<table>
<thead>
<tr>
<th>Title</th>
<th>Type II codes over $F_4 + uF_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Ling, San; Sole, Patrick</td>
</tr>
<tr>
<td>Date</td>
<td>2001</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/9864">http://hdl.handle.net/10220/9864</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2001 Academic Press. This is the author created version of a work that has been peer reviewed and accepted for publication by European Journal of Combinatorics, Academic Press. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<a href="http://dx.doi.org/10.1006/eujc.2001.0509">http://dx.doi.org/10.1006/eujc.2001.0509</a>].</td>
</tr>
</tbody>
</table>
Type II Codes Over $\mathbf{F}_4 + u\mathbf{F}_4$

SAN LING† AND PATRICK SOLÉ

A special class of self dual codes over an alphabet of size 16 which contains both $\mathbf{F}_4$ and $\mathbf{F}_2 + u\mathbf{F}_2$ is studied. Applications to codes over these two alphabets and unimodular lattices (Gaussian, golden and integer) are given.

1. Introduction

Self-dual codes over $\mathbf{F}_4$ for the Euclidean scalar product $[2, 6]$ and over $\mathbf{F}_2 + u\mathbf{F}_2$ $[1, 5]$ received some attention lately. In the present article, we study codes over an alphabet $R$ of size 16 that contains both alphabets as subrings. As a consequence, we obtain via suitable Gray maps self-dual codes over these two subrings which, in turn, give self-dual binary codes by the Gray maps of $[6]$ and $[5]$. In particular, we introduce a subclass (Type II codes) of these self-dual codes over $R$ which yield, after double Gray mapping, doubly even binary codes.

Following a trend illustrated in [1] we also give constructions of lattices; specifically $\mathbb{Z}$-lattices, Gaussian lattices and lattices over the golden integers via Construction A. A connection with Tits quaternionic construction of the Leech lattice $[4, 8]$ is pointed out.

2. Notations and Definitions

In this section, we give the required notations and definitions. In particular, we introduce Type II codes which are a remarkable class of self-dual codes. First, we need to recall some notations and definitions concerning codes over $\mathbf{F}_4$ and $\mathbf{F}_2 + u\mathbf{F}_2$, before introducing notations and definitions for codes over $\mathbf{F}_4 + u\mathbf{F}_4$.

2.1. Codes over $\mathbf{F}_4$ and $\mathbf{F}_2 + u\mathbf{F}_2$. Consider the number field $\mathbb{Q}(\sqrt{5})$ with a ring of integers $\mathbb{Z}[\tau]$, where $\tau = \frac{1 + \sqrt{5}}{2}$ is the golden ratio. The quotient $\mathbb{Z}[\tau]/(2)$ is the finite field $\mathbf{F}_4$. Let the elements of $\mathbf{F}_4$ be $0, 1, \omega, \bar{\omega}$, where $\omega$ is the image of $\tau$ under reduction mod 2. Codes over $\mathbf{F}_4$ of length $n$ are defined to be $\mathbf{F}_4$-subspaces of $\mathbf{F}_4^n$. An additive code is a subgroup of $(\mathbf{F}_4^n, +)$. Duality of such codes is understood to be with respect to the Euclidean form $\sum_i x_i y_i$. Two codes over $\mathbf{F}_4$ are equivalent if one can be obtained from the other by permuting the coordinates. The Lee weights of the elements of $\mathbf{F}_4$ are given as follows:

$$w_L(0) = 0, \quad w_L(1) = 2, \quad w_L(\omega) = 1, \quad w_L(\bar{\omega}) = 1.$$ 

The Lee weight of a vector in $\mathbf{F}_4^n$ is the rational sum of the Lee weights of its coordinates. A self-dual code over $\mathbf{F}_4$ is said to be of Type II if the Lee weight of every codeword is a multiple of 4. Such codes were studied in detail in $[6]$.

A notion of Euclidean weight was introduced in $[6]$. For the purpose of this paper, we define the Euclidean weight on $\mathbf{F}_4$ slightly differently. Our version may be regarded as a twisted version of the definition in $[6]$. It may also be regarded as the one in $[6]$ except that

†To whom correspondence should be addressed.
the choices of $\omega$ and $\overline{\omega}$ have been interchanged. The Euclidean weights of the elements of $F_4$ are given as follows:

$$w_E(0) = 0, \quad w_E(1) = 1, \quad w_E(\omega) = 2, \quad w_E(\overline{\omega}) = 1.$$ 

Observe that $\tau \mapsto \omega \tau$ is an isometry from $(F_4, w_L)$ to $(F_4, w_E)$. Therefore, a Type II code over $F_4$ can also be defined to be a self-dual code over $F_4$ in which the Euclidean weight of every codeword is a multiple of 4.

We also recall that there is a Gray map $\psi'$ that is an $F_2$-linear isometry from $(F_4^n, $Lee distance$)$ to $(F_2^{2n}, $Hamming distance$)$, where the Lee distance of two codewords $c$ and $c'$ is the Lee weight of $c - c'$. It is given by

$$\psi'(\omega x + \overline{\omega} y) = (x, y),$$

where $x, y \in F_2^n$.

We also note that, if $C$ is a self-dual code over $F_4$, then $C$ contains the all-one vector. This can be seen easily by, for example, using the fact that $\psi'$ preserves self-duality [6, Proposition 3.1] and that a self-dual binary code must contain the all-one vector.

Similarly, by considering the number field $Q(\sqrt{5}, i)$, where $i = \sqrt{-1}$, with ring of integers $Z[i]$, the quotient $Z[i]/(2)$, or equivalently $Z[X]/(2, (X + 1)^2)$, is the finite ring $F_2 + uF_2$, where $u$ denotes the residue class of $X + 1$, or equivalently the residue class of $1 + i$ in the quotient $Z[i]/(2)$. Note that $u^2 = 0$. Codes over $F_2 + uF_2$ of length $n$ are defined to be $F_2 + uF_2$-submodules of $(F_2 + uF_2)^n$. Duality of such codes is understood to be with respect to the Euclidean form $\sum_i x_i y_i$. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and exchanging 1 and 1 + $u$ in certain coordinates. The Lee weights of the elements of $F_2 + uF_2$ are given as follows:

$$w_L(0) = 0, \quad w_L(1) = 1, \quad w_L(u) = 2, \quad w_L(1 + u) = 1.$$ 

The Lee weight of a vector in $(F_2 + uF_2)^n$ is the rational sum of the Lee weights of its coordinates. A self-dual code over $F_2 + uF_2$ is said to be of Type II if the Lee weight of every codeword is a multiple of 4. Such codes were studied in details in [5].

