Isodual Codes over $\mathbb{Z}_{2k}$ and Isodual Lattices (Revised Version 6)

Christine Bachoc
Laboratoire d'Algorithmique Arithmétique, 351
Cours de la Libération
F–33405 Talence
France,

T. Aaron Gulliver
Department of Electrical and Electronic Engineering
University of Canterbury
Private Bag 4800
Christchurch, New Zealand
and
Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan

June 7, 1999

Abstract

A code is called isodual if it is equivalent to its dual code, and a lattice is called isodual if it is isometric to its dual lattice. In this note, we investigate isodual codes over $\mathbb{Z}_{2k}$. These codes give rise to isodual lattices; in particular, we construct a 22-dimensional isodual lattice with minimum norm 3 and kissing number 2464.

1 Introduction

A code is called isodual if it is equivalent to its dual code, and a lattice is called isodual if it is isometric to its dual lattice. Conway and Sloane [5] introduced the concept of isodual lattices, which is a generalization of unimodular lattices. A lot of known dense lattices are isodual [5], like the rescaled Barnes-Wall lattice or the Coxeter-Todd lattice. In the coding theory context, isodual codes play a similar role with respect to the extensively studied family of self-dual codes (cf. [10]). In this note, we investigate a remarkable class of isodual codes over $\mathbb{Z}_{2k}$, the double circulant ones, and use them to construct isodual lattices. In particular, we construct a 22-dimensional isodual lattice of minimum norm 3.

In Section 2, we study the properties of isodual codes and present double circulant codes. We investigate the symmetrized weight enumerators of isodual codes over $\mathbb{Z}_{2k}$, in particular, for small k, we give a basis for the space of invariants to which the symmetrized weight enumerators belong.

In Section 3, we describe how isodual lattices can be constructed from isodual codes over $\mathbb{Z}_{2k}$.

In Section 4, we construct double circulant codes over $\mathbb{Z}_4$ and $\mathbb{Z}_6$ with the highest minimum Euclidean weight among all double circulant codes of length up to 24. These examples show that there are isodual codes which have a higher minimum Euclidean weight than any self-dual code of the same length.

We then consider the lattices obtained from these codes. The most interesting are the 22-dimensional isodual lattices with minimum norm 3 and kissing number 2464 constructed from the double circulant codes over $\mathbb{Z}_4$ of length 22 and minimum Euclidean weight 12.

In Section 5, we show that there are up to equivalence exactly six double circulant codes over $\mathbb{Z}_4$ of length 22 and minimum Euclidean weight 12. We show that, from each of these codes, an extremal binary Type II codes of length 24 can be constructed, pointing out a close connection between the 22-dimensional isodual lattices and the Leech lattice.

Finally, in Section 6 we show that these lattices are all isometric to a single lattice L_{22} constructed from the binary $[22, 11, 6]$ self-dual code. In particular its automorphism group is proved to be isomorphic to $\{\pm 1\}^{11}.M_{22}.2$, and it is caracterised by the following properties: it is the unique up to isometry isodual 22-dimensional lattice of minimum norm 3 and containing an integral sublattice of index 2.

2 Isodual Codes

2.1 Codes

A *linear* code C of length n over $\mathbb{Z}_{2k}$ is a $\mathbb{Z}_{2k}$-submodule of $\mathbb{Z}_{2k}^n$ where $\mathbb{Z}_{2k}$ is the ring of integers modulo $2k$. We shall take for a representative set of the elements of $\mathbb{Z}_{2k}$ either $\{0, 1, 2, \cdots, 2k-1\}$ or $\{0, \pm 1, \pm 2, \pm 3, \ldots, \pm(k-1), k\}$, using whichever set is convenient. An element of C is called a codeword of C. A *generator matrix* of C is a matrix whose rows generate C. The *Hamming weight* $wt_H(x)$ of a vector x in $\mathbb{Z}_{2k}^n$ is just the number of non-zero components. The *Euclidean weight* $wt_E(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ over

$\mathbb{Z}_{2k}$ is $\sum_{i=1}^{n} \min\{x_i^2, (2k-x_i)^2\}$ where $\mathbb{Z}_{2k} = \{0, 1, 2, \dots, 2k-1\}$. The minimum Hamming and Euclidean weights, d_H and d_E, of C are the smallest Hamming and Euclidean weights among all non-zero codewords of C, respectively. Define the inner product of x and y in $\mathbb{Z}_{2k}^n$ by $x \cdot y := x_1 y_1 + \cdots + x_n y_n$. The *dual code* $C^\perp$ of C is then $C^\perp := \{x \in \mathbb{Z}_{2k}^n \mid x \cdot y = 0 \text{ for all } y \in C\}$.

In view of some applications, there is no need to distinguish between codeword components which differ in sign, i.e., $+1$ and -1. Hence, two codes are said to be *equivalent* if one can be obtained from the other by permuting and changing signs on the coordinates. C is called *isodual* if C is equivalent to $C^\perp$, and C is called *self-dual* if $C = C^\perp$. Clearly a self-dual code is isodual. We define the *symmetrized weight enumerator* (*swe*) of C by

$$swe_C(x_0, x_1, \dots, x_k) := \sum_{c \in C} x_0^{n_0(c)} x_1^{n_1(c)} \cdots x_{k-1}^{n_{k-1}(c)} x_k^{n_k(c)},$$

where $n_0(x), n_1(x), \dots, n_{k-1}(c), n_k(c)$ are the numbers of $0, \pm 1, \dots, \pm(k-1), k$ components of c, respectively. Equivalent codes have identical symmetrized weight enumerators. The *Hamming weight enumerator* of C is defined as $W_C(x, y) := \sum_{c \in C} x^{n - wt_H(c)} y^{wt_H(c)}$. An isodual code and its dual code have several identical weight enumerators (e.g., symmetrized weight enumerators, Hamming weight enumerators and biweight enumerators).

2.2 Constructions

Lemma 2.1 *If $2k$ is a square, then an isodual code over $\mathbb{Z}_{2k}$ exists for all lengths. If $2k$ is not a square, then an isodual code exists for length n if and only if n is even.*

Proof. If $2k$ is a square (say, α^2) then a code with generator matrix $(\ \alpha\ )$ is isodual. For a code C of length n over $\mathbb{Z}_{2k}$, it is known that $|C||C^\perp| = 2k^n$. If C is an isodual code then $|C| = |C^\perp| = 2k^{n/2}$. Thus n must be even if $2k$ is not a square. Moreover a code with generator matrix $(\ 1\ ,\ \beta\ )$ is isodual where $\beta \in \mathbb{Z}_{2k}$. $\square$

Lemma 2.2 *Suppose that C and D are isodual codes of lengths n and m with minimum Euclidean weights d_E and d'_E, respectively. Then the direct sum $C \oplus D := \{(c, d) \mid c \in C,\ d \in D\}$ is an isodual code of length $n + m$ with minimum Euclidean weight* $\min\{d_E, d'_E\}$.

Proof. Let σ and σ' be equivalent maps such that $C^\sigma = C^\perp$ and $D^{\sigma'} = D^\perp$. Then $C^\sigma \oplus D^{\sigma'} = C^\perp \oplus D^\perp$. It is easy to see that $(C \oplus D)^\perp = C^\perp \oplus D^\perp$. Therefore $(C \oplus D)$ is equivalent to $(C \oplus D)^\perp$. The minimum Euclidean weight follows from the construction. $\square$

From the above lemma, when searching for codes with high minimum Euclidean weight, it is sufficient to consider only codes which are not the direct sum of codes.

