JOURNAL OF ALGEBRA 52, 168–181 (1978)

Codes over $GF(4)$ and Complex Lattices

N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by Walter Feit

Received March 15, 1977

This paper studies the relationship between error-correcting codes over $GF(4)$ and complex lattices (more precisely, $\mathbb{Z}[\omega]$-modules in $\mathbb{C}^n$, where $\omega = e^{2\pi i/3}$). The theta-functions of self-dual lattices are characterized. Two general methods are presented for constructing lattices from codes. Several examples are given, including a new lattice sphere-packing in $\mathbb{R}^{36}$.

1. INTRODUCTION

The connections between binary and ternary error-correcting codes on the one hand, and lattices and sphere-packings in $\mathbb{R}^n$ on the other have been studied by several authors [6, 7, 19–21, 26, 29, 30, 39, 40]. Since the theorem of Gleason, Pierce and Turyn [1, p. 381; 2] states that codes over $GF(2)$, $GF(3)$ and $GF(4)$ have especially nice properties not shared by codes over other fields, one might expect that codes over $GF(4)$ should also be connected with sphere-packings. It is the aim of the present paper to show that there are natural connections between codes over $GF(4)$ and complex lattices and sphere-packings. For example the weight enumerator of the code and the theta-function of the lattice have similar properties: compare Theorem 3 below with Theorem 1, and Theorem 4 with Theorem 9. The cusp form $\Delta(z) = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24} = \sum_{m=0}^{\infty} a_m q^{2m}$ (where the a_m are the Ramanujan numbers and $q = e^{\pi i z}$) plays a special role in characterizing the theta-functions of even unimodular lattices in $\mathbb{R}^n$. The same role for our complex lattices is played by $\Delta_6(z)$; compare Eqs. (19), (20), and Theorems 9, 10. In Sections 6 and 8 two constructions are given for obtaining lattices from codes over $GF(4)$. In this way it is possible to construct the densest known lattice packings A_2 in $\mathbb{R}^2$, E_6 in $\mathbb{R}^6$ and K_{12} in $\mathbb{R}^{12}$ directly from codes (filling in a gap in [21]); we also find a very dense lattice packing in $\mathbb{R}^{36}$ (Example 7).

Complex lattices have also been used in studying complex polytopes and simple groups [8–11, 14, 14a, 23, 36, 37] and are related to the problem of finding sets of lines in $\mathbb{C}^n$ having a prescribed number of angles [12]

0021-8693/78/0521–0168$02.00/0

2. Complex Lattices and Sphere-Packings

A (real) lattice in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$ which spans $\mathbb{R}^n$, in the sense that any point of $\mathbb{R}^n$ can be written as a linear combination of lattice points with real coefficients. In particular a real lattice is a $\mathbb{Z}$-module. In this paper a *complex lattice* (or *$\mathscr{E}$-lattice*) in $\mathbb{C}^n$ will always mean a discrete subgroup of $\mathbb{C}^n$ which (i) spans $\mathbb{C}^n$ in the sense that any point of $\mathbb{C}^n$ can be written as a linear combination of lattice points with complex coefficients, and (ii) is a free $\mathscr{E}$-module, where $\mathscr{E} = \{a + b\omega : a, b \in \mathbb{Z}\}$, $\omega = e^{2\pi i/3}$, denotes the Eisenstein integers (cf. [9, p. 421; 10, p. 145; 11; 14, p. 635; 17, p. 179; 22]). Thus $\mathscr{E}$ plays the same role for these complex lattices as $\mathbb{Z}$ plays for real lattices. In particular, the *dual* lattice $\Lambda^\perp = \{\mathbf{x} \in \mathbb{C}^n : \mathbf{x} \cdot \bar{\mathbf{y}} \in \mathscr{E} \text{ for all } \mathbf{y} \in \Lambda\}$, where $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i$ and the bar denotes conjugation.

Let $\{\mathbf{e}^1 = (e_1{}^1, \ldots, e_n{}^1), \ldots, \mathbf{e}^n = (e_1{}^n, \ldots, e_n{}^n)\}$ be an $\mathscr{E}$-basis for Λ. The $n \times n$ matrix M with (i, j)th entry equal to $e_j{}^i$ is called a *generator matrix* for Λ. Any $\mathbf{x} \in \Lambda$ can be written uniquely as $\mathbf{x} = \mathbf{c}M$ where $\mathbf{c} \in \mathscr{E}^n$. It is easy to see that $(\bar{M}^{-1})^{tr}$ is a generator matrix for $\Lambda^\perp$. The determinant of Λ is defined to be

$$\det \Lambda = |\det M|,$$

and $\det \Lambda^\perp = (\det \Lambda)^{-1}$. If $\Lambda = \Lambda^\perp$ then Λ is called *self-dual.* For example $\mathscr{E}^n$ is a self-dual lattice in $\mathbb{C}^n$ with $M = I_n$. Also Λ is self-dual if and only if $\det \Lambda = 1$ and $\mathbf{e}^i \cdot \bar{\mathbf{e}}^j \in \mathscr{E}$ for all i, j. The self-dual lattices in $\mathbb{C}^n$ for $n \leqslant 12$ have been classified by Feit [14a].

The *minimum squared length* of Λ is

$$d = \min_{\mathbf{x} \in \Lambda - \{0\}} \mathbf{x} \cdot \bar{\mathbf{x}}.$$

If complex spheres of radius $\rho = \frac{1}{2} d^{1/2}$ are centered at the points of Λ these spheres do not overlap and form a complex *$\mathscr{E}$-lattice sphere-packing* in $\mathbb{C}^n$. The *density* of this packing or lattice is the fraction of $\mathbb{C}^n$ covered by the spheres, given by

$$\Delta = \frac{V_{2n} \rho^{2n}}{(\det \Lambda)^2 (3^{1/2}/2)^n}, \tag{1}$$

where $V_n = \pi^{n/2} / \Gamma(n/2 + 1)$. The *contact number*, or number of spheres touching one sphere, is $\tau = \#\{\mathbf{x} \in \Lambda : \mathbf{x} \cdot \bar{\mathbf{x}} = d\}$. Although it is not our goal in the present paper, one can now study $\Delta^o(n)$ and $\tau^o(n)$, the largest Δ and τ attained by $\mathscr{E}$-lattice packings in $\mathbb{C}^n$. The determinant, density and contact number of a real lattice are defined in the analogous way (see [34, 21]).

