

Steinitz classes of unimodular lattices

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

9 December 2002

Abstract

For each prime l with $l \equiv 7 \pmod{8}$, we define an action of the ring $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{-l})]$ on the unimodular lattice D_{l+1}^+ using a Paley matrix. We determine the isomorphism class of D_{l+1}^+ as an $\mathcal{O}$ -module. In particular we show that unless $l = 7$, D_{l+1}^+ is not a free $\mathcal{O}$ -module. We note a consequence for the Leech lattice.

1 Introduction

In [1] the author explained how given an n -by- n skew-symmetric conference matrix W one can give $\mathbf{R}^n$ a structure of a vector space over $\mathbf{C}$. When n is a multiple of 8, with respect to this structure the unimodular lattice D_n^+ becomes a module over the ring $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{1-n})]$. Using this module structure we can derive other unimodular lattices. One natural question is to determine the structure of D_n^+ as a $\mathcal{O}$ -module. Here we answer this question completely whenever W is a conference matrix of Paley type. It turns out that unless $n = 8$, D_n^+ is not free over $\mathcal{O}$. As a corollary we show that the Leech lattice is not a free module with respect to a natural action of $\mathbf{Z}[\frac{1}{2}(1 + \sqrt{-23})]$.

2 The Paley matrix

We fix a prime l congruent to 7 modulo 8 and define n to be $l + 1$.

We define the Paley matrix W_l as follows. Let

$$W_l = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & W'_l & \\ -1 & & & \end{pmatrix}$$

where the l -by- l matrix W' is the circulant matrix whose (i, j) -entry is the Legendre symbol $\left(\frac{j-i}{l}\right)$.

As the Paley matrix is intimately related to quadratic residue codes, we follow the usual practice with quadratic residue codes and label the entries of a typical vector of length $n = l + 1$ using the elements of the projective line $\mathbf{P}^1(\mathbf{F}_l)$ over $\mathbf{F}_l$ as follows: $\mathbf{v} = (v_\infty, v_0, v_1, v_2, \dots, v_{l-1})$. We let $\mathbf{e}_\infty, \mathbf{e}_0, \mathbf{e}_1, \dots, \mathbf{e}_{l-1}$ denote the corresponding unit vectors, that is, $\mathbf{e}_\mu$ has a one in the position labelled μ , and zeros elsewhere.

A *conference matrix* of order n is a square matrix A with zeroes on the main diagonal and off-diagonal entries ± 1 satisfying $AA^t = (n - 1)I$.

Lemma 1 (Paley) *The matrix W_l is a skew-symmetric conference matrix of order $l + 1$.*

Proof See for instance [3, Chapter 18]. □

In particular $W_l^2 = -lI$. We define an action of $\mathbf{C} = \mathbf{R}(\sqrt{-l})$ on the Euclidean space $\mathbf{R}^n$ by $(a + b\sqrt{-l})\mathbf{u} = a\mathbf{u} + b\mathbf{u}W$. Let $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{-l})]$. Then $\mathcal{O}$ is the maximal order of the quadratic number field $K = \mathbf{Q}(\sqrt{-l})$ and so $\mathcal{O}$ is a Dedekind domain. In [1] the author proved that the unimodular lattice D_n^+ is a $\mathcal{O}$ -module, under this action. We shall investigate its Steinitz class.

Let us recall the definition of D_n^+ . It consists of all $(a_\infty, a_0, \dots, a_{l-1}) \in \mathbf{R}^n$ such that all $2a_\mu$ are integers of the same parity and $\sum_\mu a_\mu$ is even. It is an even unimodular lattice. As an $\mathcal{O}$ -module, D_n^+ is finitely generated and torsion-free. Hence it is a projective $\mathcal{O}$ -module. If $\mathcal{M}$ is a finitely generated projective module over $\mathcal{O}$ then $\mathcal{M} \cong \mathcal{O}^{r-1} \oplus \mathcal{I}$ where $\mathcal{I}$ is an ideal of $\mathcal{O}$. The Steinitz class of $\mathcal{M}$ is the class $[\mathcal{I}]$ of $\mathcal{I}$ in the classgroup of $\mathcal{O}$. It is uniquely determined by $\mathcal{M}$. We shall denote it by $s(\mathcal{M})$. If $\mathcal{M}'$ is a submodule of $\mathcal{M}$ with $\mathcal{M}/\mathcal{M}'$ torsion, then $s(\mathcal{M}') = [|\mathcal{M} : \mathcal{M}'|]s(\mathcal{M})$. Here $|\mathcal{M} : \mathcal{M}'|$ is the module index: if $\mathcal{M}/\mathcal{M}' \cong \bigoplus_{j=1}^k (\mathcal{O}/\mathcal{I}_j)$ then $|\mathcal{M} : \mathcal{M}'| = \prod_{j=1}^k \mathcal{I}_j$.

