Midwest cousins of Barnes-Wall lattices

filename: **mwfirstcousinsrevision6sep09**;
version 6 September, 2009;
this replaces previous versions of "Midwest cousins of Barnes-Wall lattices"

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109 USA

Abstract

Given a rational lattice and suitable set of linear transformations, we construct a cousin lattice. Sufficient conditions are given for integrality, evenness and unimodularity. When the input is a Barnes-Wall lattice, we get multi-parameter series of cousins. There is a subseries consisting of unimodular lattices which have ranks $2^{d-1} \pm 2^{d-k-1}$, for odd integers $d \geq 3$ and integers $k = 1, 2, \cdots, \frac{d-1}{2}$. Their minimum norms are moderately high: $2^{\lfloor \frac{d}{2} \rfloor - 1}$.

Keywords: even integral lattice, minimum norm, Barnes-Wall, finite group, 2/4 generation, commutator density

Contents

1 Introduction

In this article, lattice means a finite rank free abelian group with rational-valued positive definite symmetric bilinear form.

We develop a general lattice construction method which is inspired by finite group theory. We call it a *midwest procedure* because many significant

developments in finite group theory took place in the American midwest during the late twentieth century, especially in Illinois, Indiana, Michigan, Ohio and Wisconsin.

The idea is to start with a lattice L and take a finite subgroup F of $O(\mathbb{Q} \otimes L)$. In the rational span of F in $End(\mathbb{Q} \otimes L)$, we take an element h. We define a new lattice, L', in some way using L and h, for example $L \cap Ker(h)$, $L^* \cap Ker(h)$, Lh, ..., or sums of such things. After finitely many repetitions of this procedure, the sequence $L, L', \ldots$ arrives at a new lattice, which is called a *midwest cousin* of L. In this article, we restrict this procedure to the midwest cousins defined in (3.1).

In (3.3), we specialize further to the dimension 2^d Barnes-Wall lattices BW_{2^d} and the Bolt-Room-Wall groups $BRW^+(2^d)$, of shape $2^{1+2d}_+\Omega^+(2d, 2)$, which are the full isometry groups of BW_{2^d} if $d \neq 3$. The sophisticated groups $BRW^+(2^d)$ help us manage the linear algebra and combinatorics. We create multi-parameter series of cousin lattices, called *the first cousins of the Barnes-Wall lattices*. The dimension of a first cousin is $2^{d-1} \pm 2^{d-k-1}$, for some $k \in \{1, 2, \cdots, \lfloor \frac{d}{2} \rfloor\}$. The auxiliary finite isometry groups F_i are cyclic groups of orders 2 and 4. When d is odd and $d - 2k \geq 3$, the minimum norms are $2^{\lfloor \frac{d}{2} \rfloor - 1}$ and the lattices are even and unimodular. We include a partial analysis of minimal vectors.

We are grateful to the University of Michigan, National Cheng Kung University, Zhejiang University, and the U. S. National Science Foundation for financial support (NSF DMS-0600854). We thank Harold N. Ward for useful discussions and the referee for many helpful comments.

1.1 Conventions and List of Notations

Group elements and endomorphisms usually act on the right. Table 1 summarizes notations. An appendix to this article summarizes background. For more details, see [10, 13, 12]. The upcoming book [14] may be helpful.

2 Involutions on Barnes-Wall lattices

We use the notations and results of [13] and [12], which are recommended for background.

Table 1: List of Notations, Part 1

Notation	Summary	Comments
$BRW^+(2^d)$	the Bolt-Room-Wall group, $2_+^{1+2d}\Omega^+(2d,2)$	
BW_{2^d}	the Barnes-Wall lattice of rank 2^d	
BW-level		(9.4)
commutator density		(9.15)
$Mod(D,-)$	category of modules for $D \cong Dih_8$ where central involution acts as -1	
core	$S_1 \cap \cdots \cap S_r$ as in cubi sum (below)	(9.10)
cubi sum	$S_1 + \cdots + S_r$, S_i affine codimension 2 subspaces in $\mathbb{F}_2^d$ so that $codim(S_1 \cap \cdots \cap S_r) = 2r$	(9.10) cubi theory [12]
defect	invariant of an involution in $BRW^+(2^d)$	(2.2)(2.3),(2.8)
ε_S	$v_i \mapsto v_i, -v_i$, as $i \notin S, i \in S$	
fourvolution	an isometry of order 4 whose square is -1	
frame, lower frame		(9.14)
G, G_{2^d}	$BRW^+(2^d)$, a subgroup of $O(BW_{2^d})$	(9.11)
Jordan number, JNo		(2.4)
k^{th} layer	$L(k)/L(k-1)$	
level	least ℓ so that $2^\ell x$ has integer coordinates	(9.4)
level sublattice		(4.1)
$L^\varepsilon(t)$	eigenlattice for involution t	
k^{th} level, $L(k)$	the set of lattice elements of level at most k	
long codeword	$RM(2,d)$ codeword of weight more than 2^{d-1}	
$L^+(t), L^-(t)$	eigenlattices for involution t	
lower element	element of G_{2^d} contained in R_{2^d}	
lower frame		(9.14)
$MC(L,t,f,\varepsilon)$	a cousin lattice	(3.1)
$MC(BW_{2^d},t,f,\varepsilon)$	a cousin lattice	(3.3)
$MC_1(d,k,\varepsilon)$	a cousin lattice	(3.3)
$\mu(L)$	the minimum norm in the lattice L	
$O(L)$	isometry group of quadratic space L	

Table 2: List of Notations, Part 2

$O_p(X)$	the largest normal p-subgroup of the group X (p prime)	
$O_{p'}(X)$	the largest normal subgroup of the group X of order prime to p	
$\mathcal{P}(X)$	the power set of the set X	(9.4), (9.6)
quotient code	quotient space of a code which has code structure	(9.8)
R, R_{2^d}	$O_2(G_{2^d})$	(9.11)
$RM(k,d)$	the Reed-Muller code of length 2^d	(9.1)
RM-level		(9.4)
sBW, $ssBW$	scaled, suitably scaled BW lattice	[13]
short codeword, short involution	codeword in $\mathbb{F}_2^n$ of weight $< \frac{1}{2}n$	(9.9)
split, nonsplit	involution of G_{2^d} which centralizes, does not centralize, a lower elementary abelian 2^{d+1}	(2.1)
standard frame, basis		(9.14)
standard generators	certain set of $2^{-m}v_A$ in BW_{2^d}	(9.12)
$t = \varepsilon_A$	a diagonal involution in $BRW^+(2^d)$	
$\tau_\omega, \omega \in \Omega$	translation by ω on Ω or $V := \mathbb{Q} \otimes BW_{2^d}$	(9.11)
$\tau(core(Z))$	the group $\{\tau_c \mid c \in core(Z)\}$	
$Tel(L,E), E$ abelian	total eigenlattice on lattice L, the sum of eigenlattices	
$Tel(L,t), t$ involution	total eigenlattice on lattice L, $L^+(t) \perp L^-(t)$	(2.5), (3.2)
$top(x)$	part of vector x representing the highest power of 2 in denominator	(4.3)
top closure	$top(x)$ is in lattice if x is in lattice	(4.3), (4.4)
upper element	element of G_{2^d} not contained in R_{2^d}	
$V^\varepsilon(t), V$	$\mathbb{Q} \otimes L^\varepsilon(t)$, $V := \mathbb{Q} \otimes L$	(3.1)
$v_i, v_X \in \mathbb{R}^\Omega$	$(v_i, v_j) = 2^{\lfloor \frac{d}{2} \rfloor}\delta_{ij}$; $v_X := \sum_{i \in X} v_i$	(9.12)
$Z, Z + \Omega \in RM(2,d)$	weight $2^{d-1} \pm 2^{d-k-1}$ codewords	(2.3), (9.10)
2/4, 3/4 generation	a property of some objects in $Mod(D, -)$	(9.16)
Ω, Ω_d	index set for orthogonal basis of $\mathbb{R}^{2^d}$	(9.11)

Definition 2.1. We recall that an involution in $BRW^+(2^d)$ has trace 0 if and only if it is conjugate to its negative in $BRW^+(2^d)$ (equivalent, conjugate to its negative by an element of R_{2^d} [8, 13, 12]).

An involution in $BRW^+(2^d)$ is *split* if it centralizes a maximal elementary abelian subgroup of R_{2^d} and is *nonsplit* otherwise.

For a summary of properties and classification of such involutions, see [12] Appendix: About BRW groups. We have changed some terminology since that article. We mention one often-used result.

