PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 133, Number 3, Pages 661–670
S 0002-9939(04)07724-X
Article electronically published on September 20, 2004

CODES OVER GF(4) AND $\mathbf{F}_2 \times \mathbf{F}_2$ AND HERMITIAN LATTICES OVER IMAGINARY QUADRATIC FIELDS

KOK SENG CHUA

(Communicated by Wen-Ching Winnie Li)

Abstract. We introduce a family of bi-dimensional theta functions which give uniformly explicit formulae for the theta series of hermitian lattices over imaginary quadratic fields constructed from codes over $\mathbf{GF}(\mathbf{4})$ and $\mathbf{F}_2 \times \mathbf{F}_2$, and give an interesting geometric characterization of the theta series that arise in terms of the basic strongly ℓ modular lattice $\mathbf{Z} + \sqrt{\ell}\mathbf{Z}$. We identify some of the hermitian lattices constructed and observe an interesting pair of non-isomorphic 3/2 dimensional codes over $\mathbf{F}_2 \times \mathbf{F}_2$ that give rise to isomorphic hermitian lattices when constructed at the lowest level 7 but nonisomorphic lattices at higher levels. The results show that the two alphabets $\mathbf{GF}(\mathbf{4})$ and $\mathbf{F}_2 \times \mathbf{F}_2$ are complementary and raise the natural question as to whether there are other such complementary alphabets for codes.

1. Introduction

There is a well-known (mod 2) construction for constructing lattices from linear codes, which maps self-dual codes to unimodular lattices. It also gives an isomorphism between the invariant ring of polynomials for the weight enumerators and the appropriate space of modular forms for the theta series of the constructed lattices. The first result appears in [3] for a self-dual binary code and unimodular lattice. Sloane, in [6] extended this correspondence to codes over $\mathbf{GF}(\mathbf{4})$ and lattices over the Eisenstein integers $\mathbf{Z}[(-1+\sqrt{-3})/2]$. It is clear that one can extend this to other imaginary quadratic fields, but one needs to distinguish between the two cases where the level ℓ is either 3 or 7 mod 8 (see [1]) corresponding to the cases where the prime ideal (2) either stays prime or splits, and this corresponds to codes over $\mathbf{GF}(\mathbf{4})$ and the ring $\mathbf{F}_2 \times \mathbf{F}_2$ respectively.

In this note, we introduce a one-parameter family of bi-dimensional theta functions (see section 3) which give explicitly the theta series of the level ℓ ($\ell \equiv 3$ mod 4) hermitian lattices constructed from codes over the two alphabets when they are substituted into the weight enumerator of the codes (Theorem 5.2). It is interesting to note that they are given by the same form for the two rather different alphabets. We also make the interesting observation (which seems not to have been spelt out explicitly before) that the theta series that occur for level ℓ can be characterized geometrically as the theta series of the even sublattice, the odd part and the shadow

Received by the editors March 3, 2003 and, in revised form, October 29, 2003.
2000 *Mathematics Subject Classification.* Primary 11H71, 94B75; Secondary 11H31.
Key words and phrases. Codes over rings, Hermitian lattices, theta series.

of the basic two-dimensional strongly ℓ modular (see [13]) lattice $\mathbf{Z}+\sqrt{\ell}\mathbf{Z}$. In the lowest levels 3 and 7, we note that there is an additional symmetry (in the form of equality of some of the theta functions) that reduces Theorem 5.2 to the simpler result of Sloane [18] and the 7-modular case in [5].

In view of our result, it is natural to ask if there are other such complementary alphabets for codes where the theta series of the constructed lattices can be parameterized uniformly. One possible hint would be to look for alphabets where the MacWilliams Identities are identical (see Lemma 4.2).

We note that some of our bi-dimensional theta series were introduced in [4], [5] where a generalized Jacobi Identity was given and used to give two new quadratically convergent algorithms for computing π analogous to those based on the AGM. A more extensive higher-dimensional generalization of these theta functions and the Jacobi Identity has also been given in [6]. Note that our results give a way of constructing explicit bi-dimensional theta identities (which was our original motivation) from every self-dual code, for example by using Cor. 5.6.

Finally in section 6, we constructed some hermitian lattices from some well-known self-dual codes over $\mathbf{GF}(\mathbf{4})$ and $\mathbf{F}_2\times\mathbf{F}_2$, and by computing their theta series, we can identify some of them on Schulze-Pillot's data base [15]. Our constructions give the extremal ℓ modular lattice of minimum norm 4 (see [13]) for level 3 (Coxeter-Todd) and level 7 (Craig's $A_6^{(2)}$) from the well-known 3-dimensional hexacode over $\mathbf{GF}(\mathbf{4})$ and a dimension 3/2 code over $\mathbf{F}_2\times\mathbf{F}_2$ observed in [5]. We also note in section 6, Example 4, an interesting pair of nonisomorphic codes over $\mathbf{F}_2\times\mathbf{F}_2$ which give isomorphic lattices $\mathbf{Z}[(-1+\sqrt{-7})/2]^3$ in level 7 but nonisomorphic lattices at higher levels.

