Journal of Algebraic Combinatorics, 21, 39–53, 2005

Higher Power Residue Codes and the Leech Lattice

MEHRDAD AHMADZADEH RAJI m.raji@ex.ac.uk
Department of Mathematical Sciences, University of Exeter, Exeter EX4 4QE, UK

Received August 30, 2001; Revised January 5, 2004; Accepted January 27, 2004

Abstract. We shall consider higher power residue codes over the ring $\mathbf{Z}_4$. We will briefly introduce these codes over $\mathbf{Z}_4$ and then we will find a new construction for the Leech lattice. A similar construction is used to construct some of the other lattices of rank 24.

Keywords: self-dual code, even unimodular lattice, Hensel lifting

1. Introduction

Let p, l be prime numbers. Let $\mathbf{F}_l$ be a finite field of order l and $\mathbf{F}_{l^2}$ be a finite extension of degree 2 over the finite field $\mathbf{F}_l$. Chapman introduced higher power residue codes W over the Galois field $\mathbf{F}_{l^2}$ [3]. These are codes over $\mathbf{F}_{l^2}$ but linear only over $\mathbf{F}_l$, not $\mathbf{F}_{l^2}$, and they satisfy $W \otimes_{\mathbf{F}_l} \mathbf{F}_{l^2} = (\mathbf{F}_{l^2})^{p+1}$. They depend on characters $\chi : \mathbf{F}_p^* \to \mathbf{F}_{l^2}^*$ where for a given field $\mathbf{F}$, $\mathbf{F}^* = \mathbf{F} - \{0\}$.

Here we begin the task of generalizing this construction to Galois rings. We confine ourselves here to the Galois ring $\mathbf{Z}_4[\omega]$ where $\omega^2 + \omega + 1 = 0$. The characters we consider here have orders 3 or 6, so we call the corresponding codes cubic or sextic residue codes.

When $p \equiv 7 \pmod{24}$ we can combine sextic residue codes over $\mathbf{Z}_4[\omega]$ with quadratic residue codes to form self-dual codes of length $3(p+1)$ over $\mathbf{Z}_4$. These yield unimodular lattices. The first case is $p = 7$ which we deal with in detail.

2. Higher power residue codes over $\mathbf{Z}_4$

Let $\mathbf{Z}_4[\omega] = \{a + b\omega : a, b \in \mathbf{Z}_4\}$ where ω is a primitive cube root of unity. So ω satisfies $\omega^2 + \omega + 1 = 0$. We define the following automorphism on $\mathbf{Z}_4[\omega]$.

$$\begin{aligned} \bar{\ } : \mathbf{Z}_4[\omega] &\longrightarrow \mathbf{Z}_4[\omega] \\ a + b\omega &\longmapsto a + b\omega^2 \end{aligned}$$

This is an automorphism of order two.

Let p be a prime number with $p \equiv 1 \pmod 6$. Now consider

$$\Omega = \{(\alpha, \beta) : \alpha, \beta \in \mathbf{Z}_p\} - \{(0, 0)\}$$

Define $\mathbf{Z}_4[\omega]^* = \mathbf{Z}_4[\omega] - \{0, 2, 2\omega, 2\omega^2\}$ the group of units of $\mathbf{Z}_4[\omega]$. Let $\chi : \mathbf{Z}_p^* \to \mathbf{Z}_4[\omega]^*$ be a character of order 3 or 6 such that $\chi(\alpha) \in \{\pm\omega^j\}$ where $j \in \{0, 1, 2\}$, $\alpha \in \mathbf{Z}_p$ and $\chi(\alpha)^{-1} = \overline{\chi(\alpha)}$. We define the $\mathbf{Z}_4[\omega]$-module M with generators e_v where $v \in \Omega$ and relations $e_{\alpha v} = \chi(\alpha)e_v$. Let

$$\Delta = \{e_\infty, e_0, e_1, \ldots, e_{p-1}\} \tag{1}$$

where $e_\infty = e_{(1,0)}$ and $e_\alpha = e_{(\alpha,1)}$ for $\alpha \in \mathbf{Z}_p$. We suppose that there is no non-trivial linear relation among the elements of Δ. So the $\mathbf{Z}_4[\omega]$-module M can be generated as a finitely generated module of rank $p + 1$ by linear combinations of the elements of Δ.

We denote the general linear group of degree 2 over $\mathbf{Z}_p$ by $\mathbf{GL}(2, p)$. Define the action of $\mathbf{GL}(2, p)$ on the projective line $\mathbf{P}^1(\mathbf{Z}_p)$ over $\mathbf{Z}_p$ as

$$v \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{v\alpha + \gamma}{v\beta + \delta}$$

and

$$\infty \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{\alpha}{\beta}.$$

Therefore if $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, we have

$$e_v A = \chi(v\beta + \delta)e_{v\cdot A}$$

for $v \neq \infty$ and

$$e_\infty A = \chi(\beta)e_{\infty\cdot A}.$$

One can easily verify that

$$e_{\alpha v} A = e_{\alpha v A} = \chi(\alpha)e_{vA} = \chi(\alpha)e_v A. \tag{2}$$

Definition 2.1 Let $f : M_1 \to M_2$ be a map between $\mathbf{Z}_4[\omega]$-modules M_1 and M_2. We say f is semi-linear if $f(\lambda m) = \bar{\lambda} f(m)$ for all $\lambda \in \mathbf{Z}_4[\omega]$, $m \in M$.

We aim to find a $\mathbf{Z}_4$-submodule W of M with the property that the natural map $W \otimes_{\mathbf{Z}_4} \mathbf{Z}_4[\omega] \to M$ is an isomorphism. This is equivalent to $M = W \oplus \omega W$.

