Conference Matrices and Unimodular Lattices

Robin Chapman
School of Mathematical Sciences
University of Exeter
Exeter, EX4 4QE, UK
rjc@maths.ex.ac.uk

19 July 2000

1 Introduction

We use conference matrices to define an action of the complex numbers on the real Euclidean vector space $\mathbb{R}^n$. In certain cases, the lattice $D_n^+$ becomes a module over a ring of quadratic integers. We can then obtain new unimodular lattices, essentially by multiplying the lattice $D_n^+$ by a non-principal ideal in this ring. We show that lattices constructed via quadratic residue codes, including the Leech lattice, can be constructed in this way.

Recall that a lattice $\Lambda$ is a discrete subgroup of a finite dimensional real vector space $V$. We suppose that $V$ has a given Euclidean inner product $(u, v) \mapsto u \cdot v$ and the rank of $\Lambda$ equals the dimension of $V$. In this case $\Lambda$ has a bounded fundamental region in $V$. We call the volume of such a fundamental region (measured with respect to the Euclidean structure on $V$) the volume of the lattice $\Lambda$.

The lattice $\Lambda$ is integral if $u \cdot v \in \mathbb{Z}$ for all $u, v \in \Lambda$. It is even if $|u|^2 = u \cdot u \in 2\mathbb{Z}$ for all $u \in \Lambda$. Even lattices are necessarily integral. The lattice $\Lambda$ is unimodular if $\Lambda$ is integral and has volume 1. It is well known [8, Chapter VIII, Theorem 8] that if $\Lambda$ is an even unimodular then the rank of $\Lambda$ is divisible by 8.

For convenience we call the square of the length of a vector its norm. The minimum norm of a lattice is the smallest non-zero norm of its vectors.
2 Conference matrices

Let $l$ be a positive integer. A conference matrix of order $n$ [4, Chapter 18] is an $n$-by-$n$ matrix $W$ satisfying

(a) the diagonal entries of $W$ vanish, while its off-diagonal entries lie in $\{-1, 1\}$,

(b) $WW^\top = (n - 1)I$, where $I$ denotes the $n$-by-$n$ identity matrix.

Let $W_n$ denote the set of skew-symmetric conference matrices of order $n$.

Let $W \in W_n$. Then $H = I + W$ satisfies $HH^\top = (I + W)(I - W) = I - W^2 = I + WW^\top = nI$. As all the entries of $H$ lie in $\{-1, 1\}$ then $H$ is a Hadamard matrix. Consequently [7, Theorem 18.1] $n = 1, 2$ or is a multiple of 4.

Suppose that $n$ is a multiple of 4 and let $l = n - 1$. Fix $W \in W_n$ and let $V = \mathbb{R}^n$ denote the $n$-dimensional real vector space under the standard Euclidean dot product. Then, since $W^2 = -lI$, $V$ becomes also a complex vector space when we define

$$(r + s\sqrt{-l})v = v(r + sW)$$

for $r, s \in \mathbb{R}$. Let $|v| = \sqrt{v \cdot v}$ denote the Euclidean length of a vector $v \in \mathbb{R}^n$. This action of $\mathbb{C}$ on $\mathbb{R}^n$ transforms lengths in the obvious way. Let $z^*$ denote the complex conjugate of the complex number $z$.

Lemma 2.1 (a) If $z_1, z_2 \in \mathbb{C}$ and $v_1, v_2 \in \mathbb{R}^n$ then $(z_1v_1) \cdot (z_2v_2) = (z_1\overline{z}_2)^*v_1 \cdot v_2$

(b) If $z \in \mathbb{C}$ and $v \in \mathbb{R}^n$ then $|zv| = |z||v|$.

Proof Let $z_j = r_j + s_j\sqrt{-l}$ with $r_j, s_j \in \mathbb{R}$. Then

$$(z_1v_1) \cdot (z_2v_2) = (z_1v_1)(z_2v_2)^\top$$

$= v_1(r_1I + s_1W)(r_2I + s_2W)^\top v_2^\top$

$= v(r_1I + s_1W)(r_2I - s_2W)v^\top$

$= v((r_1r_2 + ls_1s_2)I + (s_1r_2 - r_1s_2)W)v^\top$

$= (z_1\overline{z}_2v_1) \cdot v_2$

as claimed.

Consequently

$$|zv|^2 = (zv) \cdot (zv) = (zz^*v) \cdot v = |z|^2v \cdot v = |z|^2|v|^2.$$

Thus for fixed nonzero $z$, the map $v \mapsto vz$ is a similarity of $\mathbb{R}^n$ with scale factor $|z|$. 

[4]
3 Quadratic fields

We retain the previous notation. Suppose in addition that \( l = n - 1 \) is squarefree. Let \( K \) denote the quadratic field \( \mathbb{Q}(\sqrt{-l}) \). Since \( l \) is square-free, the ring of integers of \( K \) is

\[
\mathcal{O} = \mathbb{Z} \left[ \frac{1 + \sqrt{-l}}{2} \right] = \left\{ \frac{a + b\sqrt{-l}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\}.
\]

In particular \( \mathcal{O} \) is a Dedekind domain. We shall show that some of the familiar lattices in \( \mathbb{R}^{l+1} \) are modules for the ring \( \mathcal{O} \).

Let

\[
L_0 = \{ (a_1, \ldots, a_n) \in \mathbb{Z}^n : a_1 + \cdots + a_n \equiv 0 \pmod{2} \}
\]

be the \( D_n \) root lattice.

Lemma 3.1 The lattice \( L_0 \) is an \( \mathcal{O} \)-module.

Proof It suffices to show that \( \frac{1}{2}(1 + \sqrt{-l})v = \frac{1}{2}v(I + W) \in L_0 \) whenever \( v \in L_0 \). Indeed it suffices to show this whenever \( v \) lies in a generating set for \( L_0 \). Now \( L_0 \) is generated by the vectors \( 2e_j \) and \( e_j + e_k \) (for \( j \neq k \)) where \( e_j \) denotes the \( j \)-th unit vector. Firstly \( e_j(I + W) \) is a row of the Hadamard matrix \( I + W \). As it contains \( n \) instances of \( \pm 1 \) and \( n \) is even, it lies in \( L_0 \). Next \( \frac{1}{2}(e_j + e_k)(I + W) \) is the sum of two rows of the Hadamard matrix \( I + W \). Two rows of an \( n \)-by-\( n \) Hadamard matrix agree in exactly \( n/2 \) places. Hence \( \frac{1}{2}(e_j + e_k)(I + W) \) has \( n/2 \) zeros and \( n/2 \) instances of \( \pm 1 \). As \( n/2 \) is even then \( \frac{1}{2}(e_j + e_k)(I + W) \in L_0 \). This completes the proof. \( \square \)

Now consider the set

\[
S = \{(a_1, \ldots, a_n) : a_j \in \{-1/2, 1/2\}\}.
\]

The difference of two vectors in \( S \) lies in \( L_0 \) if and only if those vectors agree in an even number of places. Thus there are exactly two cosets \( v + L_0 \) as \( v \) runs through \( S \).

