Pure and Applied Mathematics Quarterly
Volume 1, Number 4
(*Special Issue: In Memory of Armand Borel, Part 3 of 3*)
989—1022, 2005

Involutions on the Barnes-Wall Lattices and their Fixed Point Sublattices, I.

Robert L. Griess Jr.

Abstract: We study the sublattices of the rank 2^d Barnes-Wall lattices BW_{2^d} which occur as fixed points of involutions. They have ranks 2^{d-1} (for dirty involutions) or $2^{d-1} \pm 2^{k-1}$ (for clean involutions), where k, the defect, is an integer at most $\frac{d}{2}$. We discuss the involutions on BW_{2^d} and determine the isometry groups of the fixed point sublattices for all involutions of defect 1. Transitivity results for the Bolt-Room-Wall group on isometry types of sublattices extend those in [PO2^d]. Along the way, we classify the orbits of $AGL(d, 2)$ on the Reed-Muller codes $RM(2, d)$ and describe *cubi sequences* for short codewords, which give them as Boolean sums of codimension 2 affine subspaces.

Contents

Received July 22, 2005.

1. Introduction

We continue to study the Barnes-Wall lattices BW_{2^d} and their isometry groups, which are the Bolt-Room-Wall groups $BRW^+(2^d) \cong 2_+^{1+2d}\Omega^+(2d,2)$ for $d \geq 2, d \neq 3$ and W_{E_8} for $d = 3$. In particular, we classify involutions in $BRW^+(2^d)$ and determine properties of their fixed point sublattices, including automorphism groups. For background, we analyze words of the Reed-Muller code $RM(d,2)$ in some detail and in particular determine the orbits of $AGL(d,2)$.

We shall be using the Barnes-Wall-Ypsilanti uniqueness theory as developed in [PO2^d]. We recommend this article for background and terminology. *Notational warning:* $O(L)$ *means orthogonal group on a quadratic space* L *but* $O(G)$ *means* $O_{2'}(G)$ *for a finite group* G.

The main results of this article are described below. See 3.18, 3.19

Theorem 1.1. *The orbits for the action of* $AGL(d,2)$ *on the Reed-Muller code* $RM(2,d)$ *are as follows (for each category, there is one orbit for each allowed value of* k*):*

Short sets of defect $k = 0, \dots, \lfloor \frac{d}{2} \rfloor$*, which are of the form* $S_1 + \cdots + S_k$*, where the* S_i *are affine codimension 2 spaces which are linearly coindependent with respect to an origin in their common intersection; such a set has cardinality (or Hamming weight)* $2^{d-1} - 2^{d-k-1}$*.*

Long sets, which are complements of short sets.

Midsets, of cardinality 2^{d-1}*, which are either affine hyperplanes (defect* 0*) or nonaffine midsets of the form* $S + H$*, where* H *is an affine hyperplane and* S *is a* *short set of weight $2^{d-1} - 2^{d-k-1}$, for a unique $k \in \{1, \dots, \lfloor \frac{d-1}{2} \rfloor\}$. (Note: $k \neq \frac{d}{2}$ here.)*

Some background in the structure of BRW groups is required to state our main results. We refer the reader to the Appendix for a summary and notations. For definitions of clean and dirty, see 9.3 and for defect, see 9.5.

Theorem 1.2. *(i) When d is odd, the conjugacy classes for involutions in the BRW group $BRW^+(2^d)$ are represented by the transformations:*

(Split Case) ε_X, where X is a codeword as listed in 1.1, one for each value of the defect, $k \leq \frac{d-1}{2}$.

(Nonsplit Case) $\eta_{d,2k,\varepsilon}$, for $k = 1, \dots, \frac{d-1}{2}$, $\varepsilon = \pm$.

(ii) When d is even, the conjugacy classes for involutions in the BRW group $BRW^+(2^d)$ are represented by the transformations:

(Split Case) ε_X, where X ranges over the codewords listed in 1.1, but one for each value of the defect, k, together with the single clean involution ε_Y^τ, where Y is a short codeword with defect $k = \frac{d}{2}$ and τ is an outer automorphism of $BRW^+(2^d)$.

(Nonsplit Case) $\eta_{d,2k,\varepsilon}$, for $k = 1, \dots, \frac{d}{2}$, where $\varepsilon = \pm$ except for $k = \frac{d}{2}$ when $\varepsilon = +$ only.

The next result extends transitivity results in [PO2^d] to a wider class of sublattices.

Procedure 1.3. (Conjugacy for involution fixed point sublattices and recognition criteria for such.) Two RSSD sublattices M_1, M_2 of BW_{2^d} are in the same orbit of G_{2^d} if and only if their associated involutions are conjugate. We may use 1.2 as a guide to orbits of $BRW^+(2^d)$ on RSSD sublatttices. In particular, whether two given RSSD sublattices are in the same orbit of $BRW^+(2^d)$ may be decided *within the lattice* by surveying a family of RSSD sublattices of BW_{2^d}. It is unnecessary to examine the explicit representation of the group $BRW^+(2^d)$. See 4.1.

Definition 1.4. In general, if X is a subobject of Y, the *inherited group* means the image in $Sym(X)$ of $Stab_{Aut(Y)}(X)$.

In the next result, this applies to the containment $L^\varepsilon(t) \leq L := BW_{2^d}$.

Theorem 1.5. *Consider a clean involution t of defect 1 on $L := BRW^+(2^d)$.*

When the trace of t is positive, the rank of $L^+(t)$ is $2^{d-2}3$. The automorphism group is inherited when $d \geq 2, d \neq 3$ and for $d = 3$ it is W_{B_6}.

When the trace of t is negative, the rank of $L^+(t)$ is 2^{d-2} and the fixed point sublattice is a scaled version of $BW_{2^{d-2}}$, whose automorphism group is $BRW^+(2^{d-2})$ if $d \neq 5$ and is W_{E_8} if $d = 5$.

Theorem 1.6. *The automorphism groups of the involution fixed point sublattices is inherited when the involution is dirty, split, of defect 1 and when $d \geq 5$ is odd.*

Theorem 1.7. *The automorphism groups of the involution fixed point sublattices is not inherited when the involution is nonsplit of defect is 1 and $d \geq 5$. The fixed point sublattices are isometric to $ssBW_{2^{d-2}} \perp ssBW_{2^{d-2}}$.*

The author thanks Alex Ryba for many useful discussions. The author has been supported by NSA grant USDOD-MDA904-03-1-0098.

2. Notation and terminology

We mention some special terminology, definitions and notation; see [PO2^d].

BW_{2^d}, the Barnes-Wall lattice in dimension 2^d	[PO2^d]
$BRW^0(2^d, \pm)$	Bolt, Room and Wall group, [PO2^d]
clean	an element of $BRW^0(2^d, \pm)$ not conjugate to its negative
D, a lower dihedral group	a dihedral group of order 8 in the lower group R
defect of an involution	9.5
density, commutator density	[PO2^d]
determinant of a lattice, L	$\lvert\mathcal{D}(L)\rvert$
diagonal	3.14
dirty	an element of $BRW^0(2^d, \pm)$ conjugate to its negative
$\mathcal{D}(L)$, discriminant group of an integral lattice L	$\mathcal{D}(L) = L^*/L$
L^*, the dual of the lattice L	$\{x \in \mathbb{Q} \otimes L \mid (x, L) \leq \mathbb{Z}\}$
ε_S	3.14
fourvolution	a linear transformation whose square is -1
$G = G_{2^d}$	$BRW^+(2^d)$
inherited	1.4
lower	in R
$R = R_{2^d}$	$O_2(BRW^+(2^d))$
SSD, semiselfdual, RSSD, relatively semiselfdual	applies to certain sublattices of an integral lattice; there are associated involutions,
sBW, sBW_{2^k}	scaled copy of some BW_{2^k}

	$\cong \sqrt{s}BW_{2^k}$ for some integer $s > 0$.
ssBW, $ssBW_{2^d}$ (for a sublattice of BW_{2^d})	suitably scaled copy of BW_{2^k} = a scaled BW_{2^k} with scale 2^h, $h = \frac{d-k}{2}$ for $d-k$ even; $h = \frac{d-k-1}{2}$ for $d-k$ odd, d even; $h = \frac{d-k-1}{2} + 1$ for $d-k$ odd, d odd.
total eigenlattice, $Tel(E), Tel(L, E)$	the sum of the eigenlattices of an elementary abelian 2-group or involution E on the lattice L
upper	in G but not in R

Conventions. Our groups and most endomorphisms act on the right, often with exponential notation. Group theory notation is mostly consistent with [Gor, Hup, G12]. The commutator of x and y means $[x, y] = x^{-1}y^{-1}xy$ and the conjugate of of x by y means $x^y := y^{-1}xy = x[x, y]$. These notations extend to actions of a group on an additive group.

Here are some fairly standard notations used for particular extensions of groups: p^k means an elementary abelian p-group; $A.B$ means a group extension with normal subgroup A and quotient B; $p^{a+b+\cdots}$ means an iterated group extension, with factors $p^a, p^b, \ldots$ (listed in upward sense); $A{:}B$, $A{\cdot}B$ mean, respectively, a split extension, nonsplit extension.

3. Preliminaries

3.1. Groups.

Definition 3.1. The *Dickson invariant* is a natural homomphism $O^+(2d, 2) \to \mathbb{Z}_2$ which has the property that it is nontrivial on orthogonal transvections. (For an exact definition, see [Dieud]). The kernel is the subgroup $\Omega^+(2d, 2)$. Elements of the latter group are called *even* and elements of $O^+(2d, 2)$ which are not even are called *odd*.

This notion extends to the full holomorph $2^{1+2d}.O^+(2d, 2)$ in $GL(2^d, \mathbb{C})$, so that the BRW group $BRW^+(2^d)$ is considered its even subgroup [GrMont].

Notation 3.2. From now on, $d \geq 2$, $G_{2^d} := BRW^+(2^d)$, $R_{2^d} := O_2(G_{2^d})$. Reference to d will typically be suppressed and we use G for G_{2^d} and R for R_{2^d}.

Lemma 3.3. *Let t be an isometry of V, a vector space in characteristic 2 with an alternating bilinear form. Then $[V, t] = Im(t - 1)$ is totally isotropic.*

Proof. Let $x, y \in V$. Then $(x(t-1), y(t-1)) = (x,y) - (x,yt) - (xt,y) + (xt,yt)$. Since we are in characteristic 2 and t is an isometry, the first and last terms cancel. Since $t^2 = 1$, the middle two terms cancel. □

Remark 3.4. When t leaves invariant a quadratic form associated to the alternating bilinear form, the totally isotropic space of 3.3 may be totally singular or not.

Notation 3.5. Let R be an extraspecial group and H a subgroup of R which contains $Z(R)$. Then H has a central product decomposition, $H = AB$, where $A = Z(H)$ and $B = Z(R)$ or B is extraspecial. Clearly, $A \cap B = Z(R)$. The group B is not unique if $A > Z(R)$, but the set of such B forms an orbit under $Stab_{Aut(R)}(H)$ if A is elementary abelian. We call such a decomposition of H a *CMZ-decomposition* (for complement modulo the center) and such a B is called a *CMZ-subgroup.*

Lemma 3.6. *An involution t which acts on an extraspecial group $R \cong 2_+^{1+2d}$ as an even automorphism fixes a noncentral involution if $d \geq 2$.*

Proof. If t is inner, this is obvious. Suppose that t acts nontrivially on the Frattini factor of R. Since $[R,t]$ is not contained in $Z(R)$ and is normal in R, $Z(R) \leq [R,t]$. Also, $[R,t]$ is abelian (by 3.3). Since t inverts a set of generators for $[R,t]$, it inverts $[R,t]$, so centralizes $\Omega_1([R,t])$. Also, $[R,t]$ is noncyclic since for even orthogonal transformations, the space of fixed points is even dimensional (see 9.5). This completes the proof. □

Lemma 3.7. *Let t be an upper involution in the automorphism group of an extraspecial 2-group of plus type. Then t centralizes a maximal elementary abelian subgroup if and only if its image in the outer automorphism group is even and $[R,t]$ is elementary abelian.*

Proof. The necessity follows from the well-known facts that $\Omega^+(2d,2)$ has two orbits on maximal totally singular subspaces and that they are fused by $O^+(2d,2)$ [GrElAb].

We now prove sufficiency. We may assume that the order of the extraspecial group R is 2^{1+2d}, for $d \geq 2$ (there are no even upper involutions for $d = 1$). Let t be an upper involution.

