Proceedings of the Jangjeon Mathematical Society
29 (2026), No. 2, pp. 319 – 329

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2026.29.2.013

# LATTICES AND SELF-DUAL CODES OVER A RING

ANKUR SINGH, PRATYUSH KUMAR*, AND PUNIT JAIN

Abstract. We consider a biquadratic field $K = \mathbb{Q}(\sqrt{-l}, \sqrt{-m})$ with $-l \equiv 1 \pmod 4$ and $-m \equiv 3 \pmod 4$ and define the ring of integers that corresponds to the field $K$. We construct lattices on the ring of integers $\mathcal{O}$ and discuss unimodular lattices. We shall define the self-dual codes over the ring $R$ and give the MacWilliams relation over the ring $R$. We shall be considering three situations for the ring $R$ depending on the prime 2 being inert, ramified, and split for the ring of integers.

2010 Mathematics Subject Classification 94B05, 11T71, 11H06 .
Keywords and phrases. Lattices, Self-dual codes, MacWilliams Identity.

Submission Date: 30 January 2024

## 1. Introduction

As explained in [22], lattices and modular forms have several intriguing relationships with their weight enumerators over the Frobenius ring. Various academics have explored for a long time, codes were generated over the ring and lattice over the imaginary quadratic field. Christine Bachoc [6] considered an imaginary quadratic field of discriminant $l$ and also considered the quaternion field over $\mathbb{Q}$ which is ramified at $l$ and $\infty$ to discuss the modular lattices. For a detailed description we refer to [11, 15, 16, 18, 19].

Bachoc [6] over the imaginary quadratic field constructed the ring of integers and identified the form of $p\mathcal{O}_K$ to consider the quotient $\mathcal{O}_K/p\mathcal{O}_K$. In [12], Chua examined $\mathbb{Q}(\sqrt{-l})$ the imaginary quadratic field and identified $GF(4)$ and $\mathbb{F}_2 \times \mathbb{F}_2$ as the order 4 ring for different $l$. Chua built a lattice over $GF(4)$ and $\mathbb{F}_2 \times \mathbb{F}_2$ and investigated the theta series, which were Hermitian, which also connects the various weight enumerators of different levels. For a detailed description we refer to [1–5, 9, 10].

In [20], Shaska and Shor investigated $K = \mathbb{Q}(\sqrt{-l})$, with $l$ being an integer, which is square-free and we get $\mathbb{F}_4$ and $\mathbb{F}_2 \times \mathbb{F}_2$ as the ring of order 4 for $l$ being different. They talked about the theta series and their relationship to the symmetrized weight enumerator and complete weight enumerator. They have seen that different $l$ values lead to the theta series symmetrized weight enumerator polynomial. They expanded the concept in [21] to the ring of size $p^2$, giving the generic form of $\mathcal{O}_K/p\mathcal{O}_K$ and discussing bounds for the theta series.

In [13] Dougherty et.al, considered the quotient of $\mathcal{O}_K$ by $p^e\mathcal{O}_K$ over the quadratic imaginary field $\mathbb{Q}(\sqrt{-l})$ and for different values of $l$ with a polynomial of order 2 they found the ring as $GR(p^e, 2)$, for $u^2 = 0$, $\mathbb{Z}_{p^e} + u\mathbb{Z}_{p^e}$,

*Corresponding Author.

$\mathbb{Z}_{p^e} \times \mathbb{Z}_{p^e}$. In various circumstances, they described the theta series and weight enumerator across these rings.

Some of my recent works on quadratic imaginary field [1, 3] motivated me to extend the work to biquadratic imaginary field. In this work, we look at the biquadratic imaginary field $\mathbb{Q}(\sqrt{-l}, \sqrt{-m})$, where $l$ and $m$ are relatively prime and $\mathcal{O}$ is the ring of integers. To visualise the form of the ring in different scenarios where $l$ and $m$ are relatively prime, we take the quotient of $\mathcal{O}$ by $2\mathcal{O}$. We consider various situations for the polynomial $f(x)$ and $g(y)$ and we see that if 2 is inert in $\mathbb{Z}[w_l]$ and $g(y)$ is irreducible mod 2 then $\mathcal{O}/2\mathcal{O} \simeq \mathbb{F}_{16}$. If 2 is ramified in $\mathbb{Z}[w_l]$ and $g(y) \equiv (y-c)^2 \pmod 2$ then $\mathcal{O}/2\mathcal{O} \simeq \mathbb{F}_4 + u\mathbb{F}_4$, with $u^2 = 0$. If 2 is split in $\mathbb{Z}[w_l]$ and $g(y) \equiv (y-c)(y-c') \pmod 2$ with $c \neq c' \pmod 2$ the $\mathcal{O}/2\mathcal{O} \simeq \mathbb{F}_4 \times \mathbb{F}_4$. We also discuss some results on lattices and codes over a ring $R$ with Hermitian inner product and we found the ring of integers as $\mathbb{Z}[w_l, w_m]$ as $l$ and $m$ are relatively prime. Over a ring $R$, we explore self-dual codes in all possible situations and we also discuss the MacWilliams identity for a code over the ring $R$ by defining the matrix $T_i$ that correspond to a ring in each case for the associated ring.