Lemma 2.1 *Let W be a $\mathbf{Z}_4$-submodule of M with $M = W \oplus \omega W$. Then*

$$\begin{aligned} \tau : \quad M &\to M \\ r + \omega s &\mapsto r + \bar{\omega} s \end{aligned}$$

where $r, s \in W$, is a semi-linear involution.

Proof: Let $r, s \in W$ and $\lambda \in \mathbf{Z}_4[\omega]$. Thus $\lambda = a + b\omega$ for some $a, b \in \mathbf{Z}_4$. Then

$$\begin{aligned}\tau(\lambda(r+\omega s)) &= \tau(ar + br\omega + as\omega + bs(-1-\omega))\\ &= ar - bs + (br + as - bs)\bar{\omega}\\ &= \bar{\lambda}(r + \bar{\omega}s)\\ &= \bar{\lambda}(\tau(r+\omega s)).\end{aligned}$$

Hence τ is semi-linear. Finally

$$\tau^2(r+\omega s) = \tau(r + \bar{\omega}s) = r + \omega s.$$

The converse of Lemma 2.1 is also true. □

Lemma 2.2 *Let $\tau : M \to M$ be a semi-linear involution and $W = \{m \in M : \tau(m) = m\}$. Then W is a $\mathbf{Z}_4$-submodule and $M = W \oplus \omega W$.*

Proof: Suppose that $\tau : M \to M$ is a semi-linear involution. Since $\bar{a} = a$ for all $a \in \mathbf{Z}_4$, the set W is a $\mathbf{Z}_4$-submodule of M. Since $\omega \neq \omega^2$, $\lambda = \omega - \bar{\omega} \in \mathbf{Z}_4[\omega]^*$.

It is clear that $\bar{\lambda} = -\lambda$. We shall show that for all $m \in M$ there exist $r, s \in W$ such that $m = r + \omega s$. For this set

$$\begin{aligned}r &= \frac{1}{\lambda}(\omega\tau(m) - \bar{\omega}m)\\ s &= \frac{1}{\lambda}(m - \tau(m)).\end{aligned}$$

Therefore

$$\tau(r) = \frac{\bar{\omega}}{\bar{\lambda}}m - \frac{1}{\bar{\lambda}}\omega\tau(m) = \frac{-1}{\lambda}(\bar{\omega}m - \omega\tau(m)) = r$$

and

$$\tau(s) = s.$$

So we have proved that $M = W + \omega W$. Now suppose $\hat{r} \in W \cap \omega W$. Since $\hat{r} \in W$, we have $\tau(\hat{r}) = \hat{r}$. On the other hand, $\hat{r} \in \omega W$ so $\hat{r} = \omega\hat{s}$ for some $\hat{s} \in W$. Hence $\hat{s} = \omega^{-1}\hat{r}$ and

$$\tau(\hat{r}) = \tau(\omega\hat{s}) = \bar{\omega}\hat{s} = \bar{\omega}\omega^{-1}\hat{r} = \omega^2\omega^{-1}\hat{r} = \omega\hat{r}.$$

Since $1 - \omega \in \mathbf{Z}_4[\omega]^*$, we have $\hat{r} = 0$. Hence

$$M = W \oplus \omega W.$$

□

Denote by $\mathbf{SL}(2, p)$ the set of all 2×2 matrices A with entries in $\mathbf{Z}_p$ such that $\det A = 1$. Then $\mathbf{SL}(2, p)$ is called the 2-dimensional special linear group over $\mathbf{Z}_p$. We aim to find such a W invariant under the action of $\mathbf{SL}(2, p)$.

Lemma 2.3 *Let $\tau : M \to M$ be a semi-linear involution, and $W = \{m \in M : m = \tau(m)\}$. Then W is invariant under the action of $\mathbf{SL}(2, p)$ if and only if $\tau(mA) = \tau(m)A$ for all $A \in \mathbf{SL}(2, p)$ and $m \in M$.*

Proof: Suppose W is invariant under $\mathbf{SL}(2, p)$ and $r, s \in W$. Then

$$\begin{aligned}\tau((r + \omega s)A) &= \tau(rA + \omega sA) = \tau(rA) + \tau(\omega sA)\\ &= rA + \bar{\omega} sA = (r + \bar{\omega} s)A\\ &= \tau(r + \omega s)A.\end{aligned}$$

Conversely if $\tau(mA) = \tau(m)A$ for all $m \in M$ and $A \in \mathbf{SL}(2, p)$, then for $m \in W$

$$\tau(mA) = \tau(m)A = mA.$$

Hence W is invariant under $\mathbf{SL}(2, p)$. □

Quaternary quadratic residue codes are invariant under the corresponding action of $\mathbf{SL}(2, p)$ defined from the quadratic character $\chi(a) = (\frac{a}{p})$ (see [2]).

Definition 2.2 We consider such a submodule W which is invariant under the action of SL$(2, p)$ according to Lemma 2.3. We call W a higher power residue code. In particular when χ is a character of order 3 we call W a cubic residue code and when χ has order 6 we call W a sextic residue code.

Now we are going to define a hermitian structure on M.

Definition 2.3 A $\mathbf{Z}_4$- bilinear form $\Phi : M \times M \to \mathbf{Z}_4[\omega]$ satisfying

(1) $\Phi(\lambda_1 m_1 + \lambda_2 m_2, \hat{m}_1) = \bar{\lambda}_1 \Phi(m_1, \hat{m}_1) + \bar{\lambda}_2 \Phi(m_2, \hat{m}_1)$
(2) $\Phi(m_1, \lambda_1 \hat{m}_1 + \lambda_2 \hat{m}_2) = \lambda_1 \Phi(m_1, \hat{m}_1) + \lambda_2 \Phi(m_1, \hat{m}_2)$

for all $m_1, m_2, \hat{m}_1, \hat{m}_2 \in M$, $\lambda_1, \lambda_2 \in \mathbf{Z}_4[\omega]$ is called a sesquilinear form on M.