(For basic results on projective modules over Dedekind domains see, for instance, [2, §9.6].)

3 The main theorem

We state and prove a theorem giving the Steinitz class of D_n^+ with respect to the Paley matrix W_l .

Theorem 1 *Let $n = l + 1$ where l is prime and $l \equiv 7 \pmod{8}$. The Paley matrix W_l induces the structure of an $\mathcal{O}$ -module on D_n^+ where $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{-l})]$. The Steinitz class of D_n^+ with respect to this $\mathcal{O}$ -module structure is $[\langle n/8, \frac{1}{2}(1 - \sqrt{-l}) \rangle]$.*

Proof We identify a $\mathcal{O}$ -submodule Λ of D_n^+ for which we can calculate $|D_n^+ : \Lambda|$. We shall prove that Λ is free over $\mathcal{O}$.

Let

$$\Lambda = \{(u_\infty, \dots, u_{l-1}) \in D_n^+ : u_\infty + \dots + u_{l-1} \equiv 0 \pmod{n/4}\}.$$

It is clear that Λ is a sublattice of D_n^+ and that D_n^+/Λ is a cyclic group of order $n/8$ generated by the image of $2\mathbf{e}_\infty$. We need to show that Λ is a $\mathcal{O}$ -module. For that it is sufficient that $\frac{1}{2}(1 + \sqrt{-l})\Lambda \subseteq \Lambda$. In fact, $\frac{1}{2}(1 + \sqrt{-l})D_n^+ \subseteq \Lambda$. The lattice D_n^+ is spanned by the vectors $v = \frac{1}{2} \sum_\mu \mathbf{e}_\mu$ and the $\mathbf{e}_\infty + \mathbf{e}_\mu$ for $\mu \in \mathbf{P}^1(\mathbf{F}_l)$. Now $\frac{1}{2}(1 + \sqrt{-l})v = v - (n/4)\mathbf{e}_\infty \in \Lambda$, $\frac{1}{2}(1 + \sqrt{-l})2\mathbf{e}_\infty = 2v \in \Lambda$ and each vector $\frac{1}{2}(1 + \sqrt{-l})(\mathbf{e}_\infty + \mathbf{e}_j)$ for $0 \leq j < l$ has $n/2$ ones and $n/2$ zeroes and so lies in Λ . Thus Λ is an $\mathcal{O}$ -module, and the $\mathcal{O}$ -module D_n^+/Λ is annihilated by $\frac{1}{2}(1 + \sqrt{-l})$. But D_n^+/Λ is a cyclic group of order $n/8$ and so is a cyclic $\mathcal{O}$ -module whose annihilator contains the ideal $\mathcal{J} = \langle n/8, \frac{1}{2}(1 + \sqrt{-l}) \rangle$. As $|\frac{1}{2}(1 + \sqrt{-l})|^2 = n/4$ is a multiple of $n/8$, this ideal has norm $n/8$. Hence $D_n^+/\Lambda \cong \mathcal{O}/\mathcal{J}$ as $\mathcal{O}$ -modules.

The Steinitz class of D_n^+ is

$$s(D_n^+) = [\mathcal{J}]^{-1}s(\Lambda) = [\overline{\mathcal{J}}]s(\Lambda) = \left[\left\langle n/8, (1 - \sqrt{-l})/2 \right\rangle \right] s(\Lambda).$$

To prove the theorem it only remains to prove that Λ is a free $\mathcal{O}$ -module.

