Journal of Algebraic Combinatorics **6** (1997), 119–131

Double Circulant Codes over $\mathbb{Z}_4$ and Even Unimodular Lattices

A.R. CALDERBANK rc@research.att.com
N.J.A. SLOANE njas@research.att.com
Information Sciences Research Center, AT&T Labs-Research, Murray Hill, New Jersey 07974

Received August 16, 1995

Abstract. With the help of some new results about weight enumerators of self-dual codes over $\mathbb{Z}_4$ we investigate a class of double circulant codes over $\mathbb{Z}_4$, one of which leads to an extremal even unimodular 40-dimensional lattice. It is conjectured that there should be "Nine more constructions of the Leech lattice".

Keywords: quarterly code, unimodular lattice, $\mathbb{Z}_4$, Leech lattice, invariant theory

1. Introduction

The inspiration for this work was the discovery made in [2] that the Leech lattice can be obtained by lifting the binary Golay code of length 24 to a self-dual code over $\mathbb{Z}_4$ and applying Construction A_4 (cf. Section 4). We were interested in seeing if other binary codes could be lifted to $\mathbb{Z}_4$ codes so as to produce unimodular lattices.

In Section 3 we investigate a class of double circulant codes over $\mathbb{Z}_4$ that lie above the binary double circulant codes $\mathcal{B}$ studied in Chapter 16, Section 7 of [14]. These are self-dual codes over $\mathbb{Z}_4$ in which the norm of every vector is divisible by 8, and in Section 2 we establish some new results about the weight enumerators of such codes. In Section 4 we show that the code of length 40 leads to an extremal even unimodular 40-dimensional lattice. In the last section we reconsider the Leech lattice, give another construction for it based on a different double circulant code, and suggest that there may be seven more constructions awaiting discovery! (But see the Postscript.)

2. Weight enumerators of codes over $\mathbb{Z}_4$

In this section we use invariant theory to establish some new results about weight enumerators of codes over $\mathbb{Z}_4$. For background information about this technique, see [17] or [14], Chapter 19.

As in [10, 12] we use the following terminology. The elements of $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ are denoted by $\{0, 1, 2, 3\}$, and their Lee weights (denoted by *wt*) are respectively $0, 1, 2, 1$. The Lee distance between vectors $u, v \in \mathbb{Z}_4^n$ is $\mathrm{dist}(u, v) = \sum_{i=1}^{n} \mathrm{wt}(u_i - v_i)$. In the present paper we also consider the Euclidean norms (denoted by *norm*) of the elements of $\mathbb{Z}_4$, which are respectively $0, 1, 4, 1$, so that $\mathrm{norm}(u_i) = \mathrm{wt}(u_i)^2$. The Euclidean norm

between vectors $u, v \in \mathbb{Z}_4^n$ is $\text{norm}(u, v) = \sum_{i=1}^{n} \text{norm}(u_i - v_i)$. A linear code C of length n over $\mathbb{Z}_4$ is a subset of $\mathbb{Z}_4^n$ which is closed under addition. Duality is defined with respect to the standard inner product $u \cdot v = u_1 v_1 + \cdots + u_n v_n$. As in [6] we say that C has type $1^{k_1} 2^{k_2}$ if by a suitable permutation of coordinates the generator matrix can be put into the form

$$\begin{bmatrix} I_{k_1} & X & Y \\ 0 & 2I_{k_2} & 2Z \end{bmatrix},$$

for appropriate matrices X, Y, Z. If C is a linear code of length n over $\mathbb{Z}_4$ there are two binary codes of length n associated with it:

$$C_1 = \{c(\text{mod } 2) : c \in C\}, \tag{2.1}$$

$$C_2 = \left\{ \frac{1}{2}c : c \in C, \quad c \equiv 0(\text{mod } 2) \right\}. \tag{2.2}$$

Lemma 1 *If C is of type 1^k then $C_1 = C_2$.*

We omit the elementary proof.

The *complete weight enumerator* (or c.w.e.) of a linear code C is

$$\text{cwe}_C(a, b, c, d) = \sum_{u \in C} a^{n_0(u)} b^{n_1(u)} c^{n_2(u)} d^{n_3(u)},$$

where $n_i(u)$ is the number of components of u that are equal to i $(i = 0, 1, 2, 3)$. Following Klemm [13] we also use the variables

$$T_0 = (a + c)/\sqrt{2}, \quad T_1 = (b + d)/\sqrt{2},$$
$$T_2 = (a - c)/\sqrt{2}, \quad T_3 = (b - d)/\sqrt{2}.$$

A disadvantage of the c.w.e. is that it contains too much information. For most purposes there is no need to distinguish between coordinates that are 1 and coordinates that are 3. We therefore define the *symmetrized weight enumerator* (or s.w.e.) of C to be

$$\text{swe}_C(a, b, c) = \text{cwe}_C(a, b, c, b).$$

We will use upper case letters for c.w.e.'s and lower case letters for s.w.e.'s. The subscript gives the degree.

