JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

ROBIN CHAPMAN
STEVEN T. DOUGHERTY
PHILIPPE GABORIT
PATRICK SOLÉ

2-modular lattices from ternary codes

Journal de Théorie des Nombres de Bordeaux, tome 14, nº 1 (2002), p. 73-85

<http://www.numdam.org/item?id=JTNB_2002__14_1_73_0>

© Université Bordeaux 1, 2002, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Journal de Théorie des Nombres
de Bordeaux **14** (2002), 73–85

2–modular lattices from ternary codes

par Robin CHAPMAN, Steven T. DOUGHERTY,
Philippe GABORIT et Patrick SOLÉ

Résumé. L'alphabet $\mathbf{F}_3 + v\mathbf{F}_3$ où $v^2 = 1$ est vu ici comme le quotient de l'anneau des entiers du corps de nombres $\mathbf{Q}(\sqrt{-2})$ par l'idéal (3). Les codes sur cet alphabet qui sont autoduaux pour le produit scalaire hermitien donnent des réseaux 2–modulaires par la construction A_K. Il existe une application de Gray qui envoie les codes auto-duaux pour le produit scalaire euclidien sur les codes de Type III avec une involution sans points fixes dans leur groupe d'automorphismes. On démontre des théorèmes style Gleason pour les polynômes de poids symmétrisés des codes auto-duaux euclidiens et pour les polynômes de poids "longueur" des codes auto-duaux hermitiens. Une application est la construction d'un réseau 2–modulaire optimal de dimension 18 et de norme 3 et de nouveaux réseaux 2–modulaires de norme 3 en dimensions $16, 18, 20, 22, 24, 26, 28$ et 30.

Abstract. The alphabet $\mathbf{F}_3 + v\mathbf{F}_3$ where $v^2 = 1$ is viewed here as a quotient of the ring of integers of $\mathbf{Q}(\sqrt{-2})$ by the ideal (3). Self-dual $\mathbf{F}_3 + v\mathbf{F}_3$ codes for the Hermitian scalar product give 2–modular lattices by construction A_K. There is a Gray map which maps self-dual codes for the Euclidean scalar product into Type III codes with a fixed point free involution in their automorphism group. Gleason type theorems for the symmetrized weight enumerators of Euclidean self-dual codes and the length weight enumerator of Hermitian self-dual codes are derived. As an application we construct an optimal 2-modular lattice of dimension 18 and minimum norm 3 and new odd 2-modular lattices of norm 3 for dimensions $16, 18, 20, 22, 24, 26, 28$ and 30.

1. Introduction

Recent years witnessed a burst of activity in codes over $\mathbf{Z}_4$ [6, 11, 12, 14, 2, 3, 20] with applications to (nonlinear) binary codes [14] and unimodular lattices [2, 20]. Another important alphabet of size 4 besides $\mathbf{Z}_4$ is $\mathbf{F}_2 + u\mathbf{F}_2$ introduced in [1] to construct lattices, and explored further in [10] to study self-dual binary codes with a fixed point free (fpf) involution in

Manuscrit reçu le 14 décembre 2000.

their automorphism groups. This last class of codes was introduced in [4]. The current work is a ternary analogue of [10]. Here self-dual ternary codes with a fixed point free involution are characterized as Gray images of self-dual codes over $R_3 := \mathbf{F}_3 + v\mathbf{F}_3$ for the Euclidean scalar product. For instance Pless symmetry codes admit a natural description as Gray images of extended cyclic codes over R_3. The natural weight is the Lee weight defined as the Hamming weight of the Gray image with values $0, 1, 2$.

While $\mathbf{F}_2 + u\mathbf{F}_2$ is a local ring like $\mathbf{Z}_4$ the alphabet $\mathbf{F}_3 + v\mathbf{F}_3$ is a semi-local ring like $\mathbf{Z}_6$. It is, as noticed in [1] abstractly isomorphic to $\mathbf{F}_3 \times \mathbf{F}_3$. The main technical tool in that context is therefore the Chinese Remainder Theorem (CRT). Another way to look at it would be the $(u+v, u-v)$ construction [15, 16].