If Λ is an $\mathscr{E}$-lattice in $\mathbb{C}^n$ with parameters d, Δ, τ, let $\Lambda_R \subset \mathbb{R}^{2n}$ consist of all points

$$(\mathrm{Re}(x_1), \mathrm{Im}(x_1), \mathrm{Re}(x_2), \ldots, \mathrm{Im}(x_n))$$

where $(x_1, \ldots, x_n) \in \Lambda$. Then Λ_R is a lattice in $\mathbb{R}^{2n}$ with minimum squared length d. If real spheres of radius $\rho = \frac{1}{2}d^{1/2}$ are centered at the points of Λ_R, a lattice sphere-packing in $\mathbb{R}^{2n}$ is obtained, having determinant $\det \Lambda_R = (3^{1/2}/2)^n(\det \Lambda)^2$, density $= \Delta$, and contact number $= \tau$. (Note that in general $(\Lambda^\perp)_R \neq (\Lambda_R)^\perp$.) Since the largest Δ for a lattice packing in $\mathbb{R}^n$ is known for $n \leqslant 8$ (see [34, 21]), we have

$$\Delta^o(1) \leqslant V_2 \cdot 2^{-1} \cdot 3^{-1/2}, \qquad \Delta^o(2) \leqslant V_4 \cdot 2^{-3}, \qquad \Delta^o(3) \leqslant V_6 \cdot 2^{-3} \cdot 3^{-1/2},$$
$$\Delta^o(4) \leqslant V_8 \cdot 2^{-4} \tag{2}$$

Examples 4 and 5 will show that equality holds for $\Delta^o(1)$ and $\Delta^o(3)$.

3. The Theta-Function of a Lattice

The theta-function of an $\mathscr{E}$-lattice Λ in $\mathbb{C}^n$ is

$$\Theta_\Lambda(z) = \sum_{x \in \Lambda} e^{\pi i z \mathbf{x} \cdot \bar{\mathbf{x}}}$$

and is holomorphic for $z \in \mathscr{H} = \{z \in \mathbb{C}: \operatorname{Im}(z) > 0\}$.

Theorem 1. *For* $z \in \mathscr{H}$,

$$\Theta_{\Lambda^\perp}(z) = (\det \Lambda)^2 \, (2i/3^{1/2}z)^n \, \Theta_\Lambda(-4/3z). \tag{3}$$

Remark. For a real lattice $\Lambda \subset \mathbb{R}^n$ with theta-function $\Theta_\Lambda(z) = \sum_{\mathbf{x} \in \Lambda} \times \exp(\pi i z \mathbf{x} \cdot \mathbf{x})$, the analogous result is

$$\Theta_{\Lambda^\perp}(z) = (\det \Lambda)(i/z)^{n/2} \, \Theta_\Lambda(-1/z). \tag{4}$$

(see for example [13, Chap. 2, Sect. 11.3; 35, Chap. VII, Sect. 6].) Note that an $\mathscr{E}$-lattice Λ and the real lattice Λ_R have the same theta-function.

Proof. Equation (3), like (4), is a consequence of the appropriate version of the Poisson summation formula. For $z = z_a + \omega z_b = z_r + i z_i \in \mathbb{C}$, where z_a, z_b, z_r, z_i are real, define $R\colon \mathbb{C} \to \mathbb{R}$ by

$$R(z) = z_a = z_r + (1/3^{1/2})\, z_i .$$

If $z' = z'_a + \omega z'_b$ then $R(z\bar{z}') = z_a z'_a - z_a z'_b + z_b z'_b$. If Λ is an $\mathscr{E}$-lattice in $\mathbb{C}^n$, the functions $\chi_\mathbf{y} : \mathbb{C}^n/\Lambda \to \mathbb{C}$ given by

$$\chi_\mathbf{y}(\mathbf{x}) = e^{2\pi i R(\mathbf{x} \cdot \bar{\mathbf{y}})}, \qquad \mathbf{x} \in \mathbb{C}^n/\Lambda,$$

for $\mathbf{y} \in \Lambda^\perp$ form the character group of $\mathbb{C}^n/\Lambda$, which is isomorphic to $\Lambda^\perp$. The

Poisson summation formula [13, p. 220; 18, p. 44; 24, p. 153] implies that if f is a Schwartz function on $\mathbb{C}^n$ then

$$\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = (\det \Lambda)^{-2} \left(\frac{2}{3^{1/2}}\right)^n \sum_{\mathbf{y}\in\Lambda^\perp} \hat{f}(\mathbf{y}), \tag{5}$$

where

$$\hat{f}(\mathbf{y}) = \int_{\mathbb{C}^n} f(\mathbf{x})\, e^{-2\pi i R(\mathbf{x}\cdot\bar{\mathbf{y}})}\, d\mathbf{x}.$$

Equation (3) follows from (5) by taking

$$f(\mathbf{x}) = (4i/3z)^n\, e^{-4\pi i \mathbf{x}\cdot\bar{\mathbf{x}}/3z}, \qquad \hat{f}(\mathbf{y}) = e^{\pi i z \mathbf{y}\cdot\bar{\mathbf{y}}}.$$

COROLLARY 2. *If Λ is a self-dual lattice in $\mathbb{C}^n$,*

(i) $\Theta_\Lambda(z+2) = \Theta_\Lambda(z)$,

(ii) $\Theta_\Lambda(-4/3z) = (3^{1/2}z/2i)^n\, \Theta_\Lambda(z)$, (6)

(iii) *if n is even, $\theta_\Lambda(2z)$ is a modular form of weight n for the congruence group $\Gamma_0(3)$. (Here we are using "weight" as defined in* [35] *or* [38], *not as in* [15].)