The Molien series of a polynomial ring R is the series $\Phi(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d$, where a_d is the dimension of the subspace of R consisting of the homogeneous polynomials of degree d (see [1, 14, 17–19]).

The first theorem is due to Klemm.

Theorem 2 (Klemm [13]) *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains 1^n. Then the c.w.e. of C is an element of the ring*

$$\begin{aligned}&\mathcal{R}_0 \oplus A_8\mathcal{R}_0 \oplus A_8^2\mathcal{R}_0 \oplus B_{16}\mathcal{R}_0 \oplus A_8B_{16}\mathcal{R}_0 \oplus A_8^2B_{16}\mathcal{R}_0\\ &\quad = \big(1 \oplus A_8 \oplus A_8^2\big)(1 \oplus B_{16})\mathcal{R}_0\end{aligned} \tag{2.3}$$

with Molien series

$$\frac{(1+\lambda^8+\lambda^{16})(1+\lambda^{16})}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{16})}\,, \tag{2.4}$$

where $\mathcal{R}_0$ is the ring of symmetric functions of T_0^4, T_1^4, T_2^4, T_3^4, and

$$\begin{aligned}A_8 &= T_0^4T_3^4 + T_1^4T_2^4,\\ B_{16} &= (T_0T_1T_2T_3)^2\big(T_0^4T_1^4 + T_2^4T_3^4 - T_0^4T_2^4 - T_1^4T_3^4\big).\end{aligned}$$

Proof: We sketch the proof, since this will be the basis for the following proofs. The c.w.e. of C is invariant under the following linear transformations of the variables T_0, T_1, T_2, T_3:

$$\begin{bmatrix}1&&&\\&1&&\\&&i&\\&&&i\end{bmatrix}, \begin{bmatrix}1&&&\\&1&&\\&&1&\\&&&-1\end{bmatrix}, \begin{bmatrix}1&&&\\&&1&\\&1&&\\&&&i\end{bmatrix}, \begin{bmatrix}&1&&\\1&&&\\&&&1\\&&1&\end{bmatrix}, \tag{2.5}$$

and hence is also invariant under the group G_0 that they generate, which has order 1024. The Molien series of G_0 can be calculated directly, for example using Magma [5], and is equal to (2.4). It is easily checked that A_8, B_{16} and the elements of $\mathcal{R}_0$ are invariant under G_0, and that the Molien series (2.4) describes the structure of the direct sum in (2.3). The result then follows. □

The next result, which follows from Theorem 2, was given in [10].

Corollary 3 *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains a vector $\pm 1^n$. Then the s.w.e. of C is an element of the ring*

$$R_0 \oplus a_8R_0 \oplus a_8^2R_0, \tag{2.6}$$

with Molien series

$$\frac{1+\lambda^8+\lambda^{16}}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})} = 1 + \lambda^4 + 3\lambda^8 + 4\lambda^{12} + 7\lambda^{16} + 9\lambda^{20} + 13\lambda^{24} + \cdots, \tag{2.7}$$

where R_0 is the ring $\mathbb{C}[\phi_4, \phi_8, \phi_{12}]$ and

$$\begin{aligned}\phi_4 &= a^4 + 6a^2c^2 + 8b^4 + c^4,\\ \phi_8 &= (a^2c^2 - b^4)\{(a^2 + c^2)^2 - 4b^4\},\\ \phi_{12} &= b^4(a^2 - c^2)^4,\\ a_8 &= b^4(a - c)^4.\end{aligned}$$

Proof: When we set $d = b$ the ring $\mathcal{R}_0$ collapses to R_0 and (2.3) collapses to (2.6). The structure of the latter ring is described by the Molien series (2.7). □

Codes whose weight enumerators yield all the polynomials needed to obtain the rings (2.3) and (2.6) were given in [10].

The codes used in the present paper have an additional property, described in the following theorem, which we believe to be new.