Lemma 2.3 *Let C be a code over $\mathbb{Z}_{2k}$ with generator matrix $(\ I\ ,\ A\ )$ where I is the identity matrix. If there are $(0,1,-1)$-monomial matrices P and Q such that $A^T = PAQ$ then C is isodual where A^T denotes the transpose of A.*

Proof. The matrix $(\ -A^T\ ,\ I\ )$ is a generator matrix of the dual code $C^\perp$. Since $A^T = PAQ$, C and the code with generator matrix $(\ I\ ,\ -A^T\ )$ are equivalent. $\square$

If A is symmetric or skew-symmetric (that is, $A^T = A$ or $A^T = -A$) then A satisfies the assumption of the above lemma.

Double circulant codes are a remarkable class of isodual codes. A *pure double circulant* code of length $2n$ has a generator matrix of the form $(\ I\ ,\ R\ )$ where R is an n by n circulant matrix. A code with a generator matrix of the form

$$(1)\qquad \left(\begin{array}{ccccc} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I & \vdots & & R' & \\ & \gamma & & & \end{array}\right),$$

where R' is an $n-1$ by $n-1$ circulant matrix, is called a *bordered double circulant* code of length $2n$. These two families of codes are collectively called *double circulant* codes.

Lemma 2.4 *A double circulant code is isodual.*

Proof. Follows from Lemma 2.3. $\square$

quadratic

2.3 Symmetrized Weight Enumerators

We now investigate the symmetrized weight enumerators of isodual codes over $\mathbb{Z}_{2k}$. We obtain invariants to which the symmetrized weight enumerators belongs. First define the following matrix:

$$M_{2k} := \frac{1}{\sqrt{2k}} \begin{pmatrix} 1 & 2 & 2 & \cdots & 1 \\ 1 & \eta + \eta^{2k-1} & \eta^2 + \eta^{2k-2} & \cdots & \eta^k \\ 1 & \eta^2 + \eta^{2(2k-1)} & \eta^4 + \eta^{2(2k-2)} & \cdots & \eta^{2k} \\ 1 & \eta^3 + \eta^{3(2k-1)} & \eta^6 + \eta^{3(2k-2)} & \cdots & \eta^{3k} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \eta^k + \eta^{k(2k-1)} & \eta^{2k} + \eta^{k(2k-2)} & \cdots & \eta^{k^2} \end{pmatrix},$$

where η is a primitive $2k$-th root of unity. This matrix corresponds to the MacWilliams identities for codes over $\mathbb{Z}_{2k}$ [1]. In other words,

$$swe_C^{\perp}(x_0, x_1, \ldots, x_k) = M_{2k} swe_C(x_0, x_1, \ldots, x_k).$$

Thus the symmetrized weight enumerator of an isodual code is invariant under transformation by M_{2k}. By Lemma 2.1, if $2k$ is not a square then the symmetrized weight enumerator is also invariant under transformation by the diagonal matrix $N := \operatorname{diag}(-1, -1, \ldots, -1)$ derived from the restriction on the length. Therefore we have the following:

Proposition 2.5 *The symmetrized weight enumerator of an isodual code over $\mathbb{Z}_{2k}$ is invariant under the group generated by M_{2k}, which has order 2. Moreover if $2k$ is not a square then the symmetrized weight enumerator of an isodual code over $\mathbb{Z}_{2k}$ is invariant under the group generated by M_{2k} and N, which has order 4.*

Magma can easily be used to compute a basis for the invariant ring of small matrix groups. As examples, we give a basis for the invariant rings corresponding to the symmetrized weight enumerators of isodual codes over $\mathbb{Z}_4$ and $\mathbb{Z}_6$.

Corollary 2.6 *If C is an isodual code over $\mathbb{Z}_4$, then the symmetrized weight enumerator $swe_C(a, b, c)$ of C is an element of the ring*

$$\mathbb{C}[a + c, b - c, a^2 + 4bc - c^2],$$

with Molien series

$$\frac{1}{(1-\lambda)^2(1-\lambda^2)} = 1 + 2\lambda + 4\lambda^2 + 6\lambda^3 + 9\lambda^4 + \cdots.$$

Remark. The set of symmetrized weight enumerators of all isodual lattices over $\mathbb{Z}_4$ cannot generate the above ring since there is a unique isodual lattice of length 1.

Corollary 2.7 *If C is an isodual code over $\mathbb{Z}_6$, then the symmetrized weight enumerator $swe_C(a, b, c, d)$ of C is an element of the ring*

$$\mathbb{C}[\phi_{6,1}, \phi_{6,2}, \phi_{6,3}, \phi_{6,4}] \oplus \phi_{6,5}\mathbb{C}[\phi_{6,1}, \phi_{6,2}, \phi_{6,3}, \phi_{6,4}]$$
$$\oplus \phi_{6,6}\mathbb{C}[\phi_{6,1}, \phi_{6,2}, \phi_{6,3}, \phi_{6,4}] \oplus \phi_{6,7}\mathbb{C}[\phi_{6,1}, \phi_{6,2}, \phi_{6,3}, \phi_{6,4}]$$

with Molien series

$$\frac{1 + 2\lambda^2 + \lambda^4}{(1-\lambda^2)^4} = 1 + 6\lambda^2 + 19\lambda^4 + 44\lambda^6 + 85\lambda^8 + \cdots,$$

where

$$\begin{aligned}
\phi_{6,1} &= a^2+4bd+8c^2-12cd+5d^2,\\
\phi_{6,2} &= ab-cd,\\
\phi_{6,3} &= ac-bd-4c^2+6cd-2d^2,\\
\phi_{6,4} &= ad+b^2-4bd-3c^2+8cd-3d^2,\\
\phi_{6,5} &= ad-2bd+2cd-d^2,\\
\phi_{6,6} &= bc-bd-3c^2+5cd-2d^2,\\
\phi_{6,7} &= abcd-abd^2-3ac^2d+5acd^2-2ad^3-2b^2cd+2b^2d^2+8bc^2d\\
&\quad -13bcd^2+5bd^3-6c^3d+13c^2d^2-9cd^3+2d^4.
\end{aligned}$$

3 Construction of Isodual Lattices

In this section we recall some basic notions on lattices and recall the basic construction of lattices from codes. For details, we refer to [4], [1].

An n-dimensional lattice Λ in $\mathbb{R}^n$ is the set of integral linear combinations of n linearly independent vectors $v_1, \dots, v_n$. An n by n matrix whose rows generate Λ is called a generator matrix G of Λ. The determinant of Λ is the determinant of the Gram matrix GG^T of a generator matrix G of Λ. The *dual* lattice Λ^* of Λ is given by $\Lambda^* := \{x \in \mathbb{R}^n | [x,a] \in \mathbb{Z} \text{ for all } a \in \Lambda\}$ where $[x,a]$ is the standard inner product of x and a. The norm of x is $[x,x]$. A lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$. An integral lattice with $\Lambda = \Lambda^*$ is called *unimodular*. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ. The theta series $\Theta_\Lambda(q)$ of Λ is the formal power series

$$\Theta_\Lambda(q) := \sum_{x\in\Lambda} q^{[x,x]} = \sum_{m=0}^{\infty} N_m q^m,$$

where N_m is the number of the vectors of norm m. The kissing number is the second coefficient of the theta series.

lattice A lattice is said to be *isodual* if it is isometric to its dual lattice. This is a natural generalization of unimodular lattices, introduced in [5] where isodual lattices in small dimensions are studied.

In [9], H.-G. Quebbemann has introduced the notion of *modular lattice of level l*. Such a lattice L is caracterized by the following property: both L and $\sqrt{l}L^*$ are even lattices, and are isometric. Famous examples are the Coxeter-Todd lattice K_{12} of level 3 and dimension 12, and the Barnes-Wall lattice BW_{16} of level 2 and dimension 16. The rescaled lattice $l^{-1/4}L$ is then isodual.

isodual

Here we use a generalized "Construction A" to construct isodual lattices from our isodual codes. Construction A was first defined in [4] (see also [1] for the case of $\mathbb{Z}_{2k}$-codes).