We have already defined $v = \sum_\mu \mathbf{e}_\mu$. Define, for $0 \leq j < l$, $u_j = \mathbf{e}_\infty - \mathbf{e}_j$. Note that $v \in \Lambda$ and each $u_j \in \Lambda$. We shall prove that the $n/2$ vectors $v, u_0, u_1, \dots, u_{n/2-2}$ generate Λ freely over $\mathcal{O}$. Let Λ' be the $\mathcal{O}$ -submodule of Λ generated by $v, u_0, u_1, \dots, u_{n/2-2}$. It suffices to prove that $\Lambda' = \Lambda$. The lattice Λ' is the set of integer linear combinations of the vectors

$$(1 - \sqrt{-l})v/2, u_0, u_1, \dots, u_{n/2-2}, \\ (1 + \sqrt{-l})u_0/2, (1 + \sqrt{-l})u_1/2, \dots, (1 + \sqrt{-l})u_{n/2-2}/2, v.$$

Let M denote the n -by- n matrix with the above vectors as rows, in the order given. Then $|D_n^+ : \Lambda'| = |\det(M)|$ and so the assertion that $\Lambda' = \Lambda$ is equivalent to the assertion that $\det(M) = \pm n/8$.

Now

$$M = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix}$$

where the matrices M_i are $n/2$ -by- $n/2$. Hence $\det(M) = \det(M_1)\det(M_3)$. Also

$$M_1 = \begin{pmatrix} n/4 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{pmatrix}$$

and so $\det(M_1) = \pm n/4$. It suffices to prove that $\det(M_3) = \pm 1/2$.

The entries of M_3 are given by

$$(M_3)_{i,j} = \begin{cases} \frac{1}{2} \left[1 - \left(\frac{j-i+(l-1)/2}{l} \right) \right] & \text{if } i < n/2, \\ 1/2 & \text{if } i = n/2. \end{cases}$$

It suffices to show that $\det(N) = \pm 1$ where N is the $n/2$ -by- $n/2$ matrix with entries

$$N_{i,j} = \begin{cases} \frac{1}{2} \left[1 - \left(\frac{j-i+(l-1)/2}{l} \right) \right] & \text{if } i < n/2, \\ 1 & \text{if } i = n/2. \end{cases}$$

To show that $\det(N) = \pm 1$, we shall show that the matrix N , which has integer entries, is nonsingular considered as a matrix modulo every prime number p .

We extend the matrix N to an $n/2$ by l matrix N' with entries

$$N'_{i,j} = \begin{cases} 0 & \text{if } i < n/2, \text{ and } \left(\frac{j-i}{l} \right) = 1 \\ 1 & \text{if } i < n/2, \text{ and } \left(\frac{j-i}{l} \right) = -1 \\ t & \text{if } i < n/2, \text{ and } i = j \\ 1 & \text{if } i = n/2. \end{cases}$$

where we shall specify t later. The matrix N is formed by taking the last $n/2$ columns of N' . We claim that it is possible to choose t such that N' is the generator matrix of a cyclic code.

For each field K and positive integer m , we can identify the vector space K^m with the quotient ring $K[X]/\langle X^m - 1 \rangle$ by identifying the vector $(a_0, a_1, \dots, a_{m-1})$ with the polynomial $\sum_{j=0}^{m-1} a_j X^j$. A subspace of K^m corresponding to an ideal of $K[X]/\langle X^m - 1 \rangle$ is called a *cyclic code*. Each

ideal of $K[X]/\langle X^m - 1 \rangle$ is principal, and equals $\langle g(X) \rangle$ where g is a monic factor of $X^m - 1$. If the degree of g is d then the dimension of the corresponding cyclic code is $m - d$. The polynomial g is called the *generator polynomial* of the cyclic code. A matrix whose rows form a basis of a cyclic code is called a *generator matrix* of the cyclic code.

For $p \neq l$ we take K to be the finite field $\mathbf{F}_p(\zeta)$ where ζ is a primitive l -th root of unity, and for $p = l$ we take $K = \mathbf{F}_p$ and set $\zeta = 1$.

