Jacobi Forms and Hilbert-Siegel Modular Forms over Totally Real Fields and Self-Dual Codes over Polynomial Rings $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$

YoungJu Choie *
Dept. of Math. POSTECH
Pohang, Korea 790-784
email: yjc@postech.ac.kr
Steven Dougherty
Dept.of Math. University of Scranton
Scranton, PA 18510, USA
email: doughertys1@scranton.edu
Hongwei Liu
Dept. of Math. Huazhong Normal University
Wuhan, Hubei 430079 , China
email: h_w_liu@yahoo.com.cn

July 3, 2008

Abstract

In this paper, we study codes over polynomial rings and give a connection to Jacobi Hilbert modular forms, in particular, Hilbert modular forms over the totally real field via the complete weight enumerators of codes over polynomial rings.

Keywords: Hilbert Modular form, Jacobi Hilbert modular form, totally real field, polynomial ring, codes over rings.

2000 Mathematical Subject Classification: Primary: 94B05, Secondary: 13A99

*This work was partially supported by KOSEF R01-2003-00011596-0 and KRF-2007-412-J02302 grants.

1 Introduction

The connection between self-dual codes, modular lattices and modular forms has been brought out in a number of papers. There has been intensive research connecting invariant theory and coding theory over fields. The complete weight enumerators of codes over fields can be considered as an invariant polynomial under a certain finite group. It is known that one can construct various modular forms from the weight enumerators of the code by plugging special types of theta-functions, see for example [1], [2], [3], [4] and [5]. Generally, the lattices constructed in those works were either real, complex or quaternionic. In this work, we study this relationship to finite polynomial rings and lattices over totally real fields. This generalizes the construction of integral lattices induced from codes over $\mathbb{F}_4$, which has connections with Jacobi forms over the real quadratic field $K = \mathbb{Q}(\sqrt{5})$ and Hilbert modular forms over K (see [2]).

This paper is organized as follows. In Section 2, the necessary definitions and notations are introduced. In Section 3, we describe codes over the rings $\mathbb{Z}_{2m}/\langle g(x)\rangle$. In Section 4, we recall the notions of Jacobi forms and their theta series expansions. In Section 5, the complete weight enumerators of codes over $Poly(2m, r)$ are defined and the MacWilliams identities of those are derived. In Section 6, the theory of shadows is discussed. Invariant ring and Modular lattices are constructed using the MacWilliams relations in Section 7. In Section 8, by plugging proper Jacobi theta series to the complete weight enumerators of Type II codes over $Poly(2m, r)$ we construct Jacobi forms over $\mathbf{O}_K$. Moreover, we construct an algebra homomorphism between a certain invariant ring and that of Jacobi forms over $\mathbf{O}_K$.

2 Notations and Definitions

Let p be an odd prime and $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{\frac{2\pi i}{p}}$. Then its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. For convenience, let $\alpha_p := \zeta_p + \zeta_p^{-1}$, then $\mathcal{O}_K = \mathbb{Z}[\alpha_p]$. Then the elements of $\mathbb{Z}[\alpha_p]$ can be written as follows:

$$\mathcal{O}_K = \mathbb{Z}[\alpha_p] = \{a_0 + a_1\alpha_p + \cdots + a_n\alpha_p^n \mid a_i \in \mathbb{Z}, n \geq 0\}.$$

Let $\mathbb{Z}_m$ denote the residue ring of integers modulo m, and let $\mathbb{Z}_m[x]$ be the polynomial rings. We take the monic irreducible polynomial $g_1(x) \in \mathbb{Z}[x]$

of degree $r = \frac{p-1}{2}$ corresponding to α_p, i.e., $g_1(x) = b_0 + b_1x + \cdots + b_{r-1}x^{r-1} + x^r$ is irreducible and $g_1(\alpha_p) = 0$. Since for any $f(\alpha_p) \in \mathbb{Z}[\alpha_p]$, where $f(x) \in \mathbb{Z}[x]$, there exist unique polynomials $q(x), r(x) \in \mathbb{Z}[x]$ such that

$$f(x) = q(x)g_1(x) + r(x),$$

where $\deg r(x) < \deg g_1(x)$ or $r(x) = 0$. This gives that $f(\alpha_p) = r(\alpha_p)$. Hence we have that

$$\mathcal{O}_K = \mathbb{Z}[\alpha_p] = \{a_0 + a_1\alpha_p + \cdots + a_{r-1}\alpha_p^{r-1} \mid a_i \in \mathbb{Z}\}.$$

Let $g(x)$ be a polynomial in $\mathbb{Z}_{2m}[x]$ such that $g(x) \equiv g_1(x) (\bmod 2m)$. Then $g(x)$ is a monic polynomial, and there is a homomorphism

$$\Psi : \mathcal{O}_K \to \mathbb{Z}_{2m}[x]/\langle g(x)\rangle$$

given by

$$\Psi(a_0+a_1\alpha_p+a_2\alpha_p^2+\cdots+a_{\frac{p-3}{2}}\alpha_p^{\frac{p-3}{2}}) = a_0+a_1x+a_2x^2+\cdots+a_{\frac{p-3}{2}}x^{\frac{p-3}{2}} (\bmod g(x)).$$

It is easy to obtain that the kernel of Ψ is generated by $2m$, that is $\mathrm{Ker}(\Psi) = \langle 2m\rangle$. We let $Poly(2m, r)$ denote the ring $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$.

Example 2.1. *Let $p = 5$ and $m = 3$, then $r = \frac{5-1}{2} = 2$, and $\alpha_5 = e^{\frac{2\pi i}{5}} + e^{\frac{-2\pi i}{5}} = 2\cos\frac{2\pi}{5}$. Let $g_1(x) = x^2 + x - 1$. We have that*

$$\begin{aligned} \alpha_5^2 + \alpha_5 - 1 &= (\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 \\ &= \zeta_5^2 + \zeta_5^{-2} + 2 + \zeta_5 + \zeta_5^{-1} - 1 \\ &= 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0, \end{aligned}$$

since $\zeta_5^5 = 1$. This gives that $g(x) = x^2 + x + 5$, and $g(x)$ is irreducible over $\mathbb{Z}_6$. Then $\mathbb{Z}_6[x]/\langle g(x)\rangle = \{a + bx + \langle g(x)\rangle \mid a, b \in \mathbb{Z}_6\}$.