Proof. (ii) follows from Theorem 1. Put $f(z) = \Theta_\Lambda(2z)$. Then $f(z+1) = f(z)$ and $f(-1/3z) = (-i\, 3^{1/2}z)^n f(z)$, which imply $f(z/(3z+1)) = (3z+1)^n f(z)$. Since $\binom{11}{01}$ and $\binom{10}{31}$ generate $\Gamma_0(3)$, (iii) follows. Note that (iii) is strictly weaker than (i) and (ii).

4. JACOBI THETA-FUNCTIONS

The theta-functions of lattices are conveniently expressed in terms of the Jacobi theta-functions, defined as follows (cf. [4, 33, 41, 43]).

$$\theta'_1(z) = \theta'_1(0 \mid z) = 2 \sum_{m=0}^{\infty} (-1)^m (2m+1)\, q^{(m+1/2)^2}$$

$$= 2q^{1/4} \prod_{m=1}^{\infty} (1-q^{2m})^3, \tag{7}$$

$$\theta_2(z) = \theta_2(0 \mid z) = 2 \sum_{m=0}^{\infty} q^{(m+1/2)^2},$$

$$\theta_3(z) = \theta_3(0 \mid z) = 1 + 2 \sum_{m=1}^{\infty} q^{m^2},$$

$$\theta_4(z) = \theta_4(0 \mid z) = 1 + 2 \sum_{m=1}^{\infty} (-q)^{m^2},$$

where $q = e^{\pi i z}$, $z \in \mathscr{H}$. The following are the most useful of the "labyrinth" of identities relating the θ_i.

$$\theta'_1(z) = \theta_2(z)\,\theta_3(z)\,\theta_4(z), \tag{8}$$

$$\theta_2\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \theta_4(z), \qquad \theta_3\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \theta_3(z), \tag{9}$$

$$\theta_2(z)^2 = 2\theta_2(2z)\,\theta_3(2z), \qquad \theta_3(z)\,\theta_4(z) = \theta_4(2z)^2, \tag{10}$$

$$\theta_3(z)^2 + \theta_4(z)^2 = 2\theta_3(2z)^2, \qquad \theta_3(z)^2 - \theta_4(z)^2 = 2\theta_2(2z)^2, \tag{11}$$

$$\theta_3(z) + \theta_4(z) = 2\theta_3(4z), \qquad \theta_3(z) - \theta_4(z) = 2\theta_2(4z). \tag{12}$$

EXAMPLE 1. The lattice $\mathscr{E}$ in $\mathbb{C}^1$ has theta-function

$$\begin{aligned} \Theta_{\mathscr{E}}(z) &= \sum_{a+b\omega\in\mathscr{E}} q^{|a+b\omega|} = \sum_{a=-\infty}^{\infty} \sum_{b=-\infty}^{\infty} q^{a^2-ab+b^2} \\ &= \theta_2(z)\,\theta_2(3z) + \theta_3(z)\,\theta_3(3z) = \phi_0(\tfrac{1}{2}z) \quad \text{(say)} \\ &= 1 + 6q + 6q^3 + 6q^4 + 12q^7 + 6q^9 + \cdots. \end{aligned} \tag{13}$$

5. CODES OVER $GF(4)$

Let the elements of $GF(4)$ be $0, 1, \omega, \omega^2$, with $\omega^2 + \omega + 1 = 0$. The conjugate of $x \in GF(4)$ is $\bar{x} = x^2$. Let $\mathscr{C}$ be a linear code over $GF(4)$ of length n and dimension k (see [27], [28]). The *dual* code $\mathscr{C}^\perp = \{\mathbf{u} \in GF(4)^n : \mathbf{u} \cdot \bar{\mathbf{v}} = 0$ for all $\mathbf{v} \in \mathscr{C}\}$, where $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^n u_i v_i$, and has dimension $n - k$. (A different definition of $\mathscr{C}^\perp$ was used in [27].) If $\mathscr{C} = \mathscr{C}^\perp$, $\mathscr{C}$ is called *self-dual* (and n is even). A code can be defined by giving its *generator matrix* M, which is a $k \times n$ matrix whose rows span the code. If $M = [I \mid B]$ is a generator matrix for $\mathscr{C}$ then $[\bar{B}^{tr} \mid I]$ is a generator matrix for $\mathscr{C}^\perp$. Also $\mathscr{C}$ is self-dual if and only if $B\bar{B}^{tr} = I$ (i.e. B is unitary). The weight $wt(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, ..., x_n)$ is the number of nonzero x_i. The *minimum distance* of $\mathscr{C}$ is

$$\text{dist}(\mathscr{C}) = \min\{wt(\mathbf{u}) : u \in \mathscr{C}, \mathbf{u} \neq 0\}$$

and the *weight enumerator* is

$$\begin{aligned} W_{\mathscr{C}}(x, y) &= \sum_{\mathbf{u}\in\mathscr{C}} x^{n-wt(\mathbf{u})} y^{wt(\mathbf{u})} \\ &= \sum_{r=0}^{n} A_r x^{n-r} y^r, \end{aligned}$$

where A_r is the number of codewords in $\mathscr{C}$ of weight r. The automorphism group of $\mathscr{C}$, Aut($\mathscr{C}$), consists of all $n \times n$ monomial matrices over $GF(4)$ which set-wise preserve the code.

THEOREM 3 (MacWilliams [25, 28]).

$$W_{\mathscr{C}^\perp}(x, y) = 4^{-k} W_{\mathscr{C}}(x + 3y, x - y)$$

THEOREM 4 [26]. *If $\mathscr{C}$ is self-dual then $W_{\mathscr{C}}(x, y) \in \mathbb{C}[f_2, f_6]$, where*

$$f_2 = x^2 + 3y^2, \qquad f_6 = y^2(x^2 - y^2)^2.$$

EXAMPLE 2. The self-dual code $C_2 = \{00, 11, \omega\omega, \omega^2\omega^2\}$ has $n = 2$, $k = 1$, dist$(C_2) = 2$, $W_{C_2}(x, y) = f_2$, and Aut$(C_2) = 3\mathscr{S}_2$.