We also recall that there is a Gray map $\phi'$ that is an $F_2$-linear isometry from $((F_2 + uF_2)^n, $Lee distance$)$ to $(F_2^{2n}, $Hamming distance$)$, where the Lee distance of two codewords $c$ and $c'$ is the Lee weight of $c - c'$. It is given by

$$\phi'(x + uy) = (y, x + y),$$

where $x, y \in F_2^n$.

### 2.2. Codes over $F_4 + uF_4$.

Now consider the number field $Q(\sqrt{5}, i)$ with ring of integers $Z[\tau, i]$. In the quotient $Z[\tau, i]/(2)$, or equivalently,

$$Z[\tau, X]/(2, (X + 1)^2),$$

let $u$ denote the residue class of $X + 1$. This quotient is then the ring $F_4 + uF_4$, where $u^2 = 0$. Throughout this paper, we let $R$ denote this ring $F_4 + uF_4$.

A code $C$ of length $n$ over $R$ is an $R$-submodule of $R^n$. An additive code is a subgroup of $(R^n, +)$. An element of $C$ is called a codeword. Duality for codes is understood with respect to the Euclidean form $\sum_i x_i y_i$. The dual of $C$ is denoted $C^\perp$. A code $C$ is said to be self-dual if $C = C^\perp$. Two codes over $R$ are said to be equivalent if one can be obtained from the other
by permuting the coordinates. For $x \in R$, we define the Lee weight $w_L(x)$ and the Euclidean weight $w_E(x)$ of $x$ as in Table 1. The Lee (resp. Euclidean) weight of a vector in $R^n$ is the rational sum of the Lee (resp. Euclidean) weights of the coordinates. For $i \in \{0, 1, 2, 3, 4\}$ and a vector $c \in R^n$, let $n_i(c)$ denote the number of coordinates that have Lee weight $i$. Then the Lee weight of $c$ is $w_L(c) = \sum_{i=0}^{4} i \cdot n_i(c)$. The symmetrized weight enumerator (swe for short) for a code $C$ over $R$ is defined as

$$\text{swe}_C(a, b, c, d, e) = \sum_{c \in C} a^{n_0(c)} b^{n_1(c)} c^{n_2(c)} d^{n_3(c)} e^{n_4(c)}.$$ 

We also define a Gray map $\phi : R^n \rightarrow F_4^{2n}$ and two Gray maps $\psi, \nu : R^n \rightarrow (F_2 + uF_2)^{2n}$ as follows:

$$\phi : R^n \rightarrow F_4^{2n}, \quad x + uy \mapsto (y, x + y),$$

where $x, y \in F_4^n$, and

$$\psi : R^n \rightarrow (F_2 + uF_2)^{2n}, \quad \omega x + \omega y \mapsto (x, y), \quad \nu : R^n \rightarrow (F_2 + uF_2)^{2n}, \quad \omega x + \omega y \mapsto (x + y, x),$$

where $x, y \in (F_2 + uF_2)^n$.

The Gray map $\phi$ is an $F_4$-linear isometry from $(R^n, \text{Lee distance})$ to $(F_4^{2n}, \text{Lee distance})$, where the Lee distance of two codewords $c$ and $c'$ is the Lee weight of $c - c'$. It is also an isometry from $(R^n, \text{Euclidean distance})$ to $(F_4^{2n}, \text{Euclidean distance})$.

The Gray map $\psi$ is an $F_2 + uF_2$-linear isometry from $(R^n, \text{Lee distance})$ to $((F_2 + uF_2)^{2n}, \text{Lee distance})$, while the Gray map $\nu$ is an $F_2 + uF_2$-linear isometry from $(R^n, \text{Euclidean distance})$ to $((F_2 + uF_2)^{2n}, \text{Lee distance})$.

\footnote{Note that the notation $w_L$ is used to denote three different Lee weights, viz. for $F_4$, $F_2 + uF_2$ and $R$. However, it should be clear from the context which one of the three is referred to.}

<table>
<thead>
<tr>
<th>$x$</th>
<th>$w_L(x)$</th>
<th>$\phi(x)$</th>
<th>$\psi(x)$</th>
<th>$\nu(x)$</th>
<th>$w_E(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>01</td>
<td>11</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>1 + u</td>
<td>10</td>
<td>1 + u, 1 + u</td>
<td>0, 1 + u</td>
<td>1 + u, 1 + u</td>
<td>2</td>
</tr>
<tr>
<td>1 + $\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>1</td>
</tr>
<tr>
<td>1 + $\overline{\omega}$</td>
<td>$\overline{\omega}$</td>
<td>$\overline{\omega}$</td>
<td>$\overline{\omega}$</td>
<td>$\overline{\omega}$</td>
<td>1</td>
</tr>
<tr>
<td>$\omega$</td>
<td>0$\omega$</td>
<td>0$\omega$</td>
<td>0$\omega$</td>
<td>0$\omega$</td>
<td>0</td>
</tr>
<tr>
<td>$\omega + u$</td>
<td>$\omega + u$</td>
<td>$\omega + u$</td>
<td>$\omega + u$</td>
<td>$\omega + u$</td>
<td>0</td>
</tr>
<tr>
<td>$\omega + \overline{\omega}$</td>
<td>3 $\omega + \overline{\omega}$</td>
<td>$\omega + \overline{\omega}$</td>
<td>$\omega + \overline{\omega}$</td>
<td>$\omega + \overline{\omega}$</td>
<td>3</td>
</tr>
<tr>
<td>$\overline{\omega}$</td>
<td>3 $\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 1.
A self-dual code over $R$ is said to be of Type II if the Lee weight of every codeword is a multiple of 4 and of Type I otherwise. Noting that $x \mapsto \omega x$ is an isometry from $(\mathbb{R}^n, w_L)$ to $(\mathbb{R}^n, w_E)$, a Type II code over $R$ can also be defined to be a self-dual code over $R$ in which the Euclidean weight of every codeword is a multiple of 4.

3. First Properties

3.1. Gray map. We first connect the properties of a code $C$ over $R$ with those of its Gray images. We begin by observing that the Gray images $\psi(C)$ and $\nu(C)$ are indeed the same.

**Lemma 3.1.** The maps $\psi \circ \omega, \nu : \mathbb{R}^n \rightarrow (\mathbb{F}_2 + u\mathbb{F}_2)^{2n}$, where $\omega$ is the map on $\mathbb{R}^n$ induced by multiplication by $\omega$, are equal. Therefore, for a code $C$ over $R$, we have $\psi(C) = \nu(C)$.

**Proof.** The first statement is true because $\omega(\omega x + \omega y) = \omega(x + y) + \omega x$. The second statement follows because $\overline{\omega}(C) = C$. \qed

**Proposition 3.2.** Let $C$ be a code over $R$. If $C$ is self-orthogonal, so are $\phi(C)$ and $\psi(C)$. In this case, $C$ is a Type I (resp. Type II) code over $R$ if and only if $\phi(C)$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, and if and only if $\psi(C)$ is a Type I (resp. Type II) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of $C$ is the same as the minimum Lee weight of $\phi(C)$ and $\psi(C)$. The minimum Euclidean weight of $C$ is the same as the minimum Euclidean weight of $\phi(C)$.