For each \( j \), \( \frac{1}{2}e_j(I + W) \in S \), and for each \( j \) and \( k \), \( \frac{1}{2}(e_j - e_k)(I + W) \in L_0 \) by Lemma 3.1. Thus the cosets \( \frac{1}{2}e_j(I + W) + L_0 \) are identical. Let

\[
S_+ = \{ v \in S : v - \frac{1}{2}e_1(I + W) \in L_0 \}
\]

and

\[
S_- = S \setminus S_+.
\]

As \( \frac{1}{2}e_j(I + W) - \frac{1}{2}e_j(-I + W) = e_j \notin L_0 \) then \( \frac{1}{2}e_j(-I + W) \in S_- \) for each \( j \).
If \( v \in S \) then \( 2v \) has \( n \) entries \( \pm 1 \) and so \( 2v \in L_0 \). It follows that \( L_0 \cup (v + L_0) \) is a lattice, which depends only on whether \( v \in S_+ \) or \( v \in S_- \). We write \( L_+ \) for \( L_0 \cup (v + L_0) \) when \( v \in S_+ \) and \( L_- \) for \( L_0 \cup (v + L_0) \) when \( v \in S_- \). Both \( L_+ \) and \( L_- \) are isometric to the lattice usually denoted by \( D_n^+ \) \cite[Chapter 4, §7.3]{[5]}. The lattice \( D_n^+ \) is unimodular for each \( n \) divisible by 4, and it is even unimodular whenever \( n \) is divisible by 8.

**Lemma 3.2** If \( n \) is divisible by 8 then the lattices \( L_+ \) and \( L_- \) are \( \mathcal{O} \)-modules.

**Proof** Let \( L = L_+ \) or \( L_- \). Then \( L = L_0 + (v + L_0) \) for some \( v \in S \) and by Lemma 3.1 it suffices to show that \( \frac{1}{2}(1 + \sqrt{-l})v = \frac{1}{2}v(I + W) \in L \). Note that \( \frac{1}{4}(l + 1) \) is an even integer by the hypothesis.

We may assume that \( v = \frac{1}{2}e_1(\pm I + W) \). If \( v = \frac{1}{2}e_1(I + W) \) then
\[
\frac{1}{2}v(I + W) = \frac{1}{4}e_1(I + W)^2 = \frac{1}{4}e_1((1 - l)I + 2W) = \frac{1}{2}e_1(I + W) - \frac{l + 1}{4}e_1
\]
which lies in \( L \) as \( \frac{1}{2}e_1(I + W) \in L \).

If \( v = \frac{1}{2}e_1(-I + W) \) then
\[
\frac{1}{2}v(I + W) = \frac{1}{4}e_1(-I + W)(I + W) = \frac{1}{4}e_1(-(l + 1)I)
\]
which lies in \( L \). \( \square \)

Let \( \mathcal{I} \) be an ideal of \( \mathcal{O} \). If \( M \) is a \( \mathcal{O} \)-module, then \( \mathcal{I}M \), defined as the subgroup of \( M \) generated by the \( \alpha m \) for \( \alpha \in \mathcal{I} \) and \( m \in M \), is also a \( \mathcal{O} \)-module.

**Theorem 3.1** Suppose that \( l \equiv 7 \pmod{8} \) and that \( \mathcal{I} \) is a nonzero ideal of \( \mathcal{O} \) with norm \( N = N(\mathcal{I}) \). If \( L = L_+ \) or \( L_- \) then
\[
L[\mathcal{I}] = \frac{1}{\sqrt{N}}\mathcal{I}L
\]
is an even unimodular lattice. Also if \( \mathcal{I} \) and \( \mathcal{J} \) lie in the same ideal class of \( \mathcal{O} \), the lattices \( L[\mathcal{I}] \) and \( L[\mathcal{J}] \) are isometric.

**Proof** First of all we show that the index \( |L : \mathcal{I}L| \) equals \( N^{n/2} \). As an \( \mathcal{O} \)-module, \( L \) is finitely generated. Also if \( \alpha \in \mathcal{O} \) and \( v \in L \) are nonzero, then \( |\alpha v| = |\alpha||v| \neq 0 \) by Lemma 2.1 and so \( L \) is torsion free as an \( \mathcal{O} \)-module.

By the theory of modules over Dedekind domains \cite[§9.6]{[4]}, as \( L \) is a finitely generated torsion-free module over the Dedekind domain \( \mathcal{O} \), then \( L = L_1 \oplus \cdots \oplus L_k \) where each \( L_j \) is isomorphic to a nonzero ideal \( \mathcal{A}_j \) of \( \mathcal{O} \).
Each of the $A_j$ is a free abelian group of rank 2, and as $L$ is a free abelian group of rank $n$ it follows that $k = n/2$. Then $\mathcal{IL} = \mathcal{I}L_1 \oplus \cdots \oplus \mathcal{I}L_{n/2}$ and so $|L : \mathcal{IL}| = \prod_{j=1}^{n/2} |L_j : \mathcal{IL}_j|$. But

$$|L_j : \mathcal{IL}_j| = |A_j : \mathcal{IA}_j| = \frac{|O : \mathcal{IA}_j|}{|O : A_j|} = \frac{N(\mathcal{IA}_j)}{N(A_j)}.$$  

But $N(\mathcal{IA}_j) = N(\mathcal{I})N(A_j)$ and so $|L_j : \mathcal{IL}_j| = N(\mathcal{I}) = N$. Consequently $|L : \mathcal{IL}| = N^{n/2}$ as claimed.

We now show that $L[\mathcal{I}]$ is unimodular. The lattice $\mathcal{IL}$ is generated by elements $u = \alpha v$ where $\alpha \in \mathcal{I}$ and $v \in L$. Let $u_j = \alpha_j v_j (j = 1, 2)$ with $\alpha_j \in \mathcal{I}$ and $v_j \in L$. Then by Lemma 2.1,

$$u_1 \cdot u_2 = (\alpha_1 v_1) \cdot (\alpha_2 v_2) = (\alpha_1 \alpha_2^* v_1) \cdot v_2.$$  

But $\alpha_1 \alpha_2^* \in \mathcal{II}^* = N(\mathcal{I})\mathcal{O}$ [3, §VIII.1] so that.

$$u_1 \cdot u_2 = N(\gamma v_1) \cdot v_2$$

where $\gamma \in \mathcal{O}$. As $\gamma v_1 \in L$ (by Lemma 3.2) and $L$ is an integral lattice, then $u_1 \cdot u_2 \equiv 0 \pmod{N}$. Consequently $L[\mathcal{I}] = N^{-1/2} \mathcal{IL}$ is an integral lattice. But $L$ is unimodular, so it has volume 1. Thus $\mathcal{IL}$ has volume $|L : \mathcal{IL}| = N^{n/2}$ and so $L[\mathcal{I}] = N^{-1/2} \mathcal{IL}$ has volume 1. Thus $L[\mathcal{I}]$ is a unimodular lattice.

