Few-cosine spherical codes and Barnes-Wall lattices

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1109
rlg@umich.edu

revision, 15 October, 2007

Abstract

Using Barnes-Wall lattices and 1-cocycles on finite groups of monomial matrices, we give a procedure to construct tricosine spherical codes. This was inspired by a 14-dimensional code which Ballinger, Cohn, Giansiracusa and Morris discovered in studies of the universally optimal property. Their code has 64 vectors and cosines $-\frac{3}{7}, -\frac{1}{7}, \frac{1}{7}$. We construct the *Optimism Code*, a 4-cosine spherical code with 256 unit vectors in 16-dimensions. The cosines are $0, \pm\frac{1}{4}, -1$. Its automorphism group has shape $2^{1+8}{\cdot}GL(4,2)$. The Optimism Code contains a subcode related to the BCGM code. The Optimism Code implies existence of a nonlinear binary code with parameters $(16, 256, 6)$, a Nordstrom-Robinson code, and gives a context for determining its automorphism group, which has form $2^4{:}Alt_7$.

Contents

1 Introduction

A *spherical code* is a finite set of unit vectors in Euclidean space. A *cosine* of a spherical code is the inner product of distinct unit vectors in the code. Call a spherical code *n-cosine* if the inner products of distinct unit vectors form an n-set. When $n = 3$, we use the term *tricosine*.

We present a general existence criterion (2.7) for tricosine spherical codes, based on the unidefect concept (2.5). We record an infinite series of examples and some special ones in dimensions 14 to 16. The 14-dimensional one is isometric to a 64-point spherical code $\mathcal{BCGM}$, which which was discovered during a recent study of the universally optimal property. This code is discussed later in this introduction.

We construct and analyze the *Optimism Code*, a spherical 4-cosine code of 256 vectors which are 16-tuples of shape $(\pm\frac{1}{4}^{16})$. The Optimism Code can be used to derive all our special examples. Its existence depends on an easy result from group extension theory.

Our procedures involve several finite groups and their 1-cocycles (also called derivations; see (7.1)). The most important of these groups are subgroups of $BRW^+(2^4) \cong 2^{1+8}\Omega^+(8,2)$, the isometry group of the rank 16 Barnes-Wall lattice.

The Optimism Code has isometry group which is a nonsplit extension $2^{1+8}GL(4,2)$. We derive existence of a nonlinear binary Nordstrom-Robinson type code by taking signs of Optimism Code vectors. In this context, we easily prove that the automorphism group of this binary code is isomorphic to $2^4{:}Alt_7$. If we multiply the Optimism Code vectors by 2, we get a set of 256 minimal vectors of BW_{2^4}, the standard rank 16 Barnes-Wall lattice (which has 4320 minimal vectors). This set of norm 4 vectors spans BW_{2^4}. Such a linkage of a Nordstrom-Robinson type binary code and the rank 16 Barnes-Wall lattice was unexpected.

This article was inspired by the spherical code $\mathcal{BCGM}$ found by Brandon Ballinger, Henry Cohn, Noah Giansiracusa and Elizabeth Morris, while investigating the universally optimal property [7]. Their code has these properties:

BCGM1. $\mathcal{BCGM}$ has 64 unit vectors in dimension 14, two of which make angles with cosines $\{-\frac{3}{7}, -\frac{1}{7}, \frac{1}{7}\}$.

BCGM2. Its isometry group $\widetilde{H}$ has these properties:
(i) $O_2(\widetilde{H})$ is nonabelian of order 2^7, $O_2(\widetilde{H})' = Z(O_2(\widetilde{H}))$.
(ii) $\widetilde{H}/O_2(\widetilde{H}) \cong GL(3,2)$.
BCGM3. $\mathcal{BCGM}$ is an association scheme.

News of the $\mathcal{B}CGM$ code led us to think about connections with lattices. The rhythm of $\{-\frac{3}{7}, -\frac{1}{7}, \frac{1}{7}\}$ suggested the ZOPT property for the set of minimal vectors of Barnes-Wall lattices ($ZOPT$ is the property of a set of vectors that the absolute value of the inner product of any two members is zero or a power of 2 [14]; the gaps for the set $\{-\frac{3}{7}, -\frac{1}{7}, \frac{1}{7}\}$ of cosines suggested the gaps in inner products $\{-1, 0, 1\}$ for certain sets of norm 4 vectors in BW_{2^4}). The Barnes-Wall lattices were therefore considered a possible source of interesting spherical codes. To search for $\mathcal{BCGM}$ in this context, it seemed natural to look at BW_{2^4}, whose automorphism group is $BRW^+(2^4)$, which has shape $2_+^{1+8}\Omega^+(8,2)$ and contains many subgroups which look roughly like $\widetilde{H}$. We found a good subgroup and orbit of it on the minimal vectors of BW_{2^4} which was used to make a spherical code. The isometry of our code with $\mathcal{BCGM}$ follows from the recent uniqueness proof [1].

Notation and terminology follows that in [14] and [15]. The *cubi theory* of [15] is recommended (see Section 3, especially 3.21 ff.). A few techniques from group cohomology are collected in an appendix.

Table 1: Summary of our unidefect tricosine codes

(In row 1: $3 \le m \le d$, $2^m - 1$ is a Mersenne prime and k is some integer satisfying $1 \le k \le \lfloor \frac{d}{2} \rfloor$.)

Symbol	Dimension	Number of unit vectors	Cosines
$\mathcal{DSC}_{2^d-\ell,2^{d+m}}$	$2^d - \ell$, ℓ small	2^{m+d}	$\frac{-2^{d-k}-\ell}{2^d-\ell}, \frac{-\ell}{2^d-\ell}, \frac{2^{d-k}-\ell}{2^d-\ell}$
$\mathcal{NSC}_{16,64}$	16	64	$-\frac{1}{4}, 0, \frac{1}{4}$
$\mathcal{NSC}_{15,64}$	15	64	$-\frac{1}{3}, -\frac{1}{15}, \frac{1}{5}$
$\mathcal{NSC}_{14,64}$	14	64	$-\frac{3}{7}, -\frac{1}{7}, \frac{1}{7}$
$\mathcal{NSC}_{16,128}$	16	128	$-\frac{1}{4}, 0, \frac{1}{4}$
$\mathcal{NSC}_{15,128}$	15	128	$-\frac{1}{3}, -\frac{1}{15}, \frac{1}{5}$

Table 2: Summary of the Optimism Code

Symbol	Dimension	Number of unit vectors	Cosines
$\mathcal{O}C$	16	256	$-1, -\frac{1}{4}, 0, \frac{1}{4}$

1.1 Two viewpoints which guided our strategy

The first viewpoint is the observation that certain lattices are combinatorially very rich. One thinks of dense packings, families of equiangular lines associated to root lattices, notable rank 3 graphs embedded as sets of minimal vectors in the Leech lattice, etc.

The set of inner products in $\mathcal{BCGM}$ made us think of the ZOPT property of Barnes-Wall lattices. The resemblance hinted that some set of minimal vectors of BW_{2^4}, suitably modified, could become a spherical code like $\mathcal{BCGM}$.

The second viewpoint is that group theory could help find the desired code. One might try to find the right group and the right vector in 14-space so that the orbit would be a copy of the $\mathcal{BCGM}$ spherical code. The right group would be a group extension, of the form $GL(3,2)$ extended downwards by a normal 2-subgroup of order 2^7. There are many isomorphism types of such groups, and many low-dimensional representations of them. One needs more focus before heavy searching.

These two viewpoints strongly suggested a look inside the automorphism group of BW_{2^4}, which is isomorphic to $BRW^+(2^4) \cong 2^{1+8}_+\Omega^+(8,2)$, since this group contains many downward extensions of $GL(3,2)$ by 2-subgroups *and* the set of minimal vectors in BW_{2^4} is well-understood and satisfies the ZOPT property.

In conducting a search, we must consider aspects of $GL(3,2)$-actions on 2-groups. There are two frequently-studied permutation representations of $GL(3,2)$, the actions on its vector space $\mathbb{F}_2^3$ and on the dual space (these actions are not equivalent, but are related by an outer automorphism). For such actions, the orbits have lengths 1 and 7. In addition, we shall need to consider *transitive* actions of $GL(3,2)$ on a set of size 8. (recall that there is a well-known isomorphism $GL(3,2) \cong PSL(2,7)$, and that the $PSL(2,7)$ acts transitively on the 8-point projective line over $\mathbb{F}_7$). There is a transitive degree 8 permutation representation which is closely related to the above

actions on $\mathbb{F}_2^3$ and on the dual space. We consider the transitive action of the affine general linear group $AGL(3,2)$ on $\mathbb{F}_2^3$. The stabilizer of the origin is the above $GL(3,2)$. In a transitive permutation representation of a group, any two point stabilizers are conjugate. However, there is a subgroup of $AGL(3,2)$ which is isomorphic to $GL(3,2)$ but which does not stabilize a point. Its action on $\mathbb{F}_2^3$ is transitive. Existence of such a subgroup may be proved with degree 1 group cohomology.

For the goals of this paper, we begin by looking for subgroups of $BRW^+(2^4)$ which are downward extensions of $GL(3,2)$ by 2-groups and which have a transitive permutation representation of degree 64. A length 64 orbit of such a subgroup on the minimal vectors of BW_{2^4} could be used to define a code like $\mathcal{BCGM}$. As we consider such subgroups, we find that naive candidates do not meet our conditions for one reason or another (such as wrong orbit lengths or orbits having more than three cosines, which can happen if the extending 2-group is too large). Therefore, we are forced to consider more exotic subgroups. As in the last paragraph, cohomology is used to guide our choices, but the work is technically more difficult than with $GL(3,2)$.

For a discussion of exceptional nonvanishing cohomology in finite simple group theory, see [12]. We mention that degree 1 and 2 cohomology of $GL(d,2)$ on $\mathbb{F}_2^d$ is 0 for $d \geq 6$, so our procedures for $d \geq 4$ can not be copied for higher dimensional Barnes-Wall lattices.

Acknowledgements. We thank Henry Cohn for describing $\mathcal{BCGM}$ and explaining background. For useful consultations, we thank Eichii Bannai, Etsuko Bannai and Akihiro Munemasa. This work was begun at the Oberwolfach Mathematische Forschungsinstitut at the meeting 21-25 November, 2005, and was supported in part by grants NSA (NSA-H98230-05-1-0024) and NSF (DMS-0600854).

1.2 List of Notations and Definitions

$A.B$ means an extension of groups (A normal, giving quotient B).

$A{\cdot}B, A{:}B$ mean nonsplit, split extensions, respectively.

p^m means an elementary abelian p-group of rank m (p prime).

$O_p(G)$ means the largest normal p-subgroup of the finite group G (p prime).

$C_G(X), N_G(X)$ shall mean the centralizer, normalizer, respectively, in a group G of a subset X (subscript G may be omitted); this notation extends

to subsets X of a set on which G has a permutation representation.

$P(S)$ means the power set of the set S, considered as a vector space over $\mathbb{F}_2$, and $PE(S)$ means the subspace of even subsets of the finite set S.

The term *weight* refers to weight of a binary codeword, i.e., the cardinality of its support. We generally identify a binary codeword with its support and vector addition with the symmetric difference of subsets.

$Mon(n, \{\pm 1\})$ denotes the group of degree n monomial matrices with entries $0, \pm 1$ only.

