The Invariants of the Clifford Groups

Gabriele Nebe*

Abteilung Reine Mathematik der Universität Ulm
89069 Ulm, Germany
nebe@mathematik.uni-ulm.de

and

E. M. Rains and N. J. A. Sloane

Information Sciences Research, AT&T Shannon Labs
180 Park Avenue, Florham Park, NJ 07932-0971, U.S.A.
rains@research.att.com, njas@research.att.com

December 6, 1999; revised September 8, 2000

ABSTRACT

The automorphism group of the Barnes-Wall lattice L_m in dimension 2^m ($m \neq 3$) is a subgroup of index 2 in a certain "Clifford group" $\mathcal{C}_m$ of structure $2_+^{1+2m}.O^+(2m,2)$. This group and its complex analogue $\mathcal{X}_m$ of structure $(2_+^{1+2m} \curlyvee Z_8).Sp(2m,2)$ have arisen in recent years in connection with the construction of orthogonal spreads, Kerdock sets, packings in Grassmannian spaces, quantum codes, Siegel modular forms and spherical designs. In this paper we give a simpler proof of Runge's 1996 result that the space of invariants for $\mathcal{C}_m$ of degree $2k$ is spanned by the complete weight enumerators of the codes $C \otimes \mathbb{F}_{2^m}$, where C ranges over all binary self-dual codes of length $2k$; these are a basis if $m \geq k-1$. We also give new constructions for L_m and $\mathcal{C}_m$: let M be the $\mathbb{Z}[\sqrt{2}]$-lattice with Gram matrix $\begin{bmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}$. Then L_m is the rational part of $M^{\otimes m}$, and $\mathcal{C}_m = \mathrm{Aut}(M^{\otimes m})$. Also, if C is a binary self-dual code not generated by vectors of weight 2, then $\mathcal{C}_m$ is precisely the automorphism group of the complete weight enumerator of $C \otimes \mathbb{F}_{2^m}$. There are analogues of all these results for the complex group $\mathcal{X}_m$, with "doubly-even self-dual code" instead of "self-dual code".

KEYWORDS: Clifford groups, Barnes-Wall lattices, spherical designs, invariants, self-dual codes

*Most of this work was carried out during G. Nebe's visit to AT&T Labs in the Summer of 1999

1 Introduction

In 1959 Barnes and Wall [2] constructed a family of lattices in dimensions 2^m, $m = 0, 1, 2, \ldots$. They distinguished two geometrically similar lattices $L_m \subseteq L'_m$ in $\mathbb{R}^{2^m}$. The automorphism group† $\mathcal{G}_m = \mathrm{Aut}(L_m)$ was investigated in a series of papers by Bolt, Room and Wall [8], [9], [10], [50]. $\mathcal{G}_m$ is a subgroup of index 2 in a certain group $\mathcal{C}_m$ of structure $2_+^{1+2m}.O^+(2m, 2)$. We follow Bolt et al. in calling $\mathcal{C}_m$ a Clifford group. This group and its complex analogue $\mathcal{X}_m$ are the subject of the present paper.

These groups have appeared in several different contexts in recent years. In 1972 Broué and Enguehard [12] rediscovered the Barnes-Wall lattices and also determined their automorphism groups. In 1995, Calderbank, Cameron, Kantor and Seidel [13] used the Clifford groups to construct orthogonal spreads and Kerdock sets, and asked "is it possible to say something about [their] Molien series, such as the minimal degree of an invariant?".

Around the same time, Runge [39], [40], [41], [42] (see also [20], [36]) investigated these groups in connection with Siegel modular forms. Among other things, he established the remarkable result that the space of homogeneous invariants for $\mathcal{C}_m$ of degree $2k$ is spanned by the complete weight enumerators of the codes $C \otimes_{\mathbb{F}_2} \mathbb{F}_{2^m}$, where C ranges over all binary self-dual (or type I) codes of length $2k$, and the space of homogeneous invariants for $\mathcal{X}_m$ of degree $8k$ is spanned by the complete weight enumerators of the codes $C \otimes_{\mathbb{F}_2} \mathbb{F}_{2^m}$, where C ranges over all binary doubly-even self-dual (or type II) codes of length $8k$. One of our goals is to give a simpler proof of these two assertions, not involving Siegel modular forms (see Theorems 4.9 and 6.2).

Around 1996, the Clifford groups also appeared in the study of fault-tolerant quantum computation and the construction of quantum error-correcting codes [4], [15], [16], [29], and in the construction of optimal packings in Grassmannian spaces [14], [17], [44]. The story of the astonishing coincidence (involving the group $\mathcal{C}_3$) that led to [14], [15] and [16] is told in [16]. (Other recent references that mention these groups are [23], [30], [51].)

Independently, and slightly later, Sidelnikov [45], [46], [47], [48] (see also [28]) came across the group $\mathcal{C}_m$ when studying spherical codes and designs. In particular, he showed that for $m \geq 3$ the lowest degree harmonic invariant of $\mathcal{C}_m$ has degree 8, and hence that the orbit under $\mathcal{C}_m$ of any point on a sphere in $\mathbb{R}^{2^m}$ is a spherical 7-design. (Venkov [49] had earlier shown that for $m \geq 3$ the minimal vectors of the Barnes-Wall lattices form 7-designs.)

In fact it is an immediate consequence of Runge's results that for $m \geq 3$ $\mathcal{C}_m$ has a unique harmonic invariant of degree 8 and no such invariant of degree 10 (see Corollary 4.13). The space of homogeneous invariants of degree 8 is spanned by the fourth power of the quadratic form and the complete weight enumerator of the code $H_8 \otimes_{\mathbb{F}_2} \mathbb{F}_{2^m}$, where H_8 is the $[8, 4, 4]$ Hamming code. An explicit formula for this complete weight enumerator is given in Theorem 4.14.

Our proof of the real version of Runge's theorem is given in Section 4 (Theorem 4.9), following two preliminary sections dealing with the group $\mathcal{C}_m$ and with generalized weight enumerators.

In Section 5 we study the connection between the group $\mathcal{C}_m$ and the Barnes-Wall lattices. We define the balanced Barnes-Wall lattice M_m to be the $\mathbb{Z}[\sqrt{2}]$-lattice $\sqrt{2}L'_m + L_m$. Then $M_m = M_1^{\otimes m}$ (Lemma 5.2), which leads to a simple construction: the Barnes-Wall lattice is just the rational part of $M_1^{\otimes m}$. Furthermore $\mathcal{C}_m = \mathrm{Aut}(M_m)$ (Proposition 5.3).

†More precisely, $\mathcal{G}_m = \mathrm{Aut}(L_m) \cap \mathrm{Aut}(L'_m)$ for all m, and $\mathcal{G}_m = \mathrm{Aut}(L_m)$ unless $m = 3$.

Also, if C is any binary self-dual code that is not generated by vectors of weight 2, $\mathcal{C}_m = \mathrm{Aut}(\mathrm{cwe}(C \otimes \mathbb{F}_{2^m}))$ (Corollary 5.7). The proof of this makes use of the fact that $\mathcal{C}_m$ is a maximal finite subgroup of $GL(2^m, \mathbb{R})$ (Theorem 5.6). Although there are partial results about the maximality of $\mathcal{C}_m$ in Kleidman and Liebeck [30], this result appears to be new. The proof does not use the classification of finite simple groups.

The analogous results for the complex Clifford group $\mathcal{X}_m$ are given in Section 6. Theorem 6.2 is Runge's theorem. Extending scalars, let $\mathbb{M}_m$ be the hermitian $\mathbb{Z}[\zeta_8]$-lattice $\mathbb{Z}[\zeta_8] \otimes_{\mathbb{Z}[\sqrt{2}]} M_m$. Then $\mathcal{X}_m$ is the subgroup of $U(2^m, \mathbb{Q}[\zeta_8])$ preserving $\mathbb{M}_m$ (Proposition 6.4). Theorem 6.5 shows that, apart from the center, $\mathcal{X}_m$ is a maximal finite subgroup of $U(2^m, \mathbb{C})$, and Corollary 6.6 is the analogue of Corollary 5.7.

Bolt et al. [8], [9], [10], [50] and Sidelnikov [45], [46], [47] also consider the group $\mathcal{C}_m^{(p)}$ obtained by replacing 2 in the definition of $\mathcal{C}_m$ by an odd prime p. In the final section we give some analogous results for this group.

In recent years many other kinds of self-dual codes have been studied by a number of authors. Nine such families were named and surveyed in [38]. In a sequel [35] to the present paper we will give a general definition of the "type" of a self-dual code which includes all these families as well as other self-dual codes over rings and modules. For each "type" we investigate the structure of the associated "Clifford-Weil group" (analogous to $\mathcal{C}_m$ and $\mathcal{X}_m$ for types I and II) and its ring of invariants.

The results in this paper and in Part II can be regarded as providing a general setting for Gleason's theorems [24], [32], [38] about the weight enumerator of a binary self-dual code (cf. the case $m = 1$ of Theorem 4.9), a doubly-even binary self-dual code (cf. the case $m = 1$ of Theorem 6.2) and a self-dual code over $\mathbb{F}_p$ (cf. the case $m = 1$ of Theorem 7.1). They are also a kind of discrete analogue of a long series of theorems going back to Eichler (see for example [7], [39], [40], [42]), stating that under certain conditions theta series of quadratic forms are bases for spaces of modular forms: here complete weight enumerators of generalized self-dual codes are bases for spaces of invariants of "Clifford-Weil groups".

2 The real Clifford group $\mathcal{C}_m$

This initial section defines the real Clifford group $\mathcal{C}_m$. The extraspecial 2-group $E(m) \cong 2_+^{1+2m}$ is a subgroup of the orthogonal group $O(2^m, \mathbb{R})$. If $m = 1$ then

$$E(1) := \left\langle \sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \cong D_8$$

is the automorphism group of the 2-dimensional standard lattice. In general $E(m)$ is the m-fold tensor power of $E(1)$:

$$E(m) := E(1)^{\otimes m} = E(1) \otimes \cdots \otimes E(1) \, ,$$

and is generated by the tensor products of σ_1 and σ_2 with 2×2 identity matrices I_2.

Definition 2.1 *The* real Clifford group $\mathcal{C}_m$ *is the normalizer in* $O(2^m, \mathbb{R})$ *of the extraspecial 2-group* $E(m)$.

The natural representation of $E(m)$ is absolutely irreducible. So the centralizer of $E(m)$ in the full orthogonal group is equal to $\{\pm I_{2^m}\}$, which is the center of $E(m)$. Then $\mathcal{C}_m/E(m)$ embeds into the outer automorphism group of $E(m)$. The quotient group $E(m)/Z(E(m))$ is isomorphic to a $2m$-dimensional vector space over $\mathbb{F}_2$. Since every outer automorphism has to respect the $\{+1,-1\}$-valued quadratic form

$$E(m)/Z(E(m)) \cong \mathbb{F}_2^{2m} \to Z(E(m)) \cong \mathbb{F}_2, \quad x \mapsto x^2,$$

it follows easily that the outer automorphism group of $E(m)$ is isomorphic to $O^+(2m,2)$, the full orthogonal group of a quadratic form of Witt defect 0 over $\mathbb{F}_2$ (see e.g. [51]).