Lemma 2.4 *Define a sesquilinear form Φ on M by*

$$\Phi(e_\alpha, e_\beta) = \begin{cases} 1 & \alpha = \beta \\ 0 & \alpha \neq \beta \end{cases} \tag{3}$$

for $\alpha, \beta \in \mathbf{P}^1(\mathbf{Z}_p)$. Then Φ has the following properties:
(i) $\Phi(e_v, e_w) = \overline{\Phi(e_w, e_v)}$ *for all $v, w \in \Omega$*
(ii) $\Phi(e_v A, e_w A) = \Phi(e_v, e_w)$ *for all $v, w \in \Omega$*

Proof:

(i) First of all suppose v and w are linearly independent. In this case both sides of (i) are zero. Now suppose $w = \alpha v$. Therefore:

$$\overline{\Phi(e_w, e_v)} = \overline{\chi(\alpha)}. \tag{4}$$

On the other hand $v = \alpha^{-1} w$ and

$$\Phi(e_w, e_v) = \chi(\alpha^{-1}). \tag{5}$$

The result follows from (4), (5) and the fact that $\chi(\alpha^{-1}) = \overline{\chi(\alpha)}$.

(ii) One can achieve the result by using the same process as (i) and definition of $e_v A$ and applying (2). □

Corollary 2.1 *Let Φ be as in Lemma* 2.4. *Then for all $m_1, m_2 \in M$ and $A \in \mathbf{SL}(2, p)$ we have*

(i) $\Phi(m_2, m_1) = \overline{\Phi(m_1, m_2)}$
(ii) $\Phi(m_1 A, m_2 A) = \Phi(m_1, m_2)$.

Proof:

(i) is clear by sesquilinearity of Φ.
(ii) follows from (ii) of Lemma 2.4 and the linearity of Φ.

Recall $\Omega = (\mathbf{Z}_p \times \mathbf{Z}_p) - \{(0, 0)\}$. □

Lemma 2.5 *Let τ be a semi-linear involution $\tau : M \to M$ such that $\tau(mA) = \tau(m)A$ for all $A \in \mathbf{SL}(2, p)$ and $m \in M$, and $\chi : \mathbf{Z}_p^* \to \mathbf{Z}_4[\omega]^*$ be a character of order $s > 2$. Define $\Psi : \Omega \times \Omega \to \mathbf{Z}_4[\omega]^*$ by $\Psi(v, w) = \Phi(\tau(e_v), (e_w))$. Then Ψ satisfies the following.*

(i) $\Psi(\alpha v, \beta w) = \chi(\alpha\beta)\Psi(v, w)$ for $\alpha, \beta \in \mathbf{Z}_p$
(ii) $\Psi(vA, wA) = \Psi(v, w)$
(iii) $\Psi(v, w) = 0$ whenever v and w are linearly dependent.

Proof:

(i)

$$\begin{aligned}\Psi(\alpha v, \beta w) &= \Phi(\tau(e_{\alpha v}), e_{\beta w}) = \Phi(\tau(\chi(\alpha) e_v), \chi(\beta) e_w) \\ &= \Phi(\overline{\chi(\alpha)}\tau(e_v), \chi(\beta) e_w) = \chi(\alpha)\chi(\beta)\Phi(\tau(e_v), e_w) \\ &= \chi(\alpha\beta)\Psi(v, w).\end{aligned} \tag{6}$$

(ii)

$$\begin{aligned}\Psi(vA, wA) &= \Phi(\tau(e_{vA}), e_{wA}) = \Phi(\tau(e_v A), e_w A)\\ &= \Phi(\tau(e_v)A, e_w A)\\ &= \Phi(\tau(e_v), e_w)\\ &= \Psi(v, w).\end{aligned} \tag{7}$$

(iii) Suppose α is an element of $\mathbf{Z}_p^*$ such that $\chi(\alpha) \neq \pm 1$. Such an element exists, since otherwise, the order of χ does not exceed two. Now we can find a matrix $A \in \mathbf{SL}(2, p)$ such that $vA = \alpha v$, and then also $wA = \alpha w$. Therefore, $\Psi(v, w) = \Psi(vA, wA) = \Psi(\alpha v, \alpha w) = \chi(\alpha)^2 \Psi(v, w)$. Hence, $\Psi(v, w) = 0$. □

Lemma 2.6 *Let Ψ be as in Lemma 2.5 and $v = (\alpha, \beta)$, $w = (\gamma, \delta)$ be linearly independent elements of Ω, $A = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ and $\hat{x} = \det A$.*

(i) There exists some $\zeta \in \mathbf{Z}_4[\omega]$ such that $\Psi(v, w) = \zeta\chi(\hat{x})$
(ii) $\Psi(w, v) = \chi(-1)\Psi(v, w)$.

Proof:

(i) Let $v_0 = (1, 0)$, $w_0 = (0, 1)$. Hence $v = v_0 A'$, $w = \hat{x} w_0 A'$ where

$$A' = \begin{pmatrix}\alpha & \beta\\ \hat{x}^{-1}\gamma & \hat{x}^{-1}\delta\end{pmatrix} \in \mathbf{SL}(2, p).$$

Then

$$\Psi(v, w) = \Psi(v_0 A', \hat{x} w_0 A') = \chi(\hat{x})\Psi(v_0, w_0). \tag{8}$$

Taking ζ as $\Psi(v_0, w_0)$, completes the proof.