Groups actions on sets and modules will be on the right, sometimes with exponential notation. The conjugate of x by y is $x^y = y^{-1}xy$ and the commutator of x and y is $[x, y] = x^{-1}y^{-1}xy$.

A module is *uniserial* if it has only one composition series.

A set S of vectors in $\mathbb{R}^n$ has the *ZOPT property* if for any $x, y \in S$, $(x, y) \in \{0, \pm 2^k | k = 0, 1, 2, \cdots\}$ (ZOPT stands for: zero or power of 2).

2 Unidefect criterion for a tricosine spherical code

We give a criterion for constructing tricosine spherical codes in (2.7). The cosines for a pair of minimal vectors in BW_{2^d} form the set $\{0, \pm\frac{1}{2}, \pm\frac{1}{4}, \cdots, \pm 2^{-\lfloor \frac{d}{2} \rfloor}\}$. The idea is to look for a subgroup of the isometry group of the Barnes-Wall lattice BW_{2^d} and an orbit of it on minimal vectors so that the set of cosines within the orbit is limited to three values, but the orbit is large enough to be interesting.

First, we need to sketch notation for the Barnes-Wall lattices, BW_{2^d}. This is taken from our recent article [14]. See also the classic articles [2], [5].

Notation 2.1. We take the rank 2^d Barnes-Wall lattice BW_{2^d} and the subgroup $G := BRW^+(2^d) \cong 2^{1+2d}_+\Omega^+(2d, 2)$ of the automorphism group, which for $d \neq 3$ is the full automorphism group. As in [14], we set $R := O_2(G) \cong 2^{1+2d}_+$. Let F be a sultry frame (this is an R-orbit of minimal vectors in BW_{2^d} [14]) and $\mathcal{B} \subset F$, an orthogonal basis of V, the ambient real vector space. We use indices $\{0, 1, \ldots, 2^d - 1\}$ to label the orthonormal basis $2^{-\frac{d}{2}}\mathcal{B} = \{v_0, v_1, \ldots\}$ and vector space $\Omega := \mathbb{F}_2^d = \{\omega_0, \omega_1, \ldots\}$. When A is a subset of Ω, write $v_A := \sum_{i \in A} v_i$. The group R is generated by two easily-described sets of involutions. One is the sign changes on F at indices

corresponding to affine hyperplanes and the second corresponds to translations of indices by elements of Ω.

For a subset A of Ω, let ε_A be the orthogonal transformation which takes each v_i to $\begin{cases} -v_i & i \in A \\ v_i & i \notin A \end{cases}$. In G, take the associated diagonal subgroup D and N its normalizer. The group D consists of all ε_A where A ranges over the Reed-Muller code $RM(2,d)$. Also we assume that $\mathcal{B}$ is chosen so that N is a semidirect product DP, for a group $P \cong AGL(d,2)$ of permutation matrices with respect to $\mathcal{B}$. We assume that the bijection $v_i \mapsto \omega_i$ is an equivariance respecting the identification $P \cong AGL(d,2)$.

Notation 2.2. We identify V with $\mathbb{R}^{2^d}$ by use of the orthonormal basis $v_i, i \in \Omega$ (2.1). We denote by v_Ω the all-1 vector $(1,1,1,\ldots,1,1)$. (If d is even, v_Ω is in the standard BW_{2^d}.) Finally, we suppose that Q is a subgroup of P and J a subgroup of D which is normalized by Q such that $-1 \notin J$.

Definition 2.3. A spherical code is a *diagonal code* if it is an orbit of v_Ω by a subgroup of the diagonal group D in a $BRW^+(2^d)$-group.

Definition 2.4. The *defect* of an involution $t \in G$ is the integer k so that $2^{2(d-k)}$ is the order of $C_{R/Z(R)}(t)$. We have $0 \le k \le \frac{d}{2}$ [14, 15]. The *defect* of a codeword $c \in RM(2,d)$ is the defect of the involution $\varepsilon_c \in G$. (We mention that the defect of a codeword c has another interpretation, the least number of codimension 2 affine subspaces needed to sum to an element of $c+RM(1,d)$). See [15] for a detailed discussion of defects of both an involution in G and of a codeword in $RM(2,d)$.)

The main properties we need here are that the weight of a defect k codeword is one of the values 2^{d-1} or $2^{d-1} \pm 2^{d-k-1}$, and the fact that every involution of G in a given coset of R has a common defect (this implies that defect is constant for any coset of $RM(1,d)$ in $RM(2,d)$). A codeword of weight $2^{d-1} \pm 2^{d-k-1}$ is *clean* and one of weight 2^{d-1} is *dirty*.

Definition 2.5. Call a function $f : Q \to J$ a *near-derivation* if the associated function $\bar{f} : Q \to J/[J \cap R]$ is a derivation, i.e., a 1-cocycle; see (7.1). The *strong unidefect condition* on the function $f : Q \to J$ is that there exists a fixed integer k, $1 \le k \le \frac{d}{2}$ so that for all $x \in Q$, $f(x) \in R$ or $f(x)$ is a defect k involution, i.e., has the form ε_A, where A is a defect k codeword. An alternate formulation is that there exists a fixed integer k, $1 \le k \le \frac{d}{2}$ so that every value of f has defect 0 or defect k.

The *unidefect condition* on f is that every nonidentity value of f is an involution of trace 0 or of the form ε_A, where A is a clean defect k codeword. This is weaker than the strong unidefect condition because it allows $f(x)$ to have defect not k as long as $f(x)$ has trace 0.

Remark 2.6. If $f : Q \to J$ is a near-derivation as in (2.5), one can define $Ker(f) := \{x \in Q | f(x) = 0\}$, but it may not be a subgroup. It is contained in $Ker(\bar{f})$, which is a subgroup since $\bar{f}$ is a derivation.

Proposition 2.7. *Let $f : Q \to J$ be a near-derivation (2.5). Assume that f satisfies the unidefect condition for defect k. Let $H := (J \cap R)\{f(x)x | x \in Q\}$ be the group containing $J \cap R$ which is associated to f; see (7.3).*

Then the orbit $v_\Omega H$ is a set of vectors of common norm 2^d for which the inner product of two distinct members is 0 or $\pm 2^{d-k}$. The length of this orbit is $|J \cap R||Q{:}Ker(\bar{f})|$ (see (7.4)).

Proof. Since H consists of isometries, every vector in $v_\Omega H$ has norm 2^d. Every coordinate of a vector in the orbit has value ± 1, so an inner product of two such vectors depends just on the set of coordinates where their coordinate values differ. Such a set is a codeword of weight $0, 2^{d-1} - 2^{d-k-1}, 2^{d-1} + 2^{d-k-1}$ or 2^d. The length of the orbit is the index of the stabilizer of v_Ω, which (since H consists of monomial matrices) is just $H \cap P$, the subgroup of H consisting of permutation matrices. We take $rf(x)x$, for $r \in J \cap R, x \in Q$ and ask when it is a permutation matrix. The condition is $rf(x) = 1$, i.e., $f(x) = r$. Such a pair r, x exists if and only if $x \in Ker(\bar{f})$. Therefore, $Ker(\bar{f}) = H \cap P$ is the stabilizer in H of v_Ω. $\square$

Remark 2.8. (i) When $f = 0$, the code is diagonal (2.3).

(ii) A change in cocycle values may change the cosines.

Definition 2.9. Suppose that S is a set of equal norm nonzero vectors in V and that W is a subspace of V so that every element of S has the same projection to $W^\perp$. Then S may be projected to W and rescaled to make a spherical code in W (excluding the exceptional case $S \subset W^\perp$). If S is n-cosine, then so is the projection. This process is called *reduction to W* and the resulting code is called the *reduction of S* or just the *reduced code*.

Proposition 2.10. *In the situation of (2.7), (2.9), let W be a subspace spanned by a subset of $\{v_i | i \in \Omega\}$ which contains all v_i moved by H. Then*

$W^\perp$ is spanned by a subset of those $v_i \in \Omega$ which are fixed by H. Denote $\ell := dim(W^\perp)$. The reduced spherical code has cosines in the set $\{\frac{-2^{d-k}-\ell}{2^d-\ell}, \frac{-\ell}{2^d-\ell}, \frac{2^{d-k}-\ell}{2^d-\ell}\}$.

Proof. The projections of any two vectors $x, y \in v_\Omega H$ to $W^\perp$ are the same: a single vector of norm ℓ. The projections of x and y to W have norm $2^d - \ell$ and these projections have inner product $(x, y) - \ell$. $\square$

Definition 2.11. A spherical code is called a *unidefect code* if it is created from an orbit by projecting and rescaling as in (2.9).

3 Diagonal codes

3.1 $\mathcal{DSC}_{2^d-\ell,2^{d+m}}$, for small ℓ

The technically simplest cases of (2.7) (small Q (2.2) and $f = 0$ (2.8)) can be interesting, as the following examples show.

Definition 3.1. Fix an integer $k > 0, k \leq \frac{d}{2}$. A subset Y of D is *defect $\{0, k\}$-pure* if every involution in it has defect 0 (i.e., is in the lower group R) or defect k.

It would be useful to find large pure *subgroups*.

Lemma 3.2. *Let $\langle g\rangle$ be a cyclic group of prime order $p > 2$. Define $m := min\{j > 0 | 2^j \equiv 1 (mod\ p)\}$. The group algebra $\mathbb{F}_2\langle g\rangle$ decomposes into a direct sum of indecomposable ideals $I_0 \oplus I_1 \oplus \cdots \oplus I_r$, where $r = \frac{p-1}{m}$ and $I_0 \cong \mathbb{F}_2$ and $I_k \cong \mathbb{F}_{2^m}$ as rings, for $k = 1, \cdots, r$.*

Proof. The group algebra is commutative and, by coprimeness $(p, 2) = 1$, is semisimple, so is a direct sum of finite fields. One indecomposable summand is just the span of $\sum_{i=0}^{p-1} g^i$. Let I be another indecomposable summand. Then the projection h of g to I is not the identity, so h generates a subgroup of order p in the group of units $I^\times$. Since h generates I as a ring, $I \cong \mathbb{F}_{2^m}$. A dimension count implies that $p = 1 + rm$. $\square$

Definition 3.3. *A family of diagonal codes associated to Mersenne primes.*

Let $p = 2^m - 1$ be a Mersenne prime and suppose that $3 \leq m \leq d$. Take $g \in P$ of order p and assume that g fixes v_0 (see (2.1)). For the action of $Q := \langle g\rangle$ on D, every irreducible constitutent has dimension 1 or m (3.2).

When $m = d$, there is a single nontrivial constituent in $D \cap R$ and $\frac{d-1}{2}$ of them in $D/D \cap R$ (reason: we may interpret the permutation matrix g as a linear transformation on the vector space Ω, where it fixes only the origin; the only subsets of Ω fixed by g are $\emptyset$, $\{\omega_0\}$, $\Omega \setminus \{\omega_0\}$ and Ω, and so $\emptyset$ and Ω are the only members of $RM(2,d)$ fixed by g).

Let J be a $\langle g \rangle$-invariant subgroup of D so that J fixes v_0, $J \cap R = C_{D \cap R}(v_0)$ and $J/J \cap R$ is a $\langle g \rangle$-irreducible module. Then $J \cap R$ has order 2^d and J has order 2^{m+d}. Since $\langle g \rangle$ acts transitively on the nontrivial elements of $J/J \cap R$, J is $\{0,k\}$-pure for some $k > 0$.