First define the reduction modulo $2k$ $\rho : \mathbb{Z}^n \to \mathbb{Z}_{2k}^n$ by

$$\rho(x_1, \ldots, x_n) := (x_1 \pmod{2k}, \ldots, x_n \pmod{2k})$$

We set

$$A_{2k}(C) := \frac{1}{\sqrt{2k}}\{x \in \mathbb{Z}^n \mid \rho(x) \in C\}.$$

Lemma 3.1 *If C is an isodual code over $\mathbb{Z}_{2k}$ with minimum Euclidean weight d_E then $A_{2k}(C)$ is an isodual lattice with minimum norm* $\min\{d_E/2k, 2k\}$.

Proof. It is not difficult to show that $A_{2k}(C^\perp) = A_{2k}(C)^*$ for a code C over $\mathbb{Z}_{2k}$. A code-equivalent map from C to $C^\perp$ induces an isometry map from $A_{2k}(C)$ to $A_{2k}(C^\perp)$. Thus $A_{2k}(C)$ is isodual. The assertion about the minimum norm follows from [1]. $\square$

4 Double Circulant Codes and Their Lattices

In this section, we investigate the highest minimum norm of isodual lattices constructed from double circulant codes of length up to 24 over $\mathbb{Z}_4$ and $\mathbb{Z}_6$. For example, consider the double circulant code $D_{4,6}$ of length 6 over $\mathbb{Z}_4$ with 210 as the first row of R. This code has minimum Euclidean weight 6. Thus the isodual lattice $A_4(D_{4,6})$ constructed from $D_{4,6}$ by Construction A_4 has minimum norm $\frac{3}{2}$. The highest minimum norm among all known six-dimensional isodual lattices is $1 + \sqrt{\frac{1}{3}}$ $(= 1.5773\ldots)$ [5].

In Table 1, we present the first row of R or R' for double circulant codes over $\mathbb{Z}_4$ with the highest minimum Euclidean weight among all double circulant codes for each length up to 24. This was done by constructing all double circulant codes of that length. If the code is bordered, the values of (α, β, γ) are also given. Codes are given only for length $10 \leq 2n \leq 24$ because densest isodual lattices in dimensions up to 4 and 8 have been given in [5]. The fourth column of the table gives the minimum Euclidean weight d_E of the code.

It is known in [10] that the highest minimum Euclidean weight among all self-dual codes of lengths 10 and 16 over $\mathbb{Z}_4$ are 4 and 8, respectively. $D_{4,10}$ is an isodual code of length 10 with minimum Euclidean weight 8 and $D_{4,16}$ is an isodual code of length 16 with minimum Euclidean weight 9. Thus we have the following:

Proposition 4.1 *There exist isodual codes over $\mathbb{Z}_4$ which have a higher minimum Euclidean weight than any self-dual code of the same length.*

Table 1: Double Circulant Codes over $\mathbb{Z}_4$

Code	Length n	First Row	d_E
$D_{4,10}$	10	22100	8
$D_{4,12}$	12	221000	8
$D_{4,14}$	14	2210000	8
$D_{4,16}$	16	2312100 $(\alpha, \beta, \gamma) = (1, 2, 2)$	9
$D_{4,18}$	18	211200000	9
$D_{4,20}$	20	2112000000	10
$D_{4,22}$	22	31321121000	12
$D_{4,24}$	24	31321121000 $(\alpha, \beta, \gamma) = (1, 2, 2)$ (self-dual)	16

Double circulant codes over $\mathbb{Z}_6$ are given in Table 2. The first row of R or R' for codes with the highest minimum Euclidean weight are given for each length up to 24. If the code is bordered, the values of (α, β, γ) are also given. The fourth column of these tables gives the minimum Euclidean weight d_E of the code.

Table 2: Double Circulant Codes over $\mathbb{Z}_6$

Code	Length n	First Row	d_E
$D_{6,10}$	10	42100	10
$D_{6,12}$	12	513010	12
$D_{6,14}$	14	3321000	12
$D_{6,16}$	16	41431000	14
$D_{6,18}$	18	134010000	14
$D_{6,20}$	20	3013101000	16
$D_{6,22}$	22	35530010000	16
$D_{6,24}$	24	24313412010 $(\alpha, \beta, \gamma) = (3, 2, 2)$ (self-dual)	18

We next use these double circulant codes to construct dense isodual lattices by Construction A_{2k}. Let $\mu(D_{2k,2n})$ be the minimum norm of the isodual lattice $A_{2k}(D_{2k,2n})$ constructed from the double circulant code $D_{2k,2n}$. Let $\mu(2n) := \max\{\mu(D_{2k,2n}) \mid k = 2, 3\}$, that is, $\mu(2n)$ is the maximal number among the minimum norm of the lattices $A_{2k}(D_{2k,2n})$ where $k = 2, 3$ for each dimension $2n$.

In Table 3, we list $\mu(2n)$ for $10 \leq 2n \leq 24$, and the third column gives the double circulant code which provides $\mu(2n)$. The fourth and fifth columns list the highest minimum norms $\mu_K(2n)$ and $\mu_U(2n)$ among known isodual lattices and unimodular lattices, from [5], [11] and [3], respectively. Note that information on the highest minimum norm among isodual lattices in dimensions 17 to 22 is lacking in [5]. In that range of dimensions, the best known isodual lattices are in the family of modular lattices of level l. If such a lattice has minimum norm μ, then the corresponding idodual one has minimum norm $\mu/\sqrt{l}$. We refer to the survey [11] for information on lattices with parameters: $(n,l,\mu) = (12,3,4), (14,3,4), (16,2,4), (18,3,4), (20,7,8)$.

in lattice

Table 3: The Minimum Norm for Isodual Lattices from Double Circulant Codes

Dimension $2n$	$\mu(2n)$	Code	$\mu_K(2n)$	$\mu_U(2n)$
10	2	$D_{4,10}$	2	1
12	2	$D_{6,12}$	$\sqrt{16/3}$	2
14	2	$D_{4,14}, D_{6,14}$	$\sqrt{16/3}$	2
16	$\frac{7}{3}$	$D_{6,16}$	$\sqrt{8}$	2
18	$\frac{7}{3}$	$D_{6,18}$	$\sqrt{16/3}$	2
20	$\frac{7}{3}$	$D_{6,20}$	$8/\sqrt{7}$	2
22	3	$D_{4,22}$	$\sqrt{16/3}$	2
24	4	$D_{4,24}$	4	4

From Table 3, note the following:

Proposition 4.2 *There is a 22-dimensional isodual lattice with minimum norm 3.*

It appears that $A_4(D_{4,22})$ is the first example of an isodual lattice with minimum norm 3 in dimension 22. Isodual lattices in dimensions 23 and 24 with minimum norm 3 are known, namely the shorter Leech lattice and the odd Leech lattice. Thus $A_4(D_{4,22})$ is the smallest known isodual lattice with minimum norm 3.