Remark 2.2. *We note that the example above shows that $g_2(x) = x^2+x+1$ and $g_3(x) = x^2 + x + 2$ are both irreducible over $\mathbb{Z}_2$ and $\mathbb{Z}_3$ respectively. But this is not always true. The following is a counter example.*

Let $m = 5$ in example above, we get that $g(x) = x^2 + x + 9$ is irreducible over $\mathbb{Z}_{10}$, but $g_5(x) = x^2 + x + 4 = (x - 2)^2$ is reducible over $\mathbb{Z}_5$.

A code C over the ring $Poly(2m, r)$ of length n is a subset of $Poly(2m, r)^n$. The code is said to be *linear* if it is a submodule. All codes are assumed to

be linear unless otherwise stated. To the ring $Poly(2m, r)$ we attach an involution $\overline{z}$ which corresponds to algebraic conjugation in the ring $\mathcal{O}_K/\langle 2m \rangle$. The involution satisfies the usual properties in that it is additive and multiplicative (since the ring is commutative). Additionally, the involution is the identity on $\mathbb{Z}_{2m}$. The ambient space $Poly(2m, r)^n$ is equipped with the following inner product

$$[v, w] = \sum v_i \overline{w_i}.$$

The orthogonal of a code is defined to be

$$C^{\perp} = \{v \mid v \in Poly(2m, r)^n \text{ such that } [v, w] = 0 \text{ for all } w \in C\}.$$

The orthogonal of a linear code is linear and satisfies $|C||C^{\perp}| = (2m)^{rn}$.

We say that a code is *self-orthogonal* if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$. We define the norm of an element $z \in Poly(2m, r)$ by $N(z) = z\overline{z}$ where the computation is done in $Poly(4m, r)$ and each coefficient in the polynomials is read as an element in $\mathbb{Z}_{4m}$ rather than as an element of $\mathbb{Z}_{2m}$. For a vector $v = (v_i)$ we define $N(v) = \sum N(v_i) = \sum v_i \overline{v_i}$. We always read the norm as an element of $Poly(4m, r)$. If a self-dual code C over $Poly(2m, r)$ has $N(v) = 0$ for all $v \in C$ then C is said to be a *Type II code*, otherwise it is said to be *Type I*. Note that the norms of self-orthogonal vectors must either be 0 or $2m$ since their inner product is 0 in $Poly(2m, r)$.

3 Codes over the Rings $\mathbb{Z}_{2m}[x]/\langle g(x) \rangle$

In this section, we first discuss some properties on the ring $\mathbb{Z}_{2m}[x]/\langle g(x) \rangle$ and then show the existence of a basis of codes over the ring $\mathbb{Z}_{2m}[x]/\langle g(x) \rangle$.

3.1 Some Properties of the Rings $\mathbb{Z}_{2m}[x]/\langle g(x) \rangle$

Suppose $2m = p_1^{e_1} \cdots p_s^{e_s}$ with p_i prime and $p_i \neq p_j$ if $i \neq j$. Let

$$\begin{aligned} \varphi : \mathbb{Z}_{2m} &\to \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}} && (1) \\ a &\mapsto (a \pmod{p_1^{e_1}}, \cdots, a \pmod{p_s^{e_s}}) && (2) \end{aligned}$$

be the canonical isomorphism. Let

$$\begin{aligned} \varphi_{p_i} : \mathbb{Z}_{2m} &\to \mathbb{Z}_{p_i^{e_i}}, && (3) \\ a &\mapsto a \pmod{p_i^{e_i}}. && (4) \end{aligned}$$

For the function $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathbb{Z}_{2m}[x]$, define

$$f_{p_i}(x) = \varphi_{p_i}(a_0) + \varphi_{p_i}(a_1)x + \cdots + \varphi_{p_i}(a_t)x^t.$$

Let $f(x) + \langle g(x)\rangle, f'(x) + \langle g(x)\rangle \in \mathbb{Z}_{2m}[x]/\langle g(x)\rangle$. Suppose $f(x) + \langle g(x)\rangle = f'(x) + \langle g(x)\rangle$ and $\deg f(x), \deg f'(x) < \deg g(x)$, then there exists a polynomial $g'(x)$ such that

$$f(x) - f'(x) = g(x)g'(x).$$

Since $g(x)$ is monic, if $g'(x) \neq 0$ then

$$\deg g(x) > \deg(f(x) - f'(x)) = \deg(g(x)g'(x)) = \deg g(x) + \deg g'(x) > \deg g(x).$$

This is a contradiction. This means that for each element of $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$, there exists a unique $f(x) + \langle g(x)\rangle \in \mathbb{Z}_{2m}[x]/\langle g(x)\rangle$ such that $\deg f(x) < \deg g(x)$.

Theorem 3.1. *Assume the notation given above. Then*

$$\mathbb{Z}_{2m}[x]/\langle g(x)\rangle \cong \mathbb{Z}_{p_1^{e_1}}[x]/\langle g_{p_1}(x)\rangle \times \cdots \times \mathbb{Z}_{p_s^{e_s}}[x]/\langle g_{p_s}(x)\rangle,$$

where the isomorphism is given as follows:

$$\varphi(f(x) + \langle g(x)\rangle) = (f_{p_1}(x) + \langle g_{p_1}(x)\rangle, \cdots, f_{p_s}(x) + \langle g_{p_s}(x)\rangle),$$

and $f(x)$ is the unique representative element of $f(x) + \langle g(x)\rangle$ with $\deg f(x) < \deg g(x)$ and $g_{p_i}(x)$ is $g_1(x)$ mod $p_i^{e_i}$.

Proof It is easy to get that the map above is a homomorphism. Let $f(x) + \langle g(x)\rangle \in \mathrm{Ker}(\varphi)$, where $f(x) = a_0 + a_1x + \cdots + a_tx^t$ with $t < \deg g(x)$. Then we get that

$$(f_{p_1}(x) + \langle g_{p_1}(x)\rangle, \cdots, f_{p_s}(x) + \langle g_{p_s}(x)\rangle) = (\langle g_{p_1}(x)\rangle, \cdots, \langle g_{p_s}(x)\rangle).$$

