HILBERT MODULAR FORMS AND CODES OVER $\mathbf{F}_{p^2}$

JIM BROWN[1], BEREN GUNSOLUS[2], JEREMY LILLY[3], AND FELICE MANGANIELLO[4]

ABSTRACT. Let p be an odd prime and consider the finite field $\mathbf{F}_{p^2}$. Given a linear code $\mathcal{C} \subset \mathbf{F}_{p^2}^n$, we use algebraic number theory to construct an associated lattice $\Lambda_{\mathcal{C}} \subset \mathcal{O}_L^n$ for L an algebraic number field and $\mathcal{O}_L$ the ring of integers of L. We attach a theta series $\theta_{\Lambda_{\mathcal{C}}}$ to the lattice $\Lambda_{\mathcal{C}}$ and prove a relation between $\theta_{\Lambda_{\mathcal{C}}}$ and the complete weight enumerator evaluated on weight one theta series.

1. INTRODUCTION

Let p be a prime, $q = p^f$ and $\mathcal{C} \subset \mathbf{F}_q^n$ be an $[n, k]$-code, i.e., a k-dimensional $\mathbf{F}_q$-subspace of $\mathbf{F}_q^n$. Let $\mathcal{O}$ be a $\mathbf{Z}$-module and suppose we have a surjection $\Pi : \mathcal{O}^n \to \mathbf{F}_q^n$. For instance, one could take $f = 1$, $\mathcal{O} = \mathbf{Z}$, and Π to be the projection modulo p map in each coordinate. One obtains a lattice by considering $\Lambda_{\mathcal{C}} = \Pi^{-1}(\mathcal{C}) \subset \mathcal{O}^n$. Furthermore, one can associate a theta series $\theta_{\Lambda_{\mathcal{C}}}$ to the lattice $\Lambda_{\mathcal{C}}$. The relationship between the code $\mathcal{C}$, the lattice $\Lambda_{\mathcal{C}}$, and the theta series $\theta_{\Lambda_{\mathcal{C}}}$ can be exploited to use properties of one to prove results on the others. For example, one can show if $\Lambda \subset \mathbf{R}^n$ is an even unimodular lattice, then $n \equiv 0 \pmod 8$ by studying the associated theta series.

The relations between codes, lattices, and theta series have been studied by numerous authors. For instance, van der Geer and Hirzebruch studied the case of codes over $\mathbf{F}_p$, $\mathcal{O} = \mathbf{Z}[\zeta_p]$, and showed the associated theta series is a Hilbert modular form of full level $\mathrm{SL}_2(\mathbf{Z}[\zeta_p + \zeta_p^{-1}])$. They use these results to prove the theta series is the Lee weight enumerator polynomial of the code evaluated on various weight one theta series. One can see [7, Chapter 5] for a survey of this work. In [4], they use Hilbert Jacobi forms instead and prove results on the complete weight enumerator. Codes over $\mathbf{F}_4$ are studied in [2] in relation

Date: July 13, 2020.

2010 *Mathematics Subject Classification.* Primary 11F41, 06B99 , Secondary 05E99, 11T71.

Key words and phrases. Coding theory, lattices, theta series.

Part of this work was conducted during the 2018 REU at Clemson University. The authors would like to thank the NSF for support under DMS #1547399.

to Siegel Hilbert modular forms defined over $\mathbf{Q}(\sqrt{5})$. Taking p to be an odd prime and considering codes over $\mathbf{F}_{p^2}$ and $\mathbf{F}_p \times \mathbf{F}_p$, one can see [11, 12] in the context of imaginary quadratic fields and theta series defined over the imaginary quadratic field. There has been work done for codes defined over rings as well, see for example [1, 3, 5].

In this paper we study codes defined over $\mathbf{F}_{p^2}$ for p an odd prime, but rather than working with imaginary quadratic fields we consider the ring of integers $\mathcal{O}_L$ of $L = \mathbf{Q}(\zeta_p, \sqrt{D})$ for $D > 1$ square-free and p inert in $\mathbf{Q}(\sqrt{D})$. Given a code $\mathcal{C} \subset \mathbf{F}_{p^2}^n$, we study the arithmetic of $\mathcal{O}_L$ and use it to construct an even integral lattice $\Lambda_\mathcal{C} \subset \mathcal{O}_L^n$ and show that it is not unimodular. We construct theta series that are Hilbert modular forms and prove a relation between this theta series and the complete weight enumerator polynomial of the code evaluated on certain weight one theta series. We note that the weight one theta series are not algebraically independent, so our result is not optimal. Finding the appropriate generalized Lee weight and associated polynomial is the subject of future work.

2. Some algebraic number theory

In this section we give some of algebraic number theory results that are necessary for our lattice construction. Most of these results are fairly standard, but we collect them here in one section with references and proofs for the convenience of the reader. One can see [13] for more results on cyclotomic fields.

Let E/F be a Galois extension of number fields. Let $\mathcal{O}_E$ (resp. $\mathcal{O}_F$) denote the ring of integers of E (resp. F); it is a free $\mathcal{O}_F$-module of rank $m = [E : F]$. Let $\mathrm{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_m\}$. The trace map from E to F is a F-linear map defined by

$$\mathrm{Tr}_{E/F}(x) = \sum_{i=1}^{m} \sigma_i(x).$$

Moreover, $\mathrm{Tr}_{E/F}(\mathcal{O}_E) \subset \mathcal{O}_F$. The norm map from E to F is also a F-linear map; it is defined by

$$\mathrm{N}_{E/F}(x) = \prod_{i=1}^{m} \sigma_i(x).$$

Let $F = \mathbf{Q}$. The discriminant of the number field E is given by

$$\begin{aligned} \Delta_E &= \det(\mathrm{Tr}_{E/\mathbf{Q}}(x_i x_j)) \\ &= \det(\sigma_i(x_j))^2 \end{aligned}$$

where $\{x_1, \ldots, x_m\}$ is a $\mathbf{Z}$-basis of $\mathcal{O}_E$.

We will also make use of the different of a number field. Define

$$\mathcal{O}_E^\vee = \{x \in E : \mathrm{Tr}_{E/\mathbf{Q}}(xy) \in \mathbf{Z} \text{ for every } y \in \mathcal{O}_E\}.$$

The different of the number field E is given by

$$\mathfrak{D}_E = (\mathcal{O}_E^\vee)^{-1} = \{x \in E : xy \in \mathcal{O}_E \text{ for every } y \in \mathcal{O}_E^\vee\}$$

We now specialize to the case of interest for this paper. Fix an odd prime p and a positive square-free integer D so that p is inert in the field $K = \mathbf{Q}(\sqrt{D})$, i.e., so that $f(x) = x^2 - D$ is irreducible modulo p if $D \equiv 2, 3 \pmod 4$ or $f(x) = x^2 - x + (1-D)/4$ is irreducible modulo p if $D \equiv 1 \pmod 4$. Let $\mathcal{O}_K$ denote the ring of integers of K. In particular, we have $\mathcal{O}_K = \mathbf{Z}[\sqrt{D}]$ if $D \equiv 2, 3 \pmod 4$ and $\mathcal{O}_K = \mathbf{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ if $D \equiv 1 \pmod 4$. Let ζ_p be a primitive pth root of unity and set $L = \mathbf{Q}(\sqrt{D}, \zeta_p)$.