Theorem 4 *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains 1^n and has all norms divisible by 8. Then the c.w.e. of C is an element of the ring*

$$\big(1 \oplus H_8 \oplus H_8^2 \oplus H_8^3\big)(1 \oplus H_{16})(1 \oplus H_{32})\mathcal{R}_1, \tag{2.8}$$

with Molien series

$$\frac{(1 + \lambda^8 + \lambda^{16} + \lambda^{24})(1 + \lambda^{16})(1 + \lambda^{32})}{(1 - \lambda^8)(1 - \lambda^{16})(1 - \lambda^{24})(1 - \lambda^{32})}, \tag{2.9}$$

where $\mathcal{R}_1$ is the ring of symmetric polynomials in T_0^8, T_1^8, T_2^8, T_3^8, and

$$\begin{aligned}H_8 &= T_0^4T_2^4 + T_2^4T_3^4 + T_3^4T_1^4 + T_1^4T_0^4 - T_0^4T_3^4 - T_1^4T_2^4,\\ H_{16} &= (T_0T_1T_2T_3)^4,\\ H_{32} &= (T_0T_1T_2T_3)^2\big(T_0^4 + T_2^4\big)\big(T_2^4 + T_3^4\big)\big(T_3^4 + T_1^4\big)\big(T_1^4 + T_0^4\big)\big(T_0^4 - T_3^4\big)\big(T_1^4 - T_2^4\big).\end{aligned}$$

Proof: The c.w.e. is now invariant under the group G_1 generated by G_0 and the additional transformation

$$\begin{bmatrix} & & 1 & \\ & \eta & & \\ 1 & & & \\ & & & \eta \end{bmatrix},$$

where $\eta = (1 + i)/\sqrt{2}$, $\eta^8 = 1$. Using Magma we find that G_1 has order 6144 and Molien series given by (2.9). We then check that H_8, H_{16}, H_{32} and the elements of $\mathcal{R}_1$ are invariant under G_1, and that there are sygygies expressing H_8^4 (but not H_8^2 or H_8^3), H_{16}^2 and H_{32}^2 as elements of the ring (2.8). The result follows. □

Corollary 5 *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains a vector $\pm 1^n$ and has all norms divisible by 8. Then the s.w.e. of C is an element of the ring*

$$R_1 \oplus h_8 R_1 \oplus h_8^2 R_1 \oplus h_8^3 R_1, \tag{2.10}$$

with Molien series

$$\frac{1+\lambda^8+\lambda^{16}+\lambda^{24}}{(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})} = 1 + 2\lambda^8 + 4\lambda^{16} + 7\lambda^{24} + 10\lambda^{32} + 14\lambda^{40} + 19\lambda^{48} + 24\lambda^{56} + 30\lambda^{64} + \cdots, \tag{2.11}$$

where R_1 is the ring $\mathbb{C}[\theta_8, \theta_{16}, \theta_{24}]$ and

$$\begin{aligned}
\theta_8 &= a^8 + 28a^6c^2 + 70a^4c^4 + 28a^2c^6 + c^8 + 128b^8, \\
\theta_{16} &= \{a^2c^2(a^2+c^2)^2 - 4b^8\}\{(a^4 + 6a^2c^2 + b^4)^2 - 64b^8\}, \\
\theta_{24} &= b^8(a^2-c^2)^8, \\
h_8 &= \{ac(a^2+c^2) - 2b^4\}^2 .
\end{aligned}$$

Proof: Parallel to the proof of Corollary 3. $\mathcal{R}_1$ collapses to R_1 when we set $d = b$. □

It is possible, although as we shall see not necessarily desirable, to impose a further condition on the code.

Theorem 6 *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains 1^n and has all norms divisible by 8 and all Lee weights divisible by 4. Then the c.w.e. of C is an element of the free polynomial ring $\mathcal{R}_2$ generated by H_{16} and all symmetric polynomials in T_0^8, T_1^8, T_2^8, T_3^8. This ring has Molien series*

$$\frac{1}{(1-\lambda^8)(1-\lambda^{16})^2(1-\lambda^{24})} . \tag{2.12}$$

Proof: The c.w.e. is invariant under the group G_2 generated by G_1 and

$$\begin{bmatrix} & & 1 & \\ & i & & \\ 1 & & & \\ & & & i \end{bmatrix}.$$

Again using Magma we find that G_2 has order 49152 and Molien series (2.12). G_2 is a unitary reflection group (cf. [16]), and consists of all monomial matrices whose elements are powers of η such that the product of all the entries in each matrix is an even power of η. It is then easily seen that the ring of invariants is equal to $\mathcal{R}_2$. □

Corollary 7 *Let C be a self-dual code of length n over $\mathbb{Z}_4$ that contains a vector $\pm 1^n$ and has all norms divisible by 8 and all Lee weights divisible by 4. Then the s.w.e. of C is an*

element of the ring R_1 with Molien series

$$\frac{1}{(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})} = 1+\lambda^8+2\lambda^{16}+3\lambda^{24}+4\lambda^{32}+5\lambda^{40}+7\lambda^{48} + 8\lambda^{56}+10\lambda^{64}+\cdots. \tag{2.13}$$