This means that $f_{p_i}(x) + \langle g_{p_i}(x)\rangle = \langle g_{p_i}(x)\rangle$ for all i. This implies that $g_{p_i}(x) | f_{p_i}(x)$. Note that $g_{p_i}(x)$ is a monic polynomial, and $\deg f_{p_i}(x) < \deg g_{p_i}(x)$. This implies that $f_{p_i}(x) = 0$. In fact, suppose there exists a polynomial $h(x) \neq 0$ such that $f_{p_i}(x) = g_{p_i}(x)h(x)$. Without loss of generality, suppose $h(x) = h_0 + h_1x + \cdots + h_lx^l$ with $h_l \neq 0$, then we have that

$$\deg f_{p_i}(x) = \deg g_{p_i}(x)h(x) = \deg g_{p_i}(x) + l \geq \deg g_{p_i}(x) > \deg f_{p_i}(x),$$

since $g_{p_i}(x)$ is a monic polynomial. This is a contradiction. Therefore, for each a_j we have that

$$a_j \equiv 0 \,(\mathrm{mod}\, p_i^{e_i}) \quad \text{for all } i.$$

Since $\gcd(p_1^{e_1}, \cdots, p_s^{e_s}) = 1$, this gives that for each a_j we have that $a_j \equiv 0 (\mathrm{mod}\, 2m)$. Hence $a_j = 0$ for all j and we get that $f(x) = 0$. This implies that the homomorphism above is an isomorphism. □

Lemma 3.2. *Let $\tilde{g}(x)$ be a monic polynomial over $\mathbb{Z}_{p^e}[x]$ with $\tilde{g}(x) = \Pi_{i=1}^{s} p_i^{e_i}(x)$, where $p_i(x)$ and $p_j(x)$ are relatively prime if $i \neq j$. Then*

$$\mathbb{Z}_{p^e}[x]/\langle \tilde{g}(x) \rangle \cong \mathbb{Z}_{p^e}[x]/\langle p_1^{e_1}(x) \rangle \times \cdots \times \mathbb{Z}_{p^e}[x]/\langle p_s^{e_s}(x) \rangle.$$

Proof Let

$$\varphi_1 : \mathbb{Z}_{p^e}[x]/\langle \tilde{g}(x) \rangle \rightarrow \mathbb{Z}_{p^e}[x]/\langle p_1^{e_1}(x) \rangle \times \cdots \times \mathbb{Z}_{p^e}[x]/\langle p_s^{e_s}(x) \rangle, \quad (5)$$

$$f(x) + \langle \tilde{g}(x) \rangle \mapsto (f(x) + \langle p_1^{e_1}(x) \rangle, \cdots, f(x) + \langle p_s^{e_s}(x) \rangle). \quad (6)$$

If $f(x) + \langle \tilde{g}(x) \rangle = f'(x) + \langle \tilde{g}(x) \rangle$ then $f(x) - f'(x) = \tilde{g}(x)h(x)$ for some $\tilde{h}(x)$ in $\mathbb{Z}_{p^e}[x]$. This means that

$$f(x) - f'(x) = (p_1^{e_1}(x) \cdots p_{i-1}^{e_{i-1}}(x) p_{i+1}^{e_{i+1}}(x) \cdots p_s^{e_s}(x) \tilde{h}(x)) p_i^{e_i}(x) \in \langle p_i^{e_i}(x) \rangle.$$

Hence we have that $f(x) + \langle p_i^{e_i}(x) \rangle = f'(x) + \langle p_i^{e_i}(x) \rangle$. This implies that the corresponding φ_1 is a well-defined map. It is easy to see that the map is a homomorphism. We have that

$$\mathrm{Ker}(\varphi_1) = \{ f(x) + \langle \tilde{g}(x) \rangle \mid f(x) + \langle p_i^{e_i}(x) \rangle = \langle p_i^{e_i}(x) \rangle \text{ for all } i \}.$$

This gives that $\tilde{g}(x) \big| f(x)$ since $p_i(x)$ and $p_j(x)$ are relatively prime. We have that

$$f(x) + \langle \tilde{g}(x) \rangle = \tilde{g}(x)h(x) + \langle \tilde{g}(x) \rangle = 0 + \langle \tilde{g}(x) \rangle.$$

Therefore the homomorphism is injective. This implies that φ_1 is an isomorphism. □

Lemma 3.3. *Let α be an arbitrary positive integer. Let $p(x)$ be a monic irreducible polynomial over $\mathbb{Z}_{p^e}[x]$. Then $f(x) + \langle p^{\alpha}(x) \rangle$ is a zero divisor if and only if $p(x) \big| f(x)$.*

Proof If $p(x)|f(x)$ then there exists a polynomial $h'(x)$ and an integer $\beta \leq \alpha$ such that $f(x) = p^{\beta}(x)h'(x)$. Then

$$(f(x) + \langle p^{\alpha}(x)\rangle)(p^{\alpha-\beta}(x) + \langle p^{\alpha}(x)\rangle) = \langle p^{\alpha}(x)\rangle.$$

This gives that $f(x) + \langle p^{\alpha}(x)\rangle$ is a zero divisor.

Now suppose $f(x) + \langle p^{\alpha}(x)\rangle$ is a zero divisor then there exists a polynomial $q(x)$ such that

$$f(x)q(x) + \langle p^{\alpha}(x)\rangle = \langle p^{\alpha}(x)\rangle.$$

This implies that $f(x)q(x) = p^{\alpha}(x)r(x)$ for some $r(x)$. Hence we have that $p(x)|f(x)$ since otherwise $q(x) = p^{\alpha}(x)l(x)$ and $q(x) + \langle p^{\alpha}(x)\rangle = \langle p^{\alpha}(x)\rangle$ is zero in $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$. □

Lemma 3.4. *Assume the notation given above. If $p(x)$ is a monic irreducible polynomial over $\mathbb{Z}_{p^e}[x]$ then $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$ is a chain ring with a maximal ideal $\langle p(x)\rangle$.*

Proof Let I be an ideal of $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$. If $I = \{0\}$ then $I = (0)$. Suppose $I \neq \{0\}$. If $I \neq (p(x) + \langle p^{\alpha}(x)\rangle)^i$ for $i = 1, \cdots, \alpha - 1$. Then there exists a $h(x) + \langle p^{\alpha}(x)\rangle \in I$ such that $p(x) \not| h(x)$. Since the ring $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$ is finite, by Lemma 3.3. $h(x) + \langle p^{\alpha}(x)\rangle$ is a unit in $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$. This implies that $I = \mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$. So the chain of ideals is

$$0 \subseteq \langle p^{\alpha-1}(x) + \langle p^{\alpha}(x)\rangle\rangle \subseteq \cdots \subseteq \langle p(x) + \langle p^{\alpha}(x)\rangle\rangle \subseteq \mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle.$$

Hence $\mathbb{Z}_{p^e}[x]/\langle p^{\alpha}(x)\rangle$ is a chain ring. □

Example 3.5. *For example, $\mathbb{Z}_4[x]/\langle (x+1)^2\rangle$ is a chain ring. We know that $\langle x + 1 + \langle (x+1)^2\rangle\rangle$ is the unique maximal ideal. We have that $\langle x + 1 + \langle (x+1)^2\rangle\rangle \subseteq \langle x + 2 + \langle (x+1)^2\rangle\rangle = \mathbb{Z}_4[x]/\langle (x+1)^2\rangle$, since*

$$(x+1)(x+2) = x^2 + 3x + 2 = (x^2 + 2x + 1) + (x+1) = (x+1)^2 + (x+1).$$

We have that

$$(x+2)(ax+b) = a(x^2 + 2x + 1) + 2b - a + bx = a(x+1)^2 + 2b - a + bx.$$

This gives that $\langle x + 2 + \langle (x+1)^2\rangle\rangle = \mathbb{Z}_4[x]/\langle (x+1)^2\rangle$.