**Proof.** Let $c_1 = a + b\omega + cu + du$, $c_2 = e + f\omega + gu + hu \in C$ be two codewords, with $a, b, c, d, e, f, g, h \in \mathbb{F}_2^n$. Note that, with $\cdot$ denoting the Euclidean inner product on $\mathbb{F}_2^n$,

$$(c_1, c_2) = (a \cdot e + b \cdot f) + u(a \cdot g + b \cdot h + c \cdot e + d \cdot f) + (b \cdot e + a \cdot f + b \cdot f) + \omega(a \cdot b + b \cdot c + b \cdot d + a \cdot f) + \omega(b \cdot e + a \cdot f + b \cdot f) + \omega(b \cdot f + b \cdot h + d \cdot f + b \cdot e) + \omega(b \cdot g + d \cdot e + a \cdot f + a \cdot h + c \cdot f),$$

and

$$(\phi(c_1), \phi(c_2)) = (b \cdot f + a \cdot f + b \cdot e) + u(d \cdot f + c \cdot f + d \cdot e + b \cdot h + b \cdot g + a \cdot h).$$

(We have abused notation by using $(\cdot, \cdot)$ to denote different inner products, but no confusion should arise as a result.)

It is easy to check that $(c_1, c_2) = 0$ implies $(\phi(c_1), \phi(c_2)) = 0$ and $(\psi(c_1), \psi(c_2)) = 0$. Since $\phi$ and $\psi$ are both isometries, the last two statements follow. \qed

**Corollary 3.3.** There is a Type II code of length $n$ over $R$ if and only if $n$ is even.

**Proof.** It is known that if a Type II code of length $m$ over $\mathbb{F}_4$ (or $\mathbb{F}_2 + u\mathbb{F}_2$) exists, then $m \equiv 0 \pmod{4}$ (cf. [6, Corollary 3.2] and [5, Corollary 3.2]). Thus, if a Type II code of length $n$ over $R$ exists, then $n$ must be even. The code with the generator matrix $(1 1 + ou)$ is Type II of length 2. By taking direct sums of this code, it is possible to construct Type II codes over $R$ of any even length $n$. \qed

**Corollary 3.4.** Let $d_L(II, n)$ and $d_L(I, n)$ be the highest minimum Lee weights of a Type II and a Type I code, respectively, of length $n$ over $R$. Then

$$d_L(II, n) \leq \begin{cases} \left\lfloor \frac{n}{6} \right\rfloor + 4, \\ 4 \left\lfloor \frac{n}{12} \right\rfloor + 4 \quad \text{if } n \not\equiv 11 \pmod{12} \\ 4 \left\lfloor \frac{n}{12} \right\rfloor + 6 \quad \text{otherwise}. \end{cases}$$

$$d_L(I, n) \leq \begin{cases} 4 \left\lfloor \frac{n}{12} \right\rfloor + 4, \\ 4 \left\lfloor \frac{n}{12} \right\rfloor + 6 \quad \text{if } n \not\equiv 11 \pmod{12} \\ 4 \left\lfloor \frac{n}{12} \right\rfloor + 6 \quad \text{otherwise}. \end{cases}$$
PROOF. The Gray maps $\phi$ and $\psi$ are isometries. The upper bounds on the Lee weight of a Type II (resp. Type I) code over $F_4$ and $F_2 + uF_2$ are given in [6, Corollary 3.3] and [5, Corollary 3.3].

LEMMA 3.5. Let $C$ and $C'$ be equivalent self-dual codes over $R$. Then $\phi(C)$ and $\phi(C')$ are equivalent over $F_4$, and $\psi(C)$ and $\psi(C')$ are equivalent over $F_2 + uF_2$.

PROOF. These assertions follow from the definition of the Gray maps $\phi$ and $\psi$.

PROPOSITION 3.6. If $C$ is a self-dual code over $R$, then $C$ contains the all-$u$ vector.

PROOF. The Gray image $\psi(C)$ is also self-dual, so by [5, Proposition 3.5] contains the all-$u$ vector. The assertion of the proposition then follows from the definition of $\psi$.

Let $\sigma : F_2^{4n} \to F_2^{4n}$ be the automorphism defined by
\[
(x_1, \ldots, x_{4n+1}, \ldots, x_{2n}, x_{2n+1}, \ldots, x_{3n}, x_{3n+1}, \ldots, x_{4n}) \\
\mapsto (x_1, \ldots, x_{4n}, x_{2n+1}, \ldots, x_{3n}, x_{n+1}, \ldots, x_{2n}, x_{3n+1}, \ldots, x_{4n}).
\]

PROPOSITION 3.7. There is a commutative diagram
\[
\begin{array}{ccc}
R^n & \xrightarrow{\psi} & (F_2 + uF_2)^{2n} \\
\phi & \downarrow & \sigma \circ \phi' \\
F_4^{2n} & \xrightarrow{\psi'} & F_2^{4n}.
\end{array}
\]

PROOF. Let $a + b\omega + cu + d\omega u \in F_4^n$, where $a, b, c, d \in F_2^n$. From the definitions of the Gray maps, it is easy to verify that
\[
\phi' \circ \psi(a + b\omega + cu + d\omega u) = (c + d, a + b + c + d, a + c) \in F_2^{4n}
\]
and
\[
\psi' \circ \phi(a + b\omega + cu + d\omega u) = (c + d, a + b + c + d, c, a + c) \in F_2^{4n}.
\]
Proposition 3.7 then follows immediately.

PROPOSITION 3.8. Let $C'$ be a binary code of length $4n$. If there exist a code $C_1$ over $F_4$ and a code $C_2$ over $F_2 + uF_2$, both of length $2n$, such that $\psi'(C_1) = \sigma \circ \phi'(C_2) = C'$, then there exists a code $C$ over $R$, of length $n$, such that $\phi(C) = C_1$ and $\psi(C) = C_2$.

PROOF. By Proposition 3.7, since all the Gray maps defined are bijections, we may define $C = \phi^{-1}(C_1) = \psi^{-1}(C_2)$. We need to show that $C$ is an $R$-submodule of $R^n$.

By the linearity of the Gray maps, it follows that $C$ is an additive code over $R$. It therefore remains to show that $C$ is closed under scalar multiplication (by elements of $R$).