Remarks

1. The group G_2 is half of the full group G_3 of all monomial matrices whose elements are powers of η. G_3 has order $8^4\,4! = 98304$ and Molien series

$$\frac{1}{(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})(1-\lambda^{32})}.$$

   However, there does not seem to be any additional condition arising naturally from coding theory that can be imposed on C which will force its c.w.e. to be invariant under G_3.
2. The s.w.e.'s of the Klemm codes $\mathcal{K}_8$, $\mathcal{K}_{16}$, $\mathcal{K}_{24}$ (which are generated by 1^n and all vectors of shape $2^2 0^{n-2}$, cf. [13], [10, Eq. (43)]) span the ring R_1. By adjoining the s.w.e. of the octacode (see [10–12]) we generate the ring (2.10).
3. The next result shows why the additional property of the codes mentioned in Theorem 6 and Corollary 7 may not be a good thing. For as we saw in [12], it is quite unusual for a $\mathbb{Z}_4$-linear code to have a binary image that is also linear. Most interesting $\mathbb{Z}_4$ codes do not have this property.

Theorem 8 *If C is a self-dual code over $\mathbb{Z}_4$ with all Lee weights divisible by* 4, *then the binary image of C under the Gray map* (*cf.* [12]) *is linear.*

Proof: Let u, v be codewords in C and let $\bar{u}$, $\bar{v}$ denote their binary images. By a fundamental property of the Gray map, $\mathrm{dist}(u, v) = \mathrm{dist}(\bar{u}, \bar{v})$, the latter distance of course being Hamming distance. Since $\mathrm{dist}(u, v) \equiv \mathrm{dist}(u) \equiv \mathrm{dist}(v) \equiv 0 (\mathrm{mod}\ 4)$, $\mathrm{wt}(\bar{a} \cap \bar{b})$ is even. If $\bar{C}$ denotes the binary image of C, and D is the linear span of $\bar{C}$, we have $2^n = |\bar{C}| \le |D| \le |D^\perp|$ (where n is the length of C), and so $\bar{C} = D$. □

3. Double circulant codes over $\mathbb{Z}_4$

In this section we consider codes over $\mathbb{Z}_4$ which when read modulo 2 are the double circulant codes $\mathcal{B}$ described for example in Eq. (57), p. 507 of [14].

Definition Let $n = 2p + 2$ where p is a prime congruent to 3 (mod 8). The code D_n has generator matrix

$$M = \left[\begin{array}{c|ccc|c|ccc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & 0 & & & \\ \vdots & & I & & \vdots & & b(I+R) & \\ 1 & & & & 0 & & & \end{array}\right] \tag{3.1}$$

if $p \equiv 11 \pmod{16}$, or

$$M = \left[\begin{array}{c|ccc|c|ccc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & 0 & & & \\ \vdots & & I & & \vdots & & I + 3R + 2N & \\ 1 & & & & 0 & & & \end{array}\right] \tag{3.2}$$

if $p \equiv 3 \pmod{16}$, where $R = (R_{ij})$, $R_{ij} = 1$ if $j - i$ is a nonzero square mod p, or 0 otherwise; $N = (N_{ij})$, $N_{ij} = 1$ if $j - i$ is not a square mod p, or 0 otherwise; and b can be either $+1$ or -1.

Theorem 9 *D_n is a self-dual code over $\mathbb{Z}_4$ in which all norms are divisible by* 8.

Proof: The two cases are similar, and we give details only for $p \equiv 3 \pmod{16}$. The rows of the matrix M are indexed by the elements of the projective line $\infty, 0, 1, \ldots, p-1$.

The norm of row M_∞ is $2p + 2 \equiv 8 \pmod{16}$ and the norm of row M_i, $i \neq \infty$ is $1 + 1 + 1 + (p-1)/2 + 4(p-1)/2 = (5p+1)/2 \equiv 0 \pmod 8$. Hence the norm of every row of M is divisible by 8.

Next we check that D_n is self-orthogonal mod 4. Let

$$MM^T = \left[\begin{array}{c|c} 0 & MM_\infty^T \\ \hline M_\infty M^T & A \end{array}\right],$$

and observe that, for $i = 0, 1, \ldots, p-1$,

$$\left(MM_\infty^T\right)_i = 1 + 1 + 1 + 3(p-1)/2 + 2(p-1)/2 = (p+5)/2 \equiv 0 \pmod 8.$$

The matrix A is given by

$$A = J + I + (I + 3R + 2N)(I + 3R + 2N)^T = 2J + I + RR^T + 2(RN^T + NR^T),$$

where J is the $p \times p$ matrix with every entry equal to 1. Now we use Perron's Theorem (cf. Ch. 16, Th. 24 of [14]) to write

$$RR^T = \left(\frac{p+1}{4} - 1\right)(J - I) + \left(\frac{p-1}{2}\right) I,$$

$$RN^T = \left(\frac{p+1}{4} - 1\right) R + \left(\frac{p+1}{4}\right) N = \left(\frac{p+1}{4}\right)(J - I) - R.$$

It follows that $A \equiv 0 \pmod 4$ and that D_n is a self-dual code over $\mathbb{Z}_4$.

