J. Austral. Math. Soc. (*Series A*) **69** (2000), 287–297

DOUBLE CIRCULANT CONSTRUCTIONS OF THE LEECH LATTICE

ROBIN CHAPMAN

(Received 11 October 1999; revised 3 February 2000)

Communicated by W. W. L. Chen

Abstract

We consider the problem of finding, for each even number m, a basis of orthogonal vectors of length $\sqrt{m}$ in the Leech lattice. We give such a construction by means of double circulant codes whenever $m = 2p$ and p is a prime not equal to 11. From this one can derive a construction for all even m not of the form $2 \cdot 11^r$.

2000 *Mathematics subject classification*: primary 11H06, 11H71, 94B05.

1. Introduction

We say that the lattice L is defined by construction A_m if there is a lattice L' similar to L with $\mathbb{Z}^n \supseteq L' \supseteq m\mathbb{Z}^n$. This lattice L' corresponds to a subgroup $C = L'/m\mathbb{Z}^n$ of the group $(\mathbb{Z}/m\mathbb{Z})^n$. We can use the language of coding theory and regard C as a linear code of length n over the ring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. If the code C is self-dual over $\mathbb{Z}_m$, then $m^{-1/2}L$ is an integral unimodular lattice. In this language Leech's original construction [7] is an example of an A_8 construction.

Recently linear codes over $\mathbb{Z}_4$, the integers modulo 4, have been widely investigated. For instance Bonnecaze, Solé and Calderbank use a quadratic residue code of length 24 over $\mathbb{Z}_4$ to construct the Leech lattice, and describe this method as 'perhaps the simplest construction that is known for this lattice'. In [2] Calderbank and Sloane revisit a construction due to McKay [8] of the Leech lattice from a different self-dual code over $\mathbb{Z}_4$. However, to show the associated lattice has minimum norm 4, they find the symmetrized weight enumerator of the code by using the Bell Labs Cray

Y-MP. Here we begin by providing a computer-free proof that this construction gives the Leech lattice, and then give a simpler calculation of the symmetrized weight enumerator of the code.

Harada, Solé and Gaborit, [5] have asked for which m is there an A_m construction of the Leech lattice. This is only possible when m is even and $m \geq 4$. We show that this is true for almost all such m, namely for all m not of the form $2 \cdot 11^r$. Were there also an A_{22} construction, then this would settle the problem completely.

The author would like to thank Patrick Solé for various stimulating conversations.

2. Notation and terminology

We let $\mathbb{Z}_m$ denote the integers modulo m, and $\mathbb{F}_p$ the finite field of p elements. Most matrices are 12 by 12, and I denotes the identity matrix and J the all-ones matrix of this size. Lowercase boldface letters stand for vectors with entries either from $\mathbb{Z}$ or from $\mathbb{Z}_n$. All vectors have length 12 or 24, and the notation $\mathbf{a} = (\mathbf{b}\ \mathbf{c})$ indicates that $\mathbf{a}$ has length 24 and is the concatenation of the vectors $\mathbf{b}$ and $\mathbf{c}$ each of length 12. Also $\mathbf{j}$ denotes the all-one vector of length 12. We sometimes abuse the notation of matrix multiplication; where $\mathbf{a} = (\mathbf{b}\ \mathbf{c})$ and T is a 12 by 12 matrix then we write $\mathbf{a}T$ for $(\mathbf{b}T\ \mathbf{c}T)$.

A code over $\mathbb{Z}_m$ of length r is a subgroup of $(\mathbb{Z}_m)^r$. A lattice is a discrete subgroup of some Euclidean space. The norm of a vector in a lattice is the square of its length. If $\mathbf{a} \in (\mathbb{Z}_m)^r$, then $\mathbf{a} = (a_1, \ldots, a_r)$, where we take $|a_j| \leq m/2$. The Euclidean norm of such an $\mathbf{a}$ is $|a_1|^2 + \cdots + |a_r|^2$. We give $(\mathbb{Z}_m)^r$ the obvious dot product, and we say that a code $\mathscr{C} \subseteq (\mathbb{Z}_m)^r$ is self-dual if $\mathbf{a} \in \mathscr{C}$ if and only if $\mathbf{a} \cdot \mathscr{C} = 0$. We say that a code $\mathscr{C} \subseteq (\mathbb{Z}_m)^r$ is of type II if m is even, $\mathscr{C}$ is self-dual and the Euclidean weight of each element of $\mathscr{C}$ is divisible by $2m$.