## 2. Preliminaries

2.1. **Codes over a ring and its structure.** Let $K = \mathbb{Q}(\sqrt{-l}, \sqrt{-m})$, $l \equiv 3 \pmod 4$ and $m \equiv 1 \pmod 4$. We first look at the structure of the ring of integers $\mathcal{O}$ of $K$. The ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-l})$ is $\mathbb{Z}[w_l]$ for $l \equiv 3 \pmod 4$, where $w_l = \frac{-1+\sqrt{-l}}{2}$ and $w_l^2 + w_l + \frac{l+1}{4} = 0$. Also the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-m})$ is $\mathbb{Z}[w_m]$ for $m \equiv 1 \pmod 4$, where $w_m = \sqrt{-m}$ and $w_m^2 + m = 0$. If $f(x) \in \mathbb{Z}[x]$ and $g(y) \in \mathbb{Z}[y]$. It is simple to see $\dfrac{\mathbb{Z}[x,y]}{\langle f(x)\rangle} \simeq \dfrac{\mathbb{Z}[x]}{\langle f(x)\rangle}[y]$ and $\dfrac{\frac{\mathbb{Z}[x]}{\langle f(x)\rangle}[y]}{\langle g(y)\rangle} \simeq \dfrac{\mathbb{Z}[x,y]}{\langle f(x), g(y)\rangle}$. The ring of integers $\mathbb{Z}[w_l]$ can also be thought of as a ring which is isomorphic to $\dfrac{\mathbb{Z}[x]}{\langle f(x)\rangle}$, where $f(x)$ is an irreducible polynomial of degree 2 over $\mathbb{Z}$ whose root is $w_l$. The ring of integers $\mathcal{O}$ of $K$ is an integral extension of $\mathbb{Z}[w_l] \simeq \dfrac{\mathbb{Z}[x]}{\langle f(x)\rangle}$. Therefore the ring of integers $\mathcal{O}$ of $K$ is isomorphic to the ring $\dfrac{\frac{\mathbb{Z}[x]}{\langle f(x)\rangle}[y]}{\langle g(y)\rangle} \simeq \dfrac{\mathbb{Z}[x,y]}{\langle f(x), g(y)\rangle}$ for some irreducible polynomial $g(y)$ of degree 2 over $\mathbb{Z}$. Thus the ring of integers $\mathcal{O}$ of $K$ is isomorphic to $\dfrac{\mathbb{Z}[w_l][y]}{g(y)} \simeq \mathbb{Z}[w_l, w_m]$, where $w_l$ and $w_m$ satisfy the polynomials $w_l^2 + w_l + \dfrac{l+1}{4} = 0$ and $w_m^2 + m = 0$ respectively. Now we determine the form of the quotient $\mathcal{O}/2\mathcal{O}$. We can see that the quotient of $\mathcal{O}$ by $2\mathcal{O}$ is isomorphic to $\dfrac{\mathbb{Z}[x,y]}{\langle 2, f(x), g(y)\rangle}$, which is isomorphic to $\dfrac{\mathbb{Z}_2[x,y]}{\langle f'(x), g'(y))\rangle}$, where $f'(x) \equiv f(x) \pmod 2$ and $g'(y) \equiv g(y) \pmod 2$. Let

$R = \dfrac{\mathbb{Z}_2[x,y]}{\langle f'(x), g'(y)\rangle}$. We now consider three cases for the prime 2 in the ring of integers $\mathbb{Z}[w_l]$ for the quadratic field $\mathbb{Q}(\sqrt{-l})$.

**1.** If 2 is inert in $\mathbb{Z}[w_l]$ then $\dfrac{\mathbb{Z}_2[x]}{\langle f'(x)\rangle} \simeq GR(2,2) \simeq \mathbb{F}_4$.

**2.** If 2 is ramified in $\mathbb{Z}[w_l]$ then $\dfrac{\mathbb{Z}_2[x]}{\langle f'(x)\rangle} \simeq \mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$ and

**3.** If 2 is split in $\mathbb{Z}[w_l]$ then $\dfrac{\mathbb{Z}_2[x]}{\langle f'(x)\rangle} \simeq \mathbb{F}_2 \times \mathbb{F}_2$.

In this paper we consider the prime 2 being inert in $\mathbb{Z}[w_l]$. Let $f(x)$ be a 2 degree irreducible polynomial, since 2 is inert in $\mathbb{Z}[w_l]$ we have $\dfrac{\mathbb{Z}_2[x]}{\langle f(x)\rangle} \simeq \mathbb{F}_4$. Therefore we have the following three cases:

**1.** If $g(y)$ is irreducible (mod 2) then $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle g'(y)\rangle} \simeq \mathbb{F}_{16}$.

**2.** If $g(y) \equiv (y-c)^2 \pmod 2$ then $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle g'(y)\rangle} \simeq \mathbb{F}_4 + u\mathbb{F}_4$, with $u^2 = 0$.

**3.** If $g(y) \equiv (y-c)(y-c') \pmod 2$ with $c \neq c' \pmod 2$ then $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle g'(y)\rangle} \simeq \mathbb{F}_4 \times \mathbb{F}_4$.

Now we discuss the three cases separately in more details by considering different conditions for the polynomial $g(y)$.