(ii) $\Psi(w, v) = \zeta\chi(-\hat{x}) = \zeta\chi(-1)\chi(\hat{x}) = \chi(-1)\Psi(v, w)$.

□

Proposition 2.1 *Let ζ be an element of $\mathbf{Z}_4[\omega]$ satisfying the conditions of Lemma 2.6 and $\tau : M \to M$ be a semi-linear involution which satisfies $\tau(mA) = \tau(m)A$, for all $A \in \mathbf{SL}(2, p)$ and $m \in M$. Then*

$$\tau(e_v) = \sum_{w \in \mathbf{P}^1(\mathbf{Z}_p)} \overline{\zeta U_{vw}} e_w \tag{9}$$

where

$$U_{\alpha\beta} = \begin{cases}\chi(\alpha - \beta) & \text{if } \beta \neq \infty,\ \alpha \neq \infty\\ \chi(-1) & \text{if } \beta = \infty,\ \alpha \neq \infty\\ 1 & \text{if } \alpha = \infty,\ \beta \neq \infty\\ 0 & \text{if } \alpha = \infty,\ \beta = \infty\end{cases} \tag{10}$$

and ζ satisfies the equation

$$p\chi(-1)\zeta\bar{\zeta} = 1. \tag{11}$$

Proof: Using Lemmas 2.5 and 2.6 shows that

$$\begin{aligned}\tau(e_v) &= \sum_{w\in\mathbf{P}^1(\mathbf{Z}_p)} \Phi(e_w, \tau(e_v))e_w = \sum_{w\in\mathbf{P}^1(\mathbf{Z}_p)} \overline{\Phi(\tau(e_v), e_w)}e_w \\ &= \sum_{w\in\mathbf{P}^1(\mathbf{Z}_p)} \overline{\Psi(v, w)}e_w = \sum_{w\in\mathbf{P}^1(\mathbf{Z}_p)} \overline{\zeta U_{vw}}e_w,\end{aligned}$$

where U is the matrix defined by (10). Therefore,

$$\tau(e_\infty) = \bar{\zeta}\sum_{i=0}^{p-1} e_i,$$

and so

$$\begin{aligned}1 &= \Phi(e_\infty, e_\infty) = \Phi(\tau(e_\infty)^2, e_\infty) \\ &= \Phi(\tau(\tau(e_\infty)), e_\infty) = \Phi\left(\tau\left(\bar{\zeta}\sum_{i=0}^{p-1} e_i\right), e_\infty\right) \\ &= \Phi\left(\sum_{i=0}^{p-1} \zeta\tau(e_i), e_\infty\right) = \bar{\zeta}\left(\sum_{i=0}^{p-1} \Phi(\tau(e_i), e_\infty\right) \\ &= \bar{\zeta}\zeta p\chi(-1).\end{aligned}$$

Therefore

$$p\chi(-1)\zeta\bar{\zeta} = 1. \tag{12}$$

□

Remark 2.1 If ζ satisfies (12) and τ is defined by (9) then by Lemma 2.4,

$$\Phi(e_\alpha, e_\beta) = \Phi(\tau^2(e_\alpha), e_\beta). \tag{13}$$

Therefore, $\tau^2(m) = m$ for all $m \in M$. This shows that τ is a semi-linear involution. Moreover,

$$\begin{aligned}\Phi(\tau(e_v A), w) &= \Phi(\tau(e_{vA}), w) = \Psi(vA, w) = \Psi(v, wA^{-1}) \\ &= \Phi(\tau(e_v), wA^{-1}) = \Phi(\tau(e_v)A, w).\end{aligned} \tag{14}$$

Hence $\tau(mA) = \tau(m)A$, for all $m \in M$. So by Lemma 2.3, $W = \{m \in M : \tau(m) = m\}$ is invariant under the action of $\mathbf{SL}(2, p)$.

Remark 2.1 shows the existence of a semi-linear involution τ such that W is invariant under the action of $\mathbf{SL}(2, p)$. In fact any semi-linear involution τ on M gives a Higher power residue code W and semi-linear involutions are correspond to the solutions of (12) via (9).

One of the prominent questions is : how many different higher power residue codes are there in each case. We need to prove the following lemma

Lemma 2.7 *Let W be a higher power residue code over $\mathbf{Z}_4[\omega]$ then λW for $\lambda \in \mathbf{Z}_4[\omega]^*$ is a higher power residue code.*

Proof: What we shall do is to find a semi-linear involution $\acute{\tau}$ such that $\acute{\tau}(\lambda W) = \lambda W$. Let $\acute{\tau} = \varepsilon\tau$. So we have

$$\acute{\tau}(\lambda m) = \varepsilon\tau(\lambda m) = \varepsilon\bar{\lambda}\tau(m) = \varepsilon\bar{\lambda}m$$

for $m \in W$. So it suffices to choose $\varepsilon = \lambda/\bar{\lambda}$. Obviously $\varepsilon\bar{\varepsilon} = 1$ and this proves that $\acute{\tau}$ is a semi-linear involution. □

Proposition 2.2 *The higher power residue code is unique up to multiplication by an element of $\mathbf{Z}_4[\omega]^*$.*

Proof: Let W and $\acute{W}$ be higher power residue codes. Then they are respectively the fixed sets of semi-linear involutions τ and $\acute{\tau}$, and they are invariant under the action of $\mathbf{SL}(2, p)$. By (9) and (12) $\acute{\tau} = \epsilon\tau$ where $\epsilon\overline{\epsilon} = 1$. Such an ϵ has the form $\lambda/\overline{\lambda}$ and so $\acute{W} = \lambda W$ by the argument of Lemma 2.7. □

Proposition 2.3 *Let τ be the unique semi-linear involution $\tau : M \to M$ which is defined by* (9) *and S be the set of $\eta \in \mathbf{Z}_4[\omega]^*$ such that $\eta + \bar{\eta} \in \mathbf{Z}_4[\omega]^*$. Define*

$$\begin{aligned} h : M &\to M \\ m &\mapsto \eta m + \bar{\eta}\tau(m) \end{aligned}$$

for some $\eta \in S$. Then W is the image of h.