Following [1] we view R_3 (or $\mathbf{F}_3 \times \mathbf{F}_3$) as a quotient of the ring of integers of $\mathbf{Q}(\sqrt{-2})$ by the ideal (3). This induces a conjugation on R_3, making it necessary to introduce a Hermitian scalar product. The natural weight attached to that number field is the length function which takes values $0, 1, 2, 3$. By construction A of [17] (Chap. 7) we obtain odd 2−modular lattices as per the definition in [22].

2. Notation and Definitions

2.1. Codes. Let R_3 denote the ring with 9 elements $\mathbf{F}_3 + v\mathbf{F}_3$ where $v^2 = 1$. This ring contains two maximal ideals $(v-1)$ and $(v+1)$. Observe that both of $R_3/(v+1)$ and $R_3/(v-1)$ are $\mathbf{F}_3$. The CRT tells us that

$$R_3 = (v-1) \oplus (v+1).$$

More concretely, linear algebra over $\mathbf{F}_3$ shows that

$$a + vb = (a-b)(v-1) - (a+b)(v+1),$$

for all $a, b \in \mathbf{F}_3^n$.

A code over R_3 is an R_3−submodule of R_3^n. The Euclidean scalar product is

$$\sum_i x_i y_i.$$

The Gray map ϕ from R_3^n to $\mathbf{F}_3^{2n}$ is defined as $\phi(x+vy) = (x, y)$ for all $x, y \in \mathbf{F}_3^n$. The Lee weight of $x+vy$ is the Hamming weight of its Gray image. Define the Lee composition of x say $m_i(x)$, $i = 0, 1, 2$, as the number of entries in x of weight i. The symmetrized length weight enumerator (slwe), whose name will be justified in the next subsection, is then

$$\mathrm{slwe}_C(a, b, c) = \sum_{x \in C} a^{m_0(x)} b^{m_1(x)} c^{m_2(x)}.$$

The swap map on $\mathbf{F}_3^{2n}$ is defined as

$$s((x, y)) = (y, x)$$

for all $x, y \in \mathbf{F}_3^n$.

2.2. Lattices. Let K be the quadratic number field $\mathbf{Q}(\sqrt{-2})$ with ring of integers $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$. Then define $R_3 := \mathcal{O}/(3)$. Denote by a bar the conjugation which fixes $\mathbf{F}_3$ and maps b to $-b$. Consequently, the natural scalar product induced by the Hermitian scalar product of $\mathbf{C}^n$ is

$$\sum_i x_i \overline{y_i}.$$

The length function as defined in [1, p.96] is

$$l_K(a) := \inf\{x\overline{x} \ : x \equiv a \pmod 3\}.$$

Noticing that $\sqrt{-2} \equiv v \pmod 3$, and using the fact that K is Euclidean we see that

$$l_K(\pm 1) = 1 < 9$$

$$l_K(\pm v) = 2 < 9.$$

$$l_K(\pm 1 + \pm v) = 3 < 9.$$

We then extend l_K componentwise to R_3^n. Define the length composition $n_i(x)$ $i = 0, \ldots, 3$ of $x \in R_3^n$ as the number of coordinates of length i. The length weight enumerator (lwe) can then be defined as

$$\mathrm{lwe}_C(a, b, c, d) = \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)} d^{n_3(x)}$$

Define the minimum length $l(C)$ of a code C as the minimum of the length of a nonzero element.

Define construction $A_K(C)$ as the preimage in $\mathcal{O}^n$ of $C \subseteq R_3^n$. Recall that an integral lattice is $l-$modular [1, 18] for some prime l if its dual is equivalent to itself by a similarity of rate $\sqrt{l}$.

Theorem 2.1. *If $C \subseteq R_3^n$ is a self-dual code then the lattice $A_K(C)/\sqrt{3}$ is $2-$modular. Its norm is equal to the minimum of 3 and $l(C)/3$.*

Proof. The first assertion follows by [1, Remark 3.8] and can alternatively be derived directly by checking that $\mathcal{O}$ is 2-modular for the bilinear form

$$(x, y) \mapsto Tr_K(x\overline{y})/2.$$

The second assertion follows by observing that the lattice above contains vectors of the shape $3/\sqrt{3}(10^{n-1})$ whose norm is 3. □

3. Structure and duality of codes over R_3

By the properties of CRT any code over R_3 is permutation-equivalent to a code generated by the following matrix:

$$\begin{pmatrix} I_{k_1} & (1-v)B_1 & (1+v)A_1 & (1+v)A_2+(1-v)B_2 & (1+v)A_3+(1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix} \tag{1}$$

where A_i and B_j are ternary matrices. Such a code is said to have rank $\{9^{k_1}, 3^{k_2}, 3^{k_3}\}$.