2. Hermitian lattices over imaginary quadratic fields

Let $\ell>0$ be a square-free integer, let $K=\mathbf{Q}(\sqrt{-\ell})$ be the imaginary quadratic field with discriminant d_K, let $\mathcal{O}_K$ be its ring of integers, and let $x\to\bar{x}$ denote complex conjugation. The left K-vector space K^n is endowed with the hermitian inner product $(z,z')_K:=\sum_{i=1}^n z_i\bar{z_i'}$, which we also denote simply by $z.\bar{z'}$. A hermitian lattice Λ over K is an $\mathcal{O}_K$-submodule of K^n of full rank . Note that Λ need not be a free module in general. The ring of integers $\mathcal{O}_K$ will play the same role for these lattices as $\mathbf{Z}$ plays for the usual Euclidean lattices. In particular, the hermitian dual is defined by

$$\Lambda^*:=\{x:x\in K^n|(x,\Lambda)_K\subset\mathcal{O}_K\}, \tag{2.1}$$

and we say that Λ is self-dual (or unimodular) if $\Lambda=\Lambda^*$.

If Λ is a Hermitian lattice in K^n, there is a corresponding real lattice Λ_{real} in $\mathbf{R}^{2n}$, via the natural embedding of K in $\mathbf{C}=\mathbf{R}^2$:

$$\Lambda_{real}=\{(Re(z_1),Im(z_1),...,Re(z_n),Im(z_n)):(z_1,...,z_n)\in\Lambda\}.$$

In the case that Λ is a free $\mathcal{O}_K$-module (e.g. when the class number $h(K)=1$), we can associate a Gram matrix $G(\Lambda)$ for every $\mathcal{O}_K$ basis $\{v_1,v_2,...,v_n\}$ given by $G(\Lambda)=(v_i.\bar{v_j})_{i,j=1}^n$, and a determinant invariant $det\Lambda:=det(G)$ defined up to squares of units in $\mathcal{O}_K$. More generally if Λ is integral (as in our case here), namely $\Lambda\subset\Lambda^*$, we may take $det(\Lambda)$ to be the order of the finite group Λ^*/Λ.

We have

$$det\Lambda_{real} = \frac{|d_K|^n}{2^{2n}}(det\Lambda)^2. \tag{2.2}$$

We note that in this case, Λ is self-dual if and only if $G(\Lambda)$ has $\mathcal{E}_\ell$ (see below) entries and $det\Lambda = 1$, and $\sqrt{2}\Lambda_{real}$ will be $|d_K|$-modular in $\mathbf{R}^{2n}$ in the sense of [11], [12]. (Note that by (2.2) we have $det(\sqrt{2}\Lambda_{real}) = |d_K|^n$, which gives the correct determinant for a $2n$-dimensional $|d_K|$-modular lattice.)

The theta series of an $\mathcal{E}_\ell$-lattice Λ in K^n is given by

$$\theta_\Lambda(\tau) = \sum_{z\in\Lambda} e^{\pi i\tau z.\bar{z}}, \tag{2.3}$$

where $\tau \in H = \{z \in \mathbf{C} : Im(z) > 0\}$ and this agrees with the real theta series $\theta_{\Lambda_{real}}(\tau)$.

3. Bi-dimensional theta functions to the base ℓ

Let d be a positive integer, $\ell = 4d-1 \equiv 3 \; mod \; 4$. Let $K = \mathbf{Q}(\sqrt{-\ell})$ as before so that its ring of integers $\mathcal{E}_\ell = \mathbf{Z}[w_\ell]$, where $w_\ell = \frac{-1+\sqrt{-\ell}}{2}$ satisfies $w_\ell^2 + w_\ell + d = 0$. Let $Q_d(x,y) = |x - yw_\ell|^2 = x^2 + xy + dy^2 = (x + \frac{y}{2})^2 + \frac{\ell^2 y^4}{4}$ be the (principal) norm form of K. The ring $\mathcal{E}_\ell/2\mathcal{E}_\ell$ is isomorphic to either $\mathbf{GF(4)}$ or $\mathbf{F}_2 \times \mathbf{F}_2$ depending on whether ℓ is 3 or 7 mod 8. In either case, a complete set of coset representatives is given by $\{0, 1, w_\ell, 1 + w_\ell\}$. Let $q = e^{\pi i\tau}$ and consider the following bi-dimensional theta series for the four cosets:

$$A_d(q) := \theta_{2\mathcal{E}_\ell}(\tau) = \sum_{m,n\in\mathbf{Z}} q^{4Q_d(m,n)}, \tag{3.1}$$

$$C_d(q) := \theta_{1+2\mathcal{E}_\ell}(\tau) = \sum_{m,n\in\mathbf{Z}} q^{4Q_d(m+1/2,n)}, \tag{3.2}$$

$$G_d(q) := \theta_{w_\ell+2\mathcal{E}_\ell}(\tau) = \sum_{m,n\in\mathbf{Z}} q^{4Q_d(m,n+1/2)}, \tag{3.3}$$

$$H_d(q) := \theta_{1+w_\ell+2\mathcal{E}_\ell}(\tau) = \sum_{m,n\in\mathbf{Z}} q^{4Q_d(m+1/2,n+1/2)}. \tag{3.4}$$