Theorem 2.2. *(i) If $g \in BRW^+(2^d)$, then the trace of g on the natural 2^d-dimensional module is 0 or is $\pm 2^e$ if g has nonzero trace, where $2e$ is the dimension of the fixed point subspace for the conjugation action of g on $R_{2^d}/Z(R_{2^d})$.*

(ii) Suppose that $g \in BRW^+(2^d)$ is an involution. The defect k of g satisfies $e+k=d$. The multiplicities of eigenvalues ± 1 are (up to transposition) $2^{d-1}+2^{d-k-1}, 2^{d-1}-2^{d-k-1}$, respectively.

Remark 2.3. Let $A \in RM(2,d)$ be a short codeword of defect k (9.10). Throughout this article, we shall work with involutions of the form $t := \varepsilon_A$. Its trace is 2^{d-k}. Let $A = A_1 + \cdots + A_k$ be a cubi sum (9.10). The affine subspace $core(A) = core(Z) = \cap_i A_i$ is $(d-2k)$-dimensional. For $c \in \Omega$, the corresponding translation map is τ_c. If $c \in core(A)$, we call τ_c a *core translation*, so when $core(A)$ contains the origin, we get a group of translations. Let τ_c be a nonidentity core translation. Observe that if we take any hyperplane H which contains no translate of c, then $f := \varepsilon_H \tau_c$ is a fourvolution which commutes with t.

2.1 Involutions on Barnes-Wall lattices mod 2: JNo

We begin by studying the Jordan canonical form of involutions on the Barnes-Wall lattice modulo 2. We derive applications to discriminant groups and lattice constructions.

Definition 2.4. The *Jordan number* of an involution acting on a finite rank abelian group A is the number of degree 2 Jordan blocks in its canonical form on $A/2A$. We write $JNo(t)$ or $JNo(t,A)$ for the Jordan number of t.

Lemma 2.5. *On BW_{2^d}, the Jordan number for -1 is 0 and the Jordan number is 2^{d-2} for a lower noncentral involution.*

Proof. The first statement is obvious. The second follows since $|BW_{2^d} : Tel(t)| = 2^{2^{d-2}}$ for lower involutions t. See [13]. □

Notation 2.6. In this section, the notations of (2.4) will stand for lattices (which often are sBWs) and the involutions will be isometries of them. Let L be a sBW lattice of rank 2^d. If $t \in O(L)$ is an involution, as before, we let $JNo(t)$ be its Jordan number (2.4). Because of (2.5), we assume that the defect k is positive, i.e., that the involution is upper. If $2k < d$, there exists a lower dihedral group in $C_{G_{2^d}}(t)$.

Theorem (2.15) is the main goal of this section.

Lemma 2.7. *If t is a nonsplit involution, it has full Jordan number, i.e., $JNo(t) = 2^{d-1}$.*

Proof. A nonsplit involution is upper. By [12], there exists a lower dihedral group D so that t normalizes D and effects an outer automorphism on D, say by transposing a set of generators u, v. Using 2/4 generation of L with respect to D, we get $L = L^+(u) \oplus L^+(v)$ for a generating pair of involutions u, v so that $u^t = v$. Then obviously L is a free $\mathbb{Z}\langle t\rangle$-module, so we are done. □

Lemma 2.8. *If t centralizes a lower dihedral group, $JNo(t) = JNo(t') + JNo(t'')$, where t', t'' are defect k involutions on sBW lattices of rank 2^{d-1}.*

Proof. We may choose such a lower dihedral group D to satisfy $D \cap [R, t] = Z(R)$. Use the 2/4 property to get that t preserves each direct summand in $L = L^+(u) \oplus L^+(v)$ for a generating pair of involutions u, v of D (the summands are sBW). In the notation of [13], there exists a group $Q \cong 2_+^{1+2(d-1)}$ in $BRW^+(2^d)$ which acts trivially on $L^-(u)$ and as a lower group on $L^+(u)$. Since the action of t on R has defect k, the action of t on Q has defect k. We may therefore apply induction to the restriction of t to the summand $L^+(u)$. A similar argument applies to $L^+(v)$. □

Lemma 2.9. *When $(d, k) = (2, 1)$ and t is an upper involution, $JNo(t) = 1$ when t has nonzero trace and $JNo(t) = 2$ when t has trace zero.*

Proof. We refer to [13] for a discussion of involutions in $BRW^+(2^2) \cong W_{F_4}$.

Suppose that the involution has nonzero trace. Since its trace is ± 2, we may assume that it is 2, whence t is a reflection. Then the statement is obvious since reflections induce transvections on the lattice mod 2.

For $d = 2$, if an involution is upper and nonsplit, we may quote (2.7). For $d = 2$, if an involution is upper and split, it has nonzero trace and we may quote the previous paragraph. $\square$

Lemma 2.10. *If t has nonzero trace, $JNo(t) \leq 2^{d-1} - 2^{d-k-1}$.*

Proof. We may assume that $tr(t) > 0$. Let h be the dimension of fixed points for t on $L/2L$. Then $h + JNo(t) = 2^d$. Since the 1-eigenlattice for t has rank $2^{d-1} + 2^{d-k-1}$ and is a direct summand of L, we have $h \geq 2^{d-1} + 2^{d-k-1}$. $\square$

Lemma 2.11. *Suppose that the upper involution t lies in a subgroup S of G of order $2n$, n odd, and that every nonidentity element of S of order dividing n has the same fixed point subspace, of dimension $2e$, on R/R'. Assume further that t inverts a nonidentity odd order element of S. Then $JNo(t) \geq 2^{d-1} - \frac{1}{2}(\frac{2^d - 2^e}{n} + 2^e)$.*

Proof. Such a group S has a normal subgroup of order n. Call it C. Then every nonidentity element of C has trace $\pm 2^e$ on L (2.2). It follows that the eigenlattice M of C-fixed points has rank $\frac{1}{n}(2^d + (n-1)2^e) = \frac{1}{n}(2^d - 2^e + n2^e)$. On the annihilator $N := L \cap M^{\perp}$, C acts faithfully on every constituent, and since t inverts a nonidentity element of C, $N/2N$ is a free $\langle t \rangle$-module, whence $JNo(t) \geq \frac{1}{2} rank(N) = \frac{1}{2}(2^d - rank(M))$. $\square$

Next, we deal with the situation when t does not centralize a lower dihedral group.

Lemma 2.12. We use the hypotheses and notation of (2.11).

(i) Suppose that d is even, $n = 2^{\frac{d}{2}} + 1$ and $e = 0$. Then $JNo(t) \geq 2^{d-1} - 2^{\frac{d}{2}-1}$.

(ii) Suppose that d is odd, $n = 2^{\frac{d-1}{2}} + 1$ and $e = 1$. Then $JNo(t) \geq 2^{d-1} - 2^{\frac{d-1}{2}}$.

Proof. Straightforward with (2.11). $\square$

Lemma 2.13. *Suppose that $m \geq 1$, $2r \geq 4m \geq 4$ and that u is an involution in $\Omega^+(2r, 2)$ with commutator submodule of dimension $2m$ on its natural module $W := \mathbb{F}_2^{4m}$. Assume that $W(u-1)$ is a totally singular subspace. Let $n = 2^{2m} - 1$.*

Then u is in a group P of order $2n$, where P contains a Singer cycle C in a natural $GL(2m, 2)$-subgroup of $\Omega^+(2r, 2)$ (so C is a normal subgroup of P). Also P has the property that the nonidentity elements of C have the same fixed point subspace on $\mathbb{F}_2^{2r}$.

Proof. Recall properties of the normalizer of a Singer cycle in classical groups, [15]. Without loss, we may assume that $2r = 4m$.