The action of t fixes a noncentral involution $u \in R$, by 3.6. So, t acts on $C_R(u)/\langle u \rangle \cong 2_+^{1+2(d-1)}$. If $u \notin [R,t]$, then t acts evenly on this extraspecial group and we finish by induction. Therefore, we are done if t fixes an involution outside $[R,t]$, so suppose that none exist. Then since R has plus type, $[R,t]$ has order 2^{d+1}. Since t inverts $[R,t]$, we are done since $[R,t]$ is elementary abelian by hypothesis, so is maximal elementary abelian. □

Proposition 3.8. *We are given $V = \mathbb{F}^{2d}$ with quadratic form q and associated bilinear form $(\cdot, \cdot)$ so that $V = I \oplus J$ is a decompostion into maximal totally singular d-dimensional subspaces. Define $Inv(V, I)$ to be the set of involutions t in G, the orthogonal group for q, so that t is trivial on I and V/I and $[V, t] = I$. Then*

(0) $Inv(V, I) \neq \emptyset$ if and only if d is even.

(1) Assume that d is even. Then $Inv(V, I)$ is in bijection with these two sets:

(1.a) the set of $2d \times 2d$ matrices of the form $I_{2d} + N$, where N has rank d and is supported in the upper right $d \times d$ submatrix, which is alternating.

(1.b) The set of all sequences $v_1, w_1, \ldots, v_d, w_d$ with each $v_j \in J, w_j \in I$ so that $[v_i, t] = w_i$ for all i and $(v_i, w_j) = 0$ except for $\{i, j\}$ of the form $\{2k-1, 2k\}$ for $k = 1, \ldots, \frac{d}{2}$ in which case $(v_i, w_j) = 1$.

Proof. For (0), use 9.5. The proof of (1) is formal. □

Definition 3.9. A *natural BRW subgroup* of G is a subgroup of the form $C_G(S)$, where S is a plus type extraspecial subgroup of R. Natural BRW subgroups occur in pairs, each member being the centralizer in G of the other.

We need to discuss normalizers of lower elementary abelian subgroups in G and centralizers of clean upper involutions.

Proposition 3.10. *Let E be a lower elementary abelian group of order 2^{a+b}, where $2^a = |Z(R) \cap E|$. Let $N := N_G(E)$ and $C := C_G(E)$. Suppose that $b \geq 1$. Then N and C have the following structure.*

There are subgroups $S, T \leq R$ and $P \leq G$ so that

(a) T and S are extraspecial of respective orders $2^{1+2(d-b)}, 2^{1+2b}$ (though $T = 1$ if $b = d$), $[T, S] = 1$ and $R = TS$;

(b) $EZ(R)$ is maximal elementary abelian in S; it follows that $TEZ(R) = C_R(E)$.

(c) the group $P := C_N(C_R(E)/EZ(R)) \cap N_N(E_0)$, where E_0 complements $Z(R) \cap E$ in E, satisfies $P \cap S = EZ(R)$ and $P/T \cong 2^{\binom{b}{2}+b(2d-2b)}{:}GL(2b, 2)$;

(d) $C_C(S) = C_G(S)$ is the natural BRW-subgroup containing T;

(e) $C_P(T)S/S$ has the form $2^{\binom{b}{2}}{:}GL(2b, 2)$.

(f) $C = O_2(P)C_G(S)$;

(g) if $a = 0$, $N = CP$ and if $a = 1$, $N = CSP$.

Definition 3.11. Given an involution t in an orthogonal group over a field of characteristic 2, a *MNS-subspace for* t (minimal nonsingular) is a nontrivial, nonsingular subspace which is t-invariant, and no proper subspace of it has these properties.

Lemma 3.12. *Let t be an involution in the orthogonal group $\Omega^\varepsilon(2e,2)$ and S a MNS-subspace for t. Suppose that t acts nontrivially on S.*

Either S has dimension 2 and a basis u, v so that $u^t = v$ and $(u,v) = 1$, so that u and v are both singular or both nonsingular;

or S has dimension 4 and a basis u_1, u_2, v_1, v_2 of singular vectors so that $v_1^t = v_2, u_1^t = u_2$ and the Gram matrix for this basis is $\begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}$. *Furthermore both of the above spaces are MNS-subspaces.*

Proof. We may suppose that $dim(S) \geq 4$ and that for every singular vector $v \in S$, $(v, v^t) = 0$, then try to get the last conclusion. We note that S is spanned by its singular vectors.

Take a singular vector v_1 not fixed by t and define $v_2 := v_1^t$. Choose a singular vector $u_1 \in S$ so that $(v_1, u_1) = 1$ and $(v_2, u_1) = 0$. Using t-invariance, we find that the sequence $v_1, v_2, u_1, u_2 := u_1^t$ has Gram matrix $\begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&b\\ 0&1&b&0 \end{pmatrix}$. This matrix is nonsingular, whence S has dimension just 4. Now, if $b \neq 0$, $span\{v_1+u_2, u_1+v_2\}$ is a 2-dimensional MNS-subspace. Therefore, $b = 0$. Since $S(t-1)$ is totally singular, S is minimal. □

Lemma 3.13. *Let u be an involution in $\Omega^+(2e,2)$ of defect e. There exists a maximal totally singular subspace F so that $F \cap F^u = 0$.*

Proof. Take a MNS-subspace for S. Then t acts nontrivially on S since the defect is e. Also, t leaves invariant the summands of the decomposition $S \perp S^\perp$. We are therefore done by induction if we check it for the cases of 3.11. This is trivial for the 2-dimensional case and for the 4-dimensional case, take the span of the second and third basis elements. □

Notation 3.14. On the rational vector space spanned by a Barnes-Wall lattice, we take a sultry frame F containing a basis labeled by affine space $\mathbb{F}_2^d$ [PO2^d]. For a subset S of the index set, define the orthogonal involution ε_S to be the map which is -1 at frame elements labeled by a member of S and 1 on the other frame elements. The set of such linear maps, for $S \in RM(2,d)$, forms the *diagonal group*, denoted $\mathcal{E}$ or $\mathcal{E}_d$. It is a subgroup of $BRW^+(2^d)$. The *defect of the codeword c* is the defect of the involution ε_c.

Definition 3.15. Recall that an involution in the BRW group $BRW^+(2^d)$ is *dirty* if it is conjugate to its negative and otherwise, it is *clean*; 9.3. These properties are equivalent to having nonzero, zero trace, respectively, on the natural 2^d-dimensional module. Furthermore, if the trace is nonzero, it has the form $\pm 2^{d-k}$, where k is the defect 9.5 of the involution. We call such an involution a (d,k)-*involution*. Any involution in the lower coset of such is also called a (d,k)-*involution*. (This terminology applies to dirty involutions in such a coset.)

The dimension of the space of commutators of a defect k diagonal involution with the translation group of $AGL(d,2)$ is $2k$ since the translation group can be interpreted as a complement in R_{2^d} to the diagonal subgroup corresponding to $RM(1,d)$. The terms clean and dirty apply to codewords, according to whether the corresponding involutions are clean or dirty.

The term *absolute clean trace* or *positive clean trace* applies to any element of $BRW^+(2^d)$ and means, the absolute value of the trace of any clean element in its lower coset. So, the absolute clean trace is a power of 2 even if the element is dirty. We let $\mathcal{D}$ and $\mathcal{C}$, respectively, denote the set of dirty and clean codewords in $RM(2,d)$.

Proposition 3.16. *Let $u \in G$ be a clean (d,k)-involution, $k > 0$. Then*

(i) $C_G(u)$ has the following form: it is a subgroup of $N_G(E)$, where $E = [R,u]$ is a rank $2k+1$ elementary abelian group as in 3.10; $C_G(u)$ corresponds to the natural $Sp(2k,2)$ subgroup of $N_G(E)/C_G(E) \cong GL(2k,2)$ associated to the identification of $R/C_R(E)$ with $E/Z(R)$ derived from commutation with t;

(ii) The involution $uR \in G/R$ has centralizer $C_G(u)R/R$.

Proof. (i) It is clear from 3.10 that $C_G(u)$ has this form, except possibly for the replacement of $GL(2k,2)$ by $Sp(2k,2)$. It is clear that commutation by u gives a linear isomorphism of S/E onto $E/Z(R)$ which makes these two spaces into dual modules for $C_G(u)$. The action of $C_G(u)$ is therefore symplectic on both. It suffices to show that there is a subgroup of $C_G(u)$ which acts on both as the full group $Sp(2k,2)$.

We take an elementary abelian subgroup F of S so that $FZ(R) = F \times Z(R)$ is maximal elementary abelian and so that $F \cap F^u = 1$ (see 3.13). Then u acts on $H := C_{C_G(u)}(T) \cap N_G(F) \cap N_G(F^u)$, which has shape $2 \times GL(2(d-k),2)$ (the shape is clearly of the form $2.GL(2k,2)$ but is actually a direct product; see [PO2^d] or the Appendix). Clearly, $C_H(u)$ has shape $2 \times Sp(2k,2)$.

(ii) This follows from noticing that the set of clean elements in uR is just the union of the R-conjugacy class of u with the R-conjugacy class of $-u$. □

Remark 3.17. The exact structure of centralizers for dirty involutions is not needed in this article, but we give a sketch.

There are three main kinds of dirty involutions: lower involutions (defect 0); upper split (positive defect, with elementary abelian commutator subgroup on R); (upper) nonsplit (positive defect, with exponent 4 commutator subgroup on R).

The centralizer of a lower involution has shape $[2 \times 2^{1+2(d-1)}]2^{2(d-1)}.\Omega^+(2(d-1), 2)$.

Let t be a dirty split upper involution. Then $t = ru$, where u is an upper involution and r is a lower involution from $R \setminus [R, u]$. The structure of $C_G(u)$ is discussed in 3.16. We have $C_G(t) \leq C_G(u)$, $C_R(t)$ has index 2 in $C_R(u)$ and $C_G(t)R/R$ is a natural subgroup of $C_G(u)R/R$ of shape $2^{2(d-2k)}{:}\Omega^+(2(d-2k), 2)$.

Let t be a nonsplit involution. Let S be a maximal extraspecial subgroup of $C_R(t)$. Then $C_R(S) \geq [R, t] = [C_R(S), t]$. Also, $C_R(t) = S \times E$, where E is elementary abelian and a complement in $\Omega_1([R, t])$ to $Z(R)$. We say t has *plus type* or *minus type* according to the type of the extraspecial group S. Now, $N_G([R, t]) \geq R$ and $N_G([R, t])/R$ modulo its unipotent radical has the form $\Omega^+(2(d-2k), 2) \times GL(2k-1, 2)$. The image of $C_G(t)$ in the latter quotient has the form $\Omega^+(2(d-2k), 2) \times O(2k-1, 2)$.

3.2. **The codes $RM(2, d)$ and the diagonal group.** Our vector spaces are finite dimensional. We shall mix styles at times, so that a codeword may be written in lower case (when we think of it as a vector) or upper case (if we think of it as a geometric structure, like an affine subspace).

Notation 3.18. The *Reed-Muller code* $RM(k, d)$ is the binary code indexed by affine space $\mathbb{F}_2^d$ and spanned by all affine subspaces of codimension k. Its dimension is $\sum_{i=0}^{k} \binom{d}{i}$.

Definition 3.19. A *midset* is a codeword in $RM(2, d)$ of size 2^{d-1}. A midset is *nonaffine* if it is not a codimension 1 affine subspace. A codeword is *short* if its weight is less than 2^{d-1}. A codeword is *long* or *tall* if its weight is more than 2^{d-1}.

Lemma 3.20. *Let $t \in G$ be an involution so that $[R, t]$ is elementary abelian and $\mathcal{E}$ a given diagonal group. Then there is a conjugate of t in $\mathcal{E}$, unless possibly d is even and t has defect $\frac{d}{2}$, in which case there exists another diagonal group containing t.*

Proof. Use 3.7 and the fact that $C_R(t)$ is nonabelian if and only if $C_R(t)$ contains representatives of both G-conjugacy classes of maximal elementary abelian subgroups of R. □

Notation 3.21. We will study the action of $AGL(d,2)$ on $\mathbb{F}_2^d$ and various codes. Let $T := T(d,2)$ denote the translation subgroup and $GL(d,2)$ the stabilizer of some origin (understood from context).

Definition 3.22. Linear subspaces U_i of a vector space are *independent* if their sum is their direct sum. Linear subspaces U_i of a vector space are *coindependent* if their annihilators in the dual space are independent.

This definition extends to a collection of affine subspaces U_i of a vector space, provided their common intersection is nonempty. One then chooses any origin in $\bigcap_i U_i$ and uses the above definition (which is independent of choice of origin).