3. The construction

Let

$$S = \begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
-1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
-1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
-1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 \\
-1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0
\end{pmatrix}.$$

Deleting the first row and column of S yields a circulant matrix whose first row contains the entries $(j/11)$ in order for $0 \leq j \leq 10$. (Here $(j/11)$ is the Legendre

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

symbol.) Also $S^{\mathrm{T}} = -S$ and $S^2 = -11I$. Let $\mathscr{C}$ be the linear code of length 24 over $\mathbb{Z}_4$ with generator matrix $M = (I \;\; 2I + S)$. Applying construction A_4 to $\mathscr{C}$ gives a lattice L. Equivalently L is the set of vectors $(\mathbf{a}\ \mathbf{b})$, where $\mathbf{b} \equiv \mathbf{a}(2I + S)$ (mod 4). Note that $(2I + S)^2 = 4I + 4S + S^2 = -7I + 4S \equiv I \pmod 4$. It follows that $(2I + S \;\; I)$ is also a generator matrix for $\mathscr{C}$, and so $(\mathbf{a}\ \mathbf{b}) \in \mathscr{C}$ implies that $(\mathbf{b}\ \mathbf{a}) \in \mathscr{C}$. Since the generating matrix is formed by concatenating two bordered circulant matrices we call the code a double circulant code following Calderbank and Sloane [2].

PROPOSITION 3.1. *The lattice $\frac{1}{2}L$ is isometric to the Leech lattice.*

PROOF. It suffices by the main result of Conway [3] to show that $\frac{1}{2}L$ is an even unimodular lattice of rank 24 with no vector of norm 2.

First of all

$$MM^{\mathrm{T}} = (I \;\; 2I + S)\begin{pmatrix} I \\ 2I - S \end{pmatrix} = I^2 + (2I + S)(2I - S) = 5I - S^2 = 16I.$$

As the entries of MM^{T} are all divisible by 4, then $\mathscr{C}$ is a self-orthogonal code, and is self-dual as manifestly $|\mathscr{C}| = 4^{12}$. Also the Euclidean weight of each generator is divisible by 8 and by self-duality it follows that the Euclidean weight of all elements is divisible by 8, that is $\mathscr{C}$ is of type II. Thus $\frac{1}{2}L$ is an even unimodular lattice. To show that it is the Leech lattice, it suffices to show that its minimum weight is 4 (by Conway's characterization [3]). Equivalently one must show that the minimum Euclidean weight of $\mathscr{C}$ is 16.

The only way that $\mathscr{C}$ can fail to have minimum Euclidean weight 16 is if it has vectors of Euclidean weight 8. Such a vector will have shape $(2^2\ 0^{22})$, $(2^1\ (\pm 1)^4\ 0^{19})$ or $((\pm 1)^8\ 0^{16})$. Associated with $\mathscr{C}$ are two binary codes. Let $\mathscr{C}_1$ be the image of $\mathscr{C}$ under the reduction map $(\mathbb{Z}_4)^{24} \to (\mathbb{Z}_2)^{24}$ and let $\mathscr{C}' = \{\mathbf{a} : \mathbf{a} \in \mathscr{C} \cap \{0, 2\}^{24}\}$ be the intersection of $\mathscr{C}$ with the kernel of this reduction map. We can identify $\{0, 2\} \subseteq \mathbb{Z}_4$ with $\mathbb{Z}_2$ and we denote the binary code corresponding to $\mathscr{C}'$ as $\mathscr{C}_2$. Then $\mathscr{C}_1 \subseteq \mathscr{C}_2$ and $|\mathscr{C}| = |\mathscr{C}_1||\mathscr{C}_2|$. But $\mathscr{C}_1$ has generator matrix $(I \;\; S)$ which is congruent to $(I \;\; J - I)$ modulo 2. Thus the elements of $\mathscr{C}_1$ are $(\mathbf{a}\ \mathbf{a})$, where $\mathbf{a}$ has even weight, and $(\mathbf{a}\ \mathbf{j} - \mathbf{a})$, where $\mathbf{a}$ has odd weight. Thus $\mathscr{C}_1$ has order 2^{12} and minimum weight 4. Also $|\mathscr{C}_1| = |\mathscr{C}_2|$ and so $\mathscr{C}_1 = \mathscr{C}_2$. A vector of shape $(2^2\ 0^{22})$ in $\mathscr{C}$ would give a weight 2 word in $\mathscr{C}_2$ which is impossible.