Suppose that we are given a pair of maximal totally singular subspaces, W_1, W_2 in W such that $W = W_1 \oplus W_2$. Let H be the common stabilizer of W_1 and W_2. So, $H \cong GL(2m, 2)$. Let P be the subgroup of the normalizer of a Singer cycle in H corresponding to the Singer cycle and the group of field automorphisms of order 2. It has order $2n$ and its involutions invert nonidentity elements of C so have Jordan number $2m$ on W. If u is conjugate to such an involution, we are done. There are two conjugacy classes of involutions in $\Omega^+(2m, 2)$ with maximal Jordan number $2m$, which form a single class under the action of $O^+(4m, 2)$ [12]. By conjugacy in $O^+(4m, 2)$, u lies in such a group, P. □

Lemma 2.14. *Suppose that $d \geq 2$ and that $t \in G_{2^d}$ has defect $\frac{d}{2}$ or $\frac{d-1}{2}$. Let $R := R_{2^d}$. Suppose that $[R, t]$ is elementary abelian. Then t is in a dihedral group as in (2.11).*

Proof. Let bars indicate images in G_{2^d}/R_{2^d}. Lemma (2.13) implies that $\bar{t}$ is in an appropriate Singer normalizer, E. Let u be a conjugate of t in G so that $\bar{t}\bar{u}$ generates $O_{2'}(E)$. There exists $c \in \langle tu \rangle$ which generates a cyclic group of odd order which maps isomorphically onto $O_{2'}(E)$. Then $\langle t, c \rangle$ satisfies the conclusion. □

Now we prove the main result (2.15).

Theorem 2.15. *Let $d \geq 2$ and let t be an upper involution in $BRW^+(2^d)$ of defect $k \geq 1$. Then $JNo(t) = 2^{d-1} - 2^{d-k-1}$ if t is split, and is 2^{d-1} if t is nonsplit.*

Proof. We have $d \geq 2$. Suppose that $[R, t]$ is not elementary abelian. There exists a lower involution w so that $[w, t]$ has order 4. Then on the lower dihedral group $D := \langle w, [w, t] \rangle$, t induces an outer automorphism. Now use (2.7).

We may assume that t is split. So, $[R, t]$ is elementary abelian. If the involution t centralizes a lower dihedral group, the 2/4 generation property (9.16) and induction (2.8) implies the result. Note that the initial cases for induction are discussed in [12].

Assume that the involution t does not centralize a lower dihedral group. Then R_{2^d}/R'_{2^d} is a free $\mathbb{F}_2[\langle t \rangle]$-module, d is even and $d = 2k$. We apply (2.14), (2.13) with $r = m = k$, then (2.12) and (2.10). □

2.2 Applications to discriminant groups

Knowing JNo is quite useful. One can get sharp statements about the discriminant group, which might be hard to calculate directly from a definition of the lattice, e.g. by a spanning set.

Lemma 2.16. *Let the involution u act on the additive abelian group A. Then $2A^- \leq [A,u] \leq A^-$.*

Proof. Clearly, u negates all $a(u-1)$, so $[A,u] \leq A^-$. Also, if $a \in A^-$, $2a = a-(-a) = a(1-u) \in [A,u]$. $\square$

Corollary 2.17. *Suppose that $L \cong BW_{2^d}$ and $t \in G_{2^d}$ satisfies $tr(t) > 0$. Then $L^-(t) = [L,t]$.*

Proof. Since t is an involution, $L^-(t) \geq [L,t]$ (2.16). Since $JNo(t) = rank(L^-(t))$ (2.15), the image in $L/2L$ of $[L,t]$ has dimension equal to the rank of $[L,t]$. Therefore, $L^-(t)+2L = [L,t]+2L$. Since $[L,t] \leq L^-(t) \leq [L,t]+2L$, the Dedekind law implies that $L^-(t) \leq [L,t]+(L^-(t) \cap 2L)$. Since $L^-(t)$ is a direct summand of L, $L^-(t) \cap 2L = 2L^-(t)$. The latter is contained in $[L,t]$, by (2.16). We conclude that $L^-(t) = [L,t]$. $\square$

Corollary 2.18. *Let $d \geq 2$. Let t be a split involution of defect $k \geq 1$, and $\varepsilon = \pm$. Suppose $tr(t) > 0$.*

(i) The image of L in the discriminant group of $L^\varepsilon(t)$ is 2-elementary abelian of rank $2^{d-1} - 2^{d-k-1}$.

(ii) $L^-(t) \leq 2P^-(t)$.

(iii) If d is odd, $\mathcal{D}(L^-(t)) \cong \mathcal{D}(L^+(t))$ is 2-elementary abelian of rank $2^{d-1} - 2^{d-k-1}$. In particular, $L^-(t) = 2L^-(t)^* = 2P^-(L)$.

Proof. (i) The kernel of the natural map $\pi_\varepsilon : L \to \mathcal{D}(L^\varepsilon(t))$ is $L^+(t) \perp L^-(t)$. The cokernel is elementary abelian of rank $JNo(t)$.

(ii) Use (i) and rank considerations.

(iii) Since d is odd, unimodularity of L implies that each π_ε is onto. $\square$

3 Midwest cousins

We introduce the first midwest operator here.

Definition 3.1. The *midwest cousin (MC) lattices* are defined as follows. Let L be an integral lattice. Let $t, f \in O(L)$ so that t, f commute, t is an involution and f is a fourvolution. Let $\varepsilon = \pm$ and let P^ε be the orthogonal projection to $V^\varepsilon(t)$. Set $MC(L, t, f, \varepsilon) := L^\varepsilon(t) + P^\varepsilon(L)(f-1) = L^\varepsilon(t) + P^\varepsilon(L(f-1))$ (see (9.18)(9.19)(9.20) about alternate notation $L[p]$).

Lemma 3.2. *Let $\varepsilon = \pm$.*

(i) The midwest cousin $MC(L, t, f, \varepsilon)$ is an integral lattice.

(ii) If $L^\varepsilon(t)$ is doubly even, i.e., all norms are multiples of 4, then $MC(L, t, f, \varepsilon)$ is an even lattice.

Proof. (i) We verify that $(x, y) \in \mathbb{Z}$, for $x, y \in MC(L, t, f, \varepsilon)$. If x or y is in $L^\varepsilon(t) \leq L$, this is clear. Now suppose that $x = x'(f-1), y = y'(f-1)$ for $x', y' \in P^\varepsilon(L)$. Then $(x, y) = (x'(f-1), y'(f-1)) = 2(x', y') = (x', 2y') \in (P^\varepsilon(L), L^\varepsilon(t)) \leq (L, L^\varepsilon(t)) \leq (L, L) \leq \mathbb{Z}$.

(ii) We take $x \in L, y := P^\varepsilon(x)$. Then $2y = P^\varepsilon(2x) \in P^\varepsilon(Tel(L, t)) = L^\varepsilon(t)$ so that $2y \in L^\varepsilon(t)$. We have $(2y, 2y) \in 4\mathbb{Z}$ since by hypothesis, $L^\varepsilon(t)$ is doubly even. Therefore, $(y, y) \in \mathbb{Z}$ and so $y(f-1)$ has even norm. Since $L^\varepsilon(t)$ is even, and $(P^\varepsilon(L), L^\varepsilon(t)) \leq \mathbb{Z}$, it follows that $MC(L, t, f, \varepsilon)$ is even. $\square$

Definition 3.3. The *midwest first cousins of the Barnes-Wall lattices* are defined as follows. They are the MC lattices with input lattice BW_{2^d} and a pair t, f as in (3.1) where t is positive trace defect k involution and $f \in C_R(t)$ is a lower fourvolution (2.1). When $k < \frac{d}{2}$, such pairs are unique up to conjugacy in $BRW^+(2^d)$. In this case, we use the briefer notation $MC_1(d, k, \varepsilon)$ for $MC(BW_{2^d}, t, f, \varepsilon)$. When $k = \frac{d}{2}$, there are several conjugacy classes of pairs (t, f). One would need additional notation to distinguish these classes [13].

Remark 3.4. Let $L := BW_{2^d}$. Suppose that we have two pairs (t, f) and (t, f'), where both f, f' are lower fourvolutions which commute with t, then the resulting first cousin lattices are the same. The reasons are that $L(f-1)^p = L(f'-1)^p$, for all p (because any lower fourvolution is commutator dense for the action of R on L [13]) and the projection maps P^ε commute with f and f'. In certain commutator calculations, it may be convenient to replace $f-1$ by some $\pm f' \pm 1$.

3.1 Integrality properties of the first cousin lattices

We now specialize to the case of Barnes-Wall lattices.

Proposition 3.5. *Let $d \geq 2$, $L := BW_{2^d}$. We assume that the involution t has defect $k \geq 1$ and that its trace is positive. Then*

(i) $rank(MC_1(d,k,\pm)) = 2^{d-1} \pm 2^{d-k-1}$.

(ii) Let $\varepsilon = \pm$. If d is odd and $d \geq 3$, $MC_1(d,k,\varepsilon)$ is unimodular.

(iii) For $\varepsilon = \pm$, $k \leq \frac{d}{2} - 1$, then $P^\varepsilon(t)(f-1)$ is even integral and $L^\varepsilon(t)$ is doubly even (and so $MC_1(d,k,\varepsilon)$ is even).