**Case** 1**:** As the polynomial $g(y)$ to be an irreducible polynomial, it can be seen easily that $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle g'(y)\rangle} \simeq \mathbb{F}_{16}$.

**Case** 2**:** If $g(y) \equiv (y-c)^2 \pmod 2$, with a primary polynomial $g(y)$ over $\mathbb{Z}_2$ of the form $g(y) = (y-c')^2 + 2(a_0 + a_1 y) \pmod 2$ for some $a_0, a_1 \in \mathbb{F}_4$, where $c' \pmod 2 = c$. Now we put $h = y - c'$, we define $s(h) := g(h + c') \pmod 2$ so that $s(h) = h^2 + 2a_1 h + 2(a_0 + a_1 c') = h^2 + 2(a_1 h + a_2)$ for some $a_2 \in \mathbb{F}_4$, we thus have $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle g(y)\rangle} \simeq \mathbb{F}_4[y]/\langle s(h)\rangle \simeq \mathbb{F}_4 + u\mathbb{F}_4$, where $u$ satisfies $s(u) = 0$.

**Case** 3**:** Suppose that $g(y) = (y-c)(y-c') \pmod 2$ with $c \neq c' \pmod 2$, which can be possible only if we take $g(y) = h_1(y)h_2(y)$ in $\mathbb{F}_4[y]$ where $h_1(y)$ and $h_2(y)$ are pairwise coprime monic polynomials over $\mathbb{F}_4$. We thus have $\mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{\langle h_1(y), h_2(y)\rangle} \simeq \dfrac{\mathbb{F}_4[y]}{h_1(y)} \times \dfrac{\mathbb{F}_4[y]}{h_2(y)} \simeq \mathbb{F}_4 \times \mathbb{F}_4$.

The ring $\mathcal{O}/2\mathcal{O}$ in the above **Case** 2 is not isomorphic to $\mathbb{F}_4 \times \mathbb{F}_4$ as it is not a Galois ring.

**Note 1.** If $R$ is a Galois ring , i.e., $R = GR(2,4) = \mathbb{F}_4[w]$, where $w$ is a root of $g(y) \pmod 2 = 0$ then for $y = \jmath + \ell w$ in $R$ with $\jmath, \ell \in \mathbb{Z}_2[w]$, we define $\overline{y} = \jmath + \ell w^2$ and $\overline{y}$ is the Frobenius homomorphism. Since the order of $w$ is 3, it follows that $\bar{\bar{y}} = \overline{\jmath + \ell w^2} = \jmath + \ell w^4 = \jmath + \ell w = y$. On the contrary, as $w$ is a root of $g(y) = y^2 + m \pmod 2 = 0$, another root of $g(y) = 0$ is $-w$. Then the map $\phi : \mathbb{F}_4[w] \longrightarrow \mathbb{F}_4[w]$: $\phi(\jmath + \ell w) = \jmath + (-\ell)w$ is an automorphism of $\mathbb{F}_4[w]$ that fixes $\mathbb{F}_4$ as $\phi(\jmath + \ell w) = \jmath + \ell w$ iff $\ell = 0$. We can see that $w^2 = \overline{w} = -w$ and $\overline{\jmath + \ell w} = \jmath + (-\ell)w$.

**Note 2.** If $R$ is isomorphic to $\mathbb{F}_4 + u\mathbb{F}_4$, with $u^2 + 2(a_1 u + a_2) = 0$, then for

$y = \jmath + \ell u$ in $R$, we define $\bar{y} = \jmath + \ell(-u - 2a_1)$ therefore $\bar{\bar{y}} = \overline{\jmath + \ell(-u - 2a_1)} = \jmath + \ell(u + 2a_1 - 2a_1) = \jmath + \ell u$.

**Note 3.** If $R$ is isomorphic to $\mathbb{F}_4 \times \mathbb{F}_4$, then for $y = (\jmath, \ell)$ in $R$ we define $\bar{y} = (\ell, \jmath)$, which gives us $\bar{\bar{y}} = (\jmath, \ell) = y$.

2.2. **Lattices and construction.** We now discuss how to build lattices from linear codes over the ring. As we will show, self-dual codes can be utilised to build Hermitian unimodular lattices.

The Hermitian inner product on $R^n$ is defined for a linear code $C$ over $R$, by $[v, w] = \sum_i v_i \overline{w_i}$, where $\overline{w_i}$ is the involution of $w_i$ for each $i$.

Let $C$ be a linear code with $[n, k]$ dimensions over $R$. We define the lattice $\Lambda_l(C)$ as:

$$\Lambda_l(C) := \{x \in \mathcal{O}^n \mid \rho_l(x) \in C\}$$

where $\rho_l : \mathcal{O} \longrightarrow \mathcal{O}/2\mathcal{O}$ is a canonical map and it can further be extended componentwise to $\mathcal{O}^n$. Also as $-m \equiv 3 \pmod 4$, (and $w_m$ satisfies $w_m^2 + m = 0$). $\mathcal{O}$'s principal norm form is given by $Q(x, y) = (x - yw_m)\overline{(x - yw_m)} = x^2 + my^2$, since $w_m = \sqrt{-m}$ and $\overline{w_m} = -\sqrt{-m}$.

