbf{c},\mathbf{c}'\in\mathbf{Z}_M^{s+2t}$, by (2.5)–(2.6),

$$\begin{aligned}\langle\Theta_{\mathbf{c}},\Theta_{\mathbf{c}'}\rangle&\equiv\sum_{i=1}^{s}\frac{\eta_M(c_i^{\mathrm{I}})\eta_M({c'}_i^{\mathrm{I}})\beta_i}{n_i}+\sum_{j=1}^{t}\frac{\eta_M(c_j^{\mathrm{II}})\eta_M({c'}_j^{\mathrm{III}})+\eta_M(c_j^{\mathrm{III}})\eta_M({c'}_j^{\mathrm{II}})}{m_j}\\ &\equiv\frac{1}{M}\Big[\sum_{i=1}^{s}\eta_M(c_i^{\mathrm{I}})\eta_M({c'}_i^{\mathrm{II}})\beta_i\varepsilon_i\\ &\qquad+\sum_{j=1}^{t}(\eta_M(c_j^{\mathrm{II}})\eta_M({c'}_j^{\mathrm{III}})+\eta_M(c_j^{\mathrm{III}})\eta_M({c'}_j^{\mathrm{II}}))\gamma_j\Big]\\ &\equiv\frac{1}{M}\eta_M[\mathbf{c}^{\mathrm{I}}B_{\mathbf{d}}{\mathbf{c}'}^{\mathrm{I}^t}+\mathbf{c}^{\mathrm{II}}B_\gamma{\mathbf{c}'}^{\mathrm{III}^t}+{\mathbf{c}'}^{\mathrm{II}}B_\gamma\mathbf{c}^{\mathrm{III}^t}]\\ &\equiv\frac{1}{M}\eta_M(f(\mathbf{c},\mathbf{c}'))\pmod{\mathbf{Z}},\end{aligned} \tag{2.21}$$

where the upper right "t" means "transpose". Therefore,

$$\langle \Theta_{\mathbf{c}}, \Theta_{\mathbf{c}'} \rangle \equiv 0 \pmod{\mathbf{Z}} \iff f(\mathbf{c}, \mathbf{c}') = 0 \text{ in } \mathbf{Z}_M. \tag{2.22}$$

Hence the first statement follows from (2.21). For the second, we already know that $L(\mathcal{C})$ is integral by (2.22). Now let $u \in (L(\mathcal{C}))^{\circ}$. According to (2.2), we can write $u = \Theta_{\mathbf{c}} + v$ for some $\mathbf{c} \in \mathbf{Z}_M^{s+2t}$, $v \in L$. However for any $\mathbf{c}' \in \mathcal{C}$,

$$0 \equiv \langle \Theta_{\mathbf{c}'}, u \rangle \equiv \langle \Theta_{\mathbf{c}'}, \Theta_{\mathbf{c}} \rangle \pmod{\mathbf{Z}}. \tag{2.23}$$

This implies $\mathbf{c} \in \mathcal{C}_f^{\perp} = \mathcal{C}$ by (2.22); so $u \in L(\mathcal{C})$.

Finally we assume that $\mathcal{C} \supset \mathcal{R}[\mathbf{n}, \mathbf{m}]$ and $L(\mathcal{C})$ is self-dual. For any $\mathbf{c} \in \mathcal{C}_f^{\perp}$, we have $\Theta_{\mathbf{c}} \in (L(\mathcal{C}))^{\circ} = L(\mathcal{C})$ by (2.17) and (2.21). Then $\mathbf{c} \in \mathcal{C}$, because

$$\mathcal{C}/\mathcal{R}[\mathbf{n}, \mathbf{m}] \cong L(\mathcal{C})/L. \tag{2.24}$$

□

These two steps constitute the *gluing procedure* of our untwisted gluing technique. Next we give a decomposability theorem of construction in an important, special case.

First we need the following concept.

Definition 2.6. A set $S = \{n_i \mid i \in \Omega(k)\}$ of integers is said to be g.c.d.-connected if for any pair $n_j, n_l \in S$, there exist $n_{i_0}, \ldots, n_{i_\lambda} \in S$ such that $i_0 = j$, $i_\lambda = l$; g.c.d.$\{n_{i_\varepsilon}, n_{i_{\varepsilon+1}}\} \neq 1$, $\varepsilon = 0, 1, \ldots, \lambda - 1$.

Now let $\{(L_l; \langle \cdot, \cdot \rangle_l; x_l) \mid l \in \Omega(s)\}$ be a family of s U-shells of type I and $\langle x_l, x_l \rangle_l \equiv \beta_l / n_l \pmod{\mathbf{Z}}$. As in step 1, we get a new shell $(L; \langle \cdot, \cdot \rangle; x_i; i \in \Omega(s))$. Now all the settings are the same as in step 2 when $t = 0$.

THEOREM 2.7. *Let $\mathcal{C}$ be a self-dual code of length s over $\mathbf{Z}_M$ relative to $(\cdot, \cdot)_{\mathbf{d}}$. If $\{n_i \mid i \in \Omega(s)\}$ is not* g.c.d.*-connected, then $L(\mathcal{C})$ defined in* (2.17) *is decomposable.*

Proof. It is enough to prove that $\mathcal{C}$ is self-dually decomposable. By changing indices if necessary, we assume that

$$\text{g.c.d.}\{n_i, n_j\} = 1, \quad \text{for } i, j \in \Omega(s),\ i \leqslant k < j, \tag{2.25}$$

where k is a fixed integer and $1 \leqslant k < s$. Thus

$$n_i | \varepsilon_j, \ n_j | \varepsilon_i, \quad \text{for } i, j \in \Omega(s),\ i \leqslant k < j. \tag{2.26}$$

For any $\mathbf{c}=(c_1,\dots,c_s)$, $\mathbf{c}'=(c'_1,\dots,c'_s)\in C$, we have

$$0=(\mathbf{c},\mathbf{c}')_{\mathbf{d}}=\sum_{i=1}^{k}c_ic'_i\varepsilon_i\beta_i+\sum_{j=k+1}^{s}c_jc'_j\varepsilon_j\beta_j. \tag{2.27}$$

By the first expression in (2.26),

$$n_l\,\Big|\,\eta_M\Big(\sum_{i=1}^{k}c_ic'_i\varepsilon_i\beta_i\Big),\quad \text{for } l\in\Omega(k),\ 1\leqslant l\leqslant k. \tag{2.28}$$

According to the second expression in (2.26), we get

$$M\,\Big|\,\eta_M\Big(\sum_{i=1}^{k}c_ic'_i\varepsilon_i\beta_i\Big)\quad\Longrightarrow\quad\sum_{i=1}^{k}c_ic'_id_i=0. \tag{2.29}$$

By Proposition 2.1.7 in [24], C is a decomposable code. Therefore $L(C)$ is decomposable. □

COROLLARY 2.8. *If* $k=1$ *in* (2.25) *and* $1<n_1$ *is not square, then there is no self-dual code relative to* f *over* $\mathbf{Z}_M$.

Proof. This follows from Proposition 2.3.6 in [24]. □

3. The twisted gluing technique

This technique is much subtler than the untwisted one. The technique is based on the object that we define as follows.

Definition 3.1. Let L be an integral lattice with associated $\mathbf{Z}$-bilinear form $\langle\cdot,\cdot\rangle$. Suppose that there exist a set $\{x_i;\zeta_j;\xi_j;W;y;i\in\Omega(s),j\in\Omega(t)\}$ of vectors in L° such that:

(1) the family $(L'=\mathbf{Z}y+L;\langle\cdot,\cdot\rangle;x_i;\zeta_j;\xi_j;i\in\Omega(s),j\in\Omega(t))$ is a U-shell;

(2)

$$L^\circ=\mathbf{Z}W+\sum_{i=1}^{s}\mathbf{Z}x_i+\sum_{j=1}^{t}(\mathbf{Z}\zeta_j+\mathbf{Z}\xi_j)+\mathbf{Z}y+L; \tag{3.1}$$

(3)

$$\langle W,y\rangle\equiv\frac{1}{N}\ (\mathrm{mod}\ \mathbf{Z}),\quad 1<N\in\mathbf{Z};\quad Ny\in L. \tag{3.2}$$

Then we call $\tilde{\mathcal{S}}=(L;\langle\cdot,\cdot\rangle;x_i;\zeta_j;\xi_j;W;y;i\in\Omega(s),j\in\Omega(t))$ a *T-shell of self-dual lattices.* The vector W is called a *twist vector*, and the vector y is called a *simple root.* $\tilde{\mathcal{S}}$ is said to be of *type* I, II *and* III, respectively, if $s=0$, $t=0$ and $s=t=0$, respectively. Again, two T-shells are said to be *equivalent* if the underlying lattices are isomorphic.