Corollary 3.6. *Assume the notation given above. Then the ring* $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$ *is a principal ideal ring.*

Proof By Theorem 3.1, we have that

$$\mathbb{Z}_{2m}[x]/\langle g(x)\rangle \cong \mathbb{Z}_{p_1^{e_1}}[x]/\langle g_{p_1}(x)\rangle \times \cdots \times \mathbb{Z}_{p_s^{e_s}}[x]/\langle g_{p_s}(x)\rangle. \quad (7)$$

Suppose $g_{p_i}(x) = \prod_{j=1}^{s_i} p_{ij}^{e_{ij}}(x)$. By Lemma 3.2, for each $\mathbb{Z}_{p_i^{e_i}}[x]/\langle g_{p_i}(x)\rangle$, we have that

$$\mathbb{Z}_{p_i^{e_i}}[x]/\langle g_{p_i}(x)\rangle \cong \mathbb{Z}_{p_i^{e_i}}[x]/\langle p_{i1}^{e_{i1}}(x)\rangle \times \cdots \times \mathbb{Z}_{p_i^{e_i}}[x]/\langle p_{is_i}^{e_{is_i}}(x)\rangle. \quad (8)$$

Since the product of chain rings is a principal ideal ring, the result follows from Equation (7) and Equation (8). □

3.2 Basis of Codes over Rings $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$

It is always important to understand the generating matrix of a code. Unlike codes over fields and chain rings, the generating matrix is not always in a simple form. In this subsection, we show the existence of a basis of a code over the ring $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$. This basis forms the generator matrix of the code.

Let R be a finite principal ideal ring and let R_i be a chain ring. We begin with some definitions and lemmas. In [8] the following definitions are given with respect to Frobenius and local rings. We specialize the definitions and results to principal ideal rings and chain rings. Note that a principal ideal ring is Frobenius and a chain ring is a local ring.

Definition 1. *Let* R_i *be a chain ring with unique maximal ideal* $\mathfrak{m}_i$*, and let* $w_1, \cdots, w_s$ *be vectors in* R_i^n*. Then* $w_1, \cdots, w_s$ *are modular independent if and only if* $\sum \alpha_j w_j = 0$ *implies that* $\alpha_j \in \mathfrak{m}_i$ *for all* j*. The vectors* $v_1, \cdots, v_k$ *in* R^n *are called modular independent if* $\Phi_i(v_1), \cdots, \Phi_i(v_k)$ *are modular independent for some* i*. Let* $v_1, \cdots, v_k$ *be vectors in* R^n*. The vectors* $v_1, \cdots, v_k$ *are called independent if* $\sum \alpha_j v_j = 0$ *implies that* $\alpha_j v_j = 0$ *for all* j*.*

Remark 3.7. *It is possible to have vectors that are independent but not modular independent and to have vectors that are modular independent but not independent. See [8] for examples.*

Following the remark above, we have the following definition.

Definition 2. *Let C be a code over R. The codewords $c_1, c_2, \cdots, c_k$ are called a basis of C if they are independent, modular independent and generate C.*

Theorem 3.8. *Assume the notation given above. Let C be a code over $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$, then any basis for C contains exactly r codewords, where r is the rank of C.*

Proof By Corollary 3.6, we know that the ring $\mathbb{Z}_{2m}[x]/\langle g(x)\rangle$ is a principal ideal ring. Then the result follows from Theorem 4.9 in [8]. □

4 Jacobi form over the totally real field K

We recall the definition of Jacobi forms over the totally real field $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and theta-functions. We follow the definition given in [15].

4.1 Jacobi Group

The Jacobi group of $K = Q(\zeta_p + \zeta_p^{-1})$ will be denoted by

$$\Gamma^J(K) := SL_2(\mathcal{O}_K) \propto \mathcal{O}_K^2.$$

This group acts on $\mathcal{H}^r \times \mathbb{C}^r$, where $\mathcal{H}$ denotes the complex upper half plane. Variables of this space will be listed as, $(\tau, z) := (\tau_1, .., \tau_r, z_1, .., z_r)$. The action of $\Gamma^J(K)$ on the space $\mathcal{H}^r \times \mathbb{C}^r$ are given by, $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathcal{O}_K)$,

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot (\tau, z) := \left(\frac{\alpha^{(1)}\tau_1 + \beta^{(1)}}{\gamma^{(1)}\tau_1 + \delta^{(1)}}, .., \frac{\alpha^{(r)}\tau_r + \beta^{(r)}}{\gamma^{(r)}\tau_r + \delta^{(r)}}, \frac{z_1}{\gamma^{(1)}\tau_1 + \beta^{(1)}}, .., \frac{z_r}{\gamma^{(r)}\tau_r + \beta^{(r)}}\right)$$

and, for all $[\lambda, \mu] \in \mathcal{O}_K^2$,

$$[\lambda, \mu] \cdot (\tau, z) := (\tau_1, \tau_2, .., \tau_r, z_1 + \lambda^{(1)}\tau_1 + \mu^{(1)}, .., z_r + \lambda^{(r)}\tau_r + \mu^{(r)}).$$

Remark 4.1. *It is known(see [11]) that $SL_2(\mathcal{O}_K)$ is generated by the matrices*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \forall b \in \mathcal{O}_K.$$