Since the group $2_+^{1+2m}.O^+(2m,2)$ is a subgroup of $O(2^m,\mathbb{R})$ (cf. [10] or the explicit construction below), we find that $\mathcal{C}_m \cong 2_+^{1+2m}.O^+(2m,2)$. The order of $\mathcal{C}_m$ is

$$2^{m^2+m+2}(2^m-1)\prod_{j=1}^{m-1}(4^j-1).$$

To perform explicit calculations we need a convenient set of generators for $\mathcal{C}_m$.

Theorem 2.2 *$\mathcal{C}_m$ is generated by the following elements of $O(2^m,\mathbb{R})$:*

(1) $\mathrm{diag}((-1)^{q(v)+a})$, *where q ranges over all $\{0,1\}$-valued quadratic forms on $\mathbb{F}_2^m$ and $a \in \{0,1\}$,*

(2) $AGL(m,2)$, *acting on $\mathbb{R}^{2^m} = \otimes^m(\mathbb{R}^2) = \mathbb{R}[\mathbb{F}_2^m]$ by permuting the basis vectors in $\mathbb{F}_2^m$, and*

(3) the single matrix $h \otimes I_2 \otimes \cdots \otimes I_2$ where $h := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Proof. Let H be the group generated by the elements in (1) and (2). First, H contains the extraspecial group $E(m)$, since $\sigma_1 \otimes I_{2^{m-1}}$ and $\sigma_2 \otimes I_{2^{m-1}}$ are in H and their images under $GL(m,2)$ generate $E(m)$.

To see that $H/E(m)$ is a maximal parabolic subgroup of $O^+(2m,2)$, note that by [13] the elements $a \in GL(m,2)$ act on $E(m)/Z(E(m)) \cong \mathbb{F}_2^{2m}$ as $\begin{pmatrix} a & 0 \\ 0 & a^{-tr} \end{pmatrix}$, and the elements $\mathrm{diag}((-1)^{q(v)})$ act as $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, where b is the skew-symmetric matrix corresponding to the bilinear form $b_q(x,y) := q(x+y) - q(x) - q(y)$.

Since $h \otimes I_{2^{m-1}} \notin GL(2^m,\mathbb{Q})$ is not in H, the group generated by H and this element is $\mathcal{C}_m$. $\square$

Corollary 2.3 *$\mathcal{C}_m$ is generated by*

$$\sigma_1 \otimes I_2 \otimes \cdots \otimes I_2,\ \sigma_2 \otimes I_2 \otimes \cdots \otimes I_2,\ h \otimes I_2 \otimes \cdots \otimes I_2,\ GL(m,2),\ \mathrm{diag}((-1)^{\Phi(v)}),$$

where Φ is the particular quadratic form $(\epsilon_1,\ldots,\epsilon_m) \mapsto \epsilon_1\epsilon_2 \in \{0,1\}$ on $\mathbb{F}_2^m$.

3 Full weight enumerators and complete weight enumerators

We now introduce certain weight enumerators and show that they are invariant under the real Clifford group. Let $C \leq \mathbb{F}_2^N$ be a linear code[‡] of length N over the field $\mathbb{F}_2$. For $m \in \mathbb{N}$ let $C(m) := C \otimes_{\mathbb{F}_2} \mathbb{F}_{2^m}$ be the extension of C to a code over the field with 2^m elements.

Let V be the group algebra $V := \mathbb{R}[\mathbb{F}_{2^m}] = \oplus_{f\in\mathbb{F}_{2^m}} \mathbb{R}x_f$. Regarding $\mathbb{F}_{2^m} \cong \mathbb{F}_2^m$ as an m-dimensional vector space over $\mathbb{F}_2$, we have a tensor decomposition

$$V \cong \otimes^m(\mathbb{R}^2).$$

In the same manner the group algebra $\mathbb{R}[C(m)] = \oplus_{c\in C(m)}\mathbb{R}e_c$ embeds naturally into the group algebra

$$\mathbb{R}[\mathbb{F}_{2^m}^N] \cong \otimes^N V = \otimes^N(\otimes^m(\mathbb{R}^2)) \cong \otimes^m(\otimes^N(\mathbb{R}^2)).$$

Definition 3.1 *The* full weight enumerator *of $C(m)$ is the element*

$$\mathrm{fwe}(C(m)) := \sum_{c\in C(m)} e_c \in \mathbb{R}[C(m)] \subset \otimes^N V.$$

(This was called a generalized weight polynomial in [24] and an exact enumerator in [32, Chapter 5].)

Fix a basis $(a_1, \dots , a_m)$ of $\mathbb{F}_2^m$ over $\mathbb{F}_2$. Then a codeword $c \in C(m)$ is just an m-tuple of codewords in C. The element $c = \sum_{i=1}^m a_i c_i$ corresponds to the m-tuple $(c_1, \dots , c_m) \in C^m$, which can also be regarded as an $m \times N$-matrix M of which the rows are the elements $c_i \in C$.

Lemma 3.2 *Let*

$$\mathrm{fwe}_m(C) := \sum_{c_1,\dots,c_m\in C} e_{c_1} \otimes \dots \otimes e_{c_m} \;\in\; \otimes^m \mathbb{R}[C] \;\subset\; \otimes^m \otimes^N(\mathbb{R}^2).$$

Then the isomorphism $\otimes^m\mathbb{R}[C] \cong \mathbb{R}[C(m)]$ induced by identifying an m-tuple $(c'_1, \dots , c'_m) \in C^m$ with the codeword $c := \sum_{i=1}^m a_i c'_i \in C(m)$ maps $\mathrm{fwe}_m(C)$ onto $\mathrm{fwe}(C(m))$.

Proof. Let $c = \sum_{i=1}^m a_i c'_i = (c_1, \dots , c_N) \in C(m)$. If $c_i = \sum_{j=1}^m \epsilon_j^{(i)} a_j$ then $c'_i = (\epsilon_i^{(1)}, \dots , \epsilon_i^{(N)}) \in C$. The generator e_c of $\mathbb{R}[C(m)]$ is

$$x_{c_1} \otimes \dots \otimes x_{c_N} = (y_{\epsilon_1^{(1)}} \otimes \dots \otimes y_{\epsilon_m^{(1)}}) \otimes \dots \otimes (y_{\epsilon_1^{(N)}} \otimes \dots \otimes y_{\epsilon_m^{(N)}}) \in \otimes^N(\otimes^m(\mathbb{R}^2)),$$

where $\mathbb{R}^2 = \mathbb{R}[\mathbb{F}_2]$ has a basis y_0, y_1. Under the identification above this element is mapped onto

$$(y_{\epsilon_1^{(1)}} \otimes \dots \otimes y_{\epsilon_1^{(N)}}) \otimes \dots \otimes (y_{\epsilon_m^{(1)}} \otimes \dots \otimes y_{\epsilon_m^{(N)}}) \in \otimes^m(\otimes^N(\mathbb{R}^2)),$$

which is the element $e_{c'_1} \otimes \dots \otimes e_{c'_m} \in \otimes^m\mathbb{R}[C]$. □

[‡]A binary linear code C of length N is a subspace of $\mathbb{F}_2^N$. If $C \subseteq C^\perp$, C is self-orthogonal; if $C = C^\perp$, C is self-dual [32], [38].

Definition 3.3 *(Cf. [32, Chapter 5].) The* complete weight enumerator *of $C(m)$ is the following homogeneous polynomial of degree N in 2^m variables:*

$$\mathrm{cwe}(C(m)) := \sum_{c \in C(m)} \prod_{f \in \mathbb{F}_{2^m}} x_f^{a_f(c)} \in \mathbb{R}[x_f \mid f \in \mathbb{F}_{2^m}] ,$$

where $a_f(c)$ is the number of components of c that are equal to f.

Remark 3.4 The complete weight enumerator of $C(m)$ is the projection under π of the full weight enumerator of $C(m)$ to the symmetric power $\mathrm{Sym}_N(V)$, where $\pi : \otimes^N V \to \mathbb{R}[x_f \mid f \in \mathbb{F}_{2^m}]$ is the $\mathbb{R}$-linear mapping defined by $x_{f_1} \otimes \cdots \otimes x_{f_N} \mapsto x_{f_1} \cdots x_{f_N}$:

$$\mathrm{cwe}(C(m)) = \pi(\mathrm{fwe}(C(m))) \ \in \ \mathrm{Sym}_N(V).$$

Theorem 3.5 *Let C be a self-dual code over $\mathbb{F}_2$.*

(i) The Clifford group $\mathcal{C}_m$ preserves the full weight enumerator $\mathrm{fwe}(C(m))$.

(ii) The Clifford group $\mathcal{C}_m$ preserves the complete weight enumerator $\mathrm{cwe}(C(m))$.

Proof. Let N be the length of C, which is necessarily even. Then $\mathcal{C}_m$ acts on $\mathbb{R}[\mathbb{F}_{2^m}^N] = \otimes^N(\mathbb{R}^{2^m})$ diagonally. This action commutes with the projection $\pi : \otimes^N V \to \mathbb{R}[x_f \mid f \in \mathbb{F}_{2^m}]$. So statement (ii) follows immediately from (i) by Remark 3.4. To prove (i) it is enough to consider the generators of $\mathcal{C}_m$.

The generators $\sigma_1 \otimes I_2 \otimes \cdots \otimes I_2$, $\sigma_2 \otimes I_2 \otimes \cdots \otimes I_2$ and $h \otimes I_2 \otimes \cdots \otimes I_2$ of Corollary 2.3 are tensor products of the form $x \otimes I_{2^{m-1}}$. By Lemma 3.2 it is therefore enough to consider the case $m = 1$ for these generators. But then the matrix σ_1 acts as $\sigma_1 \otimes \cdots \otimes \sigma_1$ on $\otimes^N(\mathbb{R}^2)$, mapping a codeword $c = (c_1, \ldots , c_N) \in C$ to $c + \mathbf{1} = (c_1 + 1, \ldots , c_N + 1) \in C$, where $\mathbf{1}$ is the all-ones vector. Since C is self-dual, $\mathbf{1}$ is in C and therefore σ_1 only permutes the codewords and hence fixes $\mathrm{fwe}(C)$. Analogously, the matrix σ_2 changes signs of the components of the codewords in the full weight enumerator: if $c = (c_1, \ldots , c_N)$, then x_{c_i} is mapped to $(-1)^{c_i} x_{c_i}$. Since the codewords in C have even weight, the tensor product $x_{c_1} \otimes \cdots \otimes x_{c_N}$ is fixed by $\sigma_2 \otimes \cdots \otimes \sigma_2$. That h preserves the full weight enumerator follows from the MacWilliams identity [32, Chapter 5, Theorem 14].