A vector $\mathbf{v}$ of shape $(2^1\ (\pm 1)^4\ 0^{19})$ in $\mathscr{C}$ reduces modulo 2 to an element of $\mathscr{C}_1$. This must have shape $(\mathbf{a}\ \mathbf{a})$, where $\mathbf{a}$ has weight 2. Thus $\mathbf{v} = (\mathbf{b}\ \mathbf{c})$ where $\mathbf{b}$ and $\mathbf{c}$ have shapes $((\pm 1)^2\ 0^{10})$ and $(2\ (\pm 1)^2\ 0^9)$ in some order. As $(\mathbf{c}\ \mathbf{b})$ also lies in $\mathscr{C}$ we may assume that $\mathbf{b}$ has shape $((\pm 1)^2\ 0^{10})$. Similarly, a vector $\mathbf{v}$ of shape $((\pm 1)^8\ 0^{16})$ in $\mathscr{C}$ must have the form $(\mathbf{b}\ \mathbf{c})$, where both $\mathbf{b}$ and $\mathbf{c}$ have shape $((\pm 1)^4\ 0^8)$. It suffices,

therefore, to show that no vector of the form $\pm\mathbf{v}_1 \pm \mathbf{v}_2$ and $\pm\mathbf{v}_1 \pm \mathbf{v}_2 \pm \mathbf{v}_3 \pm \mathbf{v}_4$, where the $\mathbf{v}_i$s are (distinct) rows of M, has Euclidean weight 8. This is a straightforward, but tedious computation, but it finally proves that $\frac{1}{2}L$ is the Leech lattice.

However using the symmetry of S, the above computations can be greatly abbreviated. Let

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

and

$$C = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

Then A, B and C all commute with S. (For A and B this easily follows from the construction of S as a bordered circulant, and the fact that $(3/11) = 1$.) If $(\mathbf{a}\ \mathbf{b}) \in \mathscr{C}$, then $\mathbf{b} \equiv \mathbf{a}(2I + S) \pmod 4$. Therefore, $\mathbf{a}A(2I + S) = \mathbf{a}(2I + S)A \equiv \mathbf{b}A \pmod 4$, and so $(\mathbf{a}\ \mathbf{b})A = (\mathbf{a}A\ \mathbf{b}A) \in \mathscr{C}$. Similarly, $(\mathbf{a}\ \mathbf{b})B \in \mathscr{C}$ and $(\mathbf{a}\ \mathbf{b})C \in \mathscr{C}$. The matrices A, B and C are all monomial matrices, with non-zero entries ± 1. Denote the rows of M by $\mathbf{r}_\infty, \mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{10}$ considering the suffixes as elements of $\mathbb{P} = \mathbb{P}^1(\mathbb{F}_{11})$, the projective line over the field $\mathbb{F}_{11}$. Then for $\alpha \in \mathbb{P}$ we have $\mathbf{r}_\alpha A = \mathbf{r}_{\alpha+1}$, $\mathbf{r}_\alpha B = \mathbf{r}_{3\alpha}$ and $\mathbf{r}_\alpha C = \pm\mathbf{r}_{-1/\alpha}$. The transformations $\alpha \mapsto \alpha + 1$, $\alpha \mapsto 3\alpha$ and $\alpha \mapsto -1/\alpha$ generate the standard action of PSL(2, 11) on $\mathbb{P}$. It follows that given $a, b, c, d \in \mathbb{F}_{11}$ with $ad - bc = 1$, there is a matrix D, a product of powers of A, B and C in some order, with $\mathbf{r}_\alpha D = \pm\mathbf{r}_{(a\alpha+b)/(c\alpha+d)}$ for each $\alpha \in \mathbb{P}$. Then D is monomial and commutes with S. Hence D preserves $\mathscr{C}$ and preserves the shapes of the elements of $\mathscr{C}$.

