JOURNAL OF ALGEBRA **105**, 443–450 (1987)

Lattices with Theta Functions for $G(\sqrt{2})$ and Linear Codes

H.-G. QUEBBEMANN

Mathematisches Institüt der Universität, Einsteinstrasse 62, D-4400 Münster, Federal Republic of Germany

Communicated by Walter Feit

Received October 12, 1984

Modular hermitian lattices over $\mathbb{Z}[i]$ and, in particular, unimodular lattices over $\mathbb{Z}[e^{\pi i/4}]$ give rise to modular forms for Hecke's group $G(\sqrt{2}) = \langle \left(\begin{smallmatrix}1 & \sqrt{2}\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right) \rangle$. Two general constructions of such lattices are performed, using codes over $\mathbb{F}_2$ and $\mathbb{F}_9$. Lattices with an extremal theta-function (i.e., with the largest minimum that Hecke's theory allows) are obtained in $\mathbb{C}^{2n}$ for all $n < 12$, including the densest known sphere-packings of $\mathbb{R}^{4n}$ for $n = 1, 4$, and 8. © 1987 Academic Press, Inc.

1. INTRODUCTION

The Hecke modular group $G(\lambda)$ is the subgroup of $SL_2(\mathbb{R})$ generated by $\left(\begin{smallmatrix}1 & \lambda\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$, cf. [4] or [9, Chap. I]. There are three distinguished cases in the range $0 < \lambda < 2$, namely $\lambda = 2\cos \pi/q = 1, \sqrt{2}, \sqrt{3}$ $(q = 3, 4, 6)$, where the space $\mathcal{M}_k(\lambda)$ of modular forms of weight $k \in (4/(q-2))\mathbb{N}$ has dimension $1 + [k/12]$, $1 + [k/8]$, and $1 + [k/6]$, respectively. It is well known that theta functions of even unimodular lattices in $\mathbb{R}^{2k}$ belong to $\mathcal{M}_k(1)$, and the existence of the famous Leech lattice is connected with $\dim \mathcal{M}_k(1) = 2$ for $k = 12$; cf. [11, Chap. VII, Sect. 6]. A similar relation between unimodular $\mathbb{Z}[\omega]$-lattices in unitary spaces, where $\omega = e^{2\pi i/3}$, and modular forms for $G(\sqrt{3})$ has been observed by Sloane [12]. Following his track we shall consider the case $\lambda = \sqrt{2}$ here.

Modular forms for $G(\sqrt{2})$ arise from definite $(1+i)$-modular $\mathbb{Z}[i]$-lattices, $i = \sqrt{-1}$. Viewed as $\mathbb{Z}$-lattices in $\mathbb{R}^{2k}$ these are even and have discriminant 2^k (k must be even). The D_4 root lattice in $\mathbb{R}^4$ carries such a structure, and so does the dense Barnes–Wall lattice in $\mathbb{R}^{16}$ (cf. [1]), whose presence is explained by $\dim \mathcal{M}_8(\sqrt{2}) = 2$. But in contrast with the case $\lambda = \sqrt{3}$, $k = 12$ (cf. Feit's classification [2]), there still exists an "extremal" $\mathbb{Z}[i]$-lattice in $\mathbb{R}^{32}$ corresponding to $\dim \mathcal{M}_{16}(\sqrt{2}) = 3$. The associated dense sphere-packing was constructed already in [10]; its contact number now is forced to be 261120 by the shape of $\mathcal{M}_{16}(\sqrt{2})$.

0021-8693/87 $3.00

481/105/2-11

The three lattices mentioned above all admit an isometric action of a square root of i. In this situation the modular hermitian form over $\mathbb{Z}[i]$ comes from a unimodular hermitian form over $\mathbb{Z}[\varepsilon]$, $\varepsilon = e^{\pi i/4}$, combined with a certain "trace" $\mathbb{Q}(\varepsilon) \to \mathbb{Q}(i)$. Due to the facts that $\langle \varepsilon \rangle \cong \mathbb{F}_9^{\bullet}$ and $\mathbb{Z}[\varepsilon]/(3) \cong \mathbb{F}_9 \times \mathbb{F}_9$, with complex conjugation transposing the two factors, a unimodular $\mathbb{Z}[\varepsilon]$-lattice is quite naturally constructed from a linear code over $\mathbb{F}_9$ and its dual. In particular, the $k = 16$ extremal lattice arises from the [8, 2] (resp. [8, 6]) Reed–Solomon code. A formula is given for the theta function of a lattice in terms of a joint weight enumerator of its two codes.

