

GROUP CODING WITH COMPLEX ISOMETRIES

HYE JUNG KIM, J. B. NATION, AND ANNE V. SHEPLER

In memory of Wes Peterson.

ABSTRACT. We investigate group coding for arbitrary finite groups acting linearly on vector spaces. These yield robust codes based on real or complex matrix groups. We give necessary and sufficient conditions for correct subgroup decoding using geometric notions of minimal length coset representatives. The infinite family of complex reflection groups $\mathbf{G}(r, 1, n)$ produces effective codes of arbitrarily large size that can be decoded in relatively few steps.

1. INTRODUCTION

Permutation group codes originated in the 1950's in unpublished memos of David Slepian, who used the orbit of a point on a sphere under a group action as signals for communication. Slepian chose a group of permutations of coordinates and reversals of their signs acting on a finite-dimensional real vector space. He published this work in 1965 and extended the idea to arbitrary groups of isometries (see [1] and [2]). Ingemarsson [3] and Ericson [4] provide surveys of early work on group codes. Forney [5] considered codes in Euclidean space invariant under isometries. Recent applications of permutation codes to flash memory can be found in Jiang *et al.* [6, 7] and Barg and Mazumdar [8].

Slepian's original permutation group codes have been generalized to other real reflection groups (Coxeter groups); see Mittelholzer and Lahtonen [9] for a comprehensive account. Fossorier, Nation, and Peterson [10] developed a decoding method for group codes using a sequence of subgroups and coset representatives which yields efficient decoding of real reflection group codes. Properties of the length function (defined by simple reflections) and parabolic subgroup structure give effective codes based on Coxeter groups. Peterson asked what other groups might have an action that lends itself well to coding using these ideas.

Date: June 28, 2014.

2010 Mathematics Subject Classification. 94B60, 20G20.

Key words and phrases. group code, subgroup decoding, isometries, unitary groups, reflection groups, wreath products.

Results were presented at the RIMS Workshop on Combinatorial Structures and Information Theory in Ashikaga, Japan in August 2010. The last author was partially supported by NSF research grants #DMS-0800951 and #DMS-1101177.

In this article, we consider an arbitrary finite group \mathbf{G} acting linearly on a real or complex finite-dimensional vector space. We identify a set of messages with a finite set of vectors, *codewords*, closed under the action of the group. The codewords are simply the orbit under the group of some fixed initial vector \mathbf{x}_0 : each group element g in \mathbf{G} defines a codeword $g^{-1}\mathbf{x}_0$.

One sends a message by transmitting a codeword, but noise disturbs communication and the received vector may not be a codeword, nor even close to a codeword. We explore a technique called *subgroup decoding* that takes advantage of the abstract structure of the group, in addition to its explicit action on the vector space, to decode. Subgroup decoding uses a chain of nested subgroups,

$$\{I\} \subset \mathbf{G}_1 \subset \mathbf{G}_2 \subset \dots \subset \mathbf{G}_m = \mathbf{G},$$

to interpret the received vector as a codeword. Each element in the group has a unique factorization as a product $c_m c_{m-1} \dots c_1$ where each c_i lies in a fixed set of representatives for the left cosets of \mathbf{G}_{i-1} in \mathbf{G}_i . We argue that this factorization itself serves as an encoding of a message, and we explore how different choices of coset representatives and subgroup sequences affect decoding accuracy, efficiency, and error control.

To summarize two sample results, let us distinguish two levels of “correct decoding” and explain how coset representatives may distinguish themselves geometrically with respect to a given subgroup sequence. We say that an algorithm decodes *correctly with some noise* if there exists $\delta > 0$ such that a received vector \mathbf{r} decodes to a transmitted codeword \mathbf{w} whenever $\|\mathbf{r} - \mathbf{w}\| < \delta$. We say that an algorithm decodes *robustly* if a received vector \mathbf{r} always decodes to the nearest codeword \mathbf{w} (when a unique closest one exists). As the group is finite,

$$\text{robust decoding} \Rightarrow \text{correct decoding with some noise.}$$

A coset representative is called *minimal* (Definition 7) if the codeword it defines is closer to the initial vector \mathbf{x}_0 than any other codeword defined by its coset. A collection of representatives for the cosets of \mathbf{G}_{i-1} in \mathbf{G}_i is called *greed compatible* (Definition 11) if their inverses translate the Voronoi region of \mathbf{x}_0 for codewords defined by \mathbf{G}_i to a collection of sets covering the Voronoi region defined by \mathbf{G}_{i-1} . Note that the products $c_m c_{m-1} \dots c_{k+1}$, with each c_i in a fixed set of representatives for the left cosets of \mathbf{G}_{i-1} in \mathbf{G}_i , give a set of *induced coset representatives* for the cosets of \mathbf{G}_k in \mathbf{G} (see Lemma 18). The following two results (Theorem 15 and Corollary 22) summarize some of our findings.