(iv) $\mu(MC_1(d,k,-)) = \frac{1}{2}\mu(BW_{2^d})$.

(v) $\mu(MC_1(d,k,+)) \leq 2^{\lfloor \frac{d}{2} \rfloor}$.

(vi) If $d = 2k$ or $d = 2k+1$, $MC_1(d,k,\varepsilon)$ is an odd integral lattice.

Proof. For (i), see (2.2).

For (ii), we have that $\frac{1}{2}L^-(t) = P(L)$, which is $L^-(t)^*$ since L is unimodular (2.18)(iii). Consequently, $\mathcal{D}(L^-(t)) \cong 2^{rank(L^-(t))} = 2^{2^{d-1}-2^{d-k-1}}$. The lattice $MC_1(d,k,-)$ is between $L^-(t)$ and its dual and corresponds to the image of $f-1$, where f is a lower fourvolution in $C_R(t)$. In fact, $MC_1(d,k,-) = P^-(L)(f-1)$. Since $(f-1)^2 = -2f$ and $|\frac{1}{2}L^-(t) : MC_1(d,k,-)| = |MC_1(d,k,-) : L^-(t)|$, unimodularity follows.

The argument for $\varepsilon = +$ is similar since $\mathcal{D}(L^+(t)) \cong \mathcal{D}(L^-(t))$ as modules for $f-1$.

(iii) By (3.2), $P^\varepsilon(L)(f-1)$ is integral. We show that it is even under our restrictions on k.

Since $k < \frac{d}{2}$, there exists a lower dihedral group $D \leq C_R(t)$ so that $D \cap [R,t] = Z(R)$. If u, v form a generating set of involutions, $L = L^+(u) + L^+(v)$ by 2/4-generation (9.16). The action of t on each summand has nonzero trace and defect k.

Suppose that d is even. Then $d-1$ is odd and each summand is t-invariant and is isometric to $\sqrt{2}BW_{2^{d-1}}$. By a previous paragraph, the norms of vectors in $P^\varepsilon(L^+(u))$ and $P^\varepsilon(L^+(v))$ are integral. Therefore the norms of vectors in $P^\varepsilon(L^+(u))(f-1)$ and $P^\varepsilon(L^+(v))(f-1)$ are even integral. This suffices to prove (iii) since we have a spanning set of even vectors in an integral lattice.

For (iv), note that $L^-(t)$ contains a minimal vector of L and that $MC_1(d,k,-)$ is the -1 twist (9.18) of $L^-(t)$.

(v) This is obvious since $L^+(t)$ contains a minimal vector of L.

(vi) Integrality was proved in (3.2)(i).

If $d = 2k$, the vector $v := 2^{-k}v_Z$ is in $P^\varepsilon(L)$. Its norm is $2^{-2k}2^k(2^{d-1} + 2^{d-k-1}) = 2^{d-k-1} + \varepsilon\frac{1}{2}$. The vector $v(f-1)$ is in $MC_1(d,k,+)$ and has odd integer norm.

If $d = 2k+1$, let H be an affine hyperplane which is transverse to $core(Z)$, which is 1-dimensional. The vector $v := 2^{-k}v_{H\cap Z}$ is in $P^+(L)$ and has norm $2^{-2k}2^k(2^{d-2} + 2^{d-k-2}) = 2^{d-k-2}\varepsilon\frac{1}{2}$. The vector $v(f-1)$ is in $MC_1(d,k,-)$ and has odd integer norm. To prove the result for $\varepsilon = -$, replace Z by $Z+\Omega$ in the above reasoning.

Suppose that $d = 2k$ is even. Then $2^{-k}v_\Omega \in L$ and $2^{-k}v_Z \in P^+(L)$. Its norm is $2^{-2k}2^k(2^{d-1} + \varepsilon 2^{d-k-1}) = 2^{k-1} + \frac{1}{2}$. The vector $v(f-1)$ is in $MC_1(d,k,+)$ and has odd integer norm. A similar argument works for $\varepsilon = -$. $\square$

Remark 3.6. The unimodular integral lattices $MC_1(5,2,\pm)$ are not even since their ranks are 20 and 12, which are not multiples of 8. Another proof is (3.5).

3.2 Minimum norm for $MC_1(d,k,+)$

In this section, we determine that the minimum norm for $MC(d,k,+)$ is $2^{\frac{d-1}{2}-1}$ (3.9), the same as for $MC_1(d,k,-)$(3.5). Later, we discuss the forms for low norm vectors in the first few layers (4.1) and study orthogonal decomposability.

Notation 3.7. We let t be an involution of defect k and positive trace. We take t to have the form ε_Z, where Z has weight $2^{d-1} + 2^{d-k-1}$. As before, abbreviate P^ε for the projection to $L^\varepsilon(t)$. Let $c \in core(Z), c \neq 1$ (9.10) and let H be a hyperplane of Ω which is transverse to $\{0,c\}$ (so is moved by translation by c). We take $\tau := \tau_c$, $f := \varepsilon_H\tau$ and define $\xi := f - 1$, so that $L[k] = L\xi^k$, for all k.

Notation 3.8. $\delta := \frac{d-1}{2}$.

Theorem 3.9. *We suppose that $d - 2k \geq 3$.*

(i) $\mu(MC_1(d,k,\varepsilon)) = 2^{\delta-1}$.

(ii) A vector $v \in MC_1(d,k,\varepsilon)$ is minimal if and only if $v\xi$ is minimal in $L^\varepsilon(t)$ (equivalently, if the support of $v\xi$ is contained in Z and $v\xi$ is a minimal vector of BW_{2^d}).

(iii) The minimal vectors of $MC_1(d,k,\varepsilon)$ are in $MC_1(d,k,\varepsilon) \setminus L^\varepsilon(t)$.

Proof. (i) Let $v \in MinVec(MC_1(d,k,\varepsilon))$. Since $v\xi \in L^+(t)$, $(v,v) \geq 2^{\delta-1}$. It suffices to prove that there exists a vector in $MC_1(d,k,\varepsilon)$ of such a norm.

We let $p \geq 1$ and let A be an affine subspace of dimension $2p$ in Ω which is a translation of a subspace of $core(Z)$ (this is possible since $d-2k \geq 3$). We also choose A to be transverse to H (this is possible since $2p < d-2k$) and to be contained in Z. Therefore, $A \cap H$ is a $(2p-1)$-dimensional space. The vector $2^{-p}v_{A\cap H}$ is in $MC_1(d,k,\varepsilon)$ and has norm $2^{\delta-1}$.

(ii) Since ξ takes $MC_1(d,k,\varepsilon)$ into $L^+(t)$ and doubles norms, this follows from (i).

(iii) This follows from (ii) since the minimum norm in L is 2^δ. $\square$

Corollary 3.10. *A minimal vector of $MC_1(d,k,\varepsilon)$ has the form $2^{-m}v_A\varepsilon_S$, where A is an affine $(2m-1)$-space, $A \subseteq Z$ and $S \in RM(2,d)$.*

Proof. Use (3.9)(ii), (9.13), (10.1). $\square$

Remark 3.11. The description (3.10) of minimal vectors in $MC_1(d,k,\varepsilon)$ is similar to (9.13) for BW_{2^d}, but is not as definitive.

4 Lattices with binary bases

To prove our main results about short vectors in the lattices $MC_1(d,k,\varepsilon)$, we begin with a general theory for lattices with a binary basis. Later, we shall specialize to the Barnes-Wall lattices.

Definition 4.1. Let L be an integral lattice and M in another lattice in $\mathbb{Q}\otimes L$ so that $L \leq \mathbb{Z}[\frac{1}{2}] \otimes M$. Let $q \geq 0$ be an integer. Define $L(q) := 2^{-q}M \cap L$. Call this the *M-level q sublattice of L*. The *level* of $0 \neq x \in L$ with respect to M is $min\{k \geq 0 \mid x \in L(k)\}$. The *$q$-th layer* of L is $L(q)/L(q-1)$. If S is a subset of $\mathbb{Q} \otimes L$ which is $\mathbb{Q}$-linearly independent and such that its $\mathbb{Z}[\frac{1}{2}]$-span contains L, we call S a *binary basis* and define *level* of $x \in L$ with respect to S to be the level of $x \in L$ with respect to $span_{\mathbb{Z}}(S)$. We do not assume that S is an orthogonal set.