Proposition 2.1. *We have*

$$\mathcal{O}_L = \begin{cases} \mathbf{Z}[\sqrt{D}, \zeta_p] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbf{Z}\left[\frac{1+\sqrt{D}}{2}, \zeta_p\right] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Proof. In light of [13, Theorem 2.6], it only remains to show that $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$. As the degree of K over $\mathbf{Q}$ is two, we either have $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$ or $K \subset \mathbf{Q}(\zeta_p)$. However, as p is totally ramified in $\mathbf{Q}(\zeta_p)$ and inert in K, it cannot be that $K \subset \mathbf{Q}(\zeta_p)$. □

As noted in the previous proof, p is totally ramified in $\mathbf{Q}(\zeta_p)$. In particular, $p\mathbf{Z}[\zeta_p] = \langle 1 - \zeta_p \rangle^{p-1}$. Set $\mathfrak{p} = (1-\zeta_p)\mathcal{O}_L$. It is well-known that $\mathfrak{p} = (1-\zeta_p^a)\mathcal{O}_L$ for any integer a with $a \not\equiv 0 \pmod p$.

Proposition 2.2. *The ramification degree of $\mathfrak{p}$ over p is $p-1$ and the residue class degree is 2, i.e., $p\mathcal{O}_L = \mathfrak{p}^{p-1}$ and $\mathcal{O}_L/\mathfrak{p} \cong \mathbf{F}_{p^2}$.*

Proof. This follows immediately from the fact that p is inert in K, totally ramified in $\mathbf{Q}(\zeta_p)$, and $\mathcal{O}_L = \mathcal{O}_K \cdot \mathbf{Z}[\zeta_p]$. □

Since $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$, basic Galois theory gives $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathrm{Gal}(K/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^\times$. This allows us to enumerate the elements of $\mathrm{Gal}(L/\mathbf{Q})$ as $\sigma_{r,j}$ for $j = 0, 1$ and $1 \le r \le p-1$ where

$$\sigma_{r,j}(\zeta_p) = \zeta_p^r$$
$$\sigma_{r,j}(\sqrt{D}) = (-1)^j\sqrt{D}.$$

Lemma 2.3. *Let $x \in \mathbf{Q}(\zeta_p)$. Then $\mathrm{Tr}_{L/\mathbf{Q}}(x\sqrt{D}) = 0$.*

Proof. Observe

$$\begin{aligned}\mathrm{Tr}_{L/\mathbf{Q}}(x\sqrt{D}) &= \sum_{r=1}^{p-1}(\sigma_{r,0}(x\sqrt{D}) + \sigma_{r,1}(x\sqrt{D})) \\ &= \sum_{r=1}^{p-1}(\sqrt{D}\sigma_{r,0}(x) - \sqrt{D}\sigma_{r,1}(x)) \\ &= 0\end{aligned}$$

since $\sigma_{r,0}|_{\mathbf{Q}(\zeta_p)} = \sigma_{r,1}|_{\mathbf{Q}(\zeta_p)}$. □

Lemma 2.4. *Given $x \in \mathcal{O}_L$, $\mathrm{Tr}_{L/\mathbf{Q}}(x) \in 2^\star\mathbf{Z}$ where $\star = 0$ if $D \equiv 1 \pmod 4$ and $\star = 1$ if $D \equiv 2, 3 \pmod 4$.*

Proof. The case $D \equiv 1 \pmod 4$ is obvious so we only need to consider the case $\mathcal{O}_L = \mathbf{Z}[\sqrt{D}, \zeta_p]$. Let $x \in \mathcal{O}_L$ and write $x = \sum_{j=0}^{p-2}(a_j + b_j\sqrt{D})\zeta_p^j$ with $a_j, b_j \in \mathbf{Z}$. Observe that

$$\begin{aligned}\mathrm{Tr}_{L/\mathbf{Q}}(x) &= \sum_{j=0}^{p-2}(a_j \,\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j) + b_j \,\mathrm{Tr}_{L/\mathbf{Q}}(\sqrt{D}\zeta_p^j)) \\ &= \sum_{j=0}^{p-2} a_j \,\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j) \\ &= \sum_{j=0}^{p-2}\sum_{r=0}^{p-2} a_j(\sigma_{r,0}(\zeta_p^j) + \sigma_{r,1}(\zeta_p^j)) \\ &= \sum_{j=0}^{p-2}\sum_{r=0}^{p-2} a_j 2\sigma_{r,0}(\zeta_p^j) \\ &= 2\sum_{j=0}^{p-2} a_j \,\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p^j) \\ &\in 2\mathbf{Z}.\end{aligned}$$

□

Lemma 2.5. *We have $\mathrm{Tr}_{L/\mathbf{Q}}(\mathfrak{p}) \subset p\mathbf{Z}$.*

Proof. Let $x \in \mathfrak{p}$. We can write $x = y(1 - \zeta_p)$ for some $y \in \mathcal{O}_L$. Note that $\sigma(x) = \sigma(y)(1 - \zeta_p^{a_\sigma})$ for some integer a_σ for each $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$. Thus, $\sigma(x) \in \mathfrak{p}$ for each $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$. This gives that $\mathrm{Tr}_{L/\mathbf{Q}}(x) \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. □

The largest totally real subfield of L, denoted L^+, is the field fixed by complex conjugation. The fact that $\mathbf{Q}(\zeta_p)^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ and $D > 0$ gives $L^+ = \mathbf{Q}(\sqrt{D}, \zeta_p + \zeta_p^{-1})$ and so $[L : L^+] = 2$.

Lemma 2.6. *Let $x \in \mathcal{O}_{L^+}$. Then $\mathrm{Tr}_{L/\mathbf{Q}}(x) \in 2 \cdot 2^\star\mathbf{Z}$.*

Proof. It is enough to show $\mathrm{Tr}_{L/\mathbf{Q}}(x) \in 4\mathbf{Z}$ for $x \in \{1, \sqrt{D}, (\zeta_p^j + \zeta_p^{-j}), \sqrt{D}(\zeta_p^j + \zeta_p^{-j})\}$ and $\mathrm{Tr}_{L/\mathbf{Q}}(x) \in 2\mathbf{Z}$ for $x \in \left\{1, \frac{1+\sqrt{D}}{2}, (\zeta_p^j + \zeta_p^{-j}), \frac{1+\sqrt{D}}{2}(\zeta_p^j + \zeta_p^{-j})\right\}$. Note that $\mathrm{Tr}_{L/\mathbf{Q}}(1) = [L : \mathbf{Q}]$, which is divisible by 4. We saw above that $\mathrm{Tr}_{L/\mathbf{Q}}(x\sqrt{D}) = 0$ for $x \in \mathbf{Q}(\zeta_p)$. Consider $\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j + \zeta_p^{-j})$. Note that given a tower of number fields $F_1 \subset F_2 \subset F_3$, we have

$$\mathrm{Tr}_{F_3/F_1} = \mathrm{Tr}_{F_2/F_1} \circ \mathrm{Tr}_{F_3/F_2}\,.$$

Thus,

$$\begin{aligned}
\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j + \zeta_p^{-j}) &= \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\mathrm{Tr}_{L/\mathbf{Q}(\zeta_p)}(\zeta_p^j + \zeta_p^{-j})) \\
&= \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(2(\zeta_p^j + \zeta_p^{-j})) \\
&= 2(\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p^j) + \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p^{-j})) \\
&= 2(-1 - 1) \\
&= -4.
\end{aligned}$$

This gives the result in the case $D \equiv 2, 3 \pmod 4$. Note that

$$\begin{aligned}
\mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{1+\sqrt{D}}{2}\right) &= \frac{1}{2}\left(\mathrm{Tr}_{L/\mathbf{Q}}(1) + \mathrm{Tr}_{L/\mathbf{Q}}(\sqrt{D})\right) \\
&= p - 1.
\end{aligned}$$

Finally, observe

$$\begin{aligned}
\mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{1+\sqrt{D}}{2}(\zeta_p^j + \zeta_p^{-j})\right) &= \frac{1}{2}\left(\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j + \zeta_p^{-j}) + \mathrm{Tr}_{L/\mathbf{Q}}(\sqrt{D}(\zeta_p^j + \zeta_p^{-j}))\right) \\
&= -2.
\end{aligned}$$