4.2 Jacobi forms

We first introduce the following notations; for $\tau \in \mathcal{H}^r, z \in \mathbb{C}^r, \gamma, \delta, \ell \in \mathcal{O}_K$, denote

$$\mathcal{N}(\gamma\tau + \delta) := \prod_{j=1}^{r} (\gamma^{(j)}\tau_j + \delta^{(j)}),$$

$$e^{2\pi i T r_{K/Q}(\ell \frac{cz^2}{c\tau+d})} := \prod_{j=1}^{r} e^{2\pi i \ell^{(j)} \frac{c^{(j)} z_j^2}{c^{(j)}\tau_j + d^{(j)}}},$$

$$e^{-2\pi i T r(\ell(\lambda^2\tau + 2\lambda z))} := \prod_{j=1}^{r} e^{-2\pi i \ell^{(j)}(\lambda^{(j)2}\tau_j + 2\lambda^{(j)} z_j)}.$$

Definition 3. *Given $k \in \mathbb{Z}$ and $\ell \in \mathcal{O}_K$, a function $g : \mathcal{H}^r \times \mathbb{C}^r \to \mathbb{C}$ is said to be a Jacobi forms of weight k and index ℓ for the totally real field K if it is an analytic function satisfying*

1.

$$\begin{aligned}(g|_{k,\ell} M)(\tau, z) &:= \mathcal{N}(c\tau + d)^{-k} e^{-2\pi i T r(\ell \frac{cz^2}{c\tau+d})} g(M \cdot (\tau, z)) \\ &= g(\tau, z), \forall M = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_K),\end{aligned}$$

2.

$$(g|_\ell [\lambda, \mu])(\tau, z) := e^{-2\pi i T r(\ell(\lambda^2\tau + 2\lambda z))} g(\tau, [\lambda, \mu] \cdot z) = g(\tau, z).$$

It has the following Fourier expansion:

3.

$$g(\tau, z) = \sum_{n, r \in \delta_K^{-1}, n \geq 0} c(n, r) e^{2\pi i T r(n\tau + rz)}.$$

Here δ_K^{-1} is the inverse different of K. (See a standard textbook for algebraic number theory, for instance [6] (page 203), for a detailed definition of this term.)

Remark 4.2. 1. *The $\mathbb{C}$-vector space of Jacobi forms of weight k and index ℓ for the field K is denoted by $\mathcal{J}_{k,\ell}(\Gamma_1(\mathcal{O}_K))$.*

2. *Note that letting $z = 0$ one obtains a Hilbert modular form $g(\tau, 0)$ from a Jacobi form over K.*

4.3 Theta Series

The following theta-function was first introduced and studied in [15] to show the correspondence between the space of Jacobi forms over K and that of the vector valued modular forms.

$$\text{For each } \mu \in \mathcal{O}_K,\ \theta_{m,\mu}(\tau, z) := \sum_{u \in \delta_K^{-1}, u \equiv \mu \pmod{(2m)}} e^{2\pi i Tr(\frac{u^2 \tau}{4m} + uz)}. \quad (9)$$

Then, by the Poisson summation formula, the theta-series satisfies the following transformation formula.

Lemma 4.3. *1.* $(\theta_{m,\mu}|_{\frac{1}{2},m} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix})(\tau, \vec{z}) = e^{2\pi i Tr(\frac{\mu^2 b}{4m})} \theta_{m,u}(\tau, z), \forall b \in \mathcal{O}_K$.

2.

$$(\theta_{m,\mu}|_{\frac{1}{2},m} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix})(\tau, z) = \frac{\chi \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}{(4m)^{\frac{r}{2}}} \sum_{\nu \in \mathcal{O}_K / 2m\mathcal{O}_K} e^{2\pi i Tr(\frac{\mu\nu}{4m})} \theta_{m,\nu}(\tau, z),$$

with $\chi^4(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}) = 1$.

Proof The standard tool using the Poisson summation formula gives the result which was stated in [15]. □

5 Weight Enumerators and MacWilliams relations

We shall define a series of weight enumerators and find the MacWilliams relations for these weight enumerators.

For a code C over $Poly(2m, r)$ define the complete weight enumerator by

$$cwe_C(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{r-1}}) = \sum_{v \in C} \prod_{a \in Poly(2m,r)} x_a^{n_a(v)} \quad (10)$$

where $n_a(v) = |\{j \mid v_j = a\}|$. The complete weight enumerator is a homogenous polynomial in $(2m)^r$ variables.

On the ring $Poly(2m, r)$ define the relation $a \sim b$ if $a = b\epsilon$ where ϵ is a unit in the ring. Let $P_{2m,r} := Poly(2m, r)/\sim$ denote the equivalence classes of the ring under this relation. The symmetric weight enumerator is given by

$$swe_C(x_{\alpha_0}, x_{\alpha_1}, \ldots) = \sum_{v \in C} \prod_{a \in P_{2m,r}} x_a^{n'_a(v)} \tag{11}$$

where $n'_a(v) = |\{j \mid v_j \sim a\}|$. The symmetric weight enumerator is a homogenous polynomial in $|P_{2m,r}|$ variables.

The Hamming weight enumerator is given by

$$W_C(x, y) = \sum_{v \in C} x^{n-h(v)} y^{h(v)} \tag{12}$$

where $h(v)$ is the number of non-zero elements in the code. The Hamming weight enumerator is a homogenous polynomial in 2 variables.

Note that $W_C(x, y) = cwe(x, y, y, \ldots, y)$ and the symmetric weight enumerator is formed by replacing each occurrence of x_i with $x_{[i]}$, where $[i]$ denotes the equivalence class containing i.

Define the character $\chi_1 : Poly(2m, r) \to \mathbb{C}$ by

$$\chi_1(a_0 + a_1 x + \cdots + a_{r-1} x^{r-1}) = \zeta_{2m}^{\sum a_i} \tag{13}$$

and

$$\chi_\alpha(\beta) = \chi_1(\alpha \cdot \beta) \tag{14}$$

for any $\alpha, \beta \in Poly(2m, r)$.

Let T be a $(2m)^r$ by $(2m)^r$ matrix indexed lexicographically by the elements of $Poly(2m, r)$, where the α-th row and β-th column of T is given by the values of $\chi_\alpha(\beta)$. Specifically,

$$T_{a_0+a_1x+\cdots+a_rx^r, b_0+b_1x+\ldots b_{r'}x^{r'}} = \zeta_{2m}^{c_i}, \zeta_{2m} = e^{\frac{2\pi i}{2m}} \tag{15}$$

where $\sum c_i x^i = \sum a_i x^i \overline{\sum b_i x^i} \pmod{g(x)}$.

Essentially the matrix T is a character table of the underlying additive group, with the columns permuted by conjugation, where the characters are canonically associated with multiplication in the ring.