Theorem A. *Let \mathbf{G} be any finite matrix group and choose any initial vector with full orbit and any sequence of nested subgroups. The subgroup decoding algorithm decodes correctly with some noise if and only if induced coset representatives are minimal.*

Theorem B. *Let \mathbf{G} be any finite matrix group and choose any initial vector and sequence of nested subgroups. If coset representatives are greed compatible, then the group decoding algorithm decodes robustly.*

This article analyzes properties that a finite group of matrices should exhibit for a successful group coding scheme. After outlining group coding in Section 2 and subgroup decoding in Section 3, we discuss the characteristics of an effective code in Section 4. Section 5 gives a quick background on reflection groups helpful for later examples. We use analogs of Weyl chambers and Voronoi cells for arbitrary isometry groups in Section 6 to define the fundamental region and decoding region. Section 7 establishes various geometric notions of minimal coset representatives analogous to minimal length representatives in the theory of Coxeter groups. We compare these various geometric notions of minimal coset representatives in Section 8. We prove that these geometric notions yield robust codes in Section 9 and give necessary and sufficient conditions for correct subgroup decoding in Section 10. Section 11 gives a result on controlling errors using group theory. Ties are discussed in Section 12 and techniques to improve the efficiency of decoding appear in Section 13.

These ideas are implemented for general wreath products (of an isometry group with a symmetric group) in Section 14. The wreath product construction allows one to build successful group codes of arbitrary size from a successful group code of small size. We apply our ideas by constructing and analyzing effective group codes built on the infinite family of complex reflection groups $\mathbf{G}(r, 1, n)$ in Section 15. These codes include previous codes based on the Coxeter groups Sym_n (the symmetric groups) and \mathbf{WB}_n (the hyperoctahedral groups). The family $\mathbf{G}(r, 1, n)$ offers group codes of arbitrarily large size with low decoding complexity that carry special geometric significance: For each $n, r > 1$, the group $\mathbf{G}(r, 1, n)$ is the symmetry group of a Platonic solid in n -dimensional complex space, the generalized r -cube or “cross polytope”. Note that with few exceptions (thirty-four, actually), every irreducible complex reflection group is some $\mathbf{G}(r, 1, n)$ or one of its subgroups.

Section 16 gives a few remarks on how the choice of initial vector influences subgroup decoding. We give data comparing several group codes and their complexity in Section 17. Subgroup decoding does not work as well for exceptional complex reflection groups as for wreath products, and we report on these findings in Section 17 before concluding with a few general remarks in Section 18. Note that the first author [11] has developed alternate decoding algorithms which have been refined by Walker [12] for exceptional complex reflection groups (also see [13]). Appendix I describes a general version of this alternate decoding scheme and gives a sufficient condition for correct decoding. Appendix II outlines a method to improve the performance of codes based on $\mathbf{G}(r, 1, n)$ using a proper subset of the orbit of the initial vector as the set of codewords.

Of course, there are other encoding/decoding schemes for group codes which could likely extend well to complex reflection groups. Besides the more traditional sorts of group decoding schemes using sorting algorithms, Hagiwara, Kong, and Wadayama (see [14, 15]) have introduced permutation codes with linear programming decoding. This seems to be a particularly interesting approach.

Note that any finite group of complex linear transformations acts by isometries with respect to some inner product. (One may just average an arbitrary inner product on the vector space over the finite group to produce one that is invariant under the group action.) We thus always work with an inner product that is preserved by the action of the given group \mathbf{G} . For example, $\|\mathbf{v} - g\mathbf{x}_0\| = \|g^{-1}\mathbf{v} - \mathbf{x}_0\|$ for any vector \mathbf{v} and any g in \mathbf{G} . After a possible change of basis, we may also assume this inner product is standard and that the finite group \mathbf{G} consists of unitary matrices.

We have attempted to make arguments amenable to both pure mathematicians and coding theorists.

2. GROUP CODING

We begin with the basic method of group coding before proceeding to more detailed algorithms. Mathematical readers should recall that the goal of coding is not encryption, but rather the efficient transmission or storage of information while resisting channel noise (corruption) and controlling errors. There is no explicit error correction involved in group coding; rather, one may superimpose a correction scheme after the received vector is decoded.

We fix a finite group \mathbf{G} of linear transformations of a finite dimensional vector space \mathbf{V} . To simplify notation, we assume \mathbf{V} is a complex vector space, and so we may assume \mathbf{G} consists of isometries (and thus unitary matrices with respect to a given basis). Our arguments extend to isometry groups over other spaces as well: We could just as well take \mathbf{V} to be a real vector space and \mathbf{G} a group of orthogonal matrices, or take \mathbf{V} to be a vector space over the division ring \mathbb{H} of real quaternions so that \mathbf{G} consists of unitary matrices over \mathbb{H} .

2.1. The code and codewords. Fix an *initial vector* \mathbf{x}_0 on the unit sphere in \mathbf{V} . We standardize the initial vector to length one by convention. The *code* is the orbit of the initial vector under the group \mathbf{G} ,

$$\mathbf{G}\mathbf{x}_0 = \{g\mathbf{x}_0 : g \in \mathbf{G}\},$$

and the points $g\mathbf{x}_0$ are called *codewords*. (More generally, coding theory often uses a subset of the orbit of \mathbf{x}_0 as the code; e.g., see Appendix II.)