This gives the result. □

We have $\Delta_{\mathbf{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$ and $\Delta_K = 4D$ or D depending on if $D \equiv 2, 3 \pmod 4$ or $D \equiv 1 \pmod 4$. Since p was chosen to be relatively prime to $4D$, [13, Theorem 2.6] gives that

$$\begin{aligned}
\Delta_L &= \Delta_K^{p-1}\Delta_{\mathbf{Q}(\zeta_p)}^2 \\
&= \begin{cases} (-1)^{p-1}p^{2p-4}D^{p-1} & \text{if } D \equiv 1 \pmod 4 \\ (-1)^{p-1}p^{2p-4}(4D)^{p-1} & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}
\end{aligned}$$

3. Some generalities on lattices

We collect some general facts on lattices. This material can be found in [7, Chapter 1]. One generally defines a lattice as a subset $\Gamma \subset \mathbf{R}^n$ so that there exists a basis $\{v_1, \dots, v_n\}$ of $\mathbf{R}^n$ so that $\Gamma = \mathbf{Z}v_1 \oplus \cdots \oplus \mathbf{Z}v_n$. The lattices we encounter in this paper will not be subsets of $\mathbf{R}^n$, so we need a slightly more general definition. We show our more general lattices can be identified with the traditional definition of lattices.

Let R be a commutative ring with identity. A *symmetric bilinear form module* (S, b) is a free R-module S of rank n along with a symmetric bilinear form $b : S \times S \to R$. In the case that $R = \mathbf{Z}$, we will refer to S as a *symmetric integral lattice*, or just a *lattice*. The *dual module* $S^\vee$ is the module $\mathrm{Hom}_R(S, R)$. We say (S, b) is *unimodular* if the canonical homomorphism $S \to S^\vee$ given by $x \mapsto b(x, \cdot)$ is bijective.

Proposition 3.1. *The integral lattices in $\mathbf{R}^n$ are precisely the symmetric bilinear modules (S, b) over $\mathbf{Z}$ where $b : S \times S \to \mathbf{Z}$ is a positive definite symmetric bilinear form.*

Proof. Let $\Gamma \subset \mathbf{R}^n$ be an integral lattice. Then clearly Γ is a free $\mathbf{Z}$-module of rank n and the usual inner product is a positive definite symmetric bilinear form.

Now let (S, b) be a symmetric bilinear module over $\mathbf{Z}$. Consider the real vector space $V = S \otimes_{\mathbf{Z}} \mathbf{R}$. We have that b extends to a positive definite symmetric bilinear form $V \times V \to \mathbf{R}$ via

$$b\left(\sum_i x_i \otimes \alpha_i, \sum_j y_j \otimes \beta_j\right) := \sum_{i,j} \alpha_i \beta_j b(x_i, y_j).$$

As V is a real vector space with a positive definite symmetric bilinear form, we can choose an orthonormal basis $\{v_1, \dots, v_n\}$ of V with respect to b. We have V is isomorphic to $\mathbf{R}^n$ as an $\mathbf{R}$-vector space by mapping $\{v_1, \dots, v_n\}$ to the standard basis $\{e_1, \dots, e_n\}$ of $\mathbf{R}^n$. Under this isomorphism we have b is identified with the standard inner product and the image of S is an integral lattice. □

Given a lattice $\Gamma \subset \mathbf{R}^n$, we have $\mathbf{R}^n/\Gamma$ is compact. We define

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(\mathbf{R}^n/\Gamma) = |\det(v_1, \dots, v_n)|$$

where $\Gamma = \mathbf{Z}v_1 \oplus \cdots \oplus \mathbf{Z}v_n$. Set $a_{i,j} = \langle v_i, v_j \rangle$ and $A = (a_{i,j})$. We have

$$\mathrm{vol}(\Gamma) = \sqrt{\det(A)}.$$

Note that $\det(A)$ is independent of the basis $v_1, \ldots, v_n$ chosen for Γ, so we write $\operatorname{disc}(\Gamma)$ for $\det(A)$. We have that

$$\operatorname{vol}(\Gamma) = \frac{1}{\operatorname{vol}(\Gamma^\vee)}.$$

Moreover, if Γ_1 and Γ_2 are lattices in $\mathbf{R}^n$ with $\Gamma_1 \subset \Gamma_2$, then

$$\operatorname{vol}(\Gamma_1) = \operatorname{vol}(\Gamma_2)|\Gamma_2/\Gamma_1|.$$

Let $E/\mathbf{Q}$ be a number field of degree $m = r + 2s$ where r is the number of real embeddings of E and s is the number of pairs of complex embeddings. The canonical embedding of E into $\mathbf{R}^m$ is given by

$$\begin{aligned}\sigma_E : E &\to \mathbf{R}^m \\ x &\mapsto (\sigma_1(x), \ldots, \sigma_r(x), \Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), \ldots, \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x)))\end{aligned}$$

where $\sigma_1, \ldots, \sigma_r$ are the distinct real embeddings and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ are the complex embeddings ordered so that σ_{r+j} is conjugate to σ_{r+2s-j}.

As our lattices will be constructed via rings of integers in number fields, we briefly review that material. Let $E/\mathbf{Q}$ be a number field of degree m. Let Λ be a $\mathbf{Z}$-submodule of E of rank m and finite index k. We can realize Λ inside $\mathbf{R}^m$ via $\sigma_E(\Lambda)$. This is a lattice in $\mathbf{R}^m$ of rank m and volume

$$\operatorname{vol}(\sigma_E(\Lambda)) = k\sqrt{|\operatorname{disc}(E)|}.$$

Note this differs from the usual Lebesgue measure by a factor of 2^s. One can see [9, Prop. 5.2] for this formula. In terms of the symmetric bilinear modules, this corresponds to the case we take $S = \Lambda$ and $b(x, y) = \operatorname{Tr}_{E/\mathbf{Q}}(x\overline{y})$.

4. A particular bilinear form

We will make use of a particular bilinear form defined on $\mathcal{O}_L$. We define that bilinear form in this section and calculate the relevant properties.

Definition 4.1. For $x, y \in \mathcal{O}_L$, define

$$b_{L/\mathbf{Q}}(x, y) = \operatorname{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{y}}{2^\star p}\right)$$

where, as above, $\star = 0$ if $D \equiv 1 \pmod 4$ and $\star = 1$ if $D \equiv 2, 3 \pmod 4$ and $\overline{y}$ denotes complex conjugation.

It is clear from the properties of the trace map that this is in fact a bilinear form.

Proposition 4.2. *The bilinear form $b_{L/\mathbf{Q}}(\cdot, \cdot)$ is symmetric and positive definite on $\mathcal{O}_L$.*

Proof. Let $x \in \mathcal{O}_L$, $x \neq 0$. We have

$$\begin{aligned} b_{L/\mathbf{Q}}(x,x) &= \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{x}}{2^\star p}\right) \\ &= \sum_{\sigma \in \mathrm{Gal}(L/\mathbf{Q})} \sigma\left(\frac{x\overline{x}}{2^\star p}\right) \\ &= \frac{1}{2^\star p} \sum_{\sigma \in \mathrm{Gal}(L/\mathbf{Q})} \sigma(x\overline{x}) \\ &= \frac{1}{2^\star p} \sum_{\sigma \in \mathrm{Gal}(L/\mathbf{Q})} \sigma(x)\overline{\sigma(x)} \\ &> 0. \end{aligned}$$

Thus, we have that $b_{L/\mathbf{Q}}(\cdot,\cdot)$ is positive definite.