The first row of N' corresponds to the polynomial

$$f(X) = t + \sum_{\substack{0 \leq j < l \\ (j/l) = -1}} X^j.$$

All but the last row of N' is a cyclic shift of the first row, and they correspond to the $X^i f(X) \in K[X]/\langle X^l - 1 \rangle$ for $0 \leq i \leq (l-3)/2$. The last row corresponds to the polynomial

$$g(X) = \sum_{j=0}^{l-1} X^j = \frac{X^l - 1}{X - 1}.$$

Set

$$t = - \sum_{\substack{0 \leq j < l \\ (j/l) = -1}} \zeta^j$$

and

$$\phi(X) = \prod_{\substack{0 \leq j < l \\ (j/l) = 1}} (X - \zeta^j).$$

We aim to show that N' is a generator matrix for the cyclic code with generator polynomial $\phi(X)$.

We have

$$\phi(X) = \prod_{\substack{0 \leq j < l \\ (j/l) = 1}} (X - \zeta^j), \quad g(X) = \prod_{0 \leq j < l} (X - \zeta^j), \quad \text{and} \quad X^l - 1 = \prod_{0 \leq j < l} (X - \zeta^j).$$

Hence $\phi(X) \mid g(X) \mid (X^l - 1)$. Also when $\left(\frac{i}{l}\right) = 1$ we have

$$f(\zeta^i) = -t + \sum_{\substack{0 \leq j < l \\ (j/l) = -1}} \zeta^{ij} = -t + \sum_{\substack{0 \leq k < l \\ (k/l) = -1}} \zeta^k = 0.$$

Hence $(X - \zeta^i) \mid f(X)$ whenever $\left(\frac{i}{l}\right) = 1$. When $p \leq l$ there are $(l-1)/2$ distinct ζ^i with $\left(\frac{i}{l}\right) = 1$ and so $\phi(X) \mid f(X)$. Also when $\left(\frac{i}{l}\right) = -1$

$$f(\zeta^i) = -t + \sum_{\substack{0 \leq j < l \\ (j/l) = -1}} \zeta^{ij} = -t + \sum_{\substack{0 \leq k < l \\ (k/l) = 1}} \zeta^k = \sum_{k=1}^{l-1} \left(\frac{k}{l}\right) \zeta^k.$$

This last expression is a quadratic Gauss sum, whose square equals $\left(\frac{-1}{l}\right) l = -l$. When $p \neq l$ it follows that $f(\zeta^i) \neq 0$ when $\left(\frac{i}{l}\right) = -1$, and so $\phi(X)$ is the greatest common divisor of $f(X)$ and $g(X)$.

The above argument collapses when $p = l$, yet in this case it is still true that $f(X)$ and $g(X)$ have greatest common divisor $\phi(X) = (X - 1)^{(l-1)/2}$. It suffices to show that $f(X)$ is divisible by $(X - 1)^{(l-1)/2}$ but not by $(X - 1)^{(l+1)/2}$, or equivalently that the r -th derivative of f vanishes at 1 for $0 \leq r < (l - 1)/2$ but is does not vanish at 1 for $r = (l - 1)/2$. Let $r > 0$ be an integer. Then

$$f^{(r)}(1) = \sum_{\substack{0 < j < l \\ (j/l) = -1}} j(j-1) \cdots (j-r+1).$$

For $0 < s < (l - 1)/2$,

$$\sum_{\substack{0 < j < l \\ (j/l) = -1}} j^s = 0$$

and so $f^{(r)}(1) = 0$ when $r < (l - 1)/2$. But

$$\sum_{\substack{0 < j < l \\ (j/l) = -1}} j^{(l-1)/2} = -(l - 1)/2$$

and so $f^{(l-1)/2}(1) \neq 0$. In this case too, the greatest common divisor of $f(X)$ and $g(X)$ is $\phi(X)$.