Notation 4.2. If $n \in \mathbb{Z}[\frac{1}{2}]$ is nonnegative, its *2-adic expansion* is an expression $n = \sum_{i=p}^{q} a_i 2^i$, where the a_i come from $\{0,1\}$. When $n \in \mathbb{Z}[\frac{1}{2}]$ is negative, its 2-adic expansion is $\sum_{i=p}^{q} -a_i 2^i$, where $-n = \sum_{i=p}^{q} a_i 2^i$ is the 2-adic expansion of the nonnegative rational $-n$. The *level of n* is $-\infty$ if $n = 0$ and is otherwise $-min\{i \mid a_i \neq 0\}$.

Notation 4.3. Let L be a lattice of rank n with S, a linearly independent subset $v_1, \cdots, v_n$. Then $x \in L$ has a unique expression $x = \sum_i c_i v_i$, for rational numbers c_i. We assume that S is a binary basis for L (4.1). Then the c_i are in $\mathbb{Z}[\frac{1}{2}]$.

We define the *2-adic expansion of* x to be $\sum_i 2^i(\sum_j a_{i,j}v_j)$ where the $a_{i,j}$ are the 2-adic coefficients of c_j. For $x \in L$, define $level(x)$ to be the least integer m so that the coefficients of $\sum_i 2^m c_i v_i$ are integers. We define $level(0) := -\infty$.

For $x \neq 0$, we define $top(x) = top_S(x)$ to be the subsum $\sum_j a_{m,j}v_j$ of the 2-adic expansion of x (it is the part of the 2-adic expansion of x which represents the largest denominators, 2^m). Note that the definition of $top(x)$ depends on the binary basis, not on the sublattice it spans.

Remark 4.4. (i) The top of a vector may not be in the lattice. Consider the lattice L in $\mathbb{Q}^2$ which is spanned over $\mathbb{Z}$ by $(1,0), (0,1), (\frac{1}{2}, \frac{1}{4})$. For S, take $\{(1,0),(0,1)\}$. We claim that $top((\frac{1}{2}, \frac{1}{4})) = (0, \frac{1}{4})$ is not in L. If $(0, \frac{1}{4}) = a(1,0) + b(0,1) + c(\frac{1}{2}, \frac{1}{4})$, we may assume that $c \in \{0,1,2,3\}$. Clearly, c is $1(mod\ 4)$, so $c = 1$. Then the right side has first coordinate a noninteger, contradiction.

(ii) Tops do lie in BW_{2^d} for vectors of level at most 1 with respect to the the standard basis in a lower frame. For higher level, top closure may fail. For example, take $d \geq 8$ and consider a pair of 4-spaces which meet in a point.

5 Calculations in $MC_1(d, k, \varepsilon)$

Corollary 5.1. *Suppose that* $0 \neq x \in MC_1(d,k,\varepsilon)$ *has level* m. *Then* $top(x) = 2^{-m}v_B$, *where* $B \in RM(d-2m+1, d)$. *Furthermore, given* $\tau = \tau_c$ *in* $0 \neq c \in core(Z)$, *there is a decomposition* $B = S + T$, *where*

(i) $S \in RM(d-2m, d), T \in RM(d-2m+1, d)$;

(ii) $S \subseteq Z, T \subseteq Z$; *and*

(iii) T *is* τ*-invariant or* T *has form* $A \cap H$ *where* $A \in RM(d-2m+2, d)$, $A \subseteq Z$, A *is* τ*-invariant and* H *is a hyperplane transverse to* τ *(i.e., transverse to* $\{0, c\}$ *in* Ω*).*

Proof. Since $MC_1(d,k,\varepsilon) = L^\varepsilon(t) + P^\varepsilon(t)[1]$, this follows from the corresponding forms for $top(x)$, $x \in L^\varepsilon(t)$ and $x \in P^\varepsilon(t)[1]$ and the action of $f - 1$. □

5.1 Equations with codewords and commutation

We collect a few results about expressions of the form $B = S + T \in RM(d - 2m, d)$ as in (5.1).

Lemma 5.2. *Suppose that $B \in RM(i, d)$, $B = S + T \in RM(d - 2m, d)$ as in (5.1). Let r be a real number so that $|B| \leq 2^r$. If $d > r + i$, then B is τ-invariant.*

Proof. We may assume that $i \geq 1$. We have $B(\tau - 1) \in RM(i - 1, d)$, which has minimum weight $2^{d-(i-1)}$. Since $|B(\tau - 1)| \leq 2^{r+1}$, if $B(\tau - 1) \neq 0$, then $d - i + 1 \leq r + 1$, or $d \leq r + i$, contrary to hypothesis. Therefore $B(\tau - 1) = 0$, i.e., B is τ-invariant. □

Corollary 5.3. *Assume the hypotheses of (5.2). If $0 \neq |B| \leq 2$ and $i = d-2$, then B is τ-invariant.*

Proof. Take $r = 1$ in (5.2). □

Lemma 5.4. *Suppose $\tau = \tau_c$, for $c \in core(Z)$ and $c \neq 0$. Suppose $B \in RM(d - 2m + 1, d)$ is fixed by τ. Then $|B| \geq 2^{2m-1}$.*

Proof. Let bars denote images in the quotient code Ω/Γ (9.8), where $\Gamma = \{0, c\}$. Then $\bar{B}$ is a nontrivial element of $RM(d - 2m + 1, d - 1) = RM((d - 1) - (2m - 2), d - 1)$, so has weight at least 2^{2m-2}. This implies $|B| \geq 2^{2m-1}$. □

6 $MC_1(d, k, \varepsilon)$ short vectors, level at most 2

By (3.10), a minimal vector of $MC_1(d, k, \varepsilon)$ is a vector of the form $2^{-m} v_B \varepsilon_C$, for some $m \geq 0$, some $B \in RM(d - 2m + 1, d)$ and some $C \subseteq \Omega$. We can say more about short vectors in the first two levels.

Recall the concept of level (4.1). Vectors of level 0 are in BW_{2^d}, so their norms are 0 or are at least 2^δ. The set of level 0 norm 2^δ vectors is just $\{\pm v_i \mid i \in \mathbb{Z}\}$, the standard lower frame.

6.1 Short vectors at level 1

We display a set of norm $2^{\delta-1}$ vectors, which turn out to be the only level 1 vectors in $MC_1(d, k, \varepsilon)$ of norm less than 2^δ.

Lemma 6.1. *Suppose that the level of* $0 \neq x \in MC_1(d,k,\varepsilon)$ *is 1. So,* $top(x) = \frac{1}{2}v_B$. *Then:*

(i) $|B|$ *is even.*

(ii) If $(x,x) < 2^\delta$, *then* B *is a 2-set and* B *is stabilized by some* $\tau_c \neq 1$.

Proof. (i) Trivial since $B \in RM(d-2m+1,d)$ and $m=1$.

(ii) Use (5.3). □

Lemma 6.2. *The set of level 1 vectors of* $MC_1(d,k,\varepsilon)$ *of norm less than* 2^δ *consists of all* $\pm\frac{1}{2}v_i \pm \frac{1}{2}v_{i+c}$, *for* $c \neq 1, c \in core(Z)$ *and* $i \in \Omega$. *These have norm* $2^{\delta-1}$.

Proof. We get a list of candidates from (6.1)(ii). We need to see that all the vectors of indicated form are actually in $MC_1(d,k,\varepsilon)$. By (9.2), there exists $E \in RM(d-2,d)$ so that $F := E \cap Z$ is an odd set. Therefore $F(\tau-1)$ has cardinality $2(mod\ 4)$. By (9.7)(ii), there exists $S \in RM(d-2,d)$ so that $B = S + F(\tau-1)$ is a 2-set, and such a 2-set is τ-invariant (5.3) and so is one of the indicated $\{i, i+c\}$.

Remark 6.3. We recall an elementary result about positive definite integral lattices [16]. Let J be such a lattice. Call $x \in J, x \neq 0$ *decomposable* if there exist nonzero $y, z \in J$ so that $x = y + z$. If X is the set of indecomposable vectors, we define a graph structure by connecting two members of X with an edge if they are not orthogonal. We therefore get X as the disjoint union of connected components X_i. If J_i is the sublattice spanned by X_i, then X is their orthogonal direct sum. If Y is any orthogonal direct summand of J, Y is a sum of a subset of the J_i.

Corollary 6.4. *The vectors of (6.2) span a sublattice which is an orthogonal direct sum of scaled* $D_{2^{d-2k}}$ *root lattices. This sublattice has finite index in* $MC_1(d,k,\varepsilon)$.