**Lemma 2.1.** *For every $z \in \mathcal{O}^n$, $\rho_m(\bar{z}) = \overline{\rho_m(z)}$, where $\overline{\rho_m(z)}$ denotes the involution of $\rho_m(z)$.*

*Proof.* We show the relation between the involution and conjugation via the map $\rho_m$ in three different cases discussed above.

**Case I:** Suppose $R \simeq \mathbb{F}_{16}$ and $\rho_m : \mathcal{O}(= \mathbb{Z}[w_l, w_m]) \longrightarrow \mathcal{O}/2\mathcal{O}(\simeq \mathbb{F}_4[w])$, where $w$ satisfies $w^2 + m = 0 \pmod 2$. We may regard $\rho_m(\jmath + \ell w_m)$ as $\jmath + \ell w$ and this can be seen that it is a ring homomorphism from $\mathbb{Z}[w_l, w_m]$ to $\mathbb{F}_4[w]$. For $z = \jmath + \ell w_m$, $\bar{z} = \jmath + (-\ell)w_m$, and hence that $\rho_m(\bar{z}) = \jmath + (-\ell)w$. The involution of $\rho_m(z) = \jmath + \ell w$ in $R$ is $\overline{\rho_m(z)} = \overline{\jmath + \ell w} = \jmath + (-\ell)w = \rho_m(\bar{z})$.

**Case II:** Suppose $R = \mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{F}_4[y]}{< g(y) >} \simeq \mathbb{F}_4 + u\mathbb{F}_4$, then it follows from above Note 1 that $g(y) = (y - c')^2 + 2(a_0 y + a_1) \pmod 2$, for some $a_0, a_1 \in \mathbb{Z}_2[w_l]$. We also have $g(u + c') = 0 \pmod 2$. Since $0 = h(u) = g(u + c')$ as discussed in **Case 2** earlier. Therefore these relations can be combined with the fact that $g(y) = y^2 + m$, $y^2 + c'^2 - 2yc' + 2a_1 y + 2a_0 = y^2 + m$, which gives us $a_1 = c' \pmod 2$ and $(u + c')^2 + m = 0 \pmod 2$. The map $\rho_m : \mathbb{Z}[w_l, w_m] \longrightarrow \mathbb{F}_4 + u\mathbb{F}_4$ is given by $\rho_m(\jmath + \ell w_m) = \jmath + \ell(u + c')$; we can see that $\rho_m$ is a ring homomorphism.

For $z = \jmath + \ell w_m$, $\bar{z} = \jmath - \ell w_m$. Hence, $\rho_m(\bar{z}) = \rho_m(\jmath - \ell w_m) = \jmath - \ell(u + c')$. On the contrary the involution $\overline{\rho_m(z)}$ of $\rho_m(z)$ is given by $\overline{\rho_m(z)} = \jmath + \ell(\bar{u} + c') = \jmath + \ell(-u - 2a_1 + c') = \jmath + \ell(-u - c') = \jmath - \ell(u + c') = \rho_m(\bar{z})$.

**Case III:** Let $R = \mathcal{O}/2\mathcal{O} \simeq \dfrac{\mathbb{Z}_2[w_l][y]}{(y - c_1)} \times \dfrac{\mathbb{Z}_2[w_l][y]}{(y - c_2)} \simeq \mathbb{F}_4 \times \mathbb{F}_4$, where $(y - c_1)$ and $(y - c_2)$ are coprime over $\mathbb{Z}_2[w_l]$.

The map $\rho_m : \mathcal{O}(= \mathbb{Z}[w_l, w_m]) \longrightarrow \mathcal{O}/2\mathcal{O}(\simeq \mathbb{F}_4 \times \mathbb{F}_4)$ is given by $\rho_m(\jmath + \ell w_m) = (\jmath + \ell c_1, \jmath + \ell c_2)$ where $c_1$ and $c_2$ are roots of $g(y) = 0 \pmod 2$. We thus note that $c_1 + c_2 = 0 \pmod 2$ and $c_i^2 + m = 0 \pmod 2$ for $1 \le i \le 2$ and therefore $\rho_m$ is a ring homomorphism. For $z = \jmath + \ell w_m$, $\bar{z} = \jmath - \ell w_m$. Hence $\rho_m(\bar{z}) =$

$\rho_m(\jmath-\ell w_m) = (\jmath-\ell c_1, \jmath-\ell c_2)$, since $c_1 = -c_2$ this gives $\rho_m(\bar{z}) = (\jmath+\ell c_2, \jmath+\ell c_1)$. On the contrary as the involution of $(x,y)$ in $R$ is $\overline{(x,y)} = (y,x)$ we have $\overline{\rho_m(z)} = \overline{\rho_m(\jmath+\ell w_m)} = \overline{\jmath+\ell c_1, \jmath+\ell c_2} = (\jmath+\ell c_2, \jmath+\ell c_1)$. Thus $\rho_m(\bar{z}) = \overline{\rho_m(z)}$. □

**Lemma 2.2.** *Let $C$ be a code over $R$ with the Hermitian inner product. Then there is the following:*

***1.*** *The $\Lambda_m(C)$ lattice is an $\mathcal{O}$-lattice.*

***2.*** $\Lambda_m(C^\perp) = 2\Lambda_m(C)^*$.

***3.*** $\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^* = \sqrt{2}\Lambda_m(C)^*$.

***4.*** *$C$ is Hermitian self-dual iff $\frac{1}{\sqrt{2}}\Lambda_m(C)$ is unimodular.*

***5.*** *Let $m'$ equal $min\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)$ and $d$ equal $C$'s minimum Hamming weight. Then $m' \geq min\left\{2, \frac{1}{2}\cdot d\right\}$.*

*Proof.* **1.** It is clear that $\Lambda_m(C)$ is a submodule of $\mathcal{O}^n$, as $C$ is a submodule of $R^n$. Thus $\Lambda_m(C)$ is an $\mathcal{O}$-lattice.