To obtain the MacWilliams relations for the symmetric weight enumerator we define the following matrix. Let S be a $|P_{2m,r}|$ by $|P_{2m,r}|$ matrix

indexed by the elements of $P_{2m,r}$ with

$$S_{[a],[b]} = \sum_{c \sim a} T_{c,b}. \tag{16}$$

The following notation is used to describe an action of a matrix on a polynomial ring. If $A = (a_{ij})$ is an n by n matrix and $f(x_1, \ldots, x_n)$ a polynomial in $\mathbb{C}[x_1, x_2, \ldots, x_n]$ then

$$A \cdot f(x_1, \ldots, x_n) = f(\sum_{1 \le j \le n} a_{1j}x_j, \ldots, \sum_{1 \le j \le n} a_{nj}x_j). \tag{17}$$

We can now state the MacWilliams relations for the complete and symmetric weight enumerator.

Theorem 5.1. *Let C be a code over $Poly(2m, r)$ then*

$$cwe_{C^\perp}(X) = \frac{1}{|C|} cwe_C(T \cdot X) \tag{18}$$

and

$$swe_{C^\perp}(X) = \frac{1}{|C|} swe_C(S \cdot X) \tag{19}$$

Proof Follows from the results in [7]. □

Then specializing the variables we have the following.

Corollary 5.2. *Let C be a code over $Poly(2m, r)$ then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + ((2m)^r - 1)y, x - y). \tag{20}$$

Definition 4. *For codes C and D over $Poly(2m, r)$ define the complete joint weight enumerator by*

$$J_{C,D}(X) = \sum_{v \in C} \sum_{v' \in D} \prod_{(a,b) \in (Poly(2m,r))^2} x_{(a,b)}^{n_{(a,b)}(v,v')} \tag{21}$$

where $n_{a,b}(v, v') = |\{j \mid v_j = a, v'_j = b\}|$.

The complete joint weight enumerator is a homogeneous polynomial in $(2m)^{2r}$ variables.

Corollary 5.3. *Let C and D be codes over $Poly(2m, r)$ then*

$$J_{C^\perp,D^\perp}(X) = \frac{1}{|C|}\frac{1}{|D|}J_{C,D}((T \otimes T) \cdot X) \tag{22}$$

$$J_{C^\perp,D}(X) = \frac{1}{|C|}J_{C,D}((T \otimes I) \cdot X) \tag{23}$$

$$J_{C,D^\perp}(X) = \frac{1}{|D|}J_{C,D}((I \otimes T) \cdot X). \tag{24}$$

Proof Follows from Theorem 5.1 and the results in [7]. □

6 Shadows

Let C be a Type I code over $Poly(2m, r)$. A vector v in C is said to be *doubly-even* if $N(v) = 0$ in $Poly(4m, r)$.

Lemma 6.1. *The sum of two doubly-even vectors in a self-dual code C is doubly-even.*

Proof Let v and w be two doubly-even vectors in C. Do the following computation in $Poly(4m, r)$:

$$\begin{aligned}(v+w)(\overline{v+w}) &= (v+w)(\overline{v}+\overline{w}) \\ &= v\overline{v} + w\overline{w} + v\overline{w} + \overline{v}w \\ &= v\overline{w} + \overline{v}w\end{aligned}$$

since $v\overline{v}$ and $w\overline{w}$ are both 0 in $Poly(4m, r)$. Now $\overline{\overline{v}w} = v\overline{w}$. Since $v\overline{w}$ and $\overline{v}w$ are both 0 in $Poly(2m, r)$ they are actually equal since $\overline{c} = c$ where c is a constant in $\mathbb{Z}_{2m}$. Hence we have

$$v\overline{w} + \overline{v}w = 2v\overline{w} = 0$$

in $Poly(4m, r)$. □

Let C_0 be the subcode of doubly-even vectors in C. The linear map $v \to N(v)$ has kernel C_0 and an image of size 2, hence C_0 is of index 2 in C. As usual we define the shadow to be

$$S = C_0^\perp - C = C_1 \cup C_3 \tag{25}$$

and

$$C_2 = C - C_0. \tag{26}$$

Lemma 6.2. *Let C be a Type I code over Poly$(2m, r)$. Then*

$$cwe_{C_0}(x_0, \ldots, x_{g(x)-1}) = \frac{1}{2}(cwe_C(x_0, \ldots, x_{g(x)-1}) + cwe_C(y_0, \ldots, y_{g(x)-1})) \tag{27}$$

where $y_\alpha = \zeta_{4m}^{N(\alpha)} x_\alpha$.

Proof If the vector v is doubly-even then it is counted twice and if it is singly-even then it is counted once positively and once negatively. □

Theorem 6.3. *Let C be a Type I code with shadow S, then*

$$cwe_S(x_0, \ldots, x_{g(x)-1}) = \frac{1}{|C|}(T \cdot cwe_C(y_0, \ldots, y_{g(x)-1})) \tag{28}$$

where T is the matrix that gives the MacWilliams relations.

Proof Simply apply the MacWilliams relations to both sides of equation (27). That is

$$\begin{aligned}
cwe_S(x_0, \ldots, x_{g(x)-1}) &= cwe_{C_0^\perp}(x_0, \ldots, x_{g(x)-1}) - cwe_C(x_0, \ldots, x_{g(x)-1}) \\
&= \frac{1}{|C_0|}(\frac{1}{2}(cwe_C(T \cdot (x_0, \ldots, x_{g(x)-1})) \\
&+ cwe_C(T \cdot (y_0, \ldots, y_{g(x)-1}))) - cwe_C((x_0, \ldots, x_{g(x)-1})) \\
&= \frac{1}{|C|} cwe_C(T \cdot (x_0, \ldots, x_{g(x)-1})) - cwe_C(x_0, \ldots, x_{g(x)-1}) \\
&+ \frac{1}{|C|} cwe_C(T \cdot (y_0, \ldots, y_{g(x)-1})) \\
&= \frac{1}{|C|} cwe_C(T \cdot (y_0, \ldots, y_{g(x)-1}))
\end{aligned}$$

□

There exists vectors s and t with

$$C_2 = C_0 + \mathbf{t}, \quad C_1 = C_0 + \mathbf{s}, \quad C_3 = C_0 + \mathbf{s} + \mathbf{t}.$$

Let $\alpha = [\mathbf{s}, \mathbf{s}]$ and $\beta = [\mathbf{s}, \mathbf{t}]$ then it is clear that the orthogonality relations are given in Table 1.