If H is a code over R_3. Let H^+ (resp. H^-) be the ternary code such that $(1+v)H^+$ (resp. $(1-v)H^-$) is read $H \, mod\,(1-v)$ (resp. $H \, mod\,(1+v)$). We have: $H = (1+v)H^+ \oplus (1-v)H^-$ with:

$$H^+ = \{s \mid \exists t \in \mathbf{F}_3^n \mid (1+v)s + (1-v)t \in H\}$$

and

$$H^- = \{t \mid \exists s \in \mathbf{F}_3^n \mid (1+v)s + (1-v)t \in H\}$$

The code H^+ is permutation-equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix}, \tag{2}$$

where A_i are ternary matrices. And the ternary code H^- is permutation-equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix}, \tag{3}$$

where B_i are ternary matrices.

The preceding statements show that any code H over $\mathbf{F}_3$ is completely characterized by its associated codes H^+ and H^- and conversely. We give now a characterization of the dual of a code depending on the scalar product.

Theorem 3.1. *Let H be a code of length n over R_3, with associated ternary codes H^+ and H^- then for the Hermitian scalar product:*

$$H^\perp = (1+v)(H^-)^\perp \oplus (1-v)(H^+)^\perp,$$

and the self-dual codes over R_3 are the codes H with associated ternary codes H^+ and H^- verifying $H^+ = (H^-)^\perp$.

Proof. Observe that if c, c', d, d' are ternary vectors of length n then

$$(c(1-v) + d(1+v))\overline{(c'(1-v) + d'(1+v))} = a(1-v) + b(1+v)$$

with $-a = cd'$ and $-b = dc'$. This shows that $a = b = 0$ if and only if $dc' = cd' = 0$. □

Here is the analogue of the preceding theorem for Euclidean codes.

Theorem 3.2. *Let H be a code of length n over R_3, with associated ternary codes H^+ and H^-, then for the Euclidean scalar product:*

$$H^\perp = (1+v)(H^+)^\perp \oplus (1-v)(H^-)^\perp,$$

and the self-dual codes over R_3 are the codes H with associated ternary codes H^+ and H^- such that H^+ and H^- are self-dual ternary codes.

Proof. Observe that if c, c', d, d' are ternary vectors of length n then

$$(c(1-v)+d(1+v))(c'(1-v)+d'(1+v)) = a(1-v)+b(1+v)$$

with $-a = cc'$ and $-b = dd'$. This shows that $a = b = 0$ if and only if $cc' = dd' = 0$. □

This shows, in particular, that Euclidean self-dual codes exist in length n if and only if n is a multiple of 4, since self-dual codes over $\mathbf{F}_3$ exist only for length a multiple of 4.

The number of distinct self-dual sub-spaces (and therefore the mass formula) for each duality can be deduced from the preceding theorems:

Theorem 3.3. *Denote by $N_e(n)$ the number of distinct self-dual codes of length n over R_3 for the Euclidean scalar product then n is a multiple of 4 and:*

$$N_e(n) = [2\prod_{i=1}^{\frac{n-2}{2}}(3^i+1)]^2.$$

Proof. Self-dual codes over $\mathbf{F}_3$ are known to exist only for length n a multiple of 4 and the number $\sigma(n)$ of such sub-spaces has been calculated in [19]. In our case, applying the preceding theorem on the Euclidean duality, we deduce $N_e(n)$ only by squaring $\sigma(n)$. □

Theorem 3.4. *Denote by $N_h(n)$ the number of distinct self-dual codes of length n over R_3 for the Hermitian scalar product then:*

$$N_h(n) = 1 + \sum_{k=1}^{n}[\prod_{i=0}^{k-1}\frac{3^{n-i}-1}{3^{i+1}-1}].$$

Proof. Let $H(H^+, H^-)$ be a self-dual Hermitian code of length n. If H^+ is given, then H^- has to be its dual. So that the number of distinct self-dual codes is equal to the number of possible ternary code of length n. The number of ternary codes of length n and dimension k, calculated by induction, is $\prod_{i=0}^{k-1}\frac{3^{n-i}-1}{3^{i+1}-1}$, the total number follows. □