Lemma 3.23. *Suppose that we have $k \geq 1$ linearly coindependent codimension 2 affine subspaces $S_1, \dots, S_k$ in $\mathbb{F}_2^d$ with nonempty common intersection. Then $|S_1 + \cdots + S_k| = 2^{d-1} - 2^{d-k-1}$. (Note: $k \leq \frac{d}{2}$ here.)*

Proof. Let $a(d,k)$ be $2^{d-1} - 2^{d-k-1}$. We use induction on k. The result is trivial for $k = 1, 2$. We may assume that the spaces contain a common origin, so are linear.

Assume that $k \geq 3$ and that the formula holds by induction for $k-1$. We have $S_k \cap (S_1 + \cdots + S_{k-1}) = S_1 \cap S_k + \cdots + S_{k-1} \cap S_k$, which, by induction on d and coindependence in $S_k \cong \mathbb{F}_2^{d-2}$, has cardinality $a(d-2, k-1)$. It follows that $|S_1 + \cdots + S_k| = 2^{d-2} + a(d, k-1) - 2a(d-2, k-1) = a(d,k)$. □

Definition 3.24. A set of codimension 2 subspaces as in 3.23 is called a *cubi sequence of codimension 2 spaces*. Their Boolean sum is called a *a cubi sum.* [1]

Notation 3.25. Let c be a clean codeword of defect k. Let

$$Cubi(c) := \{(S_1, \dots, S_k) | \bigcap_{i=1}^{k} S_i \neq \emptyset, S_1, \dots, S_k \text{ are coindependent affine}$$

$$\text{codimension 2 subspaces, and } \sum_{i=1}^{k} S_i = c\},$$

the set of *cubi expressions* of c, i.e. the set of ordered cubi sequences as above whose sum is c.

Corollary 3.26. *Given any integer $j \in [0, \frac{d}{2}]$, there is an involution of defect j in the diagonal group.*

Proof. If $j = 0$, take a lower involution. Suppose $j > 0$. Then take $\varepsilon_{S_1 + \cdots + S_j}$, in the notation of 3.23. □

[1] We chose the term *cubi* because our theory suggested the remarkable cubi sculpture series by David Smith. See also the footnote at 3.34.

Next, we show explicitly how to realize a dirty class associated to the clean class within the diagonal group.

Lemma 3.27. *Given $d \geq 3$ and $k \geq 1$ and a length k cubi sequence in $\mathbb{F}_2^d$, there exist hyperplanes whose sum with the cubi sum has cardinality 2^{d-1}. In fact, any hyperplane which neither contains nor avoids the cubi intersection meets this condition.*

Proof. Let $S_1, \ldots, S_k$ be our cubi sequence and let $U := \bigcap_{i=1}^k S_i$. Let $\mathcal{N}$ be the set of hyperplanes which neither contain U nor avoid U. Then $|\mathcal{N}| = 2^{d+1} - 2^{2k+1}$. This is positive for $d \geq 3$ and $k \geq 1$.

Let $H \in \mathcal{N}$. Then the spaces $S_i \cap H$ have codimension 2 in H. They are coindependent with respect to H since $H \cap U$ has codimension 1 in U. Therefore, 3.23 gives $|H \cap (S_1 + \cdots + S_k)| = |(S_1 \cap H) + \cdots + (S_k \cap H)| = 2^{d-2} - 2^{d-k-2}$. Consequently, $|H + S_1 + \cdots + S_k| = 2^{d-1} + 2^{d-1} - 2^{d-k-1} - 2(2^{d-2} - 2^{d-k-2}) = 2^{d-1}$. $\square$

Remark 3.28. The codeword of weight 2^{d-1} constructed in the proof of 3.27 is not a hyperplane, since the Boolean sum of two distinct nondisjoint hyperplanes is a hyperplane and $|S_1 + \cdots + S_k| < 2^{d-1}$.

We next need to work from a nonaffine midset to the class of clean codewords that it comes from.

Definition 3.29. Let $d \geq 3$. Given a nonaffine midset a, a hyperplane h so that $a + h$ is clean is called a *cleansing hyperplane for h.* It follows that if a has defect k, and h is cleansing, then $|a \cap h| = 2^{d-2} \mp 2^{d-k-2}$. (Note that $d - k \geq 2$ for $d \geq 3$.)

Lemma 3.30. *Every coset of $RM(1, d)$ in $RM(2, d)$ contains a clean codeword.*

Proof. Take a nontrivial coset, say $u + RM(1, d)$ and take a complement S in $RM(1, d)$ to the 1-space spanned by the universe. The subgroup of the diagonal group corresponding to S has 1-dimensional fixed point sublattice, so the sum of the traces of its elements is 2^d. Assume that the lemma is false. Then every element of $\langle u, S\rangle \setminus S$ gives a diagonal map of trace 0. Therefore the sum of the traces for the subgroup of the diagonal group corresponding to $\langle u, S\rangle$ is 2^d, which is impossible since this number must be divisible by 2^{1+d}. $\square$

Lemma 3.31. *If $c \in RM(2, d)$ is clean, the number of its conjugates by R is 2^{2k}, where c has defect k.*

Proof. This is just the correspondence of the R-orbit of c under the action of conjugation on $RM(2, d)$ with the cosets of $C_R(c)$ in R, together with the definitions of defect and cleanliness. $\square$

Proposition 3.32. *In a given coset $c+RM(1,d)$, where c is clean and has defect k, the number of clean codewords is 2^{2k+1} and the number of dirty codewords is $2^{d+1}-2^{2k+1}$.*

Proof. If $c \in RM(2,d)$, the number of its transforms by R is 2^{2k}, by 3.31. The coset $c+RM(1,d)$ also contains the same number of transforms of the complement $c+\mathbb{F}_2^d$, which is also clean.

We use the irreducible module for G, which is a 2^d-dimensional complex vector space, and the trace function Tr on it. The previous paragraph implies that the sum $s(c) := \sum_{v \in c+RM(1,d)} Tr(v)^2$ is at least $2 \cdot 2^{2k+2(d-k)} = 2^{2d+1}$

Since the group $RM(1,d)$ acts on the 2^d-dimensional complex vector space so as to afford all linear characters nontrivial on the center, each with multiplicity 1, it follows from orthogonality relations for the group generated by R and c that each $s(c) = 2^{2d+1}$. The coset therefore has 2^{2k+1} clean elements and $2^{d+1}-2^{2k+1}$ dirty elements. □

Corollary 3.33. *The number of cleansing hyperplanes for a dirty codeword $s \in RM(2,d)$ is 2^{2k+1}, where k is the defect of any clean involution in the coset $s+RM(1,d)$. Thus the set $\mathcal{N}$ of 3.27 is the full set of noncleansing hyperplanes.*

Example 3.34. Let $d=4, k=1$ and let S be a defect 1 (nonaffine) midset. There are 8 cleansing hyperplanes. Write $S=A+H$, where A is short and H a cleansing hyperplane of S (this involves half the cleansing hyperplanes). Then A is a 4-set (hence an affine hyperplane) and $S \cap H$ is a 2-set. This set is stable by translation with elements of the core. Therefore, S is a union of four cosets of $S \cap H$. The assignment $H \mapsto S \cap H$ is one-to-one from the set of cleansing hyperplanes such that $S+H$ is short. By counting, this is a bijection. The union of any two sets $S \cap H$, as H varies, is an affine 2-space. Therefore, S is the disjoint union of a pair of disjoint, nonparallel affine 2-spaces, in three different ways. [2]

Corollary 3.35. *Given cleansing hyperplanes H_1, H_2 for the dirty codeword S, if $H_1 \cap S = H_2 \cap S$, then $H_1 = H_2$, i.e., for cleansing hyperplanes, H, the map $H \mapsto H \cap S$ is monic.*

Proof. If H_1 and H_2 are distinct, then, since they meet, their sum is a hyperplane. Since H_1+H_2 is contained in the complement of S, it equals the complement of S. This is a contradiction since S is not affine. □

Procedure 3.36. We now have a *procedure to determine the orbit of a dirty codeword*. It depends only on examining the code, not the action of the group $AGL(d,2)$. Call such a codeword v. Add to v all of the $2^{d+1}-2$ affine hyperplanes. A nonempty set of these will be cleansing and the corresponding sums will have

[2] These configurations also suggest the David Smith cubi theme; see 3.24.

weight of the form $2^{d-1} \pm 2^{d-k-1}$, which will give the defect k. This procedure is exponential in d.

Lemma 3.37. *Two short (resp. long) clean codewords of the same defect are in the same orbit under $AGL(d,2)$. A short clean codeword is a cubi sum.*

Proof. We interpret these codewords by their actions on the commutator quotient of R. The result follows from transitivity of the natural action of $GL(d,2)$ on alternating matrices of the same rank. □

Lemma 3.38. *Suppose that we are given $(S_1,\dots,S_k) \in Cubi(c)$ as in 3.25. The subspace $\bigcap_{i=1}^k S_i$ has dimension $d-2k$ and is the subgroup of the group of translations which fixes c. This subspace depends on c only, not on a choice from $Cubi(c)$.*

Proof. Clearly, the above intersection is a linear subspace and translations by it fix each S_i, hence also fix c. Since the space of commutators of the translation group with c has dimension $2k$, no translations outside this subspace fixes c. Therefore, this intersection depends on c only. □

Lemma 3.39. *The stabilizer in $AGL(d,2)$ of the clean codeword c of defect k is transitive on $Cubi(c)$, and the the stabilizer of a member of $Cubi(c)$ has shape $2^{d-2k}.2^{2k(d-2k)}[(\prod_{i=1}^k GL(2,2)) \times GL(d-2k,2)]$.*

Proof. The initial 2^{d-2k} refers to the group of translations which stabilize $\bigcap_{i=1}^k S_i$. The result follows from transitivity of $GL(d,2)$ on ordered direct sums of k 2-spaces in the dual. □

Definition 3.40. The *core* of a clean codeword is $\bigcap_{i=1}^k S_i$, where $(S_1,\dots,S_k) \in Cubi(c)$. The definition is independent of choice from $Cubi(c)$, by 3.38.

Theorem 3.41. *The stabilizer of a clean codeword of defect k in $AGL(d,2)$ is a group of the form $[2^{(1+2k)(d-2k)}]{:}[Sp(2k,2) \times GL(d-2k,2)]$. It has two orbits on $\mathbb{F}_2^d$, namely the core and its complement.*

Proof. The second statement follows from the structure of the stabilizer, which we now discuss.

We may think of our clean codeword c as a cubi sum for cubi sequence $(S_1,\dots,S_k)$. Choose an origin in the core 3.40, i.e., the $(d-2k)$-space $U := S_1 \cap \dots \cap S_k$.

Let H be the stabilizer of c in $AGL(d,2)$. Then $H_t := H \cap T$ is transitive on U. The last paragraph implies that $H = H_t H_0$ where H_0 is the stabilizer of the origin. So, H_t corresponds to U and H_0 lies in the stabilizer in $GL(d,2)$ of the subspace U, a parabolic subgroup P of the form $2^{2k(d-2k)}{:}[GL(2k,2) \times GL(d-2k,2)]$. Note that $O_2(P)$ is a tensor product of irreducibles for the two factors, so is irreducible.

We next argue that H_0 is a natural $2^{2k(d-2k)}{:}[Sp(2k,2) \times GL(d-2k,2)]$-subgroup of P.

Consider $C_G(t)$, where t is the diagonal matrix ε_c. Then we have the CMZ decomposition 3.5 for $C_R(t)$ and a related one for R: $R = R_1R_0$, where $[R_0, R_1] = 1$, $C_R(t) = C_1R_0$, where R_0 is extraspecial, and $C_1 \leq R_1$ and C_1 is elementary abelian and contains $Z(R)$. There is a corresponding product J_0J_1 of commuting natural BRW subgroups, with $R_i = O_2(J_i), i = 1, 2$. We have $|C_1| = 2^{2k+1}$ and $C_1 = [R, t] = [R_1, t]$. The action of t preserves R_1 and the maximal elementary abelian subgroup C_1. Also, t acts on $N_{J_1}(C_1) \cong 2^{1+4k}2^{\binom{2k}{2}}GL(2k, 2)$. There is a pair of maximal elementary abelian subgroups B_1, B_2 so that $R_1 = B_1B_2, B_1 \cap B_2 = Z(R)$ and t interchanges B_1 and B_2 (see 3.13).

Choose $D_i \leq B_i$ so that $B_i = D_1 \times Z(R)$ and t interchanges D_1 and D_1. The common stabilizer of D_1 and D_2 in $Aut(R_1)$ has the form $2 \times GL(2k, 2)$. The action of t has fixed point subgroup of the form $2 \times Sp(2k, 2)$ because D_1 and D_2 are in t-invariant duality. Therefore, the image of H in the left factor of $P/O_2(P) \cong GL(2k, 2) \times GL(d-2k, 2)$ contains a copy of $Sp(2k, 2)$. Since the image of H in the left factor stabilizes a nondegenerate form, the image is exactly $Sp(2k, 2)$.