Since D_n is generated by codewords with norms divisible by 8 and is self-orthogonal modulo 4, it follows by induction that the norm of every codeword is divisible by 8. □

Remarks

(1) The generalization to block lengths n of the form $2q+2$ where q is a prime power congruent to 3 (mod 8) is straightforward.
(2) This section began by mentioning a certain binary double circulant code $\mathcal{B}$ of length n. $\mathcal{B}$ is invariant under a permutation group G_n that is isomorphic to $\mathrm{PGL}_2(p)$. Indeed, we could have started with this permutation representation, and constructed $\mathcal{B}$ in terms of the irreducible G_n-submodules.

There are several interesting linear codes over $\mathbb{Z}_4$ that reduce to $\mathcal{B}$ when read modulo 2. For example, when $p \equiv 11 \pmod{16}$ the matrix

$$M' = \left[\begin{array}{c|ccc|c|cc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \hline 3 & & & & 2 & & & \\ \vdots & & & & \vdots & & b(I+3R) & \\ \vdots & & I & & \vdots & & +2N & \\ \vdots & & & & \vdots & & & \\ 3 & & & & 2 & & & \end{array}\right],$$

where b is $+1$ or -1, generates a self-dual code over $\mathbb{Z}_4$ with all norms divisible by 8.

However, the codes D_n are distinguished by reducing to $\mathcal{B}$ modulo 2 and by being invariant under a group $\mathcal{G}_n$ of monomial matrices that reduces to G_n when read modulo 2. Recall that extended quadratic residue codes over $\mathbb{Z}_4$ are related to extended binary quadratic residue codes in this same way (cf. [2]).

Theorem 10 *The automorphism group $\mathcal{G}_n$ of D_n is a central extension of* $\mathrm{PGL}_2(p)$; *the center $Z(\mathcal{G}_n) = \{\pm I\}$ and $\mathcal{G}_n / Z(\mathcal{G}_n) \simeq \mathrm{PGL}_2(p)$. The group $\mathcal{G}_n$ is generated by the following automorphisms*:

(1) $T_i = \left[\begin{smallmatrix} T_i' & 0 \\ 0 & T_i' \end{smallmatrix}\right]$, *where T_i' is the permutation matrix corresponding to $z \to z+i$,*
(2) $P_a = \left[\begin{smallmatrix} P_a' & 0 \\ 0 & P_a' \end{smallmatrix}\right]$, *where a is a nonzero square modulo p, and P_a' is the matrix corresponding to the permutation $z \to az$,*
(3) $S = \left[\begin{smallmatrix} 0 & P_{-1}' \\ P_{-1} & 0 \end{smallmatrix}\right]$, *where P_{-1}' is the matrix corresponding to the permutation $z \to -z$,*
(4) $\lambda = \left[\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right]$, *where* (*using $\square$ to indicate a nonzero square mod p, and $\not\square$ for a nonsquare mod p*)

$$(\lambda_1)_{ij} = \begin{cases} 1, & \text{if } i = \infty,\ j = 0, \\ 3, & \text{if } i = 0,\ j = \infty, \\ 3, & \text{if } i = \square \text{ and } j = -1/i, \\ 1, & \text{if } i = \not\square \text{ and } j = -1/i, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$(\lambda_2)_{ij} = \begin{cases} 3, & \text{if } i = \infty,\ j = 0, \\ 1, & \text{if } i = 0,\ j = \infty, \\ 3, & \text{if } i = \square \text{ and } j = -1/i, \\ 1, & \text{if } i = \not\square \text{ and } j = -1/i, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Again we give details only for $p \equiv 3 (\mathrm{mod}\ 16)$. It is clear that the transformations T_i, $i = 0, 1, \ldots, p-2$ and P_a, $a = \square$, are automorphisms of D_n.

Next we consider

$$M(MS)^T = \left[\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right],$$

where

$$B = (P'_{-1} + 3RP'_{-1} + 2NP'_{-1})^T + 3P'_{-1} + RP'_{-1} + 2NP'_{-1}.$$

Since $P'_{-1}NP'_{-1} = R$, it follows that $M(MS)^T \equiv 0 (\mathrm{mod}\ 4)$. Hence the rows of MS generate D_n and S is an automorphism of D_n as required.