We finally show that $L[\mathcal{I}]$ is an even unimodular lattice. Since $L[\mathcal{I}]$ is integral, to show that it is even it suffices to show that each vector $u$ in a generating set of $L[\mathcal{I}]$ has $|u|^2$ even. The vectors $u = N^{-1/2} \alpha v$ for $\alpha \in \mathcal{I}$ and $v \in L$ generate $L[\mathcal{I}]$. Then

$$|u|^2 = \frac{1}{N} |\alpha v|^2 = \frac{|\alpha|^2}{N} |v|^2.$$  

But $|\alpha|^2 = \alpha \alpha^* \in \mathcal{II}^* = N\mathcal{O}$ and so $|\alpha|^2/N \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$ and $|v|^2$ is an even integer, as $v \in L$, an even lattice. Thus $|u|^2$ is an even integer. Thus $L[\mathcal{I}]$ is an even unimodular lattice.

Now suppose that $\mathcal{I}$ and $\mathcal{J}$ lie in the same ideal class of $\mathcal{O}$. Then $\mathcal{J} = \alpha \mathcal{I}$ where $\alpha$ is a nonzero element of $K$. Then $\mathcal{J}L = \alpha \mathcal{J}_L$ and so

$$L[\mathcal{J}] = \frac{1}{\sqrt{N(\mathcal{J})}} \mathcal{J}L = \frac{1}{\sqrt{N(\mathcal{J})}} \alpha \mathcal{IL} = \sqrt{\frac{N(\mathcal{I})}{N(\mathcal{J})}} \alpha L[\mathcal{I}].$$  

Let $\gamma = \alpha \sqrt{N(\mathcal{I})/N(\mathcal{J})}$. Since $\mathcal{J} = \alpha \mathcal{I}$ then $N(\mathcal{J}) = |\alpha|^2 N(\mathcal{I})$ and so $|\gamma| = 1$. By Lemma 2.4, the map $v \mapsto \gamma v$ is an isometry of $\mathbb{R}^n$ and as $L[\mathcal{J}] = \gamma L[\mathcal{I}]$, the lattices $L[\mathcal{I}]$ and $L[\mathcal{J}]$ are isometric. \qed
Given $L$, we can produce a maximum of $h$ non-isometric lattices $L[I]$ where $h$ denotes the class-number of the quadratic field $K$.

It is useful to note which for which ideals $I$ is $IL_+ \subseteq \mathbb{Z}^n$.

**Lemma 3.3** Let $I$ be an ideal of $\mathcal{O}$. Then $IL_+ \subseteq \mathbb{Z}^n$ if and only if $I \subseteq \langle 2, \frac{1}{2}(1 - \sqrt{-l}) \rangle$. In this case also $N(I)\mathbb{Z}^n \subseteq IL_+$.

**Proof** Note that $L_+ \cap \mathbb{Z}^n = L_0$ and so $IL_+ \subseteq \mathbb{Z}^n$ if and only if $IL_+ \subseteq L_0$. This occurs if and only if $I$ annihilates the $\mathcal{O}$-module $M = L_+/L_0$. This module has 2 elements, so it must be isomorphic to $\mathcal{O}/\mathcal{J}$ where $\mathcal{J}$ is an ideal of norm 2. As $\langle 2, \frac{1}{2}(1 - \sqrt{-l}) \rangle$ has norm 2 and is seen to annihilate $M$ as $\frac{1}{2}(1 - \sqrt{-l})$ takes $\frac{1}{2}e_1(I + W)$ to $\frac{1}{2}(l + 1)e_1$, then $\mathcal{J} = \langle 2, \frac{1}{2}(1 - \sqrt{-l}) \rangle$. Thus $\mathcal{J}$ is the annihilator of $M$ and the first statement follows.

Suppose that $I \subseteq \langle 2, \frac{1}{2}(1 - \sqrt{-l}) \rangle$. The lattice $L_+[I]$ is unimodular so that if $u \cdot v \in \mathbb{Z}$ for all $v \in L_+[I]$ then $u \in L_+[I]$. If $u = \sqrt{N(I)}w$ with $w \in \mathbb{Z}^n$ then $u \cdot v \in \mathbb{Z}$ for all $v \in N(I)^{-1/2}\mathbb{Z}^n$ and as $L_+[I] \subseteq N(I)^{-1/2}\mathbb{Z}^n$ then $u \in L_+[I]$. Hence $\sqrt{N(I)}\mathbb{Z}^n \subseteq L_+[I]$ and so $N(I)\mathbb{Z}^n \subseteq IL_+$. □

In this case the lattice $\Lambda$ is the inverse image of a subgroup $C$ of $(\mathbb{Z}/N\mathbb{Z})^n$, where $N = N(I)$, under the projection $\pi : \mathbb{Z}^n \to (\mathbb{Z}/N\mathbb{Z})^n$. Such a subgroup is called a linear code of length $n$ over $\mathbb{Z}/N\mathbb{Z}$. We also say that $\Lambda$ is obtained from $C$ by construction $A_N$.

The standard dot product is well-defined on the group $(\mathbb{Z}/N\mathbb{Z})^n$. If a subgroup $C \subseteq (\mathbb{Z}/N\mathbb{Z})^n$ satisfies $u \cdot v = 0$ for all $u, v \in C$ then $C$ is self-orthogonal. Also $C$ is self-dual if $u \cdot C = 0$ if and only if $u \in C$. By the nondegeneracy of the dot product, $C$ is self-dual if and only if $C$ is self-orthogonal and $|C| = N^{n/2}$.

**Proposition 3.1** Let $I$ be an ideal of $\mathcal{O}$ with $I \subseteq \langle 2, \frac{1}{2}(1 - \sqrt{-l}) \rangle$ and $N(I) = N$. The lattice $L = IL_+$ is obtained from construction $A_N$ from a self-dual linear code $C$ of length $n$ over $\mathbb{Z}/N\mathbb{Z}$.

If $I = \langle N, \frac{1}{2}(a - \sqrt{-l}) \rangle$ with $a \equiv 1 \pmod{4}$ and $a^2 \equiv -l \pmod{4N}$ then $C$ is spanned by the vectors of the form $\frac{1}{2}(e_i + e_j)(aI - W)$ ($1 \leq i \leq j \leq n$).