Now take the orbit $v_\Omega J$, which is in bijection with J so has 2^{m+d} elements (note that this orbit equals $v_\Omega \langle g \rangle J$ since the permutation matrices fix $v_\Omega = (1,1,1,\ldots,1)$). The inner product of v_Ω with any other member of this orbit is one of $0, \pm 2^{d-k}$. Transitivity implies the analogous property for every member of the orbit. Rescaling gives unit vectors with inner products $0, \pm 2^{-k}$.

In general, for an element $r \in D$ of the diagonal group, $(v\Omega, v_\Omega r)$ is just the trace of r. In particular $(v_\Omega, v_\Omega r) = 0$ for $r \in J \cap R, r \neq 1$.

Lemma 3.4. *Both $\pm 2^{d-k}$ occur as inner products in the situation of (3.3).*

Proof. We use the orthogonality relations for characters of J. Let χ denote the trace function for linear transformations on V (2.1). As remarked above, for $r \in J$, the inner product $(v_\Omega, v_\Omega r)$ is just $\chi(r)$.

Define $s := \sum_{y \in J} \chi(y)$. Then, $\frac{s}{2^{d+m}}$ is the multiplicity of 1 in $V|_J$, which is at least 1 since J fixes v_0 and is at most 1 since $V|_{J \cap R}$ affords the regular representation of $J \cap R$. So, $\frac{s}{2^{d+m}} = 1$, whence $s = 2^{d+m}$.

Let $h \in J \setminus R$. In $(J \cap R)h$, the number of clean elements is 2^{2k} [15], Prop. 3.32. These are the elements of the coset $(J \cap R)h$ for which the trace is nonzero. Suppose that p of these have trace 2^{d-k} and that q have trace -2^{d-k}. Then, $p + q = 2^{2k}$ and $2^{d+m} = s = \sum_{y \in J} \chi(y) = 2^d + (p-q)2^{d-k}(2^m - 1)$, whence $2^d(2^m - 1) = 2^{d+m} - 2^d = (p-q)2^{d-k}(2^m - 1)$. This implies that $(p-q)2^{-k} = 1$, or $p - q = 2^k$. Therefore $(p,q) = (2^{2k-1} + 2^{k-1}, 2^{2k-1} - 2^{k-1})$ and so both p and q are nonzero. $\square$

Corollary 3.5. *The spherical codes of (3.3) have three cosines.*

Notation 3.6. The spherical code of (3.3) is denoted $\mathcal{DSC}_{2^d,2^{m+d}} = \mathcal{DSC}_{2^d,2^{m+d};J,g}$. The notation $\mathcal{DSC}_{2^d-\ell,2^{m+d}} = \mathcal{DSC}_{2^d-\ell,2^{m+d};J,g,W}$ means a spherical code obtained by projecting $\mathcal{DSC}_{2^d,2^{m+d};J,g}$ to W, the orthogonal of an ℓ-dimensional space fixed pointwise by $J\langle g \rangle$ (for example, $span\{v_0\}$).

Example 3.7. Take $d = m = 5, p = 31$. We get a tricosine spherical code of 1024 elements in $\mathbb{Q}^{32}$ in which the set of nonzero inner products is either $\pm\frac{1}{2}$ or $\pm\frac{1}{4}$. One may project to a 31-space for another code with respective cosine set either $\{-\frac{17}{31}, -\frac{1}{31}, \frac{15}{31}\}$ or $\{-\frac{9}{31}, -\frac{1}{31}, \frac{7}{31}\}$.

Remark 3.8. (i) It is not obvious which k in the range $1 \leq k \leq \lfloor \frac{d}{2} \rfloor$ may occur this way.

(ii) The full isometry group of such a code could contain $J\langle g \rangle$ properly, e.g. (4.13) occurs here for $p = 7, m = d = 3$.

(iii) When $p = 7, d = 4$, there are several (possibly nonisometric) codes, all with defect 1.

4 Nondiagonal codes

We construct nondiagonal spherical codes in dimension 14 through 16 using 1-cocycle theory for the simple group $GL(3, 2)$ and some of its extensions acting on various sections of the diagonal group, D. We need more detailed notation for the index set $\Omega \cong \mathbb{F}_2^4$, the Reed-Muller codes and the Barnes-Wall lattice BW_{2^4}. For example, a direct sum decomposition $\mathbb{F}_2^4 \cong \mathbb{F}_2^3 \oplus \mathbb{F}_2^1$ will determine a $GL(3, 2)$-subgroup of $P \cong AGL(4, 2)$. We shall use variations of this idea.

Notation 4.1. We continue to use the notation of (2.1) for $d = 4$. Let W be the annihilator of $W_{01} := span\{v_0, v_1\}$. We take the subgroup $E \cong 2^3$ of $D \cap R$ which is trivial on W_{01}. Let $P_{\{01\}} \cong 2 \times 2^3{:}GL(3, 2)$ be the subgroup of $P \cong AGL(4, 2)$ which stabilizes $\Omega_{\{01\}} = \{\omega_0, \omega_1\}$ and $P_{0,1}$ the subgroup which fixes both ω_0 and ω_1. It has the form $P_{0,1} = UQ$, where $Q \cong GL(3, 2)$ and $U := O_2(P_{0,1}) \cong 2^3$.

We take B_0 to be an affine hyperplane of Ω which contains ω_0 but not ω_1 and let $B_1 := \Omega \setminus B_0$, an affine hyperplane of Ω which contains ω_1 but not ω_0. We choose Q to stabilize B_0 and B_1. Let p_{01} be the involution which generates $Z(P_{\{01\}})$. It corresponds to translation from ω_0 to ω_1.

We use the Reed-Muller codes $RM(r, 4)$ spanned by affine subspaces of Ω of codimension r. Let S_i be the subspace of $P(\Omega)$ which is spanned by all affine codimension 2 subspaces which are contained in B_i. Then $dim(S_i) = 4$ for $i = 0, 1$, $S_0 \cap S_1 = 0$, $RM(2, 4) \geq S := S_0 + S_1 \geq RM(1, 4) \geq S_{01} := C_S(p_{01})$, $dim(RM(2, 4)) = 11$ and $dim(S_0 + S_1) = 8$.

Define $T_i := \{A \in S_i | \omega_i \notin A\}$, a dimension 3 subspace of S_i, for $i = 0, 1$. Let $F_i := \{\varepsilon_A | A \in T_i\} \cong 2^3$. Define $T_{01} := C_{T_0+T_1}(p_{01}) = \{x + x^{p_{01}} | x \in T_0\}$.

For $\{i, j\} = \{0, 1\}$, define $D_i := \langle \varepsilon_A | A \in PE(B_i), \omega_i \notin A \rangle \cong 2^6$. The groups D_i are not contained in $Aut(BW_{2^4})$ (in fact, $D_i \cap Aut(BW_{2^4}) = F_i, i = 0, 1$) but the diagonal group $D_{01} := C_{D_0 \times D_1}(p_{01})$ is in $Aut(BW_{2^4})$. The corresponding subspace of $PE(B_0) \oplus PE(B_1)$ is denoted $B[01]$, so that $D_{01} = \{\varepsilon_A | A \in B[01]\}$. Moreover, $J := F_0 F_1 D_{01} = C_D(\{v_0, v_1\})$ is an index 4 subgroup of D. Also, $E = D_{01} \cap J$.

The action of Q fixes the S_i and T_i and Q normalizes the F_i and D_{01}, so that $J = F_i \times D_{01}$ as Q-modules, for $i = 0, 1$. Note that $C_D(Q) = \langle \varepsilon_{B_0}, \varepsilon_{B_1} \rangle = \langle \varepsilon_{B_0}, -1 \rangle$ so that, as Q-modules, $D = J \times C_D(Q)$ (and the first direct factor may be decomposed).

Lemma 4.2. *$dim(H^1(Q, F_i)) = 1$ for $i = 1, 2$, $dim(H^1(Q, J/E)) = 1$ and $dim(H^1(Q, J)) = 2$.*

Proof. See (7.6), (7.8). Use the fact that J is the module direct sum of F_i and D_{01}. □

4.1 $\mathbb{F}_2[GL(3,2)]$-modules

Notation 4.3. Call the irreducible $\mathbb{F}_2[GL(3,2)]$-modules $\mathfrak{3}, \mathfrak{3}'$, $\mathfrak{1}$ and $\mathfrak{8}$ (the number indicates dimension and the prime indicates duality) [19], [3]. We inflate this notation to $\mathbb{F}_2 Q$-representations. Let us say that $\Omega \cong \mathbb{F}_2^4$ as a Q-module has composition factors $\mathfrak{1}, \mathfrak{3}$.

Lemma 4.4. (i) $U \cong E \cong \mathfrak{3}'$.

(ii) $T_0 \cong T_1 \cong \mathfrak{3}'$.

(iii) $F_0 \cong F_1 \cong \mathfrak{3}'$.

(iv) $D_0/F_0 \cong D_1/F_1 \cong J/F_0F_1 \cong \mathfrak{3}$.

Proof. (i) If we take ω_0 as an origin, U is in $\mathbb{F}_2$-duality with the quotient space $\Omega/\{\omega_0, \omega_1\}$.

(ii) The first isomorphism is realized by the action of p_{01}. For the second, note that T_1 may be identified with linear functionals on Ω which have $\{\omega_0, \omega_1\}$ in their kernel.

(iii) Consider the definition of F_i.

(iv) First, note that each D_i/F_i is in duality with T_i. Secondly, note that each D_i/F_i covers J/F_0F_1. □

4.2 Good subgroups of shape $2^3.GL(3,2)$

We now study a family subgroups of the form $2^3.GL(3,2)$ and the defects associated to their involutions. Certain ones will satisfy a unidefect condition.

Notation 4.5. We continue to use the notation of (4.1). We form the semidirect product JQ and consider $\mathcal{G} := \{H | E \leq H \leq JQ, H/E \cong GL(3,2)\}$. This set has cardinality 256 and is a union of four orbits under J or JQ, by (4.4), (4.2). Each orbit is represented by a 1-cohomology class of Q with coefficients in J/E. By (2.4), if $H \in \mathcal{G}$, the involutions of $H \setminus E$ have constant defect, 1 or 2. We call this defect the *defect of* $H \in \mathcal{G}$ (the involutions in E have defect 0). If γ is a near-derivation (2.5) associated to H, write $\gamma = \gamma_0\gamma_1$ to indicate the components with respect to the direct sum $F_i \times D_{01}$, for a fixed $i \in \{0,1\}$. Then γ_0 is a derivation and γ_1 is a near-derivation. Write $\bar{\gamma}_j$ for values of γ_j modulo E and $\bar{\gamma}$ for values of γ modulo E. Because of the correspondence of $H \in \mathcal{G}$ with the class of a near-derivation on Q, we may say that H has the unidefect property (2.5) if and only if such a near-derivation does.

Lemma 4.6. *Assume the notation as in (4.5). Then H splits over E if and only if $\bar{\gamma}_1$ is an inner derivation.*

Proof. The "only if" part is trivial. Assume $\bar{\gamma}_1$ is an inner derivation. Then H is conjugate by an element of D_{01} to F_iEQ modulo F_i, which is split over E. □

Remark 4.7. For each $H \in \mathcal{G}$, the orbit $\frac{1}{4}v_\Omega H$ is a spherical code whose set of cosines depends on H. We get its cardinality from (2.7) and the observation that the stabilizer in H of v_Ω is just $H \cap P$. In the notation of (4.5), $H \cap P = H \cap Q = Ker(\bar{\gamma}_0) \cap Ker(\bar{\gamma}_1)$. The derivation kernels can have indices 1, 7 or 8 in Q and $Ker(\bar{\gamma}_0) \cap Ker(\bar{\gamma}_1)$ can have indices 1, 7, 8, 42 or 56.