Remark 3.2. If L satisfies all the above conditions but $Ny\notin L$ in (3), then we can get a T-shell through the replacement of L by $\mathbf{Z}Ny+L$.

We again divide the twisted gluing technique into two steps.

Step 1. *Combining a finite number of twisted shells with a restriction into a larger T-shell.*

Let

$$\{(L_l;\langle\cdot,\cdot\rangle_l;x_{li};\zeta_{lj};\xi_{lj};W_l;y_l;i\in\Omega(s_l),j\in\Omega(t_l))\mid l\in\Omega(k)\}$$

be a family of k twisted shells. Suppose that

$$\langle W_l,y_l\rangle_l\equiv\frac{1}{N_l}\pmod{\mathbf{Z}},\quad\text{for } l\in\Omega(k)\tag{3.3}$$

and there exists $l_0\in\Omega(k)$ such that

$$N_l|N_{l_0},\quad\text{for all } l\in\Omega(k).\tag{3.4}$$

We define L and $\langle\cdot,\cdot\rangle$ as in (2.7). Furthermore, we set

$$\varrho_l=\frac{N_{l_0}}{N_l},\quad L'=L+\sum_{l=1}^{k}\mathbf{Z}(y_l-\varrho_l y_{l_0}),\quad W=\sum_{l=1}^{k}W_l.\tag{3.5}$$

THEOREM 3.3. *The family* $(L';\langle\cdot,\cdot\rangle;x_{li};\zeta_{lj};\xi_{lj};W;y_{l_0};l\in\Omega(k),i\in\Omega(s_l),j\in\Omega(t_l))$ *is a T-shell of self-dual lattices.*

Proof. First of all, we have

$$\langle W,y_l-\varrho_l y_{l_0}\rangle\equiv\frac{1}{N_l}-\frac{\varrho_l}{N_{l_0}}\equiv 0\pmod{\mathbf{Z}},\quad l\in\Omega(k)\tag{3.6}$$

by (3.5). Suppose that $u=\sum_{l=1}^{k}\lambda_l W_l\in L'^{\circ}$ with $0\leqslant\lambda_l<N_l$. Replacing u by $u-\lambda_{l_0}W$, we can assume $\lambda_{l_0}=0$. Then

$$0\equiv\langle u,y_l-\varrho_l y_{l_0}\rangle\equiv\frac{\lambda_l}{N_l}\pmod{\mathbf{Z}},\quad l\in\Omega(k).\tag{3.7}$$

This implies $\lambda_l=0$, $l\in\Omega(k)$. It is easy to check that all other conditions in Definition 3.1 are satisfied. □

Step 2. *Gluing a T-shell into a self-dual lattice.*

The situation now is much more complicated than in the previous section. Let $\tilde{\mathcal{S}}=(L;\langle\cdot,\cdot\rangle;x_i;\zeta_j;\xi_j;W;y;i\in\Omega(s),j\in\Omega(t))$ be a T-shell of self-dual lattices. The data n_i,m_j,N are as in (2.3) and (3.2). We also use the same settings as in (2.10)–(2.16) and (2.18)–(2.19).

Definition 3.4. Let $\mathcal{C}$ be a code of length $s+2t$ over $\mathbf{Z}_M$. A vector $\Upsilon(\mathcal{C})\in\mathbf{Z}_M^{s+2t}$ and a map $\psi_{\mathcal{C}}:\mathcal{C}\rightarrow\mathbf{Z}$ are called the *admissible vector and map of* $\mathcal{C}$, respectively, if

$$\langle W+\Theta_{\Upsilon(\mathcal{C})},\Theta_{\mathbf{c}}+\psi_{\mathcal{C}}(\mathbf{c})y\rangle\in\mathbf{Z},\quad\text{for all }\mathbf{c}\in\mathcal{C}.\tag{3.8}$$

If such $\Upsilon(\mathcal{C})$ and $\psi_{\mathcal{C}}$ exist, then we say that $\mathcal{C}$ is *admissible* to the T-shell $\widetilde{\mathcal{S}}$.

In the case that $\mathcal{C}$ is admissible to $\widetilde{\mathcal{S}}$, let t be an integral variable, and we call

$$J[\widetilde{\mathcal{S}},\mathcal{C};t]=\langle W+\Theta_{\Upsilon(\mathcal{C})}+ty,W+\Theta_{\Upsilon(\mathcal{C})}+ty\rangle\tag{3.9}$$

a *twist factor* of $\mathcal{C}$ with respect to $\widetilde{\mathcal{S}}$. An integer $\tilde{t}(\widetilde{\mathcal{S}},\mathcal{C})$ is called a *twist parameter* of $\mathcal{C}$ with respect to $\widetilde{\mathcal{S}}$ if

$$J[\widetilde{\mathcal{S}},\mathcal{C};\tilde{t}(\widetilde{\mathcal{S}},\mathcal{C})]\in\mathbf{Z}.\tag{3.10}$$

If such a $\tilde{t}(\widetilde{\mathcal{S}},\mathcal{C})$ exists, then we say that $\mathcal{C}$ is *twistable* with respect to $\widetilde{\mathcal{S}}$.

Next we assume that $\mathcal{C}$ is twistable with respect to $\widetilde{\mathcal{S}}$ and the related notations are the same as in the above definition. Set

$$\widetilde{W}=W+\Theta_{\Upsilon(\mathcal{C})}+\tilde{t}(\widetilde{\mathcal{S}},\mathcal{C})y;\quad\widetilde{\Theta}_{\mathbf{c}}=\Theta_{\mathbf{c}}+\psi_{\mathcal{C}}(\mathbf{c})y,\quad\text{for }\mathbf{c}\in\mathcal{C}.\tag{3.11}$$

Now we define

$$\tilde{L}(\mathcal{C})=\mathbf{Z}\widetilde{W}+\sum_{\mathbf{c}\in\mathcal{C}}\mathbf{Z}\widetilde{\Theta}_{\mathbf{c}}+L.\tag{3.12}$$

Here is another main theorem of this paper:

THEOREM 3.5. *If* $\mathcal{C}$ *is self-dual relative to* f *defined in* (2.13), *then* $\tilde{L}(\mathcal{C})$ *is a self-dual lattice.*

Proof. First we notice that for any $\mathbf{c},\mathbf{c}'\in\mathcal{C}$,

$$\langle\widetilde{\Theta}_{\mathbf{c}},\widetilde{\Theta}_{\mathbf{c}'}\rangle\equiv\langle\Theta_{\mathbf{c}},\Theta_{\mathbf{c}'}\rangle\pmod{\mathbf{Z}}.\tag{3.13}$$

Hence $\tilde{L}(\mathcal{C})$ is integral by the above assumptions and (2.21). Now we suppose that $u\in(\tilde{L}(\mathcal{C}))^{\circ}$. We can write $u=\lambda W+v$ with $\lambda\in\mathbf{Z}$, $v\in\sum_{i=1}^{s}\mathbf{Z}x_i+\sum_{j=1}^{t}(\mathbf{Z}\zeta_j+\mathbf{Z}\xi_j)+\mathbf{Z}y+L$. Replacing v by $v-\lambda\widetilde{W}$, we can assume that $\lambda=0$. Furthermore, we write $u=\Theta_{\mathbf{c}}+v'$ with $\mathbf{c}\in\mathbf{Z}_M^{s+2t}$ and $v'\in\mathbf{Z}y+L$. However, for any $\mathbf{c}'\in\mathcal{C}$,

$$0\equiv\langle u,\widetilde{\Theta}_{\mathbf{c}'}\rangle\equiv\langle\Theta_{\mathbf{c}},\Theta_{\mathbf{c}'}\rangle\pmod{\mathbf{Z}}.\tag{3.14}$$

By (2.21) and the self-duality of $\mathcal{C}$, $\mathbf{c}\in\mathcal{C}$. Replacing u by $u-\widetilde{\Theta}_{\mathbf{c}}$, we can assume $\mathbf{c}=0$. Therefore, we can write $u=\mu y+v''$ with $v''\in L$ and $\mu\in\mathbf{Z}$, $0\leqslant\mu<N$. Finally by (3.2),

$$0\equiv\langle\widetilde{W},u\rangle\equiv\frac{\mu}{N}\pmod{\mathbf{Z}}.\tag{3.15}$$

This implies $\mu=0$. That is, $\tilde{L}(\mathcal{C})$ is self-dual. □

Remark 3.6. Unfortunately we have not proved the converse theorem to the above in a general case. Later the reader will see that Theorem 3.5 does have a nice converse theorem in certain cases.

4. Untwisted type-A lattices

Let n be a positive integer. Set

$$R_n^A = \mathbf{Z}[x]/(x^{n-1}+...+x+1). \tag{4.1}$$

Denote the image of x in R_n^A by $\omega_{n,A}$.

