Some remarks for codes and lattices over imaginary quadratic fields

Tony Shaska
Oakland University, Rochester, MI, USA.

Caleb Shor
Western New England University, Springfield, MA, USA.

shaska@oakland.edu

Abstract

Let $\ell > 0$ be a square-free integer, $\ell \equiv 3 \mod 4$, $K = Q(\sqrt{-\ell})$, and $\mathcal{O}_K$ the ring of integers of K. Codes C over rings $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$ determine lattices $\Lambda_\ell(C)$ over K. The theta series $\theta_{\Lambda_\ell(C)}$ of such lattice can be written in terms of the complete weight enumerator of C. For any $\ell' > \ell$ the first $\frac{\ell+1}{4}$ terms of their corresponding theta functions are the same with those of $\Lambda_\ell(C)$. In [6] it was conjectured that for $\ell > \frac{p(n+1)(n+2)}{2}$ there is a unique complete weight enumerator corresponding to a given theta function. In this paper, we explore this conjecture and some new computational results.

Keywords
Codes, theta functions, complete weight enumerators

1 Introduction

Let $\ell > 0$ be a square-free integer congruent to 3 modulo 4, $K = \mathbb{Q}(\sqrt{-\ell})$ be the imaginary quadratic field, and $\mathcal{O}_K$ its ring of integers. Codes, Hermitian lattices, and their theta-functions over rings $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$, for small primes p, have been studied by many authors, see [1], [4], [5], among others. In [1], explicit descriptions of theta functions and MacWilliams identities are given for $p = 2, 3$. In [7] we explored codes C defined over $\mathcal{R}$ for $p > 2$. For any ℓ one can construct a lattice $\Lambda_\ell(C)$ via Construction A and define theta functions based on the structure of the ring $\mathcal{R}$. Such constructions suggested some relations between the complete weight enumerator of the code and the theta function of the corresponding lattice. In this paper we further study the weight enumerators of such codes in terms of the theta functions of the corresponding lattices.

For any prime p with $p \nmid \ell$, let $R := \mathcal{O}_K/p\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{F}_p, \omega^2 + \omega + d = 0\}$, where $d = (\ell + 1)/4$. We have the map

$$\rho_{\ell,p} : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_k =: \mathcal{R}$$

A linear code C of length n over $\mathcal{R}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. The dual is defined as $C^\perp = \{u \in \mathcal{R}^n : u \cdot \bar{v} = 0 \text{ for all } v \in C\}$. If $C = C^\perp$ then C is self-dual. We define

$$\Lambda_\ell(C) := \{u = (u_1, \ldots, u_n) \in \mathcal{O}_K^n : (\rho_{\ell,p}(u_1), \ldots, \rho_{\ell,p}(u_n)) \in C\},$$

In other words, $\Lambda_\ell(C)$ consists of all vectors in $\mathcal{O}_K^n$ in the inverse image of C, taken componentwise by $\rho_{\ell,p}$. This method of lattice construction is known as Construction A.

Let $\tau \in \mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$, the upper-half plane. And let $q = e^{\pi i \tau}$. For any lattice Λ in K^n, we have an associated theta function $\theta_\Lambda(q)$, given by

$$\theta_\Lambda(q) = \sum_{z \in \Lambda} q^{z \cdot \bar{z}},$$

where "$\cdot$" denotes the usual dot product and $\bar{z}$ denotes component-wise conjugation. Thus, for any linear code C, we have an associated lattice $\Lambda_\ell(C)$ and associated theta function $\theta_{\Lambda_\ell(C)}(q)$.

For notation, let $r_{a+pb+1} = a - b\omega$, so $\mathcal{R} = \{r_1, \ldots, r_{p^2}\}$. For a codeword $u = (u_1, \ldots, u_n) \in \mathcal{R}^n$ and $r_i \in \mathcal{R}$, we define the counting function $n_i(u) := \#\{j : u_j = r_i\}$. The complete weight enumerator of the $\mathcal{R}$ code C is the polynomial

$$cwe_C(z_1, z_2, \ldots, z_{p^2}) = \sum_{u \in C} z_1^{n_1(u)} z_2^{n_2(u)} \ldots z_{p^2}^{n_{p^2}(u)}. \tag{1}$$

We can use the complete weight enumerator polynomial to find the theta function of the lattice $\Lambda_\ell(C)$. For a proof of the following result see [7].