Note that the orbit lengths depend on actual cocycles and not just cohomology classes. We are looking for a code like $\mathcal{BCGM}$, so the case of interest is $|Q : Ker(\bar{\gamma}_0) \cap Ker(\bar{\gamma}_1)| = 8$, which means $Ker(\bar{\gamma}_0) = Ker(\bar{\gamma}_1)$ is a Frobenius group of order 21. Derivations on irreducible 3-dimensional modules with such kernels are outer and furthermore are associated to nonsplit extensions (4.6).

Finally, we comment that the orbit corresponding to a split extension contains groups of defects 0 and 1 only.

Lemma 4.8. *Suppose that $\bar{\gamma}_0$ and $\bar{\gamma}_1$ have the same kernel and $\bar{\gamma}$ takes a nontrivial value which has defect $k \geq 1$. Then all nontrivial values of $\bar{\gamma}$ have defect k and so Q, γ, J satisfy the unidefect k condition.*

Proof. We have $K := Ker(\bar{\gamma}) = Ker(\bar{\gamma}_0) = Ker(\bar{\gamma}_1)$ is isomorphic to Sym_4 or a Frobenius group of order 21. The action of Q on the cosets of K is doubly transitive. Now use (7.5)(iv). □

Lemma 4.9. *Both unidefect 1 and 2 subgroups occur in $\mathcal{G}$. In particular, the class with both components (4.5) noninner has a unidefect 2 subgroup H^* which furthermore has orbit length $|v_\Omega H^*| = 64$.*

Proof. A near-derivation $Q \to J$ whose values lie in one of the F_i is a derivation. If nontrivial, the derivation takes values which are involutions of defect 1 (because all nonzero codewords of T_i have weight 4). A member of $\mathcal{G}$ with $\bar{\gamma}_1$ trivial has defect 1 or 0.

Consider the case $\bar{\gamma}_1$ nontrivial and $\bar{\gamma}_0$ trivial. Every weight in $B[01]$ is divisible by 4 and all codewords in $B[01] \setminus RM(1,4)$ have defect 1. Therefore, γ has unidefect 1.

Suppose $\bar{\gamma}_1$ noninner and $\bar{\gamma}_0$ noninner. Assume further that $Ker(\bar{\gamma}_0) = Ker(\bar{\gamma}_1)$, whence both are Frobenius groups of order 21 (7.7)(ii). This equality does occur for some groups in this orbit. We shall demonstrate explicitly such a γ which takes value in $E\varepsilon_Y$, for a 6-set Y.

Fix an involution $t \in Q$.

Note that on $B_0 \setminus \{v_0\}$, the action of the involution $t \in Q$ has a pair of length 2 orbits, hence on $PE(B_0 \setminus \{v_0\})$ has 2-dimensional commutator space, M. Let $\{a, a'\}$ and $\{b, b'\}$ be the nontrivial orbits of t. Then $\{a, a'\}, \{b, b'\}$ span M and the 1-space $M \cap T_0$ is the span of $\{a, a', b, b'\}$, an affine 2-space.

There are fixed points d, e of t on $B_0 \setminus \{v_0\}$ so that $\{a, a', d, e\}$ is an affine 2-space (so is in T_0 (4.1)).

Similarly, b, b' is contained in $\{b, b', d, e\}$, an affine 2-space which is the sum of the two previous affine 2-spaces.

Let f be the remaining fixed point. The 4-set $\{a, a', d, f\}$ is congruent to $\{e, f\}$ modulo $span(\{a, a', d, e\})$. Both these sets are fixed by t.

Now define $u := e^{p_{01}}, v := f^{p_{01}} \in B_1$. The 6-set $Y := \{u, v, a, a', d, f\}$ is fixed by t and $Y = \{u, v, e, f\} + \{a, a', d, e\} \in B[01] + T_0 \leq RM(2,4)$. There exists a near-derivation γ so that $\gamma(t) = \varepsilon_Y$ (see (7.10)(ii), applied to $B[01]/T_{01}$ and T_i). Now use (4.8). □

Corollary 4.10. *There are $H \in \mathcal{G}$ which have unidefect 2. For such H, let γ be an associated near-derivation. Every element of H has the form rq, where q is a permutation matrix and $r \in D$ effects sign changes at no coordinates, or at a clean codeword of defect 2 (of weight 6 or 10) or at a midset (weight 8). The values of γ outside R have defect 2. The extension $1 \to E \to H \to GL(3,2) \to 1$ does not split. There exists a particular such H, called H^*, so that p_{01} normalizes H^* and satisfies $[H^*, p_{01}] = O_2(H^*)$*

Proof. All is clear except possibly for the nonsplitting. For that point, we use (4.6), (7.7)(ii) and the fact that $Ker(\bar{\gamma}_0) = Ker(\bar{\gamma}_1)$ is a Frobenius group of order 21. □

Corollary 4.11. *Suppose that S is a subgroup of DQ which is isomorphic to $2^3.GL(3,2)$. Then $S \in \mathcal{G}$.*

Proof. Since S covers $DQ/D \cong Q$, $S \cap R = E = [D \cap R, Q]$. If we write $D = C_D(Q) \times J$, then $DQ = JQ \times C_D(Q)$. Since $S = [S,S]$, $S \leq JQ$, and so $S \in \mathcal{G}$. □

4.3 Existence of $\mathcal{NSC}_{16,64}$, $\mathcal{NSC}_{15,64}$ and $\mathcal{NSC}_{14,64}$

Notation 4.12. Let $H^* \in \mathcal{G}$ be a unidefect 2 group, as in (4.10). Then $v_\Omega H^* = v_\Omega \langle p_{01}, H^* \rangle$ has cardinality 64.

Let π be the orthogonal projection $V \to W$ and ρ the orthogonal projection $V \to v_0^\perp$. We define spherical codes $\mathcal{NSC}_{16,64}$, $\mathcal{NSC}_{15,64}$, $\mathcal{NSC}_{14,64}$ as the vectors of the respective orbits $v_\Omega H^*$, $(v_\Omega H^*)\rho$ and $(v_\Omega H)\pi$, scaled to be unit vectors in 16-, 15- and 14-dimensional space.

Theorem 4.13. *(i) The set of cosines for $\mathcal{NSC}_{16,64}$ is $\{0, \pm\frac{1}{4}\}$.*
(ii) The set of cosines for $\mathcal{NSC}_{15,64}$ is $\{-\frac{1}{3}, -\frac{1}{15}, \frac{1}{5}\}$.
(iii) The set of cosines for $\mathcal{NSC}_{14,64}$ is $\{-\frac{1}{7}, -\frac{3}{7}, \frac{1}{7}\}$.

Proof. (2.10). □

4.4 Existence of $\mathcal{NSC}_{16,128}$ and $\mathcal{NSC}_{15,128}$

We get larger tricosine codes in two of the three previous situations by increasing the groups slightly.

Recall the definitions of B_0 and B_1 (4.1). Consider, in BW_{2^4}, the sign change isometry ε_{B_0}, where $\omega_0 \notin B_0$ and $\omega_1 \in B_0$.

Notation 4.14. We increase H^* to $H^{**} := H^*\langle \varepsilon_{B_0}\rangle$. Since $[H^*, \varepsilon_{B_0}] \leq E$, the dihedral group $\langle p_{01}, \varepsilon_{B_0}\rangle$ normalizes H^* but ε_{B_0} does not normalize the group $H^*\langle p_{01}\rangle$ of (4.10). Denote by $\mathcal{NSC}_{16,128}$ the spherical code in $\mathbb{R}^{16}$ obtained by scaling the elements of $v_\Omega H^{**}$ to unit length. Denote by $\mathcal{NSC}_{15,128}$ the reduced spherical code in $\mathbb{R}^{15}$ obtained projecting $v_\Omega H^{**}$ to $v_0^\perp$, then rescaling to unit length.

Theorem 4.15. *(i) $\mathcal{NSC}_{16,128}$ has cardinality 128 and cosines $\{-\frac{1}{4}, 0, \frac{1}{4}\}$;*
(ii) $\mathcal{NSC}_{15,128}$ has cardinality 128 and cosines $\{-\frac{1}{5}, -\frac{1}{15}, \frac{1}{3}\}$.

Proof. As with H^*, use (2.7) and (2.10). Since H^* satisfies the strict 2-unidefect condition, so does H^{**}, which is created from H^* by replacing E with the slightly larger lower group $E\langle \varepsilon_{B_0}\rangle$. □

Remark 4.16. (i) The automorphism group of $v_\Omega H^{**}$ excludes p_{01} (or else $-1 = [p_{01}, \varepsilon_{B_0}]$ would be an automorphism, which would enlarge the cosine set to include -1).

(ii) Projection to the 14-space W does not seem to give a tricosine code.

5 Computations

We outline a straightforward computational method for finding our unidefect spherical codes (2.7), and possibly new ones, by computer. Such a code is an orbit for a finite group H (some subgroup of the frame stabilizer $N = DP$ (4.1)), so is a union of orbits of any subgroup of H. We take the subgroup $H \cap P$, the subgroup of H consisting of permutation matrices. Since there are no signs in these matrices, orbits of this group could be relatively easy to compute if we have a convenient set of generators. For these codes, one may use an additional group $E \cong 2^e$ of sign changes at a space of codewords of $RM(1, d)$ such that E is normalized by $H \cap P$ (this group is relatively easy to work with since these represent sign changes at affine hyperplanes). We therefore look for a union of orbits of $E(H \cap P)$.

We consider the action of $E(H \cap P)$ on the set of all 2^d-tuples $\mathcal{A}$ of the form $(\pm 1, \pm 1, \ldots, \pm 1)$ with respect to the standard sultry frame. Also we have an action on $\mathcal{A}_0 := \mathcal{A} \cap BW_{2^d}$, which has cardinality $2^{1+d+\binom{d}{2}}$.

Procedure 5.1. Let $\mathcal{O}_i, i = 1, 2, \ldots$ be the orbits of $E(H \cap P)$. An easy computer program can list these explicitly and compute inner products involving two orbits. If only three different inner products occurs for some

union $\mathcal{O}_j \cup \mathcal{O}_{j'} \cup \ldots$ of two (or more!), this union (rescaled to unit length) gives a tricosine spherical code. Unlike in (2.7), there is generally no reason to expect a transitive group of isometries.

Remark 5.2. (i) A search for other codes could be done using other subgroups of N. Since the BW_{2^d} lattices contain vectors of shape $(1^X 0^{\Omega\setminus X})$, for codewords $X \in RM(2,d)$, variations of $\mathcal{A}$ and $\mathcal{A}_0$ may be tried.

(ii) One can check whether the codes created this way are association schemes by straightforward accounting of inner products (5.1).

6 The Optimism Code and a nonlinear $(16, 256, 6)$ binary code

We shall define the *Optimism Code* or *Opticode*, a 4-cosine spherical code in dimension 16 with 256 unit vectors. A byproduct is that we deduce the existence of a nonlinear binary code with parameters $(16, 256, 6)$ and determine its automorphism group. We furthermore deduce existence of a 64-point subcode with cosines $\{0, \pm\frac{1}{4}\}$, which gives another existence proof of $\mathcal{NSC}_{16,64}$.