**2.** Let $x_1 = a + 2z_1$, $x_2 = b + 2z_2$ are elements of $\Lambda_m(C)$. Then $\rho_m(x_1) = a$ and $\rho_m(x_2) = b \in C$. We have $\left\langle \frac{x_1}{2}, x_2 \right\rangle \in \mathcal{O}$ (from **1.**) if and only if $\frac{\sum_i a_i\overline{b_i}}{2} \in \mathcal{O}$ $\Leftrightarrow \sum_i a_i\overline{b_i} \in 2\mathcal{O} \Leftrightarrow \rho_m(x_1)\cdot\rho_m(\overline{x_2}) = 0$. By Lemma 2.1 $\rho_m(\bar{z}) = \overline{\rho_m(z)}$. Thus $\rho_m(x_1)\cdot\rho_m(\overline{x_2}) = 0$ is equivalent to $\rho_m(x_1).\overline{\rho_m(x_2)} = a\cdot\overline{b} = [a,b] \in C$ which is a subset of $(\mathcal{O}/2\mathcal{O})^n$. Hence $\Lambda_m(C^\perp) = 2\Lambda_m(C)^*$.

**3.** Let $x \in \left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^*$. Then $< x, y > \in \mathcal{O}$ for any $y \in \frac{1}{\sqrt{2}}\Lambda_m(C)$. Equivalently $\left\langle \frac{1}{\sqrt{2}}x, \sqrt{2}y \right\rangle \in \mathcal{O}$ for any $\sqrt{2}y \in \Lambda_m(C)$. Therefore, $\frac{1}{\sqrt{2}}x \in \Lambda_m(C)^*$, i.e., $x \in \sqrt{2}\Lambda_m(C)^*$. Conversely, suppose $x \in \sqrt{2}\Lambda_m(C)^*$. Then $\frac{1}{\sqrt{2}}x \in \Lambda_m(C)^*$. Hence $\left\langle \frac{1}{\sqrt{2}}x, y \right\rangle \in \mathcal{O}$ for any $y \in \Lambda_m(C)$. This is equivalent to $\left\langle x, \frac{1}{\sqrt{2}}y \right\rangle \in \mathcal{O}$ for any $\frac{1}{\sqrt{2}}y \in \frac{1}{\sqrt{2}}\Lambda(C)$. Therefore $x \in \left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^*$. Hence $\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^* = \sqrt{2}\Lambda_m(C)^*$.

**4.** Suppose $C$ is Hermitian self-dual, then from **1** and **3**, we have

$$\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^* = \sqrt{2}\Lambda_m(C)^* = \frac{1}{\sqrt{2}}\Lambda_m(C^\perp) = \frac{1}{\sqrt{2}}\Lambda_m(C),$$

so $\frac{1}{\sqrt{2}}\Lambda_m(C)$ is unimodular.

Conversely, suppose that $\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^* = \frac{1}{\sqrt{2}}\Lambda_m(C)$. By **1** and **3** we have

$\left(\frac{1}{\sqrt{2}}\Lambda_m(C)\right)^* = \sqrt{2}\Lambda_m(C)^* = \frac{1}{\sqrt{2}}\Lambda_m(C^\perp)$. Therefore $\frac{1}{\sqrt{2}}\Lambda_m(C^\perp) = \frac{1}{\sqrt{2}}\Lambda_m(C)$. Thus $\Lambda_m(C) = \Lambda_m(C^\perp)$. Let $x \in C$ then there exists $y \in \Lambda_m(C)$ such that $x = \rho_m(y) \in C$. Since $\Lambda_m(C) = \Lambda_m(C^\perp)$, we have $y \in \Lambda_m(C^\perp)$. Thus $\rho_m(y) \in C^\perp$, i.e., $x \in C^\perp$. This shows that $C \subseteq C^\perp$. Also similarly we can show that $C^\perp \subseteq C$. Hence $C$ is self-dual.

**5.** Note that $\Lambda_m(C)$ contains $x = (2, 0, 0, \ldots, 0)$ and minimum Hamming weight codewords. As the squared norm of $x$ is 4. Hence $m' \geq min\{2, \frac{1}{2}.d\}$. □

## 3. Self-dual codes over the ring $R$

We follow the various concepts established in [13] for the self-dual codes over the Galois ring and direct product of two rings to discuss some properties of Hermitian self-dual codes over the ring $R$. We give a theorem that describes the connection between self-dual codes over $\frac{\mathbb{Z}_2[x]}{< f(x) >}$ and $\mathbb{F}_{16}$.