Suppose that $v = a + b\omega + cu + d\omega u \in C$, where $a, b, c, d \in F_2^n$. Therefore,
\[
\phi(v) = (c + d\omega, (a + c) + (b + d)\omega) \in \phi(C) = C_1,
\]
and
\[
\psi(v) = ((a + b) + (c + d)u, a + cu) \in \psi(C) = C_2.
\]
Since $C_2$ is a code over $F_2 + uF_2$, it follows from (2) that
\[
u\psi(v) = ((a + b)u, au) \in C_2,
\]

(3)
and
\[ \sigma \circ \phi'((a + b)u, au) = (a + b, a + b, a, a) \in C'. \] (4)

Let \( \lambda = x + y\omega + z\mu + s\omega\mu \) be an element of \( R \), where \( x, y, z, s \in F_2 \). Then
\[ \lambda \nu = (xa + yb) + \omega(xb + ya + yb) + u(za + sb + xc + yd) + \omega u(zb + sa + sb + xd + yc + yd). \]

We need to show that \( \lambda \nu \in C \). We do so by demonstrating that \( \phi(\lambda \nu) \in \phi(C) = C_1 \). One checks readily that
\[ \phi(\lambda \nu) = (x + y\omega)(c + d\omega, (a + c) + (b + d)\omega) + (z + s\omega)(a + b\omega, a + b\omega). \]

By (1), to show that \( \phi(\lambda \nu) \in C_1 \), it suffices to show that \( (a + b\omega, a + b\omega) \in C_1 \).

Note that
\[ \psi'((a + b\omega, a + b\omega)) = (a + b, a + b, a, a), \]
which is in \( C' \) by (4). Hence \( (a + b\omega, a + b\omega) \in C_1 \).

This completes the proof of Proposition 3.8. \( \square \)

3.2. Weights of codewords in self-orthogonal codes. Let \( C \) be a self-orthogonal code over \( R \). For a codeword \( c \in C \), let \( n_0(c) \) denote the number of coordinates of \( c \) that are equal to 0, \( n_u(c) \) the number of coordinates equal to \( u \), \( n_\omega(c) \) the number of coordinates equal to \( \omega u \) or \( \overline{\omega u} \), \( n_1(c) \) the number of coordinates equal to 1, \( 1 + u \), \( 1 + \omega u \) or \( 1 + \overline{\omega u} \), \( n_\omega(c) \) the number of coordinates equal to \( \omega \), \( \omega + u \), \( \omega + \omega u \) or \( \omega + \overline{\omega u} \), and \( n_{\overline{\omega}}(c) \) the number of coordinates equal to \( \overline{\omega} \), \( \overline{\omega} + u \), \( \overline{\omega} + \omega u \) or \( \overline{\omega} + \overline{\omega u} \).

Self-orthogonality of \( C \) implies that \( (c, c) = 0 \), which implies that \( n_1(c) + n_\omega(c)\overline{\omega} + n_{\overline{\omega}}(c) = 0 \in F_4 \). Hence
\[ n_1(c) \equiv n_\omega(c) \equiv n_{\overline{\omega}}(c) \mod 2. \]

The Lee weight of \( c \) is
\[ w_L(c) = 4n_u(c) + 2n_\omega(c) + 2n_1(c) + n_\omega(c) + n_{\overline{\omega}}(c) + 2x \in 2Z, \]
for some integer \( x \). This proves the following lemma.

**Lemma 3.9.** If \( C \) is a self-orthogonal code over \( R \), then the Lee weight of every codeword is even.

**Proposition 3.10.** If \( C \) is a self-orthogonal code over \( R \) and if \( c, c' \) are two codewords of \( C \) such that \( w_L(c) \equiv w_L(c') \equiv 0 \mod 4 \), then \( w_L(c + c') \equiv 0 \mod 4 \).

**Proof.** The statement of the proposition is true when \( C \) is a self-orthogonal code over \( F_2 + uF_2 \) [5, Proposition 4.3]. (Though [5, Proposition 4.3] is stated only for a self-dual code \( C \), a careful reading of the proof reveals that the result holds true for a self-orthogonal code.) Proposition 3.10 is then true because of the isometric Gray map \( \psi \). \( \square \)

3.3. Lattices.

3.3.1. Lattices and norms. In this section, we consider the rings \( Z[i], Z[\tau] \) and \( Z[\tau, i] \) and the notion of norms in them.

For an element \( A + iB \) in the ring of Gaussian integers \( Z[i] \), we define its norm \( N_i(A + iB) \) to be
\[ N_i(A + iB) = A^2 + B^2. \]
For an element $A + \tau B$ in $\mathcal{Z}[\tau]$, we take the norm to be the one defined in [6, Section 2], namely

$$N_\tau(A + \tau B) = A^2 + B^2.$$ 

We define three norms on the ring $\mathcal{Z}[\tau, i]$. Let $q = A + iB + \tau C + i\tau D$ be an element of $\mathcal{Z}[\tau, i]$. We define

$$N_0(q) = (A + C)^2 + (B + D)^2 + C^2 + D^2,$$

$$N_1(q) = A^2 + B^2 + C^2 + D^2,$$

$$N_2(q) = (C - A)^2 + (D - B)^2 + A^2 + B^2.$$ 

The norm $N_0$ is known as Tits’s norm, arising by considering the icosians [4, p. 208]. The following lemma relating the three norms is readily verified, so we omit the proof.

**Lemma 3.11.** The norms $N_0$, $N_1$ and $N_2$ on $\mathcal{Z}[\tau, i]$ satisfy the following equalities:

$$N_2(q) = N_1(q), \quad N_1(q) = N_0(q),$$

where $q$ is an element of $\mathcal{Z}[\tau, i]$.

For any positive integer $n$, we define the projection $p : \mathcal{Z}[\tau, i]^n \rightarrow \mathcal{Z}[\tau]^{2n}$ to be the map $x + iy \mapsto (y, x)$, where $x, y \in \mathcal{Z}[\tau]^n$. When $\mathcal{Z}[\tau, i]^n$ is equipped with the norm $N_1$ and $\mathcal{Z}[\tau]^{2n}$ is equipped with the norm $N_\tau$, $p$ is an isometry.

We also define two projections $p_1, p_2 : \mathcal{Z}[\tau, i]^n \rightarrow \mathcal{Z}[i]^{2n}$ by the following rules:

$$p_1 : x + iy \mapsto (y - x, x),$$

$$p_2 : x + iy \mapsto (y, x + y),$$

where $x, y \in \mathcal{Z}[i]^n$. When $\mathcal{Z}[\tau, i]^n$ is equipped with $N_2$ and $\mathcal{Z}[i]^{2n}$ is equipped with $N_i$, the projection $p_1$ is an isometry. When $\mathcal{Z}[\tau, i]^n$ is equipped with $N_0$ and $\mathcal{Z}[i]^{2n}$ is equipped with $N_i$, the projection $p_2$ is again an isometry.