The glue group of $C_0^\perp / C_0$ can be either the cyclic group of order 4 or the Klein-4 group. We see that in either case $s + s = 2c \in C$ and hence $[2s, t] = 0$ and so $2[s, t] = 0$. This implies that $[s, t] = 0$ or m. But $[t, s] \neq 0$, since otherwise s would be in C. Therefore we have that $\beta = m$. We notice that $N(s) \equiv \alpha \pmod{2m}$. If the glue group is the Klein-4 group

Table 1: Orthogonality Relations

	C_0	C_1	C_2	C_3
C_0	0	0	0	0
C_1	0	α	β	$\alpha+\beta$
C_2	0	β	0	β
C_3	0	$\alpha+\beta$	β	$\alpha+2\beta$

then $2s \in C_0$ and $N(2s) \equiv 0 \pmod{4m}$. Then $4N(s) \equiv 0 \pmod{4m}$. This implies that α is either 0 or m. If the glue group is cyclic then $2s \in C_2$ and $N(2s) \equiv 2m \pmod{4m}$. Then $4N(s) \equiv 2m \pmod{4m}$ and we have $2\alpha \equiv m \pmod{2m}$ and so $\alpha = \frac{m}{2}$. This case can happen only when m is even.

7 Modular Lattices

Let "Tr " denote the trace function $Tr : K \to \mathbb{Q}$. Note that $Tr(\mathcal{O}_K) \subset \mathbb{Z}$.

We attach to K^n the inner product

$$\langle a, b\rangle = \sum Tr(a_i \cdot b_i), \tag{29}$$

The dual lattice is defined as

$$L^* = \{v \mid v \in K^n, \quad \langle v, w\rangle \in \mathcal{O}_K \text{ for all } w \in L\}. \tag{30}$$

For a lattice L in K^n we say that L is integral if $L \subseteq L^*$ and unimodular if $L = L^*$. Additionally, if $Tr(\langle v, v\rangle) \in 2\mathbb{Z}$ for all $v \in L$ then the lattice is said to be even.

We denote the inverse image $\tilde{u}$ of $u \in Poly(2m, r)$ under the reduction map modulo an ideal $(2m)$, $\Psi : \mathcal{O}_K \to Poly(2m, r)$.

For a code C over $Poly(2m, r)$ of length n define

$$\Lambda(C) = \{\frac{1}{\sqrt{(2m)^r}}\tilde{u} \mid u \in C\}. \tag{31}$$

Theorem 7.1. *If C is a self-dual code over $Poly(2m, r)$ then $\Lambda(C)$ is a unimodular lattice. Moreover, if C is Type II then $\Lambda(C)$ is even.*

Proof Let v and w be vectors in C, then

$$\begin{aligned}\langle \frac{1}{\sqrt{(2m)^r}}\tilde{v}, \frac{1}{\sqrt{(2m)^r}}\tilde{w}\rangle &= \frac{1}{(2m)^r} Tr(\sum \tilde{v_i}\tilde{w_i}) \\ &= \frac{1}{(2m)^r}\sum Tr(\tilde{v_i}\tilde{w_i}).\end{aligned}$$

Note that $Tr(\tilde{v_i}\tilde{w_i}) \equiv v_i\overline{w_i} \pmod{(2m)}$ and we have that the lattice is integral. If the code is Type II, then reading $v_i\overline{w_i} \pmod{4m}$ we see that $Tr(\tilde{v_i}\tilde{w_i}) \equiv 0 \pmod{4m}$ and so $\frac{1}{2m}Tr(\tilde{v_i}\tilde{w_i}) \in 2\mathbb{Z}$, giving that the lattice is even.

The standard proof shows that the code is unimodular, i.e. we have

$$2m\mathcal{O}_K^n \subseteq \sqrt{2m}\Lambda(C) \subseteq \mathcal{O}_K^n$$

and $V(2m\mathcal{O}_K^n) = (2m)^n$ and $|\sqrt{2m}\Lambda(C)/2m\mathcal{O}_K^n| = (2m)^{\frac{n}{2}}$. Which gives that $V(\sqrt{2m}\Lambda(C)) = (2m)^{\frac{n}{2}}$ and then $V(\Lambda(C)) = 1$. □

Let L be a lattice that is not even and let $L_0 = \{v \mid v \in L,\ Trv, v \in 2\mathbb{Z}\}$. Then L_0 is of index 2 in L and

$$L_0^* = L_0 \cup L_1 \cup L_2 \cup L_3 \tag{32}$$

with $L = L_0 \cup L_2$. The shadow is defined by $\Sigma = L_1 \cup L_3$. The next theorem follows naturally from the definition.

Theorem 7.2. *Let C be a Type I code over $Poly(2m, r)$ with $\Lambda(C) = L$. Then $\Lambda(C_0) = L_0$, $\Lambda(C_2) = L_2$ and $\Lambda(S) = \Sigma$.*

The theta series for a lattice is defined by

$$\Theta_L(q) = \sum_{v \in L} q^{\frac{<v,v>}{2}} \tag{33}$$

As usual the variable $q = e^{2\pi i z}$.

The standard proof gives that

$$\Theta_{L^*}(z) = (det\ L)^{\frac{1}{2}}(\frac{i}{z})^{\frac{n}{2}}\Theta_L(\frac{-1}{z}). \tag{34}$$

It is clear that

$$\Theta_{L_0} = \frac{1}{2}(\Theta_L(z) + \Theta_L(z+1)). \tag{35}$$

The standard computation gives that

$$\Theta_\sigma(z) = (\frac{i}{z})^{\frac{n}{2}}\Theta_L(1 - \frac{1}{z}) \tag{36}$$

8 Main Theorems

Theorem 8.1. *Let $Inv(G_{II}(cwe))$ be the invariant ring of the group defined before.*

Then the following map

$$\Phi : Inv(G_{II}(cwe)) \to \oplus_{\ell \in \mathbb{Z}} \mathcal{J}_{4\ell,(8m\ell)}(\Gamma_1(\mathcal{O}_K)),$$

given by

$$\Phi(H(x_a | \forall a \in Poly(2m,r))) = H(\theta_{m,\mu} \,|\, \forall \mu \in \mathcal{O}_K/(2m))$$

$\forall H \in Inv(G_{II}(cwe))$, *is an algebra homomorphism.*

Before we prove the main theorem we need the following lemma:

Lemma 8.2. *Let $G_{m,r}$ be a group*

$$G_{m,r} := < h_m, A_\gamma | \forall \gamma \in \mathcal{O}_K >,$$

where each of A_γ is a matrix indexed by $Poly(2m,r)$ such that

$$(A_\gamma)_{uv} = \delta_{u,v} \cdot \zeta_{2m}^{\frac{Tr(\gamma u^2)}{2}}, (h_m)_{uv} = \zeta_{4m}^{Tr(uv)}.$$

Then the group $G_{m,r}$ and the group $G_{II}(cwe)$ are the same.