The generator $d := \mathrm{diag}((-1)^{\Phi(v)}) = \mathrm{diag}(1, 1, 1, -1) \otimes I_{2^{m-2}}$ only occurs for $m \geq 2$. By Lemma 3.2 it suffices to consider the case $m = 2$. Again by Lemma 3.2, we regard d as acting on pairs (c, c') of codewords in C. Then d fixes or negates $(x_{c_1} \otimes \cdots \otimes x_{c_N}) \otimes (x_{c'_1} \otimes \cdots \otimes x_{c'_N})$, and negates it if and only if c and c' intersect in an odd number of 1's. This is impossible since C is self-dual, and so d also preserves $\mathrm{fwe}(C(m))$.

The remaining generators in $g \in GL(m, 2)$ permute the elements of $\mathbb{F}_{2^m}$. The codewords $c \in C(m)$ are precisely the elements of the form $c = \sum_{i=1}^m a_i c_i$ with $c_i \in C$ and $(a_1, \ldots , a_m)$ a fixed $\mathbb{F}_2$-basis for $\mathbb{F}_{2^m}$. Since g acts linearly on $\mathbb{F}_2^m$, mapping a_i onto $\sum_{j=1}^m g_{ij} a_j$, the word c is mapped to $\sum_{j=1}^m \sum_{i=1}^m g_{ij} a_j c_i$ which again is in $C(m)$. Hence these generators also fix $\mathrm{fwe}(C(m))$. ☐

4 The ring of invariants of $\mathcal{C}_m$

In this section we establish Runge's theorem that the complete weight enumerators of the codes $C(m)$ generate the space of invariants for $\mathcal{C}_m$.

Definition 4.1 *A polynomial p in 2^m variables is called a* Clifford invariant of genus m *if it is an invariant for the real Clifford group $\mathcal{C}_m$. Furthermore, p is called a* parabolic invariant *if it is invariant under the parabolic subgroup P generated by the elements of type* (1) *and* (2) *of Theorem 2.2, and a* diagonal invariant *if it is invariant under the group generated by the elements of type* (1).

The following is obvious:

Lemma 4.2 *A polynomial p is a diagonal invariant if and only if all of its monomials are diagonal invariants.*

Let M be an $m \times N$ matrix over $\mathbb{F}_2$. We can associate a monic monomial $\mu_M \in \mathbb{R}[x_f \mid f \in \mathbb{F}_{2^m}]$ with such a matrix by taking the product of the variables associated with its columns. Clearly all monic monomials are of this form, and two matrices correspond to the same monic monomial if and only if there is a column permutation taking one to the other.

Lemma 4.3 *A monic monomial μ_M is a diagonal invariant if and only if the rows of M are orthogonal.*

Proof. It suffices to consider quadratic forms q_{ij} with $q_{ij}(\epsilon_1, \ldots, \epsilon_m) = \epsilon_i \epsilon_j$ $(1 \leq i \leq j \leq m)$; we easily check that the action of $\mathrm{diag}((-1)^{q_{ij}})$ is to multiply μ_M by $(-1)^k$, where k is the inner product of rows i and j of M; the lemma follows. $\square$

For $g \in GL(m, 2) \leq AGL(m, 2)$ we have $g(\mu_M) = \mu_{g^{tr}M}$, and $b \in \mathbb{F}_2^m \leq AGL(m, 2)$ maps μ_M onto μ_{M+b}, where the matrix $M + b$ has entries $(M + b)_{ij} = M_{ij} + b_i$. This implies that μ_M is equivalent to $\mu_{M'}$ under the action of $AGL(m, 2)$ if and only if the binary codes $\langle M, \mathbf{1}\rangle$ and $\langle M', \mathbf{1}\rangle$ are equivalent. We can thus define a parabolic invariant $\mu_m(C)$ for any self-orthogonal code C containing $\mathbf{1}$ and of dimension at most $m + 1$ by

$$\mu_m(C) := \sum_{\substack{M \in \mathbb{F}_2^{m \times N} \\ \langle M, \mathbf{1}\rangle = C}} \mu_M.$$

We define $\mu_m(C)$ to be 0 if $\mathbf{1} \notin C$ or $\dim(C) > m + 1$. Since the invariants $\mu_m(C)$ are sums over orbits, we have:

Lemma 4.4 *A basis for the space of parabolic invariants of degree N is given by polynomials of the form $\mu_m(C)$ where C ranges over the equivalence classes of binary self-orthogonal codes of length N containing $\mathbf{1}$ and of dimension $\leq m + 1$.*

Lemma 4.5 *For any binary self-orthogonal code C containing $\mathbf{1}$,*

$$\mathrm{cwe}(C(m)) = \sum_{\mathbf{1} \in D \subseteq C} \mu_m(D).$$

Proof. From the definition,

$$\operatorname{cwe}(C(m)) = \sum_M \mu_M,$$

where M ranges over $m \times N$ matrices with all rows in C. Let M be such a matrix. Then M uniquely determines a subcode $D := \langle M, \mathbf{1} \rangle$ of C; we thus have

$$\operatorname{cwe}(C(m)) = \sum_{\mathbf{1} \in D \subseteq C} \sum_{\langle M, \mathbf{1} \rangle = D} \mu_M = \sum_{\mathbf{1} \in D \subseteq C} \mu_m(D)$$

as required. □

Theorem 4.6 *A basis for the space of parabolic invariants is given by the polynomials* $\operatorname{cwe}(C(m))$*, where C ranges over equivalence classes of self-orthogonal codes containing* $\mathbf{1}$ *and of dimension* $\leq m + 1$.

Proof. The equations in Lemma 4.5 form a triangular system which we can solve for the polynomials $\mu_m(C)$. In particular, $\mu_m(C)$ is a linear combination of the $\operatorname{cwe}(D(m))$ for subcodes $\mathbf{1} \in D \subseteq C$. □

Let X_P denote the linear transformation

$$x \quad \mapsto \quad \frac{1}{|P|} \sum_{g \in P} g \cdot x$$

where P is the parabolic subgroup of $\mathcal{C}_m$; that is, X_P is the operation of averaging over the parabolic subgroup.

Lemma 4.7 *For any binary self-orthogonal code C of even length N containing* $\mathbf{1}$ *and of dimension $N/2 - r$,*

$$X_P(h \otimes I_{2^{m-1}}) \operatorname{cwe}(C(m)) = \frac{1}{(2^m - 1)}[(2^{m-r} - 2^r) \operatorname{cwe}(C(m)) + 2^{-r} \sum_{\substack{C \subset C' \subseteq C'^{\perp} \\ [C':C]=2}} \operatorname{cwe}(C'(m))]. \tag{1}$$

The final sum is over all self-orthogonal codes C' containing C to index 2.

Proof. By the MacWilliams identity, we find that

$$(h \otimes I_{2^{m-1}}) \operatorname{cwe}(C(m)) = 2^{-r} \sum \mu_M,$$

where M ranges over $m \times N$ matrices such that the first row of M is in $C^{\perp}$ and the remaining rows are in C. For each code $\mathbf{1} \in D \subseteq C^{\perp}$, consider the partial sum over the terms with $\langle M, \mathbf{1} \rangle = D$. If $D \subseteq C$, the partial sum is just $\mu_m(D)$, so in particular is a parabolic invariant. The other possibility is that $[D : D \cap C] = 2$. For a matrix M with $\langle M, \mathbf{1} \rangle = D$, define a vector $v_M \in \mathbb{F}_2^m$ such that $(v_M)_i = 1$ if the ith row of M is in C, and $(v_M)_i = 0$ otherwise. In particular, the partial sum we are considering is

$$\sum_{\substack{\langle M,\mathbf{1}\rangle = D\\ v_M=(1,0,0,\dots)}} \mu_M.$$

If D is not self-orthogonal then this sum is annihilated by averaging over the diagonal subgroup. Similarly, if we apply an element of $AGL_m(2)$ to this sum, this simply has the effect of changing v_M. Thus, when $D \subseteq D^\perp$,

$$X_P \sum_{\substack{\langle M,\mathbf{1}\rangle = D\\ v_M=(1,0,0,\dots)}} \mu_M = \frac{1}{|\{v \in \mathbb{F}_2^m : v \neq 0\}|}\mu_m(D).$$

Hence

$$X_P(h \otimes I_{2^{m-1}})\,\mathrm{cwe}(C(m)) \;=\; 2^{-r} \sum_{\mathbf{1}\in D\subseteq C} \mu_m(D) + \frac{2^{-r}}{2^m-1} \sum_{\substack{\mathbf{1}\in D\subseteq C^\perp\\ [D:D\cap C]=2}} \mu_m(D),$$

where the sums are restricted to self-orthogonal codes D. Introducing a variable $C' = \langle D, C\rangle$ into the second sum (note that since $D \subseteq C^\perp$, $C' \subseteq C'^\perp$ precisely when $D \subseteq D^\perp$), this becomes

$$X_P(h \otimes I_{2^{m-1}})\,\mathrm{cwe}(C(m)) = 2^{-r} \sum_{\mathbf{1}\in D\subseteq C} \mu_m(D) + \frac{2^{-r}}{2^m-1} \sum_{\substack{C\subset C'\subseteq C'^\perp\\ [C':C]=2}} \sum_{\substack{D\subseteq C'\\ D\not\subseteq C}} \mu_m(D).$$

Any given C' will, of course, contain each subcode of C exactly once, so we can remove the condition $D \not\subseteq C$ as follows:

$$\begin{aligned}
&X_P(h \otimes I_{2^{m-1}})\,\mathrm{cwe}(C(m))\\
&\qquad= 2^{-r} \sum_{\mathbf{1}\in D\subset C} \mu_m(D) + \frac{2^{-r}}{2^m-1} \sum_{\substack{C\subset C'\subseteq C'^\perp\\ [C':C]=2}} \sum_{\mathbf{1}\in D\subseteq C'} \mu_m(D)\\
&\qquad\quad - (2^{2r}-1)\frac{2^{-r}}{2^m-1} \sum_{\mathbf{1}\in D\subseteq C} \mu_m(D)\\
&\qquad= \frac{1}{2^m-1}[(2^{m-r}-2^r)\,\mathrm{cwe}(C(m)) + 2^{-r} \sum_{\substack{C\subset C'\subseteq C'^\perp\\ [C':C]=2}} \mathrm{cwe}(C'(m))],
\end{aligned}$$

as required. □

Lemma 4.8 *Let V be a finite dimensional vector space, M a linear transformation on V, and P a partially ordered set. Suppose there exists a spanning set v_p of V indexed by $p \in P$ on which M acts triangularly; that is,*

$$Mv_p = \sum_{q\geq p} c_{pq} v_q,$$

for suitable coefficients c_{pq}. Suppose furthermore that $c_{pp} = 1$ if and only if p is maximal in P. Then the fixed subspace of M in V is spanned by the elements v_p for p maximal.