Definition 4.1. An *R_n^A-complex lattice* L is a lattice such that

(1) L is an R_n^A-module which can be embedded into a free R_n^A-module L' of finite rank such that $NL' \subset L$ for some $N \in \mathbf{Z}\backslash\{0\}$;

(2) the associated symmetric form $\langle \cdot , \cdot \rangle$ satisfies

$$\langle \omega_{n,A}\alpha, \omega_{n,A}\beta\rangle = \langle \alpha, \beta\rangle \quad \text{for all } \alpha, \beta \in L. \tag{4.2}$$

A lattice L is called a *type-A* lattice if L contains a sublattice L_0 such that $L_{\mathbf{Q}} = (L_0)_{\mathbf{Q}}$, and as a lattice, $L_0 = \bigoplus_{j=1}^s L_0^j$, where each L_0^j is an $R_{n_j}^A$-complex lattice.

PROPOSITION 4.2. *An integer l is divisible by $1-\omega_{n,A}$ in $\mathbf{R}_n^A$ if and only if $l \equiv 0$ (mod n). Moreover,*

$$n = (1-\omega_{n,A})[(n-1)+(n-2)\omega_{n,A}+(n-3)\omega_{n,A}^2+...+\omega_{n,A}^{n-2}]. \tag{4.3}$$

Proof. Any $a \in \mathbf{R}_n^A$ can be uniquely written as

$$a = \sum_{i=0}^{n-2} \lambda_i \omega_{n,A}^i, \quad \lambda_i \in \mathbf{Z}. \tag{4.4}$$

Moreover,

$$(1-\omega_{n,A})a = \lambda_0 + \lambda_{n-2} + \sum_{i=1}^{n-2}(\lambda_i - \lambda_{i-1} + \lambda_{n-2})\omega_{n,A}^i. \tag{4.5}$$

Hence

$$l = (1-\omega_{n,A})a \iff l = \lambda_0 + \lambda_{n-2}, \ \ \lambda_i - \lambda_{i-1} + \lambda_{n-2} = 0, \tag{4.6}$$

where $1 \leqslant i \leqslant n-2$. In particular, $\lambda_{n-3} = 2\lambda_{n-2}$. By induction on i, we get that $\lambda_i = (n-i-1)\lambda_{n-2}$. Therefore, $\lambda_0 = (n-1)\lambda_{n-2}$. This implies that $l = n\lambda_{n-2}$. When $l = n$, we let $\lambda_{n-2} = 1$ and reverse the above process so that we get (4.3). □

We set

$$\mathbf{Q}_n^A = \mathbf{Q} \otimes_{\mathbf{Z}} R_n^A. \tag{4.7}$$

Then $\mathbf{Q}_n^A$ is a $\mathbf{Q}$-linear space of dimension $n-1$. Moreover, we define the $\mathbf{Q}$-linear map $\varphi_A : \mathbf{Q}_n^A \to \mathbf{Q}$ by

$$\varphi_A(1) = \frac{n-1}{n}, \quad \varphi_A(\omega_{n,A}^j) = -\frac{1}{n}, \quad \text{for } j \not\equiv 0 \pmod{n}. \tag{4.8}$$

Furthermore, we let $\nu_{n,A}$ be the automorphism of the multiplication by $\omega_{n,A}$ on $\mathbf{Q}_n^A$. Now we define the $\nu_{n,A}$-invariant symmetric $\mathbf{Q}$-bilinear form $\langle \cdot , \cdot \rangle_{n,A}$ on $\mathbf{Q}_n^A$ by

$$\langle a, b\rangle_{n,A} = \varphi_A(a\bar{b}), \quad \text{for } a, b \in \mathbf{Q}_n^A, \tag{4.9}$$

where $\bar{b} = \sum_{j\in\mathbf{Z}_n} \lambda_j \omega_{n,A}^{-j}$ if $b = \sum_{j\in\mathbf{Z}_n} \lambda_j \omega_{n,A}^j$, $\lambda_j \in \mathbf{Q}$. Set

$$y_{n,A} = 1 - \omega_{n,A}, \quad y_{n,A}^i = \omega_{n,A}^i y_{n,A}, \quad \text{for } i \in \mathbf{Z}_n. \tag{4.10}$$

and

$$Q_{n,A} = R_n^A y_{n,A}. \tag{4.11}$$

LEMMA 4.3. *The lattice $Q_{n,A}$ is the root lattice of the simple Lie algebra* of type A_{n-1}.

Proof. For any $i, j \in \mathbf{Z}_n$,

$$\begin{aligned} \langle y_{n,A}^i, y_{n,A}^j\rangle_{n,A} &= \langle \omega_{n,A}^i(1-\omega_{n,A}), \omega_{n,A}^j(1-\omega_{n,A})\rangle_{n,A} \\ &= \varphi_A[\omega_{n,A}^i(1-\omega_{n,A})\cdot\omega_{n,A}^{-j}(1-\omega_{n,A}^{-1})] \\ &= \varphi_A(2\omega_{n,A}^{i-j} - \omega_{n,A}^{i-j-1} - \omega_{n,A}^{i-j+1}) \\ &= \begin{cases} 2(n-1)/n - (-1/n) - (-1/n) = 2, & \text{if } i-j \equiv 0, \\ 2(-1/n) - (-1/n) - (n-1)/n = -1, & \text{if } i-j \equiv \pm 1, \\ 2(-1/n) - (-1/n) - (-1/n) = 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{4.12}$$

Therefore, $\{y_{n,A}^i \mid i = 0, 1, \ldots, n-2\}$ constitute a set of the simple roots of the simple Lie algebra of type A_{n-1}. □

Notice that $\nu_{n,A}$ is the Coxeter element of the Weyl group of A_{n-1}.

LEMMA 4.4. *For $i \in \mathbf{Z}_n$,*

$$\langle 1, y_{n,A}^i\rangle_{n,A} = \begin{cases} 1, & \textit{if } i \equiv 0, \\ -1, & \textit{if } i \equiv -1, \\ 0, & \textit{otherwise.} \end{cases} \tag{4.13}$$

Proof.

$$\begin{aligned}\langle 1, y^i_{n,A}\rangle_{n,A} &= \langle 1, \omega^i_{n,A}(1-\omega_{n,A})\rangle_{n,A}\\ &= \varphi_A(\omega^{-i}_{n,A}-\omega^{-i-1}_{n,A})\\ &= \begin{cases} 1, & \text{if } i\equiv 0,\\ -1, & \text{if } i\equiv -1,\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

□

THEOREM 4.5. *The family* $\mathcal{S}_{n,A}=(Q_{n,A};\langle\cdot,\cdot\rangle_{n,A};1)$ *is a U-shell of type* I.

Proof. We first notice that for any $u=\sum_{i=0}^{n-2}\mu_i\omega^i_{n,A}\in(Q_{n,A})^\circ$,

$$0\equiv\langle u, y^{n-2}_{n,A}\rangle_{n,A}\equiv\mu_{n-2},\quad 0\equiv\langle u, y^i_{n,A}\rangle_{n,A}\equiv-\mu_{i+1}+\mu_i \pmod{\mathbf{Z}},\tag{4.14}$$

for $i=0,1,...,n-3$. By induction on i, we have $\mu_i\in\mathbf{Z}$. That is, $u\in R^A_n$. So $(Q_{n,A})^\circ=R^A_n$ by Lemmas 4.3 and 4.4. By Proposition 4.2, $R^A_n/Q_{n,A}=\langle 1+Q^A_n\rangle$ is of order n. Moreover,

$$\langle 1,1\rangle_{n,A}=\frac{n-1}{n}.\tag{4.15}$$

□

We call $\mathcal{S}_{n,A}$ the *U-shell of type* A_{n-1}.

