Codes over F_{p^2} and $F_p \times F_p$, lattices, and theta functions

T. Shaska

367 Science and Engineering Building,
Department of Mathematics and Statistics,
Oakland University,
Rochester, MI, 48309.

C. Shor

Department of Mathematics,
Bates College,
3 Andrews Road,
Lewiston, ME 04240

Let $\ell > 0$ be a square free integer and $\mathcal{O}_K$ the ring of integers of the imaginary quadratic field $K = Q(\sqrt{-\ell})$. Codes C over K determine lattices $\Lambda_\ell(C)$ over rings $\mathcal{O}_K/p\mathcal{O}_K$. The theta functions $\theta_{\Lambda_\ell}(C)$ of such lattices are known to determine the symmetrized weight enumerator $swe(C)$ for small primes $p = 2, 3$; see [1], [10].

In this paper we explore such constructions for any p. If $p \nmid \ell$ then the ring $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$ is isomorphic to $\mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$. Given a code C over $\mathcal{R}$ we define new theta functions on the corresponding lattices. We prove that the theta series $\theta_{\Lambda_\ell}(C)$ can be written in terms of the complete weight enumerator of C and that $\theta_{\Lambda_\ell}(C)$ is the same for almost all ℓ. Furthermore, for large enough ℓ, there is a unique complete weight enumerator polynomial which corresponds to $\theta_{\Lambda_\ell}(C)$.

Keywords: codes, lattices, theta functions

1. Introduction

Let $\ell > 0$ be a square free integer, $K = Q(\sqrt{-\ell})$ 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 [7, 8], [1] among others. In [1], an explicit description of theta functions and MacWilliams identities are given for $p = 2, 3$. For a general reference of the topic, see [6].

In this paper we aim to explore such constructions, under certain restrictions, for any p. Further, we study the weight enumerators of such codes in terms of the theta functions of the corresponding lattices. We aim to find MacWilliams-like identities in such cases and explore to what extent the theta functions of these lattices determine the codes. The last question was studied in [2] and [10] for $p = 2$.

This paper is organized as follows. In section 2 we give a brief overview of the basic definitions for codes and lattices and define theta functions over $\mathbb{F}_p$. In section 3 we define theta-functions on the lattice defined over $\mathcal{R} := \mathcal{O}_K / p\mathcal{O}_K$. For general odd p, among the p^2 lattices, there are $\frac{(p+1)^2}{4}$ associated theta series.

In section 4, we address a special case of a general problem of the construction of lattices: the injectivity of Construction A. For codes defined over an alphabet of size four (regarded as a quotient of the ring of integers of an imaginary quadratic field), the problem is solved completely in [10]. The analogous questions are asked for codes defined over $\mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$. The main obstacle seems to express the theta function in terms of the symmetric weight enumerator of the code. However, the theta function $\theta_{\Lambda_\ell}(C)$ can be expressed in terms of the complete weight enumerator of the code (cf. section 4). Using such an expression we prove the following two facts:

Theorem: Let p be a fixed prime and ℓ any square free integer such that $K = \mathbb{Q}(\sqrt{-\ell})$ and $\mathcal{R} := \mathcal{O}_K / p\mathcal{O}_K$ is isomorphic to $\mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$. For a given code C defined over $\mathcal{R}$, the theta series $\theta_{\Lambda_\ell}(C)$ is the same for almost all ℓ.

Theorem: 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 $\theta_{\Lambda_\ell}(C)$.

In contrary to results in [10] we did not attempt to find explicit bounds for ℓ. However, for a given small p it is possible such bounds can be determined using similar techniques as in [10]. This is intended to be completed in further work; see [11].

Acknowledgements: Some of the ideas of this paper originated during visits of the first author at The University of Maria Curie Sklodowska, Lublin, Poland. The first author wants to thank the faculty of the Department of Computer Science in Lublin for their hospitality. The paper was presented at the Vlora Conference on Algebra, Coding Theory, and Cryptography.