2.2. Minimum distance. The initial vector \mathbf{x}_0 determines the *minimum distance* of the code defined with respect to the given \mathbf{G} -invariant inner product on \mathbf{V} :

$$d_{min} = \min_{b \notin \mathbf{S}a} \|a^{-1}\mathbf{x}_0 - b^{-1}\mathbf{x}_0\| = \min_{a \notin \mathbf{S}} \|a\mathbf{x}_0 - \mathbf{x}_0\|$$

where $\mathbf{S} = \text{Stab}_{\mathbf{G}}(\mathbf{x}_0)$ denotes the stabilizer subgroup of \mathbf{x}_0 . A large minimum distance is desirable for any coding scheme. However, an initial vector which yields the largest possible minimum distance for a particular group action may not give a code with the properties required for subgroup decoding (see Section 16). Thus there may be a trade-off between minimum distance and decoding efficiency.

2.3. Group coding scheme. A *group coding scheme* uses the following general method for encoding and decoding, without specifying the details of implementation.

Identify a set of messages \mathbf{M} with group elements using some correspondence, $\gamma : \mathbf{M} \rightarrow \mathbf{G}$. We send a message \mathbf{m} in \mathbf{M} to some receiver by transmitting the corresponding codeword,

$$\mathbf{x} = g^{-1}\mathbf{x}_0 \quad (\text{transmitted vector or coded message}),$$

where

$$g = \gamma(\mathbf{m}) \quad (\text{sent message}).$$

Interference may disrupt communication, and the received vector (which may no longer lie on the unit sphere) generally has the form

$$\mathbf{r} = \mathbf{x} + \mathbf{n} \quad (\text{received vector}),$$

where $\mathbf{n} \in \mathbf{V}$ represents channel noise. Ideally, \mathbf{r} will be close to \mathbf{x} , i.e., the distance $\|\mathbf{r} - \mathbf{x}\|$ will be small. The decoded vector \mathbf{x}' is the codeword closest to \mathbf{r} :

$$\mathbf{x}' \in \mathbf{G}\mathbf{x}_0 \text{ chosen so that } \|\mathbf{r} - \mathbf{x}'\| = \min_{g \in \mathbf{G}} \|\mathbf{r} - g\mathbf{x}_0\| \quad (\text{decoded vector}).$$

The decoded message is then a group element corresponding to the decoded vector:

$$g' \in \mathbf{G} \text{ chosen with } g'(\mathbf{x}_0) = \mathbf{x}' \quad (\text{decoded message}).$$

The received message is just the message corresponding to g' , i.e., $\mathbf{m}' = \gamma^{-1}(g')$. We suppress this dependence on some choice of γ .

In other words, the receiver decodes the sent message by finding a group element g' mapping the received vector \mathbf{r} as close as possible to the initial vector \mathbf{x}_0 :

$$\|g'\mathbf{r} - \mathbf{x}_0\| \text{ minimizes } \|a\mathbf{r} - \mathbf{x}_0\| \text{ over all } a \text{ in } \mathbf{G}.$$

The goal is to test relatively few group elements in the decoding process.

2.4. Ambiguity. Two natural ambiguities may arise with a group coding scheme. The scheme may not output a unique decoded message for each sent message because

- two different codewords may both be closest to \mathbf{r} , or
- a single codeword may be defined by two different group elements.

The first type of ambiguity occurs when the received vector \mathbf{r} lies exactly on some boundary (specifically, the boundary between two decoding regions; see Section 6). In practice, this occurs with zero probability and may be ignored. (This is not to be confused with the existence of *ties* arising when two codewords are the same distance from the initial vector; see Section 12.)

The second type of ambiguity must be addressed. We now explain how to work with respect to an isotropy group so that codewords and group elements can both stand for a fixed coded message without confusion.

2.5. Orbit of the initial vector. We say that the initial vector \mathbf{x}_0 has *full orbit* if the size of its orbit is the order of the group \mathbf{G} . If \mathbf{x}_0 does not have full orbit, then the isotropy (point-wise fixer) subgroup

$$\mathbf{S} = \text{Stab}_{\mathbf{G}}(\mathbf{x}_0)$$

of \mathbf{x}_0 in \mathbf{G} is nontrivial, and several group elements a will minimize the distance between $a\mathbf{r}$ and \mathbf{x}_0 . Indeed, if a and a' lie in the same right coset of \mathbf{S} (i.e., $\mathbf{S}a = \mathbf{S}a'$), then $a\mathbf{x}_0 = a'\mathbf{x}_0$ and

$$\|a\mathbf{r} - \mathbf{x}_0\| = \|a'\mathbf{r} - \mathbf{x}_0\| .$$

Thus, we say two group elements define *equivalent* messages if they lie in the same right coset of \mathbf{S} . We seek a decoding method that outputs messages equivalent to those sent.