2. Lattices over $\mathbb{Z}[i]$

2.1. *Preliminaries*

Let V be a complex vector space of finite dimension k endowed with a positive definite hermitian inner product $\langle v, w \rangle$. A $\mathbb{Z}[i]$-submodule L of V is called a $\mathbb{Z}[i]$-*lattice* if it is generated by a basis of V. The *dual* lattice $L^{\#}$ consists of all $v \in V$ such that $\langle v, L \rangle \subset \mathbb{Z}[i]$, and is the same as the $\mathbb{Z}$-dual of L with respect to the real inner product Re $\langle v, w \rangle$. Let det L denote the determinant of the hermitian $k \times k$ matrix formed by the (complex) inner products in a $\mathbb{Z}[i]$-basis of L. If $L \subset L^{\#}$ then $(\det L)^2$ is the cardinality of $L^{\#}/L$. The *minimum squared length* of L is

$$\min L = \min\{\langle v, v \rangle \mid v \in L, v \neq 0\}.$$

The spheres of radius $\frac{1}{2}(\min L)^{1/2}$ centered at the points of L form a *packing* of V whose *contact number* $\tau(L)$ is the number of $v \in L$ with $\langle v, v \rangle = \min L$.

2.2. *Modular Lattices*

If the lattice L is equal to $\delta L^{\#}$, where $\delta \in \mathbb{Z}[i]$, then L is called δ-*modular*. This means that $\langle v, w \rangle$ lies in the principal ideal (δ) of $\mathbb{Z}[i]$ for all $v, w \in L$, and $\det L = |\delta|^k$, $k = \dim V$. If $L = \delta L^{\#}$, then also $L = (\delta^{-1} L)^{\#} = \delta^* L^{\#}$, where the star denotes complex conjugation. This implies $(\delta) = (\delta^*)$, hence $(\delta) = (d)$ or $(\delta) = ((1+i)\, d)$ for some $d \in \mathbb{N}$. We see that there are just two essentially different cases: $\delta = 1$ and $\delta = 1 + i$; the second case will be of interest here. From $L \subset (1+i)\, L^{\#}$ it follows that $\langle v, v \rangle \in (1+i) \cap \mathbb{Z}$ is *even* for all $v \in L$. The *theta function* of L is then defined by

$$\theta_L(z) = \sum_{v \in L} e^{\pi i z \langle v, v \rangle / \sqrt{2}} = \sum_{m=0}^{\infty} r_L(m)\, q^m, \qquad q = e^{\sqrt{2}\pi i z}.$$

It is a holomorphic function on the complex half plane Im $z > 0$. Of course here $r_L(m)$ is the number of representations $2m = \langle v, v \rangle$, $v \in L$.

THEOREM 1. *Let L be a $(1+i)$-modular $\mathbb{Z}[i]$-lattice.*

(a) *The dimension k is even.*

(b) *The theta function satisfies*

(i) $\theta_L(z+\sqrt{2}) = \theta_L(z)$,

(ii) $\theta_L(-1/z) = (iz)^k \theta_L(z)$.

Proof. (a) is obvious since $\det L = |1+i|^k = 2^{k/2}$ must be in $\mathbb{Z}$. $\theta_L(z)$ is a function of $q = e^{\sqrt{2}\pi i z}$, hence (i). Furthermore, $L = (1+i) L^{\#}$ implies $\theta_L(z) = \theta_{L^{\#}}(2z)$. By the transformation formula for real lattices (cf. [11, Chap. VII, Sect. 6]),

$$\theta_{L^{\#}}(2z) = (\det L)(i/\sqrt{2}z)^k\, \theta_L\left(-\frac{1}{z}\right) = \left(\frac{i}{z}\right)^k \theta_L\left(-\frac{1}{z}\right).$$

This proves (ii).

For $k = 2n$ let $\mathcal{M}_k$ be the vector space of all holomorphic functions $f(z)$, Im $z > 0$, which satisfy the conditions (i), (ii) of Theorem 1 and have no negative terms in their q-expansion, i.e., $f(z)$ is a *modular form of weight k* for the group generated by

$$\begin{pmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

THEOREM 2 (Hecke [4]; cf. [9, I–23]). $\dim \mathcal{M}_k = 1 + [k/8]$.