2. Preliminaries

Let $\ell > 0$ be a square free integer and $K = Q(\sqrt{-\ell})$ be the imaginary quadratic field with discriminant d_K. Recall that

$$d_K = \begin{cases} -\ell & \text{if } \ell \equiv 3 \mod 4, \\ -4\ell & \text{otherwise.} \end{cases}$$

Let $\mathcal{O}_K$ be the ring of integers of K. A lattice Λ over K is an $\mathcal{O}_K$-submodule of K^n of full rank. The Hermitian dual is defined by

$$\Lambda^* = \{x \in K^n \mid x \cdot \bar{y} \in \mathcal{O}_K, \textit{for all } y \in \Lambda\}, \tag{1}$$

where $x \cdot y := \sum_{i=1}^n x_i y_i$ and $\bar{y}$ denotes component-wise complex conjugation. In the case that Λ is a free $\mathcal{O}_K$ - module, for every $\mathcal{O}_K$ basis $\{v_1, v_2, ..., v_n\}$ we can associate a Gram matrix G(Λ) given by $G(\Lambda) = (v_i \cdot v_j)_{i,j=1}^n$ and the determinant $\det \Lambda := \det(G)$ defined up to squares of units in $\mathcal{O}_K$. If $\Lambda = \Lambda^*$ then Λ is Hermitian self-dual (or unimodular) and integral if and only if $\Lambda \subset \Lambda^*$. An integral lattice has the property $\Lambda \subset \Lambda^* \subset \frac{1}{det\Lambda}\Lambda$. An integral lattice is called even if $x \cdot x \equiv 0 \mod 2$ for all $x \in \Lambda$, and otherwise it is odd. An odd unimodular lattice is called a Type 1 lattice and even unimodular lattice is called a Type 2 lattice.

The theta series of a lattice Λ in K^n is given by

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

where $\tau \in H = \{z \in \mathbb{C} : Im(z) > 0\}$. Usually we let $q = e^{\pi i \tau}$. Then, $\theta_\Lambda(q) = \sum_{z \in \Lambda} q^{z \cdot \bar{z}}$. The one dimensional theta series (or Jacobi's theta series) and its shadow are given by

$$\theta_3(q) = \sum_{n \in \mathbb{Z}} q^{n^2}, \quad \theta_2(q) = \sum_{n \in \frac{1}{2} + \mathbb{Z}} q^{n^2}.$$

Let $\ell \equiv 3 \mod 4$ and d be a positive number such that $\ell = 4d - 1$. Then, $-\ell \equiv 1 \mod 4$. This implies that the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\omega_\ell]$, where $\omega_\ell = \frac{-1+\sqrt{-\ell}}{2}$ and $\omega_\ell^2 + \omega_\ell + d = 0$. The principal norm form of K is given by

$$Q_d(x, y) = |x - y\omega_\ell|^2 = x^2 + xy + dy^2. \tag{2}$$

The structure of $\mathcal{O}_K/p\mathcal{O}_K$ depends on the value of ℓ modulo p. For $(\frac{a}{p})$ the Legendre symbol,

$$\mathcal{O}_K/p\mathcal{O}_K = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{if } (\frac{-\ell}{p}) = 1, \\ \mathbb{F}_{p^2} & \text{if } (\frac{-\ell}{p}) = -1, \\ \mathbb{F}_p + u\mathbb{F}_p \text{ with } u^2 = 0 & \text{if } p \mid \ell. \end{cases} \tag{3}$$

We will concern ourselves with the cases where $p \nmid \ell$.

2.1. *Theta functions over* $\mathbb{F}_p$

Let $q = e^{\pi i \tau}$. For integers a and b and a prime p, let $\Lambda_{a,b}$ denote the lattice $a - b\omega_\ell + p\mathcal{O}_K$. The theta series associated to this lattice is

$$\begin{aligned} \theta_{\Lambda_{a,b}}(q) &= \sum_{m,n \in \mathbb{Z}} q^{|a+mp-(b+np)\omega_\ell|^2} \\ &= \sum_{m,n \in \mathbb{Z}} q^{Q_d(mp+a,np+b)} \\ &= \sum_{m,n \in \mathbb{Z}} q^{p^2 Q_d(m+a/p,n+b/p)}. \end{aligned} \tag{4}$$

For a prime p and an integer j, consider the theta series

$$\theta_{p,j}(q) := \sum_{n \in \frac{j}{2p}+\mathbb{Z}} q^{n^2}. \tag{5}$$

Note that $\theta_{p,j}(q) = \theta_{p,k}(q)$ if and only if $j \equiv \pm k \mod 2p$.

The theta series of $\Lambda_{a,b}$ can be written in terms of these series. In particular,

$$\theta_{\Lambda_{a,b}}(q) = \theta_{p,b}(q^{p^2\ell})\theta_{p,2a+b}(q^{p^2}) + \theta_{p,b+p}(q^{p^2\ell})\theta_{p,2a+b+p}(q^{p^2}). \tag{6}$$

The proof of this fact is similar to the proof of Lemma 2.1 in [5].