The level ℓ theta functions $A_d(q), C_d(q)$ were introduced recently in [4],[5],[6] where they occurred in a generalized Jacobi Identity which was used to derive two new quadratically converging algorithms for computing π analogous to those based on the AGM. Note that $\theta_{\mathcal{E}_\ell}(\tau) = A_d(q^{1/4})$. These theta series can be further expressed explicitly in terms of the standard one (real) dimensional theta series and its shadow,

$$\theta_3(q) = \sum_{m\in\mathbf{Z}} q^{m^2}, \tag{3.5}$$

$$\theta_2(q) = \sum_{m\in\mathbf{Z}} q^{(m+1/2)^2} = \sum_{m\in\mathbf{Z}+1/2} q^{m^2}. \tag{3.6}$$

We have

Lemma 3.1.

$$A_d(q) = \theta_3(q^4)\theta_3(q^{4\ell}) + \theta_2(q^4)\theta_2(q^{4\ell}), \tag{3.7}$$

$$C_d(q) = \theta_2(q^4)\theta_3(q^{4\ell}) + \theta_3(q^4)\theta_2(q^{4\ell}), \tag{3.8}$$

$$G_d(q) = H_d(q) = \frac{\theta_2(q)\theta_2(q^\ell)}{2}. \tag{3.9}$$

Proof. (3.7), (3.8) were proven in [4], Lemma 2.1. The somewhat surprising (3.9) can be proven analogously by showing that both G_d and H_d are given by the RHS of (3.9) by completing squares and noting that

$$\sum_{m\in\mathbf{Z}} q^{(4m+1)^2} = \sum_{m\in\mathbf{Z}} q^{(4m+3)^2} = \theta_2(q^4)/2.$$

□

These are all theta functions to the base (level) ℓ. We now give a geometric interpretation of these theta series which seems to be of interest. Recall that the lattice $\mathbf{Z}+\sqrt{\ell}\mathbf{Z}$ is the basic strongly ℓ-modular 2-dimensional lattice [13]. Our next observation is that all the coset theta series are derivable from that of $\mathbf{Z}+\sqrt{\ell}\mathbf{Z}$. We also note that this is in fact a very general fact which has a generalization to higher-dimensional odd diagonal lattices (see [6]).

Lemma 3.2. *$A_d(q)$ (resp. $C_d(q)$) are the theta series of the even sublattice (resp. odd part) of $\mathbf{Z}+\sqrt{\ell}\mathbf{Z}$. $2G_d(q) = 2H_d(q) = \theta_{(\mathbf{Z}+1/2)+\sqrt{\ell}(\mathbf{Z}+1/2)}(\tau)$ is the theta series of the shadow of $\mathbf{Z}+\sqrt{\ell}\mathbf{Z}$.*

Proof. By (3.7), (3.8), we have $A_d(q)+C_d(q) = (\theta_3(q^4)+\theta_2(q^4))(\theta_3(q^{4\ell})+\theta_2(q^{4\ell})) = \theta_3(q)\theta_3(q^\ell) = \theta_{\mathbf{Z}+\sqrt{\ell}\mathbf{Z}}(\tau)$ by (22) on p.104 of [8]. The first statement follows from the fact that $A_d(q)$ is even and $C_d(q)$ is odd by (3.1), (3.2). (Note that isospectral lattices in dimension two are isomorphic.) The second part follows from (3.9). □

We next define two more associated level ℓ theta series which we will need later.

Lemma 3.3.

$$B_d(q) := \sum_{m,n\in\mathbf{Z}} (-1)^{m-n} q^{Q_d(m,n)} = \theta_3(-q)\theta_3(-q^\ell), \tag{3.10}$$

$$E_d(q) := \sum_{m,n\in\mathbf{Z}} (-1)^{n} q^{Q_d(m,n)} = \theta_3(q)\theta_3(q^\ell) - \theta_2(q)\theta_2(q^\ell). \tag{3.11}$$

Proof. (3.10) has been proven in [5]. A similar method (completing the square) proves (3.11). □

We note that the functions A_d, B_d, C_d are related by a Jacobi Identity $A_d(q)^2 = B_d(q^2)^2 + C_d(q)^2$; see [4], [5] and a generalized higher-dimensional version in [6].

Lemma 3.4.

$$A_d(q) + C_d(q) - 2G_d(q) = E_d(q). \tag{3.12}$$

Proof. By Lemma 3.1, the LHS is $(\theta_3(q^4)+\theta_2(q^4))(\theta_3(q^{4\ell})+\theta_2(q^{4\ell})) - 2G_d(q) = \theta_3(q)\theta_3(q^\ell) - \theta_2(q)\theta_2(q^\ell) = E_d(q)$. □

4. Codes over $\mathbf{GF(4)}$ and $\mathbf{F}_2 \times \mathbf{F}_2$ and their weight enumerators

Let $\mathbf{GF(4)} = \{0, 1, \omega, \omega^2\}$, where $\omega^2 + \omega + 1 = 0$, be the finite field of 4 elements. The conjugate of $x \in \mathbf{GF(4)}$ is $\bar{x} = x^2$ and is an involution since $x^4 = x$, $\forall\, x \in \mathbf{GF(4)}$. In order to give a uniform treatment, we will represent $\mathbf{F}_2 \times \mathbf{F}_2$ (see [5]) by the ring $\mathbf{R_4} = \mathbf{F}_2 + \omega\mathbf{F}_2$ where $\omega^2 = \omega$. This ring contains two maximal ideals (ω) and $(\omega + 1)$ and $\mathbf{R_4}/(\omega), \mathbf{R_4}/(\omega + 1)$ are both $\mathbf{F}_2$ so that $\mathbf{R_4} = (\omega) \oplus (\omega + 1)$ by the Chinese Remainder Theorem. An explicit isomorphism is given by

$$\omega a + (\omega + 1)b \to (a, b), \quad a, b \in \mathbf{F}_2.$$

The natural conjugation in $\mathbf{R_4}$, which we denote again by $x \to \bar{x}$, is the map that fixes $\mathbf{F}_2$ and swaps ω and $\omega + 1$. Note that in both cases, we have $\bar{\omega} = \omega + 1$.