EXAMPLE 3. The matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix}$$

generates a self-dual code Q_6 with $n = 6$, $k = 3$, $W_{Q_6}(x, y) = x^6 + 45x^2y^4 + 18y^6 = f_2^3 - 9f_6$, and Aut$(Q_6) = 3\mathscr{A}_6$.

For further properties and examples see [27].

6. CONSTRUCTION OF LATTICES FROM CODES OVER $GF(4)$

The starting point is the observation that $2\mathscr{E}$ is a prime ideal in $\mathscr{E}$, and $\mathscr{E}/2\mathscr{E}$ is isomorphic to $GF(4)$. In fact, if we take coset representatives $0, 1, \omega, \omega^2$ for $2\mathscr{E}$ in $\mathscr{E}$, there is an isomorphism mapping $2\mathscr{E}$ onto 0, $1 + 2\mathscr{E}$ onto 1, $\omega + 2\mathscr{E}$ onto ω, and $\omega^2 + 2\mathscr{E}$ onto ω^2. Hence there is a map $\sigma: \mathscr{E} \to \mathscr{E}/2\mathscr{E} \to GF(4)$ which sends $\omega^r \in \mathscr{E}$ onto $\omega^r \in GF(4)$ $(r = 0, 1, 2)$.

Two constructions will be given (cf. [21]), the second in Section 8.

CONSTRUCTION A. Let $\mathscr{C}$ be a linear code over $GF(4)$ of length n and dimension k. Let $\Lambda(\mathscr{C})$ consist of all $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{C}^n$ such that $\sigma(2^{1/2}\mathbf{x}) \in \mathscr{C}$.

In words, the points of $\Lambda(\mathscr{C})$ are all vectors $\mathbf{x}$ that can be obtained from codewords by adding twice an Eisenstein integer to each component, and then dividing by $2^{1/2}$.

THEOREM 5. (i) *$\Lambda(\mathscr{C})$ is an $\mathscr{E}$-lattice in* $\mathbb{C}^n$. (ii) $\det \Lambda = 2^{n/2-k}$. (iii) $\Lambda(\mathscr{C}^\perp) = \Lambda(\mathscr{C})^\perp$. (iv) $\Lambda(\mathscr{C})$ is self-dual if and only if $\mathscr{C}$ is a self-dual code.

Proof. (i) is immediate. Without loss of generality let $\mathscr{C}$ have generator matrix $[I_k \mid B]$. Then

$$M = \frac{1}{2^{1/2}} \begin{bmatrix} I_k & B \\ 0 & 2I_{n-k} \end{bmatrix}$$

is a generator matrix for $\Lambda(\mathscr{C})$. The rest of the proof is now straightforward.

THEOREM 6. *The lattice $\Lambda(\mathscr{C})$ has the following properties*:

$$d = \begin{cases} \frac{1}{2}\,\mathrm{dist}(\mathscr{C}) & \text{if } \mathrm{dist}(\mathscr{C}) \leqslant 4, \\ 2 & \text{if } \mathrm{dist}(\mathscr{C}) \geqslant 4, \end{cases}$$

density $\Delta = V_{2n}\rho^{2n}4^k 3^{-n/2}$, where $\rho = \frac{1}{2}d^{1/2}$,

$$\begin{matrix}\text{contact} \\ \text{number}\end{matrix} \quad \tau = \begin{cases} 2^\delta A_\delta & \text{if } \mathrm{dist}(\mathscr{C}) = \delta < 4, \\ 16A_4 + 6n & \text{if } \mathrm{dist}(\mathscr{C}) = 4, \\ 6n & \text{if } \mathrm{dist}(\mathscr{C}) > 4. \end{cases}$$

Proof. Suppose $\mathrm{dist}(\mathscr{C}) = 4$. Then the lattice points closest to $\mathbf{0}$ consist of $16A_4$ {e.g. a codeword $(1\omega 1\omega^2 0 \cdots 0)$ gives rise to $(1/2^{1/2})(\pm 1, \pm\omega, \pm 1, \pm\omega^2, 0,\ldots, 0)$} plus $6n$ {of type $((\pm\omega^r\, 2^{1/2})^1\, 0^{n-1})$ for $r = 0, 1, 2$}, for a total of $\tau = 16A_4 + 6n$ at a squared distance of $d = 2$. Similarly for the other cases. The expression for Δ follows from Eq. (1).

THEOREM 7. $\Theta_{\Lambda(\mathscr{C})}(z) = W_{\mathscr{C}}(\phi_0(z), \phi_1(z))$, *where*

$$\phi_0(z) = \theta_2(2z)\,\theta_2(6z) + \theta_3(2z)\,\theta_3(6z) \qquad \text{(see (13))},$$

$$\begin{aligned} \phi_1(z) &= \theta_2(2z)\,\theta_3(6z) + \theta_2(6z)\,\theta_3(2z) \\ &= \tfrac{1}{2}\theta_2(\tfrac{1}{2}z)\,\theta_2(\tfrac{3}{2}z) \\ &= 2q^{1/2}(1 + q + 2q^3 + q^4 + 2q^6 + 2q^9 + \cdots). \end{aligned} \tag{14}$$

Proof. Consider a codeword $\mathbf{u} = (u_1, u_2, \ldots) \in \mathscr{C}$. The corresponding centers in $\Lambda(\mathscr{C})$, i.e. the points $(1/2^{1/2})\,\sigma^{-1}(\mathbf{u})$, consist of the set

$$\begin{aligned} \Lambda(\mathbf{u}) &= \{(1/2^{1/2})(x_1, x_2, \ldots) \colon x_1 \in \sigma^{-1}(u_1),\, x_2 \in \sigma^{-1}(u_2), \ldots\} \\ &= \{(y_1, y_2, \ldots) \colon y_r \in (1/2^{1/2})\, u_r + 2^{1/2}\mathscr{E},\ 1 \leqslant r \leqslant n\}. \end{aligned}$$