**3.3.2. Construction A.** With every code $C$ over $R$, we attach the lattice

$$A(C) = L(C)/\sqrt{2},$$

where we have set

$$L(C) := \{x \in \mathcal{Z}[\tau, i]^n \mid x \text{ mod } 2 \in C\}.$$ 

This is the analogue of the well-known Construction A for binary linear codes [4] as well as the Constructions A in [5] for codes over $\mathbf{F}_2 + u\mathbf{F}_2$ (which we shall call $A_u$) and [6] for codes over $\mathbf{F}_4$ equipped with the Euclidean inner product (which we call $A_2$). To be self-contained, recall that, if $C$ is a code over $\mathbf{F}_2 + u\mathbf{F}_2$, then

$$\sqrt{2}A_u(C) = C + 2\mathcal{Z}[i]^n,$$

and, if $C$ is an $\mathbf{F}_4$-code equipped with the Euclidean inner product, then

$$\sqrt{2}A_2(C) = C + 2\mathcal{Z}[\tau]^n.$$ 

**Proposition 3.12.** If $C$ is a Type II code over $R$, then $A(C)$ is even unimodular. If $C$ is of Type I, then $A(C)$ is unimodular.
PROOF. The statements follow from Lemma 3.9 and the observation that, for \( c \in C \) and \( z \in \mathbb{Z}[\tau, i]^n \), we have

\[
\left< \frac{1}{\sqrt{2}}(c + 2z), \frac{1}{\sqrt{2}}(c + 2z) \right> = \frac{1}{2}((c, c) + 4(c, z) + 4(z, z)),
\]

which belongs to \( \mathbb{Z} \) if \( C \) is self-dual, and belongs to \( 2\mathbb{Z} \) if \( C \) is of Type II. \( \square \)

The Construction A defined on codes over \( R \) is related to the Constructions \( A_u \) and \( A_2 \). Our earlier observations that \( \omega \) is the image of \( \tau \) under reduction mod 2 and \( u \) is the residue class of \( 1 + i \) in the quotient \( \mathbb{Z}[i]/(2) \) are useful in the proofs of the following propositions.

**Proposition 3.13.** There is a commutative diagram

\[
\begin{array}{ccc}
R^n & \xrightarrow{\phi} & F_4^{2n} \\
A \downarrow & & \downarrow A_2 \\
\mathbb{Z}[\tau, i]^n & \xrightarrow{p} & \mathbb{Z}[\tau]^{2n},
\end{array}
\]

where \( \mathbb{Z}[\tau, i]^n \) is equipped with the norm \( N_1 \).

**Proof.** Let \( v = (\omega a + \bar{\omega} b) + u(\omega c + \bar{\omega} d) \) be an element of \( R^n \), where \( a, b, c, d \in F_2^n \). Then

\[
A_2(\phi(v)) = (\tau c + \bar{\tau} d, \tau(a + c) + \bar{\tau}(b + d)) + 2\mathbb{Z}[\tau]^{2n},
\]

and

\[
p(A(v)) = (d + \tau(c - d), (b + d) + \tau(a - b + c - d)) + 2\mathbb{Z}[\tau]^{2n}.
\] \( \square \)

**Proposition 3.14.** There is a commutative diagram

\[
\begin{array}{ccc}
R^n & \xrightarrow{\psi} & (F_2 + uF_2)^{2n} \\
A \downarrow & & \downarrow A_u \\
\mathbb{Z}[\tau, i]^n & \xrightarrow{p_1} & \mathbb{Z}[i]^{2n},
\end{array}
\]

where \( \mathbb{Z}[\tau, i]^n \) is equipped with the norm \( N_2 \).

**Proof.** Let \( v = (\omega a + \bar{\omega} b) + u(\omega c + \bar{\omega} d) \) be an element of \( R^n \), where \( a, b, c, d \in F_2^n \). Then

\[
A_u(\psi(v)) = (a + (1 + i)c, b + (1 + i)d) + 2\mathbb{Z}[i]^{2n},
\]

and

\[
p_1(A(v)) = ((a + c) - 2b - 2d) + i(c - 2d), (b + d) + i d) + 2\mathbb{Z}[i]^{2n}
\]

\[= ((a + c) + ic, (b + d) + id) + 2\mathbb{Z}[i]^{2n}.\] \( \square \)

**Proposition 3.15.** There is a commutative diagram

\[
\begin{array}{ccc}
R^n & \xrightarrow{v} & (F_2 + uF_2)^{2n} \\
A \downarrow & & \downarrow A_u \\
\mathbb{Z}[\tau, i]^n & \xrightarrow{p_2} & \mathbb{Z}[i]^{2n},
\end{array}
\]

where \( \mathbb{Z}[\tau, i]^n \) is equipped with the norm \( N_0 \).
PROOF. Let \( v = (\omega a + \overline{\omega} b) + u(\omega c + \overline{\omega} d) \) be an element of \( R^n \), where \( a, b, c, d \in \mathbb{F}_2^n \). Then
\[
A_2(v(v)) = ((a + b) + (1 + i)(c + d), a + (1 + i)c) + 2Z[i]^{2n},
\]
and
\[
p_2(A(v)) = ((a - b + c - d) + i(c - d), (a + c) + i(c + d)) + 2Z[i]^{2n}
= ((a + b + c + d) + i(c + d), (a + c) + i(c + d)) + 2Z[i]^{2n}. \quad \square
\]

REMARK. Proposition 3.15 may also be proved by the following alternative method: from Lemma 3.1, we have \( v = \psi \circ \overline{\psi} \). Multiplication by \( \overline{\omega} \) on \( R^n \) induces the map \( p' \) on \( \mathbb{Z}[\tau, i]^{2n} \) defined by
\[
p' : x + \tau y \mapsto (x + y) + \tau x.
\]
Proposition 3.15 then follows from Proposition 3.14 and by observing that
\[
p_2(x + \tau y) = p_1 \circ p'(x + \tau y) + 2(y, 0).
\]

4. EXAMPLES

Let \( x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_4^n \) be two vectors. For \( a, b \in \mathbb{F}_4 \), let
\[
n_{a,b} = |\{ j | 1 \leq j \leq n, x_j = a \text{ and } y_j = b \}|.
\]
Let \( x * y \) be the vector \((x_1y_1, x_2y_2, \ldots, x_ny_n) \in \mathbb{F}_4^n \). The following lemma is easy, though somewhat tedious, to verify.