Observe that complex conjugation is an element of $\mathrm{Gal}(L/\mathbf{Q})$. Given any $\alpha \in \mathcal{O}_L$ we have

$$\begin{aligned} \mathrm{Tr}_{L/\mathbf{Q}}(\overline{\alpha}) &= \sum_{\sigma \in \mathrm{Gal}(L/\mathbf{Q})} \sigma(\overline{\alpha}) \\ &= \sum_{\tau \in \mathrm{Gal}(L/\mathbf{Q})} \tau(\alpha) \\ &= \mathrm{Tr}_{L/\mathbf{Q}}(\alpha). \end{aligned}$$

Thus, for $x, y \in \mathcal{O}_L$ we have

$$\begin{aligned} b_{L/\mathbf{Q}}(x,y) &= \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{y}}{2^\star p}\right) \\ &= \mathrm{Tr}_{L/\mathbf{Q}}\left(\overline{\frac{x\overline{y}}{2^\star p}}\right) \\ &= \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{y\overline{x}}{2^\star p}\right) \\ &= b_{L/\mathbf{Q}}(y,x). \end{aligned}$$

□

Proposition 4.3. *The bilinear form $b_{L/\mathbf{Q}}(\cdot,\cdot)$ has determinant*

$$\det(b_{L/\mathbf{Q}}(\cdot,\cdot)) = \frac{D^{p-1}}{p^2}.$$

Proof. We have $\{1, \zeta_p, ..., \zeta_p^{p-2}, \sqrt{D}, \sqrt{D}\zeta_p, ..., \sqrt{D}\zeta_p^{p-2}\}$ is a $\mathbf{Z}$-basis of $\mathcal{O}_L$ if $D \equiv 2, 3 \pmod 4$ and $\left\{1, \zeta_p, ..., \zeta_p^{p-2}, \frac{1+\sqrt{D}}{2}, \frac{1+\sqrt{D}}{2}\zeta_p, ..., \frac{1+\sqrt{D}}{2}\zeta_p^{p-2}\right\}$

is a $\mathbf{Z}$-basis of $\mathcal{O}_L$ if $D \equiv 1 \pmod 4$. We claim that complex conjugation acting on this basis has determinant $(-1)^{2(p-2)} = 1$. To see this, observe that each pair $\{\zeta_p^j, \zeta_p^{p-1-j}\}$ is exchanged via complex conjugation, so each such pair contributes a -1 to the determinant if $j \neq p-1-j$. Similarly, a pair $\{\sqrt{D}\zeta_p^j, \sqrt{D}\zeta_p^{p-1-j}\}$ or $\left\{\{\frac{1+\sqrt{D}}{2}\zeta_p^j, \frac{1+\sqrt{D}}{2}\zeta_p^{p-1-j}\right\}$ contributes a -1 to the determinant when $j \neq p-1-j$. There are $2(p-2)$ such pairs. The other basis elements are fixed under complex conjugation, so we have the claim.

We have via the definition of the discriminant of L that $\det(\mathrm{Tr}_{L/\mathbf{Q}}) = \Delta_L$. Composing these results gives the determinant of the bilinear form $(x, y) \mapsto \mathrm{Tr}_{L/\mathbf{Q}}(x\overline{y})$ is Δ_L. Thus, we have

$$\det(b_{L/\mathbf{Q}}(\cdot,\cdot)) = \frac{\Delta_L}{(2^\star p)^{2(p-1)}}.$$

Using that p is odd so that $(-1)^{p-1} = 1$, we have the result. □

5. Lattices from codes

With $L = \mathbf{Q}(\zeta_p, \sqrt{D})$ as before, we have a natural surjection $\pi : \mathcal{O}_L \to \mathbf{F}_{p^2}$ with kernel $\mathfrak{p}$, c.f. Proposition 2.2. We define $\Pi : \mathcal{O}_L^n \to \mathbf{F}_{p^2}^n$ by mapping componentwise via π. This is clearly still a surjection. Let $\mathcal{C} \subset \mathbf{F}_{p^2}^n$ be an $[n, k]$-code, i.e., a k-dimensional subspace. Define

$$\Lambda_{\mathcal{C}} = \Pi^{-1}(\mathcal{C}).$$

We have $\mathbf{F}_{p^2}^n/\mathcal{C} \cong \mathbf{F}_{p^2}^{n-k}$, so $\mathcal{C}$ is a subgroup of index $p^{2(n-k)}$ of $\mathbf{F}_{p^2}^n$. Thus, $\Lambda_{\mathcal{C}}$ is a subgroup of index $p^{2(n-k)}$ of $\mathcal{O}_L^n$, i.e., a free $\mathbf{Z}$-module of index $p^{2(n-k)}$.

Given $x \in \mathcal{O}_L^n$ with $x = (x_1, \ldots, x_n)$, we define $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n)$. For $x, y \in \mathcal{O}_L^n$, define

$$x \cdot y = \sum_{j=1}^{n} x_j y_j.$$

Lemma 5.1. *Let $x, y \in \mathcal{O}_L^n$. We have*

$$x \cdot y \equiv x \cdot \overline{y} \pmod{\mathfrak{p}}$$

where we recall $\mathfrak{p} = (1-\zeta_p)\mathcal{O}_L$.

Proof. It is enough to show $x_j y_j \equiv x_j \overline{y}_j \pmod{\mathfrak{p}}$ for each j. Moreover, it is enough to show this for a basis of $\mathcal{O}_L$ over $\mathbf{Z}$. Using that $D > 0$, we reduce this to showing $\zeta_p^j \equiv \overline{\zeta_p^j} \pmod{\mathfrak{p}}$. Noting that $\overline{\zeta_p^j} = \zeta_p^{p-j}$ and that $\mathfrak{p} = (1-\zeta_p^k)\mathcal{O}_L$ for any $k \not\equiv 0 \pmod p$ we have the result. □

We define a symmetric bilinear form on $\mathcal{O}_L^n$ by setting

$$\begin{aligned} B_{L/\mathbf{Q}}(x,y) &= \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{x\cdot\overline{y}}{2^\star p}\right) \\ &= \sum_{j=1}^{n} \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{x_j\overline{y}_j}{2^\star p}\right) \\ &= \sum_{j=1}^{n} b_{L/\mathbf{Q}}(x_j,y_j). \end{aligned}$$

Note that this is a positive definite symmetric bilinear form based on the fact that $b_{L/\mathbf{Q}}(\cdot,\cdot)$ is such a form.

Theorem 5.2. *Let $\mathcal{C} \subset \mathbf{F}_{p^2}^n$ be a self-orthogonal code, i.e., $\mathcal{C} \subset \mathcal{C}^\perp$ where $\mathcal{C}^\perp = \{\alpha \in \mathbf{F}_{p^2}^n : \alpha\cdot c = 0 \ \text{ for all } c \in \mathcal{C}\}$. The associated lattice $\Lambda_{\mathcal{C}}$ is integral, even, and rank $2n(p-1)$. Moreover, we have $\Lambda_{\mathcal{C}^\perp} \subsetneq \Lambda_{\mathcal{C}}^\vee$.*

Proof. Let $x, y \in \Lambda_{\mathcal{C}}$. Since $\mathcal{C} \subset \mathcal{C}^\perp$, we have $\Pi(x)\cdot\Pi(y) = 0$. As the map Π is reduction modulo $\mathfrak{p}$ componentwise, this gives that $x\cdot y \equiv 0 \pmod{\mathfrak{p}}$. Applying Lemma 5.1, we obtain that $x\cdot\overline{y} \equiv 0 \pmod{\mathfrak{p}}$ for all $x, y \in \Lambda_{\mathcal{C}}$. This allows us to conclude via Lemma 2.5 that $\mathrm{Tr}_{L/\mathbf{Q}}(x\cdot\overline{y}) \in p\mathbf{Z}$. Moreover, Lemma 2.4 gives that $\mathrm{Tr}_{L/\mathbf{Q}}(x\cdot\overline{y}) \in 2^\star\mathbf{Z}$. Since p is odd, this gives $\mathrm{Tr}_{L/\mathbf{Q}}(x\cdot\overline{y}) \in 2^\star p\mathbf{Z}$ for all $x, y \in \Lambda_{\mathcal{C}}$. Thus, $B(x,y) \in \mathbf{Z}$ for all $x, y \in \Lambda_{\mathcal{C}}$, i.e., the lattice $\Lambda_{\mathcal{C}}$ is integral.

