A Simple Construction for the Barnes-Wall Lattices

Gabriele Nebe

Lehrstuhl B für Mathematik, RWTH Aachen
Templergraben 64, 52062 Aachen, Germany

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.

To Dave Forney, on the occasion of his sixtieth birthday

ABSTRACT

A certain family of orthogonal groups (called "Clifford groups" by G. E. Wall) has arisen in a variety of different contexts in recent years. These groups have a simple definition as the automorphism groups of certain generalized Barnes-Wall lattices. This leads to an especially simple construction for the usual Barnes-Wall lattices.

{This is based on the third author's talk at the Forney-Fest, M.I.T., March 2000, which in turn is based on our paper "The Invariants of the Clifford Groups" (preprint, 1999), to which the reader is referred for further details and proofs.}

1. Background

The Barnes-Wall lattices define an infinite sequence of sphere packings in dimensions 2^m, $m \geq 0$, which include the densest packings known in dimensions 1, 2, 4, 8 and 16 [1], [13]. In dimensions 32 and higher they are less dense than other known packings, but they are still interesting for other reasons — they form one of the few infinite sequences of lattices where it is possible to do explicit calculations. For example, there is an explicit formula for their kissing numbers [13]. This talk will describe a beautifully simple construction for these lattices that we found in the summer of 1999. A more comprehensive account will appear elsewhere [20], [21]. Since Dave Forney is fond of the Barnes-Wall lattices (cf. [14], [15]) we hope he will like this construction as much as we do.

This work had its origin in 1995 when J. H. Conway, R. H. Hardin and N. J. A. S. were studying packings in Grassmann manifolds — in other words, packings of Euclidean k-dimensional subspaces in n-dimensional space [12]. One of our nicest constructions was an optimal packing of 70 4-dimensional subspaces in $\mathbb{R}^8$. The symmetry group of this packing (the subgroup of the orthogonal group $O(8, \mathbb{R})$ that fixes the collection of subspaces) has order 5160960.

Shortly afterwards, the same 8-dimensional group arose in the work of P. W. Shor and others on quantum computers (cf. [2], [18]).

This astonishing coincidence — see [11] for the full story — drew attention to earlier work on the family to which this group belongs [5], [6], [7], [8], [32]. Following Wall, we call these Clifford groups, although these are not the groups usually referred to by this name [22]. Investigation of the representations of subgroups of these groups led to further constructions of optimal packings in Grassmann manifolds [9] and constructions of quantum error-correcting codes [10], [11].

Independently, and around the same time, these groups* also occurred in the work of V. M. Sidelnikov, in connection with the construction of spherical t-designs [17], [28], [29], [30], [31].

The complete account of our work [20], [21] describes the invariants of these Clifford groups and their connections with binary self-dual codes. Much of this work had been

*Although at that time they were not recognized as the Clifford groups.

anticipated by Runge [24], [25], [26], [27]. In our two papers we clarify the connections with spherical t-designs and Sidelnikov's work, and also generalize these results to the complex Clifford groups and doubly-even binary self-dual codes. Again the main result was first given by Runge.

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 [23]. In [21] we 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" and its ring of invariants.

Some of the results in [20], [21] can be regarded as providing a general setting for Gleason's theorems [16], [19], [23] about the weight enumerator of a binary self-dual code, a doubly-even binary self-dual code and a self-dual code over $\mathbb{F}_p$. They are also a kind of discrete analogue of a long series of theorems going back to Eichler (see for example [4], [25], [26], [27]), 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. A simple construction for the Barnes-Wall lattices

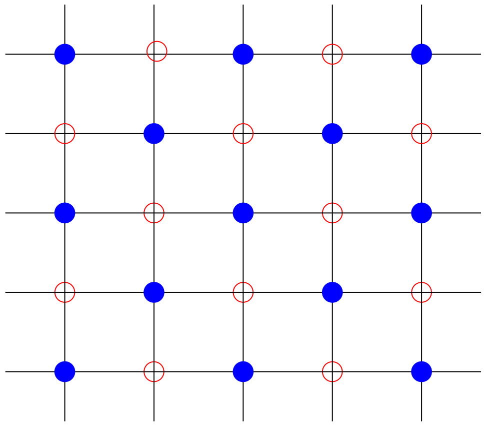
There is a pair of Barnes-Wall lattices L_m and L'_m in each dimension 2^m, $m \geq 0$. The two lattices are geometrically similar[†] and L_m is a sublattice of index 2^k, $k = 2^{m-1}$, in L'_m. In dimension 2 these lattices are shown in Fig. 1, where L_1 consists of the points marked with solid circles and L'_1 consists of the points marked with either solid or hollow circles. Both are geometrically similar to the square lattice $\mathbb{Z}^2$.