**Proof** Apart from the self-duality of $C$ we have already proved the first assertion. The self-duality of $C$ follows from the unimodularity of $N^{-1/2}IL_+$. By volume considerations

$$N^{n/2} = |Z^n : IL_+| = |(\mathbb{Z}/N\mathbb{Z})^n : C|$$

and so $|C| = N^{n/2}$. Also if $u, v \in IL_+$ then $N^{-1/2}u$ and $N^{-1/2}v$ lie in the integral lattice $N^{-1/2}IL_+$ so that $N^{-1}u \cdot v \in Z$. Hence $C$ is self-orthogonal, and as it has the correct order, it is self-dual.
The ideal \( \mathcal{I} \) contains the subgroup \( N\mathbb{Z} + \frac{1}{2}(a - \sqrt{-l})\mathbb{Z} \) of \( \mathcal{O} \) and as this subgroup also has index \( N \) in \( \mathcal{O} \) then \( \mathcal{I} = N\mathbb{Z} + \frac{1}{2}(a - \sqrt{-l})\mathbb{Z} \). It follows that \( N\mathcal{L}_+ = N\mathcal{L}_+ + \frac{1}{2}(a - \sqrt{-l})\mathcal{L}_+ \). As \( a \equiv 1 \pmod{4} \), \( \frac{1}{2}(a + \sqrt{-l}) - \frac{1}{2}(1 + \sqrt{-l}) \) is an even integer. It follows that \( L_0 + \frac{1}{2}\mathbf{e}_1(aI + W) = L_0 + \frac{1}{2}\mathbf{e}_1(I + W) \) and so \( L_+ \) is generated by \( L_0 \) and \( u = \frac{1}{2}\mathbf{e}_1(aI + W) \). Thus \( N\mathcal{L}_+ \) is generated by the \( \frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j) \) and \( N\mathbf{u} \) and \( \frac{1}{2}(a - \sqrt{-l})\mathcal{L}_+ \) is generated by the \( \frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W) \) and

\[
\frac{1}{2}\mathbf{u}(aI - W) = \frac{1}{4}\mathbf{e}_1(aI - W)(aI + W) = \frac{a^2 + l}{4}.
\]

Note that \( (a^2 + l)/4 \) is a multiple of \( N \). It follows that \( \mathcal{C} \) is generated by \( N\mathbf{u} \) and the \( \frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W) \). But \( N\mathbf{u} = (N/2)\mathbf{e}_1(I + W) \) is congruent modulo \( N \) to the word consisting of all \( N/2s \). Also \( (N/2)\mathbf{e}_1(aI - W) \) is congruent to the same word. We can drop the generator \( N\mathbf{u} \) and deduce that \( \mathcal{C} \) is generated by the \( \frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W) \).

\[ \blacksquare \]

4 Quadratic residue codes

To use the above construction of lattices, we need a supply of skew-symmetric conference matrices. Paley [8] constructed a family of such matrices of order \( n = l + 1 \) whenever \( l \equiv 3 \pmod{4} \) is prime. To apply our theory we stipulate in addition that \( l \equiv 7 \pmod{8} \). We find that the lattices \( \mathcal{I}\mathcal{L}_+ \) are derived from quadratic residue codes in this case.

We define a conference matrix \( W \in \mathcal{W}_n \) as follows. Let

\[
W = \begin{pmatrix}
0 & 1 & \cdots & 1 \\
-1 & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots \\
-1 & \ddots & \ddots & \ddots \\
\end{pmatrix}
\]

where the \( l \)-by-\( l \) matrix \( W' \) is the circulant matrix whose \((i, j)\)-entry is

\[
W'_{ij} = \frac{\left( \frac{j-i}{l} \right)}{}
\]

where \( \left( \frac{\cdot}{l} \right) \) denotes the Legendre symbol. This matrix \( W \) is called a conference matrix of Paley type. For the rest of this section \( W \) will denote this particular matrix.

We follow the usual practice with quadratic residue codes and label the entries of a typical vector of length \( n = l + 1 \) using the elements of the projective line over \( \mathbb{F}_l \) as follows: \( \mathbf{v} = (v_\infty, v_0, v_1, v_2, \ldots, v_{l-1}) \). We let \( \mathbf{e}_\infty, \mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{l-1} \) denote the corresponding unit vectors, that is, \( \mathbf{e}_\mu \) has a one in the position labelled \( \mu \), and zeros elsewhere.
Lemma 4.1 (Paley) The matrix $W$ is a skew-symmetric conference matrix.

Proof See for instance [7, Chapter 18]. □

In $\mathcal{O}$, the ideal $2\mathcal{O}$ splits as a product of two distinct prime ideals: $2\mathcal{O} = \mathcal{P}\mathcal{Q}$ where $\mathcal{P} = \langle 2, \frac{1}{2}(1 + \sqrt{\ell}) \rangle$ and $\mathcal{Q} = \mathcal{P}^* = \langle 2, \frac{1}{2}(1 - \sqrt{\ell}) \rangle$. We shall investigate the lattices $L_+[\mathcal{P}^r]$ and $L_+[\mathcal{Q}^r]$ for integers $r \geq 0$. (The discussion for $L_-[\mathcal{P}^r]$ and $L_-[\mathcal{Q}^r]$ is similar.)

We first need a lemma on the structure of the ideals $\mathcal{P}^r$ and $\mathcal{Q}^r$.

Lemma 4.2 Let $r$ be a positive integer. Then

$$\mathcal{P}^r = 2^r\mathbb{Z} + \frac{1}{2}(t + \sqrt{\ell})\mathbb{Z}$$

and

$$\mathcal{Q}^r = 2^r\mathbb{Z} + \frac{1}{2}(t - \sqrt{\ell})\mathbb{Z}$$

where $t$ is any integer with $t^2 \equiv -l \pmod{2^{r+2}}$ and $t \equiv 1 \pmod{4}$.

Proof It is well-known that if $s \geq 3$, and $a \equiv 1 \pmod{8}$ then the congruence $x^2 \equiv a \pmod{2^s}$ is soluble. Thus there exists $t$ with $t^2 \equiv -l \pmod{2^{r+2}}$. By replacing $t$ by $-t$ if necessary, we may assume that $t \equiv 1 \pmod{4}$.

Consider the ideal $\mathcal{I} = \langle 2^r, \frac{1}{2}(t + \sqrt{\ell}) \rangle$ of $\mathcal{O}$. As $2^r \in \mathcal{I}$ then $\mathcal{I}$ is a factor of $2^r\mathcal{O} = \mathcal{P}^r\mathcal{Q}^r$. But as $\frac{1}{2}(t + \sqrt{\ell}) = \frac{1}{2}(1 + \sqrt{\ell}) + 2(t - 1)/4 \in \mathcal{P}$ then $\mathcal{P}$ is a factor of $\mathcal{I}$. But $\frac{1}{4}(t + \sqrt{\ell}) \notin \mathcal{O}$, and so $2\mathcal{O}_K = \mathcal{P}\mathcal{Q}$ is not a factor of $\mathcal{I}$. Hence $\mathcal{I} = \mathcal{P}^r$ where $1 \leq r' \leq r$. Letting $\alpha = \frac{1}{2}(t + \sqrt{\ell})$ we have

$$\mathcal{I}^* = \langle 2^r, \alpha \rangle \langle 2^r, \alpha^* \rangle$$

$$= \langle 2^{2r}, 2^r\alpha, 2^r\alpha^*, \alpha\alpha^* \rangle$$

$$= \langle 2^{2r}, 2^r\alpha, 2^r\alpha^*, (t^2 + l)/4 \rangle$$

$$\subseteq 2^r\mathcal{O}$$

as $t^2 \equiv -l \pmod{2^{r+2}}$. But $\mathcal{I}^* = N(\mathcal{I})\mathcal{O} = 2^r\mathcal{O}$ and so $r = r'$, that is $\mathcal{I} = \mathcal{P}^r$.