Let the theta-function of any subset $\mathscr{S}$ of $\Lambda(\mathscr{C})$ be

$$\Theta_{\mathscr{S}}(z) = \sum_{\mathbf{y}\in\mathscr{S}} q^{\mathbf{y}\cdot\bar{\mathbf{y}}}.$$

From (13),

$$\Theta_{2^{1/2}\mathscr{E}}(z) = \Theta_{\mathscr{E}}(2z) = \phi_0(z),$$

and a similar calculation shows that if $\mathscr{S} = 2^{-1/2}w^r + 2^{1/2}\mathscr{E}$, $r = 0, 1, 2$, then

$$\Theta_{\mathscr{S}}(z) = \theta_2(2z)\,\theta_3(6z) + \theta_2(6z)\,\theta_3(2z) = \phi_1(z).$$

Hence

$$\Theta_{\Lambda(\mathbf{u})}(z) = \phi_0(z)^{n-wt(\mathbf{u})}\,\phi_1(z)^{wt(\mathbf{u})},$$

$$\Theta_{\Lambda(\mathscr{C})}(z) = \sum_{\mathbf{u}\in\mathscr{C}} \Theta_{\Lambda(\mathbf{u})}(z) = W_{\mathscr{C}}(\phi_0(z), \phi_1(z)).$$

It remains to show that the first and second lines of (14) are equal. Using (12) this identity may be rewritten as

$$\theta_2(\tau)\,\theta_2(3\tau) + \theta_4(\tau)\,\theta_4(3\tau) = \theta_3(\tau)\,\theta_3(3\tau) \tag{15}$$

(apparently not in [41] or [43]). Then

$$\theta_3(\tau)\,\theta_3(3\tau) - \theta_4(\tau)\,\theta_4(3\tau)$$

$$= 2 \sum_{\substack{m=-\infty \\ m+n \text{ odd}}}^{\infty} \sum_{n=-\infty}^{\infty} q^{m^2+3n^2} \qquad (\text{set } m = \tfrac{1}{2}(-a+3b+1),\ n = \tfrac{1}{2}(a+b+1))$$

$$= 2 \sum_{\substack{a=-\infty \\ a+b \text{ odd}}}^{\infty} \sum_{b=-\infty}^{\infty} q^{(a+1/2)^2+3(b+1/2)^2}$$

$$= \sum_{a=-\infty}^{\infty} \sum_{b=-\infty}^{\infty} q^{(a+1/2)^2+3(b+1/2)^2} = \theta_2(\tau)\,\theta_2(3\tau),$$

since

$$\sum_{\substack{a=-\infty \\ a+b \text{ odd}}}^{\infty} \sum_{b=-\infty}^{\infty} q^{(a+1/2)^2+3(b+1/2)^2} = \sum_{\substack{c=-\infty \\ c+b \text{ even}}}^{\infty} \sum_{b=-\infty}^{\infty} q^{(-c-1/2)^2+3(b+1/2)^2}.$$

This completes the proof.

EXAMPLE 4. The trivial code T_n with generator matrix I_n, $k = n$, dist $= 1$, $W_{\mathscr{C}}(x, y) = (x + 3y)^n$ produces a lattice $\Lambda(T_n)$ with $\rho = 2^{-3/2}$, $\Delta = V_{2n}(2 \cdot 3^{1/2})^{-n}$, $\tau = 6n$, and theta-function $(\phi_0(z) + 3\phi_1(z))^n$. This lattice is clearly equal to $(1/2^{1/2})\,\mathscr{E}^n$, which has theta-function $\phi_0(\tfrac{1}{4}z)^n$, thus establishing the identity

$$\phi_0(z) + 3\phi_1(z) = \phi_0(\tfrac{1}{4}z). \tag{16}$$

(Equation (16) also follows from (12) and (15).) In particular when $n = 1$ the corresponding real lattice $\Lambda(T_1)_R$ is the densest packing A_2 in $\mathbb{R}^2$.

EXAMPLE 2 (cont.). Similarly in $\mathbb{C}^2$ the lattice $\Lambda(C_2)$ is equal to $\mathscr{E}^2$, which has theta-function $\phi_0(\frac{1}{2}z)^2$, leading to the identity

$$\phi_0(z)^2 + 3\phi_1(z)^2 = \phi_0(\tfrac{1}{2}z)^2.$$

EXAMPLE 5. In $\mathbb{C}^3$ three copies of $\Lambda(T_3)$ can be fitted together without overlap. The resulting lattice is

$$\Lambda(T_3) \cup (\mathbf{u} + \Lambda(T_3)) \cup (2\mathbf{u} + \Lambda(T_3))$$

where $\mathbf{u} = 2^{1/2}\,3^{-1}(\lambda, \lambda, \lambda)$, $\lambda = 1 - \omega$; and has generator matrix

$$\frac{1}{2^{1/2}\,3}\begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ \lambda & \lambda & \lambda \end{bmatrix},$$

$\rho = 2^{-3/2}$, $\Delta = V_6/8(3^{1/2})$, and $\tau = 72$. The corresponding real lattice is E_6 (cf. [5]) and in fact this is equivalent to Coxeter's construction of E_6 (see for example [9, p. 421]). It can be seen that the theta-function of E_6 is

$$\phi_0(\tfrac{1}{4}z)^3 + \tfrac{1}{4}\{\phi_0(\tfrac{1}{12}z) - \phi_0(\tfrac{1}{4}z)\}^3.$$

EXAMPLE 3 (cont.). In $\mathbb{C}^6$ we find that $\Lambda(Q_6)$ is a self-dual lattice (U_6 in Feit's notation [14a]) with $\Delta = V_{12}/27$ and $\tau = 756$. The corresponding real lattice is K_{12}, the densest known packing in $\mathbb{R}^{12}$, and in fact this is equivalent to Coxeter and Todd's construction of K_{12} given in [11]. The automorphism group of $\Lambda(Q_6)$ is $[2\ 1;\ 3]^3$, a unitary group generated by reflections (see [16, 36, 37, 42]).