The row space of the matrix N' corresponds to the set of polynomials of the form

$$a(X)f(X) + rg(X) + c(X)(X^l - 1) \quad (*)$$

where the degree of the polynomial $a(X)$ is at most $(l-3)/2$, $r \in K$ and $c(X)$ is a polynomial. To show that N' is the generator matrix of the cyclic code with generator matrix $\phi(X)$ we must show that each multiple $b(X)\phi(X)$ of $\phi(X)$ has the form $(*)$. Certainly

$$b(X)\phi(X) = u(X)f(X) + v(X)g(X)$$

for some polynomials $u(X)$ and $v(X)$. Now $f(X) = \phi(X)f_1(X)$ and $g(X) = \phi(X)g_1(X)$ where $g_1(X)$ has degree $(l-1)/2$. We may write $u(X) = a(X) + q(X)g_1(X)$ where $a(X)$ has degree at most $(l-3)/2$. Then

$$b(X) = u(X)f_1(X) + v(X)g_1(X) = a(X)f_1(X) + [q(X)f_1(X) + v(X)]g_1(X)$$

and so

$$b(X)\psi(X) = a(X)f(X) + w(X)g(X)$$

for some polynomial $w(X)$. Now $w(X) = w(1) + (X - 1)c(X)$ for some polynomial $c(X)$ and so

$$\psi(X) = a(X)f(X) + w(1)g(X) + c(X)(X^l - 1)$$

as required.

As the cyclic code generated by $\phi(X)$ has dimension $(l + 1)/2$, the rows of N' are linearly independent. Another generator matrix for this cyclic code is the matrix B' whose rows correspond to the polynomials $X^i\phi(X)$ for $0 \leq i \leq (l - 1)/2$. The matrices N' and B' are row equivalent. Thus the matrices N and B are row equivalent where B is the matrix formed by the last $(l + 1)/2$ columns of B' . But B' is lower triangular, having all diagonal entries 1. Thus B and also N are nonsingular over K and so N is nonsingular over $\mathbf{F}_p$. As N is nonsingular over $\mathbf{F}_p$ for all primes p , then $\det(N) = \pm 1$. Thus $\det(M) = \pm n/8$, $\Lambda = \Lambda'$ is a free $\mathcal{O}$ -module and

$$s(D_n^+) = \left[\left\langle n/8, (1 - \sqrt{-l})/2 \right\rangle \right].$$

□

It is immediate that due to this theorem D_n^+ is only free over $\mathcal{O}$ when $l = 7$.

Corollary 1 *The $\mathcal{O}$ -module D_n^+ is free if and only if the prime $l = 7$.*

Proof The classgroup of $\mathbf{Z}[\frac{1}{2}(1 + \sqrt{-7})]$ is trivial, and so when $l = 7$ the $\mathcal{O}$ -module D_8^+ must be free.

Suppose that $l > 7$. The $\mathcal{O}$ -module D_n^+ is free if and only if the ideal $\mathcal{I} = \langle n/8, \frac{1}{2}(1 - \sqrt{-l}) \rangle$ is principal. Suppose that $\mathcal{I} = \langle \alpha \rangle$. Then $|\alpha|^2 = n/8 > 1$. We cannot have $\alpha \in \mathbf{Z}$ for then $|\alpha| > 1$ and so $\alpha \nmid \frac{1}{2}(1 - \sqrt{-l})$ in $\mathcal{O}$. On the other hand if $\alpha \notin \mathbf{Z}$ then $|\alpha|^2 \geq \min(l, (l + 1)/4) = n/4$ which is a contradiction. We conclude that $\mathcal{I}$ is not principal and D_n^+ is not free over $\mathcal{O}$. □

In [1] the Leech lattice Λ_{24} was constructed by considering the action of $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{-23})]$ on D_{24}^+ as given by the Paley matrix W_{23} . With this $\mathcal{O}$ -module structure, Λ_{24} is $2^{-1/2}\mathcal{I}D_{24}^+$ where $\mathcal{J} = \langle 2, \frac{1}{2}(1 + \sqrt{-l}) \rangle$. Consequently, $s(\Lambda_{24}) = [\mathcal{J}]^{12}s(D_{24}^+) = s(D_{24}^+)$ as the classgroup of $\mathcal{O}$ has order 3. Thus Λ_{24} and D_{24}^+ are isomorphic as $\mathcal{O}$ -modules, and we obtain the amusing result that under a very natural action of the ring $\mathcal{O}$, the Leech lattice is not a free module.

References

- [1] R. Chapman, ‘Conference matrices and unimodular lattices’ *European J. Combin.* **22** (2001), 1033–1045
- [2] P. M. Cohn, *Algebra* vol. 2 (2nd ed.), John Wiley & Sons, 1989.
- [3] J .H. van Lint & R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.