Now $\mathcal{P}^r \subseteq 2^r\mathbb{Z} + \frac{1}{2}(t + \sqrt{\ell})\mathbb{Z}$, but both these groups have index $2^r$ in $\mathcal{O}$ so they are equal. The statement about $\mathcal{Q}^r$ now follows by complex conjugation. □

We now consider the lattices $\mathcal{Q}^rL_+$ for $r \geq 1$. Since $\mathcal{Q}^r \subseteq \mathcal{Q}$ and $\mathcal{Q} = \langle 2, \frac{1}{2}(1 - \sqrt{\ell}) \rangle$ then by Proposition [3.4] $\mathcal{Q}^rL_+$ is obtained by construction $\Lambda_{2^r}$ from a self-dual code $\mathcal{C}_r$ over $\mathbb{Z}/2^r\mathbb{Z}$. We shall show that $\mathcal{C}_r$ is the Hensel lift of an extended quadratic residue code in the sense of [1].
Recall that the integer \( t \) satisfies \( t \equiv 1 \pmod{4} \) and \( t^2 \equiv -l \pmod{2^{r+2}} \). By Proposition \([\ref{prop:1}]\) it follows that \( C_r \) is generated by the vectors \( \frac{1}{2}(e_i + e_j)(W - tI) \). It is plain that we need only these vectors with \( i = \infty \) and so \( C_r \) is spanned by \( u = e_\infty(W - tI) \) and \( v_j = \frac{1}{2}(e_\infty + e_j)(W - tI) \) for \( 0 \leq j < l \).

Let \( \phi : (\mathbb{Z}/2^r\mathbb{Z})^n \to (\mathbb{Z}/2^r\mathbb{Z})^l \) be the map given by deleting the first coordinate of the vector. The code \( C_r \) contains the vector \( u = (-t, 1, 1, \ldots, 1) \).

As \( r \) is odd and \( C_r \) is self-dual, the intersection of \( C_r \) and the kernel of \( \phi \) is trivial. Thus \( C_r' = \phi(C_r) \) has the same order as \( C_r \). Then \( \phi(u) \) is the all-ones vector, and \( \phi(v_j) \) are cyclic shifts of \( \phi(v_0) \). Also \( \phi(v_0) = (c_0, c_1, \ldots, c_{p-1}) \) where

\[
c_j = \begin{cases} 
(1 - t)/2 & \text{if } j = 0, \\
1 & \text{if } j \text{ is a quadratic residue modulo } l, \\
0 & \text{if } j \text{ is a quadratic nonresidue modulo } l.
\end{cases}
\]

Thus \( C_r' \) is a cyclic code over \( \mathbb{Z}/2^r\mathbb{Z} \).

We recall the definition of quadratic residue codes. Consider the polynomial \( X^l - 1 \) over the field \( \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \). Then \( X^l - 1 \) splits into linear factors in some finite extension \( \mathbb{F}_{2^k} \) of \( \mathbb{F}_2 \). In fact

\[
X^l - 1 = \prod_{j=0}^{l-1} (X - \zeta^j)
\]

where \( \zeta \) is a primitive \( l \)-th root of unity in \( \mathbb{F}_{2^k} \). We write

\[
X^l - 1 = (X - 1)f_+(X)f_-(X)
\]

where

\[
f_+(X) = \prod_{(j, l) = 1} (X - \zeta^j) \quad \text{and} \quad f_-(X) = \prod_{(j, l) = -1} (X - \zeta^j).
\]

As \( l \equiv 7 \pmod{8} \), then 2 is a quadratic residue modulo \( l \), and so the coefficients of both \( f_+ \) and \( f_- \) are invariant under the Frobenius automorphism \( \delta \mapsto \delta^2 \) of \( \mathbb{F}_{2^k} \). Consequently both \( f_+ \) and \( f_- \) have coefficients in \( \mathbb{F}_2 \). The labelling of these factors as \( f_+ \) and \( f_- \) depends on the choice of \( \zeta \). Replacing \( \zeta \) by another primitive \( l \)-th root of unity either preserves or interchanges \( f_+ \) and \( f_- \). The coefficients of \( X^{(l-3)/2} \) in \( f_+ \) and \( f_- \) are 0 and 1 is some order, so we can, and shall, choose \( \zeta \) such that

\[
f_+(X) = X^{(l-1)/2} + 0X^{(l-3)/2} + \cdots \quad \text{and} \quad f_-(X) = X^{(l-1)/2} + X^{(l-3)/2} + \cdots.
\]

The cyclic codes of length \( l \) over \( \mathbb{F}_2 \) with generator polynomials \( f_+(X) \) and \( f_-(X) \) are called the quadratic residue codes.
Bonnecaze, Solé and Calderbank \cite{BN97} extended the notion of quadratic residue code to codes over \( \mathbb{Z}/2^r\mathbb{Z} \). By Hensel’s lemma there exist unique polynomials \( f_+(X) \) and \( f_-(X) \) with coefficients in \( \mathbb{Z}/2^r\mathbb{Z} \) such that

\[
X^l - 1 = (X - 1)f_+(X)f_-(X),
\]

\[
f_+(X) \equiv f_+(X) \pmod{2} \quad \text{and} \quad f_-(X) \equiv f_-(X) \pmod{2}.
\]

The cyclic codes over \( \mathbb{Z}/2^r\mathbb{Z} \) with generator polynomials \( f_+(X) \) and \( f_-(X) \) are called lifted quadratic residue codes over \( \mathbb{Z}/2^r\mathbb{Z} \).

**Theorem 4.1** The code \( C'_r \) is the lifted quadratic residue code over \( \mathbb{Z}/2^r\mathbb{Z} \) with generator polynomial \( f_+(X) \).

**Proof** Cyclic codes of length \( l \) over \( R = \mathbb{Z}/2^r\mathbb{Z} \) correspond to ideals of the polynomial ring \( R[X]/\langle X^l - 1 \rangle \). The code \( C'_r \) corresponds to the ideal \( I = \langle g, h \rangle \) where

\[
g(X) = \sum_{j=0}^{p-1} X^j
\]

and

\[
h(X) = \frac{1 - t}{2} + \sum_{(j/l)=1} X^j.
\]

We first consider the case where \( r = 1 \). Then \( I = \langle u(X) \rangle \) where \( u(X) \) is the greatest common divisor of \( g(X) \) and \( h(X) \). Let \( \zeta \) be a root of \( f_+(X) = 0 \) in an extension field of \( \mathbb{F}_2 \). The roots of \( g(X) \) are the \( \zeta^j \) where \( p \nmid j \). As \( t \equiv 1 \pmod{4} \) then \( \frac{1}{2}(1 - t) \) is even and so \( h(X) = \sum_{(j/l)=1} X^j \). Now

\[
\sum_{(j/l)=1} \zeta^j = 0 \quad \text{and} \quad \sum_{(j/l)=-1} \zeta^j = 1.
\]

It follows that

\[
h(\zeta^a) = \sum_{(j/l)=1} (\zeta^a)^j = 0
\]

if and only if \( \left( \frac{a}{l} \right) = 1 \). Thus \( u(X) = f_+(X) \).