We claim that the stabilizer of c in $AGL(d, 2)$ contains the natural $GL(d-2k, 2)$ subgroup which commutes with the above copy of $Sp(2k, 2)$. This follows since the stabilizer of a member of $Cubi(c)$ involves a copy of $GL(d-2k, 2)$ which acts faithfully on the core and commutes with the action of the above $Sp(2k, 2)$, which acts trivially on the core and faithfully on a complement to the core (meaning, on a linear complement, assuming the origin is chosen from the core).

The claim implies that H maps onto the right factor of $P/O_2(P) \cong GL(2k, 2) \times GL(d-2k, 2)$. It follows that $O_2(P)$ is an irreducible module for H (a tensor product of irreducibles for the factors $Sp(2k, 2)$ and $GL(d-2k, 2)$), whence $H \cap O_2(P)$ is either 1 or $O_2(P)$. The latter group preserves all cosets of U in $\mathbb{F}_2^d$ and each S_i is a union of such cosets, whence $O_2(P) \leq H$. □

Lemma 3.42. *Two dirty codewords of the same defect are in the same orbit under $AGL(d, 2)$.*

Proof. This is obvious from 3.27 and how the stabilizer of the core in $AGL(d, 2)$ acts on $\mathbb{F}_2^d$. □

Remark 3.43. The main theorems 1.1 and 1.2 follow from 3.37, 3.42, 9.14, 9.13. Note that, as a corollary, we get the well-known result that the minimum weight codewords in $RM(2, d)$ are the affine codimension 2 subspaces.

Proposition 3.44. *Let c be a clean codeword of defect k.*

(i) The stabilizer in $AGL(d,2)$ of the coset $c + RM(1,d)$ is $T(d,2)S$, where $T(d,2)$ is the full translation group and S is the stabilizer of c in $AGL(d,2)$ (see 3.41).

(ii) Let $s \in c+RM(1,d)$ be a dirty codeword. The commutator space $[T(d,2), s]$ has dimension $2k$ The stabilizer of s in $AGL(d,2)$ is a subgroup of S of index $2^{d+1} - 2^{2k+1}$ of shape $[2^{(1+2k)(d-2k-1)}][Sp(2k,2) \times AGL(d-2k-1,2)]$. It is $Stab_S(h)$, where $h = s + c$ is an affine codimension 1 subspace which meets the core of c in a codimension 1 subspace of it. The initial $2^{1\cdot(d-2k-1)}$ corresponds to translations by the intersection of the core of c with a cleansing hyperplane.

Proof. (i) This is clear since the set of clean elements in $c + RM(1,d)$ is just the set of 2^{2k} $T(d,2)$-transforms of c.

(ii) Since s is dirty, $d - 2k > 0$.

Consider the set $\mathcal{P}$ of all pairs $(s,r) \in c + RM(1,d)$ so that s is dirty, r is short and clean (whence $s+r$ is a hyperplane, so is a cleansing hyperplane; 3.29). We refer to 3.41. Let H be the stabilizer of this coset in $AGL(d,2)$. Then H acts transitively on $\mathcal{P}$, which has cardinality $(2^{d+1} - 2^{2k+1})2^{2k}$, so $Stab_H((s,r))$ has index $2^{d+1} - 2^{2k+1}$ in $Stab_H(r)$, which has form $[2^{(1+2k)(d-2k)}]{:}[Sp(2k,2) \times GL(d-2k,2)]$.

Now, consider a hyperplane h in $\mathbb{F}_2^d$ which meets U in a codimension 1 subspace of U. By 3.27, $r+h$ is a midset, so $(r+h, r) \in \mathcal{P}$. Since $H_{(r+h,h)}$ stabilizes h, it follows that $H_{(r+h,r)}$, hence every $H_{(s,r)}$, has the form $[2^{(d-2k-1)+2k(d-2k)}]{:}[Sp(2k,2)\times AGL(d-2k-1,2)]$. □

4. The conjugacy classes of involutions in G_{2^d} and orbits on RSSD sublattices

We continue to let $G := G_{2^d}$, $R := R_{2^d}$ and let $t \in G$ be an involution. We summarize the conjugacy classes of involutions.

Suppose that t centralizes a maximal elementary abelian subgroup (so is in a diagonal group). For each maximal elementary abelian subgroup E of $C_R(t)$, we have representatives of $\lfloor \frac{d}{2} \rfloor$ clean classes of upper involutions in a diagonal group $C_G(E)$. Upper involutions of the same defect and trace are conjugate in G except for the case where d is even and the involutions have full defect $\frac{d}{2}$. Two such involutions are clean and are conjugate if and only if their traces are equal and maximal elementary abelian subgroups in their lower centralizers are in the same orbit under the even orthogonal group.

Suppose that t does not centralize a maximal elementary abelian subgroup. Then $[R,t]$ is abelian of exponent 4 and has order 2^{1+2k} for some $k \geq 1$. It is now clear from 9.14, 9.13, that t is conjugate to some $\eta_{2k,\pm}$; see 9.7.

Procedure 4.1. In [PO2^d], we showed that two RSSD sublattices in BW_{2^d} which had the same rank, but unequal to 2^{d-1} (the clean case), are in the same orbit under $BRW^+(2^d)$ with the exception of two orbits for maximal defect $\frac{d}{2}$. Also, [PO2^d] treats the case of rank 2^{d-1} sublattices which are fixed points of lower involutions. We now give a procedure for determining when two RSSD sublattices are in the same orbit of $BRW^+(2^d)$ *which depends only on examining a restricted set of sublattices, not the whole group* $BRW^+(2^d)$. Besides the two given RSSD sublattices, we need to examine only the ones associated to lower involutions, which may be constructed directly, by induction.

Recall that for $d > 3$, the lower involutions in $BRW^+(2^3)$ are those RSSD involutions associated to $ssBW_{2^{d-1}}$ sublattices [PO2^d].

Here we deal with the general dirty case, i.e., rank 2^{d-1}, which represents many orbits. Their associated RSSD involutions are dirty, so if diagonalizable are conjugate to elements of the diagonal group supported by a midsize codeword. We assume that $d > 3$.

We are given a dirty RSSD sublattice. Multiply this involution by all lower involutions.

Suppose that a nonempty set of such products are clean involutions with common defect $k \in [0, \frac{d}{2}]$. Since the defect k is less than $\frac{d}{2}$, k determines the orbit of the sublattice, by 3.44. If $k = \frac{d}{2}$, there are two orbits, depending on which maximal elementary abelian lower group corresponds to the RSDD involution.

Suppose that no such product is clean. Then the involution is some $\eta_{2k,\pm}$. The subgroups $C_R(t)$ and $[R,t]$ determine k and the sign $\pm$ and so the orbit of the sublattice.

For completeness, we treat the case $d = 3$.

Proposition 4.2. *In $BW_{2^3} \cong L_{E_8}$, the orbits of W_{E_8} on RSSD sublattices are (i) those of $BRW^+(2^3)$ on RSSD sublattices of even rank, i.e., one for rank 2, three for rank 4 and one for rank 6; and (ii) four orbits, of respective ranks 1, 3, 5, 7, which are sublattices generated by a root, a set of three orthogonal roots, and the annihilators of such sublattices.*

Proof. Note that the determinant 1 subgroup of W_{E_8} contains a natural $BRW^+(2^3)$ subgroup of odd index. For rank 2 and 6 sublattices, we are in the clean cases in $BRW^+(2^3)$. For rank 4, we are in the dirty cases, of which there are just three, associated to a nonsplit involution (see 9.15(ii)), to a lower involution and an upper dirty involution.

There are two orbits of W_{E_8} on 4-sets of mutually orthogonal pairs consisting of roots and their negatives. One of these 4-sets spans a sublattice of BW_{2^3} which is a direct summand and the other spans a sublattice properly contained in a D_4-sublattice. These cases correpond in the above sense to the nonsplit and lower cases. The third case gives rank 4 sublattices not spanned by roots (9.15).

Now consider the case of odd rank fixed point sublattice, M. It suffices to do the ranks 1 and 3 cases. We use a lemma that if g is in a Weyl group and V is the natural module, then g is a product of reflections for roots which lie in $[V,r]$ [Car]. At once, this implies that the rank 1 lattice here is spanned by a root. Suppose now that $rank(M) = 3$. Let Φ be the set of roots in M. If there is a pair of nonorthogonal linearly independent roots, then Φ has type A_3 or A_2A_1. Since $\mathcal{D}(M)$ is an elementary abelian 2-group, neither of these is possible. We conclude that Φ has type $A_1A_1A_1$. Since M is even, it must equal the sublattice spanned by Φ. We are done since W_{E_8} has a single orbit on subsets of three orthogonal roots in a root system of type E_8. □

Remark 4.3. For simplicity, discuss the main theorems for ranks at most 3 so that we may later use the assumption $d \geq 4$, as needed.

When $d = 1$, the fixed point sublattice of any involution is 0 or a rank 1 lattice.

Assume $d = 2$. The dirty involutions in BW_{2^2} and their fixed point sublattices are analyzed in 9.15. If $t \in BRW^+(2^2)$ is clean, its fixed point sublattice has rank 1 or 3. In these respective cases, the sublattice is spanned by a vector of norm 2 or 4 or is the orthogonal of such a rank 1 sublattice, so is a root lattice of type B_3 or C_3. See the proof of 4.2.

When $d = 3$, all fixed point sublattices are accounted for in the proof of 4.2. They are all orthogonal direct sums of indecomposable root lattices.

4.1. **Containments in $RM(2,d)$.**

Lemma 4.4. *Let $A, B \in RM(2,d)$ and suppose that $0 \neq A < B \neq \mathbb{F}_2^d$. Let X^c denote the complement of the subset X of $\mathbb{F}_2^d$. Then one of the following holds:*

(i) A is a codimension 2 subspace and B is a midset; or B^c is a codimension 2 subspace and A^c is a midset.

Furthermore, (i) happens for affine hyperplanes B for any $d \geq 3$, and for nonaffine midsets B exactly when B has defect 1 and $d \geq 3$, respectively.

(ii) A is short and B is long, of respective cardinalities $2^{d-1} - 2^{d-k-1}$. $2^{d-1} + 2^{d-r-1}$, *where* $(k, r) = (1, 1), (1, 2), (2, 1)$ *or* $(2, 2)$. *We summarize:*

(k, r)	$\lvert A\rvert$	$\lvert B\rvert$	$\lvert A + B\rvert$
$(1, 1)$	$2^{d-1} - 2^{d-2} = 2^{d-2}$	$2^{d-1} + 2^{d-2} = 2^{d-2}3$	2^{d-1}
$(2, 1)$	$2^{d-1} - 2^{d-3} = 2^{d-3}3$	$2^{d-1} + 2^{d-2} = 2^{d-2}3$	$2^{d-3}3$
$(1, 2)$	$2^{d-1} - 2^{d-2} = 2^{d-2}$	$2^{d-1} + 2^{d-3} = 2^{d-3}5$	$2^{d-3}3$
$(2, 2)$	$2^{d-1} - 2^{d-3} = 2^{d-3}3$	$2^{d-1} + 2^{d-3} = 2^{d-3}5$	2^{d-2}

Note that cases (1,2) and (2,2) are dual in the sense that A *and* $A + B$ *may be interchanged. Note that the case (1,1) corresponds to (i) for the midset* $A+B$ *containing* B^c. *Note also that* A *in case (1,2) and* $A + B$ *in case (2,2) are codimension 2 affine spaces.*

Proof. If B is a midset, and A is not a codimension 2 affine subspace, then $A < B$ implies that A has cardinality $2^{d-1} - 2^{d-k-1}$ for an integer k and A is a cubi sum in the sense of 3.37. Since $A + B = A \setminus B$ is also a codeword, it has cardinality $2^{d-1} - 2^{d-r-1}$ for an integer $r \geq 1$. It follows that $k = r = 1$. Then A and A^c are affine codimension 2 subspaces. Therefore, if B is a midset, (i) holds.

It is obvious that (i) happens in an essentially unique way when B is an affine hyperplane. Assume B is a midset but not affine. The codimension 2 affine subspaces A and A' whose union is B are not translates of each other. Let A'' be a translate of A' which meets A nontrivially. The intersection has codimension 1 or 2 in each of A or A'' and it is an exercise to show that for codimension 1, this situation does happen in an essentially unique way, and that it does not happen for $k = 2$ (reason: such subspaces are affinely coindependent and so an associated linear system expressing their intersection has a solution).