The theta series $\Theta_{A_4(C)}(q)$ of the lattice constructed from a code C over $\mathbb{Z}_4$ can be obtained from the symmetrized weight enumerator $swe_C(a,b,c)$ of C by replacing a, b and c respectively by $\sum_{x\in 4\mathbb{Z}} q^{x^2/4}$, $\sum_{x\in 4\mathbb{Z}+1} q^{x^2/4}$ and $\sum_{x\in 4\mathbb{Z}+2} q^{x^2/4}$. The symmetrized weight enumerator $swe_{D_{4,22}}$ and the theta series $\Theta_{A_4(D_{4,22})}(q)$ of $A_4(D_{4,22})$ are given below.

$$\begin{aligned} swe_{D_{4,22}} \;=\; & a^{22} + 1232a^{10}b^{12} + 5632a^7b^{15} + 2464a^6b^{16} + 616a^{13}b^8c + 14784a^{10}b^{11}c \\ & +12320a^9b^{12}c + 14784a^5b^{16}c + 2464a^{13}b^7c^2 + 4004a^{12}b^8c^2 + 55440a^8b^{12}c^2 \\ & +118272a^5b^{15}c^2 + 36960a^4b^{16}c^2 + 14784a^{11}b^8c^3 + 221760a^8b^{11}c^3 + 147840a^7b^{12}c^3 \\ & +49280a^3b^{16}c^3 + 29568a^{11}b^7c^4 + 40656a^{10}b^8c^4 + 258720a^6b^{12}c^4 + 197120a^3b^{15}c^4 \\ & +36960a^2b^{16}c^4 + 83160a^9b^8c^5 + 620928a^6b^{11}c^5 + 310464a^5b^{12}c^5 + 14784ab^{16}c^5 \\ & +110880a^9b^7c^6 + 124740a^8b^8c^6 + 258720a^4b^{12}c^6 + 39424ab^{15}c^6 + 2464b^{16}c^6 \end{aligned}$$

$$
\begin{aligned}
&+176a^{15}c^7 + 140800a^7b^8c^7 + 443520a^4b^{11}c^7 + 147840a^3b^{12}c^7 + 330a^{14}c^8\\
&+140800a^7b^7c^8 + 123200a^6b^8c^8 + 55440a^2b^{12}c^8 + 83160a^5b^8c^9 + 73920a^2b^{11}c^9\\
&+12320ab^{12}c^9 + 66528a^5b^7c^{10} + 41580a^4b^8c^{10} + 1232b^{12}c^{10} + 672a^{11}c^{11}\\
&+14784a^3b^8c^{11} + 1344b^{11}c^{11} + 616a^{10}c^{12} + 9856a^3b^7c^{12} + 3696a^2b^8c^{12}\\
&+616ab^8c^{13} + 352ab^7c^{14} + 44b^8c^{14} + 176a^7c^{15} + 77a^6c^{16},
\end{aligned}
$$

$$
\begin{aligned}
\Theta_{A_4(D_{4,22})}(q) &= 1 + 2464q^3 + 45056q^{15/4} + 43164q^4 + 394240q^5\\
&+3198976q^{23/4} + 2444288q^6 + 11470272q^7 + 63393792q^{31/4}\\
&+43584860q^8 + 141182976q^9 + 629342208q^{39/4} + 404963328q^{10}\\
&+1052468320q^{11} + 4066979840q^{47/4} + 2512336288q^{12}\\
&+5583148032q^{13} + \cdots.
\end{aligned}
$$

Define the *Euclidean weight enumerator* $E_C(s)$ of a code C as $E_C(s) := \sum_{c\in C} s^{wt_E(c)}$. To save space, we only list the first few terms in the Euclidean weight enumerators for $D_{6,18}$ and $D_{6,20}$. Note that $A_6(D_{6,18})$ and $A_4(D_{4,22})$ have higher minimum norms than $\mu_K(18)$ and $\mu_K(22)$, respectively.

$$
\begin{aligned}
E_{D_{6,18}}(s) &= 1 + 288s^{14} + 792s^{16} + 1338s^{18} + 3618s^{20} + 7380s^{22} + 13134s^{24} + 23094s^{26}\\
&+37188s^{28} + 61116s^{30} + 84636s^{32} + 126846s^{34} + 174719s^{36} + 214380s^{38}\\
&+287478s^{40} + 354702s^{42} + 394758s^{44} + 468576s^{46} + 536778s^{48} + 548208s^{50}\\
&+603450s^{52} + 620793s^{54} + 607104s^{56} + 626058s^{58} + 581064s^{60} + 549414s^{62}\\
&+519462s^{64} + 456912s^{66} + 408510s^{68} + 357174s^{70} + 293511s^{72} + \cdots,\\
\Theta_{A_6(D_{6,18})}(q) &= 1 + 288q^{7/3} + 810q^{8/3} + 1356q^3 + 4032q^{10/3} + 8298q^{11/3}\\
&+15762q^4 + 30870q^{13/3} + 54216q^{14/3} + 95604q^5 + 160218q^{16/3}\\
&+266112q^{17/3} + 414794q^6 + 627786q^{19/3} + 980604q^{20/3} + \cdots.
\end{aligned}
$$

As described in Section 2, the supplemented quadratic residue code QR_{17} over $\mathbb{Z}_4$ of length 17 has minimum Euclidean weight 8. Thus this code gives an isodual lattice with minimum norm 2 in dimension 17.

5 Classification of Double Circulant Codes of Length 22 and Some 3-Designs

In this section, we classify the double circulant codes of length 22 over $\mathbb{Z}_4$ with minimum Euclidean weight 12. We also show that some of these codes contain 3-designs with parameters $(22, 7, 4)$, $(22, 8, 12)$, $(22, 9, 84)$ and $(22, 10, 156)$.

The following lemma is useful in classifying double circulant codes.

Lemma 5.1 *If the matrix* $(I \ , \ A)$ *generates an isodual code* C *over* $\mathbb{Z}_{2k}$*, then the matrices* $(I \ , \ -A)$*,* $(I \ , \ A^T)$ *and* $(I \ , \ -A^T)$ *generate isodual codes which are equivalent to* C*.*

Proof. Since C is isodual, the matrices $(I \ , \ A)$ and $(I \ , \ -A^T)$ generate equivalent codes. Obviously $(I \ , \ A)$ and $(I \ , \ -A)$ also generate equivalent codes. □

By exhaustive search, we have found all distinct double circulant codes of length 22 over $\mathbb{Z}_4$ with minimum Euclidean weight 12. This was done by considering all 11 by 11 (resp. 10 by 10) circulant matrices over $\mathbb{Z}_4$ for pure (resp. bordered) double circulant codes. Lemma 5.1 establishes the equivalence of a large number of these codes. To save space, Table 4 lists only those codes which must be checked further for equivalence to complete the classification. The symmetrized weight enumerators (column SWE) are also identified in the table, and these are listed at the end of this section. Note that $C_{1,1}$ is the same as $D_{4,22}$.

Table 4: Double Circulant Codes of Length 22

Code	First row of R	SWE	Code	First row of R	SWE
$C_{1,1}$	31321121000	$swe_{D_{4,22}}(a,b,c)$	$C_{1,2}$	21330112100	$swe_{D_{4,22}}(a,b,c)$
$C_{1,3}$	20311231010	$swe_{D_{4,22}}(a,b,c)$	$C_{1,4}$	32021310110	$swe_{D_{4,22}}(a,b,c)$
$C_{1,5}$	31032201110	$swe_{D_{4,22}}(a,b,c)$	$C_{1,6}$	23312110100	$swe_{D_{4,22}}(a,b,c)$
$C_{1,7}$	23211031100	$swe_{D_{4,22}}(a,b,c)$	$C_{1,8}$	23011211300	$swe_{D_{4,22}}(a,b,c)$
$C_{1,9}$	22131031010	$swe_{D_{4,22}}(a,b,c)$	$C_{1,10}$	20121303110	$swe_{D_{4,22}}(a,b,c)$
$C_{1,11}$	13212223110	$swe_{D_{4,22}}(a,b,c)$	$C_{1,12}$	22333231210	$swe_{D_{4,22}}(a,b,c)$
$C_{1,13}$	31231122210	$swe_{D_{4,22}}(a,b,c)$	$C_{1,14}$	22123121310	$swe_{D_{4,22}}(a,b,c)$
$C_{1,15}$	21233211120	$swe_{D_{4,22}}(a,b,c)$	$C_{2,1}$	31333321111	$swe_{C_{2,1}}(a,b,c)$
$C_{2,2}$	33113332111	$swe_{C_{2,1}}(a,b,c)$	$C_{2,3}$	31313133211	$swe_{C_{2,1}}(a,b,c)$
$C_{2,4}$	31133133211	$swe_{C_{2,1}}(a,b,c)$	$C_{2,5}$	33131231311	$swe_{C_{2,1}}(a,b,c)$
$C_{3,1}$	33331231111	$swe_{C_{3,1}}(a,b,c)$	$C_{3,2}$	31313332111	$swe_{C_{3,1}}(a,b,c)$
$C_{3,3}$	32133313111	$swe_{C_{3,1}}(a,b,c)$	$C_{3,4}$	33131133211	$swe_{C_{3,1}}(a,b,c)$
$C_{3,5}$	32133131311	$swe_{C_{3,1}}(a,b,c)$	$C_{4,1}$	33313213111	$swe_{C_{4,1}}(a,b,c)$