Now we consider the general case. The reduction of \( C'_r \) modulo 2 is \( C'_1 \). Any liftings to \( C'_r \) of a basis of \( C'_1 \) generate a free \( R \)-module (of rank \( \frac{1}{2}(l+1) \)), and so they generate the whole code \( C'_r \). As \( C_r \) is free over \( R \), it is generated as an ideal by a monic polynomial \( F(X) \), of degree \( \frac{1}{2}(l+1) \). As \( F(X) \) reduces to \( f_+(X) \) modulo 2, and \( F(X) \mid X^l - 1 \) it follows that \( F(X) = f_+(X) \) as required. \( \square \)
Given the code \( C'_r \), the code \( C_r \) can be reconstructed, since for each element of \( C'_r \) the corresponding element of \( C_r \) is uniquely determined as it is orthogonal to \((-t, 1, 1, \ldots, 1)\).

We now turn to \( P^r L_+ \). This is no longer a sublattice of \( \mathbb{Z}^n \).

**Lemma 4.3** Let \( r \) be a positive integer. The index \( |P^r L_+ : P^r L_+ \cap \mathbb{Z}^n| = 2 \). The lattice \( P^r L_+ \cap \mathbb{Z}^n \) is generated by the vectors \( 2^r(e_\infty + e_\mu) \) (\( \mu \in \{\infty, 0, 1, 2, \ldots, l-1\} \)), the vector \( u = e_\infty(W + tI) \) and the vectors \( v_j = \frac{1}{2}(e_\infty + e_j)(W + tI) \) (\( 0 \leq j < l \)). Also \( P^r L_+ \) is generated by \( P^r L_+ \cap \mathbb{Z}^n \) and \( \frac{1}{2}u - \frac{1}{4}(t^2 + l)e_\infty \).

**Proof** We have \( P^r = 2^r\mathbb{Z} + \frac{1}{2}(t + \sqrt{-l})\mathbb{Z} \). Let \( \Omega_0 \) denote the lattice generated by the \( 2^r(e_\infty + e_\mu), u \), and the \( v_j \). The lattice \( L_+ \) is generated by the \( e_\infty + e_\mu \) and \( \frac{1}{2}e_\infty(tI + W) \). Thus \( 2^r(e_\infty + e_\mu), u = \frac{1}{2}(t + \sqrt{-l})2e_\infty \) and \( v_j = \frac{1}{2}(t + \sqrt{-l})(e_\infty + e_j) \) all lie in \( P^r L_+ \). These vectors all have integer coordinates, and so \( \Omega_0 \subseteq P^r L_+ \cap \mathbb{Z}^n \).

Let \( \Omega \) be the lattice generated by \( \Omega_0 \) and \( \frac{1}{2}u - \frac{1}{4}(t^2 + l)e_\infty \). Now

\[
\frac{1}{2}(t + \sqrt{-l})\frac{1}{2}e_\infty(tI + W) = \frac{1}{4}(t + \sqrt{-l})^2e_\infty
= \left[ \frac{1}{2}(t + \sqrt{-l}) - \frac{t^2 + l}{4} \right] e_\infty
= \frac{t}{2}u - \frac{t^2 + l}{4}e_\infty.
\]

As \( t \) is odd and \( u \in \Omega_0 \) then \( \Omega \subseteq P^r L_+ \).

The lattice \( P^r L_+ \) is generated by \( \Omega \) and \( 2^{r-1}e_\infty(tI + W) = 2^{r-1}u \). But \( u - \frac{1}{2}(t^2 + l)e_\infty \in \Omega \) and as \( t^2 + l \) is divisible by \( 2^{r+1} \) then \( u \in \Omega_0 \) and so \( \Omega = P^r L_+ \). As \( \frac{1}{2}u - \frac{1}{4}(t^2 + l)e_\infty \) is not in \( \mathbb{Z}^n \) but its double is in \( \Omega_0 \), then \(|\Omega : \Omega_0| = |P^r L_+ : P^r L_+ \cap \mathbb{Z}^n| = 2 \) and so \( \Omega_0 = P^r L_+ \cap \mathbb{Z}^n \). \( \square \)

One can now proceed to express the lattices \( P^r L_+ \) and \( P^r L_+ \cap \mathbb{Z}^n \) in terms of lifted quadratic residue codes over \( \mathbb{Z}/2^r\mathbb{Z} \). For simplicity we present the details only for \( r = 1 \). Let \( D' \) denote the cyclic quadratic residue code of length \( l \) over \( \mathbb{F}_2 \) with generator polynomial \( f_\cdot(X) \), and let \( D \) denote its extension obtained by appending a parity check bit at the front.

**Theorem 4.2** The lattice \( PL_+ \cap \mathbb{Z}^n \) consists of those vectors reducing modulo 2 to elements of \( D \) and the sum of whose entries is a multiple of 4. The lattice \( PL_+ \) is obtained from \( PL_+ \cap \mathbb{Z}^n \) by adjoining the extra generator \( \frac{1}{2}((1 - l), 1, 1, \ldots, 1) \).
Proof. We may take \( t = 1 \) in the proof of Lemma 4.3. In this case the vector \( \mathbf{u} \) is the all-ones vector while each \( \mathbf{v}_j \) consists of \( \frac{1}{2}(l+1) \) ones and \( \frac{1}{2}(l+1) \) zeros. As \( \frac{1}{2}(l+1) \) is a multiple of 4 the sum of the entries of each of these vectors is a multiple of 4. As this is manifestly true for the vectors \( 2(e_\infty + e_\mu) \) too, then the sum of the entries of each vector in \( PL_+ \cap \mathbb{Z}^n \) is a multiple of 4.

If we delete the first entry of the given generators of \( PL_+ \) and reduce modulo 2 we get the all-ones vector of length \( l \) and the cyclic shifts of the vector \( w_0 = (d_0, d_1, \ldots, d_{l-1}) \) where

\[
d_j = \begin{cases} 
1 & \text{if } j = 0 \text{ or if } j \text{ is a quadratic residue modulo } l, \\
0 & \text{if } j \text{ is a quadratic nonresidue modulo } l.
\end{cases}
\]

By a similar argument to the proof of Theorem 4.1 these vectors generate the cyclic quadratic residue code \( D' \). Hence each element of \( PL_+ \cap \mathbb{Z}^n \) reduces modulo 2 to an element of \( D \). If \( \Omega \) denotes the sublattice of \( \mathbb{Z}^n \) consisting of vectors reducing modulo 2 to \( D \) and with the entries summing to a multiple of 4, then \( |\mathbb{Z}^n : \Omega| = 2^{1+n/2} = |\mathbb{Z}^n : PL_+ \cap \mathbb{Z}^n| \). Thus \( \Omega = PL_+ \cap \mathbb{Z}^n \).

Now letting \( t = 1 \) we see that \( \frac{1}{2}\mathbf{u} - \frac{1}{4}(t^2 + l)e_\infty = \frac{1}{2}(\frac{1}{2}(1-l), 1, 1, \ldots, 1) \) and so this vector together with \( PL_+ \cap \mathbb{Z}^n \) generates \( PL_+ \). \( \square \)

In the terminology of Conway and Sloane [5, Chapter 5, §3], the lattice \( PL_+ \) is obtained from the code \( D \) by construction B. Then the lattice \( PL_+ \) is obtained by density doubling. One can extend these notions to lifted quadratic residue codes to produce the lattices \( PL_r \).