Lemma 2.1. *For any integers a, b, m, n, if the ordered pair (m, n) is component-wise congruent modulo p to one of*

$$(a, b), (-a, -b), (a + b, -b), (-a - b, b),$$

then

$$\theta_{\Lambda_{m,n}}(q) = \theta_{\Lambda_{a,b}}(q)$$

Proof. We prove this by supposing either

$$\theta_{p,n}(q) = \theta_{p,b}(q) \text{ and } \theta_{p,2m+n}(q) = \theta_{p,2a+b}(q) \tag{7}$$

or

$$\theta_{p,n}(q) = \theta_{p,b+p}(q) \text{ and } \theta_{p,2m+n}(q) = \theta_{p,2a+b+p}(q). \tag{8}$$

From Eq. 7, we have four subcases corresponding to $n \equiv \pm b \mod 2p$ and $2m + n \equiv \pm(2a + b) \mod 2p$. If $n \equiv b \mod 2p$, one finds that $m \equiv a$

mod p or $m \equiv -a-b \mod p$. If $n \equiv -b \mod 2p$, one finds that $m \equiv a+b \mod p$ or $m \equiv -a \mod p$.

From Eq. 8, we have four subcases as well, corresponding to $n \equiv \pm(b+p) \mod 2p$ and $2m+n \equiv \pm(2a+b+p) \mod 2p$. If $n \equiv b+p \mod 2p$, then either $m \equiv a \mod p$ or $m \equiv -a-b \mod p$. And if $n \equiv -b-p \mod 2p$, then either $m \equiv a+b \mod p$ or $m \equiv -a \mod p$.

Therefore, if $n \equiv b \mod p$, then $m \equiv a \mod p$ or $m \equiv -a-b \mod p$. If $n \equiv -b \mod p$, then $m \equiv a+b \mod p$ or $m \equiv -a \mod p$. □

Remark 2.1. Notice that in the case of $p=2$, there are 4 lattices $\Lambda_{a,b}$ corresponding to choices of a and b modulo 2. One finds that $\theta_{\Lambda_{0,1}}(q) = \theta_{\Lambda_{1,1}}(q)$ (which is given as Equation (3.9) in Lemma 3.1 of [2]), so there are 3 associated theta series.

Remark 2.2. In the case of $p=3$, among the 9 lattices, one finds that

$$\begin{aligned} &\theta_{\Lambda_{0,1}}(q) = \theta_{\Lambda_{2,1}}(q) = \theta_{\Lambda_{1,2}}(q) = \theta_{\Lambda_{0,2}}(q), \\ &\theta_{\Lambda_{1,1}}(q) = \theta_{\Lambda_{2,2}}(q), \text{ and} \\ &\theta_{\Lambda_{1,0}}(q) = \theta_{\Lambda_{2,0}}(q), \end{aligned}$$

giving a total of 4 associated theta series.

For general odd p, among the p^2 lattices, there are $\frac{(p+1)^2}{4}$ associated theta series.

3. Theta functions of codes over $\mathcal{R}$

Let $p \nmid \ell$ and

$$\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{F}_p, \omega^2 + \omega + d = 0\}.$$

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

$$\Lambda_\ell(C) := \{x \in \mathcal{O}_K^n : \rho_\ell(x) \in C\},$$

where $\rho_\ell : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K \to \mathcal{R}$. In other words, $\Lambda_\ell(C)$ consists of all vectors in $\mathcal{O}_K^n$ which when taken mod $p\mathcal{O}_K$ componentwise are in $\rho_\ell^{-1}(C)$. This method of lattice construction is known as Construction A.

For $0 \le a, b \le p-1$, let $r_{a+pb} = a - b\omega$, so $\mathcal{R} = \{r_0, \ldots, r_{p^2-1}\}$. For a codeword $u = (u_1, \ldots, u_n) \in \mathcal{R}^n$ and $r_i \in \mathcal{R}$, we define the counting function

$$n_i(u) := \#\{i : u_i = r_i\}.$$

The complete weight enumerator of the $\mathcal{R}$ code C is the polynomial

$$cwe_C(z_0, z_1, \ldots, z_{p^2-1}) = \sum_{u \in C} z_0^{n_0(u)} z_1^{n_1(u)} \ldots z_{p^2-1}^{n_{p^2-1}(u)}. \tag{9}$$

We can use this polynomial to find the theta function of the lattice $\Lambda_\ell(C)$.