Subgroup decoding works better and the theory is more transparent when \mathbf{x}_0 has full orbit. Since we have fixed a group of isometries (rather than fixing an abstract group and then choosing a representation, i.e., an action by isometries), we may always choose an initial vector with full orbit. (If \mathbf{G} is a reflection group, for example, we fix a vector \mathbf{x}_0 off a reflecting hyperplane.) So why have we chosen to keep track of \mathbf{S} (see Theorem 15) before emphasizing the case of initial vectors with full orbit? Some readers may wish to apply the theory of group coding presented here to arbitrary representations of a finite group (which may not be faithful). In fact, it is not customary in coding theory to always use an initial vector with full orbit, and indeed, some interesting codes arise from other choices (see [9, 10, 14]). In any case, a nontrivial isotropy subgroup \mathbf{S} is not an obstacle, as we may replace γ by a map from messages to representatives of right cosets of \mathbf{S} and define a left inverse map γ^{-1} that is constant on right cosets of \mathbf{S} .

3. SUBGROUP DECODING

The group coding scheme decodes a received vector by finding the closest codeword. When the group \mathbf{G} is finite but large, it is not efficient to loop through all of its elements to determine the closest codeword. There are various methods to organize the search, among which is the *basic subgroup decoding algorithm*, which we explain in this section.

3.1. Coset Leaders. For any nested subgroups $\mathbf{H} < \mathbf{K}$ of \mathbf{G} , we may fix a set $\text{CL}(\mathbf{K}/\mathbf{H})$ of coset representatives for the left cosets of \mathbf{H} in \mathbf{K} (i.e., the sets $a\mathbf{H}$ for a in \mathbf{K}) that includes the identity I of \mathbf{G} . These representatives are called *coset leaders* of \mathbf{K} over \mathbf{H} following traditional coding theory terminology. We fix a choice of coset leaders for consecutive pairs of subgroups in our sequence of nested subgroups.

3.2. Parameters. The parameters at our disposal for basic subgroup decoding are

- a finite group \mathbf{G} of isometries acting on the vector space \mathbf{V} ,
- an initial vector \mathbf{x}_0 with $\|\mathbf{x}_0\| = 1$,
- a sequence of nested subgroups

$$\{I\} = \mathbf{G}_0 < \mathbf{G}_1 < \mathbf{G}_2 \dots < \mathbf{G}_m = \mathbf{G}, \text{ and}$$

- coset leaders $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ for \mathbf{G}_k over \mathbf{G}_{k-1} .

For the remainder of the paper, the term *subgroup sequence* will always refer to a choice of nested sequence $\{I\} = \mathbf{G}_0 < \mathbf{G}_1 < \dots < \mathbf{G}_m = \mathbf{G}$.

3.3. Canonical Form. Recall that every element of g of \mathbf{G} has a unique expression as a product of coset leaders,

$$g = c_m \cdots c_1$$

with each c_k in $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$, giving a “canonical form” for group elements. The transmitted codeword corresponding to the coded message g thus can be written as

$$\mathbf{x} = g^{-1}\mathbf{x}_0 = c_1^{-1} \cdots c_m^{-1}\mathbf{x}_0.$$

The decoding algorithm seeks this factorization geometrically.

3.4. Subgroup decoding algorithm. Let $\mathbf{r} = \mathbf{x} + \mathbf{n}$ denote the received vector and set $\mathbf{r}_0 = \mathbf{r}$. Recursively, assume $\mathbf{r}_{k-1} = d_{k-1} \cdots d_1 \mathbf{r}$ is given at the k -th step, for some sequence of coset leaders $d_j \in \text{CL}(\mathbf{G}_j/\mathbf{G}_{j-1})$. Find a coset leader $d_k \in \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ that minimizes the distance $\|a\mathbf{r}_{k-1} - \mathbf{x}_0\|$ over all $a \in \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ and set $\mathbf{r}_k = d_k \mathbf{r}_{k-1} = d_k \cdots d_1 \mathbf{r}$. (If more than one coset leader yields the minimum distance, choose the first one in some ordering.) After m steps, the algorithm outputs the decoded message

$$g' = d_m \cdots d_1$$

corresponding to the decoded vector $(g')^{-1}(\mathbf{x}_0)$. If g' minimizes the distance $\|a\mathbf{r} - \mathbf{x}_0\|$ over all a in \mathbf{G} , then the decoding scheme decoded the received vector correctly.

One could test all coset leaders at each step of the subgroup decoding algorithm to find a minimizing coset leader, but we mention a more efficient method in Section 13 that works well for many groups (including real reflection groups, see [10]). One navigates recursively through a spanning tree of the coset leader graph, yielding a *standard subgroup decoding algorithm*.

4. EFFECTIVE DECODING

What does it mean for a decoding scheme to work effectively? It should decode correctly despite channel noise and implement practically. One can ask whether an algorithm

- (1) decodes correctly with no noise,
- (2) decodes correctly with some noise,
- (3) decodes robustly, i.e., always decodes to the nearest codeword,
- (4) controls error when noise is large, and
- (5) decodes in a reasonably small number of steps.