**Theorem 3.1.** *If $x_1, x_2, \cdots, x_k$ generate a self-dual code over $\frac{\mathbb{Z}_2[x]}{< f(x) >}$ then $x_1, x_2, \ldots, x_k$ generate a Hermitian self-dual code over $\mathbb{F}_{16}$.*

*Proof.* We take the inner product of two vectors in $\mathbb{F}_{16}$-span for the vector $x_1, x_2, \cdots, x_k$.

$$[x_1v_1 + x_2v_2 + \cdots + x_kv_k, x_1u_1 + x_2u_2 + \ldots + x_ku_k] = \sum_{i,j} v_i\bar{u_j}[x_i, x_j]$$

$$= \sum_{i,j} v_i\bar{u_j}\left(\sum_{k=1}^{n}(x_i)_k\overline{(x_j)_k}\right)$$

$$= \sum_{i,j} v_i\bar{u_j}(\sum_{k=1}^{n}(x_i)_k(x_j)_k)$$

$$= \sum_{i,j} v_i\bar{u_j}(0) = 0.$$

As a result, the code over $\mathbb{F}_{16}$ is a Hermitian self-orthogonal code.
Since $\mathbb{F}_{16}$ is a 2 degree extension of $\frac{\mathbb{Z}_2[x]}{< f(x) >}$ and if there is an independent linear combination made up over $\frac{\mathbb{Z}_2[x]}{< f(x) >}$ with $\omega$ possible coefficients then there will be $\omega^2$ possible coefficients over $\mathbb{F}_{16}$. As a result, it will have the cardinality of a self-dual code, and because it is self-orthogonal, it will be Hermitian self-dual. □

It should be noted that self-dual codes are only available for even lengths over $\frac{\mathbb{Z}_2[x]}{< f(x) >}$. There are Hermitian self-dual codes that are free of even lengths over $\mathbb{F}_{16}$. The ring $\mathbb{F}_4 \times \mathbb{F}_4$ is a principal ideal ring. The units of the ring $\mathbb{F}_4 \times \mathbb{F}_4$ are of the form $(s, t)$ where $s, t$ are units in $\mathbb{F}_4$.

**Theorem 3.2.** *Hermitian self-dual codes over $\mathbb{F}_4 \times \mathbb{F}_4$ exist for all lengths n.*

*Proof.* We take the code $< (s,0) >$ of length 1, where $s \in \mathbb{F}_4$ is a unit element. The code is self-orthogonal, as we can see $[(s,0),(s,0)] = (s,0)\overline{(s,0)} = (s,0)(0,s) = (0,0)$. As a result, the code is Hermitian self-dual with 4 elements. The direct product is then used to generate self-dual codes of any length. □

**Theorem 3.3.** *Let E be a length n code over $\mathbb{Z}_2[w_l]$. Then*

$$\mathcal{F} = \{(a'_1,b'_1),(a'_2,b'_2),\cdots,(a'_n,b'_n) \mid (a'_1,a'_2,\ldots,a'_n) \in E, (b'_1,b'_2,\ldots,b'_n) \in E^{\perp}\}$$

*is a length n Hermitian self-dual code.*

*Proof.* Since the cardinality of $\mathcal{F}$ is same as the number of self-dual code that is $4^n$. Therefore it is Hermitian self-dual code as the code is self-orthogonal. □

We now discuss Hermitian self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ with $u^2 = 0$. The units of the ring $\mathbb{F}_4 + u\mathbb{F}_4$ is of the form $s + tu$ where $s \in \mathbb{F}_4$ is a unit and $t$ is any arbitrary element.

**Theorem 3.4.** *For all length n, self-dual codes exist over $\mathbb{F}_4 + u\mathbb{F}_4$ if $u^2 = 0$.*

*Proof.* We take length 1 code $C =< u >$. Since $u\bar{u} = u(-u) = -u^2 = 0$, so the code $C$ is self-orthogonal. The code $C$ will have elements of the form $au$, $a \in \mathbb{F}_4$, therefore $C$ will have 4 element. Hence $C$ is self-dual. Then we get the Hermitian self-dual code of all length by taking the direct product. □

## 4. MacWilliams Identity

In each case of the ring $R$ we consider $\mathbb{F}_4 \times \mathbb{F}_4$ as the additive group of $R$. We order the elements in the order such as $(\eta,\chi) < (\gamma,\delta)$ if $\eta < \gamma$ or if $\eta = \gamma$ and $\chi < \delta$.
We define $C$'s complete weight enumerator as:

$$cwe_C(x_{0,0},x_{0,1},x_{0,2},x_{0,3},x_{1,0},x_{1,1},\ldots,x_{3,3}) = \sum_{c\in C}\prod x_{\eta,\chi}^{n_{\eta,\chi}},$$

where $n_{\eta,\chi}$ denotes the number of occurrence corresponding to $(\eta,\chi) \in c$.
We discuss MacWilliams relations for different situations in each case over the ring [17]. For each element $a$ of the ring $R$ let $\chi_a$ denotes the character corresponding to the element $a$. Then the matrix defined by $T_{a,b} = \chi_a(\bar{b})$ gives the MacWilliams relation. Also, $\chi$ is the generating character associated with the Frobenius ring element 1. Then for each ring that we consider we have $T_{a,b} = \chi(a\bar{b})$. To do this we need to define a matrix $T_i$ that correspond to each ring. Let $\zeta = e^{2\wp i/2} = e^{\wp i}$.
First we consider the ring $R = \mathbb{F}_{16}$ and use the involution $\overline{\eta + \chi w} = \eta + \chi w^2$. Then $(\eta + \chi w)\overline{(\gamma + \delta w)} = (\eta + \chi w)(\gamma + \delta w^2) = g_1 + g_2 w$, where $g_1, g_2$ are function of $\eta,\chi,\gamma,\delta$. Now define the matrix $T_1$ by:

$$(T_1)_{(\eta,\chi)(\gamma,\delta)} = \zeta^{g_1+g_2}.$$

Now we consider the ring $R = \mathbb{F}_4 \times \mathbb{F}_4$ and use involution $\overline{(\eta,\chi)} = (\chi,\eta)$. Then $(\eta,\chi)\overline{(\gamma,\delta)} = (\eta,\chi)(\delta,\gamma) = (\eta\delta,\chi\gamma)$. Hence

$$(T_2)_{(\eta,\chi)(\gamma,\delta)} = \zeta^{\eta\delta+\chi\gamma}$$

In last case we consider the ring $R = \mathbb{F}_4 + u\mathbb{F}_4$, where $u^2 = 0$ and use involution $\overline{(\eta+\chi u)} = \eta - \chi u$. Then $(\eta+\chi u)\overline{(\gamma+\delta u)} = (\eta+\chi u)(\gamma-\delta u) = \eta\gamma + (\chi\gamma - \eta\delta)u$. Hence,

$$(T_3)_{(\eta,\chi)(\gamma,\delta)} = \zeta^{\eta\gamma+(\chi\gamma-\eta\delta)}.$$

We take $\widehat{R} = \{\wp \mid \wp \text{ is a character of the additive group of } R\}$. It is worth noting that the additive group of $R$ and $\widehat{R}$ is isomorphic. To each element of $\widehat{R^n}$, the natural correspondence is associated with an element of $R^n$. Since $(\widehat{R})^n = \widehat{R^n}$, the code $C^\perp$ is related to the set $\{\zeta \in \widehat{R^n} \mid \zeta(c) = 1, \forall c \in C\}$. $X^t$ represents the $X$ transpose. We recall some results from [ [**?**], Chapter 3]. Let $h_i(c_i) = x_{c_i}$ and $h(x) = \prod_{i=1}^{n} h_i(x_i)$. The Poisson summation formula is thus given for a subgroup $\mathcal{H}$ of $G$,

$$\sum_{x\in\mathcal{H}} h(x) = \frac{1}{|(\widehat{G}:\mathcal{H})|} \sum_{\wp\in(\widehat{G}:\mathcal{H})} \widehat{h}(\wp),$$

and $\widehat{h}(\wp) = \sum_{x\in G} \wp(x)h(x)$. Here, we take $G = R_{u^3}$, $\widehat{G} = \widehat{R}$, $\mathcal{H} = C^\perp$ and $|\widehat{R^n} : C^\perp| = |C|$. Therefore,

$$\begin{aligned}\sum_{x\in C^\perp} h(x) &= \sum_{(c_1,\ldots,c_{16})\in C^\perp} x_{c_1}\cdots x_{c_{16}} \\ &= \sum_{(c_1,\ldots,c_{16})\in C^\perp} x_{0,0}^{n_{0,0}(c)}\cdots x_{3,3}^{n_{3,3}(c)} \\ &= cwe_{C^\perp}(x_{0,0}, x_{0,1}, \ldots, x_{3,3}).\end{aligned}$$

**Theorem 4.1.** *Set $X = (x_{0,0}, x_{0,1}, x_{0,2}, x_{0,3}, x_{1,0}, x_{1,1}, \ldots, x_{3,3})$. Let $C$ be a linear code over the ring $R$ in above three cases then*

$$cwe_C(X) = \frac{1}{|C|} cwe_C(T_i \cdot X).$$

*Proof.* From the discussion above

$$\sum_{x\in C^\perp} h(x) = \frac{1}{|(\widehat{R}:C^\perp)|} \sum_{\wp\in(\widehat{R}:C^\perp)} \widehat{h}(\wp)$$

$$cwe_{C^\perp}(x_{0,0}, x_{0,1}, \ldots, x_{3,3}) = \frac{1}{|C|} \sum_{\wp\in(\widehat{R}:C^\perp)} \left( \sum_{x\in R} \wp(x)h(x) \right),$$

where $x = (c_1, c_2, \ldots c_{16})$, $\wp = (\wp_1, \wp_2, \ldots, \wp_{16})$ and $\wp_i = \zeta_{a_j}$ for some $i$ and $j$. Therefore, $\wp(x) = \zeta_{a_1}(c_1)\ldots\zeta_{a_{16}}(c_{16})$, where $\zeta_{a_i}$ represents the matrix $T_{a,b}$

defined above. Thus,

$$cwe_{C^\perp}(X) = \sum_{(c_1,\ldots,c_{16})\in R} \Big(\prod \zeta_{a_i}(c_j)\Big) x_{0,0}\cdots x_{3,3}$$
$$= cwe_C(T_i \cdot X).$$

□

## 5. Conclusion

In this paper we have considered the biquadratic field $\mathbb{Q}(\sqrt{-l}, \sqrt{-m})$ with $-l \equiv 1 \pmod 4$ and $-m \equiv 3 \pmod 4$. We have discussed the different algebraic properties over the biquadratic field and also discussed the construction of ring structure. We gave the construction of lattices to discuss the properties of lattices and self-dual codes over the ring $R$ and MacWilliams identity has been given. Work can be done in the future to develop a link between Jacobi forms and the complete weight enumerator of a code over the ring.