Proof. Consider the natural graph on this set of vectors where edges between distinct vectors are based on nonorthogonality. The connected components span lattices of type D (6.2). □

6.2 Short vectors at level 2

For the moment, $d \geq 5$ is odd and arbitrary. Recall that top closure may fail in BW_{2^d} above level 1 (4.4).

Proposition 6.5. *Suppose that $d \geq 5$ and $d - 2k \geq 3$. If the norm of the level 2 vector $x \in MC_1(d, k, \varepsilon)$ is $2^{\delta-1}$, then there exists $C \in \mathcal{P}(\Omega)$ and B is affine 3-space so that $x = \frac{1}{4} v_B \varepsilon_C$.*

Proof. Since $B \in RM(d - 2m + 1, d)$, we use (9.3). □

Remark 6.6. We do not assert that vectors as in (6.6) exist.

7 Decomposability and indecomposability

We prove that the first cousins are orthogonally decomposable for $k = 1$ and indecomposable for $k \geq 2$. As in (3.7), t has positive trace.

Proposition 7.1. *Let $k = 1$. The lattice $MC_1(d, 1, -)$ is isometric to $BW_{2^{d-2}}$.*

Proof. By ancestral theory [13], $L^-(t) \cong BW_{2^{d-2}}[1]$. By (2.18)(iii), $MC_1(d, 1, -) \cong 2^{-\frac{1}{2}} L^-(t) \cong BW_{2^{d-2}}$. □

Proposition 7.2. *Let $k = 1$. The lattice $MC_1(d, 1, +)$ is isometric to $BW_{2^{d-2}} \perp BW_{2^{d-2}} \perp BW_{2^{d-2}}$.*

Proof. By hypothesis, $k = 1$. Thus, Z is the complement in Ω of a codimension 2 affine space. There are three affine hyperplanes contained in Z. Call them Z_1, Z_2, Z_3 and let Z_{ij} denote the intersection of Z_i and Z_j.

The proof is a consequence of the theory of [13]. For a subset T of Ω, we let $L(T)$ be the set of vectors in L whose support is contained in T. Then $L(Z_i)$ is a scaled $BW_{2^{d-1}}$. The sublattice $L(Z)$ is coelementary abelian of index $2^{2^{d-2}}$ in the orthogonal direct sum $\frac{1}{2}L(Z_{12}) \perp \frac{1}{2}L(Z_{23}) \perp \frac{1}{2}L(Z_{31})$. Furthermore, a set of coset representatives for $L(Z_i) \perp L(\Omega + Z_i)$ in L is just the set S of all $x + xu$, where u is a fixed involution interchanging $L(Z_i)$ and $L(\Omega + Z_i)$ and where $x \in L(Z_i)[-1]$. (The relevant lower fourvolution f should be chosen to have an expression $f = \prod f_i$, where f_i is a lower fourvolution on Z_i; see [13, 12]).

It follows that the set $P^+(S)(f - 1)$ represents all the cosets of $L(Z)$ in $\frac{1}{2}L(Z_{12}) \perp \frac{1}{2}L(Z_{23}) \perp \frac{1}{2}L(Z_{31})$. (It may help to think that $\mathbb{F}_2^3$ is spanned by $(1, 1, 1)$ and the space of vectors with coordinate sum 0.) □

Lemma 7.3. Suppose that M is an integral lattice and N a finite index sublattice. Suppose that N is spanned by vectors which are indecomposable in M and that N is orthogonally indecomposable. Then M is orthogonally indecomposable.

Proof. The hypotheses on M and N imply that N meets every indecomposable summand of M nontrivially. See (6.3). $\square$

Lemma 7.4. *Recall that H is a hyperplane which is transverse to core(Z). Set $v := 2^{-\delta} v_H$, a minimal vector in BW_{2^d}. Then $P^{\varepsilon}(v)$ has norm $2^{\delta}\frac{|Z|}{2^d} = r2^{\delta}$, for some $r \in [\frac{1}{4}, \frac{3}{4}]$. Also, $P^{\varepsilon}(v)(f-1)$ has norm $r2^{\delta+1} = s2^{\delta-1}$, for some $s \in [1,3]$. Therefore, if we write $P^{\varepsilon}(v)(f-1) = w_1 + \cdots + w_n$ as an orthogonal sum of indecomposable nonzero vectors, $n \leq 3$.*

Proof. Use the formula for $|Z|$ (3.7), (3.9) and the fact that $P^{\varepsilon}(v)(f-1) \in MC_1(d,k,\varepsilon)$. $\square$

Proposition 7.5. *Suppose that $d \geq 7$ is odd and $k \geq 2$.*

(i) The minimal vectors of the level 1 sublattice are indecomposable in $MC_1(d,k,+)$. The sublattice of $MC_1(d,k,+)$ which they span is an orthogonal direct sum of scaled type $D_{2^{d-2k}}$ lattices.

(ii) When $d \geq 7$ and $d - 2k \geq 5$, the lattice spanned by the level 2 minimal vectors (which have norms $2^{\delta-1}$) is orthogonally indecomposable and has finite index in $MC_1(d,k,+)$. Therefore, $MC_1(d,1,+)$ is orthogonally indecomposable.

Proof. (i) The first statement is trivial since they are minimal vectors in $MC_1(d,k,+)$. The second statement follows from analysis as in the proof of (6.6).

(ii) Let $L_1, \ldots, L_r$ be the set of scaled type $D_{2^{d-2k}}$-lattices as described in (i). Each is orthogonally indecomposable since $d - 2k \geq 3$.

Take a vector hyperplane H and vector v as in (7.4). Then v has nonzero inner product with vectors of each L_i and so does $P^{+}(v)(f-1)$. If we write $P^{+}(v)(f-1) = w_1 + \cdots + w_n$ as a sum of indecomposable vectors, we get $n \leq 3$ by norm considerations. For each i, there exists j so that L_i has nonzero inner products with w_j. The number of L_i is $2^{d-1} + 2^{d-k-1}$, which is at least 4, and the number of w_j is at most 3. Therefore, there exists a pair of distinct indices i, i' and an index j so that both (L_i, w_j) and $(L_{i'}, w_j)$ are nonzero. Therefore in the graph of indecomposable vectors

(6.3), the minimal vectors of L_i and $L_{i'}$ are in the same component. Now we quote double transitivity of $Sp(2k, 2)$ on the set of L_i [12] to deduce that all minimal vectors of $L_1 \perp L_2 \perp \cdots \perp L_r$ are in the same component. This proves that $MC_1(d, k, +)$ is indecomposable. $\square$

8 More distant cousins

We have considered variations of the formula for first cousins. Many interesting high dimensional lattices with moderately high minimum norms may be created in the midwest style. Precise analysis of their properties would be challenging, however.

One variation creates an even unimodular rank 24 overlattice of $L^+(t)$ for $L \cong BW_{2^4}$ and $tr(t) = 8$. That overlattice has minimum norm 4, so is isometric to the Leech lattice.

Here is a sketch of the construction. In $L^+(t)$, there is a sublattice $M = M_1 \perp M_2 \perp M_3$, where $M_i \cong \sqrt{2}E_8$, for $i = 1, 2, 3$. Let f be a lower fourvolution on L which commutes with t and fixes each M_i. Then $L^+(t)(f - 1) \leq M$ and $P^+(L)(f - 1) \leq L^+(t)$. We need a lemma.

Lemma 8.1. *Suppose that we have two sublattices M, N such that $E_8 = M + N$ and $M \cong N \cong \sqrt{2}E_8$. There exists $\gamma \in O(E_8)$ which interchanges M and N.*

Proof. This follows from the analogous property of $O^+(2d, 2)$ since $O(E_8)$ acts on E_8 mod 2 as $O^+(8, 2)$. $\square$

Continuing our construction, we let γ be an isometry of M which stabilizes each M_i and satisfies $M_i(f-1) \cap M_i(f-1)\gamma = 2M_i$ and (consequently) that $M_i(f - 1) + M_i(f - 1)\gamma = M_i$ (see (8.1) and the ancestral theory [13]). Then $L^+(t) + P^+(L)(\gamma^{-1} f \gamma - 1)^2$ is isometric to the Leech lattice. There is similarity in spirit to [17, 23].

It is well-known that the Leech lattice contains sublattices isometric to BW_{2^4} (as fixed point sublattices of involutions) [4], [10]. The above result links the Leech lattice and BW_{2^5}.

9 Appendix: Some background

Standard properties of Reed-Muller binary codes [21, 20] and the Barnes-Wall lattices [1, 3, 13] will be used intensely. For convenience, we review

them here.