The theta-function $\Theta_{\Lambda(Q_6)}(z)$ is given by Theorem 7, but we are more interested in the cusp form $\Delta_6(z)$, defined by

$$\begin{aligned}\Delta_6(z) &= \frac{1}{36}\{\Theta_{\Lambda(C_2)}(z)^3 - \Theta_{\Lambda(Q_6)}(z)\} \\ &= \frac{1}{36}\{(\phi_0(z)^2 + 3\phi_1(z)^2)^3 - (\phi_0(z)^6 + 45\phi_0(z)^2\,\phi_1(z)^4 + 18\phi_1(z)^6)\} \\ &= \frac{1}{4}\phi_1(z)^2\,\{\phi_0(z)^2 - \phi_1(z)^2\}^2.\end{aligned}$$

From (10), (11), (15),

$$\begin{aligned}\phi_1(z)^2 &= \tfrac{1}{2}\{\theta_2(z)^2\,\theta_2(3z)^2 + \theta_3(z)^2\,\theta_3(3z)^2 - \theta_4(z)^2\,\theta_4(3z)^2\} \\ &= \theta_2(z)\,\theta_2(3z)\,\theta_3(z)\,\theta_3(3z),\end{aligned} \tag{17}$$

$$\phi_0(z)^2 = \tfrac{1}{2}\{\theta_2(z)^2\,\theta_2(3z)^2 + \theta_3(z^2)^2\,\theta_3(3z)^2 + \theta_4(z)^2\,\theta_4(3z)^2\},$$

$$\phi_0(z)^2 - \phi_1(z)^2 = \theta_4(z)^2\,\theta_4(3z)^2. \tag{18}$$

Therefore from (10), (17), (18), (8) and (7),

$$\begin{aligned}\Delta_6(z) &= \frac{1}{16}\left\{\theta_2\left(\frac{z}{2}\right)\theta_2\left(\frac{3z}{2}\right)\theta_3\left(\frac{z}{2}\right)\theta_3\left(\frac{3z}{2}\right)\theta_4\left(\frac{z}{2}\right)\theta_4\left(\frac{3z}{2}\right)\right\}^2 \\ &= \frac{1}{16}\,\theta'_1\left(\frac{z}{2}\right)^2\theta'_1\left(\frac{3z}{2}\right)^2 \\ &= q\prod_{m=1}^{\infty}(1-q^m)^6(1-q^{3m})^6. \end{aligned} \tag{19}$$

The coefficients of $\Delta_6(z)$ play the role of the Ramanujan numbers (see Theorem 9). The first few are as follows.

$$\begin{aligned}\Delta_6(z) = q &- 6q^2 + 9q^3 + 4q^4 + 6q^5 - 54q^6 - 40q^7 \\ &+ 168q^8 + 81q^9 - 36q^{10} - 564q^{11} + 36q^{12} + 638q^{13} \\ &+ 240q^{14} + 54q^{15} - 1136q^{16} + 882q^{17} - 486q^{18} \\ &- 556q^{19} + 24q^{20} + \cdots. \end{aligned} \tag{20}$$

7. A Basis for the Theta-Functions

Let $\mathcal{M}_n$ be the complex vector space spanned by the theta-functions of all self-dual $\mathscr{E}$-lattices in $\mathbb{C}^n$, and let $\mathcal{M} = \bigoplus_{n=0}^{\infty}\mathcal{M}_n$, a graded ring.

THEOREM 8.

$$\dim_{\mathbb{C}}\mathcal{M}_n = 1 + \left[\frac{n}{6}\right], \tag{21}$$

$$\sum_{n=0}^{\infty}\lambda^n\dim_{\mathbb{C}}\mathcal{M}_n = \frac{1}{(1-\lambda)(1-\lambda^6)}. \tag{22}$$

Proof. If $\Theta(z)\in\mathcal{M}_n$ let $\Psi(z) = \Theta(2z/3^{1/2})$ so that from Corollary 2

$$\Psi(z+3^{1/2}) = \Psi(z), \qquad \Psi\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^n\Psi(z).$$

Hence $\Psi(z)\in\mathcal{M}(3^{1/2}, n, 1)$, in the notation of Ogg [32, p. xiv]. Then (21) follows from Ogg [32, p. I-23, Theorem 3 with $q = 6$], and (22) is immediate.

THEOREM 9. $\mathcal{M} = \mathbb{C}[\Theta_{\mathscr{E}}(z), \Delta_6(z)]$ *where* $\Theta_{\mathscr{E}}(z)$, $\Delta_6(z)$ *are given by* (13), (19). *Therefore the theta-function of a self-dual* $\mathscr{E}$*-lattice in* $\mathbb{C}^n$ *can be written*

$$\Theta_\Lambda(z) = \sum_{r=0}^{[n/6]} c_r\Theta_{\mathscr{E}}(z)^{n-6r}\,\Delta_6(z)^r, \tag{23}$$

for uniquely determined integers c_r.

Proof. Since $\Theta_{\mathscr{E}}(z) \in \mathscr{M}_1$ and $\Delta_6(z) \in \mathscr{M}_6$ are algebraically independent this follows immediately from Eq. (22).

Remarks. (i) Equation (6) may be verified for $\Theta_{\mathscr{E}}(z)$ and $\Delta_6(z)$ using (8), (9) and (12).