The action of PSL(2, 11) on unordered pairs of elements of $\mathbb{P}$ has one orbit, namely that of $\{\infty, 0\}$. The action of PGL(2, 11) on 4-element subsets of $\mathbb{P}$ is governed by the cross ratio; each orbit contains a set of the form $\{\infty, 0, 1, \alpha\}$ and this lies in the same orbit as $\{\infty, 0, 1, \beta\}$ if and only if $\alpha \in \{\beta, 1-\beta, 1/(1-\beta), \beta/(1-\beta), (1-\beta)/\beta, 1/\beta\}$. It readily follows that PGL(2, 11) has two orbits on 4-element subsets of $\mathbb{P}$, namely those containing $\{\infty, 0, 1, 2\}$ and $\{\infty, 0, 1, 3\}$. The set $\{\infty, 0, 1, 2\}$ is fixed under the map $\alpha \mapsto 2 - \alpha$ and the set $\{\infty, 0, 1, 3\}$ is fixed under the map $\alpha \mapsto 3/\alpha$. These transformations are induced from the action of PGL(2, 11) but not from that of PSL(2, 11). It follows that the PGL(2, 11) and the PSL(2, 11) orbits of 4-element subsets of $\mathbb{P}$ coincide. Thus it suffices to show that $\pm\mathbf{r}_\infty \pm \mathbf{r}_0$, $\pm\mathbf{r}_\infty \pm \mathbf{r}_0 \pm \mathbf{r}_1 \pm \mathbf{r}_2$ and $\pm\mathbf{r}_\infty \pm \mathbf{r}_0 \pm \mathbf{r}_1 \pm \mathbf{r}_3$ all have Euclidean weight at least 16. But if we change the signs of two of the rows in one of these expressions, then we add a vector of the form $2\mathbf{r}_\alpha + 2\mathbf{r}_\beta$, which has shape $(2^4\ 0^{20})$, where the twos lie in positions occupied by ones in the vector we are altering. Therefore, the shape, and so the Euclidean weight of the vector is not altered, and so we only need check the six cases $\mathbf{r}_\infty \pm \mathbf{r}_0$, $\mathbf{r}_\infty + \mathbf{r}_0 + \mathbf{r}_1 \pm \mathbf{r}_2$ and $\mathbf{r}_\infty + \mathbf{r}_0 + \mathbf{r}_1 \pm \mathbf{r}_3$. The back of a modest envelope is adequate to this task. □

4. Weight enumerators

By exploiting the symmetry of $\mathscr{C}$ under PSL(2, 11) we can compute the symmetrized weight enumerator of $\mathscr{C}$ without much difficulty. Given a word $\mathbf{w} \in \mathscr{C}$ define $\phi(\mathbf{w}) = X^a Y^b Z^c$, where a is the number of 0s in $\mathbf{w}$, c is the number of 2s in $\mathbf{w}$ and $b = 24 - a - c$ is the number of ± 1s in $\mathbf{w}$. The *symmetrized weight enumerator* of $\mathscr{C}$ is

$$W_{\mathscr{C}}(X, Y, Z) = \sum_{\mathbf{w} \in \mathscr{C}} \phi(\mathbf{w}).$$

The polynomial $W_{\mathscr{C}}(X, Y, Z)$ is called symmetrized, as the numbers 1 and -1 play

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

an equal role; this also facilitates the computation. The symmetrized weight enumerator also determines the theta series of the lattice produced from $\mathscr{C}$ by construction A_4.

To calculate this we calculate, for each $\mathbf{w}_1 \in \mathscr{C}_1$, the sum

$$W_{\mathbf{w}_1} = \sum_{\mathbf{w} \to \mathbf{w}_1} \phi(\mathbf{w}),$$

where the sum is over all words $\mathbf{w}$ in $\mathscr{C}$ reducing modulo 2 to $\mathbf{w}_1$.

The words $\mathbf{w}_1 \in \mathscr{C}_1$ are of two types: there are words $(\mathbf{a}\ \mathbf{a})$ with $\mathbf{a}$ of even weight and $(\mathbf{b}\ \mathbf{j} - \mathbf{b})$ with $\mathbf{b}$ of odd weight. The following of lemmas deal with each possible case.

LEMMA 4.1. (i) *For* $\mathbf{w}_1 = (0\ 0)$ *we have*

$$W_{\mathbf{w}_1} = \frac{(X^2 + Z^2)^{12} + (X^2 - Z^2)^{12}}{2} + 2^{11} X^{12} Z^{12}.$$

(ii) *For* $\mathbf{w}_1 = (\mathbf{j}\ \mathbf{j})$ *we have*

$$W_{\mathbf{w}_1} = 2^{12} Y^{24}.$$

PROOF. Let $\mathbf{w}_1 = (0\ 0)$. The words reducing to $(0\ 0)$ are those in $2\mathscr{C}_2$. For even j the code $\mathscr{C}_2$ has $\binom{12}{j}$ words $(\mathbf{c}\ \mathbf{c})$ where $\mathbf{c}$ has weight j. Also $\mathscr{C}_2$ has 2^{11} words of the form $(\mathbf{c}\ \mathbf{j} - \mathbf{c})$. It follows that

$$W_{\mathbf{w}_1} = \frac{(X^2 + Z^2)^{12} + (X^2 - Z^2)^{12}}{2} + 2^{11} X^{12} Z^{12}$$

as claimed.