Together, these criteria give us a way to determine how well a given coding scheme works. We address these questions in order for the subgroup decoding algorithm.

4.1. Correct Decoding (with noise). Correct decoding occurs when the greedy algorithm produces a global minimum (of distance back to the initial vector \mathbf{x}_0) even though, at each stage of the algorithm, only coset leaders are tested for finding a local minimum. It is not clear that the initial vector and coset leaders always can be adjusted to ensure correct decoding after a subgroup sequence has been fixed. For example, see the code based on the exceptional complex reflection group \mathbf{G}_{25} in [11]. This explains why the conditions for decoding correctly with noise in Sections 9 and 10 are somewhat involved. Note that except for artificial examples, however, a decoding scheme that works with zero noise will decode correctly whenever the received vector is in some neighborhood of a codeword. See the results in Sections 9 and 10. For example, Corollary 22 gives necessary and sufficient conditions for correct decoding with some noise.

4.2. Robust Decoding. Robust decoding is of course desirable and implies correct decoding with some noise. But it is not always easy to verify robust decoding, while it is often straightforward to check that an algorithm decodes correctly with some noise. A sufficient condition for robust decoding is given in Theorem 15 and applied in Section 15 to the codes based on the groups $\mathbf{G}(r, 1, n)$.

4.3. Error Control. When noise is large, the received vector \mathbf{r} may lie closer to a codeword $h^{-1}\mathbf{x}_0$ than to the transmitted codeword $g^{-1}\mathbf{x}_0$. The algorithm then will output decoded message h instead of g when decoding correctly (up to equivalence by the isotropy subgroup of \mathbf{x}_0). We may control error even with large noise by choosing the correspondence γ between messages and group elements so that $\gamma^{-1}(g)$ and $\gamma^{-1}(h)$ do not differ much whenever $h^{-1}\mathbf{x}_0$ and $g^{-1}\mathbf{x}_0$ are close, at least with high probability. For the purposes of this paper, we will consider the message $\gamma(g)$ to be the actual sequence of coset leaders c_1, \dots, c_m such that $g = c_m \cdots c_1$. More generally, γ could be some function of this sequence, e.g., a bitstring determined by the coset leaders. (Each coset leader could determine a piece of a long

bitstring, for example.) Thus, when possible, we want to choose the coset leaders so that if $g = c_m \cdots c_1$ and $h = d_m \cdots d_1$ with $\|g^{-1}\mathbf{x}_0 - h^{-1}\mathbf{x}_0\|$ sufficiently small, then $c_i = d_i$ for almost all i , thereby controlling error when interference produces large noise. This is the effect of Theorem 30.

4.4. Number of steps. The complexity of encoding and decoding with a particular method can be analyzed by counting the number of operations in the algorithm (in some reasonable way). This is done explicitly for codes based on the groups $\mathbf{G}(r, 1, n)$ in Table 15.8.1 and for other group codes in Table 17.2.1. The use of subgroups and coset leaders allows us to break the decoding process into parts of manageable size and there are often natural candidates for the subgroup sequence, perhaps more than one. *Efficiency dictates that the subgroup sequence should be chosen so as to make the index $[\mathbf{G}_i : \mathbf{G}_{i-1}]$ of consecutive subgroups small.* That statement may be vague, but the principle is not: The efficiency of encoding and decoding is roughly proportional to the sum of the indices of the consecutive subgroups. For at each stage of decoding, one must choose a coset leader d_k from a collection of $[\mathbf{G}_{k-1} : \mathbf{G}_k]$ possibilities. Thus there are at most $\sum_{k=1}^n [\mathbf{G}_{k-1} : \mathbf{G}_k]$ steps to subgroup decoding, compared with $|\mathbf{G}| = \prod_{k=1}^n [\mathbf{G}_{k-1} : \mathbf{G}_k]$ steps needed to search through the whole group. Other techniques to make subgroup decoding more efficient are discussed in Section 13.

5. UNITARY GROUPS AND REFLECTION GROUPS

Before we explore subgroup decoding for the general case of an arbitrary complex matrix group \mathbf{G} , we take a brief interlude to recall some basic facts about reflection groups that may help the reader interpret examples appearing throughout the rest of the article. (Many of our remarks and examples will address real and complex reflection groups because of the wealth of interesting geometry they convey.)

The set of all $n \times n$ complex unitary matrices forms a group $\mathbf{U}(n)$, and the various groups we use for coding are contained in its infinite subgroup of monomial matrices (i.e., those with a single nonzero entry in each row and in each column) whose nonzero entries have norm 1. If $r \geq 1$ is an integer, the group $\mathbf{G}(r, 1, n)$ consists of monomial $n \times n$ matrices whose nonzero entries are r -th roots of unity. For any integer p dividing r , the group $\mathbf{G}(r, p, n)$ consists of those matrices in $\mathbf{G}(r, 1, n)$ whose nonzero entries multiply to an (r/p) -th root of unity. For example, $\mathbf{G}(2, 2, n)$ is the real Coxeter group \mathbf{WD}_n .