Assume that neither A nor B is a midset. In case both are long, we may replace with complements to assume both are short. In any case, we may assume that A is short, of cardinality $2^{d-1} - 2^{d-k-1}$, for some integer k, $0 < k \leq \frac{d}{2}$.

First assume that B is short, say of cardinality $2^{d-1} - 2^{d-r-1}$, for $r > k$. Then $A + B$ has cardinality $2^{d-k-1} - 2^{d-r-1} = 2^{d-r-1}(2^{r-k} - 1)$. Since $A + B$ is short, there exists an integer $s \leq \frac{d}{2}$ so that $2^{d-r-1}(2^{r-k} - 1) = 2^{d-1} - 2^{d-s-1} = 2^{d-s-1}(2^s - 1)$. If both sides are powers of 2, then $r = k+1$, $s = 1$ and $d-r-1 = d-s-1$ implies that $r = s = 1$ and $k = 0$, a contradiction. Therefore both sides are not powers of 2 and so $r = s$ and $s = r - k$ and so $s = r$ and $k = 0$, a final contradiction.

Therefore B is long, of cardinality $2^{d-1} + 2^{d-r-1}$, for $r > 0$. Then $A + B$ has cardinality $2^{d-r-1} + 2^{d-k-1}$. Since $r \geq 1, k \geq 1$, this number is at most 2^{d-1} and is less than 2^{d-1} if $(r, k) \neq (1, 1)$.

Suppose that $r = k$. Then $2^{d-r-1} + 2^{d-k-1} = 2^{d-r}$ is 2^{d-1} or 2^{d-2}, implying $r = k = 1, r = k = 2$, respectively.

Suppose that $r < k$. Then $A + B$ is short and there exists an integer $s \leq \frac{d}{2}$ so that $2^{d-r-1} + 2^{d-k-1} = 2^{d-1} - 2^{d-s-1}$, and $2^{d-k-1}(2^{k-r} + 1) = 2^{d-s-1}(2^s - 1)$. Now, $2^{k-r}+1$ is odd, so it follows that $s = k$, $k-r = 1$ and $s = 2$. So, $k = 2, r = 1$.

Suppose that $r > k$. Then $A + B$ is short and there exists an integer $s \leq \frac{d}{2}$ so that $2^{d-r-1} + 2^{d-k-1} = 2^{d-1} - 2^{d-s-1}$, and $2^{d-r-1}(2^{r-k} + 1) = 2^{d-s-1}(2^s - 1)$. It follows that $s = r$, $r - k = 1$ and $s = 2$. So, $k = 1, r = 2$. □

4.2. About defect 1 midsets.

Lemma 4.5. *Let $d \geq 3$. Suppose that B is a midset of defect 1. Then B contains affine hyperplanes of codimension 2. Suppose that A is an affine codimension 2 space contained in B. There exists a unique hyperplane H so that $B \cap H = A$. (The other two hyperplanes which contain A are cleansing hyperplanes for B 3.29.)*

Proof. Let A and A' be any pair of disjoint codimension 2 subspaces. Then $A + A'$ is a midset and it has defect 0, 1 or 2 if A' has a translate which meets A in codimension 0, 1 or 2, respectively. The first statement follows from 3.32 and transitivity of $AGL(d, 2)$ on midsets of a given defect 3.42.

For the second, consider the three hyperplanes H_1, H_2, H_2 which contain A. Suppose that $H_1 \cap B > A$. Then $|H_1 + B| = |H_1| + |B| - 2|H_1 \cap B| = 2^d - 2|H_1 \cap B| < 2^{d-1}$, whence H_1 is a cleansing hyperplane, and so $|H_1 + B| = 2^{d-1} - 2^{d-1-1} = 2^{d-2}$ and $|H_1 \cap B| = \frac{1}{2}(2^{d-1} + 2^{d-1} - \cdot 2^{d-2}) = 2^{d-3}3$. This means that at most two of the H_i meet B in a set larger than A. Therefore, since $H_i \setminus A$ for $i = 1, 2, 3$, partition $\mathbb{F}_2^d \setminus A$, exactly two of the H_i meet B in a set larger than A and so there exists an H which meets B in A, and by above counting, it is unique. □

5. More group theory for BRW groups

We list some assumed results from group theory.

Lemma 5.1. *(i) A faithful module for $\prod_1^k Sym_3$ in characteristic 2 has dimension at least $2k$.*

(ii) A faithful module for $Sp(2k, 2)$ in characteristic 2 has dimension at least $2k$.

Proof. Let $K_1 \times \cdots \times K_k$ be the natural direct product of $K_i \cong Sp(2, 2) \cong Sym_3$ in $Sp(2k, 2)$. Clearly, (i) implies (ii). We prove (i).

We may assume that the field F is algebraically closed and that $k \geq 2$. Let M be a module of minimal dimension. Consider the decomposition $M = M' \oplus M''$, where $M' = [M, O_3(K_1)]$ and $M'' = C_M(O_3(K_1))$.

Clearly, $dim(M')$ is a positive even integer. Suppose $M'' \neq 0$. Then by induction applied to the action of $K_2 \times \cdots \times K_k$ on M'', we have $dim(M'') \geq 2(k-1)$ and we are finished. Suppose $M'' = 0$. Then we may decompose $M'' = P \oplus Q$ where P and Q represent the two distinct linear characters of $O_3(K_1)$. The actions of $K_2 \times \cdots \times K_k$ on P and Q are faithful and equivalent since P and Q are interchanged by elements of K_1. We now finish by induction. □

Lemma 5.2. *Let $\mathbb{F}_2^{2m}$ have a nonsingular quadratic form of type $\nu = \pm$ and let $sv(m,\nu)$, $av(m,\nu)$ denote the number of singular and nonsingular vectors in the case of type $\nu = \pm$. Then $sv(m,\nu) = (2^m - \nu 1)(2^{m-1} + \nu 1)$ and $av(m,\nu) = (2^m - \nu 1)2^{m-1}$.*

Proof. Well-known. Note that $sv(m,\nu) + av(m,\nu) + 1 = 2^{2m}$. □

Lemma 5.3. *Let $k \geq 2$. Let U be the essentially unique $2k+1$ dimensional $\mathbb{F}_2$-module for $Sp(2k,2)$ with socle of dimension 1 and quotient the natural $2k$-dimensional module. Then (i) U is the natural module for $O(2k+1,2)$; (ii) The orbits of $Sp(2k,2)$ on U consist of the two 1-point orbits lying in the radical, and the singular points and the nonsingular points. Each of the latter orbits form coset representatives for the nontrivial cosets of the radical.*

Proof. This is mainly the 1-cohomology result [Poll], plus a standard interpretation of Ext^1. □

5.1. **For clean involutions.** We use the following notation throughout this subsection.

Notation 5.4. We have the clean upper involution t of defect $k \geq 1$. Take a CMZ decompostion $C_R(t) = PZ$. Denote by q_t the quadratic form on $Z = Z_t$ described in 5.3. The subscript indicates dependence on the involution, t. Call $z \in Z$ *singular* or *nonsingular*, according to the value of $q_t(z)$.

Lemma 5.5. *Use the notation of 5.4. For all $k \geq 1$, the set map $x \mapsto [x,t]$ takes $R \setminus C_R(t)$ to the set of nonsingular vectors in Z with respect to the invariant quadratic form.*

For $k \geq 2$, the action of $C_G(t)$ as $Sp(2k,2)$ on Z is indecomposable; the upper Löwey series has factors of dimensions 1, $2k$.

Proof. Let f be the commutator map $R \to Z$ defined by $f(x) := [x,t]$. Every coset of $Z(R)$ in Z contains an element of $Im(f)$. If $f(x) = f(y)$, we have $1 =$

$f(x)f(y) = [x,t][y,t]$, which is congruent to $f(xy)$ modulo $\langle -1 \rangle$. If $f(xy) \in \langle -1 \rangle$, then $xy \in C_R(t)$. Therefore f maps $R/C_R(t)$ isomorphically onto $Z/\langle -1 \rangle$. Also, the image of f is a set of cardinality 2^{2k} which contains 1 and is invariant under $C_R(t)$, which acts on Z as $Sp(2k,2)$, i.e., $Im(f)$ is a $C_R(t)$-invariant transversal to $Z(R)$ in R.

We compute that (*) $f(xy) = [xy,t] = [x,t]^y[y,t] = f(x)^y f(y)$.

We claim that Z is an indecomposable module for $Sp(2k,2)$. Suppose it is decomposable. Then $Im(f)$ must be either a subspace of Z complementing $Z(R)$ or essentially a coset of some $C_R(t)$-invariant subspace, say Z_0, namely it is the set Y which is the notrivial coset with -1 replaced by 1. Then there exists a homomorphism $h : R \to Z_0$ with the property that $f(x) = -h(x)$ if $x \notin C_R(t)$ and $h(x) = 1$ if $x \in C_R(t)$.

It can not be a subspace since $[R,t]$ is normal in R. So, the second alternative applies to $Im(f)$. Now, we shall get a contradiction, using (*).

Note that we have an alternating bilinear form g on Z with values in $Z(R)$, defined by $g(a,b) := [a',t,b']$ where priming on $a \in Z$ means an element $a' \in R$ so that $f(a') = a$. It helps to think of the Hall commutator identity $[x,y^{-1},z]^y$ $[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$.

There is a g-totally singular subspace of dimension $k+1$ in Z, say W. Assuming that $Im(f) = Y$, we take any elements a,b,c in R so that $abc = 1$ and none of a,b,c is in $C_R(t)$. Then $f(a)f(b)f(c) = (-1)^3 h(a)h(b)h(c) = -1$. From (*), we get $f(c) = f(ab) = f(a)^b f(c)$. Now choose a,b,c so that $f(a),f(b),f(c) \in W$ (this is possible since $k \geq 2$). Then $g(f(a),f(b)) = 1$ implies that $f(a)^b = f(a)$, which implies that $f(c) = f(a)f(b)$, in contradiction with $f(a)f(b)f(c) = -1$. This proves that Z is indecomposable.

At this point, we know that $Im(f)$ is one of two orbits for $Sp(2k,2)$ in Z, the singular one and the nonsingular one. We claim that it is the singular one. Suppose otherwise. Take W and a,b,c as above. Then (*) implies that (in additive notation) the sum of two orthogonal nonsingular vectors is nonsingular, a contradiction. $\square$

Definition 5.6. Let ϕ be a linear character of Z which is nontrivial on $Z(R)$. Then $Ker(\phi)$ is a nonsingular quadratic space by restriction of q_t 5.4. Its *type* is plus or minus, according to the Witt index of the restriction of q_t.

Lemma 5.7. *Consider* $X := \{(\varphi,z) | \varphi \in Hom(Z,\mathbb{F}_2), z \in Z\}$ *and let* $Y_{\varepsilon,\zeta,\eta} := \{(\varphi,z) \in X | \varphi(Z(R)) \neq 1, z \neq 1, q_t(z) = \zeta, type(\varphi) = \varepsilon, \varphi(z) = \eta\}$, *for* $\zeta,\eta \in \mathbb{F}_2$. *Then* $C(t)$ *is transitive on* $Y_{\varepsilon,\zeta,\eta}$, *for* $\zeta,\eta = 0,1$.

The orbit lengths are

$|Y_{\varepsilon,0,0}| = (2^{2k-1} + \varepsilon 2^{k-1}) sv(k,\varepsilon)$;

$|Y_{\varepsilon,0,1}| = (2^{2k-1} + \varepsilon 2^{k-1})av(k, \varepsilon)$;

$|Y_{\varepsilon,1,0}| = (2^{2k-1} + \varepsilon 2^{k-1})av(k, \varepsilon)$;

$|Y_{\varepsilon,1,1}| = (2^{2k-1} + \varepsilon 2^{k-1})sv(k, \varepsilon)$.

Note that rows 2 and 3 are equal and rows 1 and 4 are equal.

Proof. It is well-known that $C(t)/O_2(C(t)) \cong Sp(2k, 2)$ acts with two orbits on characters of Z which take nontrivial value on $Z(R)$. These orbits have respective stabilizers the natural subgroups $O^\varepsilon(2k, 2)$ and respective lengths $2^{2k-1} + \varepsilon 2^{k-1}$. The rest follows from 5.2. □

Notation 5.8. Let $t \in G$ be an involution. Then $C_G(t)$ acts on each eigenlattice $L^\varepsilon(t)$. Its image in $O(L^\varepsilon(t))$ is denoted G_ε.

Lemma 5.9. The action of $C_G(t)$ on $L^\pm(t)$ is irreducible. The center of G_ε is just $\{\pm 1\}$.