The case $\mathbf{w}_1 = (\mathbf{j}\ \mathbf{j})$ is clear. □

LEMMA 4.2. *Let* $\mathbf{w}_1 = (\mathbf{a}\ \mathbf{a})$, *where* $\mathbf{a}$ *has even weight* j *and* $j \neq 0$ *or* 12. *Then*

$$W_{\mathbf{w}_1} = 2^{11-r_1-r_4} Y^{2j} (XZ)^{r_2+r_3} (X^2 + Z^2)^{r_1+r_4} + 2^{11-r_2-r_3} Y^{2j} (XZ)^{r_1+r_4} (X^2 + Z^2)^{r_2+r_3}$$

for certain integers r_j *to be defined.*

PROOF. Fix some $\mathbf{v} \in \mathscr{C}$ reducing to $\mathbf{w}_1$ and let $\mathbf{v}' = \mathbf{v} + (0\ 2\mathbf{j})$. Then each $\mathbf{w} \in \mathscr{C}$ reducing to $\mathbf{w}_1$ has the form $\mathbf{v} + (2\mathbf{a}\ 2\mathbf{a})$ or $\mathbf{v}' + (2\mathbf{a}\ 2\mathbf{a})$ for some $\mathbf{a}$ of even weight.

Let $\mathbf{v} = (\mathbf{v}_1\ \mathbf{v}_2)$ and note that $\mathbf{v}_1 \equiv \mathbf{v}_2 \pmod 2$. By applying the same permutation to the order of coordinates in $\mathbf{v}_1$ and $\mathbf{v}_2$ we get

$$\mathbf{v}_1 = ((\pm 1)^j\ 0^{r_1}\ 0^{r_2}\ 2^{r_3}\ 2^{r_4}) \qquad \text{and} \qquad \mathbf{v}_2 = ((\pm 1)^j\ 0^{r_1}\ 2^{r_2}\ 0^{r_3}\ 2^{r_4}),$$

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

where $r_1 + r_2 + r_3 + r_4 = 12 - j$. As $j 0$ we can replace $\mathbf{v}$ by $\mathbf{v} + 2(\mathbf{a}\ \mathbf{a})$ for a suitable $\mathbf{a}$ of even weight and rearrange again to get

$$\mathbf{v}_1 = ((\pm 1)^j\ 0^{r_1+r_4}\ 0^{r_2}\ 2^{r_3}) \qquad \text{and} \qquad \mathbf{v}_2 = ((\pm 1)^j\ 0^{r_1+r_4}\ 2^{r_2}\ 0^{r_3}).$$

It is apparent that

$$\phi(\mathbf{v} + 2(\mathbf{a}\ \mathbf{a})) = Y^{2j}(XZ)^{r_2+r_3}X^{2(r_1+r_4-s)}Z^{2s},$$

where s is the number of 1s in $\mathbf{a}$ corresponding to positions where the entries of $\mathbf{v}_1$ and $\mathbf{v}_2$ both vanish. The number of $\mathbf{a}$ of even weight giving rise to a particular value for s is $2^{11-r_1-r_4}\binom{r_1+r_4}{s}$ and so the sum of $\phi(\mathbf{v} + 2(\mathbf{a}\ \mathbf{a}))$ over all $\mathbf{a}$ of even weight $\mathbf{a}$

$$2^{11-r_1-r_4}Y^{2j}(XZ)^{r_2+r_3}(X^2 + Z^2)^{r_1+r_4}.$$

Replacing $\mathbf{v}$ by $\mathbf{v}'$ interchanges the rôles of $r_1 + r_4$ and $r_2 + r_3$ and so

$$W_{\mathbf{w}_1} = 2^{11-r_1-r_4}Y^{2j}(XZ)^{r_2+r_3}(X^2 + Z^2)^{r_1+r_4} + 2^{11-r_2-r_3}Y^{2j}(XZ)^{r_1+r_4}(X^2 + Z^2)^{r_2+r_3}.$$

□

LEMMA 4.3. *If* $\mathbf{w}_1 = (\mathbf{b}\ \mathbf{j} - \mathbf{b})$ *with* $\mathbf{b}$ *of odd weight, then*

$$W_{\mathbf{w}_1} = Y^{12}[(X + Z)^{12} - (X - Z)^{12}].$$

PROOF. Let $\mathbf{v} \in \mathscr{C}$ reduce to $\mathbf{w}_1$ modulo 2. Clearly, $\phi(\mathbf{v}) = X^a Y^{12} Z^{12-a}$ for some integer a. We claim that a is odd. This follows as $\mathbf{v}$ is equal to the modulo 4 reduction of $\sum_\alpha c_\alpha \mathbf{r}_\alpha$, where $\sum_\alpha c_\alpha$ is odd. Then as the $\mathbf{r}_\alpha$ are orthogonal and of norm 12 we have