A *reflection* on a real or complex vector space is a nonidentity linear transformation that fixes a hyperplane in that space pointwise. Every reflection s satisfies

$$s(\mathbf{x}) = \mathbf{x} + l_H(\mathbf{x})\boldsymbol{\alpha} \text{ for all } \mathbf{x} \in \mathbf{V}$$

for some fixed vector $\boldsymbol{\alpha}$ in \mathbf{V} and some linear form l_H in the dual space \mathbf{V}^* that defines the reflecting hyperplane H fixed by s (i.e., $\ker l_H = H$). If s is an isometry, then s is the diagonal matrix $\text{diag}(\lambda, 1, \dots, 1)$ with respect

to some basis of V with $\lambda = \det(s)$ the nonidentity eigenvalue of absolute value 1. In particular, s has finite order if and only if λ is a root of unity. In this case, we may choose α to be a vector perpendicular to H (with respect to an s -invariant inner product $\langle \cdot, \cdot \rangle$ on \mathbf{V}) of length one and choose l_H to be the function

$$l_H(\mathbf{x}) = (\lambda - 1)\langle \alpha, \mathbf{x} \rangle \text{ for all } \mathbf{x} \in \mathbf{V}.$$

If s is a reflection on a real vector space, then $\lambda = -1$, and s is an involution.

A complex *reflection group* is a group generated by a set of reflections on $\mathbf{V} = \mathbb{C}^n$. We assume all reflection groups are finite and thus unitary with respect to the standard inner product. Real reflection groups (generated by reflections on \mathbb{R}^n) are called *Coxeter groups*; note that every real reflection group defines a complex reflection group after extending scalars. The finite irreducible complex reflection groups were classified in a classic paper of Shephard and Todd [17]: Every finite irreducible complex reflection group is

- (1) $\mathbf{G}(r, p, n)$ for some $r, p, n \geq 1$ with p dividing r , or
- (2) one of the exceptional groups denoted $\mathbf{G}_4, \dots, \mathbf{G}_{37}$.

The irreducible real reflection groups (acting orthogonally) are commonly designated as $\mathbf{W}A_n, \mathbf{W}B_n, \mathbf{W}D_n, \mathbf{W}E_6, \mathbf{W}E_7, \mathbf{W}E_8, \mathbf{W}F_4, \mathbf{I}_r(2), \mathbf{H}_3$ and \mathbf{H}_4 or some variant of this notation; see standard texts such as Grove and Benson [18], Humphreys [19] or Kane [20]. We are mainly interested in groups generalizing the infinite families $\text{Sym}_n = \mathbf{G}(1, 1, n)$ (the symmetric group acting by $n \times n$ permutation matrices), $\mathbf{W}B_n = \mathbf{G}(2, 1, n)$, and $\mathbf{W}D_n = \mathbf{G}(2, 2, n)$. These are often called *permutation groups* in the literature on group coding as they generalize the permutation group Sym_n .

6. FUNDAMENTAL REGIONS AND DECODING REGIONS

Recall that \mathbf{G} is an arbitrary finite group of complex matrices. We take an open Voronoi region (in complex space) to define an analog of a fundamental domain containing the trivial codeword \mathbf{x}_0 (see Forney [5]).

Definition 1. *The fundamental region of a subgroup $\mathbf{H} \leq \mathbf{G}$ is the set of vectors which are closer to \mathbf{x}_0 than to any other codeword in $\mathbf{H}\mathbf{x}_0$:*

$$\text{FR}(\mathbf{H}) = \{\mathbf{x} \in \mathbf{V} : \|\mathbf{x} - \mathbf{x}_0\| < \|h\mathbf{x} - \mathbf{x}_0\| \text{ whenever } h \in \mathbf{H} - \text{Stab}_{\mathbf{H}}(\mathbf{x}_0)\}.$$

Thus, the vectors in the fundamental region $\text{FR}(\mathbf{G})$ are precisely those that decode to I (or to a message equivalent to I) under correct decoding. Note that if $\|\mathbf{x} - \mathbf{x}_0\| < \frac{1}{2}d_{\min}$, then $\mathbf{x} \in \text{FR}(\mathbf{G})$. We likewise define a decoding region for each group element g to be the set of vectors that decode to g (or any message equivalent to g) under correct decoding:

Definition 2. *The decoding region of $g \in \mathbf{G}$ is the set of vectors that are closer to codeword $g^{-1}\mathbf{x}_0$ than to any other codeword:*

$$\text{DR}(g) = \{\mathbf{x} \in \mathbf{V} : \|g\mathbf{x} - \mathbf{x}_0\| < \|a\mathbf{x} - \mathbf{x}_0\| \text{ whenever } a \notin \mathbf{S}g\}$$

for $\mathbf{S} = \text{Stab}_{\mathbf{G}}(\mathbf{x}_0)$.