We look briefly at the lattices \( IL_+ \) for more general ideals \( I \). Consider the case where \( I = A \), an ideal of norm \( p \), an odd prime. Then \( A = \langle p, t + \sqrt{-l} \rangle \) where \( t^2 \equiv -l \pmod{p} \). The rows of the matrix \( tI + W \) generate a self-dual linear code \( C \) over \( \mathbb{F}_p \) which turns out to be an extended quadratic residue code. The coordinates of vectors in \( L_+ \) are half-integers, and it is meaningful to reduce these modulo the odd prime \( p \). Then the lattice \( AL_+ \) simply consists of the vectors in \( L_+ \) which reduce modulo \( p \) to elements of \( C \). More generally \( A^rL_+ \) will have a similar description in terms of an extended lifted quadratic residue code over \( \mathbb{Z}/p^r\mathbb{Z} \). Finally by splitting a general ideal \( I \) into a product of powers of prime ideals \( A^r \), we can describe \( IL_+ \) in terms of the various \( A^r \) using the Chinese remainder theorem.

5 Examples

Since the ring \( \mathbb{Z}[[\frac{1}{2}(1 + \sqrt{-7})]] \) has class number 1 (and each even unimodular rank 8 lattice is isometric to the \( E_8 \) root lattice) the first interesting examples
occur when \( l = 15 \) and the first interesting examples with Paley matrices occur when \( l = 23 \).

5.1 \( l = 23 \) and \( l = 31 \)

In both these cases we take \( W \) to be the Paley matrix. We first consider the case \( l = 23 \).

The class group of \( \mathcal{O} = \mathbb{Z}[(1 + \sqrt{-23})/2] \) has order 3, and the class of each of its ideals \( \mathcal{P} = \langle 2, \frac{1}{2}(1 + \sqrt{-23}) \rangle \) and \( \mathcal{Q} = \langle 2, \frac{1}{2}(1 - \sqrt{-23}) \rangle \) generates its class group. The lattice \( L_+ \) itself is the lattice \( D_{24}^+ \). The lattices \( Q^rL_+ \) are obtained by applying construction \( A_r^+ \) to the lifted quadratic residue codes \( C_r^+ \). The code \( C_1^+ \) is the extended binary Golay code. It is plain that \( Q^2L_+ \) is obtained by applying construction \( A \) [Chapter 5, §2] to the binary Golay code, and so \( L_+[Q] \) is isometric to the Niemeier lattice with root system \( A_{24}^+ \).

The isometry classes of the unimodular lattices \( L_+[Q^r] \) depend only on the congruence class of \( r \) modulo 3. If \( r \equiv 0 \) (mod 3) then \( L_+[Q^r] \) is isometric to \( D_{24}^+ \) while if \( r \equiv 1 \) (mod 3) then \( L_+[Q^r] \) is isometric to the Niemeier lattice with root system \( A_{24}^+ \). To identify \( L_+[Q^r] \) when \( r \equiv 2 \) (mod 3) note that \( Q^2 \) lies in the same ideal class as \( P \). Hence for \( r \equiv 2 \) (mod 3), \( L_+[Q^r] \) is isometric to \( L_+[\mathcal{P}] \). By Theorem 4.2 it is plain that \( L_+[\mathcal{P}] \) is the Leech lattice, as given by Leech’s original construction \( \mathcal{L} \). Applying Theorem 3.1 gives an explicit isomorphism between \( L_+[\mathcal{P}] \) and \( L_+[Q^2] \) which is equivalent to that constructed in \( \mathcal{L} \).

In general if \( s \) is the order of the class of the ideal \( \mathcal{P} \) in the class group of \( \mathcal{O} \), then up to isometry \( L_+[\mathcal{P}^r] \) and \( L_+[Q^r] \) depend only on the congruence class of \( r \) modulo \( s \). Also \( L_+[\mathcal{P}^r] \) and \( L_+[Q^r] \) will be isometric whenever \( r \equiv -r' \) (mod \( s \)). For \( l = 31 \) we also have \( s = 3 \) and the above discussion is valid for \( l = 31 \) too. In particular \( L_+[\mathcal{P}] \) is isometric to \( L_+[Q^2] \), and we recover \( \mathcal{L} \) Theorem 1.

We can give alternative constructions of the Leech lattice at will simply by writing down ideals of \( \mathbb{Z}[(1 + \sqrt{-23})/2] \) equivalent to \( \mathcal{P} \). Let \( \mathcal{I} = \langle 3, \frac{1}{2}(1 + \sqrt{-23}) \rangle \) and \( \mathcal{J} = \langle 3, \frac{1}{2}(-1 + \sqrt{-23}) \rangle \). Then \( \mathcal{P}, \mathcal{J} \) and \( Q\mathcal{I} = \langle 6, \frac{1}{2}(-5 + \sqrt{-23}) \rangle \) all lie in the same ideal class.

The lattice \( \mathcal{J}L_+ \) is generated using density doubling from the lattice \( L' \) consisting of all vectors in \( \mathbb{Z}^{24} \) whose entries sum to zero and which reduce modulo 3 to elements of the extended ternary quadratic residue code with generator matrix \( I - W \). Then \( \mathcal{J}L_+ \) is generated by \( L' \) and the vector \( \frac{1}{2}(5, 1, 1, \ldots, 1) \). The lattice \( L_+[\mathcal{J}] = 3^{-1/2}\mathcal{J}L_+ \) is isometric to the Leech lattice.
Next consider the lattice $\mathbb{Q}\mathcal{I}L_+$. This consists of the vectors in $\mathbb{Z}^{24}$ reducing modulo 2 and modulo 3 to elements of appropriately chosen binary and ternary quadratic residue codes. The binary code in question is that generated by vectors $\frac{1}{2}(e_\infty + e_\alpha)(I - W)$ for $\alpha \in \{\infty, 0, 1, 2, \ldots, l - 1\}$ and the ternary code is generated by the rows of $I + W$. Then $L_+[\mathcal{I}] = 6^{-1/2}Q\mathcal{I}L_+$ is isometric to the Leech lattice.