Lemma 1. *Let C be a code defined over $\mathcal{R}$ and cwe_C its complete weight enumerator as above. For integers a and b and a prime p, let $\Lambda_{a,b}$ denote the lattice $a - b\omega_\ell + p\mathcal{O}_K$. Then,*

$$\theta_{\Lambda_\ell(\mathcal{C})}(q) = cwe_{\mathcal{C}}(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \ldots, \theta_{\Lambda_{p-1,p-1}}(q)).$$

Note that the q^2 arguments of this polynomial can be computed in terms of certain one-dimensional theta series which are defined in Section 2.1 of [7].

In [2], for $p = 2$, the symmetric weight enumerator polynomial $swe_{\mathcal{C}}$ of a code $\mathcal{C}$ over a ring or field of cardinality 4 is defined to be

$$swe_{\mathcal{C}}(X, Y, Z) = cwe_{\mathcal{C}}(X, Y, Z, Z).$$

For $\Lambda_{\Lambda_\ell(\mathcal{C})}(q)$, the lattice obtained from $\mathcal{C}$ by Construction A, by Theorem 5.2 of [2], one can then write

$$\theta_{\Lambda_\ell(\mathcal{C})}(q) = swe_{\mathcal{C}}(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{0,1}}(q)).$$

These theta functions are referred to as $A_d(q), C_d(q)$, and $G_d(q)$ in [2] and [8].

Remark 1. *The connection between complete weight enumerators of self-dual codes over $\mathbb{F}_p$ and Siegel theta series of unimodular lattices is well known. Construction A associates to any length n code $C = C^\perp$ an n-dimensional unimodular lattice; see [3] for details.*

For $p > 2$, however, there are $\frac{(p+1)^2}{4}$ theta functions associated to the various lattices, so our analog of the symmetric weight enumerator polynomial needs more than 3 variables.

Problem 1. *Determine an explicit relation between theta functions and the symmetric weight enumerator polynomial of a code defined over $\mathcal{R}$ for $p > 3$.*

We expect that the answer to the above problem is that the theta function is given as the symmetric weight enumerator swe_C of C, evaluated on the theta functions defined on cosets of $\mathcal{O}_K/p\mathcal{O}_K$.

2 Theta functions and the corresponding complete weight enumerator polynomials

For a fixed prime p, let C be a linear code over $\mathcal{R} = \mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$ of length n and dimension k. An admissible level ℓ is an integer ℓ such that $\mathcal{O}_K/p\mathcal{O}_K$ is isomorphic to $\mathcal{R}$. For an admissible ℓ, let $\Lambda_\ell(C)$ be the corresponding lattice as in the previous section. Then, the **level ℓ theta function** $\theta_{\Lambda_\ell(C)}(q)$ of the lattice $\Lambda_\ell(C)$ is determined by the complete weight enumerator cwe_C of C, evaluated on the theta functions defined on cosets of $\mathcal{O}_K/p\mathcal{O}_K$. We consider the following questions. How do the theta functions $\theta_{\Lambda_\ell(C)}(q)$ of the same code C differ for different levels ℓ? Can non-equivalent codes give the same theta functions for all levels ℓ?

We give a satisfactory answer to the first question (cf. Theorem 1, Lemma 2) and for the second question we conjecture that:

Conjecture 1. *Let C be a code of size n defined over $\mathcal{R}$ and $\theta_{\Lambda_\ell(C)}$ be its corresponding theta function for level ℓ. Then, for large enough ℓ, there is a unique complete weight enumerator polynomial which corresponds to $\theta_{\Lambda_\ell(C)}$.*

Let C be a code defined over $\mathcal{R}$ for a fixed $p > 2$. Let the complete weight enumerator of C be the degree n polynomial $cwe_C = f(x_1, \ldots, x_r)$, for $r = p^2$. Then from Lemma 1 we have that

$$\theta_{\Lambda_\ell(\mathcal{C})}(q) = f(\theta_{\Lambda_{0,0}}(q), \ldots, \theta_{\Lambda_{p-1,p-1}}(q))$$

for a given ℓ. First we want to address how $\theta_{\Lambda_\ell(\mathcal{C})}(q)$ and $\theta_{\Lambda_{\ell'}(\mathcal{C})}(q)$ differ for different ℓ and ℓ'.