Proof of Theorem 8.1 It is enough to check the transformation formula for
$g(\tau,z) := H(\theta_{m,\mu}(\tau,z) \,|\, \mu \in Poly(m,r))$; with $degree(H) = \ell, \forall b \in \mathcal{O}_K$,

$$\begin{aligned} g(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot (\tau,z)) &= H((\theta_{m,\mu}(\tau+b,z) | \mu \in Poly(m,r))) \\ &= H((\zeta_{2m}^{\frac{Tr(\mu^2 b)}{2}} \cdot \theta_{m,\mu}(\tau,z) | \mu \in Poly(m,r))) \\ &= H(A_b(\theta_{m,\mu}(\tau,z) | \mu \in Poly(m,r))) \\ &= H(\theta_{m,\mu}(\tau,z) | \mu \in Poly(m,r)). \end{aligned}$$

Last equality follows from the fact that $H(x_a) \in Inv(G_{II}(cwe))$ and $A_b = (A_b)_{\mu\mu} = (\zeta_{2m}^{\frac{Tr(\mu^2 b)}{2}}) \in Inv(G_{m,r}), \forall b \in \mathcal{O}_K$ from Lemma4.3.

Next,

$$g(-\frac{1}{\tau}, \frac{z}{\tau}) = H(\theta_{m,\mu}(-\frac{1}{\tau}, \frac{z}{\tau}) | \mu \in Poly(m,r))$$

$$= H(\chi \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mathcal{N}(\frac{\tau}{2})^{\frac{1}{2}} e^{2\pi i Tr(m\frac{z^2}{\tau})} 2^{\frac{r}{2}} h_m \cdot (\theta_{m,\mu}(\tau,z)|\mu \in Poly(m,r)))$$

$$= \mathcal{N}(\tau)^{\frac{\ell}{2}} e^{2\pi i Tr(m\ell\frac{z^2}{\tau})} \quad H \quad (h_m \cdot (\theta_{m,\mu}(\tau,z)|\mu \in Poly(m,r)))$$
$$(\text{ since } \ell = deg(F) \equiv 0 \pmod 4)$$

$$= \mathcal{N}(\tau)^{\frac{\ell}{2}} e^{2\pi i Tr(m\ell\frac{z^2}{\tau})} H((\theta_{m,\mu}(\tau,z)|\mu \in Poly(m,r))).$$

Here, $M \cdot (\theta_{m,\mu}|\mu \in Poly(m,r))$ denotes matrix multiplication. Next, to check the elliptic property, first note that, for any $(\lambda_1, \lambda_2) \in \mathcal{O}_K^2$, and for each $\mu \in Poly(m,r)$,

$$\theta_{m,\mu}(\tau, z+\lambda_1\tau+\lambda_2) = \sum_{r\in\delta_K^{-1}, r\equiv\mu \pmod{(2m)}} e^{2\pi i Tr(\frac{r^2\tau}{4m}+r(z+\lambda_1\tau+\lambda_2))}$$

$$= e^{-2\pi i Tr(m(\lambda_1^2\tau+2\lambda_1 z))} \sum_{r\in\delta_K^{-1}, r\equiv\mu \pmod{(2m)}} e^{2\pi i Tr(\frac{(r+2\lambda_1)^2}{4m}\tau+(r+2\lambda_1)z)}$$

$$= e^{-2\pi i Tr(m(\lambda_1^2\tau+2\lambda_1 z))}\theta_{m,\mu}(\tau,z).$$

So, the elliptic property of $g(\tau,z)$ is now immediate. The condition at the cusps can also be checked from that of each theta-series $\theta_{m,\mu}(\tau,z)$. We omit the detailed proof. □

References

[1] E. Bannai, S.T. Dougherty, M. Harada, and M. Oura, Type II Codes, Even Unimodular Lattices, and Invariant Rings, *IEEE-IT*, Vol. 45, No. 4, 1194-1205, 1999.

[2] K. Betsumiya and Y. Choie, Jacobi Forms over Totally Real Fields and Type II Codes over Galois Rings $GR(2^m, f)$, Euro. Journal of Combinatorics, Vol. 25, No. 4, 475-486, 2004.

[3] Y. Choie and S.T. Dougherty, Codes over Rings, Complex Lattices and Hermitian Modular Forms, Euro. Journal of Combinatorics, Vol. 26, No. 2., 145-165, 2005.

[4] Y. Choie and S.T. Dougherty, Codes over Σ_{2m} and Jacobi Forms over the Quaternions, Appl. Algebra Engr. Com. Comput., Vol. 15, No. 2, 129-147, 2004.

[5] Y. Choie and N. Kim, The Complete Weight Enumerator of Type II Code over $\mathbb{Z}_4$ and Jacobi Forms, *IEEE-IT*, Vol. 4, No. 1, 396-399, 2001.

[6] H.Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1995.

[7] S.T. Dougherty, MacWilliams Relations for Codes over Groups and Rings, preprint.

[8] S.T. Dougherty, H. Liu, Independence of Vectors in Codes over Rings, submitted.

[9] P.Gaborit, V. Pless, P.Solé and O.Atkin, Type II codes over $\mathbb{F}_4$, Finite Fields and Their Applications, Vol. 8, 171-183, 2002.

[10] A.M.Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in Actes, Congrés International de Mathématiques (Nice, 1970), Gauthiers-Villars, Paris, Vol. 3, 221-215, 1971.

[11] B. Liehl, On the Group $S\ell_2$ over Orders or Arithmetic Type, J. Reine Angew. Math., Vol. 323, 153-171, 1981.

[12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[13] F.J. MacWilliams, A.M. Odlyzko and N.J.A. Sloane, Self-Dual Codes over $GF(4)$, J. Comb. Th.(Ser. A), Vol. 25, 288–318, 1978.

[14] G. Nebe, H.-G. Quebbemann, E.M. Rains, and N.J.A. Sloane, Complete Weight Enumerators of Generalized Doubly-Even Self-Dual Codes, Finite Fields and Their Applications, Vol. 10, 540-550, 2004.

[15] H. Skogman, Jacobi Forms over Totally Real Number Fields, Results Math., Vol. 39, No 1-2, 169-182, 2001.