To see $\Lambda_{\mathcal{C}}$ is even, just use the fact that $x\cdot\overline{x}$ is real, so $\mathrm{Tr}_{L/\mathbf{Q}}(x\cdot\overline{x}) \in 2\cdot 2^\star\mathbf{Z}$ by Lemma 2.6. Thus, $\mathrm{Tr}_{L/\mathbf{Q}}(x\cdot\overline{x}) \in 2\cdot 2^\star p\mathbf{Z}$ for all $x \in \Lambda_{\mathcal{C}}$, which gives $B_{L/\mathbf{Q}}(x,x) \in 2\mathbf{Z}$.

Let $x \in \Lambda_{\mathcal{C}}$ and $y \in \Lambda_{\mathcal{C}^\perp}$. Then $\Pi(x) \in \mathcal{C}$ and $\Pi(y) \in \mathcal{C}^\perp$, so $\Pi(x)\cdot\Pi(y) = 0$. As above, this gives $x\cdot y \equiv 0 \pmod{\mathfrak{p}}$ and $B_{L/\mathbf{Q}}(x,y) \in \mathbf{Z}$. Thus, $\Lambda_{\mathcal{C}^\perp} \subset \Lambda_{\mathcal{C}}^\vee$.

It remains to show the containment is proper. To do this, we show the volumes are not equal. From above we have the index of $\Lambda_{\mathcal{C}}$ in $\mathcal{O}_L^n$ is $p^{2(n-k)}$. We also have that $\mathrm{vol}(\mathcal{O}_L^n) = \sqrt{\frac{D^{n(p-1)}}{p^{2n}}}$, so

$$\mathrm{vol}(\Lambda_{\mathcal{C}}) = \frac{D^{n(p-1)/2}}{p^n}p^{2(n-k)} = D^{n(p-1)/2}p^{n-2k}.$$

Thus,

$$\mathrm{vol}(\Lambda_{\mathcal{C}}^\vee) = D^{n(1-p)/2}p^{2k-n}.$$

Now we must calculate $\mathrm{vol}(\Lambda_{\mathcal{C}^\perp})$. Note that the dimension of $\mathcal{C}^\perp$ is $n-k$, so the index of $\Lambda_{\mathcal{C}^\perp}$ in $\mathcal{O}_L^n$ is p^{2k}. Thus, we have

$$\mathrm{vol}(\Lambda_{\mathcal{C}^\perp}) = \frac{D^{n(p-1)/2}}{p^n}p^{2k} = D^{n(p-1)/2}p^{2k-n}.$$

Note that if we use the equation for volumes, we have

$$\begin{aligned}|\Lambda_{\mathcal{C}}^{\vee}/\Lambda_{\mathcal{C}^{\perp}}| &= \operatorname{vol}(\Lambda_{\mathcal{C}^{\perp}})/\operatorname{vol}(\Lambda_{\mathcal{C}}^{\vee}) \\ &= D^{n(p-1)}.\end{aligned}$$

Thus, the containment is strict since $D > 1$. □

6. Theta Series

In this section we set-up the general theory we will need before specializing back to the case of interest in the following section.

Let E be a totally real number field of degree $m = [E : \mathbf{Q}]$, embeddings $\sigma_1, \ldots, \sigma_m : E \to \mathbf{R}$, and ring of integers $\mathcal{O}_E$. Let V be an n-dimensional E-vector space with a totally positive definite symmetric bilinear form $b(\cdot, \cdot)$, i.e., $b : V \times V \to E$ is a symmetric bilinear form so that $\sigma_j(b(v, v)) > 0$ for all nonzero $v \in V$. Let Λ be an E-lattice in V. We assume Λ is integral and even. Note this gives that $\Lambda \subset \Lambda^{\vee}$. We now explain how to attach theta functions to the lattice Λ.

Define the complex upper half plane as

$$\mathfrak{h} = \{z \in \mathbf{C} : \Im(z) > 0\}.$$

We have an action of $\mathrm{SL}_2(\mathcal{O}_E)$ on $\mathfrak{h}^m$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \left(\frac{\sigma_j(a) z_j + \sigma_j(b)}{\sigma_j(c) z_j + \sigma_j(d)} \right)_{j=1,\ldots,m}$$

where $z = (z_1, \ldots, z_m) \in \mathfrak{h}^m$.

Let $\mathfrak{I} \subset \mathcal{O}_E$ be an ideal. We define subgroups $\Gamma(\mathfrak{I})$, $\Gamma_1(\mathfrak{I})$, and $\Gamma_0(\mathfrak{I})$ of $\mathrm{SL}_2(\mathcal{O}_E)$ as

$$\begin{aligned}\Gamma_0(\mathfrak{I}) &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathcal{O}_E) : c \equiv 0 \pmod{\mathfrak{I}} \right\} \\ \Gamma_1(\mathfrak{I}) &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(\mathfrak{I}) : a \equiv d \equiv 1 \pmod{\mathfrak{I}} \right\},\end{aligned}$$

and

$$\Gamma(\mathfrak{I}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(\mathfrak{I}) : b \equiv 0 \pmod{\mathfrak{I}} \right\}.$$

Let $f : \mathfrak{h}^m \to \mathbf{C}$ and $k \in \mathbf{Z}$. We define an action of $\mathrm{SL}_2(\mathcal{O}_E)$ on such functions by defining

$$(f|_k\gamma)(z) = \prod_{j=1}^{m} (\sigma_j(c) z_j + \sigma_j(d))^{-k} f(\gamma \cdot z)$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $z = (z_1, \ldots, z_m)$. Let Γ be $\Gamma(\mathfrak{I})$, $\Gamma_1(\mathfrak{I})$, or $\Gamma_0(\mathfrak{I})$ for some ideal $\mathfrak{I}$. We say a holomorphic function $f : \mathfrak{h}^m \to \mathbf{C}$ (if $E = \mathbf{Q}$ we also require "holomorphic at the cusps") that satisfies $(f|_k\gamma)(z) = f(z)$ for all $\gamma \in \Gamma$ is a modular form of weight k and level Γ. We denote the space of such forms by $M_k(\Gamma)$. Let $\chi : (\mathcal{O}_E/\mathfrak{I})^\times \to \mathbf{C}^\times$ be a character. We denote the space of modular forms f satisfying $(f|_k\gamma)(z) = \chi(d)f(z)$ for all $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(\mathfrak{I})$ by $M_k(\mathfrak{I}, \chi)$. While we will not need it, there is a very rich theory of modular forms as they play a seminal role in number theory. The interested reader can see [6] in the case $E = \mathbf{Q}$ and [8] for the general case.

For a given $v_0 \in V$, define a theta function $\theta : \mathfrak{h}^m \to \mathbf{C}$ by setting

$$\theta_{v_0+\Lambda}(z) = \sum_{v \in v_0+\Lambda} e^{\pi i \operatorname{Tr}(zB(v,v))},$$

where

$$\operatorname{Tr}(zB(v,v)) = \sum_{j=1}^{m} z_j \sigma_j(B(v,v)).$$

We have via [7, Proposition 5.7] that $\theta_{v_0+\Lambda}$ is holomorphic on $\mathfrak{h}^m$.