Now we let $\mathcal{R}$ denote either the ring $\mathbf{R_4}$ or $\mathbf{GF(4)}$. A linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is simply an $\mathcal{R}$-submodule of $\mathcal{R}^n$. Note that in the case of $\mathbf{GF(4)}$ it is a linear subspace of $\mathbf{GF(4)}^n$. The (hermitian) dual code is $\mathcal{C}^\perp := \{u \in \mathcal{R}^n : u.\bar{v} = \sum_j u_j \bar{v}_j = 0, \forall v \in \mathcal{C}\}$ and $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$. Self-dual codes over $\mathbf{GF(4)}$ up to length 16 have been classified in [7]. They are necessarily even (all words have even weight). Some self-dual codes over $\mathbf{R_4}$ were constructed in [1]. They are in general not free submodules but we recall the following useful criteria for generating self-dual codes over $\mathbf{R_4}$ which follow easily from the remarks in [1] :

Lemma 4.1. *If R is a binary linear code and $R^\perp$ its binary dual, then $\omega R \oplus (1 + \omega)R^\perp$ is a self-dual code over $\mathbf{R_4}$.*

For a codeword $u = (u_1, u_2, ..., u_n) \in \mathcal{R}^n$ and an $\alpha \in \mathcal{R}$, we define the counting function $n_\alpha(u) = \#\{j : u_j = \alpha\}$. Next for an $\mathcal{R}$ code $\mathcal{C}$, we define the complete weight enumerator (*cwe*) to be

$$cwe_{\mathcal{C}}(X, Y, Z, W) := \sum_{u \in \mathcal{C}} X^{n_0(u)} Y^{n_1(u)} Z^{n_\omega(u)} W^{n_{\omega+1}(u)}, \tag{4.1}$$

and in view of Lemma 3.1, a symmetrized weight enumerator *swe* to be

$$swe_{\mathcal{C}}(X, Y, Z) := cwe_{\mathcal{C}}(X, Y, Z, Z), \tag{4.2}$$

and finally by a further contraction, we have the Hamming weight enumerator

$$W_{\mathcal{C}}(X, Y) = swe_{\mathcal{C}}(X, Y, Y). \tag{4.3}$$

Next we note the following MacWilliams Identity, which is identical for both $\mathbf{GF(4)}$ and $\mathbf{F}_2 \times \mathbf{F}_2$ codes:

Lemma 4.2.

$$swe_{\mathcal{C}^\perp}(X, Y, Z) = \frac{1}{|\mathcal{C}|} swe_{\mathcal{C}}(X + Y + 2Z, X + Y - 2Z, X - Y). \tag{4.4}$$

Proof. The case of $\mathbf{GF(4)}$ is given in [14], p. 19, while the $\mathbf{F}_2 \times \mathbf{F}_2$ case is covered in Theorem 4.2 of [1]. □

5. Constructing Hermitian lattices from codes over $\mathbf{GF(4)}$ and $\mathbf{F}_2 \times \mathbf{F}_2$

Throughout ℓ will be a positive square-free integer with $\ell \equiv 3 \ mod\ 4$, $K = \mathbf{Q}(\sqrt{-\ell})$ the quadratic field with discriminant $d_K = -\ell$ and $\mathcal{E}_\ell = \mathbf{Z}[w_\ell]$ its ring of algebraic integers. We have to distinguish between two cases. If $\ell \equiv 3 \ mod\ 8$ so that $d = (\ell + 1)/4$ is odd, and $d_K \equiv 5 \ mod\ 8$, $\left(\frac{-\ell}{2}\right) = -1$, $2\mathcal{E}_\ell$ remains a prime

ideal in $\mathcal{E}_\ell$, and its residual field $\mathcal{E}_\ell/2\mathcal{E}_\ell$ is isomorphic to $\mathbf{GF(4)}$. If $\ell \equiv 7 \ mod\ 8$, $d = (\ell+1)/4$ is even, and $\left(\frac{-\ell}{2}\right) = 1$, $2\mathcal{E}_\ell$ splits in $\mathcal{E}_\ell$ so that $\mathcal{E}_\ell/2\mathcal{E}_\ell \cong \mathbf{F}_2 \times \mathbf{F}_2 \cong \mathbf{R_4}$.