Proof: If $m \in W$ and $\eta \in S$ then $\eta m + \tau(\eta m) = (\eta + \bar{\eta})m$. Set $n = (\eta + \bar{\eta})^{-1}m$. Therefore $h(n) = m$. □

Definition 2.4 Define a $\mathbf{Z}_4$-bilinear map

$$\begin{aligned} [\quad,\quad] : M \times M &\to \mathbf{Z}_4 \\ (m_1, m_2) &\longmapsto \Phi(m_1, m_2) + \overline{\Phi(m_1, m_2)}. \end{aligned}$$

We denote the dual space of W by

$$W' = \{m_2 \in M : [m_1, m_2] = 0 \quad \text{for all } m_1 \in W\}. \tag{15}$$

Proposition 2.4 *Suppose* $\chi(-1) = -1$. *Then* W *is self dual under* $[\ ,\ ]$.

Proof: By Lemma 2.6

$$\Phi(\tau(m_1), m_2) = -\Phi(\tau(m_2), m_1), \tag{16}$$

for all $m_1, m_2 \in M$. So for all $m_1, m_2 \in W$ we have

$$\Phi(m_1, m_2) = \Phi(\tau(m_1), m_2) = -\Phi(\tau(m_2), m_1) = -\Phi(m_2, m_1) = -\overline{\Phi(m_1, m_2)}. \tag{17}$$

We know that $|M| = |W| \times |W'|$ and $|W| = \sqrt{|M|}$, so $W = W'$. This completes the proof. □

Suppose $p = 7$ and in Proposition 2.1 define $\chi : \mathbf{Z}_7^* \longrightarrow \mathbf{Z}_4[\omega]^*$ such that $\chi(5) = -\omega$ and choose $\zeta = 1$ which is one of the solutions of (12). In this case by calculation, the space which is spanned by the rows of the following matrix over $\mathbf{Z}_4$ has rank 8 over $\mathbf{Z}_4$. Therefore W is spanned over $\mathbf{Z}_4$ by the rows of this matrix.

$$\begin{bmatrix} \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\ -\omega^2 & \omega & -\omega^2 & -\omega & 1 & -1 & \omega & \omega^2 \\ -\omega^2 & \omega^2 & \omega & -\omega^2 & -\omega & 1 & -1 & \omega \\ -\omega^2 & 1 & \omega^2 & \omega & -\omega^2 & -\omega & 1 & -1 \\ -\omega^2 & -1 & 1 & \omega^2 & \omega & -\omega^2 & -\omega & 1 \\ -\omega^2 & 1 & -1 & 1 & \omega^2 & \omega & -\omega^2 & -1 \\ -\omega^2 & -\omega & 1 & -1 & 1 & \omega^2 & \omega & -\omega^2 \\ -\omega^2 & -\omega^2 & -\omega & 1 & -1 & 1 & \omega^2 & \omega \end{bmatrix} \tag{18}$$

This W is a sextic residue code. This construction generalizes that of Chapman[3].

The symmetrized weight enumerator of a code W over $\mathbf{Z}_4[\omega]$ is defined as follows.

Consider a specific codeword $r \in W$. Now, let $n_0(r)$ be the number of zeroes in the codeword, $n_1(r)$ be the number of elements of $\mathbf{Z}_4[\omega]^*$, $n_2(r)$ be the number of elements of $2\mathbf{Z}_4[\omega] - \{0\}$ in the codeword. The *symmetrized weight enumerator* of W is

$$swe_W(x, y, z) = \sum_{r \in W} x^{n_0(r)} y^{n_1(r)} z^{n_2(r)}. \tag{19}$$

The symmetrized weight enumerator of W, the sextic residue code of length 8 is as follows.

$$\begin{aligned} swe_W(x, y, z) = x^8 &+ 42\,x^4z^4 + 672\,x^3y^4z + 2688\,x^2y^6 + 2016\,x^2y^4z^2 \\ &+ 168\,x^2z^6 + 16128\,xy^6z + 4704\,xy^4z^3 + 11520\,y^8 \\ &+ 24192\,y^6z^2 + 3360\,y^4z^4 + 45\,z^8. \end{aligned}$$

3. The Leech lattice

Now we are going to construct the Leech lattice and one of the Niemeier lattices by using a higher power residue code of length 8 over $\mathbf{Z}_4[\omega]$.