Corollary 3.5. *If (C, D) denotes a pair of self-dual ternary codes of length n then $\phi(C(1-v)+D(1+v))$ is a self-dual code with a fixed point free involution involutory automorphism.*

Proof. By preceding Theorem we know that $C(1-v)+D(1+v)$ is self-dual. But $(a+vb)(a'+vb')=0$ yields $aa'+bb'=0$ i.e. $\phi(a+vb)\phi(a'+vb')=0$. The first assertion follows. The second assertion follows by noticing that the Gray image of multiplication by v is the swap of the Gray image :

$$\phi(v(x+vy)) = (y,x) = s(\phi(x+vy)).$$

□

Now, we characterize a class of ternary self-dual codes with a special symmetry property.

Theorem 3.6. *Up to permutation of coordinates, every self-dual ternary code T of length $2n$ with a fixed point free involutory automorphism can be realized as $\phi(C)$ for some self-dual C of length n over R_3 for the Euclidean scalar product.*

Proof. Let σ be such an automorphism. Write an arbitrary element of T as $(a,\sigma(a))$ with $a \in \mathbf{F}_3^n$. Take C to be the code of R_3^n consisting of all $a+v\sigma(a)$. To check that C is self-dual observe that if $t := (a,b)$ and $t' := (a',b')$ are in T so is $s(t') = (b',a')$. Now the inner product $\phi^{-1}(t)\phi^{-1}(t') = (a+bv)(a'+b'v)$ is $tt' + v(ts(t'))$. □

Examples of Euclidean self-dual R_3-codes

1. Let p be a prime $\equiv -11 \pmod{12}$. Consider the Pless symmetry code S_{2p+2}, of length $2p+2$. It is held invariant by the natural swap map by [17], p. 511 (in particular, if $p=11$ we get the ternary Golay code). We denote by IS_{p+1} the inverse Gray image of length $p+1$. In the next section this is constructed as a quadratic residue code over R_3.
2. Let W be a n by n weighing matrix of weight k (i.e. $WW^T = kI$) with $k \equiv \epsilon \pmod 3$ with $\epsilon = \pm 1$. Assume that $W^T = \epsilon W$. Then, the R_3-span of $W - \epsilon vI$ is self-dual of length n.

Are there R_3-codes which are both Euclidean self-dual and Hermitian self-dual? The answer is simple.

Proposition 3.7. *An R_3-code C is self-dual for both the Hermitian and Euclidean scalar product if and only if it is self-conjugate. In particular it is the R_3-span of a ternary matrix the $\mathbf{F}_3-$span of which is self-dual.*

Proof. The first assertion is immediate from the definitions. The second assertion follows by combining Theorems 3.1 and 3.2 to get $C^+ = C^-$ a ternary self-dual code. □

This is the case in particular of Example 2 as the next section shows.

4. Pless Symmetry Codes

Pless defined symmetry codes over $\mathbf{F}_3$. These codes have length $2(p+1)$ where p is a prime congruent to 5 modulo 6. These can be expressed as

Gray images of extended quadratic residue codes defined over R_3 when p is congruent to 11 modulo 12.

Let p be a prime congruent to 5 modulo 6. Let $\epsilon = (-1/p)$.

If $p \equiv 11 \pmod{12}$ then $\epsilon = -1$ and let $\delta = v \in R_3$. Note that $\delta^2 = \epsilon p$ in R_3. Denote the action of natural involution of R_3 by a bar, so that $\overline{x + yv} = x - yv$ for $x,\, y \in \mathbf{F}_3$. We shall construct quadratic residue codes of length $p+1$ over R_3.