Proposition 6.1. [7, Proposition 5.8] *Let $k = n/2$, $v \in \Lambda^\vee$, and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathcal{O}_E)$. We have*

$$\theta_{v+\Lambda}|_k\gamma = i^{-km} \operatorname{N}_{E/\mathbf{Q}}(c)^{-k} \left[\Lambda^\vee : \Lambda\right]^{-1/2} \cdot \sum_{w \in \Lambda^\vee/\Lambda} \left(e^{-\pi i \operatorname{Tr}(2bB(v,w)+bdB(w,w))} \sum_{\substack{u \in \Lambda^\vee/c\Lambda \\ u \equiv v+dw \pmod{\Lambda}}} e^{\pi i \operatorname{Tr}\left(\frac{a}{c}B(u,u)\right)} \right) \theta_{w+\Lambda}$$

if $c \neq 0$ and

$$\theta_{v+\Lambda}|_k\gamma = \operatorname{N}_{E/\mathbf{Q}}(d)^{-k} e^{\pi i \operatorname{Tr}(abB(v,v))} \theta_{av+\Lambda}$$

if $c = 0$.

We define the level of Λ as

$$\mathfrak{L} = \left\{ x \in \mathcal{O}_E : \operatorname{Tr}\left(x\mathcal{O}_E \frac{B(v,v)}{2} \right) \subset \mathbf{Z} \text{ for all } v \in \Lambda^\vee \right\}.$$

We have that $\mathfrak{L}$ is an ideal in $\mathcal{O}_E$ via [7, Proposition 5.9]. Moreover, the same reference gives that $\mathfrak{L} = \mathcal{O}_E$ if and only if $\Lambda = \Lambda^\vee$.

Given $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(\mathfrak{L})$, define

$$\varepsilon(\gamma) = \begin{cases} i^{-km}\, \mathrm{N}_{E/\mathbf{Q}}(c)^{-k}\, [\Lambda^\vee : \Lambda]^{-1/2} \sum_{u \in \Lambda/c\Lambda} e^{\pi i \,\mathrm{Tr}\left(\frac{a}{c} B(u,u)\right)} & \text{for } c \neq 0, \\ \mathrm{N}_{E/\mathbf{Q}}(d)^{-k} & \text{for } c = 0. \end{cases}$$

Proposition 6.2. [7, Proposition 5.10] *There exists a character* $\chi : (\mathcal{O}_E/\mathfrak{L})^\times \to \{\pm 1\}$ *so that*

$$\varepsilon(\gamma) = \chi(d)$$

for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(\mathfrak{L})$ *where the input in* χ *is understood to be modulo* $\mathfrak{L}$. *Moreover, for* $\ell \in \mathbf{Z}$ *with* $\gcd(\ell, \mathfrak{L}) = 1$, ℓ *prime, one has*

$$\chi(\ell) = \left(\frac{(-1)^{mn/2}\, [\Lambda^\vee : \Lambda]}{\ell} \right).$$

Theorem 6.3. [7, Theorem 5.8] *For* $v \in \Lambda^\vee$ *we have*

$$\theta_{v+\Lambda}|_k \gamma = \theta_{v+\Lambda}$$

for all $\gamma \in \Gamma(\mathfrak{L})$ *and*

$$\theta_\Lambda|_k \gamma = \chi(d)\theta_\Lambda$$

for all $\gamma \in \Gamma_0(\mathfrak{L})$, *i.e.,* $\theta_{v+\Lambda} \in M_k(\Gamma(\mathfrak{L}))$ *and* $\theta_\Lambda \in M_k(\mathfrak{L}, \chi)$.

7. Theta series and lattices from codes

In this section we apply the results on theta series from the previous section to the lattices constructed from codes in Section 5.

Recall we have $L = \mathbf{Q}(\sqrt{D}, \zeta_p)$ and $L^+ = \mathbf{Q}(\sqrt{D}, \zeta_p + \zeta_p^{-1})$. Note that L^+ is a totally real number field of degree $p-1$, i.e., in the setting of the previous section we have $E = L^+$ and $m = p - 1$. We set $V = L$, a 2-dimensional L^+-vector space. Observe that $\mathfrak{p} \subset \mathcal{O}_L$ is a L^+-lattice in L. Define a positive definite symmetric bilinear form $b_{L/L^+} : L \times L \to L^+$ by setting

$$\begin{aligned} b_{L/L^+}(x, y) &= \mathrm{Tr}_{L/L^+}\left(\frac{x\overline{y}}{2^\star p} \right) \\ &= \frac{\overline{x}y + x\overline{y}}{2^\star p}. \end{aligned}$$

It is easy to check this is well-defined and is a positive definite symmetric bilinear form. Note that

$$b_{L/L^+}(x, x) = \frac{2^{1-\star} x\overline{x}}{p}.$$

Let $\mathrm{Gal}(L^+/\mathbf{Q}) = \{\sigma_1, \ldots, \sigma_{p-1}\}$. For each $j \in \mathfrak{p}^\vee$ we define a theta function as in the previous section by

$$\begin{aligned}\theta_j(z) &:= \theta_{j+\mathfrak{p}}(z) \\ &= \sum_{x \in j+\mathfrak{p}} e^{\pi i \operatorname{Tr}(z b_{L/L^+}(x,x))}\end{aligned}$$

where $z = (z_1, \ldots, z_{p-1}) \in \mathfrak{h}^{p-1}$ and

$$\begin{aligned}\operatorname{Tr}(z b_{L/L^+}(x,x)) &= \sum_{j=1}^{p-1} z_j \sigma_j(b_{L/L^+}(x,x)) \\ &= \sum_{j=1}^{p-1} \frac{2^{1-\star}}{p} z_j \sigma_j\left(x\overline{x}\right).\end{aligned}$$

Thus, we have via Theorem 6.3 that $\theta_j \in M_1(\Gamma(\mathfrak{L}))$. We now show that $\mathfrak{L} = \wp := \mathfrak{p} \cap L^+$. Our first step in this is calculating

$$\mathfrak{p}^\vee = \{x \in L : \operatorname{Tr}_{L^+/\mathbf{Q}}(b_{L/L^+}(x,z)) \in \mathbf{Z} \text{ for all } z \in \mathfrak{p}\}.$$

Observe that

$$\begin{aligned}\operatorname{Tr}_{L^+/\mathbf{Q}}(b_{L/L^+}(x,z)) &= \operatorname{Tr}_{L^+/\mathbf{Q}}\left(\operatorname{Tr}_{L/L^+}\left(\frac{x\overline{z}}{2^\star p}\right)\right) \\ &= \operatorname{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{z}}{2^\star p}\right).\end{aligned}$$

Thus, we can rewrite $\mathfrak{p}^\vee$ as

$$\mathfrak{p}^\vee = \left\{x \in L : \operatorname{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{z}}{2^\star p}\right) \in \mathbf{Z} \text{ for all } z \in \mathfrak{p}\right\}.$$

The main facts we use in this calculation we saw before, namely,

$$\begin{aligned}\operatorname{Tr}_{L/\mathbf{Q}}(a) &= a[L:\mathbf{Q}] \quad \text{for all } a \in \mathbf{Q}, \\ \operatorname{Tr}_{L/\mathbf{Q}}(\zeta_p^j) &= -2 \quad \text{for all } j \not\equiv 0 \pmod{p}, \\ \operatorname{Tr}_{L/\mathbf{Q}}(x\sqrt{D}) &= 0 \quad \text{for all } x \in \mathbf{Q}(\zeta_p).\end{aligned}$$