EXAMPLE 1. We set $V = \mathbb{C}^2$, $\langle (v_1, v_2), (w_1, w_2) \rangle = v_1 w_1^* + v_2 w_2^*$, and let L_1 be the $\mathbb{Z}[i]$-lattice generated by $(1, 1)$ and $(1, i)$. The matrix of inner products is $\left(\begin{smallmatrix} 2 & 1-i \\ 1+i & 2 \end{smallmatrix}\right)$, hence L_1 is $(1+i)$-modular. The corresponding sphere-packing of $\mathbb{R}^4$ is usually denoted by D_4. With $\sigma(m) =$ sum of the positive divisors of $m \in \mathbb{N}$ we have for odd m and $l \geqslant 0$ (cf. [5]),

$$r_{L_1}(2^l m) = 24\sigma(m).$$

2.3. *Root Lattices*

Suppose $L \subset (1+i) L^{\#}$. The *root system* of L is the set $R(L) = \{v \in L \mid \langle v, v \rangle = 2\}$. For example, $R(L_1)$ has 24 elements. On the other hand, a root system $R(L)$ is said to be of *standard type* if it is a (possibly empty) union of pairwise orthogonal four-element sets $\{\pm w, \pm iw\}$. If $R(L)$ is of standard type, it has $r_L(1) = 4j$ elements, where $0 \leqq j \leqq k$. Examples will be obtained in the next section.

THEOREM 3. *A $\mathbb{Z}[i]$-lattice $L \subset (1+i)L^{\#}$ has an orthogonal decomposition $L = L^{(1)} \perp L^{(2)}$, where $L^{(1)} \cong L_1 \perp \cdots \perp L_1$ and $R(L^{(2)})$ is of standard type.*

Proof. Let v, w be two nonproportional roots, and put $\beta = \langle v, w \rangle$. Since $1+i$ divides β and $\begin{pmatrix} 2 & \beta \\ \beta^* & 2 \end{pmatrix}$ must be positive definite, we have $\beta = 0$ or $\beta = \pm(1 \pm i)$. In the second case v and w generate a $\mathbb{Z}[i]$-lattice isometric to L_1. Being $(1+i)$-modular this splits off.

COROLLARY. *Any $(1+i)$-modular $\mathbb{Z}[i]$-lattice of dimension $k \leq 6$ is isometric to L_1, $L_1 \perp L_1$, or $L_1 \perp L_1 \perp L_1$.*

Proof. Otherwise $\mathcal{M}_k$ would contain two different theta functions, but this would contradict Theorem 2.

2.4. *Lattices from Binary Codes* (Cf. [13, Sect. 5.5])

A subspace C of $\mathbb{F}_2^k$ is called a *linear binary code*. The *dual code* $C^{\perp}$ consists of all $x \in \mathbb{F}_2^k$ such that $x \cdot y = 0$ for all $y \in C$, where $x \cdot y = x_1 y_1 + \cdots + x_k y_k$. If $C \subset C^{\perp}$, then C is called *self-orthogonal*, and if $C = C^{\perp}$, then C is called *self-dual*. The *weight* $\mathrm{wt}(x)$ is the number of nonzero components of x, and

$$\min \mathrm{wt}(C) = \min\{\mathrm{wt}(x) \mid x \in C, x \neq 0\}.$$

Two codes are *equivalent* if they can be transformed into each other by a permutation of the components. Using the isomorphism $\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2$ one associates to C the $\mathbb{Z}[i]$-lattice

$$L(C) = \{v \in \mathbb{Z}[i]^k \mid v \ (\mathrm{mod}\ 1+i) \in C\}$$

on $\mathbb{C}^k$, where $\langle v, w \rangle = v_1 w_1^* + \cdots + v_k w_k^*$ (Sloane's Construction A). It is clear that $L(C^{\perp}) = (1+i) L(C)^{\#}$, and equivalent codes yield equivalent (i.e., isometric) lattices. If $\min \mathrm{wt}(C) > 2$, then the canonical basis vectors of $\mathbb{C}^k$ multiplied by $\pm(1 \pm i)$ are precisely the roots of $L(C)$.