Thus an algorithm decodes robustly exactly when it decodes every vector in $\text{DR}(g)$ to a group element equivalent to g . Note that the decoding region for g is just a translate of the fundamental region for \mathbf{G} :

$$g \text{DR}(g) = \text{DR}(I) = \text{FR}(\mathbf{G}) .$$

Also note that the fundamental regions of subgroups of \mathbf{G} are nested in the reverse order: If $\mathbf{H} \leq \mathbf{K} \leq \mathbf{G}$, then $\text{FR}(\mathbf{H}) \supseteq \text{FR}(\mathbf{K}) \supseteq \text{FR}(\mathbf{G})$.

Remark 3. If \mathbf{x}_0 has full orbit, then no vector in \mathbf{V} fixed by a nonidentity group element lies in a decoding region. In particular, if \mathbf{G} is a real or complex reflection group, the decoding regions exclude vectors on reflecting hyperplanes. In fact, they give us an analog of (Weyl) *chambers*: If \mathbf{G} is a Coxeter group, then the fundamental region is just a fundamental chamber that contains \mathbf{x}_0 and the decoding region of g in \mathbf{G} is just the chamber containing $g^{-1}\mathbf{x}_0$.

Remark 4. The fundamental region depends on the choice of initial vector \mathbf{x}_0 in ways one might not expect. For example, replacing the initial vector by a different vector in the fundamental region can change the fundamental region. This is a difference between complex reflection groups and real reflection groups. If \mathbf{G} is a real reflection group, then the fundamental region and decoding regions are determined solely by the reflecting hyperplanes: If \mathbf{x}_0 is the given initial vector and \mathbf{y}_0 is in the fundamental region determined by \mathbf{x}_0 , then \mathbf{x}_0 and \mathbf{y}_0 determine the same fundamental and decoding regions, i.e., for any $\mathbf{x} \in \mathbf{V}$ and $g, a \in \mathbf{G}$,

$$\|g\mathbf{x} - \mathbf{x}_0\| < \|a\mathbf{x} - \mathbf{x}_0\| \quad \text{iff} \quad \|g\mathbf{x} - \mathbf{y}_0\| < \|a\mathbf{x} - \mathbf{y}_0\| .$$

This simply is not true for complex reflection groups. (For example, consider the four element group acting on \mathbb{C} by multiplication by ± 1 or $\pm i$.)

Let us now verify that closures of fundamental regions are indeed analogs of Voronoi regions in Euclidean space.

Lemma 5. *Let $\mathbf{H} \leq \mathbf{G}$, and choose an initial vector \mathbf{x}_0 . A vector $\mathbf{r} \in V$ lies in the closure $\overline{\text{FR}(\mathbf{H})}$ if and only if $\|\mathbf{r} - \mathbf{x}_0\| \leq \|h\mathbf{r} - \mathbf{x}_0\|$ for all $h \in \mathbf{H}$.*

Proof. One direction is routine. Assume $\mathbf{r} \in \overline{\text{FR}(\mathbf{H})}$. Let $\mathbf{r}_i \in \text{FR}(\mathbf{H})$ be a sequence of vectors converging to \mathbf{r} . Then for any $h \in \mathbf{H} - \text{Stab}_{\mathbf{H}}(\mathbf{x}_0)$,

$$\begin{aligned} \|\mathbf{r} - \mathbf{x}_0\| &\leq \|\mathbf{r} - \mathbf{r}_i\| + \|\mathbf{r}_i - \mathbf{x}_0\| \\ &< \|\mathbf{r} - \mathbf{r}_i\| + \|h\mathbf{r}_i - \mathbf{x}_0\| \\ &\leq \|\mathbf{r} - \mathbf{r}_i\| + \|h\mathbf{r}_i - h\mathbf{r}\| + \|h\mathbf{r} - \mathbf{x}_0\| \\ &\leq \|\mathbf{r} - \mathbf{r}_i\| + \|\mathbf{r}_i - \mathbf{r}\| + \|h\mathbf{r} - \mathbf{x}_0\| . \end{aligned}$$

Since $\|\mathbf{r} - \mathbf{r}_i\|$ converges to zero, $\|\mathbf{r} - \mathbf{x}_0\| \leq \|h\mathbf{r} - \mathbf{x}_0\|$ for all $h \in \mathbf{H}$.

For the converse, assume that $\|\mathbf{r} - \mathbf{x}_0\| \leq \|h\mathbf{r} - \mathbf{x}_0\|$ for all $h \in \mathbf{H}$. For any $\epsilon > 0$, let \mathbf{r}' be a vector on the line between \mathbf{r} and \mathbf{x}_0 with $\|\mathbf{r} - \mathbf{r}'\| = \epsilon$, i.e., $\mathbf{r}' = \mathbf{r} + \epsilon\mathbf{x}_0$. Then with respect to the G -invariant inner product $\langle \cdot, \cdot \rangle$,