Proof. The second statement follows from orthogonality of the representation plus absolute irreducibility, which we now prove. We prove irreduciblity for a natural subgroup of $C_G(t)$ of the form AB, where $[A, B] = 1$, $A \cong 2^{1+2(d-k)}$, $Z \leq B, B/Z \cong Sp(2k, 2)$; see 3.5, 5.5. Every faithful irreducible of A has dimension 2^{d-2k}. The central involution of R is in Z and so every irreducible of B on $\mathbb{Q} \otimes L$ involves an orbit of characters of Z of cardinality $2^{2k-1} \pm 2^{k-1}$, and both orbit lengths occur with multiplicity 2^{d-2k}. Therefore, just two irreducibles for AB occur in $\mathbb{Q} \otimes L$, and they have respective dimensions $2^{d-2k}(2^{2k-1} \pm 2^{k-1}) = 2^{d-1} \pm 2^{d-k-1}$. The conclusion follows. □

Lemma 5.10. *Assume t is clean with positive trace. Let $z \in Z$, $z \neq \pm 1$. The trace of z on $L^\pm(t)$ is $\pm 2^{d-k-1}$ if z is q_t-singular and is $\mp 2^{d-k-1}$ if z is q_t-nonsingular.*

Proof. We use the subgroup denoted AB in the proof of 5.9. For AB, the module $L^\varepsilon(t)$ decomposes as a tensor product of irreducibles. It suffices to prove that the trace of z on the tensor factor irreducible for B is $\pm 2^{k-1}, \mp 2^{k-1}$, respectively.

Note that $2^{2k} - 1 - sv(k, \varepsilon) = (2^k - \varepsilon)(2^k - \varepsilon - (2^{k-1} + \varepsilon)) = (2^k - \varepsilon)2^{k-1}$.

We use 5.2 to deduce that

$$|Y_{\varepsilon,0,0}| = 2^{k-1}(2^k + \varepsilon)sv(k, \varepsilon) = 2^{k-1}(2^k + \varepsilon)(2^k - \varepsilon)(2^{k-1} + \varepsilon)$$

and

$$|Y_{\varepsilon,0,1}| = 2^{k-1}(2^k + \varepsilon)(2^{2k} - 1 - sv(k, \varepsilon)) = 2^{k-1}(2^k + \varepsilon)(2^k - \varepsilon)2^{k-1}.$$

Let $\Phi_\varepsilon := \{\varphi | \varphi(Z(R)) \neq \{1\}\}$. A given singular $z \in Z$ is in the kernel of $2^{k-1}(2^{k-1} + \varepsilon) = 2^{2k-2} + \varepsilon 2^{k-1}$ characters in Φ_ε and outside the kernel of 2^{2k-2}

characters in Φ_ε. It follows that the trace of z on $L^\varepsilon(t)$ is $\varepsilon 2^{k-1}$. Singular and nonsingular elements of $Z \setminus Z(R)$ are paired by congruence modulo $Z(R)$. Therefore, nonsingular elements have trace $-\varepsilon 2^{k-1}$. □

5.2. **For dirty involutions.** We assume the following notation throughout this subsection.

Notation 5.11. Let t be a dirty split upper involution of defect k. A *UL factorization of* t is an expression $t = u\ell$, where u is a clean involution and ℓ is a lower involution (note that all of t, u, ℓ commute). Write $\mathcal{U}L(t)$ for all pairs (u, ℓ) as above. Let $\mathcal{U}(t)$ be the set of u and let $\mathcal{L}(t)$ be the set of ℓ which arise this way. We have $|\{\mathcal{U}L(t)\}| = 2^{1+2(d-2k)+2k} - 2^{1+2k}$.

We get a result for traces of u and ℓ on $L^\varepsilon(t)$ which is similar to 5.10.

Lemma 5.12. *On $L^\varepsilon(t)$, the trace of $z \in Z \setminus Z(R)$ is 0 and the trace of ℓ is $\pm 2^{d-k-1}$, for all $\ell \in \mathcal{L}(t)$.*

Proof. We assume $\varepsilon = +$ (the other case is similar). It suffices to consider the sublattices $L(a, b)$, where u acts as a and ℓ acts as b. Recall that the eigenlattices for ℓ are $ssBW_{2^{d-1}}$ lattices, for which we may use 5.7 to compute the traces for z. Without loss, we may assume that z has nonnegative traces. We get:

sublattice	*rank*	*multiplicity of* $+1$ *for* z	*multiplicity of* -1 *for* z
$L(+1,+1)$	$2^{d-2}+2^{d-k-2}$	$2^{d-3}+2^{d-k-2}$	2^{d-3}
$L(+1,-1)$	$2^{d-2}+2^{d-k-2}$	$2^{d-3}+2^{d-k-2}$	2^{d-3}
$L(-1,+1)$	$2^{d-2}-2^{d-k-2}$	$2^{d-3}-2^{d-k-2}$	2^{d-3}
$L(-1,-1)$	$2^{d-2}-2^{d-k-2}$	$2^{d-3}-2^{d-k-2}$	2^{d-3}

□

6. About inherted groups

We continue to use the notations $G := G_{2^d}$, $R := R_{2^d}$. See the ancestor section of [PO2^d] for discussion.

Notation 6.1. We use bars for images under restriction $C_G(t) \to O(L^\varepsilon(t))$. As in 5.8, we write G_ε for the image of $C_G(t)$ in $O(L^\varepsilon(t))$ under the restriction homomorphism.

Lemma 6.2. *Suppose that Z is an elementary abelian subgroup of R containing $Z(R)$ and that rank$(Z) = s+1$. Let L_λ be the eigenlattice for L, defined by the linear character λ of Z, which is assumed to be nontrivial on $Z(R)$. The set $\mathcal{F}$ of such λ has cardinality 2^s.*

There is a finite subgroup of the orthogonal group $O(\mathbb{Q} \otimes L^{\varepsilon}(t))$ of the form $\prod_{\lambda} R_{\lambda}$ with the property that R_{λ} acts on L_{λ} as a lower group and acts trivially on L_{μ} for $\mu \neq \lambda$. We have $|\prod_{\lambda} R_{\lambda}| = 2^{s(1+2(d-s))}$.

(i) When $s = 1$, $\overline{C_G(Z)} \geq \prod_{\lambda} R_{\lambda}$.

(ii) When $s = 2$, $\overline{C_G(Z)} \cap \prod_{\lambda} R_{\lambda}$ is an index $2^{2(d-2)}$ subgroup of $\prod_{\lambda} R_{\lambda}$ with the property that if $\mathcal{J}$ is any 3-set in $\mathcal{F}$, then the projection of $\overline{C_G(Z)}$ to $\prod_{\lambda \in \mathcal{J}} R_{\lambda}$ is onto. The kernel of this homomorphism is just $Z(R_{\mu})$, where $\mu \in \mathcal{F}$ is the index missing from $\mathcal{J}$.

Lemma 6.3. *Let $\mathcal{I} \subseteq \mathcal{F}$ be any nonempty collection of characters as in 6.2 and let $J := J(\mathcal{I})$ be the direct summand of L determined by span$\{J_{\nu} | \nu \in \mathcal{I}\}$. If $\lambda \in \mathcal{I}$ and $g \in C_G(Z)$ acts trivially on J_{λ}, then g acts on J as an element of the group $\prod_{\lambda} R_{\lambda}$, defined in 6.2.*

Proof. If μ, ν are any two distinct indices so that L_{μ} and L_{ν} are stable under $h \in G$, then if h acts trivially on L_{μ} modulo its first lower twist, then h does the same on L_{ν}. By considering all distinct pairs of indices $\mu, \nu \in \mathcal{I}$, we deduce that g acts on J as a member of $\prod_{\eta \in \mathcal{I}} R_{\lambda}$. See [PO2^d] □

Corollary 6.4. *Use the notation of 6.3. Assume that $s = 2$, $\mathcal{I}$ has cardinality 3 and $N_{O(J)}(\overline{Z}) = \overline{N_G(Z)} C_{O(J)}(\overline{Z})$. Then $N_{O(J)}(\overline{Z})$ is inherited.*

Proof. 6.3 and 6.2(ii). □

Corollary 6.5. *Let $t \in G$ be an involution and let $Z := Z(C_R(t))$.*

(i) Suppose that t is a clean involution of defect 1. Then $N_{O(L^{\varepsilon}(t))}(\overline{Z})$ is inherited.

(ii) Suppose that t is a split dirty involution of defect 1. Then $N_{O(L^{\varepsilon}(t))}(\overline{Z})$ is inherited.

Proof. Note that defect 1 implies that $s = 2$, in the notation of 6.2. (i): This follows from 6.4.

(ii): Let t be such an involution. Let $t = u\ell$ be a UL-factorization 5.11. We define Z_u as $Z(C_R(u))$ and define $Z := Z(C_R(t)) = Z_u \times \langle \ell \rangle$. A character value analysis shows that elements of Z_u have 0 trace on $L^{\varepsilon}(t)$ and elements of the coset $Z_u \ell$ have nonzero trace 5.12. Therefore, $N_{O(L^{\varepsilon}(t))}(\overline{Z}_u) \geq N_{O(L^{\varepsilon}(t))}(\overline{Z})$.

We shall use 6.4 to prove that $N_{O(L^{\varepsilon}(t))}(\overline{Z}_u)$ is inherited by showing that the latter group induces only $Sp(2,2)$ on Z. Assume that this is false. We have an action of $AGL(2,2) \cong Sym_4$ on Z. Let H be the linear group which $N_{O(L^{\varepsilon}(t))}(\overline{Z}_u)$ induces on Z_u. The action of $N_{C_G(t)}(Z_u)$ on Z_u preserves the coset $Z_u \setminus Z$ and has orbits modulo $Z(R)$ of lengths 1 and 3. Its orbits on $Z_u \setminus Z$ must have lengths 1,1,3,3 since elements in that coset have nonzero trace on $L^\varepsilon(t)$ so are not conjugate to their negatives. It follows that a Sylow 2-group S of $N_{O(L^\varepsilon(t))}(\overline{Z}_u)$ fixes an element, say ℓ, in this coset. If $x \in Z \setminus Z(R)$, then there exists $g \in S$ so that $x^g = -x$, since we are assuming an action of $AGL(2,2)$ on Z. It follows that $(x\ell)^g = -x\ell$, which is a contradiction since $(x\ell, xu)$ is a UL factorization of t (because $xu \in uZ = u^R$ consists of clean elements). □

7. The split defect 1 cases

7.1. **The clean defect 1 case.**

Definition 7.1. Suppose that M is an integral lattice and X is a SSD lattice. Define $SSD(M,X)$ to be the subgroup of $O(M)$ generated by the SSD involutions associated to sublattices of M which are isometric to X.

This is clearly a normal subgroup of $O(M)$.

We continue to use the notation 3.5. Since the defect is 1, $rank(Z) = 3$. The case $d = 3$ is treated in 4.2, so we assume $d \geq 4$.

Remark 7.2. In the notation of 7.1, if X is SSD and $det(M) = 1$, then $M \cap X^\perp$ is SSD. This will apply for us when $M \cong BW_{2^d}$ and d is odd.

Lemma 7.3. Suppose that $d > 3$. Let t be a clean involution of defect 1 and positive trace. Then $SSD(L^+(t), ssBW_{2^{d-1}}) = Z$.

Proof. A sublattice X of $L^+(t)$ which is isometric to $ssBW_{2^{d-1}}$ is SSD in the overlattice L. By [PO2^d], the associated SSD involution is lower (here, we are using $d > 3$), so lies in $C_R(t)$. Since $Tr_{L^+(t)}(\varepsilon_X) \neq 0$ (see 5.10), $\varepsilon_X \in Z$, the only elements of $C_R(t)$ which have nonzero trace on $L^+(t)$. The action of $C_G(t)$ on Z is that of $O(2k+1,2)$ on its natural module 5.5. Therefore, every element of $Z \setminus Z(R)$ is such an SSD involution. □

Lemma 7.4. Suppose that $d > 3$. Let t be a clean involution of defect 1 and positive trace. Then $O(L^+(t))$ is inherited.

Proof. By 7.3, $\overline{Z}$ is normal in $O(L^+(t))$. Now use 6.4 □

Remark 7.5. If t is a clean involution of defect 1 and positive trace, $L^-(t) \cong ssBW_{2^{d-1}}$, whose automorphism group is known.