Since the rows of MS generate D_n we may prove that λ is an automorphism by showing that $(MS\lambda)M^T \equiv 0 (\mathrm{mod}\ 4)$. There are several different cases: we shall only present a typical calculation to show the general method. We consider the inner product of $M_{-1}S\lambda$ with M_a where $a = \not\square$ and $a+1 = \not\square$ (the same argument applies to $(M_bS\lambda, M_a)$ where b is an arbitrary nonsquare).

$$\begin{array}{rccccc|ccccccccccc} M_{-1} = (& 1 & 0 & \cdots & 0 & 1 & 0 & 3 & & & 3 & & 2 & &) \\ & & & & & & \infty & 0 & & & a+1=\square & & a+1\neq\square & & \end{array}$$

$$\begin{array}{rccccc|ccccccccccc} M_{-1}S = (& 0 & 3 & \cdots & \cdot & \cdot & 3 & 0 & 3 & 0 & \cdots & & \cdots & & 0 &) \\ & & & & & & \infty & 0 & 1 & & & & & & -1 & \end{array}$$

$$\begin{array}{rccccc|ccccccccccc} M_{-1}S\lambda = (& 1 & 0 & \cdots & \cdot & \cdot & 0 & 1 & 0 & & \cdots & & \cdots & 0 & 1 &) \\ & & & & & & \infty & 0 & 1 & & & & & & -1 & \end{array}$$

Next we take the inner product with M_a; note that $(M_a)_0 = (M_a)_{-1} = 3$ since $a = \not\square$ and $a+1 = \not\square$.

$$\begin{array}{rccccccccc|ccccccc} M_a = (& 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & | & 0 & 3 & \cdots & \cdots & 3 &) \\ & \infty & & & & a & & & & & 0 & & & & -1 & \end{array}$$

We need to calculate $(M_{-1}S\lambda)_{a_L}$ where the subscript L indicates the left half. We know

$$a = \frac{1}{\ell} = \not\square \qquad \text{and} \qquad a+1 = \frac{\ell+1}{\ell} = \not\square.$$

If $(M_{-1}S\lambda)_{a_L} = 1$ then $(M_{-1}S\lambda, M_a) \equiv 0 \pmod 4$, as required. Since $\ell = \not\emptyset$, $(M_{-1}S\lambda)_{a_L} = 1$ if and only if $(M_{-1}S)_{-\ell_L} = 3$. Finally $(M_{-1}S)_{-\ell} = 3$ if and only if $(M_{-1})_{\ell_R} = 3$, and this follows from the assumption $\ell + 1 = \not\emptyset$. □

4. The case $n = 40$ and a 40-dimensional even unimodular lattice

Theorem 11 *In the case* $p = 19$, *the code* D_{40} *defined by* (3.1) *is a self-dual code of length 40 over* $\mathbb{Z}_4$ *with norms divisible by* 8 *and with minimal norm* 16.

Proof: In view of the results of the previous section it is only necessary to show that the minimal norm is not 8. In this proof we denote the code by C. We show by computer that the binary image C_1 (see (2.1)) is a [40, 20, 8] code, in which there are 285 words of weight 8. By Lemma 1, this also holds for C_2.

Let $u \in C$, $u \neq 0$ have minimal norm. If all coordinates of u are even, $\text{norm}(u) \geq 32$, by the previous paragraph. Otherwise u has exactly eight ± 1 coordinates and some unknown number of 2 coordinates. The vectors in C of shape $\pm 1^8 2^* 0^*$ fall into 285 sets according to their binary image. The following argument shows that the group of C acts transitively on these 285 sets.

It is easy to verify that the vector c given by

$$c = (\ \underset{\infty}{3} \ \cdots \ \underset{2}{1}\ \underset{3}{1}\ \underset{14}{1}\ \cdot \ | \ \underset{\infty}{0}\ \underset{0}{1}\ \underset{1}{0}\ \underset{2}{2}\ \underset{3}{2}\ \underset{4}{0}\ \underset{5}{2}\ \underset{6}{0}\ \underset{7}{0}\ \underset{8}{0}\ \underset{9}{0}\ \underset{10}{3}\ \underset{11}{0}\ \underset{12}{0}\ \underset{13}{3}\ \underset{14}{2}\ \underset{15}{3}\ \underset{16}{2}\ \underset{17}{2}\ \underset{18}{0}\ )$$

is a codeword in C. The permutation group G obtained from the automorphism group of C by reduction modulo 2 is isomorphic to $\text{PGL}_2(19)$ and has order $20.19.18 = 285.24$. This permutation group is in fact the automorphism group of the binary code obtained from C by reduction modulo 2. Let $S = \{\infty_L, 2_L, 3_L, 14_L, 0_R, 10_R, 13_R, 15_R\}$ be the set of coordinate positions indexing entries ± 1 in the codeword c (the subscripts L and R correspond to Left and Right coordinate positions). It is sufficient to prove that the subgroup $\text{Stab}_G(S)$ of G that fixes S setwise has order exactly 24. We observe that this subgroup contains a group of order 24 generated by the following automorphisms:

1) a symmetry g_1 corresponding to $z \to 1/z$ which interchanges the left and right halves because the underlying permutation is not in $\text{PSL}_2(19)$,
2) a symmetry g_2 corresponding to $z \to 7z$ which acts as the 3-cycle (2, 13, 14) on the left and as the 3-cycle (10, 13, 15) on the right,
3) a symmetry g_3 corresponding to $z \to 2(\frac{z+4}{z-2})$ which acts on the left as $(0, 15)(10, 13)$ and on the right as $(\infty, 2)(3, 14)$.

The subgroup generated by g_2 and g_3 has order 12 and is isomorphic to the alternating group A_4 (this is clear from the action on either half). If $|\text{Stab}_G(S)| > 24$ then there must exist $g_4 \in \text{Stab}_G(S)$, fixing the left and right halves, such that $\langle g_2, g_3, g_4 \rangle$ is isomorphic to the full symmetric group S_4. However, this provides a contradiction since it is not possible to realize $(\infty)(2)(3, 14)$ as a permutation in $\text{PSL}_2(19)$.

We now chose one vector $u \in C$ of shape $\pm 1^8 2^* 0^*$, and examine the set $\{u + 2c : c \in C\}$ by computer. It is found that the minimal Lee weight is 20, achieved by 512 vectors of shape $\pm 1^8 2^6 0^{10}$. These vectors have norm 32, which is therefore the smallest norm in the set. This completes the proof. □

We had hoped to use Corollary 5 to determine the s.w.e. of D_{40}. As we see from (2.11), there are 14 degrees of freedom in the s.w.e. Unfortunately, even using everything we know about this code (minimal Lee weight, the projections onto the binary codes C_1 and C_2, complete information about the words of shape $\pm 1^8 2^* 0^*$, the theta series of the corresponding lattice—see below), there still remains one undetermined coefficient. Any further piece of information, such as knowledge of the words of shape $\pm 1^{12} 2^* 0^*$, would be enough to pin down the s.w.e.

We now use this code to obtain a lattice, by using the following version of Construction A_4 (cf. [2, 9]). Suppose C is a self-dual code of length n over $\mathbb{Z}_4$ of type $1^{n/2}$ with generator matrix $[I\,A]$. Suppose also that all norms in C are divisible by 8 and that the minimal norm in C is N. Then the matrix

$$\frac{1}{2}\begin{bmatrix} I & A \\ 0 & 4I \end{bmatrix}$$

generates an even unimodular n-dimensional lattice with minimal norm $\min\{4, N/4\}$.

When applied to the code D_{40} this construction produces an extremal even unimodular 40-dimensional lattice. We do not know if this is the same as any of the known lattices of this class (cf. [9], p. 194). (But see the Postscript.) It would be a worthwhile project for someone to investigate the known extremal even unimodular lattices in dimensions 32 and 40 and to determine which ones are distinct.

5. Further constructions for the Leech lattice

There are nine doubly-even self-dual binary codes of length 24 [15]: the Golay code and eight codes of minimal distance 4. The latter are best described by specifying the subcodes spanned by the weight 4 words, which are d_{24}, $d_{16}e_8$, d_{12}^2, $d_{10}e_7^2$, e_8^3, d_8^3, d_6^4 and d_4^6 (see Table E of [7]).

We conjecture that each of these nine codes can be lifted to a self-dual code over $\mathbb{Z}_4$ such that applying Construction A_4 yields the Leech lattice. This would give "Nine more constructions for the Leech lattice" (compare [8]).

As already remarked, the Golay code can certainly be lifted in this way [2]. We now show that the d_{24} code can also be lifted. The other seven cases are still open! (But see the Postscript.)