**Lemma 4.1.** For \( x, y \in \mathbb{F}_4^n \), we have
\[
w_L(x + y) = w_L(x) + w_L(y) - 2w_L(x * y) + 4(n_{a,b} + n_{\overline{a},\overline{b}}).
\]

Since the Gray map \( \phi \) is an isometry, using the observation \( w_L(x + uy) = w_L(y) + w_L(x + y) \), where \( x, y \in \mathbb{F}_4^n \), together with Lemma 4.1, we obtain

**Lemma 4.2.** For \( x, y \in \mathbb{F}_4^n \), we have
\[
w_L(x + uy) = w_L(x) + 2w_L(y) - 2w_L(x * y) + 4(n_{a,b} + n_{\overline{a},\overline{b}}).
\]

**Proposition 4.3.** Let \( C \) be a self-orthogonal code over \( \mathbb{F}_4 \) with respect to the Euclidean inner product. Suppose that \( C \) contains the all-one vector and the Lee weights of all the codewords of \( C \) are multiples of 4. Then \( C + uC^\perp \) is a self-dual Type II code over \( R \).

**Proof.** Since \( C \) is self-orthogonal, it follows that \( C + uC^\perp \) is also self-orthogonal. By considering cardinality, we see that \( C + uC^\perp \) is self-dual over \( R \).

The typical codeword in \( C + uC^\perp \) has the form \( x + uy \), where \( x \in C \) and \( y \in C^\perp \). The weight of this codeword can be determined using Lemma 4.2.

By assumption, \( w_L(x) \) is a multiple of 4.

For \( y \in C^\perp \), let \( n_1(y) \) (resp. \( n_{\omega y}(y) \) and \( n_{\overline{\omega} y}(y) \)) denote the number of coordinates of \( y \) that are equal to 1 (resp. \( \omega \) and \( \overline{\omega} \)). Since \( C \) contains the all-one vector \( 1 \), the inner product \( (y, 1) \) yields the condition
\[
n_1(y) + \omega n_{\omega y}(y) + \overline{\omega} n_{\overline{\omega} y}(y) = 0 \in \mathbb{F}_4.
\]
This implies that

\[ n_1(y) \equiv n_\omega(y) \equiv n_{\overline{\omega}}(y) \mod 2. \]

Therefore,

\[ w_L(y) = 2n_1(y) + n_\omega(y) + n_{\overline{\omega}}(y) \in 2\mathbb{Z}. \]

Since \((x, y) = 0\), we obtain

\[ (n_{1,1} + n_{\omega, \omega} + n_{\overline{\omega}, \omega}) + (n_{1,\omega} + n_{\omega, 1} + n_{\overline{\omega}, \omega})\omega + (n_{1, \overline{\omega}} + n_{\omega, \omega} + n_{\overline{\omega}, 1})\overline{\omega} = 0 \in F_4, \]

i.e.,

\[ n_1(x \ast y) + n_\omega(x \ast y)\omega + n_{\overline{\omega}}(x \ast y)\overline{\omega} = 0 \in F_4, \]

which implies that \(w_L(x \ast y) \in 2\mathbb{Z}\).

Hence, by Lemma 4.2, \(w_L(x + uy)\) is a multiple of 4. Therefore, \(C + uC^\perp\) is a Type II code over \(R\).

\[ \square \]

**Corollary 4.4.** If \(C\) is a Type II code over \(F_4\) with respect to the Euclidean inner product, then \(C + uC\) is of Type II over \(R\) and \(\phi(C + uC) = C \bigoplus C\).

**Proof.** Since \(C\) is self-orthogonal, we have that, for all \(x \in C\), \((x, x) = 0\), hence

\[ 1 \in C^\perp = C. \]

By Proposition 4.3, the result follows. \[ \square \]

For every even integer \(n\), let \(R_n\) be the repetition code over \(F_4\) and \(P_n\) its dual the parity-check code. The code \(K_n := R_n + uP_n\) is a self-dual code. When \(n\) is a multiple of 4, \(K_n\) is of Type II.

Next we apply Proposition 4.3 to construct Type II codes over \(R\), starting from the generalized Reed–Muller codes over \(F_4\). Let \(m \geq 2\) be an integer and let \(r \leq \lfloor \frac{3m-1}{2} \rfloor\) be another integer. Denote by \(RM_4(r, m)\) the generalized Reed–Muller code over \(F_4\) of order \(r\) and length \(4^m\). Let \(C_{m,r} := RM_4(r, m) + uRM_4(3m - 1 - r, m)\).

**Corollary 4.5.** For \(m \geq 2\) and \(r \leq \lfloor \frac{3m-1}{2} \rfloor\), the code \(C_{m,r}\) is a Type II code over \(R\).

**Proof.** It suffices to prove that, for \(m\) and \(r\) as given, the generalized Reed–Muller code \(RM_4(r, m)\) over \(F_4\) is self-orthogonal, contains the all-one vector and all its codewords have Lee weights divisible by 4.

Let \(a_1, \ldots, a_{4^m}\) be all the \(m\)-tuples in \(F_4^m\). Let \(x_1, \ldots, x_m\) be \(m\) variables. Let \(V\) be the \(F_4\)-vector space spanned by the monomials \(x_1^{i_1} \cdots x_m^{i_m}\), with \(0 \leq i_k \leq 3\) and \(\sum i_k \leq r\), for \(1 \leq k \leq m\). Then the generalized Reed–Muller code \(RM_4(r, m)\) is defined to be

\[ RM_4(r, m) := \langle (f(a_1), \ldots, f(a_{4^m})) \mid f \in V \rangle. \]

It is well known that, for \(r_1 \leq r_2\), we have \(RM_4(r_1, m) \subseteq RM_4(r_2, m)\) and, for any \(r\), \(RM_4(r, m)^\perp = RM_4(3m - 1 - r, m)\).

Therefore, \(RM_4(r, m)\) is self-orthogonal for the given \(m\) and \(r\). It also contains the all-one vector because \(RM_4(0, m)\) is contained in \(RM_4(r, m)\).

It remains to see that all the codewords in \(RM_4(r, m)\) have Lee weights divisible by 4. We show this in three steps.
Step (I): When \( f \) is a monomial of the form \( x_1^{i_1} \cdots x_m^{i_m} \).

If \( i_1 = \cdots = i_m = 0 \), then the word defined by \( f \) is the all-one vector, whose Lee weight is \( 2 \cdot 4^m \).

Otherwise, we may suppose that \( z \) of the values \( i_1, \ldots, i_m \) are 0 and \( m - z \) of them are positive. Note also that, among the \( m \)-tuples \( a_1, \ldots, a_{4^m} \), each element of \( F_4 \) occurs exactly \( 4^{m-1} \) times in each coordinate.

To determine the number of coordinates in the word \( f(a_1), \ldots, f(a_{4^m}) \) that are equal to 1 (resp. \( \omega \) and \( \overline{\omega} \)), it suffices to determine the number of \( i \) such that \( f(a_i) = 1 \) (resp. \( \omega \) and \( \overline{\omega} \)). If there exists an \( i_k \) equal to 1 or 2, then it is easy to see that this number is \( 4^z \cdot 3^{m-1-z} \).