Theorem 1. *Let C be a code defined over $\mathcal{R}$. For all admissible ℓ, ℓ' with $\ell < \ell'$ the following holds*

$$\theta_{\Lambda_\ell(C)}(q) = \theta_{\Lambda_{\ell'}(C)}(q) + \mathcal{O}(q^{\frac{\ell+1}{4}}).$$

Proof. See [6] for details. □

We have the following lemma; see [6].

Lemma 2. *Let C be a fixed code of size n defined over $\mathcal{R}$ and $\theta(q) = \sum \lambda_i q^i$ be its theta function for level ℓ. Then, there exists a bound $B_{\ell,p,n}$ such that $\theta(q)$ is uniquely determined by its first $B_{\ell,p,n}$ coefficients.*

For notation, when p and n are fixed, we will let $B_\ell = B_{\ell,p,n}$. To extend the theory for $p = 2$ to $p > 2$ we have to find a relation between the theta function $\theta_{\Lambda_\ell(C)}$ and the number of complete weight enumerator polynomials corresponding to it.

Fix an odd prime p and let C be a given code of length n over $\mathcal{R}$. Choose an admissible value of ℓ such that there are $\frac{(p+1)^2}{4}$ independent theta functions. Then, the complete weight enumerator of C has degree n and $r = \frac{(p+1)^2}{4}$ variables $x_1, \ldots, x_r$. We call a **generic complete weight enumerator polynomial** a homogenous polynomial $P \in \mathbb{Q}[x_1, \ldots, x_r]$.

Denote by $P(x_1, \ldots, x_r)$ a generic r-nary, degree n, homogeneous polynomial. Assume that there is a length n code C defined over $\mathcal{R}$ such that $P(x_1, \ldots, x_r)$ is the symmetric weight enumerator polynomial. In other words,

$$swe_C(x_1, \ldots, x_r) = P(x_1, \ldots, x_r)$$

Fix the level ℓ. Then, by replacing

$$x_1 = \theta_{\Lambda_{0,0}}(q), \ \ldots\ldots\ , x_r = \theta_{\Lambda_{p-1,p-1}}(q),$$

we compute the left side of the above equation as a series $\sum_{i=0}^{\infty} \lambda_i q^i$. By equating both sides of $\sum_{i=0}^{\infty} \lambda_i q^i = P(x_1, \ldots, x_r)$, we can get a linear system of equations. Since the first $\lambda_0, \ldots, \lambda_{B_\ell - 1}$ determine all the coefficients of the theta series then we have to pick B_ℓ equations (these equations are not necessarily independent).

Consider the coefficients of the polynomial $P(x_1, \ldots, x_r)$ as parameters $c_1, \ldots c_s$. Then, the linear map

$$L_\ell : \mathbb{C}^s \to \mathbb{C}^{B_\ell - 1}$$
$$(c_1, \ldots c_s) \mapsto (\lambda_0, \ldots, \lambda_{B_\ell - 1})$$

has an associated matrix M_ℓ. For a fixed value of $(\lambda_0, \ldots, \lambda_{B_\ell - 1})$, determining the rank of the matrix M_ℓ would determine the number of polynomials giving the same theta series. There is a unique complete weight enumerator corresponding to a given theta function when

$$\text{null } (M_\ell) = s - \text{rank } (M_\ell) = 0$$

Conjecture 2. *For $\ell \geq \frac{p(n+1)(n+2)}{n} - 1$ we have* null $M_\ell = 0$*, or in other words*

$$\text{rank } (M_\ell) = \frac{\left(n - 1 + \frac{(p+1)^2}{4}\right)!}{n! \cdot \left(\frac{(p+1)^2}{4} - 1\right)!}$$

The choice of ℓ is taken from experimental results for primes $p = 2$ and 3. More details are given in the next section.