There is a famous nonlinear binary code with parameters $(16, 256, 6)$, the Nordstrom-Robinson code. Existence of such a code has been given in several ways (see [21], [9]). There are references (e.g., in [8, 20]) to a 1973 uniqueness proof by S. L. Snover [24], but the proof seems to be unpublished. Recently, H. N. Ward announced a new uniqueness proof [25]. Our cocycle-style existence proof is probably new.

6.1 Near-derivations for $AGL(4,2)$ on $RM(2,4)$ and associated spherical and binary codes

In this subsection, we continue to use the general discussion of BW_{2^4} and subgroups of its standard frame group, starting with (4.1), but do not use the cohomology studies for $GL(3,2)$. Instead, we work with a much easier situation, involving degree 1 cohomology of $\mathbb{F}_2[GL(4,2)]$ on its 6-dimensional module. Applications to a tricosine spherical code and binary code follow easily.

The relevant modules are easy to describe as part of a general setting. Let Γ be an n-set with the natural action of Sym_n and let $Y := \mathbb{F}_2\Gamma$ be the permutation module. Define $\varepsilon : Y \to \mathbb{F}_2$ to be the map which sends a

linear combination $\sum_{\alpha\in\Gamma} c_\alpha\alpha$ of Γ to $\sum_{\alpha\in\Gamma} c_\alpha$, the sum of its coordinates. The only $\mathbb{F}_2 Sym_n$-submodules of Y are $Y_0 := Ker(\varepsilon)$ (dimension $n-1$) and Y_1, the span of $\sum_{\alpha\in\Gamma}\alpha$ (dimension 1). Then $Y = Y_0 \oplus Y_1$ if n is odd and Y is uniserial with Loewey series $Y > Y_0 > Y_1 > 0$ if n is even. The same is true for $Sym'_n = Alt_n$ if $n \geq 3$.

For our purposes, we need only the special result (6.1) (in which the 6-dimensional irreducible module Y_0/Y_1 for $GL(4,2) \cong Alt_8 \cong \Omega^+(6,2)$ is denoted by M).

Notation 6.1. Let M be the 6-dimensional irreducible module for $\mathbb{F}_2[GL(4,2)]$ which occurs in the tensor square of the standard 4-dimensional module. Then $H^1(GL(4,2), M)$ is 1-dimensional [22]. If X is the 8-dimensional permutation module for $GL(4,2) \cong Alt_8$, X is uniserial with Loewey factors $\mathbb{F}_2, M, \mathbb{F}_2$ and every derivation on M is inherited from a derivation on X.

Notation 6.2. We use the notation of (6.1) and identify $D/(D\cap R)$ as a subquotient of X. Let f be the near-derivation $P \to D$ whose associated derivation $\bar{f}$ to $D/(D\cap R)$ is identified with the derivation inherited from X whose kernel K is an $2^4{:}Alt_7$ subgroup of $2^4{:}Alt_8$ (in more concrete language, we suppose that the permutation module for Alt_8 has basis $e_1, \ldots, e_8$; then $\bar{f}$ is identified with the map which sends permutation g to $e_1 + e_{1g}$ modulo $\mathbb{F}_2(e_1+\cdots+e_8)$). The set of nontrivial cosets of $D\cap R$ contained in $Im(f)(D\cap R)$ forms an orbit of length 7 for the action of $K = Ker(\bar{f})$ (7.5).

We need to check that $Im(f)(D\cap R)$ has weights 0, 6, 8, 10, 16 only (i.e., 4 and 12 do not occur).

Lemma 6.3. *For the natural quadratic form on $RM(2,4)$, the radical is $RM(1,4)$. The action of $AGL(4,2)$ on $RM(2,4)/RM(1,4)$ induces the associated $\Omega^+(6,2)$ and has kernel the translation subgroup.*

Proof. The first part follows from the well-known annihilation results for Reed-Muller codes [20]. The rest follows for example from group orders. □

Corollary 6.4. *The weights in $Im(f)(D\cap R)$ are just 0, 6, 8, 10 and 16.*

Proof. Let K_0 be the stabilizer in K of a nontrivial coset of $D\cap R$ in the orbit of (6.2). Then $K_0/O_2(K_0) \cong Alt_6$. Such a coset in $D/(D\cap R)$ may be interpreted as a nonsingular vector in the sense of the natural nondegenerate quadratic form on $D/(D\cap R)$ (this is clear since the stabilizer of a singular

vector in the associated orthogonal group, which is isomorphic to $\Omega^+(6,2)$, has shape $2^4.3^2.2^2$ and so is solvable, whereas K_0 induces on $D/(D\cap R)$ a nonsolvable group of transformations, isomorphic to Alt_6). The natural quadratic form on Y_0 (see beginning of this subsection) takes $y \in Y_0$ to half its weight modulo 2. Therefore, the weights in such a coset of $D \cap R$ in the orbit of (6.2) are $2(mod\ 4)$. A weight in $RM(2,4)$ is either 0, 8 or a number of the form $2^{d-1} \pm 2^{d-k-1}$ for $d = 4$ and $k \leq \frac{d}{2} = 4$, so we must have $k = 2$ and $2^{d-1} \pm 2^{d-k-1}$ is 6 or 10.

The defects on involutions in a coset of $D \cap R$ in D are constant. Besides the cosets from the above orbit, the only other coset in $Im(f)(D \cap R)$ is $D \cap R$, in which weights 0, 8, 16 are represented. $\square$

Notation 6.5. We now let $\mathcal{OG}$ be the subgroup between $D\cap R$ and $N = DP$ (4.1) which corresponds to the near-derivation f as in (6.2). Then $\mathcal{OG}$ has shape $2^{1+8}_+ GL(4,2)$. Define $\mathcal{OC} := \frac{1}{4}v_\Omega \mathcal{OG}$. The stabilizer of v_Ω in $\mathcal{OG}$ is just $\mathcal{OG} \cap P \cong 2^4{:}Alt_7$. This code clearly has cardinality 256 and the minus signs occur with multiplicities equal to the weights of (6.4).

The binary code $\mathcal{BC}_{16,256,6}$ is defined to be the set of 256 binary vectors corresponding to the elements of $\mathcal{OC}$ as follows: if $a = (a_i) \in \mathbb{F}_2^{16}$ corresponds to $y = (y_i) \in \mathcal{OC}$, then $a_i = 0, 1$ according to whether $y_i = \frac{1}{4}, -\frac{1}{4}$, respectively.

Definition 6.6. We call $\mathcal{OG}$ the *Optimism Group* and $\mathcal{OC}$ the *Optimism Code*. For short, we say *Optigroup* and *Opticode*.

As in (2.1), for a subset A of Ω, $v_A = \sum_{i\in A} v_i$ (so that $v_\Omega = v_\Omega$).

Lemma 6.7. *(i) For any $B \subseteq \Omega$, $(v_\Omega, v_\Omega - 2v_B) = 16 - 2|B|$.*
(ii) Let X be an orbit for $D \cap R$ on $\mathcal{OC}$. Then $(X,X) = \{0, \pm 1\}$.
(iii) If X, Y are different orbits for $D \cap R$ on $\mathcal{OC}$, then $(X,Y) = \{\pm\frac{1}{4}\}$.

Proof. (i) We compute that $(v_\Omega, v_B) = |B|$ and so $(v_\Omega, v_\Omega - 2v_B) = 16 - 2|B|$.

(ii) This is clear since $v_\Omega - 2v_B$ is in the orbit of v_Ω if and only if B is a hyperplane or 0 or Ω, i.e., $B \in RM(1,4)$.

(iii) Let $x \in X, y \in Y$. We may assume by transitivity of $\mathcal{OG}$ that $x = \frac{1}{4}v_\Omega$. Then $y = \frac{1}{4}v_\Omega - \frac{1}{2}v_S$, where S has defect 2, whence S has weight 6 or 10 (weight 8 is impossible here since the number of clean elements in the coset $S+RM(1,4)$ is $2^{2k+1} = 2^5$, by [15], Prop. 3.32). Therefore, $(x,y) = \pm\frac{1}{4}$. Since $X = -X$, the result follows. $\square$

Definition 6.8. Let F be a sultry frame in BW_{2^d} and let $U_F := \{x \in BW_{2^d} | x \in \sum_{f\in F} 2^{-\lfloor \frac{d}{2} \rfloor + 1}\}$. This is a sublattice of index 2 in BW_{2^d} ([5, 2, 14]), called the *even sublattice of BW_{2^d} with respect to the sultry frame F.*

Lemma 6.9. *Let $d \geq 4$ and F a sultry frame in BW_{2^d}. Then $Aut(U_F)$ is the stabilizer of F in $Aut(BW_{2^d})$, a group of the form $2^{d+\binom{d}{2}}{:}AGL(d, 2)$.*

Proof. This follows since the set of minimal vectors v of U_F which satisfy $(v, U_F) \leq 2\mathbb{Z}$ is just F [5, 2, 14]. □

Corollary 6.10. *(i) The $\mathbb{Z}$-span of $2\mathcal{OC} + 2\mathcal{OC}$ is the even sublattice of the Barnes-Wall lattice BW_{2^4} (2.1) with respect to F, the standard sultry frame of all $(0^{15}, \pm 2^1)$.*

(ii) The $\mathbb{Z}$-span of $2\mathcal{OC}$ is BW_{2^4}.

(iii) $Aut(\mathcal{OC})$ is contained in $Stab_{Aut(BW_{2^4})}(F)$, where F is a frame as in (i). The shape of $Stab_{Aut(BW_{2^4})}(F)$ is $2^{11}{:}AGL(4, 2)$.

Proof. First, note that $2\mathcal{OC}$ is contained in our standard BW_{2^4}, as a set of minimal vectors. Denote by M the sublattice of BW_{2^4} spanned by $2\mathcal{OC}$ and let M_0 the sublattice of BW_{2^4} spanned by $2\mathcal{OC}+2\mathcal{OC}$. Since every element of $2\mathcal{OC}$ has inner product ± 1 with members of F, $|M : M_0| = 2$. Therefore, (i) implies (ii). A consequence of (ii) is that $Aut(\mathcal{OC})$ is contained in $Aut(BW_{2^4})$ and, by (i), is in the subgroup of it stabilizing the frame. So, both (ii) and (iii) follow from (i), which we now prove.

We let U_0 be the $\mathbb{Z}$-span of the standard sultry frame of all $(0^{15}, \pm 2^1)$ and let U be the associated even sublattice of BW_{2^4} (6.8).

We shall prove that M contains
(1.a) all v_B, for B an affine hyperplane;
(1.b) all $2v_B$ for all dimension 2 affine subspaces B;
(1.c) all $2v_B$ for all even sets B;
(1.d) some $2v_B$, for $|B|$ odd;
(1.e) all $2v_i, i \in \Omega$.

We shall use the following equation several times:

$$(*) \qquad v_{S_1} + v_{S_2} = v_{S_1+S_2} + 2v_{S_1\cap S_2}, \quad \text{for} S_1, S_2 \subseteq \Omega.$$

Let $X := \frac{1}{4}v_\Omega(D \cap R)$, the orbit containing the all-$\frac{1}{4}$ vector $\frac{1}{4}v_\Omega$ and the vectors obtained from it by changing signs at an index set in $RM(1, 4)$. Then $\{\frac{1}{2}v_\Omega + 2x' | x' \in X\}$, consists of all v_A, for $A \in RM(1, 4)$. This implies (1.a). Use (*) to get (1.b).