THEOREM 4. *This construction sets up a one-to-one correspondence between the classes of self-orthogonal (resp. self-dual) codes C in $\mathbb{F}_2^k$ with* $\min \mathrm{wt}(C) > 2$ *and the classes of k-dimensional $\mathbb{Z}[i]$-lattices L such that $L \subset (1+i)L^{\#}$ (resp. L is $(1+i)$-modular), $R(L)$ is of standard type, $r_L(1) = 4k$.*

Proof. If L is a lattice with these properties we can identify $K = ((1+i)/2)\, \mathbb{Z}R(L)$ with the standard lattice $\mathbb{Z}[i]^k$. Then L corresponds to the code $C = L/(1+i)K$. An isometry between two such lattices $L(C)$ and $L(D)$ stabilizes their root lattice $(1+i)\,\mathbb{Z}[i]^k$ and hence induces an equivalence between C and D.

The first example of a $(1+i)$-modular lattice as in Theorem 4 arises for $k=8$ from the extended Hamming code. There is a third and more interesting $(1+i)$-modular $\mathbb{Z}[i]$-lattice in $\mathbb{C}^8$ (cf. 3.3). Theorem 4 has been inspired by [14, Proposition 4].

3. Lattices over $\mathbb{Z}[e^{\pi i/4}]$

3.1. *Preliminaries*

We set $\varepsilon = e^{\pi i/4} = (1+i)/\sqrt{2}$, a primitive eighth root of unity. The ring $\mathbb{Z}[\varepsilon]$ is a principal ideal domain; cf. [3, p. 570]. It is naturally embedded in the algebra

$$A = \mathbb{Z}[\varepsilon] \otimes \mathbb{R} \cong \mathbb{R}[X]/(X^4+1) \cong \mathbb{C} \times \mathbb{C}.$$

Let the automorphism $\alpha \mapsto \alpha'$ of A be defined by $\varepsilon' = \varepsilon^3$; it permutes the two factors of A. The automorphism $\alpha \mapsto \alpha^*$ of A is defined by $\varepsilon^* = \varepsilon^{-1}$; it is complex conjugation on either factor. We shall identify $\mathbb{C}$ with the subfield $\mathbb{Z}[i] \otimes \mathbb{R}$ of A consisting of all $\alpha = \alpha'$. With this convention a functional $t\colon A \to \mathbb{C}$ is defined by

$$t(\alpha) = \operatorname{trace}_{\mathbb{Q}(\varepsilon)/\mathbb{Q}(i)}(\alpha/(2-\sqrt{2})) = 2\beta + (1+i)\,\gamma$$

for $\alpha \in \mathbb{Z}[\varepsilon]$, $\alpha = \beta + \gamma\varepsilon$, where $\beta, \gamma \in \mathbb{Z}[i]$. The following property is easily checked.

PROPOSITION 1. *An element $\alpha \in A$ satisfies $t(\alpha\mathbb{Z}[\varepsilon]) \subset (1+i)\,\mathbb{Z}[i]$ if and only if $\alpha \in \mathbb{Z}[\varepsilon]$.*

Let V be a finitely generated free A-module endowed with a hermitian form $h\colon V \times V \to A$ with respect to $*$, and let h be totally positive definite, i.e., for $v \neq 0$ both components of $h(v, v) \in \mathbb{R} \times \mathbb{R}$ are positive. A $\mathbb{Z}[\varepsilon]$-submodule L of V is an *integral* $\mathbb{Z}[\varepsilon]$*-lattice* if it is generated by an A-basis of V and satisfies $h(L, L) \subset \mathbb{Z}[\varepsilon]$. It is a *unimodular* $\mathbb{Z}[\varepsilon]$-lattice if, in addition, $h(v, L) \subset \mathbb{Z}[\varepsilon]$ for $v \in V$ implies $v \in L$.

COROLLARY. *L is an integral (resp. unimodular) $\mathbb{Z}[\varepsilon]$-lattice if and only if, as a $\mathbb{Z}[i]$-lattice with respect to the $\mathbb{C}$-valued inner product $\langle v, w\rangle = t(h(v, w))$, it satisfies $L \subset (1+i)\,L^{\#}$ (resp. is $(1+i)$-modular).*

In particular, the $\mathbb{Z}[i]$-lattice L_1 of example 1 can be identified with $\mathbb{Z}[\varepsilon]$ itself, where $h(\alpha, \beta) = \alpha\beta^*$ for $\alpha, \beta \in A$. The $\mathbb{Z}[i]$-basis $1, \varepsilon$ gives the matrix $\left(\begin{smallmatrix} 2 & 1-i \\ 1+i & 2 \end{smallmatrix}\right)$.