In both cases, we may take $0, 1, w_\ell, 1 + w_\ell$ as coset representatives for $2\mathcal{E}_\ell$ in $\mathcal{E}_\ell$, and there is an isomorphism mapping $2\mathcal{E}_\ell$ to 0, $1 + 2\mathcal{E}_\ell$ to 1, $w_\ell + 2\mathcal{E}_\ell$ to ω, and $1 + w_\ell + 2\mathcal{E}_\ell$ to $1 + \omega$ since the relation $w_\ell^2 + w_\ell + d = 0$ is preserved by $\omega^2 + \omega + d \equiv 0 \ mod\ 2$ in $\mathcal{R}$. Hence there is a map $\rho_\ell : \mathcal{E}_\ell \to \mathcal{E}_\ell/2\mathcal{E}_\ell \to \mathcal{R}$ that sends $w_\ell^r \in \mathcal{E}_\ell$ onto $\omega^r \in \mathcal{R}$ $(r = 0, 1, 2)$. Note that ρ_ℓ respects conjugation, i.e. $\rho_\ell(\bar{z}) = \overline{\rho_\ell(z)}$ since $\bar{w}_\ell = -1 - w_\ell \equiv 1 + w_\ell \ mod\ 2\mathcal{E}_\ell$. We now define the following standard construction:

CONSTRUCTION A (level ℓ): Let $\mathcal{R}$ be the ring $\mathbf{GF(4)}$ if $\ell \equiv 3 \ mod\ 8$, or the ring $\mathbf{R_4} \cong \mathbf{F}_2 \times \mathbf{F}_2$ when $\ell \equiv 7 \ mod\ 8$. Letting $\mathcal{C}$ be a linear code over $\mathcal{R}$ of length n and dimension k, we define $\Lambda_\ell(\mathcal{C}) := \{x \in {\mathcal{E}_\ell}^n : \rho_\ell(x) \in \mathcal{C}\}$. In other words, $\Lambda_\ell(\mathcal{C})$ consists of all vectors in ${\mathcal{E}_\ell}^n$ which when taken mod $2\mathcal{E}_\ell$ componentwise are in $\rho_\ell^{-1}(\mathcal{C})$.

Note that we omit the usual scaling by $\sqrt{2}$ so that $\Lambda_\ell(\mathcal{C})$ is always integral and is a union of cosets. We choose this normalization because it brings out the geometric meaning of the theta series in our main Theorem 5.2 below. The following usual consequence is immediate.

Lemma 5.1. (i) *$\Lambda_\ell(\mathcal{C})$ is an $\mathcal{E}_\ell$-lattice.* (ii) $\Lambda_\ell(\mathcal{C}^\perp) = 2\Lambda_\ell(\mathcal{C})^*$. (iii) *$\mathcal{C}$ is self-dual if and only if $\Lambda_\ell(\mathcal{C})/\sqrt{2}$ is self-dual. In this case $\Lambda_\ell(\mathcal{C})_{real}$ is $2n$-dimensional even, and ℓ-modular if the different of K is principal.*

Proof. (i) $\Lambda_\ell(\mathcal{C})$ is a submodule of ${\mathcal{E}_\ell}^n$ follows from $\mathcal{C}$ is a submodule of $\mathcal{R}^n$. (ii) For $a + 2z_1, b + 2z_2 \in \Lambda_\ell(\mathcal{C})$, $\langle (a + 2z_1)/2, b + 2z_2\rangle \in (\sum a_i\bar{b}_i)/2 + \mathcal{E}_\ell \in \mathcal{E}_\ell$ if and only if $a.\bar{b} = 0$ in $\mathcal{C}$. (iii) follows from (ii) and the fact that $(\Lambda_\ell(\mathcal{C})_{real})^* = {\mathcal{D}_K}^{-1}\Lambda_\ell(\mathcal{C})^*$ where ${\mathcal{D}_K}^{-1}$ is the inverse different of O_K (see [2]). □

We now state our main result:

Theorem 5.2. *Let $\ell \equiv 3 \ mod\ 4$, let $\mathcal{C}$ be a code over $\mathbf{GF(4)}$ or $\mathbf{R_4}$ accordingly, and let $\Lambda_\ell(\mathcal{C})/\sqrt{2}$ be the hermitian lattice constructed via the construction Λ_ℓ above. Then we have*

$$\theta_{\Lambda_\ell(\mathcal{C})}(\tau) = swe_{\mathcal{C}}(A_d(q), C_d(q), G_d(q)), \tag{5.1}$$

where the three theta functions $A_d(q), C_d(q), G_d(q)$ are respectively the theta series of the even sublattice, the odd part, and half the shadow of the strongly ℓ-modular lattice $\mathbf{Z} + \sqrt{\ell}\mathbf{Z}$.

Proof. It is clear that $\theta_{\Lambda_\ell(\mathcal{C})}$ can be expressed as the *cwe* of the theta series of the cosets of $2\mathcal{E}_\ell$ since $\theta_{\Lambda_\ell(\mathcal{C})}(\tau) = \sum_{u\in\mathcal{C}} \theta_{\Lambda_\ell(u)}(\tau)$, where $\theta_{\Lambda_\ell(u)}(\tau) = \sum_{x\in u+2{\mathcal{E}_\ell}^n} e^{\pi i\tau x.\bar{x}}$, splits further into a product

$$\prod_j \sum_{x\in u_j+2\mathcal{E}_\ell} q^{x.\bar{x}} = \theta_{2\mathcal{E}_\ell}(\tau)^{n_0(u)}\theta_{1+2\mathcal{E}_\ell}(\tau)^{n_1(u)}\theta_{w_\ell+2\mathcal{E}_\ell}(\tau)^{n_\omega(u)}\theta_{1+w_\ell+2\mathcal{E}_\ell}(\tau)^{n_{1+\omega}(u)}.$$