## Acknowledgments:

The first and second author is supported by National Board of Higher Mathematics (Department of Atomic Energy), India with grant number 02011/15/2025/NBHM/R&D-II/1188.

## Declarations

- **Funding:** NBHM(DAE), India.
- **Conflicts of Interest:** The author declare that there is no conflict of interest regarding the publication of this manuscript.

## References

[1] Ankur, Pratyush Kumar, and Ankur Shukla. BConstruction of lattices over the real sub-field of $\mathbb{Q}(\zeta_8)$ for block fading (wiretap) coding. *Discrete Mathematics, Algorithms and Applications*, (2024) 1–16.

[2] Ankur, P.K. Kewat. Binary Self-dual codes and Jacobi forms over a totally real subfield of $\mathbb{Q}(\zeta_8)$. *Applicable Algebra in Engineering, Communications and Computing*, (2023) 377–392.

[3] Ankur, P.K. Kewat. Self-dual codes over $\mathbb{F}_2[u]/\langle u^4\rangle$ and Jacobi forms over a totally real subfield of $\mathbb{Q}(\zeta_8)$. *Designs, Codes and Cryptography*, (2021) 1091–1109.

[4] Ankur & P.K. Kewat. Type I and Type II codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Asian-European Journal of Mathematics*, **12(2)** (2019) 1950025.

[5] Ankur. Self-dual codes over the ring GR $(p^m, g)$ and Jacobi forms. *Asian-European Journal of Mathematics* **10** (2017) 1750055.

[6] C. Bachoc. Applications of coding theory to the construction of modular lattices. *Journal of Combinatorial Theory, Series A*, **78(1)** (1997) 92–119.

[7] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura. Type II codes, even unimodular lattices, and invariant rings. *IEEE Transactions on Information Theory*, **45(4)** (1999) 1194–1205.

[8] K. Betsumiya and Y. Choie. Jacobi forms over totally real fields and Type II codes over Galois rings GR($2^m, f$). *European Journal of Combinatorics*, **25(4)** (2004) 475–486.

[9] Y. Choie, E. Jeong. Jacobi forms over totally real fields and codes over $\mathbb{F}_p$. *Illinois Journal of Mathematics*, **46(2)** (2002) 627–643.

[10] Y. Choie and H. Kim. Codes over $\mathbb{Z}_{2m}$ and Jacobi forms of genus $n$. *Journal of Combinatorial Theory, Series A*, **95(2)** (2001) 335–348.

[11] Y. Choie and N. Kim. The complete weight enumerator of Type II code over $\mathbb{Z}_{2m}$ and Jacobi forms. *IEEE Transactions on Information Theory*, **47(1)** (2001) 5397.

[12] K.Chua. Codes over $GF(4)$ and $\mathbb{F}_2 \times \mathbb{F}_2$ and hermitian lattices over imaginary quadratic fields. *Proceedings of the American Mathematical Society*, **133(3)** (2005) 661–670.

[13] S. Dougherty, J. L. Kim and Y. Lee. Codes over rings and Hermitian lattices. *Des. Codes Cryptogr.*, **76** 2015 519–535

[14] M. Eichler and D. Zagier. The theory of Jacobi forms, *Springer*, **55** (1985).

[15] V. A. Gritsenko. The action of modular operators on the Fourier-Jacobi coefficients of modular forms. *Sbornik Mathematics*, **47(1)** (1984) 237–267.

[16] K. K. Haverkamp. Hermitian jacobi forms. *Results in Mathematics*, **29(1-2)** (1996) 78–89.

[17] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes. *Elsevier*, (1977).

[18] J.P.Serre. A course in Mathematics. *Springer Science & Business Media*, **7** 2012.

[19] H. Skogman. Jacobi forms over totally real number fields. *Results in Mathematics*, **39(1-2)** (2001) 169–182.

[20] T. Shashka and C. Shor. Codes over $\mathbb{F}_{p^2}$ and $\mathbb{F}_p \times \mathbb{F}_p$, lattices and theta functions. *Adv. Coding Theory Cryptogr.*, **3** (2007) 70–80.

[21] T. Shashka, C. Shor and S. Wijesiri. Codes over rings of size $p^2$ and lattices over imaginary quadratic fields *Finite Fields Appl.* **16(2)** (2010) 75–87.

[22] J.A. Wood. Duality for modules over finite rings and applications to coding theory *Am. J Math.* **121(3)** (1999) 555–575.

Department of Mathematics (SoT), Pandit Deendayal Energy University, Gandhinagar 382426, India
*Email address*: ankur786ankur@gmail.com

Department of Mathematics, Ganesh Dutt College, Begusarai Lalit Narayan Mithila University, Darbhanga, Bihar, India
*Email address*: vikey397@gmail.com

Department of Mathematics (SoT), Pandit Deendayal Energy University, Gandhinagar 382426, India
*Email address*: punitjain51@gmail.com