Now let $n_1,...,n_k$ be k integers greater than 1. Set

$$L_j=R^A_{n_j},\quad Q_{A,j}=Q_{n_j,A},\quad \langle\cdot,\cdot\rangle_j=\langle\cdot,\cdot\rangle_{n_j,A}\ \text{ on } L_j;\quad x_{A,j}=1\ \text{ in } L_j,\tag{4.16}$$

for $j\in\Omega(k)$. Define $L=\bigoplus_{j=1}^k L_j$, $\langle\cdot,\cdot\rangle_A=\bigoplus_{j=1}^k\langle\cdot,\cdot\rangle_j$ as in (2.7) and let $Q_{\mathbf{n},A}=\bigoplus_{j=1}^k Q_{A,j}$ where $\mathbf{n}=(n_1,...,n_k)$. Set

$$M=\text{l.c.m.}\{n_j\mid j\in\Omega(k)\},\quad \varepsilon_j=\frac{M}{n_j},\quad \mathbf{d}=(\varepsilon_1,...,\varepsilon_k).\tag{4.17}$$

For $\mathbf{c}=(c_1,...,c_k)\in\mathbf{Z}^k_M$, define

$$x_{A,\mathbf{c}}=\sum_{j=1}^k\eta_M(c_j)x_{A,j}.\tag{4.18}$$

Let C be a code of length k over $\mathbf{Z}_M$. We define

$$L_A[\mathbf{n},C]=\sum_{\mathbf{c}\in C}\mathbf{Z}x_{A,\mathbf{c}}+Q_{\mathbf{n},A}.\tag{4.19}$$

Like (2.19), set

$$\mathcal{R}[\mathbf{n}]=\{(c_1n_1,...,c_kn_k)\mid c_j\in\mathbf{Z}_M\}.\tag{4.20}$$

Then by Theorem 2.5, we have:

10-950414 *Acta Mathematica* 175. Imprimé le 1 septembre 1995

THEOREM 4.6. *The lattice* $L_A[\mathbf{n},\mathcal{C}]$ *is integral if and only if* $\mathcal{C}$ *is self-orthogonal relative to* $\mathbf{d}$. *Moreover, if* $\mathcal{C}$ *is self-dual relative to* $\mathbf{d}$, *then* $L_A[\mathbf{n},\mathcal{C}]$ *is a self-dual lattice. Conversely, if* $\mathcal{C}\supset\mathcal{R}[\mathbf{n}]$ *and* $L_A[\mathbf{n},\mathcal{C}]$ *is a self-dual lattice, then* $\mathcal{C}$ *is a self-dual lattice relative to* $\mathbf{d}$. □

Remark 4.7. For any $\mathbf{c},\mathbf{c}'\in\mathbf{Z}_M^k$,

$$\langle x_{A,\mathbf{c}},x_{A,\mathbf{c}'}\rangle_A=\sum_{j=1}^{k}\frac{n_j-1}{M}\varepsilon_j\eta_M(c_j)\eta_M(c_j'). \tag{4.21}$$

Therefore, $L_A[\mathbf{n},\mathcal{C}]$ is even if M is odd and $\mathcal{C}$ is self-orthogogal relative to $\mathbf{d}$. When M is even and $\mathcal{C}$ is self-orthogonal relative to $\mathbf{d}$, then $L_A[\mathbf{n},\mathcal{C}]$ is even if and only if

$$\sum_{j=1}^{k}(n_j-1)\varepsilon_j\eta_M(c_j)\eta_M(c_j)\equiv 0 \pmod{2M} \tag{4.22}$$

for any $\mathbf{c}\in\mathcal{C}$. By Proposition 4.2 and Lemma 4.3, this condition is equivalent to that the generators of $\mathcal{C}$ satisfy (4.22). An example of such codes is a doubly-even self-dual code when all n_j are equal to 2.

If all the n_j above are equal to n, we denote $L_A[\mathbf{n},\mathcal{C}]$ by $L_{n,A}[\mathcal{C}]$. Notice that $L_{n,A}[\mathcal{C}]$ is a type-A complex lattice. Set

$$Q_{E_8}=L_{3,A}[\mathcal{C}_3^4],\quad Q_{E_6}=L_{3,A}[\mathbf{Z}\mathbf{1}_3], \tag{4.23}$$

where $\mathcal{C}_3^4$ is a ternary code generated by the rows of the matrix:

$$\begin{pmatrix}1&1&1&\\&1&-1&1\end{pmatrix}. \tag{4.24}$$

Then Q_{E_8} and Q_{E_6} are the root lattices of the simple Lie algebras of types E_8 and E_6, respectively. One can find the equivalent definition of Q_{E_8} in [29]. So far, we did not find the above construction of Q_{E_6} in the literatures.

Remark 4.8. In [24], we present the induced U-shells by means of untwisted type-A lattices. We also present the U-shells of type D.

5. Twisted type-A lattices

Let n be a positive integer. All the related settings are the same as in the last section. Set

$$W_{n,A}=\frac{\omega_{n,A}}{1-\omega_{n,A}}, \tag{5.1}$$

where $1-\omega_{n,A}$ is invertible in $\mathbf{Q}_n^A$ by Proposition 4.2. Then we have the following important properties.

LEMMA 5.1. *$W_{n,A} \in \mathbf{Q}_n^A$ and*

$$\langle W_{n,A}, W_{n,A}\rangle_{n,A} = \frac{n^2-1}{12n}, \quad \langle W_{n,A}, y^j_{n,A}\rangle_{n,A} = \begin{cases} -(n-1)/n, & \text{if } j \equiv 0, \\ 1/n, & \text{otherwise.} \end{cases} \tag{5.2}$$

Proof. By (4.3),

$$W_{n,A} = \frac{1}{n}\sum_{j=1}^{n-1}(n-j)\omega^j_{n,A} \in \mathbf{Q}_n^A. \tag{5.3}$$

According to (4.15),

$$\begin{aligned} \langle \omega^s_{n,A}, W_{n,A}\rangle_{n,A} &= \left\langle \omega^s_{n,A}, \frac{1}{n}\sum_{j=1}^{n-1}(n-j)\omega^j_{n,A}\right\rangle_{n,A} \\ &= \frac{n(n-s)-\sum_{j=1}^{n-1}(n-j)}{n^2} \\ &= \frac{n(n-s)-\frac{1}{2}n(n-1)}{n^2} \\ &= \frac{n+1-2s}{2n}, \end{aligned} \tag{5.4}$$

where $1 \leqslant s \leqslant n-1$. Furthermore,

$$\begin{aligned} \langle W_{n,A}, W_{n,A}\rangle_{n,A} &= \left\langle \frac{1}{n}\sum_{s=1}^{n-1}(n-s)\omega^s_{n,A}, W_{n,A}\right\rangle_{n,A} \\ &= \frac{1}{2n^2}\sum_{s=1}^{n-1}(n-s)(n+1-2s) \\ &= \frac{1}{2n^2}\sum_{s=1}^{n-1}[n(n+1)-(3n+1)s+2s^2] \\ &= \frac{n(n-1)(n+1)-\frac{1}{2}n(n-1)(3n+1)+2\cdot\frac{1}{6}(n-1)n(2n-1)}{2n^2} \\ &= \frac{(n-1)[6(n+1)-3(3n+1)+2(2n-1)]}{12n} \\ &= \frac{n^2-1}{12n}. \end{aligned}$$

By (4.13) and (5.3), we have

$$\begin{aligned} \langle W_{n,A}, y^j_{n,A}\rangle_{n,A} &= \left\langle \frac{1}{n}\sum_{s=1}^{n-1}(n-s)\omega^s_{n,A}, y^j_{n,A}\right\rangle_{n,A} \\ &= \sum_{s=1}^{n-1}\frac{(n-s)}{n}\langle 1, y^{j-s}_{n,A}\rangle_{n,A} \\ &= \begin{cases} -(n-1)/n, & \text{if } j \equiv 0, \\ 1/n, & \text{otherwise.} \end{cases} \end{aligned}$$

□

Any $y \in Q_{n,A}$ can be uniquely written as $y = \sum_{i=0}^{n-2} \lambda_i y_{n,A}^i$ with $\lambda_i \in \mathbf{Z}$. We define

$$T(y) = \sum_{i=0}^{n-2} \lambda_i. \tag{5.5}$$

LEMMA 5.2. *For any* $y \in Q_{n,A}$,

$$T(\omega_{n,A} y) \equiv T(y) \pmod{n}. \tag{5.6}$$

Proof. Assume $y = \sum_{i=1}^{n-2} \lambda_i y_{n,A}^i$. Then

$$\omega_{n,A} y = \sum_{i=0}^{n-3} \lambda_i \omega_{n,A}^{i+1} y_{n,A} - \lambda_{n-2} \left(\sum_{i=0}^{n-2} \omega_{n,A}^i \right) y_{n,A} = \sum_{i=0}^{n-3} \lambda_i y_{n,A}^{i+1} - \sum_{i=0}^{n-2} \lambda_{n-2} y_{n,A}^i.$$

Hence $T(\omega_{n,A} y) = T(y) - n\lambda_{n-2}$. □

Set

$$\tilde{Q}_{n,A} = \{ y \in Q_{n,A} \mid T(y) \equiv 0 \pmod{n} \}. \tag{5.7}$$

Then by the lemma above, $\tilde{Q}_{n,A}$ is an $\mathbf{R}_n^A$-module. By (4.3), $\tilde{Q}_{n,A} = R_n^A \tilde{y}_{n,A}$ is a free R_n^A-module of rank 1, where $\tilde{y}_{n,A} = (1-\omega_{n,A}) y_{n,A}$.

THEOREM 5.3. *The family* $\tilde{S}_{n,A} = (\tilde{Q}_{n,A}; \langle \cdot, \cdot \rangle_{n,A}; 1; W_{n,A}; y_{n,A})$ *is a T-shell of type* I.