If Y is an orbit different from X, it follows that $\frac{1}{2}v_\Omega + 2y$, $y \in Y$, consists of v_S, where S has weight 6 or 10. Let S be such a 6-set and let H be any affine hyperplane. Then $S \cap H$ is even and $S + H \in RM(2,4)$ has defect 2, whence only weights 6, 10 are possible for $S + H$. Therefore the unordered pair $\{|S + H|, |S + H + \Omega|\}$ is $\{6, 10\}$ and the unordered pair $\{|S \cap H|, |S \cap (H + \Omega|)\}$ is $\{2, 4\}$. If S, H are as above and $|S \cap H| = 2$, then (*) implies that $2v_{S\cap H} \in M$. Since the group $(D \cap R)K \cong 2^4{:}Alt_7$ acts doubly transitively on coordinates and preserves M, (1.c) follows. (One may avoid using group action here with a counting argument.)

Let U_1 be the sublattice of U spanned by the vectors $2v_i$ and $v_A, A \in RM(1,4)$. Then $U_1/U_0 \cong RM(2,4)$. Note that if Z is an orbit of $D \cap R$ on $\mathcal{OC}$, then all elements of $2Z$ are congruent modulo U_1. The quadratic space $RM(2,4)$ has radical $RM(1,4)$. In the 6-dimensional nonsingular quadratic space $U/U_1 \cong RM(2,4)/RM(1,4)$, the 7 vectors $2Y + 2X + U_1$, for Y ranging over all $D \cap R$-orbits different from X, give mod 2 Gram matrix $(1 + \delta_{ij})$; see (6.7). This matrix has rank 6 (because the all-1 matrix is idempotent of rank 1). Therefore, these 7 vectors span U/U_1 and so

(**) $M_1 + U_1 = U$ where M_1 is generated by the set of v_A such that A a 6-set and $v_A \in M$.

Therefore, given a 6-set S as above, there exists a 6-set $T \in RM(2,4)$ so that $\frac{1}{2}v_\Omega\varepsilon_T$ is in $2\mathcal{OC}$ and $|S \cap T|$ is odd. Then (1.d) follows. At once, (1.c) and (1.d) imply (1.e). Since (1.a) and (1.e) imply that $U_1 \leq M$, (i) follows from (**). □

Corollary 6.11. *Let* $X := \frac{1}{4}v_\Omega(D \cap R)$. *Then* $Stab_{Aut(\mathcal{OC})}(X) = (D \cap R)K = RK = RK_0 \leq Aut(BW_{2^4})$.

Proof. From (6.10)(iii), $Stab_{Aut(\mathcal{OC})}(X)$ embeds as a subgroup of $Stab_{Aut(BW_{2^4})}(F)$ which contains $(D \cap R)K$. Since $Aut(\mathcal{OC})$ acts transitively on the set of $D \cap R$-orbits in $\mathcal{OC}$, $Stab_{Aut(\mathcal{OC})}(X)D/D$ is isomorphic to Alt_7. Since $Stab_{Aut(\mathcal{OC})}(X)$ contains $(D \cap R)K$, the Dedekind law implies that $(D \cap R)K \leq Stab_{Aut(\mathcal{OC})}(X) = (D \cap Stab_{Aut(\mathcal{OC})}(X))K$. Since $Stab_D(v_\Omega) = 1$, $D \cap Stab_{Aut(\mathcal{OC})}(X) = D \cap R$ and the result follows. □

Theorem 6.12. *The isometry group of the optimism code is just the optimism group* $\mathcal{OG}$, *of shape* $2^{1+8}_+GL(4,2)$.

Proof. Use (6.11) and the fact that $\mathcal{OG}$ is a subgroup of $BRW^+(2^4)$ and is transitive on the orbits of $(D \cap R)$. □

Proposition 6.13. *The isometry group of $\mathcal{BC}_{16,256}$ is isomorphic to $2^4{:}Alt_7$.*

Proof. The isometry group of this binary code embeds by coordinatewise action on V in $\mathcal{OG}$ as the subgroup $\mathcal{OG} \cap P$. This is just the subgroup of the monomial group $\mathcal{OG}$ stabilizing v_Ω. $\square$

Remark 6.14. For earlier determinations of the automorphism group of the Nordstrom-Robinson code, see [4], [9], [24].

6.2 $\mathcal{NSC}_{16,64}$ as subcode of the Optimism Code

We continue to use the notation of the previous subsection.

Notation 6.15. For distinct indices $i, j \ldots$, let $\mathcal{OG}_{ij\ldots}$ be the pointwise stabilizer in $\mathcal{OG}$ of each of the 1-spaces $\mathbb{Q}v_i$, $\mathbb{Q}v_j, \ldots$ and let $\mathcal{OG}_{[ij\ldots]}$ be the global stabilizer in $\mathcal{OG}$ of each of the 1-spaces $\mathbb{Q}v_i$, $\mathbb{Q}v_j, \ldots$. Thus, the quotient group $\mathcal{OG}_{[ij\ldots]}/\mathcal{OG}_{ij\ldots}$ induces a group of sign changes at each of the subspaces $\mathbb{Q}v_i$, $\mathbb{Q}v_j, \ldots$. Note that $\mathcal{OG}_{[i]}$ has shape $2^5.GL(4,2)$ and $\mathcal{OG}_{[ij]}$ has shape $2^5.2^3.GL(3,2)$.

We are interested in $H := \mathcal{OG}_{0,1}$, which has shape $2^3.2^3.GL(3,2)$. Note that $H \cap R = E$, the same group E used in Section 4 (4.1). Also, p_{01} fixes v_Ω and normalizes H; in fact, $[H, p_{01}] = E$. Finally, $H \cap K \leq P_{0,1} \cong 2^3{:}GL(3,2)$ and so (7.12) implies that $H \cap K$ is a subgroup of K isomorphic to $GL(3,2)$ and acting indecomposably on $\Omega \cong \mathbb{F}_2^4$, fixing the 1-space $\{\omega_0, \omega_1\}$.

Lemma 6.16. *The group H of (6.15) has shape $4^3{:}GL(3,2)$.*

Proof. The action of an element of order 7 in H on $O_2(H)$ forces $O_2(H)$ to be abelian by a standard Lie ring argument [10], since the two composition factors therein are isomorphic 3-dimensional modules (by commutation with p_{01}, for example).

We assume that $O_2(H)$ is elementary abelian, then derive a contradiction. Then $O_2(H)$ is completely reducible as a module for $H/O_2(H) \cong GL(3,2)$ (it is easy to prove with a minimal resolution [3] that $Ext^1(Y,Y) = 0$ for a 3-dimensional irreducible Y). We therefore may choose a subgroup $T \leq O_2(H)$ so that $T \cong 2^3$, $T \cap E = 1$ and T is normal in H.

Then H splits over $H \cap R = E$ since $T(H \cap K)$ is a complementing subgroup (see (6.15)). By Gaschütz's theorem [18], $\mathcal{OG}_0$, which has shape $2^4.GL(4,2)$, splits over $O_2(\mathcal{OG}_0)$, whence $\mathcal{OG}_0 \cong AGL(4,2)$.

On the other hand, consider a subgroup H_1 of H such that $H_1 \geq E = H \cap R$ and $H_1/E \cong GL(3,2)$ acts decomposably on Ω. Then $H_1 \in \mathcal{G}$ (4.11) and because H_1 is not contained in K, the kernel of the derivation f, H_1 has positive defect. Since f has defect 2, H_1 is isomorphic to the nonsplit extension $2^3{\cdot}GL(3,2)$ (4.10). This gives a contradiction since the nonsplit extension $2^3{\cdot}GL(3,2)$ does not embed in $AGL(4,2)$ (7.13).

We conclude that $O_2(H) \cong 4^3$. Existence of the subgroup $H \cap K \cong GL(3,2)$, explained above, implies the claimed factorization. $\square$

Definition 6.17. We define the spherical code $\mathcal{S} := \frac{1}{4}v_\Omega H$, where H is as in (6.15). The cosines are just $\{0, \pm\frac{1}{4}\}$. Its cardinality is $|H : H \cap P| = 64$. In fact, $O_2(H)$ acts regularly on $\mathcal{S}$.

Remark 6.18. (i) We may view H as the subgroup between E and $N_X(E)$ which corresponds to the near-derivation f restricted to the subgroup of P_0 (see (6.15)) which stabilizes the points ω_0 and ω_1, equivalently, which normalizes E. Therefore, $\mathcal{S}$ is identified with some $\mathcal{NSC}_{16,64}$, which was defined as $\frac{1}{4}v_\Omega H^*$, where H^* is a subgroup in (4.12) (reason: the cocycle f we used in (6.2) could have been used to define a suitable group H^* as in (4.12) since its values have the right weights).

(ii) This new realization of $\mathcal{NSC}_{16,64}$ has the advantage of exhibiting $H\langle p_{01}\rangle$, a larger group of isometries than $H^*\langle p_{01}\rangle$. Upon projection to 14-space W, we get a code like $\mathcal{BCGM}$.

(iii) Some of the group extensions occuring in this article appear in the context of [11].

6.3 Concluding Remarks

Remark 6.19. *Alternate constructions of the Optimism Code and a* $(16, 256, 6)$ *nonlinear binary code.* We take our spherical code $\mathcal{NSC}_{16,64}$ and the group $D \cap R \cong 2^5$. The new spherical code $\mathcal{NSC}_{16,64}(D \cap R)$ has 256 vectors and cosine set $\{0, \pm\frac{1}{4}, -1\}$. The binary code $\mathcal{BC}_{16,256,6}$ is a set of 256 binary vectors corresponding to the elements of $\mathcal{NSC}_{16,256}$ as follows: $a = (a_i) \in \mathbb{F}_2^{16}$ corresponds to $y = (y_i) \in \mathcal{NSC}_{16,256}$ by the rule $a_i = 0, 1$ according to whether $y_i = \frac{1}{4}, -\frac{1}{4}$, respectively. Finally, one may start with a Nordstrom-Robinson type binary code and reverse the previous procedure to define a spherical code.

Remark 6.20. *Spherical codes and energy.* It is clear that one can make many spherical codes in $\mathbb{R}^n$ by taking orbits of the all-1 vector by subgroups of the degree n monomial group $Mon(n, \{\pm 1\})$. One can get larger spherical codes as orbits by overgroups of such monomial groups, e.g. the optimism group is contained in a natural $2^{1+8}.Alt_9$ subgroup of $BRW^+(2^4)$. There are many candidates to try. It is not clear which are likely to be associated to universally optimal situations. Known examples involve exceptional objects as well as series (see the table on page 2 of [7]).

7 Appendix: Background on 1-cocycles and derivations

Definition 7.1. A *right 1-cocycle* or *right derivation* from the group X to the additive right X-module A is a function $f : X \to A$ so that $f(xy) = f(x) + f(y)^{x^{-1}}$ for all $x, y \in X$. A *1-coboundary* or *inner derivation* is such a function of the form $f(x) = a - a^{x^{-1}}$, for a fixed $a \in A$. A noninner derivation is sometimes called an *outer derivation*.

In case A is a multiplicative group, the derivation condition reads $f(xy) = f(x)f(y)^{x^{-1}}$ and the inner derivation condition reads $f(x) = aa^{-x^{-1}}$.