$$\left|\sum_\alpha c_\alpha \mathbf{r}_\alpha\right|^2 = 12\sum_\alpha c_\alpha^2 \equiv 12 \pmod{24}$$

and as

$$\left|\sum_\alpha c_\alpha \mathbf{r}_\alpha\right|^2 = 12 + 4a \pmod 8$$

then a must be odd. Each $\mathbf{u} \in \mathscr{C}$ reducing modulo 2 to $\mathbf{w}_1$ has the form $\pm\mathbf{v} + 2(\mathbf{c}\ \mathbf{c})$, where $\mathbf{c}$ has even weight. Write $\mathbf{u} = \pm\mathbf{v} + 2(\mathbf{c}\ \mathbf{c}) = (\mathbf{u}_1\ \mathbf{u}_2)$. For each position in $\mathbf{u}_1$ either the element there or the corresponding element in $\mathbf{u}_2$ is even but not both. The set of such positions where this even element is 2 has odd cardinality, and we get each such set exactly twice. Thus

$$W_{\mathbf{w}_1} = 2Y^{12}\sum_{r=0}^{5}\binom{12}{2r+1}X^{12-2r}Z^{2r} = Y^{12}\left[(X + Z)^{12} - (X - Z)^{12}\right].$$

□

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

Given a subset $S \subseteq \mathbb{P}^1(\mathbb{F}_{11})$ define $\mathbf{r}_S = \sum_{\alpha \in S} \mathbf{r}_\alpha$. If $|S|$ is even, then $\mathbf{r}_S$ has $r_3 = r_4 = 0$ in the notation of Lemma 4.2. Note that replacing $\mathbf{w}_1$ by $\mathbf{w}_1 D$, where D lies in the group generated by matrices A, B and C, does not alter $W_{\mathbf{w}_1}$. So we need only compute $W_{\mathbf{w}_1}$ for one representative of each orbit under PSL(2, 11) of even size subsets S of $\mathbb{P}^1(\mathbb{F}_{11})$.

The following table gives the orbits of the non-trivial subsets of even cardinality of $\mathbb{P}^1(\mathbb{F}_{11})$ under the action of PSL(2, 11) where we record r_1 and r_2 for the appropriate $\mathbf{r}_S$.

set	size	length of orbit	r_1	r_2
$\{\infty, 0\}$	2	66	5	5
$\{\infty, 0, 1, 2\}$	4	165	4	4
$\{\infty, 0, 1, 3\}$	4	330	6	2
$\{\infty, 1, 3, 4, 5, 9\}$	6	132	1	5
$\{\infty, 2, 6, 7, 8, 10\}$	6	132	5	1
$\{\infty, 0, 2, 5, 6, 9\}$	6	110	3	3
$\{\infty, 1, 2, 3, 4, 9\}$	6	110	3	3
$\{\infty, 2, 7, 8, 9, 10\}$	6	110	3	3
$\{\infty, 0, 2, 3, 5, 7\}$	6	330	3	3
$\{3, 4, 5, 6, 7, 8, 9, 10\}$	8	165	4	0
$\{2, 4, 5, 6, 7, 8, 9, 10\}$	8	330	2	2
$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$	10	66	1	1

The symmetrized weight enumerator of $\mathscr{C}$ is

$$
\begin{aligned}
&(X^2+Z^2)^{12}/2 + (X^2-Z^2)^{12}/2 + 2^{11}X^{12}Z^{12} + 2^{12}Y^{24} \\
&\quad + 66\cdot 2^7 Y^4 (XZ)^5 (X^2+Z^2)^5 + 165\cdot 2^8 Y^8 (XZ)^4 (X^2+Z^2)^4 \\
&\quad + 330\cdot 2^9 Y^8 (XZ)^6 (X^2+Z^2)^2 + 330\cdot 2^5 Y^8 (XZ)^2 (X^2+Z^2)^6 \\
&\quad + 264\cdot 2^6 Y^{12} XZ (X^2+Z^2)^5 + 264\cdot 2^{10} Y^{12} (XZ)^5 (X^2+Z^2) \\
&\quad + 660\cdot 2^9 Y^{12} (XZ)^3 (X^2+Z^2)^3 + 165\cdot 2^{11} Y^{16} (XZ)^4 \\
&\quad + 165\cdot 2^7 Y^{16} (X^2+Z^2)^4 + 330\cdot 2^{10} Y^{16} (XZ)^2 (X^2+Z^2)^2 \\
&\quad + 66\cdot 2^{11} Y^{20} XZ (X^2+Z^2) + 2^{11} Y^{12} (X+Z)^{12} - 2^{11} Y^{12} (X-Z)^{12} \\
&= X^{24} + 66X^{20}Z^4 + 495X^{16}Z^8 + 8448X^{15}Y^4Z^5 + 10560X^{14}Y^8Z^2 \\
&\quad + 42240X^{13}Y^4Z^7 + 105600X^{12}Y^8Z^4 + 2972X^{12}Z^{12} + 66048X^{11}Y^{11}Z \\
&\quad + 84480X^{11}Y^4Z^9 + 496320X^{10}Y^8Z^6 + 1323520X^9Y^{12}Z^3 \\
&\quad + 84480X^9Y^4Z^{11} + 21120X^8Y^{16} + 802560X^8Y^8Z^8 + 495X^8Z^{16} \\
&\quad + 4697088X^7Y^{12}Z^5 + 42240X^7Y^4Z^{13} + 422400X^6Y^{16}Z^2 \\
&\quad + 496320X^6Y^8Z^{10} + 4697088X^5Y^{12}Z^7 + 8448X^5Y^4Z^{15} \\
&\quad + 1140480X^4Y^{16}Z^4 + 105600X^4Y^8Z^{12} + 66X^4Z^{20} + 135168X^3Y^{20}Z \\
&\quad + 1323520X^3Y^{12}Z^9 + 422400X^2Y^{16}Z^6 + 10560X^2Y^8Z^{14}
\end{aligned}
$$