It is obvious that Conjecture 2 implies Conjecture 1. If Conjecture 1 is true then for large enough ℓ there would be a one to one correspondence between the complete weight enumerator polynomials and the corresponding theta functions. Perhaps, more interesting is to find ℓ and p for which there is not a one to one such correspondence. Consider the map

$$\Phi(\ell, p) = (\lambda_0(\ell, p), \ldots, \lambda_{B_\ell - 1}(\ell, p)),$$

where $\lambda_0, \ldots, \lambda_{B_\ell - 1}$ are now functions in ℓ and p. Let V be the variety given by the Jacobian of the map Φ. Finding integer points ℓ, p on this variety such that ℓ and p satisfy our assumptions would give us values for ℓ, p when the above correspondence is not one to one. However, it seems quite hard to get explicit description of the map Φ. Next, we will try to shed some light over the above conjectures for fixed small primes p.

3 Bounds for small primes

In [8] we determine explicit bounds for the above theorems for prime $p = 2$. In this section we give some computation evidence for the generalization of the result for $p = 3$. We recall the theorem for $p = 2$.

Theorem 2 ([8], Thm. 2)**.** *Let $p = 2$ and C be a code of size n defined over $\mathcal{R}$ and $\theta_{\Lambda_\ell}(C)$ be its corresponding theta function for level ℓ. Then the following hold:*

i) *For $\ell < \frac{2(n+1)(n+2)}{n} - 1$ there is a δ-dimensional family of symmetrized weight enumerator polynomials corresponding to $\theta_{\Lambda_\ell}(C)$, where $\delta \geq \frac{(n+1)(n+2)}{2} - \frac{n(\ell+1)}{4} - 1$.*

ii) *For $\ell \geq \frac{2(n+1)(n+2)}{n} - 1$ and $n < \frac{\ell+1}{4}$ there is a unique symmetrized weight enumerator polynomial which corresponds to $\theta_{\Lambda_\ell}(C)$.*

These results were obtained by using the explicit expression of theta in terms of the symmetric weight enumerator valuated on the theta functions of the cosets.

Next we want to find explicit bounds for $p = 3$ as in the case of $p = 2$. In the case of $p = 3$ it is enough to consider four theta functions, $\theta_{\Lambda_{0,0}}(q)$, $\theta_{\Lambda_{1,0}}(q)$, $\theta_{\Lambda_{0,1}}(q)$, and $\theta_{\Lambda_{1,1}}(q)$ since $\theta_{\Lambda_{2,0}}(q) = \theta_{\Lambda_{1,0}}(q)$, $\theta_{\Lambda_{2,2}}(q) = \theta_{\Lambda_{1,1}}(q)$ and $\theta_{\Lambda_{0,2}}(q) = \theta_{\Lambda_{1,2}}(q) = \theta_{\Lambda_{2,1}}(q) = \theta_{\Lambda_{0,1}}(q)$. If we are given a code C and its weight enumerator polynomial then we can find the theta function of the lattice constructed from C using Construction A. Let $\theta(q) = \sum_{i=0}^{\infty} \lambda_i q^i$ be the theta series for level ℓ and

$$p(x, y, z, w) = \sum_{i+j+k+m=n} c_{i,j,k} x^i y^j z^k w^m$$

be a degree n generic 4-nary homogeneous polynomial. We would like to find out how many polynomials $p(x, y, z, w)$ correspond to $\theta(q)$ for a fixed ℓ. For a given ℓ find $\theta_{\Lambda_{0,0}}(q)$, $\theta_{\Lambda_{1,0}}(q)$, $\theta_{\Lambda_{0,1}}(q)$ and $\theta_{\Lambda_{1,1}}(q)$ and substitute them in the $p(x, y, z, w)$. Hence, $p(x, y, z, w)$ is now written as a series in q. We get infinitely many equations by equating the corresponding coefficients of the two sides of the equation

$$p(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{0,1}}(q), \theta_{\Lambda_{1,1}}(q)) = \sum_{i=0}^{\infty} \lambda_i q^i.$$

Since the first $\lambda_0, \ldots, \lambda_{B_\ell - 1}$ determine all the coefficients of the theta series then it is enough to pick the first B_ℓ equations. The linear map

$$L_\ell : (c_1, \ldots c_{20}) \mapsto (\lambda_0, \ldots, \lambda_{B_\ell - 1})$$

has an associated matrix M_ℓ. If the nullity of M_ℓ is zero then we have a unique polynomial that corresponds to the given theta series. We have calculated the nullity of the matrix and B_ℓ for small n and ℓ.