9.1 Review of Reed-Muller codes

Notation 9.1. For integers $d \geq 1$ and $k \in \{0, 1, \cdots, d\}$, there is defined a Reed-Muller binary code $RM(k, d)$ of length 2^d. We use $\Omega = \Omega_d$, a copy of affine space $\mathbb{F}_2^d$, as indices. A binary vector may be interpreted as an $\mathbb{F}_2$-valued function of its index set $\mathbb{F}_2^d$, or as a subset of the index set (the support of the previous function). Addition is the boolean sum. The Reed-Muller code $RM(k, d)$ is spanned by the vectors which are the characteristic functions of affine subspaces of codimension at most k (or, in the power set interpretation $\mathbb{F}_2^\Omega$, as the actual affine subspaces). For all $p \leq -1$, $RM(p, d) := 0$.

We mention a few facts for use in this article.

Proposition 9.2. *For $d \geq 1$ and for $i = 0, 1, 2, \ldots, d-1$, $RM(i, d)^\perp = RM(d-1-i, d)$.*

Lemma 9.3. *In $RM(k, d)$, the minimum weight is 2^{d-k} and the codewords of minimum weight are the affine subspaces of codimension k;*

Proof. This is well-known; see [18], Theorem 3, p. 375 and Theorem 8, p. 380.

□

Definition 9.4. For $A \in \mathcal{P}(\Omega)$, we define the *BW-level* of A to be $max\{m \geq 0 \mid A \in RM(d-2m, d)\}$ and the *RM-level* of A to be $max\{i \mid A \in RM(d-i, d)\}$. We abbreviate these terms by *BW-level(A)* and *RM-level(A)*, respectively. We extend the concept of level to elements of BW_{2^d} by using the notation (4.3) with respect to the basis v_i of (9.1).

Remark 9.5. If $i =$ RM-level(A), then the elements of $A + RM(d-i-1, d)$ have RM-level i. If $m =$ BW-level(A), then the elements of $A + RM(d-2m-2, d)$ have BW-level m.

Proposition 9.6. *Suppose that τ is a translation in $AGL(d, 2)$. Then*

(i) $RM(j, d)(\tau - 1) \leq RM(j-1, d)$;

(ii) $\mathcal{P}(\Omega)$ is a free module for $\mathbb{F}_2[\mathbb{F}_2^d]$. The image of $\tau - 1$ is the set of all τ-invariant codewords. Also, $\mathcal{P}(\Omega)$ is a free $\mathbb{F}_2[\langle\tau\rangle]$-module.

(iii) If $x \in Ker(\tau - 1) = Im(\tau - 1)$ and $x \in RM(d-k, d)$, there exists $y \in RM(d-k+1, d)$ so that $x = y(\tau - 1)$.

(iv) If we identify the group algebra $\mathbb{F}_2[\mathbb{F}_2^d]$ with $\mathcal{P}(\Omega)$, the powers of the augmentation ideal of $\mathbb{F}_2[\mathbb{F}_2^d]$ are the codes $RM(j,d)$.

Proof. (i) The first part is obvious since $RM(j,d)$ is spanned by affine subspaces S of codimension j, and $S + S\tau$ is either empty or is a $(j+1)$-dimensional affine subspace.

(ii) Since $\mathcal{P}(\Omega)$ is a free module for $\mathbb{F}_2[\mathbb{F}_2^d]$, it is a free module for the subalgebra $\mathbb{F}_2[\langle\tau\rangle]$. The statements follow.

(iii) Since $\mathcal{P}(\Omega)$ is a free module for $\mathbb{F}_2[\langle\tau\rangle]$ (by (ii)), $Ker(\tau-1) = Im(\tau-1)$. Assume that c is a τ-invariant codeword in $RM(k,d)$. Since τ is an involution, c is an even set, whence $k \leq d-1$. Let h be an affine hyperplane which is transverse to every τ-invariant 1-space. Then $c \cap h \in RM(k+1,d)$ and $c = (c \cap h)(\tau - 1)$.

(iv) This follows from (ii) and (iii). □

Lemma 9.7. *Let X be a subset of Ω. Then*

(i) if $|X|$ is even, $X(\tau-1)$ is in $RM(d-2,d)$; and

(ii) if $|X|$ is odd, there is Q, a 1-space invariant under τ, such that $X(\tau-1)$ is in $Q + RM(d-2,d)$.

(iii) In (ii), if Q, Q' are 1-spaces such that $X(\tau-1)$ is in $Q + RM(d-2,d) = Q' + RM(d-2,d)$, then Q' is a translate of Q and both are τ-invariant.

Proof. To prove (i), use (9.6)(i). Next, (ii) follow easily from the case $|X| = 1$. For (iii), we may assume X is a 1-set. First notice that since $Q + Q' \in RM(d-2,d)$, whose minimal weight codewords are affine 2-spaces, Q' is a translate of Q. One is τ-invariant if and only if the other one is. On the other hand, there exists some 1-space Q'' which is τ-invariant and which satisfies $X(\tau-1) \in Q'' + RM(d-2,d)$ (just take $Q'' = \{x, x\tau\}$, for any $x \in X$, and use (i),(ii)). Therefore, both Q and Q' are τ-invariant. □

Definition 9.8. Suppose that Γ is a subspace of Ω. Let $\mathcal{P}(\Omega,\Gamma)$ be the members of $\mathcal{P}(\Omega)$ which are unions of cosets of Γ. Then members of $\mathcal{P}(\Omega,\Gamma)$ may be interpreted as subsets of the quotient vector space Ω/Γ and so we have an isomorphism $\mathcal{P}(\Omega,\Gamma) \to \mathcal{P}(\Omega/\Gamma)$. This may be interpreted as an isomorphism of a subspace of binary vectors of length $|\Omega|$ with the full space of binary vectors of length $|\Omega/\Gamma|$.

Definition 9.9. Given a codeword $c \in RM(2,d)$, there is at most one integer $k \in \{1, 2 \ldots, \frac{d}{2}\}$ such that the coset $c + RM(1,d)$ contains a codeword of weight $2^{d-1} - 2^{d-k-1}$. If there is such a k, we say c has *defect* k. If there is no

such k, we say that c has defect 0. We say that c is *short* if it has cardinality less than 2^{d-1}, *long* if it has cardinality greater than 2^{d-1} and otherwise we say c is a *midset* or a *midword*. [12]

Definition 9.10. A sum $S_1+\cdots+S_k$ of $k>0$ affine codimension 2 subspaces whose intersection is nonempty, is called a *cubi sum* if its cardinality is $2^{d-1}-2^{d-k-1}$. A short defect k codeword c may be written as a cubi sum. We define the *core* of a cubi sum to be the intersection of the k summands. It depends only on c and not on the particular cubi sum for c.

9.2 Review of PO2^d-theory and Barnes-Wall lattices

The Reed-Muller codes can be used to construct Barnes-Wall lattces [1], [3]. Alternatively, they may be deduced from existence of Barnes-Wall lattices [13].

Notation 9.11. The *Barnes-Wall lattice* BW_{2^d} in rank 2^d, $d\geq 2$, is an even lattice whose isometry group contains $G_{2^d}\cong 2_+^{1+2d}\Omega^+(2d,2)$. This is the full isometry group when $d\neq 3$. These lattices are scaled so as to make BW_{2^d} unimodular when d is odd and to make the discriminant group elementary abelian of rank 2^{d-1} when d is even. Finally, define $R_{2^d}:=O_2(G_{2^d})\cong 2_+^{1+2d}$.

Definition 9.12. For BW_{2^d}, there is a standard generating sets (as abelian groups). We start with the a set $\{v_i \mid i\in\Omega\}$ of vectors in BW_{2^d}. As in (9.1), $\Omega=\mathbb{F}_2^d$. We often use the maps ε_S, which take v_i to $-v_i$ if $i\in S$ and to v_i if $i\notin S$. This map is in G_{2^d} if and only if $S\in RM(2,d)$ and is in R_{2^d} if and only if $S\in RM(1,d)$ (9.11). The *standard generating set* is all of vectors of the form $\frac{1}{2^m}v_A$, where m is a nonnegative integer and A is an affine $2m$-space in Ω. In fact, this is just the set of minimal vectors of BW_{2^d}.