7.2. **The split dirty defect 1 case.**

Lemma 7.6. *Suppose that $d > 3$ and d is odd. Let t be a split dirty involution of defect 1. Then $SSD(L^\varepsilon(t), ssBW_{2^{d-2}}) = \overline{C_R(t)}$ and $\overline{Z}$ is a subgroup of $Z(SSD(L^\varepsilon(t), ssBW_{2^{d-2}}))$ which is normal in $O(L^\varepsilon(t))$.*

Proof. We may suppose that $t = \varepsilon_b$ for a defect 1 midset $b \in RM(2,d)$ and we may assume that $\varepsilon = +$. Since d is odd, a $ssBW_{2^{d-2}}$ sublattice is SSD. Let X be such a sublattice of $L^\varepsilon(t)$. Its associated involution in $O(L)$ is conjugate to an involution of the form $\varepsilon_c \in \mathcal{E}$, where the codeword c is an affine codimension 2 subspace.

Since ε_c acts nontrivially on $L^+(t)$, $c \cap b = \emptyset$ Let b' be the complement of b. We may consider the involution ε_h where h is a hyperplane so that $h \cap b' = c$(*see* 4.5). Then ε_c acts on $L^+(t)$ as ε_h, which is a lower involution.

Define K to be the normal subgroup of $O(L^+(t))$ generated by all $\overline{\varepsilon_X}$, where X is a SSD sublattice isometric to $ssBW_{2^{d-2}}$. This is a subgroup of $\overline{C_R(t)}$ which is normal in $\overline{C_G(t)}$ and contains $\overline{\varepsilon_h}$, so is not contained in $\overline{Z(R)}$. The normal subgroups are $\overline{1}, \overline{Z(R)}, \overline{Z}, \langle \overline{Z}, \overline{\ell} \rangle, \overline{C_R(t)}$, where $\ell \in \mathcal{L}(t)$ is any lower part of a UL-factorization. For all such normal subgroups, Y not contained in $Z(R)$, we claim that Z is normal in $N_{O(L^+(t))}(Y)$. This is obvious except when Y is one of the latter two cases. In those cases, $Z(Y) = \langle Z, \ell \rangle$. In the action on $L^+(t)$, the elements of $Z \setminus Z(R)$ have trace 0 and the elements of $Z\ell$ have nonzero trace (see 5.12). The claim follows and so does the lemma since K is normal in $O(L^+(t))$. □

Lemma 7.7. *Suppose that $d > 3$ and d is odd. Let t be a split dirty involution of defect 1. Then $O(L^\varepsilon(t))$ is inherited.*

Proof. Use 7.6 and 6.5(ii). □

This completes the proof of 1.6.

8. The nonsplit defect 1 case

The style of proof here is rather different. The smallest value of d for this case is $d = 2$. Involutions in $BRW^+(2^2) \cong W_{F_4}$ are discussed in 9.15. Involutions in $BRW^+(2^3)$ are discussed in 4.2(i), the even rank sublattice cases.

Lemma 8.1. *If t is a nonsplit involution of defect 1, $L/2L$ is a free $\mathbb{F}_2\langle t \rangle$-module, i.e., the Jordan canonical form for t consists of 2^{d-1} blocks of degree 2.*

Proof. The result may be checked directly for $d \leq 2$ since we know $Tel(t)$ and $Tel(t) + 2L/2L$ is the fixed point space for the action of t on $L/2L$ (see [PO2^d]). The idea is to use induction on d plus the fact that t leaves invariant the summands of a decomposition $L = L^\pm(u) \oplus L^\pm(v)$, where u, v generate a lower dihedral group which centralizes t. This proves that L is a free $\mathbb{Z}\langle t \rangle$-module, so reduction modulo 2 has the claimed structure. □

Lemma 8.2. *Let t be a nonsplit involution of defect 1. Then $L^\varepsilon(t)$ is doubly even for $d \geq 4$, i.e., $\frac{1}{\sqrt{2}} L^\varepsilon(t)$ is an even integral lattice.*

Proof. When $d=4$, $L^{\pm}(u) \cong \sqrt{2}L_{E_8}$, so the property is clearly true. By 8.1, we have $Tel(t) = 2L + [L,t]$. For $x, y \in L$, $(x(t-1), y(t-1)) = (x,y) + (xt, yt) - (x, yt) - (xt, y) = 2(x,y) - 2(x, yt) \in 2\mathbb{Z}$. It follows that $(Tel(t), Tel(t)) \leq 2\mathbb{Z}$. We take $x = y$. We want $(x, xt) \in 2\mathbb{Z}$ to conclude that $x(t-1)$ has norm divisible by 4. This will follow if it is so for a spanning set. Consider the summands of a decomposition $L = L^{\pm}(u) \oplus L^{\pm}(v)$, where u, v generate a lower dihedral group which centralizes t. For $x \in L^{\pm}(u)$, which is a $ssBW_{2^{d-1}}$, $x(t-1)$ has norm divisible by 4 for $d \geq 5$, by induction. □

Lemma 8.3. *Let t be a nonsplit involution of defect 1 in $BRW^+(2^4)$. Then $L^{\varepsilon}(t) \cong \sqrt{2}BW_{2^2} \perp \sqrt{2}BW_{2^2} \cong \sqrt{2}L_{D_4} \perp \sqrt{2}L_{D_4}$.*

Proof. Let $L = BW_{2^4} \cong L_{E_8}$. We follow the strategy in the proof of 4.2. Then there exists a lower dihedral group $D \leq C_R(t)$. Let u, v be involutions which generate D. Then by 2/4-generation [PO2^d], $L = L^{\pm}(u) \oplus L^{\pm}(v)$, all summands are $ssBW_{2^3} \cong \sqrt{2}L_{E_8}$ lattices which are t-invariant and on them t acts like a nonsplit dirty involution. It follows that each $L^{\pm}(w)^{\varepsilon}(t)$ is isometric to $\sqrt{2}L_{A_1^4}$, for any noncentral involution $w \in D$. Reasoning as in 4.2, we argue that $Tel(t)$ has index 2^8 in L and $det(Tel(t)) = 2^{16}det(L) = 2^{24}$. From 8.2, we know that $Tel(t)$ is doubly even. Therefore, each $L^{\varepsilon}(t)$ is doubly even and has determinant 2^{12}. Therefore, there is an even integral lattice, P, so that $L^{\varepsilon}(t) \cong \sqrt{2}P$, $det(P) = 2^4$ and P contains a sublattice Q isometric to $L_{A_1^8}$, of index 4 in P.

Let $r_1, \ldots, r_8$ be an orthogonal basis of roots for Q. Any nontrivial coset of Q in P consists of even norm vectors, so contains an element of shape $\frac{1}{2}\sum_{i \in I} r_i$, where $I \subseteq \{1,2,3,4,5,6,7,8\}$ and $|I| = 4$ or 8 (note that $exp(P/Q) \neq 4$ since vectors of shape $\sum_{i=1}^{8} \pm\frac{1}{4}r_i$ have norm 1).

Let I, I' be any two 4-sets which arise as above. We claim that they are disjoint. Assume otherwise. Since P is even, $I \cap I'$ is a 2-set. Then P is isometric to $L_{D_6} \perp L_{A_1} \perp L_{A_1}$, whence $C_R(t)$ fixes the unique indecomposable orthogonal summand isometric to L_{D_6}. This is impossible since $C_R(t)$ contains a subgroup of shape 2_+^{1+4}, whose faithful irreducibles have dimension divisible by 4. We conclude that there exists a partition J', J'' of $\{1,2,3,4,5,6,7,8\}$ so that J' and J'' are 4-sets and $P = P' \perp P''$, where $P' := \{x \in P | supp(x) \subseteq J'\}$, $P'' := \{x \in P | supp(x) \subseteq J''\}$ and $P' \cong P'' \cong BW_{2^2} \cong L_{D_4}$. □

Proposition 8.4. *For all $d \geq 2$, if $t \in BRW^+(2^d)$ is a nonsplit dirty involution, then $L^{\varepsilon}(t) \cong ssBW_{2^{d-2}} \perp ssBW_{2^{d-2}}$.*

Proof. If $d = 2$, this is true by the discussion in 9.15. For $d = 3, 4$, we use 4.2, 8.3.

Let $d \geq 5$. Then there exists a lower dihedral group $D \leq C_R(t)$. Let u, v be involutions which generate D. Then by 2/4-generation [PO2^d], $L = L^{\pm}(u) \oplus$

$L^{\pm}(v)$, all summands are ss$BW_{2^{d-1}}$ lattices which are t-invariant and on them t acts like a nonsplit dirty involution. By induction, we know the eigenlattices for t on each.

Consider $L^+(u) \perp L^-(u)$. The involution v interchanges the summands and acts trivially on $L/L^+(u) \perp L^-(u)$. The same is therefore true for the actions of v on $L^+(u)^\varepsilon(t) \perp L^-(u)^\varepsilon(t)$ and $L^\varepsilon(t)/L^+(u)^\varepsilon(t) \perp L^-(u)^\varepsilon(t)$.

Since $d-1 \geq 4$, induction implies that each $L^{\pm}(u)^\varepsilon(t)$ is the orthogonal sum of two orthogonally indecomposable lattices. Furthermore, if S is one of these two indecomposable direct summands of $L^+(u)^\varepsilon(t)$, we deduce that the same is true for the actions of v on $S \perp S^v$ and on $L^\varepsilon(t) \cap (\mathbb{Q} \otimes (S \perp S^v))/S \perp S^v$.

We finish by quoting the uniqueness theorem [PO2^d, PO2^dcorr], applied to the containment of $S \perp S^v$ in $L^\varepsilon(t) \cap (\mathbb{Q} \otimes (S \perp S^v))$, for each S. Note that t centralizes a natural $BRW^+(2^{d-2})$-subgroup of $BRW^+(2^d)$ and that it stabilizes S and S^v. □

The main result 1.7 follows.

9. Appendix: About BRW groups.

This is an updated and corrrected version of Appendix 2 from [PO2^d].

Basic theory of extraspecial groups extended upwards by their outer automorphism group has been developed in several places. We shall use [GrEx, GrMont, GrDemp, GrNW, Hup, BRW1, BRW2, B].

Notation 9.1. Let $R \cong 2_\varepsilon^{1+2d}$ be an extraspecial group which is a subgroup of $GL(2^d, \mathbb{F})$, for a field $\mathbb{F}$ of characteristic 0. Let $N := N_{GL(2^d,\mathbb{F})}(R) \cong \mathbb{F}^\times.2^{2d}O^\varepsilon(2d,2)$. The *Bolt-Room-Wall group* is a subgroup of this of the form $2_\varepsilon^{1+2d}.\Omega^\varepsilon(2d,2)$. If $d \geq 3$ or $d = 2, \varepsilon = -$, N' has this property. For the excluded parameters, we take a suitable subgroup of such a group for larger d. We denote this group by $BRW^0(2^d, \varepsilon)$ or $\mathcal{D}(d)$. It is uniquely determined up to conjugacy in $GL(2^d, \mathbb{F})$ by its isomorphism type if $d \geq 3$ or $d = 2, \varepsilon = -$. It is conjugate to a subgroup of $GL(2^d, \mathbb{Q})$ if $\varepsilon = +$. Let $R = R_{2^d}$ denote $O_2(G_{2^d})$. We call R_{2^d} *the lower group* of $BRW^0(2^d, +)$ and call G_{2^d}/R_{2^d} *the upper group* of $BRW^0(2^d, +)$.

For $g \in N$, define $C_{R\ mod\ R'}(g) := \{x \in R | [x, g] \in R'\}$, $B(g) := Z(C_{R\ mod\ R'}(g))$ and let $A(g)$ be some subgroup of $C_{R\ mod\ R'}(g)$ which contains R' and complements $B(g)$ modulo R', i.e., $C_{R\ mod\ R'}(g) = A(g)B(g)$ and $A(g) \cap B(g) = R'$. Thus, $A(g)$ is extraspecial or cyclic of order 2. Define $c(d) := dim(C_{R/R'}(g))$, $a(g) := \frac{1}{2}|A(g)/R'|$, $b(g) := \frac{1}{2}|B(g)/R'|$. Then $c(d) = 2a(d) + 2b(d)$.

Corollary 9.2. Let L be any $\mathbb{Z}$-lattice invariant under $H := BRW^0(2^d, +)$. Then H contains a subgroup $K \cong AGL(d, 2)$ and L has a linearly independent set of vectors $\{x_i | i \in \Omega\}$ so that there exists an identification of Ω with $\mathbb{F}_2^d$ which makes the $\mathbb{Z}$-span of $\{x_i | i \in \Omega\}$ a permutation module for $AGL(d,2)$ on Ω.