We are going to use the same action of $\mathbf{SL}(2, 7)$ on the code. Under this action for each $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbf{SL}(2, 7)$

$$e_v A = \vartheta(A, v)e_w \tag{20}$$

where $w = \frac{\alpha v+\gamma}{\beta v+\delta}$ and $\vartheta(A, v) = \sigma(A, v)\omega^{j(A,v)}$, where $\sigma(A, v)$ is either 1 or -1 and $j(A, v)$ is 0, 1 or -1. We regard $j(A, v)$ are lying in the integers modulo 3. It is also apparent that for each $A \in \mathbf{SL}(2, 7)$ there exists an invertible 8×8 matrix $\hat{A}$ such that

$$e_v A = e_v \hat{A}. \tag{21}$$

Lemma 3.1 *Let* $\vartheta(A, v)$ *be defined by* (20). *Then*

$$\vartheta(AB, v) = \vartheta(A, v)\vartheta(B, v \cdot A)$$

Proof:

$$\begin{aligned} (e_v A)B &= \vartheta(A, v)e_{v\cdot A}B \\ &= \vartheta(A, v)\vartheta(B, v \cdot A)e_{(v\cdot A)\cdot B}. \end{aligned}$$

On the other hand,

$$e_v(AB) = \vartheta(AB, v)e_{v\cdot AB}.$$

Since the left hand sides are equal, the proof is complete. □

Let W be the sextic residue code of length 8 over $\mathbf{Z}_4[\omega]$ with character χ where $\chi(-1) = -1$ and $\chi(5) = -\omega$. Each $\zeta \in \mathbf{Z}_4[\omega]$ can be written uniquely as $\zeta = a_0 + a_1\omega + a_2\omega^2$, $a_i \in \mathbf{Z}_4$ where $a_0 + a_1 + a_2 = 0$.

Let $\hat{M}$ be a free $\mathbf{Z}_4$-module generated by $\{f_{\alpha,j} : \alpha \in \mathbf{P}^1(\mathbf{Z}_7), 0 \le j \le 2\}$. So we define

$$\begin{aligned} \hat{\phi} : \; M \; &\rightarrow \qquad\qquad \hat{M} \\ \zeta e_\alpha &\mapsto a_0 f_{\alpha,0} + a_1 f_{\alpha,1} + a_2 f_{\alpha,2} \end{aligned}$$

The map (22) can be easily extended to the map $\phi : W \rightarrow \hat{M}$ which takes $r \in W$ to

$$(a_{\infty,0}, a_{\infty,1}, a_{\infty,2}, a_{0,0}, a_{0,1}, a_{0,2}, \ldots, a_{6,0}, a_{6,1}, a_{6,2})$$

where

$$a_{\alpha,0} + a_{\alpha,1} + a_{\alpha,2} \equiv 0 \pmod 4 \qquad \text{for } \alpha \in \mathbf{P}^1(\mathbf{Z}_7).$$

We denote the code $\phi(W)$ by T.

We consider the matrix (18) and we replace each array by its three coordinates as above. So we have a generator matrix for the code T over $\mathbf{Z}_4$ as follows.

$$\begin{bmatrix}
1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 \\
3 & 3 & 2 & 1 & 2 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 1 & 1 & 1 & 2 \\
3 & 3 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 1 \\
3 & 3 & 2 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 & 2 & 3 & 3 \\
3 & 3 & 2 & 2 & 3 & 3 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 \\
3 & 3 & 2 & 2 & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 3 & 3 & 2 & 3 & 2 & 3 \\
3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 3 & 3 & 2 \\
3 & 3 & 2 & 3 & 3 & 2 & 3 & 2 & 3 & 2 & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1
\end{bmatrix}$$

We consider the inner product on $\hat{M}$ with respect to the inner product with the $f_{\alpha,i}$ orthonormal and we set the *weight* of 0, 1, 2, 3 in $\mathbf{Z}_4$ as 0, 1, 4, 1 respectively. So the *Euclidean weight* of a codeword r is the sum of the weights of its coordinates. It can be easily seen that the Euclidean weight of each codeword in T is divisible by 8. This shows that the code T is self-orthogonal.

We shall define an action of $\mathbf{SL}(2, 7)$ on $\hat{M}$. Define,

$$f_{v,i} A = \sigma(A, v) f_{v \cdot A, i+j(A,v)}$$

where the suffix $i + j(A, v)$ read modulo 3. We can show that this action is well-defined.

$$(f_{v,i}A)B = \sigma(A, v)f_{v\cdot A,i+j(A,v)}B = \sigma(A, v)\sigma(B, v\cdot A)f_{(v\cdot A)\cdot B,i+j(A,v)+j(B,v\cdot A)}$$

On the other hand,

$$f_{v,i}AB = \sigma(AB, v)f_{v\cdot AB,i+j(AB,v)}$$

and by Lemma 3.1 $\sigma(A, v)\sigma(B, v\cdot A) = \sigma(AB, v)$ and $j(A, v) + j(B, v\cdot A) = j(AB, v)$ which completes the proof. □

Now it is easy to see that ϕ is $\mathbf{Z}_4$-linear and $\phi(rA) = \phi(r)A$ for all $r \in W$ and $A \in \mathbf{SL}(2, 7)$.

Proposition 3.1 *Suppose $\bar{W}$ is a code of length* 8 *over* $\mathbf{Z}_4[\omega]$ *with generator matrix* $\bar{G}$ *and* $\hat{A}$ *is the matrix which is defined by* (21). *If* $\bar{G}\hat{A} = \hat{A}\bar{G}$ *then* $\bar{W}$ *is invariant under the action of* $\mathbf{SL}(2, 7)$.