Proof. (1) and (3) in Definition 3.1 are satisfied by Theorem 4.4 and (5.2), (5.7). Any $u \in (\tilde{Q}_{n,A})^\circ$ can be uniquely written as $u = \sum_{i=1}^{n-1} \mu_i \omega_{n,A}^i$. By the fact that $n y_{n,A}^i \in \tilde{Q}_{n,A}$,

$$\langle u, n y_{n,A}^i \rangle_{n,A} = -n\mu_{n-1} \in \mathbf{Z}. \tag{5.8}$$

Since $(1-\omega_{n,A}^{-1}) y_{n,A}^i = y_{n,A}^i - y_{n,A}^{i-1} \in \tilde{Q}_{n,A}$, we have

$$\begin{aligned} 0 &\equiv \langle u, (1-\omega_{n,A}^{-1}) y_{n,A}^i \rangle_{n,A} \\ &\equiv \langle (1-\omega_{n,A}) u, y_{n,A}^i \rangle_{n,A} \\ &\equiv \sum_{j=1}^{n-1} \mu_j \langle y_{n,A}^j, y_{n,A}^i \rangle_{n,A} \\ &\equiv 2\mu_i - \mu_{i-1} - \mu_{i+1} \pmod{\mathbf{Z}}, \end{aligned} \tag{5.9}$$

for $1 < i < n-1$. Similarly,

$$0 \equiv \langle u, (1-\omega_{n,A}^{-1}) y_{n,A}^{n-1} \rangle_{n,A} \equiv 2\mu_{n-1} - \mu_{n-2} \pmod{\mathbf{Z}}. \tag{5.10}$$

Therefore, $\mu_{n-2} \equiv 2\mu_{n-1}$ (mod $\mathbf{Z}$). By (5.9) and the induction on i, we can prove that $\mu_{n-i} \equiv i\mu_{n-1}$ (mod $\mathbf{Z}$). We can assume $\mu_{n-1} \equiv \mu/n$ (mod $\mathbf{Z}$), $\mu \in \mathbf{Z}$ by (5.8). Thus $u = \mu W_{n,A} + v$, $v \in R_n^A$. This proves (2) in Definition 3.1. ☐

We call $\widetilde{S}_{n,A}$ the *T-shell of type* A_{n-1}.

Let $n_1, \dots, n_k$ be k integers greater than 1 and assume

$$n_j | n_1, \quad j \in \Omega(k). \tag{5.11}$$

We use the same settings as in (4.16)–(4.18). Set

$$\widetilde{S}_{\mathbf{n},A} = \{(\widetilde{Q}_{n_j,A}; \langle \cdot , \cdot \rangle_{n_j,A}; 1; W_{n_j,A}; y_{n_j,A}) \mid j \in \Omega(k)\}. \tag{5.12}$$

PROPOSITION 5.4. *When n_1 is odd, any code of length k over $\mathbf{Z}_{n_1}$ is admissible with respect to $\widetilde{S}_{\mathbf{n},A}$. If n_1 is even, a length-k code C is admissible with respect to $\widetilde{S}_{\mathbf{n},A}$ if and only if*

$$\sum_{j=1}^{k} \varepsilon_j \eta_{n_1}(c_j) \text{ is even for all } \mathbf{c} = (c_1, \dots, c_k) \in C. \tag{5.13}$$

In particular, if C is self-orthogonal relative to $\mathbf{d}$, *then C is admissible.*

Proof. Set

$$W_{\mathbf{n},A} = \bigoplus_{j=1}^{k} W_{n_j,A}. \tag{5.14}$$

Notice that

$$\begin{aligned} \langle x_j, W_{\mathbf{n},A} \rangle_A = \langle 1, W_{n_j,A} \rangle_A &= \left\langle 1, \frac{1}{n_j} \sum_{i=1}^{n_j-1} (n_j - i)\omega_{n_j,A}^i \right\rangle_A \\ &= -\sum_{i=1}^{n_j-1} \frac{n_j - i}{n_j^2} = -\frac{1}{n_j^2}\left(\frac{n_j(n_j-1)}{2}\right) = \frac{1-n_j}{2n_j}. \end{aligned} \tag{5.15}$$

Let $\Upsilon \in \mathbf{Z}_{n_1}^k$ be any given vector and t be an integral indeterminate. For any $\mathbf{c} \in \mathbf{Z}_{n_1}^k$, consider the equation

$$\begin{aligned} \langle W_{\mathbf{n},A} + x_{A,\Upsilon}, x_{A,\mathbf{c}} + t y_{A,1} \rangle_A &\equiv \sum_{j=1}^{k} \eta_{n_1}(c_j) \langle W_{\mathbf{n},A}, x_j \rangle_A \\ &\qquad + \langle x_{A,\Upsilon}, x_{\mathbf{c}} \rangle_A + t \langle W_{\mathbf{n},A}, y_{A,1} \rangle_A \\ &\equiv \sum_{j=1}^{k} \frac{1-n_j}{2n_j} \eta_{n_1}(c_j) + \frac{t - \eta_{n_1}(\Upsilon, \mathbf{c})_{\mathbf{d}}}{n_1} \\ &\equiv \frac{2(t - \eta_{n_1}(\Upsilon, \mathbf{c})_{\mathbf{d}}) + \sum_{j=1}^{k} (\varepsilon_j - n_1)\eta_{n_1}(c_j)}{2n_1} \\ &\equiv 0 \pmod{\mathbf{Z}}. \end{aligned} \tag{5.16}$$

If n_1 is odd, then all ε_j are odd. Hence $\varepsilon_j - n_1$ is even for each $j \in \Omega(k)$. Set

$$\psi_{A,\Upsilon}(\mathbf{c}) = \eta_{n_1}(\Upsilon, \mathbf{c})_{\mathbf{d}} + \frac{1}{2}\sum_{j=1}^{k}(\varepsilon_j - n_1)\eta_{n_1}(c_j). \tag{5.17}$$

So $t = \psi_{A,\Upsilon}(\mathbf{c})$ is a solution of (5.16). If n_1 is even, then (5.16) has a solution if and only if

$$\sum_{j=1}^{k}(\varepsilon_j - n_1)\eta_{n_1}(c_j) \equiv 0 \pmod 2 \iff \sum_{j=1}^{k}\varepsilon_j\eta_{n_1}(c_j) \equiv 0 \pmod 2. \tag{5.18}$$

If (5.18) is satisfied, $t = \psi_{A,\Upsilon}(\mathbf{c})$ is again a solution. Since $\varepsilon_j(\eta_{n_1}(c_j))^2$ and $\varepsilon_j\eta_{n_1}(c_j)$ must be even or odd simultaneously and $\eta_{n_1}(c_j^2) \equiv (\eta_{n_1}(c_j))^2 \pmod{n_1}$, equation (5.18) is satisfied if $(\mathbf{c}, \mathbf{c})_{\mathbf{d}} = 0$. For any length-$k$ code $\mathcal{C}$ satisfying (5.13) over $\mathbf{Z}_{n_1}$, then Υ and $\psi_{A,\Upsilon}$ are the related admissible vector and map, respectively. When $\mathcal{C}$ is self-orthogonal relative to $\mathbf{d}$, $\mathcal{C}$ must satisfy (5.13). The proof is completed. □

Remark 5.5. Notice that $\Upsilon, \psi_{A,\Upsilon}$ above are independent of any specific code, and Υ can be chosen arbitrarily.

Now the assumptions and settings are the same as in Proposition 5.4 and its proof. For a given $\Upsilon = (\sigma_1, \ldots, \sigma_k) \in \mathbf{Z}_{n_1}^k$, we have

$$\begin{aligned}
&\langle W_{\mathbf{n},A} + x_{A,\Upsilon} + ty_{A,1}, W_{\mathbf{n},A} + x_{A,\Upsilon} + ty_{A,1}\rangle_A \\
&\quad \equiv \sum_{j=1}^{k}\frac{n_j^2 - 1}{12n_j} + 2\sum_{j=1}^{k}\eta_{n_1}(\sigma_j)\left(\frac{1-n_j}{2n_j}\right) + \sum_{j=1}^{k}(\eta_{n_1}(\sigma_j))^2\left(\frac{n_j - 1}{n_j}\right) + \frac{2t}{n_1} \\
&\quad \equiv \frac{\sum_{j=1}^{k}\varepsilon_j(n_j^2-1) + 24\left[t + \sum_{j=1}^{k}\frac{1}{2}\varepsilon_j\eta_{n_1}(\sigma_j)(1-\eta_{n_1}(\sigma_j))\right]}{12n_1} \pmod{2\mathbf{Z}}
\end{aligned} \tag{5.19}$$

by (5.2) and (5.15).