Proof. In H, let E, F be maximal elementary abelian subgroups and let K be their common normalizer. It satisfies $K/R \cong GL(d,2)$. Now, let z generate $Z(R)$ and let E_1 complement $\langle z \rangle$ in E and F_1 complement $\langle z \rangle$ in F. The action of K on the hyperplanes of E which complement $Z(R)$ satisfies $N_K(E_1)F = K, N_F(E_1) = Z(R)$. Now consider the action of $N_K(E_1)$ on the hyperplanes of F which complement $Z(R)$. We have that $K_1 := N_K(E_1) \cap N_K(F_1)$ covers $N_K(E_1)/E$. Therefore, $K_1/Z(R) \cong GL(d,2)$. Let K_0 be the subgroup of index 2 which acts trivially on the fixed points on L of E_1, a rank 1 lattice. So, $K_0 \cong GL(d,2)$. Let x be a basis element of this fixed point lattice. Then the semidirect product $F_1{:}K_0$ is isomorphic to $AGL(d,2)$ and $\{x^g | g \in F_1\}$ is a permutation basis of its $\mathbb{Z}$-span. □

Definition 9.3. We use the notation of 9.1. An element $x \in N$ is *dirty* if there exists g so that $[x,g] = xz$, where z is an element of order 2 in the center. If g can be chosen to be of order 2, call x *really dirty* or *extra dirty.* If x is not dirty, call x *clean.*

Lemma 9.4. *Let $\mathbb{F}_2^{2d}$ be equipped with a nondegenerate quadratic form with maximal Witt index. The set of maximal totally singular subspaces has two orbits under $\Omega^+(2d,2)$ and these are interchanged by the elements of $O^+(2d,2)$ outside $\Omega^+(2d,2)$.*

Proof. This is surely well known. For a proof, see [GrElAb]. □

Definition 9.5. An involution in $BRW^+(2^d)$ has *defect k* if its commutator space on the Frattini factor of the lower group has dimension $2k$. The defect is an integer in the range $[0, \frac{d}{2}]$. Note that an automorphism of R_{2^d} has even dimensional commutator space on $R_{2^d}/Z(R_{2^d})$ if and only if it is even; see [GrMont], [GrElAb].

Definition 9.6. An involution in $BRW^+(2^d)$ is *split* if it centralizes a maximal elementary abelian subgroup of R_{2^d}, and is otherwise *nonsplit.*

Notation 9.7. Write $R = D_1 \dots D_d$ as a central product of dihedral groups, D_i of order 8. The involution $\alpha_{d,r}$ in $Aut(BRW^+(2^d))$, defined up to conjugacy, acts trivially on $d-r$ of the D_i and performs an outer automorphism on the other r of them. When $r = 2k$ is even, $\alpha_{d,2k}$ is represented in $BRW^+(2^d)$ by an involution $\eta_{d,2k,+}$ (see 9.13). In case $r = 2k < d$, we define an involution $\eta_{d,2k,-} := \eta_{d,2k,+}z$, where z is a noncentral involution in the above product of the $d-r$ elementwise fixed D_i.

Theorem 9.8. *We use the notation of 9.1, 9.3. Let $g \in N$. Then $Tr(g) = 0$ if and only if g is dirty. Assume now that g is clean and has finite order. Then $Tr(g) = \pm 2^{a(g)+b(g)}\eta$, where η is a root of unity. If $g \in BRW(d,+)$, we may take*

$\eta = 1$. Furthermore, every coset of R in $BRW(d,\varepsilon)$ contains a clean element and if g is clean, the set of clean elements in Rg is just $g^R \cup -g^R$.

Proof. [GrMont]. □

Lemma 9.9. *Suppose that t, u are involutions in $\Omega^+(2d, 2)$, for $d \geq 2$. Suppose that their commutators on the natural module $W := \mathbb{F}_2^{2d}$ are totally singular subspaces of the same dimension, e. Suppose that $e < d$ or that $e = d$ and that $[W, t]$ and $[W, u]$ are in the same orbit under $\Omega^+(2d, 2)$. Then t and u are conjugate.*

Proof. Induction on d. □

Corollary 9.10. *Suppose that t, u are clean involutions in H so that $Tr(t) = Tr(u) \neq 0$. Then t and u are conjugate in G_{2^d}, if their common defect is less than $\frac{d}{2}$. If the defects are $\frac{d}{2}$, then there are two classes.*

Proof. We may assume that t, u are noncentral. These involutions are not lower and have the same dimension of fixed points on $R/R' \cong \mathbb{F}_2^{2d}$. Let $T, U \leq R$ be their respective centralizers in R. Since both t, u are clean, $[R, t]$ and $[R, u]$ are elementary abelian subgroups of T, U, respectively. From 9.9, we deduce that Rt and Ru are conjugate in G_{2^d} if their common defect is less than $\frac{d}{2}$ and there are two possible conjugacy classes in case of common defect $\frac{d}{2}$. We may assume that $Rt = Ru$. Now use 9.8 to deduce that t is R-conjugate to u or $-u$. The trace condition implies that t is conjugate to u. □

Remark 9.11. The extension $1 \to R_{2^d} \to G_{2^d} \to \Omega^+(2d, 2) \to 1$ is nonsplit for $d \geq 4$. This was proved first in [BRW2], then later in [BE] and in [GrEx] (for both kinds of extraspecial groups, though with an error for $d = 3$; see [GrDemp] for a correction). The article [GrEx] gives a sufficient condition for a subextension $1 \to R_{2^d} \to H \to H/R_{2^d} \to 1$ to be split, and there are interesting applications, e.g. to the centralizer of a 2-central involution in the Monster [Gr72]. A general discussion of exceptional cohomology in simple group theory is in [GrNW].

Lemma 9.12. *Let $V = \mathbb{F}_2^{2d}$ have a nonsingular quadratic form, q, of plus type. Let W be an isotropic subspace, $U := W^{\perp}$. Then every nontrivial coset of U contains singular and nonsingular vectors if $d > 1$.*

Proof. Suppose that $v + U$ is a coset which consists entirely of either singular or nonsingular vectors. Then for all $x, y \in v + U$, $q(x + y) = (x, y) + q(x) + q(y) = (x, y)$. Take $a, b \in U$ so that $a + b = x + y$. Then $(x, y) = q(a + b) = q(a) + q(b) + (a, b)$. Also $(x + a, y + a) = (x, y)$ implies that $0 = (x, a) + (a, y) = (x + y, a) = (a + b, a) = (a, b)$. It follows that for any two elements a, b of U, $(a, b) = 0$. Since U is the annihilator of W, $U = W$. Let $Z := \{x \in W | q(x) = 0\}$, a subspace of W of codimension 0 or 1. Suppose $d > 1$. Let $x \in V \setminus W$. If there is $z \in Z$ so that $(x,z)=1$, then x and $x+z$ have different values under the quadratic form. If this fails to be so, then $dim(Z)=0$, i.e., $d=2$ and W contains nonsingular vectors. Then x annihilates a nonsingular vector, $w \in W$ and so x and $x+w$ have different values under the quadratic form. □

Lemma 9.13. *Let $V = \mathbb{F}_2^{2d}$ and let g be an involution in $\Omega^+(2d,2)$ so that $[V,g]$ has dimension $r > 1$ and contains nonsingular vectors. There exists a basis of singular vectors $x_1, \dots, x_d, y_1, \dots y_d$ so that $(x_i, y_j) = \delta_{ij}$ and g interchanges x_i and y_i for $i = 1, \dots, r$ and fixes each x_j, y_j for $j \geq r+1$.*

Proof. Let W be the codimension 1 subspace of $[V,g]$ which contains all the singular vectors of $[V,g]$. Take a basis u_i, $i = 1, \dots, 2k$, of $[V,g]$ of nonsingular vectors. For $x \in [V,g]$, let $P(x) := \{v \in V | v(g-1) = x\}$, a coset of $[V,g]^\perp$. For all x, $P(x)$ contains singular vectors (see 9.12). We therefore may take x_1 so that $x_1(g-1) = u_1$ and we define $y_1 := x_1^g$. We may use induction on $span\{x_1, y_1\}^\perp$. The only problem might be that we are unable to use 9.12 at the last stage in case $r = \frac{d}{2}$. But then we use the fact that V has plus type and the conclusion is forced. □

Lemma 9.14. *(i) Suppose that t is a clean upper involution of G_{2^d}. Then the coset tR_{2^d} represents $s+1$ different conjugacy classes of involutions in G_{2^d}, where s is the number of orbits of $C_{G_{2^d}}(t)$ on the cosets of $[R,t]$ in $C_{R_{2^d}}(t)$ which contain involutions. We have $s=1$ if $k = \frac{d}{2}$ and $s=2$ if $k < \frac{d}{2}$. This gives respectively one and two dirty classes of involutions in the coset.*

(ii) If t is $\eta_{d,2k,\pm}$ (so is dirty and nonsplit), the coset tR_{2^d} represents one class of involutions if $k = \frac{d}{2}$, and two otherwise; all involutions in tR_{2^d} are dirty.

Proof. Exercise. □

Lemma 9.15. *(i) A defect k involution in $G_{2^d}/R_{2^d} \cong \Omega^+(2d,2)$ is represented in $BRW^+(2^d)$ by an involution, specifically, by either a clean involution of defect k, or the dirty nonsplit involution $\eta_{d,2k,+}$, for a unique integer $k \leq \frac{d}{2}$. Furthermore, for any d and positive $k \leq \frac{d}{2}$, both cases occur and are mutually exclusive.*

(ii) An eigenlattice of $\eta_{2,2,+}$ has an orthogonal basis, of norms 2, 4.

Proof. It is clear from a direct construction (or 3.26) and 9.14 that both cases occur and that they are mutually exclusive. Since G_{2^d} contains a natural central product of k natural $BRW^+(2^2) \cong W_{F_4}$ subgroups, it suffices to give a direct construction for the case $k = \frac{d}{2} = 1$, which we now do. Notice that for $d=2$, $BRW^+(2^2) \cong W_{F_4}$ contains two conjugacy classes of reflection (upper and clean, of defect 1, representing the two classes when $k = \frac{d}{2}$) and a nonsplit involution. Note that the product of two reflections for orthogonal roots has trace 0, so is dirty. There are two orbits of W_{F_4} on orthogonal pairs of roots, distinguished by root lengths, but the resulting products of two reflections represent only two classes: one class (for the pairs of equal length roots) and a second class for the case of unequal root lengths. The latter gives the upper class. For this case, we have an orthogonal set of vectors of norms 2 and 4 in a given eigenlattice, M, corresponding to orthogonal roots of different lengths. □

References

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

[BRW1] 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.

[BRW2] Beverly Bolt, T. G. Room and G. E. Wall, On the Clifford Collineations, Transform and Similarity Groups, II. Journal of the Australian Mathematical Society, 1961, 80-96.

[B] Beverly Bolt, On the Clifford Collineations, Transform and Similarity Groups, III; Generators and Relations, Journal of the Australian Mathematical Society, 2 1961/62, 334-343.

[Bour] N. Bourbaki, Élements de Mathématique, Groupes et algèbres de Lie, Chapitres 2 et 3, Diffusion C.C. L. S., Paris, 1972.

[BE] 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.

[Car] Roger Carter, Simple Groups of Lie Type, Wiley-Interscience, London (1972).

[CR] Charles Curtis and Irving Reiner, Representation Theory of Groups and Associative Algebras, Interscience, 1962.

[Dieud] Jean Dieudonne, La Géométrie des Groupes Classiques, Springer, Berlin Heidelberg New York, 1971.

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

[Gr72] 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.

[GrDemp] Robert L. Griess, Jr., On a subgroup of order $2^{15}|GL(5,2)|$ in $E_8(C)$, the Dempwolff group and $Aut(D_8 \circ D_8 \circ D_8)$, J. Algebra, 40, 1976, 271-279.

[GrElAb] Robert L. Griess, Jr., Elementary abelian subgroups of algebraic groups, Geometria Dedicata, **39**, 253-305, 1991.

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

[GrNW] Robert L. Griess, Jr., Sporadic groups, code loops and nonvanishing cohomology, J. Pure Appl. Algebra, 44, 1987, 191-214.

[GrMont] 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.

[G12] Robert L. Griess, Jr., Twelve Sporadic Groups, Springer Verlag, 1998.

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

[PO2^d] Robert L. Griess, Jr., Pieces of 2^d: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. 56 pages. To appear in Advances in Mathematics. ; see also

[PO2^dcorr] Robert L. Griess, Jr., Corrections and additions to " Pieces of 2^d: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. ", which will be posted on the author's web site and on arxiv.

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

[MS] Jesse MacWilliams and Neal Sloane, The Theory of Error Correcting Codes, North-Holland, 1977.

[McL] Jack E. McLaughlin, Some subgroups generated by transvections, Arch. Math. 18 (1969), 108-115.

[MH] Milnor and Husemoller, Symmetric Bilinear Forms, Ergebnisse der Mathematick und Ihrer Grenzgebiete, Band 73, Springer Verlag, New York, 1973.

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

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

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA
E-mail: rlg@umich.edu