3.2. *Reduction Modulo* 3.

Denoting the image of i in $\mathbb{F}_9 = \mathbb{Z}[i]/(3)$ by i again, we have the reduction homomorphism $\alpha \mapsto \bar{\alpha}$ from $\mathbb{Z}[\varepsilon]$ onto $\mathbb{F}_9 \times \mathbb{F}_9$ defined by

$\bar{\varepsilon} = (1-i, -1+i)$. Now * will also denote the nontrivial automorphism of $\mathbb{F}_9$ as well as the automorphism $(b, c) \mapsto (c^*, b^*)$ of $\mathbb{F}_9 \times \mathbb{F}_9$ which is induced by complex conjugation in $\mathbb{Z}[\varepsilon]$. The functional t induces the functional $\bar{t}(b, c) = (1-i)\, b + (1+i)\, c$ on $\mathbb{F}_9 \times \mathbb{F}_9$.

PROPOSITION 2. *For each $a \in \mathbb{F}_9 \times \mathbb{F}_9$ with $\bar{t}(aa^*) = 2$ (resp. $= 1$), there is a unique $\alpha \in \mathbb{Z}[\varepsilon]$ with $\bar{\alpha} = a$, $t(\alpha\alpha^*) = 2$ (resp. $= 4$). For each $a \in \mathbb{F}_9 \times \mathbb{F}_9$, $a \neq (0, 0)$ with $\bar{t}(aa^*) = 0$, there are precisely three elements $\alpha \in \mathbb{Z}[\varepsilon]$ with $\bar{\alpha} = a$, $t(\alpha\alpha^*) = 6$.*

Proof. We have to investigate reduction mod 3 on the hermitian $\mathbb{Z}[i]$-lattice L_1. Two different nonzero vectors of squared length at most 4 cannot be congruent mod 3, hence these 48 vectors of L_1 are mapped bijectively to the 48 anisotropic vectors of $L_1/3L_1$. This also implies that the $\mathbb{Z}[i]$-automorphism group of L_1 is mapped isomorphically onto the unitary group $U_2(\mathbb{F}_9)$. Then it is clear how the 96 vectors $v \in L_1$ of squared length 6 reduce to the 32 nonzero isotropic vectors mod 3.

For $a \in \mathbb{F}_9 \times \mathbb{F}_9$ we define $\theta_a(z) = \sum e^{\pi i z t(\alpha\alpha^*)/3\sqrt{2}}$ for $\operatorname{Im} z > 0$, where the summation extends over all $\alpha \in \mathbb{Z}[\varepsilon]$ with $\bar{\alpha} = a$. For $a \neq (0, 0)$ this function only depends on the value $\bar{t}(aa^*)$, and we have $\theta_{(0,0)}(z) = \theta_{L_1}(3z)$.

3.3. *Lattices from Nonary Codes.*

The definitions concerning codes over $\mathbb{F}_9$ are the same as in 2.4, except that now equivalence is defined with respect to monomial matrices [7, p. 238], and for $x, y \in \mathbb{F}_9^n$ the inner product is $x \cdot y = x_1 y_1^* + \cdots + x_n y_1^*$. Let $p_0(x, y)$ be the number of positions $v \in \{1, \ldots, n\}$ at which $x_v = y_v = 0$, and for $j = 1, 2, 3$, let $p_j(x, y)$ be the number of positions at which $a_v = (x_v, y_v)$ is $\neq (0, 0)$, $\bar{t}(a_v a_v^*) = 2j \pmod 3$. The partition $(p_0(x, y), p_1(x, y), p_2(x, y), p_3(x, y))$ of n is called the *type* of (x, y), and the number $p(x, y) = \sum j p_j(x, y)$ will play the role of a "weight." Note that $p(x, y)$ is a multiple of 3 if $x \cdot y = 0$.