Suppose we multiply the points of L'_1 by $\sqrt{2}$. Then the eight minimal vectors of L_1 and $\sqrt{2}\, L'_1$ now have the same length and form the familiar configuration of points used in the 8-PSK signaling system (Fig. 2).

We now define the generalized or "balanced" Barnes-Wall lattice M_1 to be the set of all $\mathbb{Z}[\sqrt{2}]$-integer combinations of the eight vectors in Figure 2. That is, we take integer combinations of these vectors where "integer" now means a number of the form $a + b\sqrt{2}$, $a, b \in \mathbb{Z}$. In more formal language, M_1 is a $\mathbb{Z}[\sqrt{2}]$-lattice (or $\mathbb{Z}[\sqrt{2}]$-module). Note that we

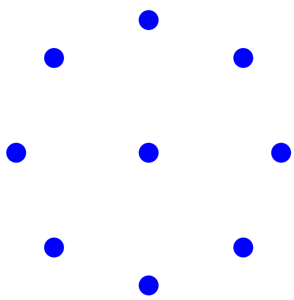
[†] In other words they differ only by a rotation and change of scale.

Figure 1: The two Barnes-Wall lattices L_1 (solid circles) and L_1' (solid or hollow circles) in two dimensions.



[F1]

Figure 2: The eight minimal vectors of L_1 and $\sqrt{2}\ L_1'$. The $\mathbb{Z}[\sqrt{2}]$ span of these points is the "balanced" Barnes-Wall lattice M_1.



[F2]

can recover L_1 from M_1 by taking just those vectors in M_1 whose components are integers.

In general we define the rational part of a $\mathbb{Z}[\sqrt{2}]$-lattice Λ to consist of the vectors which have rational components, and the irrational part to consist of the vectors whose components are rational multiples of $\sqrt{2}$. We can now state the construction.

Theorem 2.1. [th1] *Define the balanced Barnes-Wall lattice M_m to be the m-fold tensor product $M_1^{\otimes m}$. Then the rational part of M_m is the Barnes-Wall lattice L_m, and the purely irrational part is $\sqrt{2}\ L_m'$.*

For the proof see [20].

To be quite explicit, note that we need only two of the vectors in Fig. 2, and we can take

$$G_1 = \begin{pmatrix} \sqrt{2} & 0 \\ 1 & 1 \end{pmatrix}$$

as a generator matrix for M_1. Then the m-fold tensor power of this matrix,

$$G_m = G_1^{\otimes m} = G_1 \otimes G_1 \otimes \cdots \otimes G_1$$

is a generator matrix for M_m.

For example, $G_2 = G_1 \otimes G_1$ is

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ \sqrt{2} & \sqrt{2} & 0 & 0 \\ \sqrt{2} & 0 & \sqrt{2} & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} .$$

The rational part, L_2, is generated by

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \text{ or equivalently } \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} .$$

This lattice is geometrically similar to D_4 ([13], Chap. 4, Eq. (90)). The purely irrational part, $\sqrt{2}L_2'$, is generated by

$$\begin{bmatrix} 2\sqrt{2} & 0 & 0 & 0 \\ \sqrt{2} & \sqrt{2} & 0 & 0 \\ \sqrt{2} & 0 & \sqrt{2} & 0 \\ \sqrt{2} & \sqrt{2} & \sqrt{2} & \sqrt{2} \end{bmatrix}, \text{ or equivalently } \sqrt{2}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix},$$

which another version of D_4 ([13], Chap. 4, Eq. (86)).

We may avoid the use of coordinates and work directly with Gram matrices or quadratic forms, provided we select an appropriate element ϕ of the Galois group. Let u_1 and u_2 be the generating vectors corresponding to the rows of the matrix G_1, and let ϕ negate u_1 and fix u_2.

Then M_1 is the $\mathbb{Z}[\sqrt{2}]$-lattice with Gram matrix

$$A_1 = G_1 G_1^{tr} = \begin{pmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 2 \end{pmatrix},$$

L_1 is the sublattice of M_1 fixed by ϕ and $\sqrt{2}\ L_1'$ is the sublattice negated by ϕ.

Furthermore, ϕ has a rational extension to $M_m = M_1^{\otimes m}$, and L_m is the sublattice of M_n fixed by ϕ and $\sqrt{2}\ L_m'$ is the sublattice negated by ϕ.