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

$$+ 135168XY^{20}Z^3 + 66048XY^{12}Z^{11} + 4096Y^{24} + 21120Y^{16}Z^8 + Z^{24}$$

in agreement with the computer-assisted computation in [2].

5. Constructions of type A_n

Let a, b, c and d be integers with $c \equiv 2a + b \pmod 4$ and $d \equiv a + 2b \pmod 4$. Then the matrix

$$N = \begin{pmatrix} aI + bS & cI + dS \\ -cI + dS & aI - bS \end{pmatrix}$$

satisfies $NN^T = (a^2 + 11b^2 + c^2 + 11d^2)I_{24}$, and all its rows are in L. Thus the Leech lattice contains an orthogonal frame of 24 vectors each of norm $\frac{1}{4}(a^2+11b^2+c^2+11d^2)$. In [5] Harada, Solé and Gaborit ask whether for $k \geq 2$ there is always a type II code over $\mathbb{Z}_{2k}$ of length 24 and minimum Euclidean weight $8k$. By construction A_{2k} this gives the Leech lattice and an orthogonal frame of vectors of norm $2k$ inside it. From such a frame in the Leech lattice, we can reverse this construction to obtain a type II code over $\mathbb{Z}_{2k}$ and minimum Euclidean weight $8k$. So we can construct such a code given integers a, b, c and d with $c \equiv 2a + b \pmod 4$, $d \equiv a + 2b \pmod 4$ and $k = \frac{1}{8}(a^2+11b^2+c^2+11d^2)$. It is straightforward to express the codes corresponding to such frames as double circulant codes.

LEMMA 5.1. *Let n be a positive integer divisible by 4. If the rank n lattice L contains an orthogonal frame of n vectors of norm m, then it contains an orthogonal frame of n vectors of norm km, for each positive integer k.*

PROOF. By passing to the sublattice generated by the given frame and scaling we may assume that $L = \mathbb{Z}^n$ and the frame consists of the n coordinate vectors. Then as $4 \mid n$ we can further assume that $n = 4$. But the result now reduces to the four-square theorem; we can take the new frame to be (a, b, c, d), $(-b, a, -d, c)$, $(-c, d, a, -b)$ and $(-d, -c, b, a)$ where $k = a^2 + b^2 + c^2 + d^2$. □

THEOREM 5.2. *For each prime $p \neq 11$ there exist a, b, c, $d \in \mathbb{Z}$ with $c \equiv 2a + b \pmod 4$, $d \equiv a + 2b \pmod 4$ and $2p = \frac{1}{4}(a^2 + 11b^2 + c^2 + 11d^2)$.*

PROOF. Consider the lattice

$$L = \{(a, b, c, d) \in \mathbb{Z}^4 : \ d \equiv a + 2b, \ c \equiv 2a + b \pmod 4\}$$

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

but not with the standard inner product, but rather that induced by the quadratic form $\frac{1}{4}(a^2 + 11b^2 + c^2 + 11d^2)$. This lattice is spanned over $\mathbb{Z}$ by vectors $(4, 0, 0, 0)$, $(1, 0, 2, 1)$, $(2, 1, 1, 0)$ and $(0, 0, 4, 0)$ with Gram matrix

$$M = \begin{pmatrix} 4 & 1 & 2 & 0 \\ 1 & 4 & 1 & 2 \\ 2 & 1 & 4 & 1 \\ 0 & 2 & 1 & 4 \end{pmatrix}.$$