Therefore we must have $\theta_{\Lambda_\ell(\mathcal{C})}(\tau) = cwe_{\mathcal{C}}(A_d(q^2), C_d(q^2), G_d(q), H_d(q))$ by (3.1)-(3.4). (5.1) follows immediately from the symmetry $G_d(q) = H_d(q)$, in (3.9). The geometric interpretation follows from Lemma 3.2. □

Note that Theorem 5.2 can be thought of as an explicit version of the cases (3) and (5) of Proposition 2.1 of [1] in the case of an imaginary quadratic field. The

constructed lattices appear to be extremal only in the smallest levels $\ell = 3, 7$ since the minimal distances are fixed while by (2.2) the volumes increase with ℓ.

In the case of the two lowest levels $\ell = 3, 7$, there is an additional symmetry and there is a simpler version of (5.1). We recover Theorem 7 of Sloane [18] and an explicit form of [5], Theorem 3.2.

Corollary 5.3. *For $\ell = 3$, $d = 1$ and a $\mathbf{GF(4)}$ code $\mathcal{C}$, we have*

$$\theta_{\Lambda_3(\mathcal{C})}(\tau) = W_{\mathcal{C}}(A_1(q), C_1(q)). \tag{5.2}$$

Proof. This follows from the fact that when $\ell = 3, d = 1$, the norm form $Q_1(x, y) = x^2 + xy + y^2$ is symmetric in x and y, and by (3.2), (3.3), $G_d(q) = C_d(q)$. The result then follows from Theorem 5.2 and (4.3). □

Corollary 5.4. *For $\ell = 7$, $d = 2$ and an $\mathbf{F}_2 \times \mathbf{F}_2$ code, we have*

$$\theta_{\Lambda_7(\mathcal{C})}(\tau) = W_{\mathcal{C}}(A_2(q), C_2(q), A_2(\sqrt{q}) - A_2(q)). \tag{5.3}$$

Proof. This follows from the additional symmetry $G_2(q) = A_2(\sqrt{q}) - A_2(q)$, which follows from Lemma 4.3 and Proposition 4.4 of [5]. □

Corollary 5.5. *If $\mathcal{C}$ is an $[n, k]$ code over $\mathcal{R}$, then*

$$\theta_{2\Lambda_\ell(\mathcal{C})^*}(\tau) = \frac{1}{4^k} swe_{\mathcal{C}}(A_d(q^{1/4}), E_d(q), B_d(q)). \tag{5.4}$$

Proof. This follows from Lemma 5.1 (ii), (4.4) and the identity (6.1) below, (3.12) and the fact that $B_d(q) = \theta_{\mathbf{Z}+\sqrt{\ell}\mathbf{Z}}(-q) = A_d(q) - C_d(q)$. □

Corollary 5.6. *If a code $\mathcal{C}$ over $\mathcal{R}$ is self-dual, then*

$$swe_{\mathcal{C}}(A_d(q), C_d(q), G_d(q)) = \frac{1}{4^k} swe_{\mathcal{C}}(A_d(q^{1/4}), E_d(q), B_d(q)). \tag{5.5}$$

Proof. This is an immediate consequence of (5.4), Lemma 5.1(ii) and Theorem 5.2. □

6. Examples

(1) Let $R_1 = \{0, 1, \omega, \omega^2\}$ be the repetition code of length 1. Clearly then $swe_{R_1}(X, Y, Z) = X + Y + 2Z$ and also it is clear that $\Lambda_\ell(R_1) = R_1 + 2\mathcal{E}_\ell = \mathcal{E}_\ell$ since R_1 gives exactly the coset representatives of $2\mathcal{E}_\ell$ in $\mathcal{E}_\ell$. We have by Theorem 5.2,

$$A_d(q^{1/4}) = \theta_{\mathcal{E}_\ell}(\tau) = A_d(q) + C_d(q) + 2G_d(q). \tag{6.1}$$

(2) Let $c_2 = \{00, 11, \omega\omega, \omega^2\omega^2\}$ be the repetition code of length two, which is also the unique self-dual code of length 2 for both the rings $\mathcal{R}$. By Theorem 5.2, $\Lambda_\ell(\mathcal{C})/\sqrt{2}$ must be a hermitian lattice over $\mathbf{Q}(\sqrt{-\ell})$ of dimension 4. But by Table 1 in [17], for the two lowest levels $\ell = 3, 7$ this lattice is unique and must be ${\mathcal{E}_\ell}^2$. So we have $\Lambda_3(c_2) = c_2 + 2{\mathcal{E}_\ell}^2 = \sqrt{2}{\mathcal{E}_\ell}^2$. But this is actually true for all $\ell \equiv 3 \bmod 4$, by counting volume. Clearly $swe_{c_2}(X, Y, Z) = X^2 + Y^2 + 2Z^2$. So Theorem 5.2 implies the less obvious identities

$$A_d(\sqrt{q})^2 = A_d(q)^2 + C_d(q)^2 + 2G_d(q)^2. \tag{6.2}$$

It can be proven easily, using the formulae in terms of the one-dimensional theta functions (3.7)-(3.11), that (6.1),(6.2) actually holds for all odd ℓ, which are not

necessary square free. Note that $\Lambda_\ell(c_2)$ is ℓ-modular (if $h(\mathcal{E}_\ell)$ is one) with minimal norm 4 and Gram matrix $\begin{pmatrix} 2 & 1 \\ 1 & 2d \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2d \end{pmatrix}$.