Let B and C be linear codes of length n over $\mathbb{F}_9$. The numbers of pairs $(x, y) \in B \times C$ of fixed type are the coefficients of the polynomial

$$P_{B,C}(T_0, T_1, T_2, T_3) = \sum_{x \in B} \sum_{y \in C} \prod_{j=0}^{3} T_j^{p_j(x,y)}$$

a kind of "joint weight enumerator" (cf. [7, p. 147]) in four indeterminates. With $V = A^n$, $h(v, w) = \frac{1}{3}(v_1 w_1^* + \cdots + v_n w_n^*)$, we now associate to B and C the $\mathbb{Z}[\varepsilon]$-lattice

$$L(B, C) = \{v \in \mathbb{Z}[\varepsilon]^n \mid \bar{v} \in B \times C\},$$

where $\bar{v} = (\overline{v_1}, \ldots, \overline{v_n})$ is viewed as an element of $\mathbb{F}_9^n \times \mathbb{F}_9^n$. Obviously the dual of $L(B, C)$ with respect to h is $L(C^\perp, B^\perp)$. Equivalent codes B give rise to equivalent lattices $L(B, B^{\perp})$. As before, the theta function is defined with respect to the hermitian form $\langle v, w\rangle = t(h(v, w))$.

THEOREM 5. *Let the codes B and C be orthogonal to each other.*

(a) *$L(B, C)$ is an integral $\mathbb{Z}[\varepsilon]$-lattice; it is a unimodular $\mathbb{Z}[\varepsilon]$-lattice if and only if $C = B^{\perp}$.*

(b) *$\theta_{L(B,C)}(z) = P_{B,C}(\theta_{(0,0)}(z), \theta_{(1,1)}(z), \theta_{(1,2)}(z), \theta_{(1,0)}(z))$. In particular, the first coefficients are*

$$r_{L(B,C)}(m) = \sum_{\substack{(x,y)\in B\times C\\ p(x,y)=3m}} 3^{p_3(x,y)} + \begin{cases} 0 & \text{for } m = 1, 2,\\ 24n & \text{for } m = 3.\end{cases}$$

Proof. Part (a) follows from the preceding remarks. The expression for the theta function is obtained in the usual way; cf. [12, p. 174]. The last formula follows directly from Proposition 2.

EXAMPLE 2. For $n \geq 4$ we set $L_n = L(B, B^{\perp})$ where $B \subset \mathbb{F}_9^n$ is the "repetition" code consisting of all $(b, b,..., b)$, $b \in \mathbb{F}_9$. Since $\mathrm{wt}(x) > 3$ for $x \in B$, $x \neq 0$, and $\mathrm{wt}(y) > 1$ for $y \in B^{\perp}$, $y \neq 0$, we have $p(x, y) > 3$ for all $(x, y) \neq (0, 0)$. It follows that $\min L_n = 4$. In particular, $L_4 \subset \mathbb{R}^{16}$ is the dense lattice packing Λ_{16} of [1] with

$$\theta_{L_4}(z) = 1 + 4320q^2 + 61440q^3 + \cdots.$$

3.4. *Extremal Lattices*

In $\mathcal{M}_8$ we have the (unique normalized) cusp form

$$\Delta_4(z) = \tfrac{1}{96}(\theta_{L_1}(z)^4 - \theta_{L_4}(z)) = q - 8q^2 + 12q^3 + \cdots.$$

(One can prove that $\Delta_4(z) = q\prod_{m=1}^{\infty}(1-q^m)^8(1-q^{2m})^8$.) For $k = 2n$, $\mu = [k/8]$, the functions $\theta_{L_1}(z)^{n-4\nu}\Delta_4(z)^{\nu}$ with $0 \leqslant \nu \leqslant \mu$ are a basis of $\mathcal{M}_k$ (see Theorem 2). Hence there is a unique

$$f(z) = 1 + r_{\mu+1}q^{\mu+1} + r_{\mu+2}q^{\mu+2} + \cdots \in \mathcal{M}_k.$$

After Sloane, a $(1+i)$-modular $\mathbb{Z}[i]$-lattice will be called *extremal* if it has this modular form as its theta function. For example, L_1, L_1^2, L_1^3, L_4, L_5, L_6, L_7 are extremal. Next, for $n = 8$ the modular form in question is

$$\begin{aligned} f(z) &= \theta_{L_1}(z)^8 - 192\theta_{L_1}(z)^4\Delta_4(z) + 576\Delta_4(z)^2\\ &= 1 + 261120q^3 + \cdots. \end{aligned}$$