Let R and R' be two square matrices of the same order. If there are $(0, 1, -1)$-monomial matrices P and Q such that $R = PR'Q$, then $(I \ , \ R)$ and $(I \ , \ R')$ generate equivalent codes over $\mathbb{Z}_{2k}$. For the codes in Table 4, let $R_{i,j}$ be R in the generator matrix of $C_{i,j}$. Permutation matrices P_j and Q_j can be found such that $R_{1,j} = P_j R_{1,j+1} Q_j$ for $j = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13$ and 14. Thus the codes $C_{1,i}$ $(i = 1, 2, 3, 4, 5)$ are equivalent, the codes $C_{1,i}$ $(i = 6, 7, 8, 9, 10)$ are equivalent, and the codes $C_{1,i}$ $(i = 11, 12, 13, 14, 15)$ are equivalent. Similarly, it can be shown that the codes $C_{2,i}$ $(i = 1, 2, 3, 4, 5)$ are equivalent and the codes $C_{3,i}$ $(i = 1, 2, 3, 4, 5)$ are equivalent. Note that $C_{4,1}$ is the unique double circulant code with $swe_{C_{4,1}}(a, b, c)$.

It is now shown that $C_{1,1}$, $C_{1,6}$ and $C_{1,11}$ are inequivalent using the methods in [6] and [7]. Let C be a code of length $2n$. Let $M_t := (m_{ij})$ be the A_t by $2n$ matrix with rows composed of the codewords of Hamming weight t in C, where A_i denotes the number of codewords of Hamming weight i in C. For an integer k $(1 \le k \le 2n)$, let $n_t(j_1, \dots, j_k)$ be the number of r $(1 \le r \le A_t)$ such that $m_{rj_1} \cdots m_{rj_k} \neq 0$ over $\mathbb{Z}$ for $1 \le j_1 < \cdots < j_k \le 2n$. We consider the set

$$S_t := \{n_t(j_1, \dots, j_k) | \text{ for any } k \text{ distinct columns } j_1, \dots, j_k \ \}.$$

Let $M_t(k)$ and $m_t(k)$ be the maximal and minimal numbers in S_t, respectively. Since two equivalent codes over $\mathbb{Z}_4$ have the same values for S_t, these numbers are invariant under the equivalence of codes. Table 5 gives some values of $M_t(k)$ and $m_t(k)$ for codes $C_{1,1}$, $C_{1,6}$ and $C_{1,11}$.

Now let $c_{i,1}, c_{i,2}, \dots, c_{i,A_i}$ be the codewords of Hamming weight i in C. Let

$$d_i(j) := \#\{wt(c_{i,k_1} - c_{i,k_2}) = j \mid 1 \le k_1 < k_2 \le A_i\},$$

where $wt(x)$ denotes the Hamming weight of a vector x. The numbers $d_i(j)$ are also invariant under the equivalence of codes for any i and j. Table 6 gives some values of $d_i(j)$ for codes $C_{1,1}$ and $C_{1,6}$.

Table 5: Inequivalence values for $C_{1,1}$ and $C_{1,11}$

Code	$M_9(3)$	$m_9(3)$	$M_9(4)$	$m_9(4)$	$M_{10}(3)$	$m_{10}(3)$	$M_{10}(4)$	$m_{10}(4)$
$C_{1,1}$	168	168	60	44	312	312	124	108
$C_{1,6}$	168	168	60	44	312	312	124	108
$C_{1,11}$	168	168	60	42	312	312	126	108

From Tables 5 and 6, $C_{1,1}$, $C_{1,6}$ and $C_{1,11}$ are inequivalent, and this completes the classification.

Proposition 5.2 *There are exactly six inequivalent double circulant codes of length* 22 *over* $\mathbb{Z}_4$ *with minimum Euclidean weight* 12.

Remark. We denote the six inequivalent double circulant codes $C_{1,1}$, $C_{1,6}$, $C_{1,11}$, $C_{2,1}$, $C_{3,1}$ and $C_{4,1}$ by $C_{22}^1, \dots, C_{22}^5$ and C_{22}^6, respectively.

A t-(v, k, λ) design D is a set of v points with a collection of k-subsets called blocks, so that any t-points are contained in exactly λ blocks. The incidence matrix of D is the

Table 6: Inequivalence values for $C_{1,1}$ and $C_{1,6}$

Code	$d_9(0)$	$d_9(1)$	$d_9(2)$	$d_9(3)$	$d_9(4)$	$d_9(5)$	$d_9(6)$	$d_9(7)$
$C_{1,1}$	0	0	0	0	0	0	0	8624
$C_{1,6}$	0	0	0	0	0	0	0	8624
Code	$d_9(8)$	$d_9(9)$	$d_9(10)$	$d_9(11)$	$d_9(12)$	$d_9(13)$	$d_9(14)$	$d_9(15)$
$C_{1,1}$	7700	143616	219824	657712	837760	761376	1215896	509168
$C_{1,6}$	7700	144672	219384	655952	837320	762432	1217480	508640
Code	$d_9(16)$	$d_9(17)$	$d_9(18)$	$d_9(19)$	$d_9(20)$	$d_9(21)$	$d_9(22)$	
$C_{1,1}$	292688	85888	1408	0	0	0	0	
$C_{1,6}$	292072	86064	1320	0	0	0	0	

matrix $M = (m_{ij})$ with $m_{ij} = 1$ if the j-th point is contained in the i-th block and $m_{ij} = 0$ otherwise. A design may be identified by its incidence matrix. Two designs are isomorphic if the incidence matrix of one design can be obtained from the incidence matrix of the other by permuting its rows and columns.

Corollary 5.3 *The supports of Hamming weights* 7, 8, 9 *and* 10 *in* $C_{1,1}$, $C_{1,6}$ *and* $C_{1,11}$ *form* 3-*designs with parameters* $(22, 7, 4)$, $(22, 8, 12)$, $(22, 9, 84)$ *and* $(22, 10, 156)$, *respectively.*

Proof. Let C be one of $C_{1,1}$, $C_{1,6}$ and $C_{1,11}$. The residue code $C^{(1)}$ and the torsion code $C^{(2)}$ of C are $\{c \pmod 2 \,|\, c \in C\}$ and $\{c/2 \,|\, c \equiv 0 \pmod 2, c \in C\}$, respectively. It is easy to see that $C^{(1)} = C^{(2)}$ and $C^{(1)}$ is the binary isodual $[22, 11, 7]$ code B which has the Mathieu group M_{22} as its automorphism group. From $swe_C(a, b, c)$, the codewords of Hamming weights 7 and 8 are in $C^{(2)}$. It is known that the codewords of Hamming weights 7 and 8 in B form a 3-$(22, 7, 4)$ design and a 3-$(22, 8, 12)$ design, respectively. Thus the supports of Hamming weights 7 and 8 in C form a 3-$(22, 7, 4)$ design and a 3-$(22, 8, 12)$ design, respectively.