Therefore, the Lee weight of the codeword defined by \( f \) is \( 4 \cdot 4^z \cdot 3^{m-1-z} \), which is divisible by 4. If all the \( i_k \) are equal to 0 or 3, then the number of \( i \) such that \( f(a_i) = 1 \) is \( 4^z \cdot 3^m \) and there are no \( i \) such that \( f(a_i) = \omega \) or \( \overline{\omega} \). Hence the Lee weight of the codeword defined by \( f \) is \( 2 \cdot 4^z \cdot 3^{m-z} \). Since \( z > 0 \) in this case (for otherwise \( r \geq 5m \)), the Lee weight is divisible by 4.

Step (II): When \( f \) is of the form \( \lambda x_1^{i_1} \cdots x_m^{i_m} \), where \( \lambda \in F_4 \).

If \( \lambda = 0 \), then the codeword is the zero codeword. Otherwise, the analysis is similar to the case in Step (I).

Step (III): General \( f \in V \).

For \( x, y \in RM_4(r, m) \), the argument in the proof of Proposition 4.3 shows that \( w_L(x \ast y) \in 2Z \), since \( RM_4(r, m) \) is self-orthogonal for the given \( m \) and \( r \).

Lemma 4.1 then implies that

\[
w_L(x + y) = w_L(x) + w_L(y) \mod 4.
\]

By Steps (I) and (II), an inductive argument now completes the proof that the Lee weights of all the codewords of \( RM_4(r, m) \) are divisible by 4.

\( \square \)

REMARKS.

(1) When \( r \leq \lceil \frac{m-1}{2} \rceil \), the proof of the classical McEliece theorem in [9] can be modified (by changing the 0 in the equations to any of 0, 1, \( \omega \) and \( \overline{\omega} \)) to yield the following generalization of the McEliece theorem for Lee weights: When \( r \leq \lceil \frac{m-1}{2} \rceil \), the Lee weights of all the words in \( RM_4(r, m) \) are divisible by \( 4^{m/r-1} \).

(2) When \( m \leq r \leq \lceil \frac{3m-1}{2} \rceil \), by considering the word defined by \( f = x_1 \cdots x_m \), it can be shown that there exists a word in \( RM_4(r, m) \) whose Lee weight is exactly divisible by 4.

(3) When \( r = 0 \), note that \( C_{m,r} = K_{2^m} \).

The next example is a class of double circulant self-dual codes. Let \( D_{2m} \) be a code of length \( 2m \) with generator matrix of the form \((I, uJ + (1 + u)I)\), where \( J \) is the \( m \times m \) all-one matrix.

PROPOSITION 4.6. For \( m > 1 \), the \( R \)-code \( D_{2m} \) is a self-dual code of length \( 2m \) with minimum Lee weight 4 and minimum Hamming weight 2. When \( m \) is even, \( D_{2m} \) is a Type II \( R \)-code.

PROOF. The self-orthogonality of the code follows immediately from the form of the generator matrix. Self-duality follows from the self-orthogonality and the cardinality. It is not difficult to see that the minimum Lee weight is 4 and the minimum Hamming weight is 2, in both cases given by \( u \) times a row of the generator matrix.

To see that \( D_{2m} \) is Type II when \( m \) is even, we first note that any scalar multiple of any row in the generator matrix has Lee weight divisible by 4 and then proceed with an inductive argument using Proposition 3.10. \( \square \)
We next give a characterization of Euclidean codes over $\mathbb{F}_4$ that are Gray images of codes over $R$. For an arbitrary splitting of the coordinate positions (for vectors in $\mathbb{F}_4^{2n}$) into two equal parts, we define the swap map $s$ as $s((x|y)) = (y|x)$. A swap map shall be said to be attached to a Gray map (from $R^n$ to $\mathbb{F}_4^{2n}$) if they both correspond to the same partition of coordinate places.

**Theorem 4.7.** Fix a Gray map from $R^n$ to $\mathbb{F}_4^{2n}$. A Euclidean code $C$ over $\mathbb{F}_4$ of length $2n$ is the image of an $R$-code of length $n$ by that Gray map if and only if it is left wholly invariant by the swap map attached to that Gray map. More generally, $C$ is the image of some $R$-code by some Gray map if and only if it admits a fixed-point free involution in its automorphism group.

**Proof.** The condition is a necessary one because the $R$-code has to be left invariant by the map $c \mapsto (1 + u)c$ and $\phi((1 + u)(x + uy)) = s((x|y))$.

It is also sufficient since being left invariant by $s$ and hence by $1 + s$ is equivalent for an $\mathbb{F}_4$-code to be an $\mathbb{F}_4[u]$-module.

The second assertion follows directly from the first. □

**Corollary 4.8.** For a given Gray map $\phi : R^n \rightarrow \mathbb{F}_4^{2n}$, the Euclidean code $C$ over $\mathbb{F}_4$ is the Gray image of a self-dual code over $R$ if and only if $C$ is a self-dual code and invariant by the swap map attached to $\phi$. More generally, the self-dual code $C$ is the image of some self-dual $R$-code by some Gray map if and only if it admits a fixed-point free involution in its automorphism group.

**Proof.** The necessity follows from Proposition 3.2 and Theorem 4.7.

For the sufficiency, Theorem 4.7 already shows that $C$ is the Gray image of an $R$-code. It suffices to show that this code over $R$ is self-orthogonal, as self-duality then follows by considering its cardinality. Consider a pair of vectors $z = x + uy$ and $z' = x' + uy'$ in this $R$-code. We need to show that $\langle z, z' \rangle = \langle x, x' \rangle + u(\langle x, y' \rangle + \langle x', y \rangle) = 0$.

Since $\phi(z), \phi(uz') \in C$, we have

$$\langle \phi(z), \phi(uz') \rangle = \langle x, x' \rangle = 0. \tag{5}$$

Since $\phi(z), \phi(z') \in C$, we have

$$\langle \phi(z), \phi(z') \rangle = \langle x, x' \rangle + \langle x', y \rangle + \langle x, y' \rangle = 0. \tag{6}$$

Combining (5) and (6), we obtain

$$\langle x', y \rangle + \langle x, y' \rangle = 0. \tag{7}$$

It follows from (5) and (7) that $\langle z, z' \rangle = 0$. This completes the proof of the first statement of the corollary.

The second statement follows directly from the first. □

5. **Examples of Type II Codes**

We now give some more examples of Type II codes over $R$ ranked by increasing lengths.

5.1. $n = 2$. There is a unique Type II code $C_2$. The lattice obtained by Construction A is $E_8$, the unique Type II lattice in dimension 8.
5.2. \( n = 4 \). There is a decomposable code \( C_2 \oplus C_2 \), and at least one indecomposable code obtained by extension of scalars from \( \mathbf{F}_2 + u\mathbf{F}_2 \) to \( \mathbf{F}_4 + u\mathbf{F}_4 \).