Let S_p be the matrix

$$S_p = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ \epsilon & & & & \\ \epsilon & & S'_p & & \\ \vdots & & & & \\ \epsilon & & & & \end{pmatrix}$$

where S'_p is the circulant matrix whose (i,j)-entry is $((j-i)/p)$. Then $S_p^{\mathrm{t}} = \epsilon S_p$ and $S_p^2 = \epsilon p I$. Let $\mathcal{Q}$ be the submodule of R_3^{p+1} spanned by the rows of $\delta I + S_p$. We show that $\mathcal{Q}$ is self-dual in an appropriate sense. If $\epsilon = -1$ then $R = R_3$ and $\delta I + S_p = vI + S_p$. Hence

$$(\delta I + S_p)(\delta I + S_p)^{\mathrm{t}} = (vI + S_p)(vI - S_p) = I - S_p^2 = 0.$$

As it will become apparent that $|\mathcal{Q}| = 3^{p+1}$, then $\mathcal{Q}$ is self-orthogonal.

Recall the Gray code map $\phi : R^{p+1} \to \mathbf{F}_3^{2(p+1)}$ as above for R_3. This map preserves orthogonality and so $\phi(\mathcal{Q})$ is self orthogonal. In each case $\phi(\mathcal{Q})$ contains the code with generator matrix $(S_p\ I)$, and so $|\mathcal{Q}| \geq 3^{p+1}$. Consequently $\phi(\mathcal{Q})$ has this generator matrix and is the Pless symmetry code.

5. The MacWilliams Relations

The complete weight enumerator for a code over R_3 is given by:

$$W_C(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) = \sum A_{(\alpha_0,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8)} \prod a_i^{\alpha_i}$$

where there are $A_{(\alpha_0,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8)}$ vectors in C with a_i appearing α_i times in the vector.

5.1. The Euclidean Inner Product. Notice there is no generating character for the ring, hence the MacWilliams relations in [24] do not apply. Instead we use a slightly modified approach using a symmetric character table for the additive group of the ring as is done in [7]. Index the matrix by the elements of R_3 in the following order:

$$0, 1, 2, v, 1+v, 2+v, 2v, 1+2v, 2+2v$$

Then the MacWilliams relations for the complete weight enumerator are given by the following matrix where $\omega = e^{\frac{2\pi i}{3}}$.

$$M_C = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{pmatrix}$$

Specializing the variables to the symmetric (i.e. grouping the variables with their symmetric as one variable) and indexing the matrix by

$$0, \pm 1, \pm v, \pm(1+v), \pm(1+2v),$$

we obtain the MacWilliams relations for the symmetrized weight enumerator:

$$M_S = \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & -1 & -1 & -1 \\ 1 & -1 & 2 & -1 & -1 \\ 1 & -1 & -1 & -1 & 2 \\ 1 & -1 & -1 & 2 & -1 \end{pmatrix}$$

Further specialization gets the MacWilliams relations for the Hamming weight enumerator:

$$M_H = \frac{1}{3}\begin{pmatrix} 1 & 8 \\ 1 & -1 \end{pmatrix}$$

The following matrix gives the weight enumerator for the length weight enumerator and is indexed by $0, \pm 1, \pm v, \pm 1 \pm v$.

$$M_L = \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 & 4 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 2 & -2 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

The symmetrized length weight enumerator is given by the following matrix, where ± 1 and $\pm v$ are grouped together:

$$M_{SL} = \frac{1}{3}\begin{pmatrix} 1 & 4 & 4 \\ 1 & 1 & -2 \\ 1 & -2 & 1 \end{pmatrix}$$

5.2. The Hermitian Inner Product. The complete weight enumerator for the Hermitian inner product can be determined from the MacWilliams relations for the standard inner product and are given by the matrix:

$$M'_C = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \end{pmatrix}$$

We specialize variables to get the MacWilliams relations for the symmetrized weight enumerator.

$$M'_S = \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & -1 & -1 & -1 \\ 1 & -1 & 2 & -1 & -1 \\ 1 & -1 & -1 & 2 & -1 \\ 1 & -1 & -1 & -1 & 2 \end{pmatrix}$$

Then we have $M'_H = M_H$, $M'_L = M_L$, and $M'_{SL} = M_{SL}$.