Proof. Since the matrix $C = (c_{pq})$ is triangular, there exists another triangular matrix D that conjugates C into Jordan canonical form. Setting

$$w_p = \sum_{q \geq p} d_{pq} v_q,$$

($d_{pp} \neq 0$), we find

$$M w_p = \sum_{q \geq p} c'_{pq} w_q,$$

with $c'_{pp} = c_{pp}$ and $(M - c_{pp} I)^n w_p = 0$ for sufficiently large n. In other words, each w_p is in the Jordan block of M with eigenvalue c_{pp}. But the vectors w_p span V; it follows that the Jordan blocks of M on V are spanned by the corresponding Jordan blocks of C. In particular, this is true for the block corresponding to 1. ☐

Theorem 4.9 *(Runge [42].) Fix integers k and $m \geq 1$. The space of homogeneous invariants of degree $2k$ for the Clifford group $\mathcal{C}_m$ of genus m is spanned by* $\mathrm{cwe}(C(m))$*, where C ranges over all binary self-dual codes of length $2k$; this is a basis if $m \geq k-1$.*

Proof. Let p be a parabolic invariant. If p is a Clifford invariant then

$$X_P(h \otimes I_{2^{m-1}}) p = p.$$

By Lemma 4.7, the operator $X_P(h \otimes I_{2^{m-1}})$ acts triangularly on the vectors $\mathrm{cwe}_m(C)$ (ordered by inclusion); since

$$\frac{2^{m-r} - 2^r}{2^m - 1} = 1 \Rightarrow r = 0,$$

the hypotheses of Lemma 4.8 are satisfied. The first claim then follows by Lemma 4.8 and Theorem 3.5. Linear independence for $m \geq k-1$ follows from Lemma 4.4. ☐

In fact a stronger result holds:

Theorem 4.10 *For any binary self-orthogonal code C of even length N containing* **1** *and of dimension $N/2 - r$,*

$$\frac{1}{|\mathcal{C}_m|} \sum_{g \in \mathcal{C}_m} g \cdot \mathrm{cwe}(C(m)) = \prod_{1 \leq i \leq r} (2^m + 2^i)^{-1} \sum_{C'} \mathrm{cwe}(C'(m)),$$

where the sum on the right is over all self-dual codes C' containing C.

To see that this is indeed stronger than Theorem 4.9, we observe that if p is an invariant for $\mathcal{C}_m$ then

$$\frac{1}{|\mathcal{C}_m|} \sum_{g \in \mathcal{C}_m} g \cdot p \; = \; p \, .$$

Since the space of parabolic invariants contains the space of invariants, the same is true of the span of

$$\frac{1}{|\mathcal{C}_m|} \sum_{g \in \mathcal{C}_m} g \cdot p$$

where p ranges over the parabolic invariants. By Theorem 4.10 each of these can be written as a linear combination of complete weight enumerators of self-dual codes, and thus Theorem 4.9 follows.

Proof. For any self-orthogonal code C, let

$$E_m(C) \ := \ \frac{1}{|\mathcal{C}_m|} \sum_{g \in \mathcal{C}_m} g \cdot \mathrm{cwe}(C(m)).$$

Averaging both sides of equation (1) in Lemma 4.7 over $\mathcal{C}_m$, we find

$$E_m(C) = \frac{1}{(2^m-1)}[(2^{m-r}-2^r)E_m(C) + 2^{-r} \sum_{\substack{C \subset C' \subseteq C'^{\perp} \\ [C':C]=2}} E_m(C')],$$

and solving for $E_m(C)$ gives

$$E_m(C) = \frac{1}{(2^r-1)(2^m+2^r)} \sum_{\substack{C \subset C' \subseteq C'^{\perp} \\ [C':C]=2}} E_m(C').$$

By induction on r (observing that the result follows from Theorem 3.5 when $r=0$), we have

$$E_m(C) = \prod_{1 \le i \le r} (2^m+2^i)^{-1} \frac{1}{(2^r-1)} \sum_{\substack{C \subset C' \subseteq C'^{\perp} \\ [C':C]=2}} \ \sum_{C' \subset C'' = C''^{\perp}} \mathrm{cwe}_m(C'').$$

But each code C'' is counted 2^r-1 times (corresponding to the 1-dimensional subspaces of C''/C); thus eliminating the sum over C' gives the desired result. $\square$

Note that

$$\mathrm{cwe}(C(m))(x_0, \ldots, x_{2^{m-1}-1}, x_0, \ldots, x_{2^{m-1}-1}) = \mathrm{cwe}(C(m-1))(x_0, \ldots, x_{2^{m-1}-1}) \ .$$

This gives a surjective map from the space of genus m complete weight enumerators to the space of genus $m-1$ complete weight enumerators. By Theorem 4.9 it follows that this also gives a surjective map from the genus m invariants to the genus $m-1$ invariants. (Runge's proof of Theorem 4.9 proceeds by first showing this map is surjective, using Siegel modular forms, and then arguing that this implies Theorem 4.9.) Since by Theorem 4.6 the parabolic invariants of degree N become linearly independent when $m \ge \frac{N}{2} - 1$, we have:

Corollary 4.11 *Let $\Phi_m(t)$ be the Molien series of the Clifford group of genus m. As m tends to infinity, the series $\Phi_m(t)$ tend monotonically to*

$$\sum_{k=0}^{\infty} N_{2k} t^{2k} \ ,$$

where N_{2k} is the number of equivalence classes of self-dual codes of length $2k$.

(For the definition of Molien series, see for example [5] or [32, Chapter 19].)

Explicit calculations for $m = 1, 2$ show:

Corollary 4.12 *The initial terms of the Molien series of the Clifford group of genus $m \geq 1$ are given by*

$$1 + t^2 + t^4 + t^6 + 2t^8 + 2t^{10} + O(t^{12}),$$

where the next term is $2t^{12}$ for $m = 1$, and $3t^{12}$ for $m > 1$.

Sidelnikov [46], [47] showed that the lowest degree of a harmonic invariant of $\mathcal{C}_m$ is 8. Inspection of the above Molien series gives the following stronger result.

Corollary 4.13 *The smallest degree of a harmonic invariant of $\mathcal{C}_m$ is 8, and there is a unique harmonic invariant of degree 8. There are no harmonic invariants of degree 10.*

The two-dimensional space of homogeneous invariants for $\mathcal{C}_m$ of degree 8 is spanned by the fourth power of the quadratic form and by $h_m := \mathrm{cwe}(H_8 \otimes_{\mathbb{F}_2} \mathbb{F}_{2^m})$, where H_8 is the $[8, 4, 4]$ binary Hamming code. We can give h_m explicitly.

Theorem 4.14 *Let $G(m, k)$ denote the set of k-dimensional subspaces of $\mathbb{F}_2^m$. Then*

$$\begin{aligned} h_m &= \sum_{v \in \mathbb{F}_2^m} x_v^8 + 14 \sum_{U \in G(m,1)} \sum_{d \in \mathbb{F}_2^m/U} \prod_{v \in d+U} x_v^4 \\ &\quad + 168 \sum_{U \in G(m,2)} \sum_{d \in \mathbb{F}_2^m/U} \prod_{v \in d+U} x_v^2 + 1344 \sum_{U \in G(m,3)} \sum_{d \in \mathbb{F}_2^m/U} \prod_{v \in d+U} x_v \ . \end{aligned} \tag{2}$$

The second term on the right-hand side is equal to $14 \sum_{\{u,v\}} x_u^4 x_v^4$, where $\{u, v\}$ runs through unordered pairs of elements of $\mathbb{F}_2^m$. The total number of terms is

$$2^m + 14 \begin{bmatrix} m \\ 1 \end{bmatrix} 2^{m-1} + 168 \begin{bmatrix} m \\ 2 \end{bmatrix} 2^{m-2} + 1344 \begin{bmatrix} m \\ 3 \end{bmatrix} 2^{m-3} = 2^{4m},$$

where $\begin{bmatrix} m \\ k \end{bmatrix} = |G(m, k)|$.

Proof. We will compute $\mathrm{cwe}(H_8 \otimes \mathbb{F}_2^m)$ (which is equal to $\mathrm{cwe}(H_8 \otimes \mathbb{F}_{2^m})$). Let H_8 be defined by the generator matrix

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} .$$

A codeword corresponds to a choice of $(a, b, c, d) \in \mathbb{F}_2^m$, one for each row; from the columns of the generator matrix we find that the corresponding term of the weight enumerator is

$$x_d x_{c+d} x_{b+d} x_{b+c+d} x_{a+d} x_{a+c+d} x_{a+b+d} x_{a+b+c+d} \ .$$

This depends only on the affine space $\langle a, b, c \rangle + d$. The four terms on the right-hand side of Eq. (2) correspond to $\dim\langle a, b, c \rangle = 0, 1, 2, 3$; the coefficients are the number of ways of choosing (a, b, c, d) for a given affine space. If $\dim\langle a, b, c \rangle = 3$, for example, there are $7 \cdot 6 \cdot 4$ ways to choose a, b, c and 8 ways to choose d, giving the coefficient $8 \cdot 7 \cdot 6 \cdot 4 = 1344$. $\square$

Remarks

(1) The unique harmonic invariant of degree 8 integrates to zero over the sphere, and so must have zeros on the sphere. The orbit of any such point under $\mathcal{C}_m$ therefore forms a spherical 11-design, cf. [25]. This was already observed by Sidelnikov [48].

(2) The case $m = 1$: $\mathcal{C}_1$ is a dihedral group of order 16 with Molien series $1/(1-\lambda^2)(1-\lambda^8)$, as in Gleason's theorem on the weight enumerators of binary self-dual codes [24], [32, Problem 3, p. 602], [38].

(3) The case $m = 2$: $\mathcal{C}_2$ has order 2304 and Molien series

$$\frac{1+\lambda^{18}}{(1-\lambda^2)(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{24})} .$$

(The reflection group $[3, 4, 3]$, No. 28 on the Shephard-Todd list, cf. [5, p. 199], is a subgroup of $\mathcal{C}_2$ of index 2.) The unique harmonic invariants f_8 and f_{12} (say) of degrees 8 and 12 are easily computed, and then one can find real points $(x_{00}, x_{01}, x_{10}, x_{11}) \in S^3$ where both f_8 and f_{12} vanish. Any orbit of such a point under $\mathcal{C}_2$ forms a spherical 15-design of size 2304 (cf. [25]). We conjecture that such points exists for all $m \geq 2$.