Proposition 9.13. *The minimal vectors in BW_{2^d} are of the form $\frac{1}{2^m}v_A\varepsilon_S$, where m is a nonnegative integer, $0\leq m\leq 2^{\lfloor\frac{d}{2}\rfloor}$, A is an affine $2m$-space in Ω and $S\in RM(2,d)$. They have norms $2^{\lfloor\frac{d}{2}\rfloor}$.*

Proof. This is a standard result [3, 13]. □

Definition 9.14. Let $L:=BW_{2^d}$. A *lower frame* or a *standard frame* is a set of 2^{d+1} minimal vectors of L which forms an orbit under the action of the normal extraspecial subgroup of order 2^{1+2d} of $BRW^+(2^d)$. (A lower frame was called a sultry frame in [12].) A *standard basis* or a *lower basis* is

a basis contained in a standard frame with a labeling by Ω such that the set of minimal vectors of L is as described in (9.13). An arbitrary labeling by Ω of a basis contained in a frame may not have this property. See [13].

9.3 Review of commutator density

This concept was introduced in [13]. Let D be an extraspecial 2-group and let $Mod(D, -)$ be the category of modules for which the central involution of D acts as -1. Often, D is dihedral of order 8.

The basic results are summarized in this section. For a proof, see [13].

Definition 9.15. Let E be a group, S a subset of E and M a $\mathbb{Z}[E]$ module. We say that S is *commutator dense on* M if $[M, E] = [M, S]$.

Definition 9.16. Let D be a dihedral group of order 8 and let M be a $\mathbb{Z}[D]$-module. We say that M has the *2/4 generation property* if for any pair of involutions u, v which generate D, we have $M^+(u) + M^+(v) = M$.

Proposition 9.17. *Let D be a dihedral group of order 8 and let M be a $\mathbb{Z}[D]$-module on which the central involution of D acts as -1. Let $f \in D$ have order 4. Then on M, 2/4-generation and commutator density of $\{f\}$ are equivalent.*

Proof. [13]. □

Notation 9.18. Suppose that D is dihedral of order 8 and that L is in the category $Mod(D, -)$. Let f be an element of order 4 in D and let p be an integer. The *p-th twist* of L is the D-submodule $L[p] := L(f-1)^p$ of $\mathbb{Q} \otimes L$.

Proposition 9.19. *Let $L = BW_{2^d}$ and let $f \in R_{2^d}$ be a fourvolution. Then $[L, R_{2^d}] = L(f-1)$, i.e., f is commutator dense on the R_{2^d}-module L.*

Proof. [13]. □

Remark 9.20. The notation $L[p]$ (rather than $L(f-1)$) stresses dependence on R_{2^d} rather than on choice of fourvolution $f \in R_{2^d}$ (9.19). This independence can be useful.

10 Appendix: the minimal vectors of $BW_{2^d}[1]$

The minimal vectors of BW_{2^d} constitute the standard generating set (9.12), as is well-known. We need the following fact about twists of Barnes-Wall lattices. This result may be new.

Theorem 10.1. *The set of minimal vectors of $BW_{2^d}[1]$ is $K := \cup_{m\geq 0} K_m$, where K_m is the set of all $2^{-m}v_A\varepsilon_S$, where A is a $(2m+1)$-dimensional affine subspace of $\Omega = \mathbb{F}_2^d$ and $S \in RM(2,d)$.*

Proof. Define $L := BW_{2^d}$. We use the commutator density property, that $L[1]$ equals $L(\pm f \pm 1)$ for any lower fourvolution f (9.19).

Let J be the set of minimal vectors in L. Since each $f-1$ doubles norms and maps L onto $L[1]$, it takes J onto the set K' of minimal vectors of $L[1]$.

The K_m are orbits for the action of the standard monomial subgroup of $BRW^+(2^d)$. To prove $K \subseteq K'$, it suffices to prove that $J(f-1)$ contains a single member of each K_m. It suffices to prove that, given m such that $K_m \neq \emptyset$, that there exists a lower fourvolution f so that $K_m \cap J(f-1) \neq \emptyset$.

Take A, an affine $(2m+1)$-dimensional space. Let H be a hyperplane such that $dim(A \cap H) = 2m$. Let τ be a translation on Ω which fixes A and interchanges H and $H+\Omega$. Define $f := \tau\varepsilon_H$, a lower fourvolution. Then $2^{-m}v_{A\cap H} \in J$ and $2^{-m}v_{A\cap H}(1+f) = 2^{-m}v_A$.

Finally, to prove that $K' \leq K$, observe that if $v \in K$, the vector $v(f-1)^{-1} \in J$, so has the form $u = 2^{-m}v_B\varepsilon_S$, for some affine $2m$-space B. Then $u\tau\varepsilon_H = (2^{-m}v_{B\tau} - 2^{-m+1}v_{B\tau\cap H})\varepsilon_S$.

If $B = B\tau$, $v = u(f-1) = 2^{-m+1}v_{B\cap H}\varepsilon_S \in K_{m-1}$.

If $B \neq B\tau$, then $B \cap B\tau = \emptyset$ and $v = u(f-1) = 2^{-m}_{B+B\tau}\varepsilon_{S+H} \in K_{m1}$. $\square$

References

[1] E. S. Barnes and G. E. Wall, Some extreme forms defined in terms of abelian groups, JAMS 1 (1959), 47-63.

[2] Beverly Bolt, T. G. Room and G. E. Wall, On the Clifford Collineations, Transform and Similarity Groups, I. Journal of the Australian Mathematical Society, 2, 1961, 60-79.

[3] Michel Broué and Michel Enguehard, Une famille infinie de formes quadratiques entière; leurs groupes d'automorphismes, Ann. scient. Éc. Norm. Sup., 4^{eme} série, t. 6, 1973, 17-52.

[4] John Conway and Neil Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag 1988.

[5] Daniel Gorenstein, Finite Groups, Harper and Row, New York, 1968.

[6] Robert L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology (research announcement for [5]), in Finite Groups 1972: Proceedings of the Gainesville Conference on Finite Groups, (T. Gagen, M. P. Hale and E. E. Shult, eds.), North Holland Publishing Co., Amsterdam, 68-73, 1973.

[7] Robert L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, Pacific J. Math., 48, 403-422, 1973.

[8] Robert L. Griess, Jr., The monster and its nonassociative algebra, in Proceedings of the Montreal Conference on Finite Groups, Contemporary Mathematics, 45, 121-157, 1985, American Mathematical Society, Providence, RI.

[9] Robert L. Griess, Jr., Twelve Sporadic Groups, Springer Verlag, 1998.

[10] Robert L. Griess, Jr., Pieces of Eight, Advances in Mathematics, 148, 75-104 (1999).

[11] Robert L. Griess, Jr., Positive definite lattices of rank at most 8, Journal of Number Theory, 103 (2003), 77-84.

[12] Robert L. Griess, Jr., Involutions on the Barnes-Wall lattices and their fixed point sublattices, I. Pure and Applied Mathematics Quarterly, vol.1, no. 4, (Special Issue: In Memory of Armand Borel, Part 3 of 3) 989-1022, 2005.

[13] Robert L. Griess, Jr., Pieces of 2^d: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. Advances in Mathematics, 196

(2005) 147-192. math.GR/0403480; Corrections and additions to " Pieces of 2^d: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. " [Adv. Math. 196 (2005) 147-192], Advances in Mathematics 211 (2007) 819-824.

[14] Robert L. Griess, Jr., "Groups and Lattices", book to appear.

[15] Bertram Huppert, Endliche Gruppen I, Springer Verlag, Berlin, 1968.

[16] Martin Kneser, Zur Theorie der Kristalgitter, Math. Ann. 127, 105-106 (1954).

[17] James Lepowsky and Arne Meurman, An E_8 approach to the Leech lattice and the Conway groups, J. Algebra 77 (1982), 484-504.

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

[19] Harriet Ketcher Pollatsek, Cohomology groups of some linear groups over fields of characteristic 2, Illinois Journal 15 (1971) 393-417.

[20] D. E. Muller, Application of Boolean algebra to switching circuit design and to error detection, IEEE Trans. Computers, 3 (1954) 6-12.

[21] I. S. Reed, A class of multiple -error-correcting codes and the decoding scheme, IEEE Trans. Info. Theory, 4 (1954) 38-49

[22] Jean-Pierre Serre, A Course in Arithmetic, Springer Verlag, Graduate Texts in Mathematics 7, 1973.

[23] Jacques Tits, Four presentations of Leech's lattice, in "Finite Simple Groups , II, Proceedings, London Math Society Research Symposium, Durham, 1978 (M. J. Collins, Ed.), pp. 306-307 Academic Press, London/New York, 1980.