Consider the self-dual code C over $\mathbb{Z}_4$ with generator matrix $[I\,A]$, where I is a 12×12 identity matrix and A is a 12×12 bordered circulant matrix with first row and column $2\,1^{11}$. Let B be the 11×11 circulant part of A. Then $B_{ii} = 2$, $B_{ij} = 1$ if $i - j$ is a square mod 11 or 3 if $i - j$ is not a square. When read mod 2, this does indeed become the self-dual code of type d_{24}. Using the Bell Labs Cray Y-MP we calculated the s.w.e. of this code, which in

the terminology of Corollary 5 is

$$\theta_8^3 - 84\theta_8\theta_{16} - 720\theta_{24} + 2064h_8\theta_{16} - 1032h_8^2\theta_8 + 10304h_8^3.$$

Inspection of this weight enumerator shows that the minimal Lee weight is 8, the minimal norm is 16, and all norms are divisible by 8. Applying Construction A_4 we obtain an even unimodular lattice of minimal norm 4, which (see Chapter 12 of [9]) is necessarily the Leech lattice.

Note that C is a double circulant self-dual code over $\mathbb{Z}_4$ with minimal norm 16 for which the corresponding binary code C_1 has minimal distance 4. This is interesting in view of Bachoc's conjecture (quoted in [2]) that the minimal norm of an extended cyclic self-dual code over $\mathbb{Z}_4$ is twice the minimal Hamming distance of the corresponding binary code.

Postscript

(1) After this paper was written we became aware of the dissertation by Bonnecaze [2] and a preprint by Bonnecaze et al. [4] which also prove Theorem 4 and Corollary 5 (in a different but equivalent form). We thank Patrick Solé for pointing this out.

(2) Gabriele Nebe and Bernd Souvignier have determined the automorphism groups of the 40-dimensional lattice constructed in Section 4 and the McKay lattice ([9], p. 221). These groups are respectively $2 \cdot \mathrm{PGL}_2(19)$ and $2^{20} \cdot \mathrm{PGL}_2(19)$, showing that the lattices are not equivalent. Professor Nebe observes that this can also be deduced from the fact that our lattice is generated by its minimal vectors, whereas in the McKay lattice the minimal vectors span only a sublattice of index 2. Professor Nebe also found that McKay lattice can be obtained from a different code over $\mathbb{Z}_4$.

(3) The remaining seven constructions of the Leech lattice have been found by Jessica Millar Young and N.J.A.S. These will be described elsewhere.

References

1. D.J. Benson, *Polynomial Invariants of Finite Groups*, Cambridge University Press, 1993.
2. A. Bonnecaze, *Codes sur des anneaux finis et réseaux arithmétiques*, Ph.D. dissertation, University of Nice, Oct. 1995.
3. A. Bonnecaze, A.R. Calderbank, and P. Solé, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory* **41** (1995), 366–377.
4. A. Bonnecaze, P. Solé and B. Mourrain, Quaternary Type II Codes, preprint 1995.
5. W. Bosma and J. Cannon, *Handbook of Magma Functions*, Math. Dept., Univ. of Sydney, Sydney, Nov. 25, 1994.
6. A.R. Calderbank and N.J.A. Sloane, "Modular and p-adic cyclic codes," *Designs, Codes and Cryptography* **6** (1995), 21–35.
7. J.H. Conway, V. Pless, and N.J.A. Sloane, "The binary self-dual codes of length up to 32: A revised enumeration," *J. Combinatorial Theory, Series A* **60** (1992), 183–195.
8. J.H. Conway and N.J. A. Sloane, "Twenty-three constructions for the Leech lattice," *Proc. Roy. Soc. London, Series A* **381** (1982), 275–283. A revised version appears as Chapter 24 of Ref. [9].
9. J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd edition, 1993.
10. J.H. Conway and N.J.A. Sloane, "Self-dual codes over the integers modulo 4," *J. Combinatorial Theory, Series A* **62** (1993), 30–45.

11. G.D. Forney, Jr., N.J.A. Sloane, and M.D. Troff, "The Nordstrom-Robinson code is the binary image of the octacode," in *Coding and Quantization: DIMACS/IEEE Workshop October 19–21, 1992*, R. Calderbank, G.D. Forney, Jr., and N. Moayeri (Eds.) Amer. Math. Soc., 1993, pp. 19–26.
12. A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory* **40** (1994), 301–319.
13. M. Klemm, "Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4," *Archiv Math.* **53** (1989), 201–207.
14. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
15. V. Pless and N.J.A. Sloane, "On the classification and enumeration of self-dual codes," *J. Combinatorial Theory, Series A* **18** (1975), 313–335.
16. G.C. Shephard and J.A. Todd, "Finite unitary reflection groups," *Canad. J. Math.* **6** (1954), 274–304.
17. N.J.A. Sloane, "Error-correcting codes and invariant theory: New applications of a nineteenth-century technique," *Am. Math. Monthly* **84** (1977), 82–107.
18. L. Smith, *Polynomial Invariants of Finite Groups*, Peters, Wellesley, MA, 1995.
19. B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, NY, 1993.