Proof: Let $\bar{\zeta} \in \bar{W}$. Therefore, there exists $\bar{a} \in \mathbf{Z}_4^8$ such that $\bar{\zeta} = \bar{a}\bar{G}$, hence

$$\bar{\zeta}\hat{A} = \bar{a}\bar{G}\hat{A} = \bar{\zeta}\hat{A}\bar{G} = \bar{\eta}\bar{G} \in \bar{W},$$

for some $\bar{\eta} \in \mathbf{Z}_4^8$. This completes the proof. □

Now consider the construction of the extended quaternary quadratic residue codes. Let H be the matrix defined by (10) with $\chi(\alpha) = (\frac{\alpha}{7})$. Set $\widetilde{G} = 5I_{8\times 8} - Y$. The matrix H is a skew symmetric matrix and $\hat{A}\widetilde{G} = \widetilde{G}\hat{A}$, so by Proposition 3.1, $\widetilde{G}$ generates a code over $\mathbf{Z}_4$ which is invariant under the action of $\mathbf{SL}(2, 7)$. Suppose $row(G, i)$ is the ith row of the matrix G. Now set

$$\Theta = \left\{\frac{1}{2}(\pm row(\widetilde{G}, i) \pm row(\widetilde{G}, j)) : 1 \le i, j \le 8\right\}.$$

The code Q_4 which is generated by Θ is the extended quadratic residue code over $\mathbf{Z}_4$ obtained by Hensel lifting (see [4]). The code Q_4 is invariant under the action of $\mathbf{SL}(2, 7)$ (see [2]). The number of linearly independent vectors in this set is at most 8. So suffices it to consider 8 vectors as follows. Set the matrix $\hat{G}$ as a matrix where

$$row(\hat{G}, i) = (row(\widetilde{G}, 1) + row(\widetilde{G}, i))/2.$$

That is

$$\hat{G} = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 2 & 0 & 0 & -1 & 0 & -1 & -1 \\ -1 & -1 & 2 & 0 & 0 & -1 & 0 & -1 \\ -1 & -1 & -1 & 2 & 0 & 0 & -1 & 0 \\ -1 & 0 & -1 & -1 & 2 & 0 & 0 & -1 \\ -1 & -1 & 0 & -1 & -1 & 2 & 0 & 0 \\ -1 & 0 & -1 & 0 & -1 & -1 & 2 & 0 \\ -1 & 0 & 0 & -1 & 0 & -1 & -1 & 2 \end{bmatrix}. \tag{22}$$

The code over $\mathbf{Z}_4$ which is spanned by the rows of the matrix $\hat{G}$ is the same as the code generated by

$$G = \begin{bmatrix} -1 & 1 & 2 & 1 & -1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 2 & 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 2 & 1 & -1 & 0 \\ -1 & 0 & 0 & 0 & 1 & 2 & 1 & -1 \end{bmatrix}.$$

which is the extended quadratic residue code over $\mathbf{Z}_4$ obtained by Hensel lifting [10, Chapter 11].

Define

$$\begin{aligned} \psi : \mathbf{Z}_4^8 &\to \mathbf{Z}_4^{24} \\ \sum_\alpha a_\alpha e_\alpha &\mapsto \sum_\alpha \sum_{j=0}^{2} a_\alpha f_{\alpha,j}. \end{aligned} \tag{23}$$

Since Q_4 is a self-dual code then $Q^{(4)} = \psi(Q_4)$ is self-orthogonal. One can easily see that $Q^{(4)}$ is orthogonal to T. Moreover, $Q^{(4)} \cap T = 0$. So the code $Q^{(4)} + T$ is a self-orthogonal of dimension 12. So it is self-dual. We denote the code $Q^{(4)} + T$ by Γ. A code over $\mathbf{Z}_4$ which is self-dual and the Euclidean weight of each codeword is divisible by 8 is called a code of type II. Computer calculation shows that the symmetric weight enumerator of Γ is

$$\begin{aligned} swe_\Gamma = x^{24} &+ 759\,x^{16}z^8 + 12144\,x^{14}y^8z^2 + 170016\,x^{12}y^8z^4 + 2576\,x^{12}z^{12} \\ &+ 61824\,x^{11}y^{12}z + 765072\,x^{10}y^8z^6 + 1133440\,x^9y^{12}z^3 + 24288\,x^8y^{16} \\ &+ 1214400\,x^8y^8z^8 + 759\,x^8z^{16} + 4080384\,x^7y^{12}z^5 + 680064\,x^6y^{16}z^2 \\ &+ 765072\,x^6y^8z^{10} + 4080384\,x^5y^{12}z^7 + 1700160\,x^4y^{16}z^4 \\ &+ 170016\,x^4y^8z^{12} + 1133440\,x^3y^{12}z^9 + 680064\,x^2y^{16}z^6 \\ &+ 12144\,x^2y^8z^{14} + 61824\,xy^{12}z^{11} + 4096\,y^{24} + 24288\,y^{16}z^8 + z^{24}. \end{aligned}$$

Now we consider the lattice in $\mathbf{R}^{24}$ associated with Γ which is

$$L_\Gamma = \left\{ \frac{1}{2}(g + 4z) : g \in \Gamma, z \in \mathbf{Z}^{24} \right\}, \tag{24}$$

where g is regarded as n-tuples with integers 0, 1, 2, 3 as components. This construction is called construction A_4. Since the code Γ is of type II then the lattice L_Γ is an even unimodular lattice. As we see the number of the vectors of norm 2 is zero, L_Γ is isomorphic to the Leech lattice ([6] chapter 18).

Bonnecaze et al. [2] have constructed the Leech lattice by using a different code over $\mathbf{Z}_4$, but they have found the same symmetrized weight enumerator. We show that these codes are not isomorphic.

Let $\overline{Q}$ be the code described in [2]. We show that $7 \nmid |Aut(\bar{Q})|$. Since we have shown that the automorphism group of Γ contains $\mathbf{SL}(2, 7)$, the conclusion would be apparent.