Lemma 3.1. *Let C be a code defined over $\mathcal{R}$ and cwe_C its complete weight enumerator as above. Then,*

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

Proof. Since

$$\theta_{\Lambda_\ell(\mathcal{C})}(q) = \sum_{z \in \Lambda_\ell(\mathcal{C})} q^{z \cdot \bar{z}},$$

one has

$$\begin{aligned}
\theta_{\Lambda_\ell(\mathcal{C})}(q) &= \sum_{u \in \mathcal{C}} \theta_{\Lambda_\ell(u)}(q), \\
&= \sum_{u \in \mathcal{C}} \sum_{x \in u + p\mathcal{O}_K^n} q^{x \cdot \bar{x}}, \\
&= \sum_{u \in \mathcal{C}} \prod_{j=1}^{n} \sum_{x \in u_j + p\mathcal{O}_K} q^{x \cdot \bar{x}} \text{ (for } u = (u_1, \ldots, u_n)), \\
&= \sum_{u \in \mathcal{C}} \prod_{j=1}^{n} \theta_{u_j + p\mathcal{O}_K}(q), \\
&= \sum_{u \in \mathcal{C}} \prod_{i=0}^{p^2-1} (\theta_{\tilde{r}_i + p\mathcal{O}_K}(q))^{n_i(u)} \text{ (where } \tilde{r}_{a+pb} = a - b\omega_\ell \in \mathcal{O}_K), \\
&= cwe_{\mathcal{C}}(\theta_{\tilde{r}_0 + p\mathcal{O}_K}(q), \theta_{\tilde{r}_1 + p\mathcal{O}_K}(q), \ldots, \theta_{\tilde{r}_{p^2-1} + p\mathcal{O}_K}(q)), \\
&= cwe_{\mathcal{C}}(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \ldots, \theta_{\Lambda_{p-1,p-1}}(q)),
\end{aligned}$$

which completes the proof. □

3.1. *A MacWilliams identity*

Let $\mathcal{C}^\perp$ be the dual code to $\mathcal{C}$. One has the following MacWilliams identity (from Theorem 4.1 of [1]).

Theorem 3.1. *Let $\chi : (\mathcal{R}, +) \to (\mathbb{C}^*, \times)$ be a character of the additive group of $\mathcal{R}$ whose restriction to any nonzero left ideal of $\mathcal{R}$ is nontrivial.*

Then

$$cwe_{\mathcal{C}^\perp}(z_0,\ldots,z_{p^2-1}) = \frac{1}{p^2} cwe_{\mathcal{C}}(M(z_0,\ldots,z_{p^2-1})),$$

where M *is the matrix defined by*

$$M = (\chi(r_i\overline{r_j}))_{0\le i\le p-1, 0\le j\le p-1}.$$

To apply this theorem, we need an appropriate character. Define χ by $\chi(a+b\omega) = e^{2\pi ib/p}$. Any non-zero ideal $I \subset \mathcal{R}$ contains an element of $\mathcal{R} - \{0,1,\ldots,p-1\}$, so there is some $a+b\omega \in I$ with $b \neq 0$, meaning χ acts non-trivially on I. A calculation shows that

$$(a+b\omega)(\overline{s+t\omega}) = (as - at + btd) + (bt - as)\omega,$$

so $\chi((a+b\omega)(\overline{s+t\omega})) = e^{(bs-at)2\pi i/p}$. This is independent of d, so we obtain the same MacWilliams identity for codes over $\mathbb{F}_{p^2}$ and $\mathbb{F}_p \times \mathbb{F}_p$.

In the case of $p = 2$, for example, such identities can be made explicit; see [2] and [1] among others.

3.2. *A generalization of the symmetric weight enumerator polynomial*

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 $\Lambda_{\mathcal{C}}(q)$ 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 [10].)