(3) Let $C_3 = \omega\langle[1,1,1]\rangle + (1+\omega)\langle[1,1,1]\rangle^\perp$ be the 3-dimensional $\mathbf{R_4}$ code which is self-dual by Lemma 4.1 but is not a free submodule. We have $swe_{C_3}(X,Y,Z) = X^3 + Z^3 + 3XZ^2 + 3ZY^2$. By Theorem 5.2, for each $\ell \equiv 7 \bmod 8$, $\Lambda_\ell(C_3)/\sqrt{2}$ is a 3-dimensional hermitian lattice over $\mathbf{Q}(\sqrt{-\ell})$ with theta series

$$\theta_{\Lambda_\ell(C_3)}(\tau) = A_d(q)^3 + G_d(q)^3 + 3A_d(q)G_d(q)^2 + 3C_d(q)^2G_d(q).$$

We identify some of the hermitian lattices constructed with Schulze-Pillot's data base [15]:

- $\Lambda_7(C_3)$: [15] $D-7$ dim 3 #1, $\Lambda_7(C_3)/\sqrt{2}$ is the only other hermitian lattice over $\mathbf{Q}(\sqrt{-7})$ of dimension 3 other than $\mathcal{E}_7^3$ (which will be constructed as $\Lambda_7(C_{3,2})/\sqrt{2}$ below). $\Lambda_7(C_3)_{real}$ is the Craig lattice $A_6^{(2)}$, which is the unique extremal 7-modular lattice of minimal norm 4.
- $\Lambda_{15}(C_3)$: [15] $D-15$ dim 3.1 #2.
- $\Lambda_{23}(C_3)$: [15] $D-23$ dim 3 #15.
- $\Lambda_{31}(C_3)$: [15] $D-31$ dim 3 #19.
- $\Lambda_{39}(C_3)$: [15] $D-39$ dim 3.2 #10.

(4) Consider the following two codes over $\mathbf{R_4}$:

$$C_{3,2} = \omega\langle[0,1,1]\rangle + (\omega+1)\langle[0,1,1]\rangle^\perp, \tag{6.3}$$

$$C_{3,3} = \omega\langle[0,0,1]\rangle + (\omega+1)\langle[0,0,1]\rangle^\perp. \tag{6.4}$$

By Lemma 4.1 these are self-dual over $\mathbf{R_4}$. It is easy to enumerate by hand that there are eight code words so that the dimension of the code is $log_{|\mathbf{R_4}|}|C| = 3/2$. The weight enumerators are

$$\begin{aligned} swe_{C_{3,2}}(X,Y,Z) &= X^3 + X^2Z + XY^2 + 2XZ^2 + Y^2Z + 2Z^3, \\ swe_{C_{3,3}}(X,Y,Z) &= X^3 + 3X^2Z + 3XZ^2 + Z^3. \end{aligned}$$

As observed in [5],

$$\begin{aligned} swe_{C_{3,2}}(A_2(q), C_2(q), G_2(q)) &= swe_{C_{3,3}}(A_2(q), C_2(q), G_2(q)) \\ &= A_2(\sqrt{q})^3 = \theta_{\sqrt{2}\mathcal{E}_7^3}(\tau). \end{aligned}$$

We have from Schulze-Pillot's table:

- $\Lambda_7(C_{3,2}) = \Lambda_7(C_{3,3}) \cong \sqrt{2}\mathcal{E}_7^3$: [15] $D-7$ dim 3 #2.
- $\Lambda_{15}(C_{3,2}) \cong \sqrt{2}(\mathcal{E}_{15} \oplus \mathcal{E}_{15} \oplus \frac{1}{2}\mathcal{E}_{15})$: [15] $D-15$ dim 3.2 #4.
- $\Lambda_{15}(C_{3,3}) \cong \sqrt{2}(\frac{1}{2}\mathcal{E}_{15} \oplus \frac{1}{2}\mathcal{E}_{15} \oplus \frac{1}{2}\mathcal{E}_{15})$: [15] $D-15$ dim 3.2 #1.
- $\Lambda_{23}(C_{3,2}) \cong \sqrt{2}(\mathcal{E}_{23} \oplus \mathcal{E}_{23} \oplus \frac{1}{2}\mathcal{E}_{23})$: [15] $D-23$ dim 3 #18.
- $\Lambda_{23}(C_{3,3})$: [15] $D-23$ dim 3 #3 or #4.

So we have an interesting example of two non-isomorphic codes that give rise to equivalent lattices under construction Λ_7 but not under higher-level construction.