\section*{5.2 $l = 47$}

Again we take $W$ to be the Paley matrix. In [3, Chapter 7, §7] the lattice $\Lambda = P_{48q}$ is described. This is an even unimodular lattice of rank 48 and minimum norm 6. It is generated by the following vectors $(a_\infty, a_0, a_1, \ldots, a_{46})$:

(i) $(1/\sqrt{12})(-5, 1, 1, \ldots, 1),$

(ii) those vectors of the shape $(1/\sqrt{3})(1^{24}, 0^{24})$ supported on the translates modulo 47 of the set $\{0\} \cup Q$ where $Q$ is the set of quadratic residues modulo 47,

(iii) all vectors of the shape $(1/\sqrt{3})(\pm 3^2, 0^{46}).$

It is more convenient to consider instead the equivalent lattice $\Lambda'$ generated by the vectors

(i)' $(1/\sqrt{12})(5, 1, 1, \ldots, 1),$

(ii)' those vectors of the shape $(1/\sqrt{3})(1^{24}, 0^{24})$ supported on the translates modulo 47 of the set $\{0\} \cup N$ where $N$ is the set of quadratic nonresidues modulo 47,

(iii)' all vectors of the shape $(1/\sqrt{3})(\pm 3^2, 0^{46}).$

We claim that $\Lambda'$ is the lattice $L_+[\mathcal{I}]$ where $\mathcal{I} = \langle 3, \frac{1}{2}(1 - \sqrt{-47}) \rangle$. Note that the norm of $\mathcal{I}$ is 3. It suffices to show that each of the generating vectors for $\Lambda'$ is contained in $L_+[\mathcal{I}]$. Since each vector of shape $(\pm 1^2, 0^{46})$ lies in $L_+$ and $3 \in P$ then it is immediate that the vectors of type (iii)' lie in $L_+[\mathcal{I}]$. The vectors of type (ii)' are the differences of the first row and an arbitrary other row of the matrix $(1/2\sqrt{3})(I - W)$. Since $\frac{1}{2}(1 - \sqrt{-47}) \in \mathcal{I}$, the vectors of type (ii)' lie in $L_+[\mathcal{I}]$. Finally, $\frac{1}{2}(1, -1, -1, \ldots, -1)$, the first row of $\frac{1}{2}(I - W)$, lies in $2\mathcal{I}L_+$. Also $v_0 = \frac{1}{2}e_0(I + W) \in L_+$ and $3v_0 = \frac{1}{2}(3, 3, 3, \ldots, 3) \in 3\mathcal{I}L_+$. Adding these two vectors gives $\frac{1}{2}(5, 1, 1, \ldots, 1) \in 2\mathcal{I}L_+$ so that the vector of type (i)' does lie in $L_+[\mathcal{I}]$.

The ideal $\langle \frac{1}{2}(1 - \sqrt{-47}) \rangle$ has norm 12 and factors as $\mathcal{O}\mathcal{I}^2$. The class number of $\mathcal{O}(\sqrt{-47})$ is 5, and so $[\mathcal{I}] = [P^2] = [Q^5]$. Thus $\Lambda'$ is isometric to
which is constructed using construction A from the quadratic residue code of length 48 over \( \mathbb{Z}/8\mathbb{Z} \).

5.3 \( l = 15 \)

In this case there is no Paley matrix. We consider two different conference matrices of order 16.

If \( W \in \mathcal{W}_n \) then the \( 2n \times 2n \) matrix

\[
W' = \begin{pmatrix} W & I + W \\ -I + W & -W \end{pmatrix}
\]

is a skew-symmetric conference matrix of order \( 2n \). Applying this construction four times to the zero matrix in \( \mathcal{W}_1 \) gives the matrix

\[
W_1 = \begin{pmatrix}
0 & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
- & 0 & - & + & - & + & - & + & - & - & + & - & - & + & - & - \\
- & + & 0 & - & - & + & + & - & - & + & - & + & - & + & - & - \\
- & - & + & 0 & - & + & - & - & + & + & - & + & - & + & - & - \\
- & + & + & 0 & - & + & - & - & + & + & - & + & - & + & - & - \\
- & - & - & + & 0 & - & + & - & + & + & - & - & + & + & - & - \\
- & + & - & - & + & 0 & + & - & + & - & - & - & - & - & - & - \\
- & - & + & + & 0 & - & - & + & + & + & + & + & + & + & + & + \\
- & + & + & 0 & - & + & + & + & + & + & + & + & + & + & + & + \\
- & - & - & + & + & 0 & + & - & + & - & - & - & - & - & - & - \\
- & + & - & - & + & 0 & + & + & - & + & - & - & - & - & - & - \\
- & - & + & + & 0 & + & - & + & - & - & - & - & - & - & - & - \\
- & + & - & - & + & 0 & + & + & - & + & - & - & - & - & - & - \\
- & - & + & + & 0 & - & + & + & + & + & + & + & + & + & + & + \\
- & - & - & + & + & - & - & + & + & + & + & + & + & + & + & + \\
- & + & - & - & + & 0 & + & + & - & + & - & - & - & - & - & - \\
\end{pmatrix}
\]

where, for convenience, we have denoted 1 and \(-1\) by + and - respectively. The ideal class group of \( \mathbb{Z}[(1 + \sqrt{-15})/2] \) has order 2. The ideal \( \mathcal{I} = \langle 2, \frac{1}{2}(1 - \sqrt{-15}) \rangle \) is not principal and \( \mathcal{I}L^+ \) is given by construction A
from the binary code with the generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{pmatrix}.
\]
Thus \( L_+[I] \) is isometric to the orthogonal direct sum of two copies of the \( D_8^+ \) lattice. This is not isometric to \( L_+ \).

Another conference matrix of order 16 is
\[
W_2 = \begin{pmatrix}
0 & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
- & 0 & + & + & - & - & - & + & - & + & - & - & + & - & - & - \\
- & - & 0 & + & + & - & - & + & - & + & - & - & + & - & - & + \\
- & - & - & 0 & + & + & - & - & + & - & - & + & - & - & - & - \\
- & - & - & - & - & - & - & 0 & + & + & - & - & + & - & - & - \\
- & - & - & - & - & - & - & - & 0 & + & + & - & - & + & - & - & - \\
- & - & - & - & - & - & - & - & 0 & + & + & - & - & + & - & - & - \\
- & - & - & - & - & - & - & - & 0 & + & + & - & - & + & - & - & - \\
\end{pmatrix}.
\]
In this case the lattice \( IL_+ \) is obtained using construction A applied to the binary code with generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
\end{pmatrix}.
\]
Thus $L_+[\mathcal{I}]$ is isometric to the $D_{16}^+$ lattice and so to $L_+$. This example shows that the isometry class of $L_+[\mathcal{I}]$ depends on the choice of the conference matrix $W$, and also that $L_+[\mathcal{I}]$ and $L_+[\mathcal{J}]$ may be isometric even when $\mathcal{I}$ and $\mathcal{J}$ are in different ideal classes.

References

[1] A. Bonnecaze, P. Solé & A. R. Calderbank, ‘Quaternary quadratic residue codes and unimodular lattices’ IEEE Trans. Inform. Theory 41 (1995), 366–377.

[2] R. Chapman & P. Solé, ‘Universal codes and unimodular lattices’, J. Théor. Nombres Bordeaux 8 (1996), 369–376.

[3] H. Cohn, A Second Course in Number Theory, John Wiley & Sons, 1962.

[4] P. M. Cohn, Algebra vol. 2 (2nd ed.), John Wiley & Sons, 1989.

[5] J. H. Conway & N. J. A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag, 1988.

[6] J. Leech, ‘Notes on sphere packing’, Canad. J. Math. 19 (1967) 251–267.

[7] J. H. van Lint & R. M. Wilson, A Course in Combinatorics, Cambridge University Press, 1992.

[8] R. E. A. C. Paley, ‘On orthogonal matrices’, J. Math. Phys. 12 (1933), 311–320.

[9] J.-P. Serre, A Course in Arithmetic, Springer-Verlag, 1973.