(ii) A modification of [32, p. I-32] shows that $E_6(3z/2) - \frac{1}{27}E_6(z/2) \in \mathscr{M}_6$, where $E_6(z)$ denotes the Eisenstein series $1 - 504\Sigma\sigma_5(m)\, q^{2m}$ ([32, p. I-28; 35, p. 93]). This leads to the identity

$$27E_6\left(\frac{3z}{2}\right) - E_6\left(\frac{z}{2}\right) = 26\Theta_{\mathscr{E}}(z)^6 - 432\Delta_6(z). \tag{24}$$

Theorem 9 is an analog of the classical result that the theta-function of an even unimodular lattice is an element of $\mathbb{C}[E_4(z), \Delta(z)]$, where $E_4(z)$ is an Eisenstein series and $\Delta(z) = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24} = \sum_{m=0}^{\infty} a_m q^{2m}$, the a_m being the Ramanujan numbers (see for example [6, Theorems 5, 6; 7; or 40]). Just as the Ramanujan numbers are multiplicative [15, p. 68, Corollary 5; 32, p. II-15] so are the coefficients of $\Delta_6(z)$. More precisely, let $\Delta_6(z) = \sum_{m=1}^{\infty} a_m q^m$ and let $\phi_6(s)$ be the Dirichlet series

$$\phi_6(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad \mathrm{Re}(s) > 4. \tag{25}$$

THEOREM 10. *$\phi_6(s)$ has an Euler product*

$$\phi_6(s) = (1 - 9.3^s)^{-1} \prod_{p \neq 3} (1 - a^p p^{-s} + p^{5-2s})^{-1}, \tag{26}$$

and therefore the multiplication rule for the a_n is (compare (20))

$$a_m a_n = \prod_{3 \nmid d,\, d \mid (m,n)} d^5 a_{mn/d^2}\,. \tag{27}$$

Proof. From Corollary 2, $\Delta_6(2z)$ is the unique cusp form of weight 6 for $\Gamma_0(3)$. From [3, Lemma 27; 38, Sect. 3.5], $\Delta_6(2z)$ is an eigenfunction for the Hecke operators $T'(n)_{6,\psi}$ for all n, where $\psi(m) = 0$ if $3 \mid m$, $\psi(m) = 1$ if $3 \nmid m$. Then [38, Theorem 3.43] implies (26).

Suppose the coefficients $c_0, \ldots, c_\mu$, $\mu = [n/6]$, in (23) are chosen so as to make the q-expansion of the right-hand side begin

$$1 + A^*_{\mu+1} q^{\mu+1} + A^*_{\mu+2} q^{\mu+2} + \cdots. \tag{28}$$

The resulting series is called the *extremal theta-function* in dimension n (cf. [30]), and a lattice with this theta-function (if one exists) is called an *extremal lattice*. The examples $\mathscr{E}^n$ $(1 \leqslant n \leqslant 5)$ and $\Lambda(Q_6)$ are extremal lattices in dimensions 1-6. Examples for $n - 8$, 10 are provided by the lattices $\Lambda(E_8)$ (or Example 6 below) and $\Lambda(E_{10})$ (or $\Lambda(B_{10})$), using codes defined in [27]. For other examples with $n \leqslant 12$ see [14a]. The methods of [30] may be applied here, and show among other things that:

THEOREM 11. *For all* n, $A^*_{\mu+1} > 0$, *and so a self-dual* $\mathscr{E}$*-lattice has* $d \leqslant 1 + [n/6]$. *However, for all sufficiently large* n, $A^*_{\mu+2} < 0$, *and no extremal self-dual lattice exists in* $\mathbb{C}^n$.

Remark. The complex version of the Leech lattice is an $\mathscr{E}$-lattice in $\mathbb{C}^{12}$ with $\Delta = V_{24}$, $\tau = 196560$, but is not self-dual [8, 14a, 23].

8. CONSTRUCTION B

Let $\mathscr{C}$ be a linear code over $GF(4)$ of length n, dimension k, and minimum distance 8, satisfying $\mathscr{C} \subset \mathscr{C}^\perp$ and such that the all-ones vector is in $\mathscr{C}$. The latter is not a serious restriction in view of Corollary 9 of [27]. These assumptions imply that if $\mathbf{u} \in \mathscr{C}$ contains i 1's, j ω's and k ω^2's, then $i \equiv j \equiv k \equiv 0 \pmod 2$.

Construction B

With $\mathscr{C}$ as above, let $\mathscr{L}(\mathscr{C})$ consist of all $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{C}^n$ such that (i) $\sigma(\mathbf{x}) \in \mathscr{C}$, and (ii) $\sum_{i=1}^n x_i \in 4\mathscr{E}$.

The following facts are now easily verified: $\mathscr{L}(\mathscr{C})$ is an $\mathscr{E}$-lattice in $\mathbb{C}^n$ with $\det \mathscr{L}(\mathscr{C}) = 2^{n-k+1}$, $\rho = 2^{1/2}$, $\Delta = V_{2n} 2^{2k-2} 3^{-n/2}$, and $\tau = 192 A_8^{(b)} + 64 A_8 + 6n(n-1)$, where A_8 is the total number of codewords in $\mathscr{C}$ of weight 8, and $A_8^{(b)}$ is the number with 8 1's and $(n-8)$ 0's. There is a formula for the theta-function of $\mathscr{L}(\mathscr{C})$, analogous to but more complicated than Theorem 7. We omit the details.

EXAMPLE 6. The code $\{0^8, 1^8, \omega^8, (\omega^2)^8\}$ produces an extremal lattice in $\mathbb{C}^8$ with $\tau = 720$ and $\Delta_{16} \cdot 3^{-4}$.

EXAMPLE 7. The code S_{18} given in [27] produces a lattice in $\mathbb{C}^{18}$ with $\Delta = V_{36} 2^{16} 3^{-9} \approx 3.330 V_{36}$. The corresponding real lattice in $\mathbb{R}^{36}$ also has $\Delta \approx 3.330 V_{36}$, and appears to be the densest lattice yet found in this dimension. On the other hand $\tau < 189000$, compared with the present record of 234456 [21]. Incidentally an extremal lattice in $\mathbb{C}^{18}$ would have $\tau = 646380$.