Thus L is an even lattice. Define for $\mathrm{Im}(z) > 0$

$$\theta_L(z) = \sum_{\mathbf{w} \in L} q^{\mathbf{w} \cdot \mathbf{w}/2},$$

where $q = \exp(2\pi i z)$. This is the theta function of the lattice L. Then as $11M^{-1}$ has integer entries and $\det M = 11^2$ is a square, θ_L is a modular form of weight 2 for the group

$$\Gamma_0(11) = \left\{ \begin{pmatrix} a & b \\ 11c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - 11bc = 1 \right\}$$

[4, Theorem 3.2]. The space of such modular forms is two-dimensional [6, Theorem 9.10] and is spanned by forms E and ϕ as defined below. We define

$$E(z) = 10 + 24 \sum_{n=1}^{\infty} (\sigma_1(n) - 11\sigma_1(n/11))q^n$$

[9, Section VII.3.5], where $\sigma_1(n)$ is the sum of divisors of n when n is an integer and zero otherwise. (This is a multiple of the form $E(z; 11)$ in Schoeneberg's notation, but beware of the sign error in his formula). Also

$$\phi(z) = \eta(z)^2 \eta(11z)^2 = \sum_{n=1}^{\infty} c_n q^n$$

[6, Chapter XI (11.5)], where

$$\eta(z) = \exp(\pi i z/12) \prod_{n=1}^{\infty} (1 - q^n).$$

The form ϕ is the cusp form associated to the elliptic curve $y^2 + y = x^3 - x^2$ of conductor 11 [6, Chapter XI (11.15)]. In particular, the number of points in the projective closure of $y^2 + y = x^3 - x^2$ with coordinates in the field $\mathbb{F}_p$ is $1 + p - c_p$

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press

for $p \neq 11$. Hence $c_p < 2\sqrt{p}$ whenever $p \neq 11$ is prime by Hasse's Theorem [6, Theorem 10.5]. The coefficient of q^1 in θ_L vanishes, so that

$$\theta_L(z) = \frac{E(z) - 24\phi(z)}{10} = 1 + 12\sum_{n=1}^{\infty} \frac{\sigma_1(n) - 11\sigma(n/11) - c_n}{5} q^n.$$

For a prime $p \neq 11$ the q^p coefficient of θ_L is

$$(12/5)(p + 1 - c_p) > (12/5)(p + 1 - 2\sqrt{p}) = (12/5)(\sqrt{p} - 1)^2 > 0.$$

Thus L always has a vector of squared length $2p$ for $p \neq 11$. □

COROLLARY 5.3. *For each integer k which is not a power of 11, there is an orthogonal frame of norm $2k$ in the Leech lattice.*

PROOF. By Theorem 5.2 the result is true whenever k is a prime other than 11. But Lemma 5.1 shows that if it is valid for k, then it is also valid for all multiples of k. Unless k is a power of 11, k has a prime factor not equal to 11 and the result is valid for k. □

References

[1] A. Bonnecaze, P. Solé and A. R. Calderbank, 'Quaternary quadratic residue codes and unimodular lattices', *IEEE Trans. Inform. Theory* **41** (1985), 366–377.
[2] A. R. Calderbank and N. J. A. Sloane, 'Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices', *J. Algebraic Combin.* **6** (1997), 119–131.
[3] J. H. Conway, 'A characterisation of Leech's lattice', *Invent. Math.* **7** (1969), 137–142.
[4] W. Ebeling, *Lattices and codes* (Vieweg, Braunschweig/Wiesbaden, 1994).
[5] M. Harada, P. Solé and P. Gaborit, 'Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey', in: *Algebra and Combinatorics: an International Congress, ICAC '97, Hong Kong* (Springer-Verlag, Singapore, 1999).
[6] A. Knapp, *Elliptic curves* (Princeton University Press, Princeton, 1992).
[7] J. Leech, 'Notes on sphere packings', *Canad. J. Math* **19** (1967), 251–267.
[8] J. McKay, 'A setting for the Leech lattice' in: *Finite Groups '72* (ed. T. M. Gagen) (North-Holland, Amsterdam, 1973).
[9] B. Schoeneberg, *Elliptic modular functions* (Springer, Berlin, 1974).

School of Mathematical Sciences
University of Exeter
Exeter
EX4 4QE
UK
e-mail: rjc@maths.ex.ac.uk

https://doi.org/10.1017/S1446788700002469 Published online by Cambridge University Press