Remark 7.2. Assume that A is a module for a commutative ring, R. We observe that the set of 1-cocycles has a natural structure as an R-module. The set of 1-coboundaries is a submodule and the 1-cohomology group (the quotient of 1-cocycles by 1-coboundaries) has R-module structure. In this article, these objects are typically vector spaces over $R = \mathbb{F}_2$, so we may speak about their dimensions.

Proposition 7.3. *Let the group H be a semidirect product of normal abelian subgroup A by a complement X. The complements to A in H correspond to the 1-cocycles from X to A: if f is a 1-cocycle, the complement associated to it is $\{f(x)x | x \in H\}$. Two complements are conjugate by H (equivalently, by A) if and only if their corresponding 1-cocycles are cohomologous (i.e., their difference is a 1-coboundary).*

Proof. Classic. See for example [16], [18]. □

Definition 7.4. The *kernel* of a derivation as in (7.1) is $Ker(f) := \{g \in X | f(g) = 0\}$ (in the additive case) and $Ker(f) := \{g \in X | f(g) = 1\}$ (in the multiplicative case). It is a subgroup, though typically not normal.

Lemma 7.5. *Let $f : X \to A$ be as in (7.1). Let K be the kernel of the derivation f. Then*

(i) if $x, y \in X$, then $f(x) = f(y)$ if and only if $xK = yK$ (so, the left cosets of K are the level sets of the function f);

(ii) If $x \in K$, $f(xy) = f(y)^{x^{-1}}$; consequently, the values of f on the right coset Ky of K in X form a K-orbit in A.

(iii) The values of f on the double coset KxK, for $x \in X$, form a K-orbit on A, the orbit containing $f(x)$.

(iv) Suppose X acts doubly transitively on the cosets of K. Then the set of values of f is the disjoint union of $0 \in A$ with the K-orbit of values taken by f on the nontrivial double coset of K in X.

Proof. Easy work with the definition of derivation. For (i), set $a = xy, b = x$. Then $f(a) = f(b)f(b^{-1}a)^{b^{-1}}$. Consider the condition $aK = bK$. □

Proposition 7.6. *(i) $dim(H^1(GL(n, 2), \mathbb{F}_2^n)) = 0$ if $n \neq 3$;*

(ii) $dim(H^1(GL(3, 2), \mathbb{F}_2^3)) = 1$.

Proof. (i) and (ii) may be found in [17].

The result (ii) is well-known and follows trivially from modular representation theory, specifically the structure of projective indecomposable modules for $\mathbb{F}_2[GL(3, 2)]$. For a proof with resolutions, see [3]. For an elementary proof using the interpretation of complements modulo conjugacy, see [18] [13]. For another, see the proof of (7.8). □

Lemma 7.7. *Let $G \cong GL(3, 2)$ and M a 3-dimensional irreducible $\mathbb{F}_2G$-module.*

(i) If f is a nonzero inner derivation from G to M, then $Im(f)$ is a 7-subset of M containing 0. If $a \in M \setminus Im(f)$, then f is the inner derivation $x \mapsto a(1 - x^{-1})$.

(ii) If f is a noninner derivation, $Im(f) = M$. Also, $Ker(f) \cong 7{:}3$, the Frobenius group of order 21.

Proof. (i) Since f is inner, there is $a \in M$ so that $f(x) = a(1 - x^{-1})$. The kernel of f is the index 7 stabilizer of a ($a \neq 0$ since $f \neq 0$). Obviously there is no solution to $f(x) = a$. Now use (7.5)(i).

(ii) In this paragraph, we use the standard interpretation of $H^1(G, \mathbb{F}_2) \cong Ext^1_{\mathbb{F}_2G}(\mathbb{F}_2, M)$ by short exact sequences up to equivalence [16]. There is an indecomposable module, L, so that $M \leq L$ and $L/M \cong \mathbb{F}_2$. There is $a \in L$ so that $f(x) = a(1 - x^{-1})$ for all $x \in G$. Since f is noninner as a derivation

to M, $a \in L \setminus M$. The stabilizer K of a in G (equivalently, the kernel of the derivation f) must have even index, or by Maschke's theorem, L would be decomposable.

The kernel of f is a proper subgroup with index at most $|M| = 8$. The index is therefore 7 or 8. The last paragraph proves the index is not 7, and so we are done by (7.5)(i). $\square$

Proposition 7.8. *Let $G \cong GL(3,2)$ and let M be a 6-dimensional indecomposable module for $\mathbb{F}_2 G$ with two composition factors of dimension 3 which are duals of each other. Let S be the socle of M. Write $0 \to S \to M \to M/S \to 0$.*

Then

(i) $H^1(G, M)$ has dimension 1 and is the image of $H^1(G, S)$ under the map which comes from the inclusion $S \to M$;

(ii) Let $f : G \to M$ be a 1-cocycle. Either (a) the values of f are contained in S; or (b), the values of f are not contained in S and the kernel of f is contained in the index 7 subgroup of G which stabilizes a nonzero vector of M/S.

Proof. (i) Let H be a subgroup of index 7 in G. We point out that there are two conjugacy classes of such H. The shortest proof is to quote the classification of parabolic subgroups of the group $GL(3,2)$ of Lie type [6]. One can see representatives of these two conjugacy classes as the matrix subgroups $\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$ and $\begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$ of $GL(3,2)$. (One can also prove this with techniques from pure group theory. These groups are the normalizers of the two G-conjugacy classes of Klein four-groups in G [10]. The local fusion theory of Alperin settles conjugacy.)

One conjugacy class of four-groups is the set of pointwise stabilizers of hyperplanes in the natural module $\mathbb{F}_2^3$ for $GL(3,2)$ and the other conjugacy class is the set of pointwise stabilizers of hyperplanes in the dual of the natural module. Note that these conjugacy classes are fused under the action of an outer automorphism of $GL(3,2)$ (say, by the inverse-transpose).

We consider the $\mathbb{F}_2$-permutation module P on the cosets of such a subgroup H. Then P is isomorphic to the direct sum of a module, N, and the trivial module. The composition factors of N are $3, 3'$ (for example, by consideration of the Brauer characters). The module N is uniserial since H

fixes a nonzero vector in one of $3, 3'$ but not the other. Thus, N represents a nonzero element of Ext^1.

Since $dim(Ext^1(3, 3')) = dim(Ext^1(3', 3)) = 1$, the module M of the hypothesis is isomorphic to N or its dual N^*, which is obtained as a summand of the permutation module on the cosets of the other class of index 7 subgroups. So, it suffices to assume $M = N$.

We have $H^1(G, P) \cong H^1(H, \mathbb{F}_2)$ by the Eckmann-Shapiro lemma [16]. The right object has dimension 1 since $H \cong Sym_4$ and $H^1(H, \mathbb{F}_2) \cong Hom(H, \mathbb{F}_2)$. By additivity of the cohomology functor, $H^1(G, P) \cong H^1(G, N) \oplus H^1(G, \mathbb{F}_2)$ and the last summand is zero since it is isomorphic to $Hom(G, \mathbb{F}_2)$. This proves that $H^1(G, N)$ has dimension 1.

From the long exact sequence, we get $0 \to H^1(G, S) \to H^1(G, N) \to H^1(G, N/S) \to \ldots$. By dimensions, using the preceding paragraph and (7.6)(ii), we get the final statement.

Actually, we can prove (7.6)(ii) directly. Since S and N/S are related by an outer automorphism of G (see an earlier paragraph), these cohomology groups are isomorphic. Since the long exact sequence then proves that one has dimension 1, both have dimension 1.

(ii) We may assume that the values of f do not lie in S. By (i), the composition of f with the quotient modulo S is cohomologous to 0, i.e., there is $a \in M$ so that $f(x) - (a - ax^{-1}) \in S$ for all $x \in G$. Such an a is not in S. The kernel of f is therefore contained in the stabilizer in G of the nontrivial vector $a + S \in M/S$. $\square$

Lemma 7.9. *Suppose that $1 \to A \to E \to G \to 1$ is an extension of $G \cong GL(3, 2)$ by its standard module $A \cong \mathbb{F}_2^3$. Let A_1 be a maximal subgroup of A and let $C_1 := C_E(A)$. Then C_1 has order 2^5. If E does not split over A, then there is $B_1 \leq C_1, B_1 \cong 4^2$ and the elements of $C_1 \setminus B_1$ invert B_1 under conjugation.*

Proof. Such a nonsplit extension is unique and its structure is discussed in several places, e.g. [12]. We shall give a direct treatment here.

Let $N_1 := N_E(A_1)$. Then $N_1/C_1 \cong GL(2, 2) \cong Sym_3$. Let $h \in N_1$ have order 3. Then $C_A(h)$ has order 2 and h acts fixed point freely on the four-group C_1/A. It follows that C_1/A_1 is isomorphic to either $Quat_8$ or an elementary abelian group of order 8.

We claim that the case $Quat_8$ does not occur. Assume that it does. Then $A = [C_1, C_1], [A, C] = A_1$ and $C_1/A_1 \cong Quat_8$, which means that the Schur

multiplier of $Quat_8$ has order divisible by 4. It is well-known that $Quat_8$ has trivial Schur multiplier [18], a contradiction.

The claim implies that C_1/A_1 is isomorphic to an elementary abelian group of order 8 and that $C_1' = A_1$. The group $B_1 := [C_1, N_1]$ therefore has index 2 in C_1. So B_1 has order 16 and admits a fixed point free action by $\langle h \rangle$. Such a group must be abelian. The possibilities are that either B_1 is elementary abelian or $B_1 \cong 4^2$. Notice that $\langle h \rangle \times C_A(h)$ acts faithfully on B_1. In case $B_1 \cong 4^2$, the elements of $C_1 \setminus B_1$ invert B_1 under conjugation. In either case, $C_1 \setminus A$ contains involutions. Since G has one conjugacy class of involutions, every coset of A which has order 2 in E/A contains involutions.

Suppose that B_1 is elementary abelian. Let t be an involution in $N_E(B_1) \setminus O_2(N_E(B_1))$ (note that this set is a union of cosets of A, so that the last paragraph applies). Then t inverts h, an element of order 3 in $N_E(B_1)$, by the Baer-Suzuki theorem [10, 18]. The 2-dimensional irreducible module for $\mathbb{F}_2[Sym_3]$ is projective and injective, so B_1 has a splitting $A_1 \times A_2$ as modules for $\langle t, h \rangle$. Then $A_2\langle t \rangle \cong Dih_8$ meets A trivially. By Gaschütz's theorem [18], E splits over A.

If B_1 is not elementary abelian, $B_1 \cong 4^2$ and the second alternative holds. □

Lemma 7.10. *Let M be an irreducible 3-dimensional module for $\mathbb{F}_2G$, where $G \cong GL(3,2)$ and let H be an extension, so that M is normal in H and $H/M \cong G$.*

Then

(i) $Aut(H)$ is an extension of $Inn(H)$ by $\langle u \rangle$, where the involution u acts trivially on M and on H/M, so by commutation induces a noninner derivation from H/M to M;

(ii) $O_2(Aut(H))$ acts transitively on the two H-classes of involutions in $H \setminus M$; moreover, if t_1 and t_2 are involutions so that $Mt_1 = Mt_2$, there exists $g \in O_2(Aut(H))$ so that g takes t_1 to t_2 (more precisely, if $t \in G$ is in Mt_1, there exists a derivation $f : G \to M$ so that $f(t) = t_1t_2$).

(iii) If H is a split extension and $t \in H \setminus M$ is an involution, there exists a complement to M in H which contains t.