EXAMPLE 3. (cf. [10]). Let B be the two-dimensional Reed–Solomon (RS) code in $\mathbb{F}_9^8$ (cf. [7, p. 303]), i.e., B is generated by $(1, 1,..., 1)$ and

$(\eta, \eta^2, ..., 1)$, where $\eta = 1 + i$ generates the multiplicative group of $\mathbb{F}_9$. Since $\min \cdot \mathrm{wt}(B) = 7$, $\min \cdot \mathrm{wt}(B^\perp) = 3$, we have $p(x, y) > 6$ for all $x \in B$, $y \in B^\perp$, $(x, y) \neq (0, 0)$. *Hence* $M = L(B, B^\perp)$ *is extremal.* (This would not be true if we used a Reed–Solomon code of dimension 3 or 4.) The contact number $\tau(M) = 261120$ can also be obtained directly from Theorem 5. One finds that $B \times B^\perp$ has 448 elements of type $(5, 0, 0, 3)$, 36288 elements of type $(1, 6, 0, 1)$, 108864 elements of type $(1, 5, 2, 0)$, 31104 elements of type $(0, 7, 1, 0)$, and these are just the types of pairs (x, y) with $p(x, y) = 9$.

It is clear that the construction of Section 3.3 can lead to extremal lattices only for $n < 12$. Furthermore, for $n \geqq 8$ the code B must be at least two-dimensional, and if $\dim B = 2$ it is necessary and sufficient to have $\min \cdot \mathrm{wt}(B) = n - 1$ as in Example 3. Up to equivalence there are unique such two-dimensional codes for $n = 8$, 9, and 10 (Extensions of the above RS code). There is none for $n = 11$, but here we can use a three-dimensional code B obtained, for example, by puncturing twice the $[13, 3, 9]$ code $H^\perp \otimes \mathbb{F}_9$, where H is the Hamming code of length 13 over $\mathbb{F}_3$ (cf. [6, p. 58]). Thus we have constructed extremal lattices in $\mathbb{C}^{2n}$ for all $n < 12$. By the method of [8] it may be proved that this could not be done in large n.

References

1. J. H. Conway and N. J. A. Sloane, Laminated lattices, *Ann. Math.* **116** (1982), 593–620.
2. W. Feit, Some lattices over $\mathbb{Q}(\sqrt{-3})$, *J. Algebra* **52** (1978), 248–263.
3. H. Hasse, "Zahlentheorie," Adademie–Verlag, Berlin, 1969.
4. E. Hecke, Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung, *Math. Ann.* **112** (1936), 664–699; Math. Werke, pp. 591–626, Vandenhoeck und Ruprecht, Göttingen, 1959.
5. A. Hurwitz, Über die Zahlentheorie der Quaternionen, *Nachr. Akad. Wiss. Göttingen II Math. Phys. Kl.* (1896), 313–340; Math. Werke II, pp. 303–330, Birkhäuser Verlag, Basel–Suttgart, 1963.
6. J. H. van Lint, "Introduction to Coding Theory," Springer–Verlag, Berlin/Heidelberg/New York, 1982.
7. F. J. MacWilliams and N. J. A. Sloane, "The theory of Error-Correcting Codes," North–Holland, Amsterdam, 1977.
8. 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.
9. A. Ogg, "Modular Forms and Dirichlet Series," Benjamin, New York, 1969.
10. H.-G. Quebbemann, A construction of integral lattices, *Mathematika* **31** (1984), 138–141.
11. J.-P. Serre, "A course in Arithmetic," Springer–Verlag, Berlin/Heidelberg/New York, 1973.
12. N. J. A. Sloane, Codes over $\mathbb{F}_4$ and complex lattices, *J. Algebra* **52** (1978), 168–181.
13. N. J. A. Sloane, Self-dual codes and lattices, *in* "Relations between Combinatorics and Other Parts of Mathematics," pp. 273–308, Proc. Symp. Pure Math., Vol. 34, Amer. Math. Soc., Providence, R.I., 1979.
14. B. B. Venkov, On the classification of integral even unimodular 24-dimensional quadratic forms, *Proc. Steklov Inst. Math.* **4** (1980), 63–74.