Example: Let C be the code $\{0, 1+2v, 2+v\}$. Its weight enumerator is $W = a_0 + a_5 + a_7$. Applying M_C to W gives $a_0 + a_4 + a_8$ corresponding to its orthogonal in the ordinary inner product, i.e. the code $\{0, 1+v, 1+2v\}$. Applying M'_C to W gives $a_0 + a_5 + a_7$ corresponding to its orthogonal in the Hermitian inner product, i.e. the code C.

5.3. Gleason Relations. Define the matrices P_3 and P_4 as diagonal matrices with entries respectively $1, \omega, \omega^2$ and $1, \omega, \omega^2, 1$. Define the matrix groups $G_3 :=< M_{SL}, P_3, iI_3 >$, and $G_4 :=< M_L, P_4 >$. The following lemma is easily dealt with by Magma.

Lemma 5.1. *The groups G_3 and G_4 are of respective orders $48, 24$ and have Molien series (corresponding to Hironaka decomposition of their ring of invariants) respectively*

$$\frac{1+2t^8+t^{12}}{(1-t^4)^2(1-t^{12})} = 1 + 2\,t^4 + 5\,t^8 + 10\,t^{12} + 15\,t^{16} + 22\,t^{20} + O\left(t^{21}\right),$$

and

$$\frac{1}{(1-t)(1-t^2)(1-t^3)(1-t^4)} = 1 + t + 2t^2 + 3\,t^3 + 5\,t^4 + 6\,t^5 + 9\,t^6 + 11\,t^7 + 15\,t^8 + O\left(t^9\right).$$

The group G_4 is abstractly isomorphic to the group number 2 *with name* $G(1,1,4)$ *in the list of* [23].

We are now in a position to state the following analogues of Gleason theorem. The Gleason polynomials are easy to obtain in Magma and too unwieldy to be recorded.

Theorem 5.2. *The symmetrized length weight enumerator of a Euclidean code is invariant under G_3. It belongs to the ring $S \oplus h_8 S \oplus h'_8 S \oplus h_{12} S$ with*

$$S = \mathbf{C}[g_4, g'_4, g_{12}]$$

with g_4, g'_4, g_{12} are primary invariants of degree $4, 4, 12$ *respectively and h_8, h'_8, h_{12} are secondary invariants of degree* $8, 8$, *and* 12 *respectively.*

Proof. The slwe is invariant under P_3 by self-duality of the Gray image. Invariance under iI_3 follows by the fact that the length must be a multiple of 4 by Theorem 3.2. □

Theorem 5.3. *The length weight enumerator of a Hermitian code is invariant under G_4. It belongs to the ring*

$$\mathbf{C}[f_1, f_2, f_3, f_4]$$

where f_i is an homogeneous polynomial of degree i in a, b, c, d.

Proof. The lwe is invariant under P_4 by the integrality of the corresponding lattice. □

6. Some odd 2-modular lattices

In this section we give some codes over R_3 for the lengths $n = 4, 6, 8, 9, 10, 11, 12, 13, 14$ and 15, which are Hermitian self-dual and have minimum length weight 9. All these codes give by construction A_K examples of odd 2-modular lattices of dimension $2n$ and minimum norm 3 by Theorem 2.1.

The following upper bound was given in [22]:

Theorem 6.1. *If L is a strongly* 2*-modular lattice with norm μ in dimension n then:*

$$\mu \leq 2[\frac{n}{16}] + 2.$$

Thus by theorem 2.1 a direct construction A_K can only give extremal odd lattices of norm 3 for lengths strictly less than 8.

The code of length 8 leads to the unique 2-modular lattice of dimension 16 and norm 3, the so called 'odd Barnes-Wall' lattice of [22], the code of length 9 leads to a new optimal 2-modular lattice of dimension 18 since for this length there is no extremal lattice (i.e. norm 4) [22]. The other codes lead to norm 3 odd 2-modular lattices of dimension $2n$. All the lattices constructed for $n \geq 9$ are new.

The codes of lengths lower than 7 are easy to find since we only need a minimum length weight of 6 to obtain extremal codes. We now describe how we found the codes of length 8 or more: by Theorem 3.1 we know that the self-dual Hermitian codes of length n are the codes H which are written:

$$H = (1+v)C \oplus (1-v)C^{\perp},$$

with C a ternary code of length n. In order to find such codes H with length weight 9 or more, we first notice that if $C \cap C^{\perp}$ is non null then H contains words of length weight equal to 3, and also that if C or $C^{\perp}$ contain non null words of Hamming weight 2 or less then H contains words of length weight 3 or 6.