Definition 5.6. We call

$$J_A[\mathbf{n}, \Upsilon; t] = \frac{\sum_{j=1}^{k}\varepsilon_j(n_j^2-1) + 24\left[t + \sum_{j=1}^{k}\frac{1}{2}\varepsilon_j\eta_{n_1}(\sigma_j)(1-\eta_{n_1}(\sigma_j))\right]}{12n_1} \tag{5.20}$$

a *twist factor of type A*. An integer $\tilde{t}_A(\mathbf{n}, \Upsilon)$ is called a *twist parameter of type A* if $J_A[\mathbf{n}, \Upsilon; \tilde{t}_A(\mathbf{n}, \Upsilon)] \in \mathbf{Z}$. If $\Upsilon = \mathbf{0}_k$, we drop Υ in the above notations. If all n_j are equal to n, we denote $J_A[\mathbf{n}; t]$ *by* $J_A[n, k; t]$ and $\tilde{t}_A(\mathbf{n})$ by $\tilde{t}_A(n, k)$. We call them the *basic homogeneous twist factor* and *parameter of type-A self-dual complex lattices*, respectively.

Remark 5.7. Notice that

$$\tilde{t}_A(\mathbf{n}, \Upsilon) = \tilde{t}_A(\mathbf{n}) - \sum_{j=1}^{k}\tfrac{1}{2}\varepsilon_j\eta_{n_1}(\sigma_j)(1-\eta_{n_1}(\sigma_j)). \tag{5.21}$$

Set

$$\widetilde{Q}_{A,j}=\widetilde{Q}_{n_j,A}, \quad \text{for } j\in\Omega(k); \quad \widetilde{Q}_{\mathbf{n},A}=\bigoplus_{j=1}^{k}\widetilde{Q}_{A,j}+\sum_{j=1}^{k}\mathbf{Z}(y_{A,j}-\varepsilon_j y_{A,1}). \tag{5.22}$$

Furthermore, for any $\mathbf{c}\in\mathbf{Z}_{n_1}^k$, we let

$$\tilde{x}_{A,\mathbf{c}}=x_{\mathbf{c}}+\psi_{A,\Upsilon}(\mathbf{c})y_{A,1}. \tag{5.23}$$

Suppose that $\tilde{t}_A(\mathbf{n},\Upsilon)$ is a twist parameter. Set

$$\widetilde{W}_A=W_{\mathbf{n},A}+x_{A,\Upsilon}+\tilde{t}_A(\mathbf{n},\Upsilon)y_{A,1}. \tag{5.24}$$

Let $\mathcal{C}$ be a code of length k over $\mathbf{Z}_{n_1}$. Set

$$\tilde{L}_A[\mathbf{n},\mathcal{C}]=\mathbf{Z}\widetilde{W}_A+\sum_{\mathbf{c}\in\mathcal{C}}\mathbf{Z}\tilde{x}_{A,\mathbf{c}}+\widetilde{Q}_{\mathbf{n},A}. \tag{5.25}$$

Then we have

THEOREM 5.8. *The lattice $\tilde{L}_A[\mathbf{n},\mathcal{C}]$ is integral if and only if $\mathcal{C}$ is self-orthogonal relative to $\mathbf{d}$. If $\mathcal{C}$ is self-dual relative to $\mathbf{d}$, then $\tilde{L}_A[\mathbf{n},\mathcal{C}]$ is self-dual. Conversely, $\mathcal{C}$ is self-dual if the following conditions are satisfied:*

(1) $\mathcal{C}\supset\mathcal{R}[\mathbf{n}]$ (*cf.* (4.20));

(2) *when n_1 is even, $\mathcal{C}_{\mathbf{d}}^{\perp}$ satisfies* (5.13) *and* $\mathcal{C}\ni(\frac{1}{2}n_1,\dots,\frac{1}{2}n_1)$;

(3) *$\tilde{L}_A[\mathbf{n},\mathcal{C}]$ is self-dual.*

Proof. The first and second statements follow from Theorem 3.5, expressions (4.13), (4.21), and the proof of Proposition 5.4. It remains to prove the third statement. Suppose that $\mathbf{c}\in\mathcal{C}_{\mathbf{d}}^{\perp}$. Then $\tilde{x}_{A,\mathbf{c}}\in(\tilde{L}_A[\mathbf{n},\mathcal{C}])^{\perp}=\tilde{L}_A[\mathbf{n},\mathcal{C}]$. Now

$$\begin{aligned} n_1\widetilde{W}_A &\equiv \sum_{j=1}^{k}\sum_{i=1}^{n_j-1}\varepsilon_j(n_j-i)\omega_{n_j,A}^{i}x_j \equiv \sum_{j=1}^{k}\varepsilon_j\sum_{i=1}^{n_j-1}(n_j-i)x_j \\ &\equiv \sum_{j=1}^{k}\varepsilon_j\cdot\tfrac{1}{2}n_j(n_j-1)x_j \equiv \begin{cases} 0 \pmod{Q_{\mathbf{n},A}}, & \text{if } n \text{ is odd,} \\ x_{A,(n_1/2)_k} \pmod{Q_{\mathbf{n},A}}, & \text{if } n \text{ is even,} \end{cases} \end{aligned} \tag{5.26}$$

by (5.3). Now the conclusion follows from:

$$[(\tilde{L}_A[\mathbf{n},\mathcal{C}]\cap L)+Q_{\mathbf{n},A}]/Q_{\mathbf{n},A}\cong\mathcal{C}/\mathcal{R}[\mathbf{n}], \tag{5.27}$$

where $L=\bigoplus_{j=1}^{k}R_{n_j}^{A}$. □

When all n_j are equal to n, we denote $\tilde{L}_A[\mathbf{n},\mathcal{C}]$ by $\tilde{L}_{n,A}[\mathcal{C}]$.

THEOREM 5.9. *Let $\mathcal{C}$ be a self-orthogonal code of length k over $\mathbf{Z}_n$. Assume that $\mathcal{C}\supset\mathcal{R}[(n,\dots,n)]$ and $\mathcal{C}\ni\left(\frac{1}{2}n,\dots,\frac{1}{2}n\right)$ if n is even. The lattice $\tilde{L}_{n,A}[\mathcal{C}]$ is a type-A complex lattice if and only if $\mathbf{1}_k\in\mathcal{C}$ and $k\equiv 0 \pmod{2n}$ when n is even.*

Proof. If $\tilde{L}_{n,A}[\mathcal{C}]$ is complex, then

$$\begin{aligned} x_{A,\mathbf{1}_k}+\omega_{n,A}^{-1}\sum_{j=1}^{k}\eta_n(\sigma_j)y_{A,j}=\omega_{n,A}^{-1}[(1-\omega_{n,A})\widetilde{W}_A-\tilde{t}_A(n,k)(1-\omega_{n,A})y_{A,1}]\\ \in\tilde{L}_{n,A}[\mathcal{C}].\end{aligned}\tag{5.28}$$

By (5.27), $\mathbf{1}_k\in\mathcal{C}$. Furthermore, we notice that $\psi_{A,\Upsilon}(\mathbf{1})=\sum_{j=1}^{k}\eta_n(\sigma_j)+\left(\frac{1}{2}k(1-n)\right)$. Thus (5.28) implies $\frac{1}{2}k(1-n)\equiv 0 \pmod{n}$. Hence if n is even, then $k\equiv 0 \pmod{2n}$.

Conversely, if $\mathbf{1}_k\in\mathcal{C}$ and $k\equiv 0 \pmod{2n}$ when n is even, then $\frac{1}{2}k(1-n)\equiv 0 \pmod{n}$, because $k\equiv\eta_n(\mathbf{1}_k,\mathbf{1}_k)\equiv 0 \pmod{n}$ when n is odd. Therefore,

$$\begin{aligned}\omega_{n,A}x_{A,\mathbf{1}_k}+\sum_{j=1}^{k}\eta_n(\sigma_j)y_{A,j}=-\sum_{j=1}^{k}y_{A,j}+x_{A,\mathbf{1}_k}+\left(\sum_{j=1}^{k}\eta_n(\sigma_j)\right)y_{A,1}\\ +\sum_{j=1}^{k}\eta_n(\sigma_j)(y_{A,j}-y_{A,1})=\tilde{x}_{A,\mathbf{1}_k}+v,\end{aligned}\tag{5.29}$$

where $v\in\widetilde{Q}_{\mathbf{n},A}$. Hence $\omega_{n,A}\widetilde{W}_A\in\tilde{L}_A[\mathbf{n},\mathcal{C}]$ by (5.28). We have $\sum_{j=1}^{k}\eta_n(c_j)\equiv 0 \pmod{n}$ for each $\mathbf{c}\in\mathcal{C}$, since $0=(\mathbf{c},\mathbf{1}_k)_1=\sum_{j=1}^{k}c_j$ in $\mathbf{Z}_n$. Thus

$$\omega_{n,A}\tilde{x}_{A,\mathbf{c}}=\tilde{x}_{A,\mathbf{c}}-\sum_{j=1}^{k}\eta_n(c_j)y_{A,j}-\psi_{A,\Upsilon}(\mathbf{c})(1-\omega_{n,A})y_{A,1}\in\tilde{L}_A[\mathbf{n},\mathcal{C}].\tag{5.30}$$

Now the conclusion follows from the fact that $\widetilde{Q}_{\mathbf{n},A}$ is a complex lattice by Lemma 5.2 and (5.22). □

Remark 5.10. If n is even, then $\left(\frac{1}{2}n,\dots,\frac{1}{2}n\right)\in\mathcal{C}$ for any self-dual code $\mathcal{C}$ over $\mathbf{Z}_n$.