Proposition 7.1. *The lattice $\mathfrak{p}^\vee$ consists of elements in L of the form*

$$x = \sum_{j=0}^{p-2} (a_j + b_j\sqrt{D})\zeta_p^j$$

where $a_j \in \frac{1}{2^{1-\star}}\mathbf{Z}$ *and* $b_j \in \frac{1}{2^{1-\star}D}\mathbf{Z}$. *In other words, as* $\mathbf{Z}$*-modules we have*

$$\mathfrak{p}^\vee \cong \left(\bigoplus_{j=0}^{p-2} \frac{1}{2^{1-\star}}\mathbf{Z}\right) \oplus \left(\bigoplus_{j=0}^{p-2} \frac{1}{2^{1-\star}D}\mathbf{Z}\right).$$

Proof. Let $x \in L$ and write

$$x = \sum_{j=0}^{p-2} (a_j + b_j\sqrt{D})\zeta_p^j$$

with $a_j, b_j \in \mathbf{Q}$. We have $\zeta_p^j(1-\zeta_p) \in \mathfrak{p}$ for all j. For $x \in \mathfrak{p}^\vee$, we must have $b(x,z) = \mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{x\overline{z}}{2^\star p}\right) \in \mathbf{Z}$ for all $z \in \mathfrak{p}$.

Consider $z = 1 - \overline{\zeta}_p$, so $\overline{z} = 1 - \zeta_p$. We have

$$\begin{aligned}
b(x,z) &= \frac{1}{2^\star p}\,\mathrm{Tr}_{L/\mathbf{Q}}(x(1-\zeta_p)) \\
&= \frac{1}{2^\star p}\,\mathrm{Tr}_{L/\mathbf{Q}}\left(\sum_{j=0}^{p-2}(a_j + \sqrt{D}b_j)\zeta_p^j(1-\zeta_p)\right) \\
&= \frac{1}{2^\star p}\sum_{j=0}^{p-2}\left(\mathrm{Tr}_{L/\mathbf{Q}}(a_j\zeta_p^j - a_j\zeta_p^{j+1}) + \mathrm{Tr}_{L/\mathbf{Q}}(\sqrt{D}(b_j\zeta_p^j - b_j\zeta_p^{j+1}))\right) \\
&= \frac{1}{2^\star p}\sum_{j=0}^{p-2} a_j\left(\mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^j) - \mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p^{j+1})\right) \\
&= \frac{1}{2^\star p}\left(a_0(\mathrm{Tr}_{L/\mathbf{Q}}(1) - \mathrm{Tr}_{L/\mathbf{Q}}(\zeta_p))\right) \\
&= \frac{1}{2^\star p}a_0([L:\mathbf{Q}]+2) \\
&= \frac{a_0(2(p-1)+2)}{p} \\
&= 2^{1-\star}a_0.
\end{aligned}$$

Thus, we must have $a_0 \in \frac{1}{2^{1-\star}}\mathbf{Z}$. Similarly, by taking $z = \zeta_p^j(1-\overline{\zeta}_p)$ for various j, one obtains $a_1, \ldots, a_{p-2} \in \frac{1}{2^{1-\star}}\mathbf{Z}$ as well.

To restrict the possible values of $b_0, \dots, b_{p-2}$, we consider $z = \sqrt{D}\zeta_p^j(1-\overline{\zeta}_p)$. For example, setting $z = \sqrt{D}(1-\overline{\zeta}_p)$ we have

$$\begin{aligned} b(x,z) &= \frac{1}{2^\star p}\operatorname{Tr}_{L/\mathbf{Q}}(x\sqrt{D}(1-\zeta_p)) \\ &= \frac{1}{2^\star p}\operatorname{Tr}_{L/\mathbf{Q}}\left(\sum_{j=0}^{p-2}(a_j+\sqrt{D}b_j)\zeta_p^j\sqrt{D}(1-\zeta_p)\right) \\ &= \frac{1}{2^\star p}\sum_{j=0}^{p-2}\left(\operatorname{Tr}_{L/\mathbf{Q}}(\sqrt{D}(a_j\zeta_p^j - a_j\zeta_p^{j+1})) + \operatorname{Tr}_{L/\mathbf{Q}}(D(b_j\zeta_p^j - b_j\zeta_p^{j+1}))\right) \\ &= \frac{1}{2^\star p}\sum_{j=0}^{p-2} Db_j(\operatorname{Tr}_{L/\mathbf{Q}}(\zeta_p^j) - \operatorname{Tr}_{L/\mathbf{Q}}(\zeta_p^{j+1})) \\ &= \frac{Db_0([L:\mathbf{Q}]+2)}{2^\star p} \\ &= 2^{1-\star}Db_0. \end{aligned}$$

Thus, we must have $b_0 \in \frac{1}{2^{1-\star}D}\mathbf{Z}$. The same argument using $z = \sqrt{D}\zeta_p^j(1-\overline{\zeta}_p)$ gives that $b_1, \dots, b_{p-2} \in \frac{1}{2^{1-\star}D}\mathbf{Z}$ as well. □

Set $\mathfrak{N}$ to be the $\mathcal{O}_{L^+}$-submodule of L^+ generated by the elements $\dfrac{b_{L/\mathbf{Q}}(x,x)}{2}$ for $x \in \mathfrak{p}^\vee$.

Proposition 7.2. [7, Prop. 5.9(ii)] *One has* $\mathcal{L} = \mathfrak{N}^{-1}\mathfrak{D}_{L^+}^{-1}$.

This proposition gives that to calculate the level, all we need to calculate is $\mathfrak{N}$ and $\mathfrak{D}_{L^+}$. To calculate $\mathfrak{D}_{L^+}$, we make use of the following well-known theorem.

Theorem 7.3. *Let $E/\mathbf{Q}$ be a number field. The prime ideal factors of $\mathfrak{D}_E$ are the primes in E that ramify over $\mathbf{Q}$. More precisely, for any prime ideal $\mathfrak{q}$ in $\mathcal{O}_E$ lying over a rational prime q, with ramification index e, the exact power of $\mathfrak{q}$ dividing $\mathfrak{D}_E$ is $\mathfrak{q}^{e-1}$ if $e \not\equiv 0 \pmod q$ and $\mathfrak{q}^e \mid \mathfrak{D}_E$ if $q \mid e$.*

Set $\wp = \mathfrak{p} \cap L^+$, i.e., $\wp = \langle(1-\zeta_p)(1-\overline{\zeta}_p)\rangle$. The previous theorem immediately gives

$$\mathfrak{D}_{L^+} = \wp^{(p-3)/2}\langle 2^\star\sqrt{D}\rangle.$$

Now consider $\mathfrak{N}$. We have $\dfrac{b_{L/L^+}(x,x)}{2} = \dfrac{2x\overline{x}}{2^{1+\star}p} = \dfrac{x\overline{x}}{2^\star p}$. From the description above of the elements in $\mathfrak{p}^\vee$, we immediately see that $\mathfrak{N} \subset$

$\frac{1}{2^\star\sqrt{D}p}\mathcal{O}_{L^+}$. We just need to show containment in the other direction. Letting $x = 1$ we see $\mathfrak{N}$ contains $\frac{1}{2^\star p}$. Setting $x = \frac{1}{\sqrt{D}}$ we have $\frac{1}{2^\star Dp} \in \mathfrak{N}$. By setting $x = 1 + \frac{1}{\sqrt{D}}\zeta_p$ we see that

$$\begin{aligned}\frac{b_{L/L^+}(x,x)}{2} &= \frac{1}{2^\star p}\left(1+\frac{1}{\sqrt{D}}\zeta_p\right)\left(1+\frac{1}{\sqrt{D}}\zeta_p^{-1}\right)\\ &= \frac{1}{2^\star p}\left(1+\frac{1}{D}+\frac{1}{\sqrt{D}}(\zeta_p+\zeta_p^{-1})\right) \in \mathfrak{N}.\end{aligned}$$