Proof. (i) Since $Aut(G)$ acts transitively on the two isomorphism types of irreducible 3-dimensional G-modules, $Aut(H)$ induces only $Inn(G)$ on $G \cong H/M$. Let R be $C_{Aut(H)}(H/M)$. Then R acts trivially on M, by absolute irreducibility of M. Then R is identified with the 1-cocycles from G to M,

which forms a 4-dimensional space, by (7.6) (the space of 1-coboundaries is 3-dimensional and so $dim(H^1(G,M)) = 1$ implies that the space of 1-cocycles is 4-dimensional). The subgroup $O_2(Aut(H)) \cap Inn(H)$ of R is isomorphic to M. We take an complement $\langle u \rangle$ in R to $O_2(Aut(H)) \cap Inn(H)$.

(ii) If H is a split extension, $H \setminus M$ contains involutions, and if it is nonsplit, the same is true, by [12], or (7.9).

By looking at Jordan canonical forms, one sees that $H \setminus M$ has two conjugacy classes of involutions. The kernel of an outer derivation is a Frobenius group of order 21. Therefore, an involution in $H \setminus M$ has, in its action on $O_2(Aut(H))$, all of its fixed points contained in $O_2(Aut(H)) \cap Inn(H)$, the subgroup of inner automorphisms coming from elements of M. It follows that the action of $Aut(H)$ on the conjugacy classes of H fuses the two classes of involutions in $H \setminus M$. In particular, any noninner automorphism fuses this pair of classes. Such an automorphism which is in $O_2(Aut(H))$ has the form $x \mapsto xg(x)$, for $x \in H$, where $g : H \to M$ is a derivation. Since g is constant on cosets of M, we may interpret g as a derivation on $H/M \cong G$. If we take such an automorphism which moves t_1 to t_2, then $g(t_1) = t_1 t_2$.

(iii) This follows from (ii). $\square$

Lemma 7.11. *$\mathfrak{3} \otimes \mathfrak{3}$ is uniserial and has composition factors $\mathfrak{3}', \mathfrak{3}, \mathfrak{3}'$; $\mathfrak{3}' \otimes \mathfrak{3}'$ is uniserial and has composition factors $\mathfrak{3}, \mathfrak{3}', \mathfrak{3}$; also, $\mathfrak{3} \otimes \mathfrak{3}' \cong \mathfrak{1} \oplus \mathfrak{8}$.*

Proof. Well known. We give a sketch here.

Since the group $G \cong GL(3,2)$ is small, its Brauer characters may be determined from elementary arguments about modular representation theory; or see [19], [3].

Now, $\mathfrak{3} \otimes \mathfrak{3}'$ and $\mathfrak{1} \oplus \mathfrak{8}$ have the same Brauer character, and since $\mathfrak{8}$ is a projective and injective module, $\mathfrak{3} \otimes \mathfrak{3}' \cong \mathfrak{1} \oplus \mathfrak{8}$. A second proof is to note that $\mathfrak{3} \otimes \mathfrak{3}' \cong End(\mathfrak{3}')$, so that the action of G may be interpreted as conjugation on the space of 3×3 matrices, and that the scalar matrices and the trace 0 matrices are left invariant.

For $\mathfrak{3}' \otimes \mathfrak{3}'$, the Brauer characters indicate that the composition factors are isomorphic to $\mathfrak{3}, \mathfrak{3}', \mathfrak{3}$. It suffices to prove uniseriality. This tensor product $T := \mathfrak{3}' \otimes \mathfrak{3}'$ clearly has an action of an involution t which switches the tensor factors and commutes with the action of G. Therefore, T has G-submodules $Ker(t-1)$, of dimension 6, and $Im(t-1)$ (contained in $Ker(t-1)$), dimension 3. Furthermore, $T/Ker(t-1) \cong Im(t-1)$ as G-modules. Since we are in characteristic 2, $Im(t-1) \cong \mathfrak{3}'$ (i.e., $x \mapsto x \otimes x$ is linear). It follows that $T > Ker(t-1) > Im(t-1) > 0$ is a composition series, with factors $\mathfrak{3}', \mathfrak{3}, \mathfrak{3}'$.

We claim that T is a cyclic module for G. Let a_1, a_2, a_3 be a basis for $A := 3'$. Define $a_4 := a_1 + a_2 + a_3$. Then any ordered 3-subset of a_1, a_2, a_3, a_4 is a basis of A and any permutation of a_1, a_2, a_3, a_4 extends to an invertible linear transformation on A. Set $c := a_1 \otimes a_2$. The G-submodule B of T which contains c contains $a_i \otimes a_j$ for all $i \neq j$. Furthermore, by acting with $g \in G$ which fixes a_1 and sends a_2 to $a_2 + a_1$, we see that the image of $g - 1$ contains $a_1 \otimes a_1$ and so B contains all $a_i \otimes a_i$. The claim follows.

Now, let $T > U > V > 0$ be any composition series for G. We now show that the terms are t-invariant. If U were not t-invariant, $Ut \neq U$ is a submodule and $T/(U \cap Ut)$ is isomorphic to the direct sum of two copies of the irreducible T/U. Such a module is not cyclic, a contradiction to the last paragraph. Therefore, $U = Ut$. If V were not t-invariant, $Vt \neq V$ are two submodules isomorphic to V, and so, by consideration of the composition factors, both are isomorphic to $3'$. Therefore, $T/(V + Vt) \cong 3$. This is a contradiction since T has a unique irreducible quotient and that quotient is isomorphic to $3'$.

This completes the proof of uniseriality for $3'$. A proof of uniseriality for 3 is similar to this one. □

Lemma 7.12. *Let $G \cong Alt_7$ act faithfully on $V := \mathbb{F}_2^4$.*

(i) An involution in G has Jordan canonical form a sum of two indecomposable degree 2 blocks.

(ii) Let H be the stabilizer in G of a nonzero vector. Then $H \cong GL(3,2)$ and H acts indecomposably on V with composition factors of dimensions 1,3.

(iii) Let H be the stabilizer in G of a codimension 1 subspace. Then $H \cong GL(3,2)$ and H acts indecomposably on V with composition factors of dimensions 1,3.

(iv) G contains just two conjugacy classes of subgroups isomorphic to $GL(3,2)$.

Proof. (i) If the conclusion is false, such an involution is a transvection (i.e., the identity plus a rank 1 nilpotent transformation). In $GL(4,2)$, the product of two transvections has order at most 4. In G, the involution (1,5)(2,4) inverts the 5-cycle (1,2,3,4,5) under conjugation, so the product of two involutions in G can have order 5. So, (i) holds.

(ii): First observe that G acts transitively on $V \setminus \{0\}$ since a 5-cycle has no fixed points (hence 3 orbits of length 5 on $V \setminus \{0\}$ and a 7-cycle has at least one orbit of length 7 (actually, it has two).

Second, H has index 15, hence order 168, and embeds in H_v, the point stabilizer in $GL(V)$ of a nonzero vector, say v. The shape of H_v is $2^3{:}GL(3,2)$. We claim that $H \cap O_2(H_v) = 1$. If false, H contains a nonidentity element of $O_2(H_v)$ which is a transvection, contradicting (i). It follows that the restriction of the quotient map $H_v \to H_v/O_2(H_v) \cong GL(3,2)$ to H is an isomorphism onto.

Thirdly, it is clear that V has an invariant 1-space under H and the quotient is a faithful irreducible 3-dimensional module. If V were decomposable as a direct sum of modules, the involutions of H would act as transvections on V since they act as transvections on $V/\mathbb{F}_2 v$. This contradicts (i) and completes the proof of (ii).

(iii): This follows from consideration of the dual module V^* for G.

(iv): Such a subgroup has irreducibles of dimensions 1,3 and 8 only, so on V, fixes a 1-space or a codimension 1 space. □

Lemma 7.13. *The nonsplit extension $2^3{\cdot}GL(3,2)$ does not embed in $AGL(4,2)$.*

Proof. Let $J \cong 2^3{\cdot}GL(3,2)$ and suppose that $J \leq K \cong AGL(4,2)$. Let $T := O_2(K)$ and $L \cong GL(4,2)$ a complement to T on K. Since J does not embed in $GL(4,2)$, by the classification of parabolic subgroups of $GL(4,2)$ [6], $J \cap T = O_2(J)$. Thus, JT/T is a subgroup of K/T which has a faithful module $V := \mathbb{F}_2^4 \cong T$. This action of J stabilizes a codimension 1 subspace corresponding to $O_2(J) \leq T$.

By the Dedekind law, $JT = T(J \cap L)$, which contains the subgroup $J \cap L \cong GL(3,2)$. The action of J on T by conjugation has a 3-dimensional submodule, $J \cap T$. Existence of the subgroup $J \cap L$ implies that $JT/J \cap T \cong 2 \times GL(3,2)$. Therefore, $J = [J,J] \leq [JT, JT]$, which has index 2 in JT and so $J = [JT, JT] = (J \cap T)(J \cap L)$ is a split extension, contradiction. □

References

[1] Eichii Bannai, Etsuko Bannai and Hideo Bannai, Uniqueness of Certain Association Schemes, European Journal of Combinatorics, online August, 2007.

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

[3] David Benson, Modular Representation Theory: New Trends and Methods, Lecture Notes in Mathematics, vol. 1081, Spring Verlag, Berlin 1984.

[4] E. R. Berlekamp, Coding theory and the Mathieu groups, Info. Control, 18 (1971).

[5] 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.

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

[7] Henry Cohn and Abinhav Kumar, Universally optimal distribution of points on spheres, to appear in Journal of the American Mathematical Society.

[8] G. David Forney, Jr., N. J. A. Sloane, Mitchell D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, Coding and quantization (Piscataway, NJ, 1992), 19–26, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 14, Amer. Math. Soc., Providence, RI, 1993. 94B05

[9] J.-M. Goethals, On the Golay binary perfect code, J. Combin. Theory, 11 (1971) 178-186.

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

[11] 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.

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

[13] Robert L. Griess, Jr., Twelve Sporadic Groups, Springer Monographs in Mathematics, 1998, Springer-Verlag.

[14] 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 See also: Corrections and additions to " Pieces of 2^d: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. " Advances in Mathematics, to appear.

[15] Robert L. Griess, Jr., Involutions on the 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.

[16] Karl W. Gruenberg, Cohomological Topics in Group Theory, Lecture Notes in Mathematics, vol 143, Springer-Verlag, 1970.

[17] Donald G. Higman, Flag-transitive collineation groups of finite projective spaces, Illinois Journal of Mathematics 6 (1962) 434-446.

[18] Bertram Huppert, Endliche Gruppen, I; Springer-Verlag, 1967.

[19] Jansen, Christoph; Lux, Klaus; Parker, Richard; Wilson, Robert An atlas of Brauer characters. Appendix 2 by T. Breuer and S. Norton. London Mathematical Society Monographs. New Series, 11. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1995. xviii+327 pp. ISBN: 0-19-851481-6 MR1367961 (96k:20016)

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

[21] A. W. Nordstrom and J. P. Robinson, An optimum nonlinear code, Info. and Control, 11 (1967) 613-616.

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

[23] N. V. Semakov and V. A. Zinov'ev, Complete and quasi-complete balanced codes, Problems of Info. Trans., 5(2) (1969) 11-13.

[24] Steven L. Snover, The uniqueness of the Nordstrom-Robinson code, Ph. D. Thesis, Department of Mathematics, Michigan State University, 1973.

[25] Harold N. Ward, A uniqueness proof for the Nordstrom-Robinson code, preprint 2007.