Remark. One may also define the coordinate array of a point in $\mathscr{E}^n$, and hence generalize Construction C of [20, 21, 39] to $\mathscr{E}$-lattices.

ACKNOWLEDGMENTS

I should like to thank J.-M. Goethals, S. P. Lloyd, A. M. Odlyzko and J. J. Seidel for valuable discussions and helpful suggestions, and C. L. Mallows for finding the direct proof of Eq. (15). Some of the theta-functions were calculated on MACSYMA [31].

References

1. E. F. Assmus, Jr. and H. F. Mattson, Jr., Coding and combinatorics, *SIAM Rev.* **16** (1974), 349–388.
2. E. F. Assmus, Jr., H. F. Mattson, Jr., and R. J. Turyn, "Research to Develop the Algebraic Theory of Codes," Report AFCRL-67-0365, Air Force Cambridge Res. Labs., Bedford, Mass., June 1967.
3. A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.
4. R. Bellman, "A Brief Introduction to Theta Functions," Holt, Rinehart & Winston, New York, 1961.
5. N. Bourbaki, "Groupes et Algèbres de Lie," Chaps. IV–VI, Hermann, Paris, 1968.
6. M. Broué, Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratique entières définies positives à discriminant +1, pp. 71–108 *in* "Comptes Rendus des Journées Mathématiques de la Société Mathématique de France," Univ. Sci. Tech. Languedoc, Montpellier, 1974.
7. M. Broué and M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, *Ann. Sci. École Norm. Sup.* **5** (1972), 157–181.
8. J. H. Conway, private communication.
9. H. S. M. Coxeter, Extreme forms, *Canad. J. Math.* **3** (1951), 391–441.
10. H. S. M. Coxeter, "Regular Complex Polytopes," Cambridge Univ. Press, Cambridge, 1974.
11. H. S. M. Coxeter and J. A. Todd, An extreme duodenary form, *Canad. J. Math.* **5** (1953), 384–392.
12. P. Delsarte, J. M. Goethals, and J. J. Seidel, Bounds for systems of lines, and Jacobi polynomials, *Philips Res. Rep.* **30** (1975), 91*–105*.
13. H. Dym and H. P. McKean, "Fourier Series and Integrals," Academic Press, New York, 1972.
14. W. Feit, On integral representations of finite groups, *Proc. London Math. Soc.* (3) **29** (1974), 633–683.

14a. W. Feit, Some lattices over $Q(\sqrt{-3})$, *J. Algebra* **52** (1978), 248–263.

15. R. C. Gunning, "Lectures on Modular Forms," Princeton Univ. Press, Princeton, N.J., 1962.
16. C. M. Hamill, On a finite group of order 6,531,840, *Proc. London Math. Soc.* (2) **52** (1951), 401–454.
17. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 3rd ed., Oxford Univ. Press, Oxford, 1954.
18. J. Igusa, "Theta Functions," Springer–Verlag, New York, 1972.
19. J. Leech and N. J. A. Sloane, New sphere packings in dimensions 9-15, *Bull. Amer. Math. Soc.* **76** (1970), 1006–1010.
20. J. Leech and N. J. A. Sloane, New sphere packings in more than thirty-two dimensions, *in* "Proceedings of the Second Chapel Hill Conference on Combinatorial Mathematics and Applications," pp. 345–355, Chapel Hill, N.C. 1970.
21. J. Leech and N. J. A. Sloane, Sphere packings and error-correcting-codes, *Canad. J. Math.* **23** (1971), 718–745.
22. J. Lewittes, Construction of modular forms, *Israel J. Math.* **24** (1976), 145–183.
23. J. H. Lindsey II, A correlation between $PSU_4(3)$, the Suzuki group, and the Conway group, *Trans. Amer. Math. Soc.* **157** (1971), 189–204.
24. L. H. Loomis, "An Introduction to Abstract Harmonic Analysis," Van Nostrand, Princeton, N.J., 1953.

25. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79–94.
26. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Information Theory* **18** (1972), 794–805.
27. F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, Self-dual codes over *GF*(4), *J. Combinatorial Theory*, to appear.
28. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
29. D. P. Maher, "Self-Orthogonal Codes and Modular Forms," Ph.D. Thesis, Lehigh University, Bethlehem, Pa., 1976.
30. C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, Upper bounds for modular forms, lattices, and codes, *J. Algebra* **36** (1975), 68–76.
31. Mathlab Group, MACSYMA Reference Manual, Project MAC, M.I.T., Cambridge, Mass., Version 8, 1975.
32. A. Ogg, "Modular Forms and Dirichlet Series," Benjamin, New York, 1969.
33. H. Rademacher, "Topics in Analytic Number Theory," Springer–Verlag, New York, 1973.
34. C. A. Rogers, "Packing and Covering," Cambridge Univ. Press, Cambridge, 1964.
35. J.-P. Serre, "A Course in Arithmetic," Springer–Verlag, New York, 1973.
36. G. C. Shephard, Unitary groups generated by reflections, *Canad. J. Math.* **5** (1953), 364–383.
37. G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.
38. G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," Iwanami Shoten, Japan, and Princeton Univ. Press, Princeton, N.J., 1971.
39. N. J. A. Sloane, Sphere packings constructed from BCH and Justesen codes, *Mathematika* **19** (1972), 183–190.
40. N. J. A. Sloane, Binary codes, lattices, and sphere-packings, *in* "Combinatorial Surveys," (P. J. Cameron, Ed.), pp. 117–164. Academic Press, New York, 1977.
41. J. Tannery and J. Molk, Éléments de la théorie des Fonctions Elliptiques, 2nd ed., 4 vols., reprinted Chelsea, New York, 1972.
42. J. A. Todd, The invariants of a finite collineation group in five dimensions, *Proc. Cambridge Philos. Soc.* **46** (1950), 73–90.
43. E. T. Whittaker and G. N. Watson, "A Course of Modern Analysis," 4th ed., Cambridge Univ. Press, Cambridge, 1963.