Using that $(\zeta_p + \zeta_p^{-1}) \in \mathcal{O}_L^+$, $\frac{1}{2^\star p}$ and $\frac{1}{2^\star Dp}$ are in $\mathfrak{N}$, we obtain $\frac{1}{\sqrt{D}} \in \mathfrak{N}$. This gives the desired containment. Thus, we have

$$\mathfrak{N} = \wp^{(1-p)/2}\langle 2^\star\sqrt{D}\rangle^{-1}.$$

Combining this with the calculation of $\mathfrak{D}_{L^+}$, we have $\mathfrak{L} = \wp$. In other words,

$$\theta_j \in M_1(\wp, \chi)$$

for all $j \in \mathfrak{p}^\vee$ where χ is the character as defined in the previous section. For our set-up we have $\chi : \left(\mathcal{O}_L^+/\wp\right)^\times \to \{\pm 1\}$ and for $\ell \neq p$, we have

$$\chi(\ell) = \left(\frac{D^{p-1}}{\ell}\right).$$

We now turn our attention to the lattice $\Lambda_\mathcal{C}$ constructed in Section 5. Here we take $V = L^n$ and define $B_{L/L^+} : V \times V \to L^+$ by setting

$$B_{L/L^+}(v,w) = \sum_{j=1}^{n} b_{L/L^+}(v_j, w_j)$$

for $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$. Associated to $\Lambda_\mathcal{C}$ we have

$$\theta_{\Lambda_\mathcal{C}}(z) = \sum_{v\in\Lambda_\mathcal{C}} e^{\pi i \operatorname{Tr}(zB_{L/L^+}(v,v))}$$

where as above we define

$$\operatorname{Tr}(zB_{L/L^+}(v,v)) = \sum_{j=1}^{p-1} z_j\sigma_j(B_{L/L^+}(v,v)).$$

We have via Theorem 6.3 that

$$\theta_{\Lambda_\mathcal{C}} \in M_{n/2}(\mathfrak{L}_\mathcal{C}, \chi_\mathcal{C})$$

where $\mathfrak{L}_{\mathcal{C}}$ and $\chi_{\mathcal{C}}$ are as defined in Section 6 and depend on the particular code chosen. One can note in the case that $D = 1$, the associated lattice is unimodular and so then $\mathfrak{L}_{\mathcal{C}} = 1$ and $\chi_{\mathcal{C}}$ is the trivial character. In our case of $D > 1$, we know the lattice is not unimodular so we have $\mathfrak{L}_{\mathcal{C}}$ is strictly contained in $\mathcal{O}_{L^+}$.

Write $\mathbf{F}_{p^2} = \{\alpha_1, \ldots, \alpha_{p^2}\}$. Observe that we have $\mathcal{O}_L \subset \mathfrak{p}^\vee$, so we have $\mathfrak{p}^\vee \twoheadrightarrow \mathcal{O}_L \twoheadrightarrow \mathbf{F}_{p^2}$. In particular, we choose representatives $\{x_1, \ldots, x_{p^2}\}$ in $\mathfrak{p}^\vee$ so that x_j maps to α_j under the natural surjection given above. Given $c \in \mathcal{C}$, let $l_{\alpha_j}(c)$ denote the number of times α_j appears in the codeword c. We recall the complete weight enumerator of the code $\mathcal{C}$ is defined by

$$W_{\mathcal{C}}(X_1, \ldots, X_{p^2}) = \sum_{c \in \mathcal{C}} \prod_{j=1}^{p^2} X_j^{l_{\alpha_j(c)}}.$$

Theorem 7.4. *Let $\mathcal{C} \subset \mathbf{F}_{p^2}^n$ be a linear code with $\mathcal{C} \subset \mathcal{C}^\perp$. Then we have the following identity:*

$$\theta_{\Lambda_{\mathcal{C}}} = W_{\mathcal{C}}(\theta_{x_1}, \ldots, \theta_{x_{p^2}}).$$

Proof. Observe we can write

$$\theta_{\Lambda_{\mathcal{C}}}(z) = \sum_{c \in \mathcal{C}} \sum_{v \in \Pi^{-1}(c)} e^{\pi i \operatorname{Tr}(z B_{L/L^+}(v,v))}.$$

We consider the inside summation. We have

$$\sum_{v \in \Pi^{-1}(c)} e^{\pi i \operatorname{Tr}(z B_{L/L^+}(v,v))} = \prod_{j=1}^{p^2} \theta_{x_j}^{l_{\alpha_j(c)}}$$

Now we sum over $c \in \mathcal{C}$ to obtain the result. □

We should note here that the theta series $\theta_{x_1}, \ldots, \theta_{x_{p^2}}$ are not algebraically independent, so this isn't an optimal result. In fact, they are not even distinct. For instance, the transformation property for theta series gives that $\theta_j = \theta_{-j}$ for all $j \in \mathfrak{p}^\vee$. Ideally one would define a generalized Lee weight ϕ as in [10] so that one has $\theta_{\Lambda_{\mathcal{C}}}$ is the associated polynomial W_ϕ evaluated only on the algebraically independent theta series. This is the subject of future work.

References

1. K. Betsumiya and Y. Choie. Jacobi forms over totally real fields and type II codes over Galois rings $\mathrm{GR}(2^m, f)$. *European J. Combin.*, 25(4):475–486, 2004.
2. K. Betsumiya and Y. Choie. Codes over $\mathbb{F}_4$, Jacobi forms and Hilbert-Siegel modular forms over $\mathbf{Q}(\sqrt{5})$. *European J. Combin.*, 26(5):629–650, 2005.

3. Y. Choie and S. Dougherty. Codes over rings, complex lattices and Hermitian modular forms. *European J. Combin.*, 26(2):145–165, 2005.
4. Y. Choie and E. Jeong. Jacobi forms over totally real fields and codes over $\mathbb{F}_p$. *Illinois J. Math.*, 46(2):627–643, 2002.
5. Y. Choie and H. Kim. Codes over $\mathbb{Z}_{2m}$ and Jacobi forms of genus n. *J. Combin. Theory Ser. A*, 95(2):335–348, 2001.
6. F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.
7. W. Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, revised edition, 2002. A course partially based on lectures by F. Hirzebruch.
8. P. Garrett. *Holomorphic Hilbert modular forms*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1990.
9. J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
10. S. Nishimura and T. Hiramatsu. A generalization of the Lee distance and error correcting codes. *Discrete Appl. Math.*, 156(5):588–595, 2008.
11. T. Shaska and C. Shor. Codes over $\mathbf{F}_{p^2}$ and $\mathbf{F}_p \times \mathbf{F}_p$, lattices, and theta functions. In *Advances in coding theory and cryptography*, volume 3 of *Ser. Coding Theory Cryptol.*, pages 70–80. World Sci. Publ., Hackensack, NJ, 2007.
12. T. Shaska, C. Shor, and S. Wijesiri. Codes over rings of size p^2 and lattices over imaginary quadratic fields. *Finite Fields Appl.*, 16(2):75–87, 2010.
13. L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[1]Department of Mathematics, Occidental College, Los Angeles, CA 90041

E-mail address: jimlb@oxy.edu

[2]Department of Mathematics, University of Minnesota, Minneapolis, MN 55455

E-mail address: gunso010@umn.edu

[3]Department of Mathematics, Oregon State University, Corvallis, OR 97331

E-mail address: lillyj@oregonstate.edu

[4]School of Mathematical and Statistical Sciences, Clemson University, Clemson, SC 29634

E-mail address: manganm@clemson.edu