(4) The group $\mathcal{C}_3$ of order 5160960 has appeared in sufficiently many different contexts that it is worth placing its Molien series on record. It is $p(\lambda)/q(\lambda)$, where $p(\lambda)$ is the symmetric polynomial of degree 154 beginning

$$\begin{aligned} & 1+\lambda^8+\lambda^{16}+2\lambda^{20}+\lambda^{22}+2\lambda^{24}+3\lambda^{26}+4\lambda^{28} \\ + \; & 2\lambda^{30}+5\lambda^{32}+4\lambda^{34}+7\lambda^{36}+6\lambda^{38}+7\lambda^{40} \\ + \; & 8\lambda^{42}+11\lambda^{44}+9\lambda^{46}+12\lambda^{48}+13\lambda^{50}+14\lambda^{52} \\ + \; & 15\lambda^{54}+17\lambda^{56}+17\lambda^{58}+20\lambda^{60}+19\lambda^{62} \\ + \; & 20\lambda^{64}+20\lambda^{66}+25\lambda^{68}+22\lambda^{70}+22\lambda^{72} \\ + \; & 24\lambda^{74}+25\lambda^{76}+\cdots , \end{aligned}$$

and

$$q(\lambda) = (1-\lambda^2)(1-\lambda^{12})(1-\lambda^{14})(1-\lambda^{16})(1-\lambda^{24})^2(1-\lambda^{30})(1-\lambda^{40}) .$$

(5) For completeness, we mention that the Molien series for $E(1)$ is $\frac{1}{(1-\lambda^2)(1-\lambda^4)}$, with basic invariants $x_0^2 + x_1^2$ and $x_0^2 x_1^2$. For arbitrary m the Molien series for $E(m)$ is

$$\frac{1}{2n^2}\left\{\frac{1}{(1-\lambda)^n}+\frac{1}{(1+\lambda)^n}+\frac{n^2+n-2}{(1-\lambda^2)^{n/2}}+\frac{n^2-n}{(1+\lambda^2)^{n/2}}\right\} ,$$

where $n = 2^m$.

5 Real Clifford groups and Barnes-Wall-lattices

In a series of papers [2], [8], [9], [10], [50], Barnes, Bolt, Room and Wall investigated a family of lattices in $\mathbb{Q}^{2^m}$ (cf. also [12], [18]). They distinguish two geometrically similar lattices $L_m \subseteq L'_m$ in each dimension 2^m, for which if $m \neq 3$ the automorphism groups $\mathrm{Aut}(L_m) = \mathrm{Aut}(L'_m)$ are subgroups $\mathcal{G}_m$ of index 2 in the real Clifford group $\mathcal{C}_m$. When

$m = 3$, L_3 and L'_3 are two versions of the root lattice E_8, and $\mathcal{G}_3 := \mathrm{Aut}(L_3) \cap \mathrm{Aut}(L'_3)$ has index 270 in $\mathrm{Aut}(L_3)$ and index 2 in $\mathcal{C}_3$.

The lattices L_m and L'_m can be defined in terms of an orthonormal basis $b_0, \ldots, b_{2^m-1}$ of $\mathbb{R}^{2^m}$ as follows. Let $V := \mathbb{F}_2^m$ and index the basis elements $b_0, \ldots, b_{2^m-1}$ by the elements of V. For each affine subspace $U \subseteq V$ let $\chi_U \in \mathbb{Q}^{2^m}$ correspond to the characteristic function of U: $\chi_U := \sum_{i=1}^{2^m} \epsilon_i b_i$, where $\epsilon_i = 1$ if i corresponds to an element of U and $\epsilon_i = 0$ otherwise. Then L_m (resp. L'_m) is spanned by the set

$$\{2^{\lfloor (m-d+\delta)/2 \rfloor} \chi_U \mid 0 \leq d \leq m, U \text{ is a } d\text{-dimensional affine subspace of } V\} ,$$

where $\delta = 1$ for L_m and $\delta = 0$ for L'_m.

Extending scalars, we define the $\mathbb{Z}[\sqrt{2}]$-lattice

$$M_m := \sqrt{2} L'_m + L_m ,$$

which we call the balanced Barnes-Wall lattice.

From the generating sets for L_m and L'_m we have:

Remark 5.1 M_m is generated by the vectors $\sqrt{2}^{m-d} \chi_U$, where $0 \leq d \leq m$ and U runs through the affine subspaces of V of dimension d.

Lemma 5.2 *For all $m > 1$, the lattice M_m is a tensor product:*

$$M_m = M_{m-1} \otimes_{\mathbb{Z}[\sqrt{2}]} M_1 = M_1 \otimes_{\mathbb{Z}[\sqrt{2}]} M_1 \otimes_{\mathbb{Z}[\sqrt{2}]} \cdots \otimes_{\mathbb{Z}[\sqrt{2}]} M_1 \quad (\textit{with } m \textit{ factors}).$$

Proof. Write $V = \mathbb{F}_2^m = V_{m-1} \oplus V_1$ as the direct sum of an $(m-1)$-dimensional vector space V_{m-1} and a 1-dimensional space $V_1 = \langle v \rangle$, and arrange the basis vectors so that $b_0, \ldots, b_{2^{m-1}-1}$ correspond to the elements in V_{m-1} and $b_{2^{m-1}}, \ldots, b_{2^m-1}$ to the elements in $v + V_{m-1}$.

Let $\sqrt{2}^{m-d} \chi_U$ be a generator for M_m, where $U = a + U_0$ for a d-dimensional linear subspace U_0 of V and $a = a_{m-1} + a_1 \in V_{m-1} \oplus V_1$.

If $U_0 \leq V_{m-1}$, then

$$\sqrt{2}^{m-d} \chi_U = (\sqrt{2}^{m-1-d} \chi_{a_{m-1}+U_0}) \otimes \sqrt{2} \chi_{a_1} \in M_{m-1} \otimes_{\mathbb{Z}[\sqrt{2}]} M_1.$$

Otherwise $U_{m-1} := U_0 \cap V_{m-1}$ has dimension $d-1$ and $U_0 = U_{m-1} \cup (v_{m-1} + v + U_{m-1})$ for some $v_{m-1} \in V_{m-1}$. If $v_{m-1} \in U_{m-1}$, then

$$\sqrt{2}^{m-d} \chi_U = (\sqrt{2}^{m-1-(d-1)} \chi_{a_{m-1}+U_{m-1}}) \otimes \chi_{V_1}.$$

If $v_{m-1} \notin U_{m-1}$ we have the identity

$$\sqrt{2}^{m-d} \chi_U = (\sqrt{2}^{m-1-d} \chi_{a_{m-1}+U_{m-1}+\mathbb{F}_2 v_{m-1}}) \otimes \sqrt{2} \chi_{a_1} + (\sqrt{2}^{m-1-(d-1)} \chi_{a_{m-1}+v_{m-1}+U_{m-1}}) \otimes \chi_{V_1}$$
$$- \sqrt{2} (\sqrt{2}^{m-1-(d-1)} \chi_{a_{m-1}+v_{m-1}+U_{m-1}}) \otimes \sqrt{2} \chi_{a_1} .$$

Hence $M_m \subseteq M_{m-1} \otimes_{\mathbb{Z}[\sqrt{2}]} M_1$. The other inclusion follows more easily by similar arguments. $\square$

In view of Lemma 5.2, we have the following simple and apparently new construction for the Barnes-Wall lattice L_m. Namely, L_m is the rational part of the $\mathbb{Z}[\sqrt{2}]$-lattice $M_1^{\otimes m}$, where M_1 is the $\mathbb{Z}[\sqrt{2}]$-lattice with Gram matrix $\begin{bmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}$. For more about this construction see [34].

Proposition 5.3 *For all $m \geq 1$, the automorphism group $\mathrm{Aut}(M_m)$ (the subgroup of the orthogonal group $O(2^m, \mathbb{R})$ that preserves M_m) is isomorphic to $\mathcal{C}_m$.*

Proof. Let $(v_1, \ldots, v_{2^m})$ be a $\mathbb{Z}$-basis for L'_m such that $(2v_1, \ldots, 2v_{2^{m-1}}, v_{2^{m-1}+1}, \ldots, v_{2^m})$ is a $\mathbb{Z}$-basis for L_m. Then $(\sqrt{2}v_1, \ldots, \sqrt{2}v_{2^{m-1}}, v_{2^{m-1}+1}, \ldots, v_{2^m})$ is a $\mathbb{Z}[\sqrt{2}]$-basis for $M_m = \sqrt{2}L'_m + L_m$. Hence M_m has a $\mathbb{Z}$-basis $(\sqrt{2}v_1, \ldots, \sqrt{2}v_{2^m}, 2v_1, \ldots, 2v_{2^{m-1}}, v_{2^{m-1}+1}, \ldots, v_{2^m})$. Since the scalar products of the v_i are integral, the $\mathbb{Z}$-lattice M_m with respect to $\frac{1}{2}$ the trace form of the $\mathbb{Z}[\sqrt{2}]$-valued standard form on M_m is isometric to $\sqrt{2}L'_m \perp L_m$. In particular, the automorphism group of the $\mathbb{Z}[\sqrt{2}]$-lattice M_m is the subgroup of $\mathrm{Aut}(\sqrt{2}L_m \perp L'_m) \cong \mathcal{G}_m \wr S_2$ that commutes with the multiplication by $\sqrt{2}$. Hence $\mathrm{Aut}(M_m)$ contains $\mathcal{G}_m = \mathrm{Aut}(L_m) \cap \mathrm{Aut}(L'_m)$ as a subgroup of index at most two. Since

$$h \otimes I_{2^{m-1}} \in \mathrm{Aut}(M_1) \otimes \mathrm{Aut}(M_{m-1}) \subseteq \mathrm{Aut}(M_m),$$

by Lemma 5.2, $[\mathrm{Aut}(M_m) : \mathcal{G}_m] = 2$ and so $\mathrm{Aut}(M_m) \cong \mathcal{C}_m$. □

Lemma 5.4 *If $m \geq 2$, then the $\mathbb{Z}$-span (denoted $\overline{\mathbb{Z}[\mathcal{C}_m]}$) of the matrices in $\mathcal{C}_m$ acting on the 2^m-dimensional $\mathbb{Z}[\sqrt{2}]$-lattice M_m is $\mathbb{Z}[\sqrt{2}]^{2^m \times 2^m}$.*

Proof. We proceed by induction on m. Explicit calculations show that the lemma is true for $m = 2$ and $m = 3$. If $m \geq 4$ then $m - 2 \geq 2$ and by induction $\overline{\mathbb{Z}[\mathcal{C}_{m-2}]} = \mathbb{Z}[\sqrt{2}]^{2^{m-2} \times 2^{m-2}}$ and $\overline{\mathbb{Z}[\mathcal{C}_2]} = \mathbb{Z}[\sqrt{2}]^{4 \times 4}$. Since $M_m = M_2 \otimes_{\mathbb{Z}[\sqrt{2}]} M_{m-2}$, the automorphism group of M_m contains $\mathcal{C}_2 \otimes \mathcal{C}_{m-2}$. Hence

$$\mathbb{Z}[\sqrt{2}]^{2^m \times 2^m} \supseteq \overline{\mathbb{Z}[\mathcal{C}_m]} \supseteq \overline{\mathbb{Z}[\mathcal{C}_{m-2}]} \otimes_{\mathbb{Z}[\sqrt{2}]} \overline{\mathbb{Z}[\mathcal{C}_2]} = \mathbb{Z}[\sqrt{2}]^{2^m \times 2^m}.$$

□

We now proceed to show that for $m \geq 2$ the real Clifford group $\mathcal{C}_m$ is a maximal finite subgroup of $GL(2^m, \mathbb{R})$. For the investigation of possible normal subgroups of finite groups containing $\mathcal{C}_m$, the notion of a primitive matrix group plays a central role. A matrix group $G \leq GL(V)$ is called imprimitive if there is a nontrivial decomposition $V = V_1 \oplus \ldots \oplus V_s$ of V into subspaces which are permuted under the action of G. G is called primitive if it is not imprimitive. If N is a normal subgroup of G then G permutes the isotypic components of $V_{|N}$. So if G is primitive, the restriction of V to N is isotypic, i.e. is a multiple of an irreducible representation. In particular, since the image of an irreducible representation of an abelian group N is cyclic, all abelian normal subgroups of G are cyclic.