Example 1 (The case $p = 3, n = 3$)**.** *The generic homogenous polynomial is given by*

$$\begin{aligned} P(x, y, z) = {} & c_1 x^3 + c_2 x^2 y + c_3 x^2 z + c_4 x^2 w + c_5 x y^2 + c_6 x z^2 + c_7 x w^2 + c_8 x y z \\ & + c_9 x y w + c_{10} x z w + c_{11} y^3 + c_{12} y^2 z + c_{13} y^2 w + c_{14} y z^2 + c_{15} y w^2 \\ & + c_{16} y z w + c_{17} z^3 + c_{18} z^2 w + c_{19} z w^2 + c_{20} w^3. \end{aligned} \tag{2}$$

The system of equations can be written by the form of

$$A\vec{c} = \vec{\lambda}$$

where $\vec{c} = \begin{pmatrix} c_1 & c_2 & \cdots & c_{20} \end{pmatrix}^t$, $\vec{\lambda} = \begin{pmatrix} \lambda_0 & \lambda_1 & \cdots & \lambda_{15} \end{pmatrix}^t$. In the case of $\ell = 7$ the matrix M_7 has null $(M_7) = 4$. We have a positive dimension family of solution set. The case of $\ell = 11$ the matrix M_{11} has null $(M_{11}) = 1$. For any case where $\ell \geq 19$ the nullity of the matrix is 0. Hence, for every given theta series, there is a unique symmetric weight enumerator polynomial. .

We summarize the results in the following table:

ℓ	$n=3$		$n=4$		$n=5$	
	B_ℓ	*null* M_ℓ	B_ℓ	*null* M_ℓ	B_ℓ	*null* M_ℓ
7	16	4	26	9	33	24
11	19	1	30	5	42	14
19	22	0	38	0	60	0
23	25	0	37	0	58	0
31	31	0	41	0	60	0
35	34	0	48	0	61	0
43	40	0	55	0	69	0
47	43	0	60	0	74	0
55	49	0	70	0	86	0
59	52	0	75	0	92	0

Recall that $\ell \equiv 3 \mod 4$ and $p \nmid \ell$. It seems from the table that the same bound of $B_\ell = \frac{2(n+1)(n+2)}{n}$ as for $p = 2$ holds also for $p = 3, n = 3$.

We have the following conjecture for general p, n and ℓ.

Conjecture 3. *For a given theta function $\theta_{\Lambda_\ell(C)}$ of a code C for level ℓ there is a unique complete weight enumerator polynomial corresponding to $\theta_{\Lambda_\ell(C)}$ if $\ell \geq \frac{p(n+1)(n+2)}{n}$.*

It is interesting to consider such question for such lattices independently of the connection to coding theory. What is the meaning of the bound B_ℓ for the ring $\mathcal{O}_K/p\mathcal{O}_K$? Do the theta functions defined here correspond to any modular forms? Is there any difference between the cases when the ring is $\mathbb{F}_p \times \mathbb{F}_p$ or $\mathbb{F}_{p^2}$?

References

[1] C. Bachoc, Applications of coding theory to the construction of modular lattices. J. Combin. Theory Ser. A 78 (1997), no. 1, 92–119.

[2] K. S. Chua, Codes over GF(4) and $\mathbf{F}_2 \times \mathbf{F}_2$ and Hermitian lattices over imaginary quadratic fields. Proc. Amer. Math. Soc. 133 (2005), no. 3, 661–670 (electronic).

[3] J. Leech and N. J. A. Sloane, Sphere packing and error-correcting codes, Canadian J. Math., **23**, (1971), 718-745.

[4] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. II. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–ix and 370–762.

[5] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. I. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–xv and 1–369.

[6] T. Shaska, C. Shor, C. S. Wijesiri, Codes over rings of size p^2 and lattices over imaginary quadratic fields. Finite Fields Appl. 16 (2010), no. 2, 7587.

[7] T. Shaska and C. Shor, Codes over F_{p^2} and $F_p \times F_p$, lattices, and corresponding theta functions. *Advances in Coding Theory and Cryptology*, vol 3. (2007), pg. 70-80.

[8] T. Shaska and S. Wijesiri, Codes over rings of size four, Hermitian lattices, and corresponding theta functions, *Proc. Amer. Math. Soc.*, 136 (2008), 849-960.

[9] T. Shaska and C. Shor, Theta functions and complete weight enumerators for codes over imaginary quadratic fields, (work in progress).