We therefore searched for ternary codes C with the following necessary conditions:

$$W_H(C) \geq 3,\ W_H(C^{\perp}) \geq 3,\ C \cap C^{\perp} = 0.$$

The codes were found, starting from binary codes with good minimum weight read-off (mod 3) and when the code H did not have good minimum length weight, we exchanged some 1 by -1 in the ternary code C. The minimum length weight was checked by exhaustive search, using the Magma system.

- $n = 4$ $\quad C_4 = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$

- $n = 6$ $\quad C_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & -1 \end{pmatrix}$

- $n = 8$ $\quad C_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & -1 & 1 & -1 \end{pmatrix}$

- $n = 9$ $\quad C_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

- $n = 10$ $$C_{10} = \begin{pmatrix} 1&0&0&0&0&1&1&1&0&0\\ 0&1&0&0&0&0&1&1&1&0\\ 0&0&1&0&0&0&0&1&1&1\\ 0&0&0&1&0&1&0&0&1&1\\ 0&0&0&0&1&1&1&0&0&1 \end{pmatrix}$$

- $n = 11$ $$C_{11} = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&0&0\\ 0&1&0&0&0&0&1&1&1&1&0\\ 0&0&1&0&0&0&0&1&1&1&1\\ 0&0&0&1&0&1&0&0&1&1&1\\ 0&0&0&0&1&1&1&0&0&1&1 \end{pmatrix}$$

- $n = 12$ $$C_{12} = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&0&0&0\\ 0&1&0&0&0&0&1&1&1&1&0&0\\ 0&0&1&0&0&0&0&1&1&1&1&0\\ 0&0&0&1&0&1&0&0&1&1&1&1\\ 0&0&0&0&1&1&1&0&0&1&1&1 \end{pmatrix}$$

- $n = 13$ $$C_{13} = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&1&0&0&0\\ 0&1&0&0&0&0&1&1&1&1&1&0&0\\ 0&0&1&0&0&0&0&1&1&1&1&1&0\\ 0&0&0&1&0&1&0&0&1&1&1&1&1\\ 0&0&0&0&1&1&1&0&0&1&1&1&1 \end{pmatrix}$$

- $n = 14$ $$C_{14} = \begin{pmatrix} 1&0&0&0&0&0&-1&1&1&1&1&0&0&0\\ 0&1&0&0&0&0&0&1&1&1&1&1&0&0\\ 0&0&1&0&0&0&0&0&1&1&1&1&1&0\\ 0&0&0&1&0&0&0&0&0&1&1&1&1&1\\ 0&0&0&0&1&0&1&0&0&0&1&1&1&1\\ 0&0&0&0&0&1&1&1&0&0&0&1&1&1 \end{pmatrix}$$

- $n = 15$ $$C_{15} = \begin{pmatrix} 1&0&0&0&0&0&0&1&1&1&1&1&0&0&0\\ 0&1&0&0&0&0&0&0&1&1&1&1&1&0&0\\ 0&0&1&0&0&0&0&0&0&1&1&1&1&1&0\\ 0&0&0&1&0&0&0&0&0&0&1&1&1&1&1\\ 0&0&0&0&1&0&0&1&0&0&0&1&1&1&1\\ 0&0&0&0&0&1&0&1&1&0&0&0&1&1&1\\ 0&0&0&0&0&0&1&1&1&1&0&0&0&1&1 \end{pmatrix}$$

References

[1] C. BACHOC, *Application of coding Theory to the construction of modular lattices.* J. Combin. Theory Ser. A **78** (1997),92–119.

[2] A. BONNECAZE, P. SOLÉ, A. R. CALDERBANK, *Quaternary quadratic residue codes and unimodular lattices.* IEEE Trans. Inform. Theory **41** (1995), 366–377.