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

Example 3.1. For $p = 3$, from Remark 2.2, we have four theta functions corresponding to the lattices $\Lambda_{a,b}$, namely

$$\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{1,1}}(q), \theta_{\Lambda_{0,1}}(q).$$

If we define the "symmetric weight enumerator for $p = 3$" to be

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

then one finds that

$$\theta_{\Lambda_\ell C}(q) = cwe_{\mathcal{C}}(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \dots, \theta_{\Lambda_{2,2}}(q)), \quad (10)$$

$$= swe_{\mathcal{C}}(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{1,1}}(q), \theta_{\Lambda_{0,1}}(q)). \quad (11)$$

Problem 1. *Define an symmetric weight enumerator, analogous to the $p = 2$ case, for codes defined over $\mathcal{R}$ for $p > 3$. Write a MacWilliams identity for the symmetric weight enumerator and determine an explicit relation between the symmetric weight enumerator and theta functions.*

4. The injectivity of Construction A.

For a fixed prime p, let $\mathcal{R} = \mathcal{O}_K/p\mathcal{O}_K$ and C be a linear code over $\mathcal{R}$ of length n and dimension k. An admissible level ℓ is an integer ℓ such that $\mathcal{R}$ is isomorphic to $\mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$. For an admissible ℓ, let $\Lambda_\ell(C)$ be the corresponding lattice as in the previous section. Then, the **level ℓ theta function** $\theta_{\Lambda_\ell(C)}(\tau)$ 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:

i) How do the theta functions $\theta_{\Lambda_\ell(C)}(\tau)$ of the same code C differ for different levels ℓ?

ii) Can non-equivalent codes give the same theta functions for all levels ℓ?

Next we see how this can be made explicit for the case $p = 2$.

4.1. *The characteristic $p = 2$*

For $p = 2$ case these questions are fully answered in [10]. We have the following:

Theorem 4.1 ([10], Thm. 1). *Let $p = 2$ and C be a code defined over $\mathcal{R}$. For all admissible ℓ, ℓ' such that $\ell > \ell'$, the following holds*

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

Theorem 4.2 ([10], Thm. 2). *Let $p = 2$ and C be a code of length 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. Hence, a solution to Problem 1 most likely would lead to obtaining such results for all $p > 2$ and admissible ℓ. In this paper we use the complete weight enumerator polynomial to get similar results.

4.2. *The characteristic* $p > 2$

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

$$cwe_C = f(x_0, \dots, x_r)$$

for $r = p^2 - 1$. Then from Lemma 3.1 we have that

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

for a given ℓ. First we want to address how $\theta_{\Lambda_\ell(\mathcal{C})}(\tau)$ and $\theta_{\Lambda_{\ell'}(\mathcal{C})}(\tau)$ differ for different ℓ and ℓ'. We have the following:

Theorem 4.3. *Let* C *be a code defined over* $\mathcal{R}$*. For all admissible* ℓ, ℓ' *the following holds*

$$\theta_{\Lambda_\ell}(C) - \theta_{\Lambda_{\ell'}}(C) = \sum_{i=0}^{s} a_i q^s$$

for some $a_i \in \mathbb{Z}$ *and* $s \in \mathbb{Z}^+$*.*

Corollary 4.1. *Let* p *be a fixed prime and* ℓ *any square free integer such that* $K = \mathbb{Q}(\sqrt{-\ell})$ *and* $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$ *is isomorphic to* $\mathbb{F}_{p^2}$ *or* $\mathbb{F}_p \times \mathbb{F}_p$*. For a given code* C *defined over* $\mathcal{R}$*, the theta series* $\theta_{\Lambda_\ell}(C)$ *is the same for almost all* ℓ*.*

Theorem 4.4. *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* $\theta_{\Lambda_\ell}(C)$*.*

The proofs of Theorems 4.3 and 4.4 are provided in [11] where explicit bounds for ℓ are provided for small p.

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. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups. Second edition. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1993. xliv+679 pp. ISBN: 0-387-97912-3
[4] H. H. Chan, K. S. Chua and P. Solé, Seven-modular lattices and a septic base Jacobi identity, J. Number Theory, volume 99, 2003, 2, pg. 361–372,
[5] H. H. Chan, K. S. Chua and P. Solé, Quadratic iterations to π associated with elliptic functions to the cubic and septic base, Trans. AMS 355, 2003, pg. 1505-1520.
[6] W. Ebeling, Lattices and codes, a course partially based on lectures by F. Hirzenbruch, Vieweg (Braunschweig) 1994.
[7] 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.
[8] 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.
[9] N. J. A. Sloane, Codes over GF(4) and complex lattices. Information theory (Proc. Internat. CNRS Colloq., Cachan, 1977) (French), pp. 273–283, Colloq. Internat. CNRS, 276, CNRS, Paris, 1978.
[10] T. Shaska and S. Wijesiri, Codes over rings of size four, Hermitian lattices, and corresponding theta functions, *Proc. Amer. Math. Soc.*, (2007), to appear.
[11] T. Shaska, C. Shor, and S. Wijesiri, Codes, modular lattices, and corresponding theta functions, work in progress