Lemma 5.5 *Let $m \geq 2$. Let G be a finite group with $\mathcal{C}_m \leq G \leq GL(2^m, \mathbb{R})$ and let p be a prime. If p is odd, the maximal normal p-subgroup of G is trivial. The maximal normal 2-subgroup of G is either $E(m)$ if $G = \mathcal{C}_m$, or $Z(E(m)) = \langle -I_{2^m} \rangle$ if $G > \mathcal{C}_m$.*

Proof. We first observe that the only nontrivial normal subgroup of $\mathcal{C}_m$ that is properly contained in $E(m)$ is $Z(E(m)) = \langle -I_{2^m} \rangle$. Therefore, if U is a normal subgroup of G, $U \cap E(m)$ is one of 1, $Z(E(m))$ or $E(m)$.

The matrix group $\mathcal{C}_m$ and hence also G is primitive. In particular, all abelian normal subgroups of G are cyclic. Let $p > 2$ be a rational prime and $U \trianglelefteq G$ a normal p-subgroup of G. The degree of the absolutely irreducible representations of U that occur in $\mathbb{R}^{2^m}_{|U}$ is a power of p and divides 2^m. So this degree is 1 and U is abelian, hence cyclic by the primitivity of G. Therefore the automorphism group of U does not contain $E(m)/Z(E(m))$. Since $C_G(U) \cap E(m)$ is a normal subgroup of $\mathcal{C}_m$, it equals $E(m)$ and hence $E(m)$ centralizes U. Since $E(m)$ is already absolutely irreducible, U consists of scalar matrices in $GL(2^m, \mathbb{R})$, and therefore $U = 1$. If $p = 2$ and $G \neq \mathcal{C}_m$, then $U \neq E(m)$, because $\mathcal{C}_m$ is the largest finite subgroup of $GL(2^m, \mathbb{R})$ that normalizes $E(m)$. Since the normal 2-subgroups of G do not contain an abelian noncyclic characteristic subgroup, the possible normal 2-subgroups are classified in a theorem of P. Hall (cf. [27, p. 357]). In particular they do not contain $\mathcal{C}_m/Z(E(m))$ as a subgroup of their automorphism groups, so again U commutes with $E(m)$, and therefore consists only of scalar matrices. $\square$

Theorem 5.6 *Let $m \geq 2$. Then the real Clifford group $\mathcal{C}_m$ is a maximal finite subgroup of $GL(2^m, \mathbb{R})$.*

Proof. Let G be a finite subgroup of $GL(2^m, \mathbb{R})$ that properly contains $\mathcal{C}_m$. By Lemma 5.5, all normal p-subgroups of G are central. By a theorem of Brauer, every representation of a finite group is realizable over a cyclotomic number field (cf. [43, §12.3]). In fact, since the natural representation of G is real, it is even true that G is conjugate to a subgroup of $GL(2^m, K)$ for some totally real abelian number field K containing $\mathbb{Q}[\sqrt{2}]$ (cf. [19, Proposition 5.6]). Let K be a minimal such field and assume that $G \leq GL(2^m, K)$. Let R be the ring of integers of K. Then G fixes an $R\mathcal{C}_m$-lattice. By Lemma 5.4 all $R\mathcal{C}_m$-lattices are of the form $I \otimes_{\mathbb{Z}[\sqrt{2}]} M_m$ for some fractional ideal I of R, the group G fixes all $R\mathcal{C}_m$-lattices and hence also $R \otimes_{\mathbb{Z}[\sqrt{2}]} M_m$. So any choice of an R-basis for M_m gives rise to an embedding $G \hookrightarrow GL(2^m, R)$, by which we may regard G as a group of matrices. Without loss of generality we may assume that $G = \mathrm{Aut}(R \otimes_{\mathbb{Z}[\sqrt{2}]} M_m)$. Then the Galois group $\Gamma := \mathrm{Gal}(K/\mathbb{Q}[\sqrt{2}])$ acts on G by acting componentwise on the matrices. Seeking a contradiction, we assume $K \neq \mathbb{Q}[\sqrt{2}]$. It is enough to show that there is a nontrivial element $\sigma \in \Gamma$ that acts trivially on G, because then the matrices in G have their entries in the fixed field of σ, contradicting the minimality of K.

Assume first that there is an odd prime p ramified in $K/\mathbb{Q}$, and let $\wp$ be a prime ideal of R that lies over p. Then p is also ramified in $K/\mathbb{Q}[\sqrt{2}]$ and therefore the action of the ramification group, the stabilizer in Γ of $\wp$, on $R/\wp$ is not faithful, hence the first inertia group

$$\Gamma_\wp := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}[\sqrt{2}]) \mid \sigma(x) \equiv x \pmod{\wp} \text{ for all } x \in R\}$$

is nontrivial (see e.g. [22, Corollary III.4.2]). Since $G_\wp := \{g \in G \mid g \equiv I_{2^m} \pmod{\wp}\}$ is a normal p-subgroup of G, $G_\wp = 1$ by Lemma 5.5. Therefore all the elements in $\Gamma_\wp$ act trivially on G, which is what we were seeking to prove.

So 2 is the only ramified prime in K, which implies that $K = \mathbb{Q}[\zeta_{2^a} + \zeta_{2^a}^{-1}]$ for some $a \geq 3$, where $\zeta_t = \exp(2\pi i/t)$. If $a = 3$, then $K = \mathbb{Q}[\sqrt{2}]$, $G = \mathrm{Aut}(M_m) = \mathcal{C}_m$ and we are done. So assume $a > 3$ and let $\wp$ be the prime ideal of R over 2 (generated by $(1-\zeta_{2^a})(1-\zeta_{2^a}^{-1})$) and let $\sigma \in \Gamma$ be the Galois automorphism defined by $\sigma(\zeta_{2^a}+\zeta_{2^a}^{-1}) = \zeta_{2^a}^{2^{a-1}+1}+\zeta_{2^a}^{-2^{a-1}-1} = -(\zeta_{2^a}+\zeta_{2^a}^{-1})$. Then $id = \sigma^2 \neq \sigma$ and

$$(\zeta_{2^a} + \zeta_{2^a}^{-1}) - \sigma(\zeta_{2^a} + \zeta_{2^a}^{-1}) = 2(\zeta_{2^a} + \zeta_{2^a}^{-1}) \in 2\wp.$$

Therefore $\sigma \in \Gamma_{2\wp}$. Since the subgroup $G_{2\wp} := \{g \in G \mid g \equiv I_{2^m} \pmod{2\wp}\}$ of G is trivial (cf. [3, Hilfssatz 1]) one concludes that σ acts trivially on G, and thus G is in fact defined over $\mathbb{Q}[\zeta_{2^{a-1}} + \zeta_{2^{a-1}}^{-1}]$. The theorem follows by induction. $\square$

Corollary 5.7 *Let $m \geq 1$ and let C be a self-dual code over $\mathbb{F}_2$ that is not generated by vectors of weight 2. Then*

$$\mathcal{C}_m = \mathrm{Aut}_{O(2^m,\mathbb{R})}(\mathrm{cwe}(C(m)).$$

Proof. The proof for the case $m = 1$ will be postponed to Section 6. Assume $m \geq 2$. We first show that the parabolic subgroup $H \leq \mathcal{C}_m$ acts irreducibly on the Lie algebra $\mathrm{Lie}(O(2^m,\mathbb{R}))$, the set of real $2^m \times 2^m$ matrices X such that $X = -X^{tr}$. The group $AGL(m,2)$ acts 2-transitively on our standard basis $b_0, \ldots, b_{2^m-1}$ for $\mathbb{R}^{2^m}$. A basis for $\mathrm{Lie}(O(2^m,\mathbb{R}))$ is given by the matrices $b_{ij} := b_i \otimes b_j - b_j \otimes b_i$ for $0 \leq i < j \leq 2^m - 1$. Since $AGL(m,2)$ acts transitively on the b_{ij}, a basis for the endomorphism ring $\mathrm{End}_{AGL(m,2)}(\mathrm{Lie}(O(2^m,\mathbb{R})))$ is given by the orbits of the stabilizer of b_{01}. Representatives for these orbits are b_{01}, b_{02}, b_{23} and b_{24}. But the generator corresponding to the quadratic form $q(v_1, \ldots, v_m) := v_2^2$ negates b_2 and fixes b_0 and b_4, and therefore does not commute with the endomorphism corresponding to b_{02} or b_{24}. Similarly the endomorphism corresponding to b_{23} is ruled out by $q(v_1, \ldots, v_m) := v_1v_2$.

Let $G := \mathrm{Aut}_{O(2^m,\mathbb{R})}(\mathrm{cwe}(C(m))$. Then G is a closed subgroup of $O(2^m,\mathbb{R})$ and hence is a Lie group (cf. [37, Theorem 3.4]). Since G contains $\mathcal{C}_m$ it acts irreducibly on $\mathrm{Lie}(O(2^m,\mathbb{R}))$. Assume that $G \neq \mathcal{C}_m$. Then G is infinite by Theorem 5.6 and therefore G contains $SO(2^m,\mathbb{R})$. However, the ring of invariants of $SO(2^m,\mathbb{R})$ is generated by the quadratic form $\sum_{i=0}^{2^m-1} x_{b_i}^2$. The only binary self-dual codes C that produce such complete weight enumerators are direct sums of copies of the code $\{00, 11\}$. $\square$

6 The complex Clifford groups and doubly-even codes

There are analogues for the complex Clifford group $\mathcal{X}_m$ for most of the above results. (Z_a will denote a cyclic group of order a.)

Definition 6.1 *The* complex Clifford group *$\mathcal{X}_m$ is the normalizer in $U(2^m, \mathbb{Q}[\zeta_8])$ of the central product $E(m) \curlyvee Z_4$.*

As in the real case, one concludes that

$$\mathcal{X}_m \cong (2_+^{1+2m} \curlyvee Z_8).Sp(2m,2) \cong (2_+^{1+2m} \curlyvee Z_8).O(2m+1,2)$$

(cf. [33, Cor. 8.4]).

The analogue of Theorem 4.9 is the following, which can be proved in essentially the same way.