We have constructed the untwisted self-dual type-A complex lattice $L_{n,A}[\mathcal{C}]$ for each self-dual code $\mathcal{C}$ over $\mathbf{Z}_n$, and the twisted self-dual type-A complex lattice $\tilde{L}_{n,A}[\mathcal{C}]$ for each self-dual code $\mathcal{C}\ni\mathbf{1}$ over $\mathbf{Z}_n$. Next we show that these lattices are "self-dual complex lattices".

First, we notice $L_{\mathbf{Q}}=\bigoplus_{j=1}^{k}\mathbf{Q}_{n,A}\cong\mathbf{Q}_{n,A}^{k}$. We can define the generalized Hermitian form $(\cdot,\cdot)_A$ on $L_{\mathbf{Q}}$ by

$$(x,y)_A=\sum_{j=1}^{k}\lambda_j\bar{\mu}_j,\quad\text{for } x=\sum_{j=1}^{k}\lambda_jx_j,\ y=\sum_{j=1}^{k}\mu_jx_j\in L_{\mathbf{Q}}.\tag{5.31}$$

Then $\langle\cdot,\cdot\rangle_A=\bigoplus_{j=1}^{k}\langle\cdot,\cdot\rangle_{n,A}=\varphi_A\circ(\cdot,\cdot)_A$.

Definition 5.11. We define the *complex dual* of a complex R_n^A-lattice $\mathcal{L}$ by

$$\mathcal{L}^{\mathrm{cd}} = \{x \in L_{\mathbf{Q}} \mid (x,y)_A \in (1-\omega_{n,A})R_n^A = Q_{n,A} \text{ for all } y \in \mathcal{L}\}. \tag{5.32}$$

The lattice $\mathcal{L}$ is called a *complex integral* (*self-dual*) *lattice* if $\mathcal{L}^{\mathrm{cd}} \supset \mathcal{L}$ ($\mathcal{L}^{\mathrm{cd}} = \mathcal{L}$).

THEOREM 5.12. *The lattice $\mathcal{L}$ is a complex self-dual R_n^A-lattice if and only if it is a self-dual complex R_n^A-lattice with respect to $\langle\cdot,\cdot\rangle_A$.*

Proof. It is sufficient to prove $\mathcal{L}^\circ = \mathcal{L}^{\mathrm{cd}}$. First of all, $\mathcal{L}^\circ \supset \mathcal{L}^{\mathrm{cd}}$ by Proposition 4.2. Now let $x \in \mathcal{L}^\circ$. For any $y \in \mathcal{L}$, we set $(x,y)_A = a = \sum_{i=0}^{n-2} a_i \omega_{n,A}^i$. Then

$$a_j - \frac{1}{n}\sum_{i=0}^{n-2} a_i = \varphi_A((x,\omega_{n,A}^j y)_A) = \langle x, \omega_{n,A}^j y\rangle_A \in \mathbf{Z} \tag{5.33}$$

for $j = 0, \ldots, n-2$ since $\mathcal{L}$ is an R_n^A-module. Similarly, we have

$$-\frac{1}{n}\sum_{i=0}^{n-2} a_i = \langle x, \omega_{n,A}^{-1} y\rangle_A \in \mathbf{Z}. \tag{5.34}$$

Thus, we have

$$a_i \in \mathbf{Z}; \quad \sum_{i=0}^{n-2} a_i \equiv 0 \pmod{n}. \tag{5.35}$$

This implies that $a = \sum_{i=0}^{n-2} a_i + \sum_{j=1}^{n-2} a_j(\omega_{n,A}^j - 1) \in Q_{n,A}$ by Proposition 4.2. That is, $x \in \mathcal{L}^{\mathrm{cd}}$. □

Remark 5.13. (a) The terms "complex self-dual" and "self-dual complex" above are different in the sense that the first is defined with respect to $(\cdot,\cdot)_A$ and the second is defined with respect to $\langle\cdot,\cdot\rangle_A$.

(b) In another work of ours [26], we prove that $L_{p,A}[\mathcal{C}]$ and $\tilde{L}_{p,A}[\mathcal{C}]$ are free R_p^A-modules of rank k, where p is a prime number, $\mathcal{C}$ is a self-dual code of length k over $\mathbf{Z}_p$ and $\mathcal{C} \ni \mathbf{1}_k$ in the second case. One can check that $R_p^A \cong \mathbf{Z}[\omega_p] \subset \mathbf{C}$, where $\omega_p = e^{2\pi i/p}$. In particular, $L_{3,A}[\mathcal{C}]$ and $\tilde{L}_{3,A}[\mathcal{C}]$ are also complex lattices in the sense of the definition given in [22].

The following fact also shows that our definition of complex R_n^A-lattice is very reasonable.

THEOREM 5.14. *Let $\mathcal{L}$ be an R_n^A-complex lattice. If g is an R_n^A-module automorphism, then*

$$\begin{gathered}\langle g(x), g(y)\rangle_A = \langle x,y\rangle_A \quad \textit{for all } x,y \in \mathcal{L} \\ \Longleftrightarrow \\ (g(x), g(y))_A = (x,y)_A \quad \textit{for all } x,y \in \mathcal{L}.\end{gathered} \tag{5.36}$$

Proof. "$\Leftarrow$" is trivial since $\langle\cdot,\cdot\rangle_A=\varphi_A\circ(\cdot,\cdot)_A$.

Let us prove "$\Rightarrow$". For any $x,y\in\mathcal{L}$, we let

$$(g(x),g(y))_A=\sum_{i=0}^{n-2}\lambda_i\omega_{n,A}^i,\quad (x,y)_A=\sum_{i=0}^{n-2}\mu_i\omega_{n,A}^i,\quad \lambda_i,\mu_i\in\mathbf{Q}. \tag{5.37}$$

Now by assumption,

$$\lambda_j-\frac{1}{n}\sum_{i=0}^{n-2}\lambda_i=\langle g(x),\omega_{n,A}^j g(y)\rangle_A=\langle x,\omega_{n,A}^j y\rangle_A=\mu_j-\frac{1}{n}\sum_{i=0}^{n-2}\mu_i \tag{5.38}$$

for $0\leqslant j\leqslant n-2$ and

$$-\frac{1}{n}\sum_{i=0}^{n-2}\lambda_i=\langle\omega_{n,A}g(x),g(y)\rangle_A=\langle\omega_{n,A}x,y\rangle=-\frac{1}{n}\sum_{i=0}^{n-2}\mu_i. \tag{5.39}$$

Therefore, $\lambda_i=\mu_i$, $i=0,1,\ldots,n-2$. That is, $(g(x),g(y))_A=(x,y)$. □

Remark 5.15. In [24], we have constructed certain induced T-shells by means of our twisted type-A lattices. We also introduced in [24] T-shells of type D.

6. Basic homogeneous twist parameters of type *A*

By analyzing the twist factor $J_A[n,k;t]=[k(n^2-1)+24t]/(12n)$, we divide our work into the following six cases. We simply denote $J_A(n,k;t)$ as J_A.