Let x be a codeword in C of Hamming weight 9 (resp. 10). Then it follows from $swe_C(a, b, c)$ that $3x$ is a codeword of Hamming weight 9 (resp. 10), but $2x$ is not. Thus Table 5 shows that the supports of Hamming weight 9 and 10 in C form a 3-$(22, 9, 84)$ design and a 3-$(22, 10, 156)$ design without repeated blocks, respectively. □

Now we prove that the codes C_{22}^i $(i = 1, \ldots, 6)$ are closely related to extremal Type II codes of length 24 and that $A_4(C_{22}^i)$ are closely related to the Leech lattice where C_{22}^i are the six inequivalent double circulant codes in Proposition 5.2.

Let C_{22} be any of C_{22}^i $(i = 1, \ldots, 6)$.

Lemma 5.4 *Let* G_{22} *be the generator matrix* $(\ I\ ,\ R_{22}\ )$ *of* C_{22}. *Then* $R_{22}R_{22}^T = 3J - I$ *where* J *is the all-ones matrix.*

The following matrix

$$G_{23} := \begin{pmatrix} & & & 1 \\ & G_{22} & & \vdots \\ & & & 1 \\ 2 & \cdots & 2 & 2 \end{pmatrix},$$

generates a self-orthogonal code C_{23} of length 23. Since C_{22} does not contain the all-2's vector $(2, 2, 2, \ldots, 2)$, C_{23} is self-dual. The symmetrized weight enumerator of the self-orthogonal code C'_{23} generated by the first eleven rows in G_{23} can be obtained from the symmetrized weight enumerator of C_{22}, since the Euclidean weight of the codewords in C'_{23} must be divisible by 4. For any vector x over $\mathbb{Z}_4$, $n_0(x + 2\mathbf{j}) = n_2(x)$, $n_1(x + 2\mathbf{j}) = n_3(x)$, $n_2(x + 2\mathbf{j}) = n_0(x)$ and $n_3(x + 2\mathbf{j}) = n_1(x)$ where $2\mathbf{j}$ is the all-2's vector. Hence the symmetrized weight enumerator of C_{23} can be obtained directly from $swe_{C_{22}}(a, b, c)$. The minimum Euclidean weight of C_{23} is 12. The following matrix

$$G_{24} := \begin{pmatrix} & & & 10 \\ & G_{22} & & \vdots \\ & & & 10 \\ 1 & \cdots & 1 & 11 \end{pmatrix},$$

generates a Type II code C_{24} of length 24, i.e., a self-dual code with all Euclidean weights divisible by 8.

Proposition 5.5 *C_{24} is a Type II code of length 24 with minimum Euclidean weight 16, and so is extremal.*

Proof. Let C'_{24} be the bordered double circulant code with $R' = R_{22}$ and borders $(\alpha, \beta, \gamma) = (2, 3, 1)$. It is easy to see that C'_{24} is a Type II code. All extremal Type II double circulant codes of length 24 have been classified in [6], and the list in [6] shows that C'_{24} is an extremal Type II double circulant code. The lemma follows from the fact that C_{24} and C'_{24} are equivalent. $\square$

Remark. For codes C^1_{22}, C^2_{22} and C^3_{22} of length 22, the supports of Hamming weight 10 in the corresponding bordered double circulant codes of length 24 form 5-$(24, 10, 36)$ designs [6]. The 3-$(22, 9, 84)$ and 3-$(22, 10, 156)$ designs found in Corollary 5.3 are the derived and residual designs, respectively, of the 4-$(23, 10, 84)$ designs which are the residual designs of the above 5-designs.

By the above proposition, $A_4(C_{23})$ (resp. $A_4(C_{24})$) is the unique extremal unimodular lattice in dimension 23 (resp. 24), which is called the shorter Leech lattice (resp. the Leech lattice). Thus the 22-dimensional isodual lattices $A_4(C_{22})$ are related to the Leech lattice.