Theorem 6.2 *(Runge [42].) Fix integers N and $m \geq 1$. The space of homogeneous invariants of degree N for the complex Clifford group $\mathcal{X}_m$ is spanned by* $\mathrm{cwe}(C(m))$*, where C ranges over all binary doubly-even self-dual codes of length N. (In particular, when N is not a multiple of 8, the invariant space is empty.)*

The analogues of Theorem 4.10 and Proposition 5.3 are:

Theorem 6.3 *For any doubly-even binary code C of length $N \equiv 0(8)$ containing $\mathbf{1}$ and of dimension $N/2 - r$,*

$$\frac{1}{|\mathcal{X}_m|} \sum_{g \in \mathcal{X}_m} g \cdot \mathrm{cwe}(C(m)) = \prod_{0 \leq i < r} (2^m + 2^i)^{-1} \sum_{C'} \mathrm{cwe}(C'(m)),$$

where the sum is over all doubly-even self-dual codes C' containing C.

Proposition 6.4 *Let $\mathbb{M}_m := \mathbb{Z}[\zeta_8] \otimes_{\mathbb{Z}[\sqrt{2}]} M_m$. Then the subgroup of $U(2^m, \mathbb{Q}[\zeta_8])$ preserving $\mathbb{M}_m$ is precisely $\mathcal{X}_m$.*

We omit the proofs.

For the analogue of Lemma 5.4, observe that the matrices in $\mathcal{X}_m$ generate a maximal order. Even for $m = 1$ the $\mathbb{Z}$-span of the matrices in $\mathcal{X}_1$ acting on $\mathbb{M}_1$ is the maximal order $\mathbb{Z}[\zeta_8]^{2\times 2}$. Hence the induction argument used to prove Lemma 5.4 shows that $\overline{\mathbb{Z}[\mathcal{X}_m]} = \mathbb{Z}[\zeta_8]^{2^m \times 2^m}$. Therefore the analogue of Theorem 5.6 holds even for $m = 1$:

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

Proof. As in the proof of Theorem 5.6, we may assume that G is contained in $U(2^m, K)$ for some abelian number field K containing ζ_8. Let R be the ring of integers in K and T the group of roots of unity in R. Then $T\mathcal{X}_m$ is the normalizer in $U(2^m, K)$ of $TE(m)$ (cf. [33, Cor. 8.4]). As before, the $R\mathcal{X}_m$-lattices in the natural module are of the form $I \otimes_{\mathbb{Z}[\zeta_8]} \mathbb{M}_m$, where I is a fractional ideal of R. Since G fixes one of these lattices, it also fixes $R \otimes_{\mathbb{Z}[\zeta_8]} \mathbb{M}_m$. As in the proof of Theorem 5.6, we write the elements of G as matrices with respect to a basis for $\mathbb{M}_m$ and assume that G is the full (unitary) automorphism group of $R \otimes_{\mathbb{Z}[\zeta_8]} \mathbb{M}_m$. Then the Galois group $\Gamma := \mathrm{Gal}(K/\mathbb{Q}[\zeta_8])$ acts on G. Assume that $G \neq T\mathcal{X}_m$. Then $TE(m)$ is not normal in G. As in Lemma 5.5 one shows that the maximal normal p-subgroup of G is central for all primes p. Let $\wp$ be a prime ideal in R that ramifies in $K/\mathbb{Q}[\zeta_8]$, and let σ be an element of the inertia group $\Gamma_\wp$. Then for all $g \in G$, the image g^σ satisfies $a(g) := g^{-1} g^\sigma \in G_\wp := \{g \in G \mid g \equiv I_{2^m} \pmod{\wp}\}$. Since $G_\wp$ is a normal p-subgroup, where p is the rational prime divisible by $\wp$, it is central. Therefore the map $g \mapsto a(g)$ is a homomorphism of G into an abelian group, and hence the commutator subgroup G' is fixed under σ. Since any abelian extension K of $\mathbb{Q}$ that properly contains $\mathbb{Q}[\zeta_8]$ is ramified at some finite prime of $\mathbb{Q}[\zeta_8]$, we conclude that $G' \subseteq \mathrm{Aut}(\mathbb{M}_m)$. Since $E(m) \mathsf{Y} Z_8 \leq \mathrm{Aut}(\mathbb{M}_m)' \mathsf{Y} Z_8$ is characteristic in $\mathrm{Aut}(\mathbb{M}_m)$ and therefore also in $G' \mathsf{Y} Z_8$, the group $TE(m)$ is normal in G, which is a contradiction. $\square$

Corollary 6.6 *Assume $m \geq 1$ and let C be a binary self-dual doubly-even code of length N. Then*

$$\mathrm{Aut}_{U(2^m,\mathbb{C})}(\mathrm{cwe}(C \otimes \mathbb{F}_{2^m})) = \langle \mathcal{X}_m, \zeta_N I_{2^m} \rangle \ .$$

Remarks

(1) The case $m = 1$: $\mathcal{X}_1$ is a unitary reflection group (No. 9 on the Shephard-Todd list) of order 192 with Molien series $1/(1-\lambda^8)(1-\lambda^{24})$, as in Gleason's theorem on the weight enumerators of doubly-even binary self-dual codes [24], [32, p. 602, Theorem 3c], [38].

(2) The case $m = 2$: $\mathcal{X}_2$ has order 92160 and Molien series

$$\frac{1+\lambda^{32}}{(1-\lambda^8)(1-\lambda^{24})^2(1-\lambda^{40})} .$$

This has a reflection subgroup of index 2, No. 31 on the Shephard-Todd list.

(3) The case $m = 3$: $\mathcal{X}_3$ has order 743178240, and the Molien series can be written as $p(\lambda^8)/q(\lambda)$, where $p(\lambda)$ is the symmetric polynomial of degree 44 beginning

$$\begin{aligned} &1+\lambda^3+3\lambda^4+3\lambda^5+6\lambda^6+8\lambda^7+12\lambda^8+18\lambda^9+25\lambda^{10}+29\lambda^{11}+40\lambda^{12}+50\lambda^{13} \\ &\quad +58\lambda^{14}+69\lambda^{15}+80\lambda^{16}+85\lambda^{17}+96\lambda^{18}+104\lambda^{19}+107\lambda^{20}+109\lambda^{21}+112\lambda^{22}+\ldots \end{aligned}$$

and

$$q(\lambda) = (1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})^2(1-\lambda^{40})(1-\lambda^{56})(1-\lambda^{72})(1-\lambda^{120}).$$

Runge [40] gives the Molien series for the commutator subgroup $\mathcal{H}_3 = \mathcal{X}_3'$, of index 2 in $\mathcal{X}_3$. The Molien series for $\mathcal{X}_3$ consists of the terms in the series for $\mathcal{H}_3$ that have exponents divisible by 4. Oura [36] has computed the Molien series for $\mathcal{H}_4 = \mathcal{X}_4'$, and that for $\mathcal{X}_4$ can be obtained from it in the same way. Other related Molien series can be found in [1].

Proof of Corollary 5.7, case $m = 1$.

Let C be a self-dual binary code of length n with Hamming weight enumerator $\mathrm{hwe}_C(x, y)$. We will show that if C is not generated by vectors of weight 2 then $\mathrm{Aut}_{O(2)}(\mathrm{hwe}_C) = \mathcal{C}_1$.

Certainly $G := \mathrm{Aut}_{O(2)}(\mathrm{hwe}_C)$ contains $\mathcal{C}_1 = D_{16}$; we must show it is no larger. The only closed subgroups of $O(2)$ containing D_{16} are the dihedral groups D_{16k} for $k \geq 1$ and $O(2)$ itself. So if the result is false then G contains a rotation

$$\rho(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

where θ is not a multiple of $\pi/4$.

Consider the shadow $S(C)$ of C [38]; that is, the set of vectors $v \in \mathbb{F}_2^n$ such that

$$\mathrm{wt}(v+w) \equiv \mathrm{wt}(v) \pmod 4, \quad \text{for all } w \in C.$$

The weight enumerator of $S(C)$ is given by $S(x, y) = 2^{-n/2}\,\mathrm{hwe}_C(x + y, i(x - y))$. Then $\rho(\theta) \in G$ if and only if $S(x, y) = S(e^{i\theta}x, e^{-i\theta}y)$, or in other words if and only if for all $v \in S(C)$, $(n - 2\,\mathrm{wt}(v))\theta$ is a multiple of 2π.

Now, pick a vector $v_0 \in S(C)$, and consider the polynomial $W(x, y, z, w)$ given by

$$\sum_{v\in C} x^{n-\mathrm{wt}(v_0)-\mathrm{wt}((\mathbf{1}+v_0)\cap v)}\ y^{\mathrm{wt}((\mathbf{1}+v_0)\cap v)}\ z^{\mathrm{wt}(v_0)-\mathrm{wt}(v_0\cap v)}\ w^{\mathrm{wt}(v_0\cap v)} .$$

This has the following symmetries:

$$W(x, iy, z, -iw) = W(x, y, z, w),$$

$$W((x+y)/\sqrt{2},(x-y)/\sqrt{2},(z+w)/\sqrt{2},(z-w)/\sqrt{2}) = W(x,y,z,w).$$

Furthermore, since $S(C) = v_0 + C$, $\rho(\theta) \in G$ if and only if

$$W(e^{i\theta}x, e^{-i\theta}y, e^{-i\theta}z, e^{i\theta}w) = W(x,y,z,w).$$

To each of these symmetries we associate a 2×2 unitary matrix U such that (x,y) is transformed according to U and (z,w) according to $\overline{U}$. The first two symmetries generate the complex group $\mathcal{X}_1$, which is maximally finite in $PU(2)$ by Theorem 6.5. On the other hand, we can check directly that

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \notin \mathcal{X}_1,$$

even up to scalar multiplication. Thus the three symmetries topologically generate $PU(2)$; and hence W is invariant under any unitary matrix of determinant ± 1. Since $\mathrm{hwe}_C(x,y) = W(x,y,x,y)$, it follows that $G = O(2)$. But then

$$\mathrm{hwe}_C(x,y) = (x^2+y^2)^{n/2},$$

implying that C is generated by vectors of weight 2.

This completes the proof of Corollary 5.7. $\square$

7 Clifford groups for $p > 2$

Given an odd prime p, there again is a natural representation of the extraspecial p-group $E_p(m) \cong p_+^{1+2m}$ of exponent p, this time in $U(p^m, \mathbb{C})$; to be precise, $E_p(1)$ is generated by transforms

$$X : v_x \mapsto v_{x+1}, \text{ and } Z : v_x \mapsto \exp(2\pi i x/p) v_x,\ x \in \mathbb{Z}/p\mathbb{Z}\ ,$$

and $E_p(m)$ is the m-th tensor power of $E_p(1)$. The Clifford group $\mathcal{C}_m^{(p)}$ is then defined to be the normalizer in $U(p^m, \mathbb{Q}[\zeta_{ap}])$ of $E_p(m)$, where $a = gcd\{p+1, 4\}$. As above, one finds that

$$\mathcal{C}_m^{(p)} \cong Z_a \times p_+^{1+2m}.Sp(2m,p)$$

(cf. e.g. [51]).