5.3. \( n = 6 \). In [2], a unique extremal Type II Euclidean code \( \mathbf{C}_{12,7} \) of length 12 over \( \mathbf{F}_4 \) was found. The binary Gray image of \( \mathbf{C}_{12,7} \) is the Golay code. A generator matrix for \( \mathbf{C}_{12,7} \) is

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & \omega & \omega & \bar{\omega} & \bar{\omega} & 1 \\
0 & 1 & 0 & 0 & 0 & \omega & 0 & \bar{\omega} & \omega & 1 & \bar{\omega} \\
0 & 0 & 1 & 0 & 0 & \omega & \bar{\omega} & \bar{\omega} & 0 & \omega & 1 \\
0 & 0 & 0 & 1 & 0 & \bar{\omega} & \omega & 0 & \bar{\omega} & 1 & \omega \\
0 & 0 & 0 & 0 & 1 & 1 & \bar{\omega} & 1 & \omega & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & \bar{\omega} & 1 & \omega & 1 & 1
\end{pmatrix}
\]

We denote the \( i \)th row of this matrix by \( \mathbf{r}_i \). We partition the coordinates of \( \mathbf{F}_4^{12} \) into two parts, one consisting of the first six coordinates and the other consisting of the last six coordinates, and denote by \( s \) the swap map. Let \( \phi \) be the Gray map corresponding to this swap map. It is easy to show that \( \{ \mathbf{r}_i \mid 1 \leq i \leq 6 \} \) and \( \{ \mathbf{r}_i \mid 1 \leq i \leq 3 \} \cup \{ s(\mathbf{r}_i) \mid 1 \leq i \leq 3 \} \) have the same \( \mathbf{F}_4 \)-span. Hence, it follows that \( \mathbf{C}_{12,7} \) and \( \{ \mathbf{r}_i \mid 1 \leq i \leq 3 \} \cup \{ s(\mathbf{r}_i) \mid 1 \leq i \leq 3 \} \) have the same \( \mathbf{F}_4 \)-span. Hence, by Corollary 4.8, its preimage \( \phi^{-1}(\mathbf{C}_{12,7}) \) is an extremal Type II \( R \)-code of length 6, whose binary Gray image is the Golay code. It has a generator matrix of the form

\[
\begin{pmatrix}
1 + u & \omega & \omega & \bar{\omega} & \bar{\omega} & 1 \\
\omega & 1 + u & \omega & \bar{\omega} & \omega & 1 & \bar{\omega} \\
\omega & \bar{\omega} & \omega + u & 0 & \omega & 1 & \bar{\omega}
\end{pmatrix}
\]

The attached lattice is therefore the Niemeier lattice \( A_4^{24} \).

5.4. \( n = 8 \). In [2], all distinct extremal double circulant Type II codes of length 16 over \( \mathbf{F}_4 \) were also enumerated. There are four such codes up to permutation equivalence. In the notation of [2], they are called \( P_1, P_3, B_1 \) and \( B_7 \). Using Corollary 4.8, we will show that they are all Gray images of some Type II extremal \( R \)-codes.

For the two pure double circulant codes \( P_1 \) and \( P_3 \) of length 16, observe that the automorphism group of each code contains an element \( \tau = (1, 2, \ldots, 8) (9, 10, \ldots, 16) \) and \( \tau^4 \) is a fixed-point free involution. Hence, by Corollary 4.8, the preimages \( \phi^{-1}(P_1) \) and \( \phi^{-1}(P_3) \) are extremal Type II \( R \)-codes of length 8, whose binary Gray images are \( C_{83} \) and \( C_{85} \) respectively in the notations of [3].

As for the bordered double circulant codes, it is straightforward, though somewhat tedious, to check that the automorphism group of a double circulant code of length 16 over \( \mathbf{F}_4 \) admits a fixed-point free involution

\[
\]

Hence, again by Corollary 4.8, the preimages \( \phi^{-1}(B_1) \) and \( \phi^{-1}(B_7) \) are extremal Type II \( R \)-codes of length 8, whose binary Gray images are \( C_{84} \) and \( C_{83} \) respectively.

Since \( P_1, P_3, B_1 \) and \( B_7 \) are not permutation equivalent over \( \mathbf{F}_4 \), their preimages in \( R^8 \) are also not permutation equivalent.

To sum up, the three extremal Type II codes \( C_{83}, C_{84}, C_{85} \) can be obtained by Gray map from \( R \)-codes. By Koch–Venkov [7], the attached lattices are non-equivalent.
6. Invariants

Since \( R \) is a quasi-Frobenius ring, the complete weight enumerator for a code over \( R \) satisfies the MacWilliams relations [10]. It can also be verified that the swe satisfies the MacWilliams relations, with the matrix

\[
\begin{array}{cccc}
1 & 4 & 6 & 4 \\
1 & 2 & 0 & -2 \\
1 & 0 & -2 & 0 \\
1 & -2 & 0 & 2 \\
1 & -4 & 6 & -4
\end{array}
\]

The Type II congruence conditions translate into invariance of the swe under the matrix

\[
\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & i & 0 & 0 \\
0 & 0 & -1 & 0 \\
0 & 0 & 0 & -i \\
0 & 0 & 0 & 1
\end{array}
\]

The matrix group generated by these two matrices is of order 48 and affords the Molien series

\[
\frac{1 + t^4 + 4t^6 + 2t^8 + t^{10} + 3t^{12}}{(1 - t^2)^2 (1 - t^4)(1 - t^6)^2}.
\]

It can be shown that the Molien series of the group of order 8 that leaves Type I codes invariant is

\[
\frac{(1 + t^3)^2}{(1 - t)(1 - t^2)^3 (1 - t^4)}.
\]

The relevant rings of invariants are too cumbersome to display.

7. Conclusion and Open Problems

We have introduced a new ring \( R \) that bears information on codes over \( \mathbb{F}_4 \) and \( \mathbb{F}_2 + u \mathbb{F}_2 \). An immediate but important open problem is the existence of a mass formula for self-dual codes over \( R \), which could lead to classification results for codes of modest length.

Acknowledgements

This work was undertaken when S. Ling visited CNRS-13S, ESSI, Sophia Antipolis, France. He would like to thank the institution for their kind hospitality. The research performed by S. Ling was partially supported by MOE-ARF research grant R-146-000-018-112.

References


SAN LING  
Department of Mathematics,  
National University of Singapore,  
Science Drive 2,  
Singapore 117543, Republic of Singapore  
E-mail: lings@math.nus.edu.sg

AND

PATRICK SOLÉ  
CNRS, 138,  
ESSI, BP 145,  
Route des Colles,  
06 903 Sophia Antipolis, France  
E-mail: ps@essi.fr