Theorem 3.1 *The code Γ is inequivalent to the code $\bar{Q}$.*

Proof: The code is actually a lifting of the binary Golay code. Define

$$\rho : Aut(\bar{Q}) \to Aut(\mathcal{G})$$

where $\mathcal{G}$ is the Golay code and the image of an element is the element modulo 2. The image of ρ is a group of automorphisms of the Golay code and $Aut(\bar{Q}) \supseteq \mathbf{SL}(2, 23)$ but $\rho(\mathbf{SL}(2, 23)) = \mathbf{PSL}(2, 23)$, so $\mathbf{PSL}(2, 23) \subseteq \operatorname{Im} \rho$. We know that M_{24} is the full automorphism group of the Golay code $\mathcal{G}_{24}$. So we have

$$\mathbf{PSL}(2, 23) \subseteq \operatorname{Im} \rho \subseteq M_{24}.$$

But $\mathbf{PSL}(2, 23)$ is maximal in M_{24} [7], hence either $\operatorname{Im} \rho = \mathbf{PSL}(2, 23)$ or $\operatorname{Im} \rho = M_{24}$. We show that $\operatorname{Im} \rho \neq M_{24}$. Suppose $\operatorname{Im} \rho = M_{24}$. Now consider a word ϖ of shape $((\pm 1)^8 \quad 2^2 \quad 0^{14})$ in $\bar{Q}$. Let O be an 8 element set (octad) formed by the positions of the ± 1s in the word ϖ. The stabilizer of an octad is one of the maximal subgroups of M_{24} and it acts 2-transitively on the remaining points. That means for i, j, k, l which are not in the O and $i \neq j, k \neq l$, we can find g in the stabilizer of O such that $g(i, j) = (k, l)$. There are 759 octads and by acting on $\pm\varpi$ by the octad stabilizer we get at least $2\binom{16}{2}$ words of shape $((\pm 1)^8 2^2 0^{14})$ in $\bar{Q}$ with ± 1s forming the octad O. So in total there are at least $2 \times 759 \times \binom{16}{2} = 759 \times 16 \times 15$ elements of shape $((\pm 1)^8 2^2 0^{14})$ in $\bar{Q}$. But it is not possible due to swe_Γ. Therefore, $\mathbf{PSL}(2, 23) = \operatorname{Im}\rho$.

Any element of $\ker\rho$ is a diagonal matrix with ± 1s on diagonal, so has order 1 or 2. Since $\ker\rho$ is a 2-group then 7 does not divide the $|Aut(\bar{Q})|$. This completes the proof. (I am indebted to Robin Chapman for this argument). $\square$

Now suppose λ is a unit of $\mathbf{Z}_4[\omega]$. We know that W is a $\mathbf{Z}_4$-linear code but not a $\mathbf{Z}_4[\omega]$-linear code. Moreover, $\tau(\lambda r) = \bar{\lambda}\tau(r)$ for each $r \in W$ and $\bar{\lambda}\tau(r) = \lambda r$ if and only if $\lambda = \bar{\lambda}$. Therefore if $\lambda \in \mathbf{Z}_4[\omega]^*$ and $\lambda\bar{\lambda} \neq 1$, $\hat{W} = \lambda W$ is a different code from W but

$swe_W = swe_{\hat{W}}$. Replacing W by λW in the above construction of Γ gives a type II code $\hat{\Gamma}$. By applying the same process which is described in Section 3 we will find a different lattice. In fact, computer calculation shows that $swe_{\hat{\Gamma}}$ is as follows

$$\begin{aligned} swe_{\hat{\Gamma}} = x^{24} &+ 48\,x^{16}y^8 + 759\,x^{16}z^8 + 11760\,x^{14}y^8z^2 + 171360\,x^{12}y^8z^4 \\ &+ 2576\,x^{12}z^{12} + 61824\,x^{11}y^{12}z + 762384\,x^{10}y^8z^6 + 1133440\,x^9y^{12}z^3 \\ &+ 24288\,x^8y^{16} + 1217760\,x^8y^8z^8 + 759\,x^8z^{16} + 4080384\,x^7y^{12}z^5 \\ &+ 680064\,x^6y^{16}z^2 + 762384\,x^6y^8z^{10} + 4080384\,x^5y^{12}z^7 \\ &+ 1700160\,x^4y^{16}z^4 + 171360\,x^4y^8z^{12} + 1133440\,x^3y^{12}z^9 \\ &+ 680064\,x^2y^{16}z^6 + 11760\,x^2y^8z^{14} + 61824\,xy^{12}z^{11} + 4096\,y^{24} \\ &+ 24288\,y^{16}z^8 + 48\,y^8z^{16} + z^{24}. \end{aligned}$$

As we see the number of the words with minimum weight is 48. If $L \subset \mathbf{R}^n$ is a root lattice and R is its set of roots then the number $h = \frac{|R|}{n}$ is called the Coxeter number. Therefore the Coxeter number in this case is 2 and this lattice is equivalent to the Niemeier lattice A_1^{24}. See [6, Chapter 16] for the classification of Niemeier lattices.

References

1. W. A. Adkins and S.H. Weintraub, *Algebra*, Springer Verlag, New York, 1992.
2. A. Bonnecaze, P. Solé, and A.R. Calderbank, “Quaternary quadratic residue codes and unimodular lattices,” *IEEE Trans. Inform. theory* **41**(2) (1995).
3. R. Chapman, “Higher power residue codes,” *Finite Fields Appl.* **3** (1997), 353–369.
4. R. Chapman, “Conference matrices and unimodular lattices,” *European J. Combin.* **22** (2001), 1033–1045.
5. R. Chapman, Personal communication.
6. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 1st edn., Springer Verlag, New York, 1988.
7. R. T. Curtis, “The maximal subgroups of M_{24},” *Math. Proc. Cambridge Philos. Soc.* **81** (1977), 185–192.
8. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science Publishers, Amsterdam, 1991.
9. J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, New York, 1992.
10. Zhe-Xian Wan, *Quaternary Codes*, World Scientific Publishing, London, 1997.