(5) Let e_6 be the self-dual [6,3,4] hexacode over $\mathbf{GF(4)}$ (see [18], Example 3) of length 6 generated by

$$e_6 = \begin{pmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{pmatrix}.$$

Then its symmetrized and Hamming weight enumerator polynomials are:

$$\begin{aligned} swe_{e_6}(X,Y,Z) &= X^6+Y^6+2Z^6+15(X^2+Y^2)Z^4+30X^2Y^2Z^2, \\ W_{e_6}(X,Y) &= X^6+45X^2Y^4+18Y^6. \end{aligned}$$

- $\ell = 3$: [15] D-3 dim=6 #1.
  $\Lambda_3(e_6)/\sqrt{2}$ is the 6-dimensional self-dual Eisenstein lattice U_6 in [9] whose real form $(\Lambda_3(e_6))_{real} \cong K_{12}$ is the extremal 3-modular Coxeter-Todd lattice with minimal norm 4 ([8] p.127) whose theta series is by Cor. 5.3, $\theta_{K_{12}}(z) = A_1(q)^6 + 45A_1(q)^2C_1(q)^4 + 18C_1(q)^6$.
- $\ell = 11$: [15] D-11 dim=6 #26.
- $\ell = 19$: [15] D-19 dim=6 #82.

(6) Let e_8 be the self-dual [8,4,4] $\mathbf{GF(4)}$ code (see [7]) generated by

$$e_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

$$swe_{e8}(X,Y,Z) = X^8+Y^8+14X^4Y^4+28X^4Z^4+168X^2Y^2Z^4+28Y^4Z^4+16Z^8.$$

- $\ell = 3$: [15] $D-3$ dim=8 # 1. This gives the 8-dimensional complex E_8 lattice ([9] Table 1) of minimal norm 4, kissing number 720 and automorphism group of size $2^{14}.3^6.5^2.7$. The real form is the 16-dimensional 3-modular lattice $A_2 \otimes E_8$, in Nebe-Sloane catalogue [10].
- $\ell = 11$: [15] $D-11$ dim=8 #59.

Acknowledgment

The author is very much indebted to Patrick Solé from whom he first learned of the two codes in Example 4.

References

1. C. Bachoc, Applications of coding theory to the construction of modular lattices, J. Combinatorial Theory, Ser. A, **78** (1997) 92-119. MR98a:11084
2. C. Bachoc, G. Nebe, Zonal functions for the unitary groups and applications to hermitian lattices, J. Number Theory, **96** (2002), No-1, 55-75. MR2003i:33016
3. M. Broué, M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, Ann. Sc. ENS **5** (1972) 157-181. MR48:3596
4. H. H. Chan, K. S. Chua, P. Solé, Quadratic Iterations to π associated with elliptic functions to the cubic and septic base, Trans. AMS **355** (2003), 1505-1520. MR2003j:33008
5. H. H. Chan, K. S. Chua, P. Solé, Seven-modular lattices and a septic base Jacobi Identity, Journal of Number Theory, Vol **99** No. 2, (2003), 361-372. MR2003m:11102
6. K. S. Chua, P. Solé, Jacobi Identities, modular lattices, and modular towers, to appear in European Journal of Combinatorics, **25** No. 4 (2004), 495–503.
7. J. Conway, V. Pless, N. Sloane, Self-Dual Codes over $GF(3)$ and $GF(4)$ of Length not Exceeding 16, IEEE Trans on Info. Theory, Vol IT-**25**, No 3, May 1979. MR80h:94026
8. J. Conway, N. Sloane, Sphere Packings, Lattices and Groups, 3rd Edition, Springer 1991. MR93h:11069
9. W. Feit, Some Lattices over $Q(\sqrt{-3})$, Journal of Algebra, **52** (1978),248-263. MR58:16534
10. Nebe-Sloane Catalogue of lattices, `http://www.research.att.com/ njas/lattices/P16.2.html`
11. H.-G. Quebbemann, Modular Lattices in Euclidean Spaces, Journal of Number Theory **54** (1995) , 190-202. MR96i:11072
12. H.- G. Quebbemann, Atkin-Lehner eigenforms and strongly modular lattices, L'Enseignement Mathématique, t. **43** (1997), 55-65. MR98g:11081

13. E. Rains, N. Sloane, The Shadow Theory of Modular and Unimodular Lattices, Journal of Number Theory, Vol **73** (1998), 359-389. MR99i:11053
14. E. Rains, N. Sloane, Self-Dual Codes, in Handbook of Coding Theory ed. V. Pless, W. Huffman, Amsterdam, Elsevier, (1998), pp 177-294. MR1667939
15. R. Schulze-Pillot, Genera of hermitian lattices over imaginary quadratic fields `http://www.math. uni-sb.de/ag-schulze/Hermitian-lattices/`
16. R. Scharlau, R. Schulze-Pillot, Extremal Lattices, Algorithmic algebra and number theory, Heidelberg, Springer, Berlin, (1999), 139-170. MR99m:11074
17. R. Scharlau, A. Schiemann, R. Schulze-Pillot, Theta Series of Modular, Extremal, and Hermitian Lattices, Integral quadratic forms and lattices (Seoul, 1998), 221-233, Contemp. Math., 249, Amer. Math. Soc., Providence, RI, 1999. MR2001a:11066
18. N. J. A. Sloane, Codes over $GF(4)$ and Complex Lattices, Journal of Algebra, **52** (1978), 168-181. MR58:9782

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543

E-mail address: `matcks@nus.edu.sg`

Current address: Software and Computing Programme, Institute of High Performance Computing, 1 Science Park Road, #01-01, The Capricorn, Singapore Science Park II, Singapore 117528

E-mail address: `chuaks@ihpc.a-star.edu.sg`