As before, the invariants of these Clifford groups are given by codes:

Theorem 7.1 *Fix integers N and $m \geq 1$. The space of invariants of degree N for the Clifford group $\mathcal{C}_m^{(p)}$ is spanned by $\mathrm{cwe}(C(m))$, where C ranges over all self-dual codes over $\mathbb{F}_p$ of length N containing $\mathbf{1}$.*

Theorem 7.2 *For any self-orthogonal code C over $\mathbb{F}_p$ of length N containing $\mathbf{1}$ and of dimension $N/2 - r$,*

$$\frac{1}{|\mathcal{C}_m^{(p)}|} \sum_{g \in \mathcal{C}_m^{(p)}} g \cdot \mathrm{cwe}(C(m)) = \prod_{0 \leq i < r} (p^m + p^i)^{-1} \sum_{C'} \mathrm{cwe}(C'(m)),$$

where the sum is over all self-dual codes C' containing C (and in particular is 0 if no such code exists).

Regarding maximal finiteness, the arguments we used for $p = 2$ to prove Theorem 5.6 do not carry over to odd primes, since the groups $\mathcal{C}_m^{(p)}$ do not span a maximal order. Lindsey [31] showed by group theoretic arguments that $\mathcal{C}_1^{(p)}$ is a maximal finite subgroup of $SL(p, \mathbb{C})$ (cf. [6] for $p = 3$, [11] for $p = 5$). For $p^m = 9$, the theorem below follows from [21] and [26].

Theorem 7.3 *Let $p > 2$ be a prime and $m \geq 1$. If G is a finite group with $\mathcal{C}_m^{(p)} \leq G \leq GL(p^m, \mathbb{C})$, there exists a root of unity ζ such that*

$$G = \langle \mathcal{C}_m^{(p)}, \zeta I_{p^m} \rangle.$$

Proof. As before we may assume that G is contained in $U(p^m, K)$ for some abelian number field K containing ζ_p. Let $\mathcal{L}$ denote the set of rational primes l satisfying the following four properties: (i) G is l-adically integral, (ii) l is unramified in K, (iii) $|G| < |PGL(p^m, l)|$, (iv) l splits completely in K. Since all but finitely many primes satisfy conditions (i)-(iii), and infinitely many primes satisfy (iv) (by the Čebotarev Density Theorem), it follows that the set $\mathcal{L}$ is infinite.

Fix a prime $\mathfrak{l}$ over $l \in \mathcal{L}$. Since G is l-adically integral, we can reduce it mod $\mathfrak{l}$, obtaining a representation of G in $GL(p^m, l)$. Since p is ramified in K, $l \neq p$, so this representation is faithful on the extraspecial group. Since the extraspecial group acts irreducibly, the representation is in fact faithful on the entire Clifford group. Thus G mod $\mathfrak{l}$ contains the normalizer of an extraspecial group, but modulo scalars is strictly contained in $PGL(p^m, l)$ (by condition (iii)). It follows from the main theorem of [30] that for $p^m \geq 13$ G mod $\mathfrak{l}$ and $\mathcal{C}_m^{(p)}$ mod $\mathfrak{l}$ coincide as subgroups of $PGL(p^m, l)$. For $p^m < 13$ this already follows from the references in the paragraph preceding the theorem.

Fix a coset S of $\mathcal{C}_m^{(p)}$ in G. For each prime $\mathfrak{l}|l$ with $l \in \mathcal{L}$, the above argument implies that we can choose an element $g \in S$ such that $g \propto 1 \pmod{\mathfrak{l}}$. As there are infinitely many such primes, at least one such g must get chosen infinitely often. But then we must actually have $g \propto 1$ in K, and since g has finite order, $g = \zeta_S$ for some root of unity ζ_S.

Since this holds for all cosets S, G is generated by $\mathcal{C}_m^{(p)}$ together with the roots of unity ζ_S, proving the theorem. $\square$

Remark 7.4 It is worth pointing out that the proof of the main theorem in [30] relies heavily on the classification of finite simple groups, which is why we preferred to use our alternative arguments when proving Theorem 5.6.

References

[1] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 1194–1205.

[2] E. S. Barnes and G. E. Wall, Some extreme forms defined in terms of Abelian groups, *J. Australian Math. Soc.* **1** (1959), 47–63.

[3] H.-J. Bartels, Zur Galoiskohomologie definiter arithmetischer Gruppen, *J. reine angew. Math.* **298** (1978), 89–97.

[4] C. H. Bennett, D. DiVincenzo, J. A. Smolin and W. K. Wootters, Mixed state entanglement and quantum error correction, *Phys. Rev. A* **54** (1996), 3824–3851.

[5] D. J. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press, 1993.

[6] H. F. Blichfeldt, *Finite Collineation Groups*, University of Chicago Press, Chicago, 1917.

[7] S. Böcherer, Siegel modular forms and theta series, in *Theta functions (Bowdoin 1987)*, Proc. Sympos. Pure Math., **49**, Part 2, Amer. Math. Soc., Providence, RI, 1989, pp. 3–17.

[8] B. Bolt, The Clifford collineation, transform and similarity groups III: generators and involutions, *J. Australian Math. Soc.* **2** (1961), 334–344.

[9] B. Bolt, T. G. Room and G. E. Wall, On Clifford collineation, transform and similarity groups I, *J. Australian Math. Soc.* **2** (1961), 60–79.

[10] B. Bolt, T. G. Room and G. E. Wall, On Clifford collineation, transform and similarity groups II, *J. Australian Math. Soc.* **2** (1961), 80–96.

[11] R. Brauer, Über endliche lineare Gruppen von Primzahlgrad, *Math. Annalen* **169** (1967), 73–96

[12] M. Broué and M. Enguehard, Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes, *Ann. scient. Éc. Norm. Sup.* 4^e série, **6** (1973), 17–52. Summary in *C. R. Acad. Sc. Paris* **274** (1972), 19–22.

[13] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads and extremal Euclidean line-sets, *Proc. London Math. Soc.* **75** (1997), 436–480.

[14] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor and N. J. A. Sloane, A group-theoretic framework for the construction of packings in Grassmannian spaces, *J. Algebraic Combin.* **9** (1999), 129–140.

[15] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction orthogonal geometry, *Phys. Rev. Letters* **78** (1997), 405–409.

[16] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[17] J. H. Conway, R. H. Hardin and N. J. A. Sloane, Packing lines, planes, etc.: packings in Grassmannian space, *Experimental Math.* **5** (1996), 139-159.

[18] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag, New York, 1998.

[19] A. W. Dress, Induction and structure theorems for orthogonal representations of finite groups, *Annals of Mathematics* **102** (1975), 291–325.

[20] W. Duke, On codes and Siegel modular forms, *Intern. Math. Res. Notices* **5** (1993), 125–136.

[21] W. Feit, On finite linear groups in dimension at most 10, in *Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975)*, Academic Press, New York, 1976, pp. 397–407.

[22] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, 1991.

[23] S. P. Glasby, On the faithful representations, of degree 2^n, of certain extensions of 2-groups by orthogonal and symplectic groups. *J. Australian Math. Soc. Ser. A* **58**, (1995), 232–247.

[24] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes, Congrés International de Mathématiques (Nice, 1970)*, Gauthiers-Villars, Paris, 1971, Vol. 3, pp. 211–215.

[25] J.-M. Goethals and J. J. Seidel, The football, *Nieuw Archief voor Wiskunde* **29** (1981), 50–58. Reprinted in *Geometry and Combinatorics: Selected Works of J. J. Seidel*, ed. D. G. Corneil and R. Mathon, Academic Press, 1991, pp. 363–371.

[26] W. C. Huffman and D. B. Wales, Linear groups of degree nine with no elements of order seven. *J. Algebra* **51** (1978), 149–163.

[27] B. Huppert, *Endliche Gruppen I*, Springer-Verlag (1967)

[28] L. S. Kazarin, On certain groups defined by Sidelnikov (in Russian), *Mat. Sb.* **189** (No. 7, 1998), 131–144; English translation in *Sb. Math.* **189** (1998), 1087–1100.

[29] A. Y. Kitaev, Quantum computations: algorithms and error correction (in Russian), *Uspekhi Mat. Nauk.* **52** (No. 6, 1997), 53–112; English translation in *Russian Math. Surveys* **52** (1997), 1191-1249.

[30] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge Univ. Press, 1988.

[31] J.H. Lindsey II, Finite linear groups of prime degree, *Math. Annalen* **189** (1970), 47–59.

[32] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[33] G. Nebe, Finite quaternionic matrix groups, *Representation Theory* **2** (1998), 106-223.

[34] G. Nebe, E. M. Rains and N. J. A. Sloane, A simple construction for the Barnes-Wall lattices, in *Forney Festschrift*, edited R. Blahut, to appear, 2000.

[35] G. Nebe, E. M. Rains and N. J. A. Sloane, Generalized self-dual codes and Clifford-Weil groups, preprint.

[36] M. Oura, The dimension formula for the ring of code polynomials in genus 4, *Osaka J. Math.* (1997), **34**, pp. 53–72.

[37] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, San Diego, 1994.

[38] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, ed. V. Pless and W. C. Huffman, Elsevier, Amsterdam, 1998, pp. 177–294.

[39] B. Runge, On Siegel modular forms I, *J. reine angew. Math.* **436** (1993), 57–85.

[40] B. Runge, On Siegel modular forms II, *Nagoya Math. J.* **138** (1995), 179–197.

[41] B. Runge, The Schottky ideal, in *Abelian Varieties (Egloffstein, 1993)*, de Gruyter, Berlin, 1995, pp. 251–272.

[42] B. Runge, Codes and Siegel modular forms, *Discrete Math.* **148** (1996), 175–204.

[43] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, 1977.

[44] P. W. Shor and N. J. A. Sloane, A family of optimal packings in Grassmannian manifolds, *J. Algebraic Combin.* **7** (1998), 157–163.

[45] V. M. Sidelnikov, On a finite group of matrices and codes on the Euclidean sphere (in Russian), *Probl. Peredach. Inform.* **33** (1997), 35–54 (1997); English translation in *Problems Inform. Transmission* **33** (1997), 29–44 .

[46] V. M. Sidelnikov, On a finite group of matrices generating orbit codes on the Euclidean sphere, in *Proceedings IEEE Internat. Sympos. Inform. Theory, Ulm, 1997*, IEEE Press, 1997, p. 436.

[47] V. M. Sidelnikov, Spherical 7-designs in 2^n-dimensional Euclidean space, *J. Algebraic Combin.* **10** (1999), 279–288.

[48] V. M. Sidelnikov, Orbital spherical 11-designs in which the initial point is a root of an invariant polynomial (in Russian), *Algebra i Analiz* **11** (No. 4, 1999), 183–203.

[49] B. Venkov, Réseaux et "designs" sphériques, in *Réseaux euclidiens, "designs" sphériques et groupes*, L'Enseignement Mathématiques Monographie **37**, edited J. Martinet, to appear, 2000.

[50] G. E. Wall, On Clifford collineation, transform and similarity groups IV: an application to quadratic forms, *Nagoya Math. J.* **21** (1962), 199–222.

[51] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mtn. J. Math.* **2** (1972), 159–168.