$$
\begin{aligned}
swe_{C_{2,1}} &= a^{22}+1408a^{10}b^{12}+7040a^{6}b^{16}+5632a^{2}b^{20}+176a^{13}b^{8}c+22528a^{10}b^{11}c\\
&+8448a^{9}b^{12}c+28160a^{5}b^{16}c+11264ab^{20}c+176a^{16}b^{4}c^{2}+3872a^{12}b^{8}c^{2}\\
&+43648a^{8}b^{12}c^{2}+77440a^{4}b^{16}c^{2}+5632b^{20}c^{2}+352a^{15}b^{4}c^{3}\\
&+13728a^{11}b^{8}c^{3}+337920a^{8}b^{11}c^{3}+107008a^{7}b^{12}c^{3}+112640a^{3}b^{16}c^{3}+55a^{18}c^{4}\\
&+1584a^{14}b^{4}c^{4}+44704a^{10}b^{8}c^{4}+191488a^{6}b^{12}c^{4}+77440a^{2}b^{16}c^{4}+2816a^{13}b^{4}c^{5}\\
&+84304a^{9}b^{8}c^{5}+946176a^{6}b^{11}c^{5}+242176a^{5}b^{12}c^{5}+28160ab^{16}c^{5}+8272a^{12}b^{4}c^{6}\\
&+120384a^{8}b^{8}c^{6}+191488a^{4}b^{12}c^{6}+7040b^{16}c^{6}+13728a^{11}b^{4}c^{7}+141504a^{7}b^{8}c^{7}\\
&+675840a^{4}b^{11}c^{7}+107008a^{3}b^{12}c^{7}+330a^{14}c^{8}+18128a^{10}b^{4}c^{8}+120384a^{6}b^{8}c^{8}\\
&+43648a^{2}b^{12}c^{8}+22528a^{9}b^{4}c^{9}+84304a^{5}b^{8}c^{9}+112640a^{2}b^{11}c^{9}+8448ab^{12}c^{9}\\
&+18128a^{8}b^{4}c^{10}+44704a^{4}b^{8}c^{10}+1408b^{12}c^{10}+1024a^{11}c^{11}+13728a^{7}b^{4}c^{11}\\
&+13728a^{3}b^{8}c^{11}+2048b^{11}c^{11}+462a^{10}c^{12}+8272a^{6}b^{4}c^{12}+3872a^{2}b^{8}c^{12}\\
&+2816a^{5}b^{4}c^{13}+176ab^{8}c^{13}+1584a^{4}b^{4}c^{14}+352a^{3}b^{4}c^{15}+165a^{6}c^{16}\\
&+176a^{2}b^{4}c^{16}+11a^{2}c^{20}\\
swe_{C_{3,1}} &= a^{22}+1056a^{10}b^{12}+7040a^{6}b^{16}+5632a^{2}b^{20}+528a^{13}b^{8}c+22528a^{10}b^{11}c\\
&+7744a^{9}b^{12}c+28160a^{5}b^{16}c+11264ab^{20}c+88a^{16}b^{4}c^{2}+4576a^{12}b^{8}c^{2}\\
&+44704a^{8}b^{12}c^{2}+77440a^{4}b^{16}c^{2}+5632b^{20}c^{2}+176a^{15}b^{4}c^{3}+13024a^{11}b^{8}c^{3}\\
&+337920a^{8}b^{11}c^{3}+109824a^{7}b^{12}c^{3}+112640a^{3}b^{16}c^{3}+55a^{18}c^{4}+1672a^{14}b^{4}c^{4}\\
&+42592a^{10}b^{8}c^{4}+190784a^{6}b^{12}c^{4}+77440a^{2}b^{16}c^{4}+3168a^{13}b^{4}c^{5}+83952a^{9}b^{8}c^{5}\\
&+946176a^{6}b^{11}c^{5}+237952a^{5}b^{12}c^{5}+28160ab^{16}c^{5}+8536a^{12}b^{4}c^{6}+121792a^{8}b^{8}c^{6}\\
&+190784a^{4}b^{12}c^{6}+7040b^{16}c^{6}+13904a^{11}b^{4}c^{7}+142912a^{7}b^{8}c^{7}+675840a^{4}b^{11}c^{7}\\
&+109824a^{3}b^{12}c^{7}+330a^{14}c^{8}+17864a^{10}b^{4}c^{8}+121792a^{6}b^{8}c^{8}+44704a^{2}b^{12}c^{8}\\
&+21824a^{9}b^{4}c^{9}+83952a^{5}b^{8}c^{9}+112640a^{2}b^{11}c^{9}+7744ab^{12}c^{9}+17864a^{8}b^{4}c^{10}\\
&+42592a^{4}b^{8}c^{10}+1056b^{12}c^{10}+1024a^{11}c^{11}+13904a^{7}b^{4}c^{11}+13024a^{3}b^{8}c^{11}\\
&+2048b^{11}c^{11}+462a^{10}c^{12}+8536a^{6}b^{4}c^{12}+4576a^{2}b^{8}c^{12}+3168a^{5}b^{4}c^{13}\\
&+528ab^{8}c^{13}+1672a^{4}b^{4}c^{14}+176a^{3}b^{4}c^{15}+165a^{6}c^{16}+88a^{2}b^{4}c^{16}+11a^{2}c^{20}\\
swe_{C_{4,1}} &= a^{22}+704a^{10}b^{12}+7040a^{6}b^{16}+5632a^{2}b^{20}+880a^{13}b^{8}c+22528a^{10}b^{11}c\\
&+7040a^{9}b^{12}c+28160a^{5}b^{16}c+11264ab^{20}c+5280a^{12}b^{8}c^{2}+45760a^{8}b^{12}c^{2}\\
&+77440a^{4}b^{16}c^{2}+5632b^{20}c^{2}+12320a^{11}b^{8}c^{3}+337920a^{8}b^{11}c^{3}+112640a^{7}b^{12}c^{3}\\
&+112640a^{3}b^{16}c^{3}+55a^{18}c^{4}+1760a^{14}b^{4}c^{4}+40480a^{10}b^{8}c^{4}+190080a^{6}b^{12}c^{4}\\
&+77440a^{2}b^{16}c^{4}+3520a^{13}b^{4}c^{5}+83600a^{9}b^{8}c^{5}+946176a^{6}b^{11}c^{5}+233728a^{5}b^{12}c^{5}\\
&+28160ab^{16}c^{5}+8800a^{12}b^{4}c^{6}+123200a^{8}b^{8}c^{6}+190080a^{4}b^{12}c^{6}+7040b^{16}c^{6}\\
&+14080a^{11}b^{4}c^{7}+144320a^{7}b^{8}c^{7}+675840a^{4}b^{11}c^{7}+112640a^{3}b^{12}c^{7}+330a^{14}c^{8}\\
&+17600a^{10}b^{4}c^{8}+123200a^{6}b^{8}c^{8}+45760a^{2}b^{12}c^{8}+21120a^{9}b^{4}c^{9}+83600a^{5}b^{8}c^{9}\\
&+112640a^{2}b^{11}c^{9}+7040ab^{12}c^{9}+17600a^{8}b^{4}c^{10}+40480a^{4}b^{8}c^{10}+704b^{12}c^{10}\\
&+1024a^{11}c^{11}+14080a^{7}b^{4}c^{11}+12320a^{3}b^{8}c^{11}+2048b^{11}c^{11}+462a^{10}c^{12}\\
&+8800a^{6}b^{4}c^{12}+5280a^{2}b^{8}c^{12}+3520a^{5}b^{4}c^{13}+880ab^{8}c^{13}+1760a^{4}b^{4}c^{14}\\
&+165a^{6}c^{16}+11a^{2}c^{20}.
\end{aligned}
$$

6 Uniqueness of the six lattices $A_4(C_{22}^i)$

Let C_{22}^i $(i = 1, \dots, 6)$ be the six inequivalent double circulant codes in Proposition 5.2. In this section, we show that the lattices $A_4(C_{22}^i)$ are all isometric to some lattice L_{22} constructed below. L_{22} is constructed from the unique binary self-dual $[22, 11, 6]$ code (also called the shorter Golay code [10]) in a very similar way as the Leech lattice is constructed from the binary Golay code. L_{22} is not unimodular, but has a higher minimum norm than the unimodular lattices, and its automorphism group is not larger than the group arising from the automorphism group of the code.

Let C be the unique binary self-dual $[22, 11, 6]$ code, and let $U_{22} := A_2(C)$ be the unimodular lattice constructed from C by Construction A. Recall that the automorphism group of the code C is the group $M_{22}.2$. Now consider the sublattice

$$N_{22} := B_2(C) := \{(x_1, \dots, x_{22}) \in U_{22} \mid \sum_{i=1}^{22} x_i \equiv 0 \pmod 4\}$$

of index 2 in U_{22} obtained by Construction B (see [3] for Constructions A and B). N_{22} no longer contains roots and has minimum norm 3. Set

$$L_{22} := N_{22} + \mathbb{Z}x$$

where $x = (1/2, \dots, 1/2, 5/2) - 2s$, the coordinates of s are 0 or 1, and $s \pmod 2$ belongs to the shadow of C (see [4] for the shadows of binary self-dual codes).

Theorem 6.1 *Let L_{22} and U_{22} be as above. Then we have:*

(1) L_{22} is an isodual lattice with minimum norm 3, and $Aut(L_{22}) \simeq \{\pm 1\}^{11}.M_{22}.2$ is a subgroup of the automorphism group of the lattice U_{22}.

(2) Any 22-dimensional isodual lattice of minimum norm 3, containing an integral lattice of determinant 4, is isometric to L_{22}.

Proof. Let $e_i := (0, \dots, 0, 1, 0, \dots, 0)$ for all i, where the 1 stands at coordinate i. Clearly, $\mathrm{Aut}(U_{22}) = \{\pm 1\}^{22}.\mathrm{Aut}(C)$ since the only roots of U_{22} are $\pm 2e_i$. Let $e := (1, \dots, 1) = \sum_{i=1}^{22} e_i$. Then $N_{22} = (U_{22})_e := \{x \in U_{22} \mid [u, e] \equiv 0 \pmod 2\}$ and $N_{22}^* = U_{22} + \mathbb{Z}e/2$. Since $e/2$ has norm 11/42, the minimum norm of N_{22}^* is 2 and its norm 2 vectors are the ones in U_{22}. Hence $\mathrm{Aut}(N_{22})$ induces a permutation of them and $\mathrm{Aut}(N_{22}) \simeq \{\pm 1\}^{11}.\mathrm{Aut}(C)$ since the sign changes preserving N_{22} are in one-to-one correspondence with the elements of C.

We consider lattices of the form $L := N_{22} + \mathbb{Z}w/2$, where $w \in N_{22}$ is defined modulo $2N_{22}$. We search for lattices L such that L and L^* both have minimum norm 3.

Lemma 6.2 *There is a unique class $\overline{w} \in N_{22}/2N_{22}$ such that L and L^* have minimum norm* 3.