[3] A. BONNECAZE, P. SOLÉ, C. BACHOC, B. MOURRAIN, *Type II codes over* $\mathbf{Z}_4$. IEEE Trans. Inform. Theory **43** (1997), 969–976.
[4] S. BUYUKLIEVA, *On the Binary Self-Dual Codes with an Automorphism of Order 2.* Designs, Codes and Cryptography **12** (1) (1997), 39–48.
[5] J. H. CONWAY, N. J. A. SLOANE, *Sphere Packings, Lattices and Groups.* Springer, Heidelberg, 1993.
[6] J. H. CONWAY, N. J. A. SLOANE, *Self-dual codes over the integers modulo 4.* J. Combin. Theory Ser. A **62** (1993), 30–45.
[7] S. T. DOUGHERTY, *Some thought about codes over groups.* preprint.
[8] S. T. DOUGHERTY, *Shadow codes and weight enumerators.* IEEE Trans. Inform. Theory, vol. IT-41 (1995), 762–768.
[9] S. T. DOUGHERTY, P. GABORIT, M. HARADA, A. MUNEMASA, P. SOLÉ, *Self-dual Type IV codes over rings.* IEEE Trans. Inform. Theory **45** (1999), 2162–2168.
[10] S. T. DOUGHERTY, P. GABORIT, M. HARADA, P. SOLÉ, *Type II codes over* $\mathbf{F}_2 + u\mathbf{F}_2$. IEEE Trans. Inform. Theory **45** (1999), 32–45.
[11] J. FIELDS, P. GABORIT, J. LEON, V. PLESS, *All Self-Dual* Z_4 *Codes of Length 15 or Less Are Known.* IEEE Trans. Inform. Theory **44** (1998), 311–322.
[12] P. GABORIT, *Mass formula for self-dual codes over* Z_4 *and* $F_q + uF_q$ *rings.* IEEE Trans. Inform. Theory **42** (1996), 1222–1228.
[13] M. HARADA, T. A. GULLIVER, H. KANETA, *Classification of extremal double circulant self-dual codes of length up to 62.* Discrete Math. **188** (1998), 127–136.
[14] A. R. HAMMONS JR., P. V. KUMAR, A. R. CALDERBANK, N. J. A. SLOANE, P. SOLÉ, *A linear construction for certain Kerdock and Preparata codes.* Bull. AMS **29** (1993), 218–222.
[15] G. HUGHES, *Codes and arrays from cocycles.* Ph.D. thesis, Royal Melbourne Institute of Technology, 2000.
[16] G. HUGHES, *Constacyclic codes, cocycles and a* $u+v|u-v$ *construction.* IEEE Trans. Inform. Theory **46** (2000), 674–680.
[17] F. J. MACWILLIAMS, N. J. A. SLOANE, *The theory of error correcting codes.* North-Holland, 1977.
[18] J. MARTINET, *Les réseaux parfaits des espaces euclidiens.* Masson, Paris, 1996.
[19] V. PLESS, *The Number of Isotropic Subspaces in a Finite Geometry.* Atti. Accad. Naz. Lincei Rend. **39** (1965), 418–421.
[20] V. PLESS, P. SOLÉ, Z. QIAN, *Cyclic self-dual* $\mathbf{Z}_4$*-codes.* Finite Fields Their Appl. **3** (1997), 48–69.
[21] H-G. QUEBBEMANN, *Modular Lattices in Euclidean Spaces.* J. Number Theory **54** (1995), 190–202.
[22] E. RAINS, N. J. A. SLOANE, *The shadow theory of modular and unimodular lattices.* J. Number Theory **73** (1999), 359–389.
[23] G. C. SHEPHARD, J. A. TODD, *Finite unitary reflection groups.* Can. J. Math. **6** (1954), 274–304.
[24] J. WOOD, *Duality for Modules over Finite Rings and Applications to Coding Theory.* Amer. J. Math **121** (1999), 555–575.

Robin CHAPMAN
Department of Mathematics
University of Exeter
EX4 4QE, UK
E-mail : `rjc@maths.ex.ac.uk`

Steven T. DOUGHERTY
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA
E-mail : `doughertys1@tiger.uofs.edu`

Philippe GABORIT
LACO, Université de Limoges
123, Av. A. Thomas
87000 Limoges, France
E-mail : `gaborit@unilim.fr`

Patrick SOLÉ
CNRS, I3S, ESSI, BP 145
Route des Colles
06903 Sophia Antipolis, France
E-mail : `ps@essi.fr`