Case 1. $n=6s+1$, $s\in\mathbf{Z}$.

$$J_A=\frac{k(36s^2+12s)+24t}{12n}=\frac{2\left[\frac{1}{2}ks(3s+1)+t\right]}{n}, \tag{6.1}$$

where $\frac{1}{2}s(3s+1)$ is always an integer. Therefore,

$$\tilde{t}_A\equiv-\tfrac{1}{2}ks(3s+1)\pmod{n},\quad J_A\text{ is even}. \tag{6.2}$$

Case 2. $n=6s+2$, $s\in\mathbf{Z}$.

$$J_A=\frac{k(36s^2+24s+3)+24t}{12\cdot 2(3s+1)}=\frac{k(4s(3s+2)+1)+8t}{8(3s+1)}. \tag{6.3}$$

The requirement for $J_A\in\mathbf{Z}$:

$$k=8l,\quad l\in\mathbf{Z}. \tag{6.4}$$

Then

$$J_A=\frac{l[4s(3s+2)+1]+t}{3s+1}\equiv\frac{4ls+l+t}{3s+1}\pmod 4. \tag{6.5}$$

Therefore,

$$\tilde{t}_{A,1}\equiv -4ls-l \pmod n,\quad J_A \text{ is even;} \tag{6.6}$$

and

$$\tilde{t}_{A,2}\equiv -4ls-l+\tfrac{1}{2}n \pmod n,\quad J_A \text{ is odd.} \tag{6.7}$$

Case 3. $n=6s+3$, $s\in\mathbf{Z}$.

$$J_A=\frac{k(36s^2+36s+8)+24t}{12n}=\frac{2\left[k\left(\tfrac{1}{2}9s(s+1)+1\right)+3t\right]}{3n}. \tag{6.8}$$

The requirement for $J_A\in\mathbf{Z}$:

$$k=3l,\quad l\in\mathbf{Z}. \tag{6.9}$$

Then

$$J_A=\frac{2\left[l\left(\tfrac{1}{2}9s(s+1)+1\right)+t\right]}{n}. \tag{6.10}$$

Therefore,

$$\tilde{t}_A\equiv -l\left(\tfrac{1}{2}9s(s+1)+1\right) \pmod n,\quad J_A \text{ is even.} \tag{6.11}$$

Case 4. $n=6s+4$, $s\in\mathbf{Z}$.

$$J_A=\frac{k(36s^2+48s+15)+24t}{12\cdot 2(3s+2)}=\frac{k[4s(3s+4)+5]+8t}{8(3s+2)}. \tag{6.12}$$

The requirement for $J_A\in\mathbf{Z}$:

$$k=8l,\quad l\in\mathbf{Z}. \tag{6.13}$$

Then

$$J_A\equiv\frac{l(8s+5)+t}{3s+2}\pmod 4\ \equiv\frac{l(2s+1)+t}{3s+2}\pmod 2. \tag{6.14}$$

Therefore,

$$\tilde{t}_{A,1}\equiv -l(2s+1) \pmod n,\quad J_A \text{ is even;} \tag{6.15}$$

and

$$\tilde{t}_{A,2}\equiv -l(2s+1)+\tfrac{1}{2}n \pmod n,\quad J_A \text{ is odd.} \tag{6.16}$$

Case 5. $n=6s+5$, $s\in\mathbf{Z}$.

$$J_A=\frac{k(36s^2+60s+24)+24t}{12n}=\frac{2\left[k\left(\tfrac{1}{2}s(3s+5)+1\right)+t\right]}{n}, \tag{6.17}$$

where $\frac{1}{2}s(3s+5)$ is always an integer. Therefore,

$$\tilde{t}_A = -\tfrac{1}{2}k[s(3s+5)+2] \pmod{n}, \quad J_A \text{ is even.} \tag{6.18}$$

Case 6. $n=6s$, $s\in\mathbf{Z}$.

$$J_A = \frac{k(36s^2-1)+24t}{12\cdot 6s}. \tag{6.19}$$

The requirement for $J_A\in\mathbf{Z}$:

$$k=24l, \quad l\in\mathbf{Z}. \tag{6.20}$$

Then

$$J_A = \frac{l(36s^2-1)+t}{3s} \equiv \frac{-l+t}{3s} \pmod{12}. \tag{6.21}$$

Therefore,

$$\tilde{t}_{A,1} \equiv l \pmod{n}, \quad J_A \text{ is even;} \tag{6.22}$$

and

$$\tilde{t}_{A,2} \equiv l+\tfrac{1}{2}n \pmod{n}, \quad J_A \text{ is odd.} \tag{6.23}$$

Thus, we find all basic homogeneous twist parameters of type-A self-dual complex lattices. Moreover, by Remark 4.6, (5.19) and (5.21), we have:

THEOREM 6.1. *The lattice* $\tilde{L}_{n,A}[C]$ *is an even self-dual lattice under the following conditions*:

(1) n *is odd or* C *satisfies* (4.22);

(2) $\tilde{t}_A(\mathbf{n},\Upsilon)$ *is as in* (5.21), *and*

$$\tilde{t}_A(\mathbf{n}) = \begin{cases} \tilde{t}_A & \text{in Cases } 1,3,5, \\ \tilde{t}_{A,1} & \text{in Cases } 2,4,6. \end{cases} \qquad \square$$

Acknowledgments. The author of this paper would like to thank Professors J. Lepowsky and R. L. Wilson for their advice. He is also very grateful to the referee for his/her important comments.

References

[1] BLAKE, I. F. & MULLIN, R. C., *The Mathematical Theory of Coding*. Academic Press, New York–London, 1975.

[2] BORCHERDS, R. E., The Leech lattice and other lattices. Ph.D. Dissertation, University of Cambridge, 1984.

[3] — Vertex algebras, Kac–Moody algebras, and the monster. *Proc. Nat. Acad. Sci. U.S.A.*, 83 (1986), 3068–3071.

[4] CONWAY, J. H., A characterization of Leech's lattice. *Invent. Math.*, 69 (1969), 137–142.

[5] — Three lectures on exceptional groups, in *Finite Simple Groups* (G. Higman and M. B. Powell, eds.), Chapter 7, pp. 215–247. Academic Press, London–New York, 1971.

[6] CONWAY, J. H. & NORTON, S. P., Monstrous moonshine. *Bull. London Math. Soc.*, 11 (1979), 308–339.

[7] CONWAY, J. H. & SLOANE, N. J. A., Twenty-three constructions of the Leech lattice. *Proc. Roy. Soc. London Ser. A*, 381 (1982), 275–283.

[8] — On the enumeration of lattices of determinant one. *J. Number Theory*, 15 (1982), 83–94.

[9] — *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York–Berlin, 1988.

[10] DOLAN, L., GODDARD, P. & MONTAGUE, P., Conformal field theory of twisted vertex operators. *Nuclear Phys. B*, 338 (1990), 529–601.

[11] DONG, C. & LEPOWSKY, J., A Jacobi identity for relative twisted vertex operators. Preprint.

[12] FEIT, W., On integral representations of finite groups. *Proc. London Math. Soc. (3)*, 29 (1974), 633–683.

[13] FRENKEL, I. B., LEPOWSKY, J. & MEURMAN, A., A natural representation of the Fischer–Griess Monster with the modular function J as character. *Proc. Nat. Acad. Sci. U.S.A.*, 81 (1984), 3256–3260.

[14] — *Vertex Operator Algebras and the Monster*. Pure and Applied Math., 134. Academic Press, Boston, MA, 1988.

[15] GRIESS, R. L., JR., The friendly giant. *Invent. Math.*, 69 (1982), 1–102.

[16] LEECH, J., Notes on sphere packings. *Canad. J. Math.*, 19 (1967), 718–745.

[17] LEPOWSKY, J. & MEURMAN, A., An E_8-approach to the Leech lattice and the Conway group. *J. Algebra*, 77 (1982), 484–504.

[18] LINDSEY, J. H., A correlation between $PSU_4(3)$, the Suzuki group, and the Conway group. *Trans. Amer. Math. Soc.*, 157 (1971), 189–204.

[19] MEURMAN, A., Personal notes.

[20] NIEMEIER, H. V., Definite quadratische Formen der Dimension 24 und Diskriminante 1. *J. Number Theory*, 5 (1973), 142–178.

[21] SLOANE, N. J. A., Codes over $GF(4)$ and complex lattices. *J. Algebra*, 52 (1978), 168–181.

[22] — Self-dual codes and lattices. *Proc. Sympos. Pure Math.*, 34 (1979), 273–307.

[23] TITS, J., Four presentations of Leech's lattice, in *Finite Simple Groups* II, *Proc. Sympos., Univ. of Durham, Durham,* 1978 (M. J. Collins, ed.), pp. 303–307. Academic Press, London–New York, 1980.

[24] XU, X., Untwisted and twisted gluing techniques for constructing self-dual lattices. Ph.D. Dissertation, Rutgers University, 1992.

[25] — A gluing technique for constructing self-dual codes. *J. Combin. Theory Ser. A*, 66 (1994), 137–159.

[26] — Central extensions of self-dual type-A complex lattices. *Comm. Algebra*, 22 (1994), 1281–1303.

[27] — Lattice coset constructions of vertex operators. To appear in *Algebra Colloquium.*
[28] — Analogue of vertex operator triality for ternary codes. *J. Pure Appl. Algebra*, 99 (1995), 53–111.
[29] YOSHIARA, S., A lattice theoretical construction of a Gab of the Suzuki sporadic simple group. *J. Algebra*, 112 (1988), 198–239.

XIAOPING XU
Department of Mathematics
The Hong Kong University of Science and Technology
Clear Water Bay, Kowloon
Hong Kong
xiaoping@uxmail.ust.hk

Received June 10, 1993