3. The Clifford groups and their invariants

The Clifford groups $\mathcal{C}_m$ mentioned at the beginning of the paper now have a very simple definition: for all $m \geq 1$, $\mathcal{C}_m$ is $Aut(M_n)$, i.e. the subgroup of $O(2^m, \mathbb{R})$ that preserves M_m.

For the proof that this definition is equivalent to the usual one given in [8], [9], [11], see Proposition 5.3 of [20].

An invariant polynomial of $\mathcal{C}_m$ is a polynomial in 2^m variables with real coefficients that is fixed by every element of the group [3]. The ring of invariant polynomials plays an important role in constructing spherical t-designs from the group (see for example [13], Chap. 3, Section 4.2). The Molien series of the group is a generating function for the numbers of linearly independent homogeneous invariants of each degree [3], [19], [23].

In [8] it was asked "is it possible to say something about the Molien series [of the groups $\mathcal{C}_m$], such as the minimal degree of an invariant?" Such questions also arise in the work of Sidelnikov [28], [29], [30], [31]. The answers are given by the following theorem of Runge [24], [25], [26], [27].

Theorem 3.1. [th2] (*Runge; [20]*). *Fix integers k and $m \geq 1$. The space of homogeneous invariants of $\mathcal{C}_m$ of degree $2k$ is spanned by the complete weight enumerators of the codes $C \otimes GF(2^m)$, where C ranges over all binary self-dual codes of length $2k$; this is a basis if $m \geq k-1$.*

We rediscovered this result in the summer of 1999. Our proof is somewhat simpler than Runge's as it avoids the use of Siegel modular forms [20].

Corollary 3.2. [th3] *Let $\Phi_m(t)$ be the Molien series of $\mathcal{C}_m$. 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 binary self-dual codes of length $2k$.

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

Corollary 3.3. [th4] *The initial terms of the Molien series of $\mathcal{C}_m$ 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 [29], [30] 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 3.4. `[th5]` *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*.*

There is a unique harmonic invariant of degree 8, which can be taken to be the complete weight enumerator of $H_8 \otimes GF(2^m)$, where H_8 is the $[8, 4, 4]$ binary Hamming code, minus a suitable multiple of the fourth power of the quadratic form.

From Corollary 3.4 we can easily show that appropriate orbits under $\mathcal{C}_m$ form spherical 7-designs, 11-designs, etc.

We conclude by mentioning one last result (Corollary 5.7 of [20]).

Theorem 3.5. `[th6]` *Let* C *be any binary self-dual code that is not generated by vectors of weight 2, and form the complete weight enumerator of* $C \otimes GF(2^m)$*. Then the subgroup of* $O(2^m, \mathbb{R})$ *that fixes this weight enumerator is precisely* $\mathcal{C}_m$*.*

As already mentioned, there are analogues of all these results for the complex versions of the Clifford group. Now "self-dual code" is replaced by "doubly-even self-dual code".

The case $m = 1$ of Theorem 3.5 and its complex analogue imply the following.

Let C be a binary self-dual code of length N and $W(x, y)$ its Hamming weight enumerator. Let G be the subgroup of $O(2, \mathbb{R})$ that fixes $W(x, y)$. Provided C is not generated by vectors of weight 2, $G \cong \mathcal{C}_1$, of order 16. If C is doubly-even, the subgroup of the unitary group $U(2, \mathbb{C})$ that fixes $W(x, y)$ is (apart from its center, which of course may contain complex N-th roots of unity) the familiar group of order 192 arising in Gleason's theorem.

It was of course known that $W(x, y)$ is fixed by these two groups, of order 16 and 192. But we were not aware before this of any proof that the group of $W(x, y)$ could never be bigger.

References

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

[2] 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.

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

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] G. D. Forney, Jr., Coset codes - part I: introduction and geometrical classification, *IEEE Trans. Inform. Theory* **34** (1988), 1123–1151.

[15] G. D. Forney, Jr., Coset codes - part II: binary lattices and related codes, *IEEE Trans. Inform. Theory* **34** (1988), 1152–1186.

[16] 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.

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

[18] 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.

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

[20] G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, preprint, 1999.

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

[22] I. R. Porteous, *Clifford Algebras and the Classical Groups*, Cambridge, 1995.

[23] 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.

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

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

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

[27] B. Runge, Codes and Siegel modular forms, *Discrete Math.* **148** (1995), 175–205.

[28] 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 .

[29] 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.

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

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

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