Proof. Since $\pm 4e_i \pm 4e_j$ and $\pm 8e_i$ belong to $2N_{22}$, the 21 first coordinates of w can be taken in $\{0, \pm 1, 2\}$ while $w_{22} \in \{0, \pm 1, \pm 2, \pm 3, 4\}$. If one coordinate w_i of w is even, since $[2e_i, w/2] = w_i/2 \in \mathbb{Z}$, $2e_i \in L^*$ which contradicts the condition that the minimum norm of L^* is 3. Hence we can assume $w_i \in \{\pm 1\}$ for $1 \leq i \leq 21$ and $w_{22} \in \{\pm 1, \pm 3\}$. Moreover, if $w_{22} = \pm 1$, $w^2 = 11$ and the minimum norm of L is smaller than 3. Hence $w_{22} = \pm 3$, and the minimum norm of L is 3 if and only if w is minimal in its class $w + 2N_{22}$. If this is so, we notice that since $w^2/4 = 15/43$, the minimal vectors of L will be the ones of N_{22}, and hence that $\mathrm{Aut}(L) \subset \mathrm{Aut}(N_{22})$. For convenience, we assume now that $w_{22} \in \{3, 5\}$. Hence we can write $w = w(u) := e - 2\sum_{i \in u} e_i + 4e_{22}$ where $u \in \mathbb{F}_2^{22}$ is identified with its set of non-zero coordinates. It is worth noticing here that $w(u) \in N_{22}$ if and only if $2wt_H(u) \equiv 22 \pmod 4$ and $w(u) \equiv w(u_1) \pmod{2N_{22}}$ if and only if $u \equiv u_1 \pmod C$ and $wt_H(u) \equiv wt_H(u_1) \pmod 4$. □

Lemma 6.3 *Let w be as above. The class $w + 2N_{22}$ has minimum norm* 15 *if and only if u belongs to the shadow of C.*

Proof. As mentioned previously, the minimum norm of the class $w + 2N_{22}$ is lower than 15 if and only if it contains an element with coordinates ± 1, i.e. of the type $w' = e - 2\sum_{i \in u'} e_i$ where $u' \in \mathbb{F}_2^{22}$. Then $w' \in N_{22}$ if and only if $wt_H(u') \equiv 1 \pmod 2$, and $w' \in w + 2N_{22}$ if and only if $\sum_{i \in u'} e_i - \sum_{i \in u} e_i + 2e_{22} \in N_{22}$. This last condition is equivalent to the two conditions: $u' + u \in C$ and $wt_H(u') + wt_H(u) + 2 \equiv 0 \pmod 4$. By setting $c := u' + u$, we get $c \in C$ and $wt_H(c) + 2c \cdot u \equiv 2 \pmod 4$. Hence, such a codeword does not exist if and only if u is in the shadow of C. Note that in this case, $2wt_H(u) \equiv 22 \pmod 8$, which insures that $w \in N_{22}$. Now two elements of the shadow are congruent modulo C and define a single class modulo $2N_{22}$ from previous remarks. □

We have proved the two lemmas, and the fact that the minimum norm of L_{22} is 3. We have already seen that $\mathrm{Aut}(L_{22})$ is a subgroup of $\mathrm{Aut}(N_{22})$. Since the class of $N_{22}/2N_{22}$ is the unique one such that L and L^* have minimum norm 3, it is preserved by $\mathrm{Aut}(N_{22})$ and hence we have equality.

Now we prove that L_{22}^* has minimum norm 3. Since $L_{22} = N_{22} + \mathbb{Z}w/2$, ($w = w(u)$, u in the shadow of C), $L_{22}^* = (N_{22}^*)_w = (U_{22})_w \cup (U_{22} + e/2)_w$. Elements of norm lower than 3 in this lattice can only have the form $x = e/2 - \sum_{i \in u'} e_i$ with $u' \in C$ and the same computation shows that $[x, w] \equiv wt_H(u)/2 + u' \cdot u + 1 \equiv 1 \pmod 2$ and hence that x does not belong to L_{22}^*.

Let P be a 22-dimensional lattice of determinant 1 such that P and P^* have minimum norm 3, and containing an integral sublattice N with index 2. We shall prove that P is isometric to L_{22}. Since N is integral, the quotient group N^*/N has order 4 and contains a subgroup of order 2 corresponding to an integral lattice U. Hence $N \subset U \subset N^*$ and U is unimodular. The lattice U contains at most one norm 1 vector and can contain norm 2 vectors only if they are pairwise orthogonal (because, if $x_1, x_2 \in U$, $x_1 \pm x_2 \in N$ which has minimum norm 3). A look at the classification of 22-dimensional unimodular lattices (cf. [3, Chapter 16]) shows that the only possibility is $U \simeq U_{22}$. Hence $N \simeq N_{22}$ which is the only sublattice (up to isometry) of index 2 of U_{22} not containing roots. The previous discussion shows then that $P \simeq L_{22}$.

The last assertion to prove is that L_{22} is isodual. Since L_{22}^* contains U_w which is an integral sublattice of index 2, we can take $P = L_{22}^*$ and conclude that $L_{22}^* \simeq L_{22}$. Therefore the theorem follows. □

Remark. More precisely, the lattices U_w and N_{22} are exchanged by an automorphism of U of type $(x_1, \ldots, x_{22}) \to (\epsilon_1 x_1, \ldots, \epsilon_{22} x_{22})$ where $\epsilon_i = \pm 1$, and the -1 defines the support of an element of the shadow of C. Such an automorphism also exchanges L_{22} and its dual lattice.

Corollary 6.4 *For all $i = 1, \ldots, 6$, $A_4(C_{22}^i)$ is isometric to L_{22}.*

Proof. We only have to prove that these lattices contain integral sublattices of index 2. These lattices $A_4(C_{22}^i)$ are generated by the rows of matrices of the form

$$G := \frac{1}{2}\begin{pmatrix} I & R \\ O & 4I \end{pmatrix},$$

where R is circulant matrices and the first rows are listed in Table 4. $R = (R_{i,j})$ has integral coefficients and by Lemma 5.4 $RR^T = 3J - I$.

Let $r_1, \ldots, r_{11}$ be the first eleven rows of G and let $s_1, \ldots, s_{11}$ be the last eleven rows of G. We have $[s_i, s_j] = 4\delta_{i,j}$, $[s_i, r_j] = R_{j,i}$ and $[r_i, r_j] = 3/4$. Hence, one can verify that the sublattice of index 2 spanned by $\{r_i \pm r_j, s_i, \}_{1 \le i,j \le 11}$ is integral. □

Acknowledgment. The third author would like to thank Manabu Oura for helpful conversations.

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, "Type II codes, even unimodular lattices and invariant rings," *IEEE Trans. Inform. Theory*, (to appear).

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

[3] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (2nd ed.)*, Springer-Verlag, New York, 1993.

[4] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[5] J.H. Conway and N.J.A. Sloane, "On lattices equivalent to their duals," *J. Number. Theory* **48** (1994), 373–382.

[6] T.A. Gulliver and M. Harada, "Extremal Type II double circulant codes over $\mathbb{Z}_4$ and construction of 5-$(24, 10, 36)$ designs," *Discrete Math.* **194** (1999), 129–137.

[7] T.A. Gulliver and M. Harada, "Double circulant self-dual codes over $\mathbb{Z}_{2k}$," *IEEE Trans. Inform. Theory* **44** (1998), 3105–3123.

[8] G.T. Kennedy and V. Pless, "On designs and formally self-dual codes," *Des. Codes and Cryptogr.* **4** (1994), 43–55.

[9] H.-G. Quebbemann, Modular lattices in euclidean spaces, *J. Numb. Th.* **54** (1995), 190-202

[10] E. Rains and N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, eds. V. Pless et al., Elsevier, Amsterdam, 1998.

[11] R. Scharlau and R. Schulze-Pillot, Extremal Lattices, in *Algorithmic Algebra and Number Theory*, edited by B.H. Matzat, G.-M. Greuel, G. Hiss, Springer Verlag 1999.