$$\begin{aligned} \|\mathbf{r}' - \mathbf{x}_0\|^2 &= \|(\mathbf{r} - \mathbf{x}_0) + \epsilon\mathbf{x}_0\|^2 \\ &= \|\mathbf{r} - \mathbf{x}_0\|^2 + \epsilon^2 + 2\operatorname{Re}\langle \epsilon\mathbf{x}_0, \mathbf{r} - \mathbf{x}_0 \rangle \\ &= \|\mathbf{r} - \mathbf{x}_0\|^2 + \epsilon^2 + 2\operatorname{Re}\langle \epsilon\mathbf{x}_0, \mathbf{r} \rangle - 2\epsilon \end{aligned}$$

while, for $h \in \mathbf{H} - \operatorname{Stab}_{\mathbf{H}}(\mathbf{x}_0)$,

$$\begin{aligned} \|h\mathbf{r}' - \mathbf{x}_0\|^2 &= \|(h\mathbf{r} - \mathbf{x}_0) + \epsilon h\mathbf{x}_0\|^2 \\ &\geq \|\mathbf{r} - \mathbf{x}_0\|^2 + \|\epsilon h\mathbf{x}_0\|^2 + 2\operatorname{Re}\langle \epsilon h\mathbf{x}_0, h\mathbf{r} - \mathbf{x}_0 \rangle \\ &= \|\mathbf{r} - \mathbf{x}_0\|^2 + \epsilon^2 + 2\operatorname{Re}\langle \epsilon\mathbf{x}_0, \mathbf{r} \rangle - 2\operatorname{Re}\langle \epsilon h\mathbf{x}_0, \mathbf{x}_0 \rangle \\ &> \|\mathbf{r} - \mathbf{x}_0\|^2 + \epsilon^2 + 2\operatorname{Re}\langle \epsilon\mathbf{x}_0, \mathbf{r} \rangle - 2\epsilon \end{aligned}$$

by the Cauchy-Schwarz inequality, since $h\mathbf{x}_0 \neq \mathbf{x}_0$ implies that $\operatorname{Re}\langle h\mathbf{x}_0, \mathbf{x}_0 \rangle < 1$. Hence $\|\mathbf{r}' - \mathbf{x}_0\| < \|h\mathbf{r}' - \mathbf{x}_0\|$ and \mathbf{r}' lies in $\operatorname{FR}(\mathbf{H})$. We take the limit as ϵ goes to 0 and conclude that \mathbf{r} lies in $\overline{\operatorname{FR}(\mathbf{H})}$. \square

The last lemma implies the following little observation, which will be used several times:

Lemma 6. *Let $\mathbf{K} \leq \mathbf{G}$. For all k in $\mathbf{K} - \operatorname{Stab}_{\mathbf{K}}(\mathbf{x}_0)$,*

$$\operatorname{FR}(\mathbf{K}) \cap k\overline{\operatorname{FR}(\mathbf{K})} = \emptyset.$$

7. MINIMAL, REGION MINIMAL, AND GREED COMPATIBLE

We now identify conditions on coset representatives that will guarantee correct subgroup decoding, with some channel noise or without. In standard subgroup decoding for Coxeter groups, coset leaders are determined algebraically. If $\mathbf{H} \leq \mathbf{K}$ represents a consecutive pair in the subgroup sequence, then each coset leader c is chosen as an element in the coset of minimal length when written as a product of generators of \mathbf{K} . When we use a sequence of parabolic subgroups and choose simple reflections as generators, a unique shortest length element exists in each coset. The algebraic condition of minimal length (in terms of simple reflections) for real reflection groups then guarantees certain geometric properties advantageous for coding (see [10]). We seek geometric analogs of minimal length coset representatives for arbitrary (complex) isometry groups that preserve a nested sequence of regions.

The following simple definition guarantees that a coset leader maps a fundamental region to a new region that at least contains the trivial codeword.

Definition 7. *A coset leader c for groups $\mathbf{H} \leq \mathbf{K}$ is minimal if $\mathbf{x}_0 \in c(\operatorname{FR}(\mathbf{H}))$. A set of coset leaders is minimal if all its elements are.*

We rephrase this definition:

Lemma 8. *A coset leader c for groups $\mathbf{H} \leq \mathbf{K}$ is minimal if \mathbf{x}_0 is closer to the codeword $c^{-1}\mathbf{x}_0$ than to any other codeword defined by the coset $c\mathbf{H}$:*

$$\|c^{-1}\mathbf{x}_0 - \mathbf{x}_0\| < \|(ch)^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$$

for all h in $\mathbf{H} - \text{Stab}_{\mathbf{H}}(\mathbf{x}_0)$.

Effective decoding will require stronger versions of minimality:

Definition 9. *Let c be a coset leader for groups $\mathbf{H} \leq \mathbf{K}$. Then*

- c is open-region-minimal if $\text{FR}(\mathbf{K}) \subseteq c\text{FR}(\mathbf{H})$;
- c is region-minimal if $\overline{\text{FR}(\mathbf{K})} \subseteq \overline{c\text{FR}(\mathbf{H})}$.

A set of coset leaders is open-region-minimal (respectively region-minimal) if all its elements are open-region-minimal (respectively region-minimal).

The following observation can be verified with Lemma 5.

Lemma 10. *A coset leader c for groups $\mathbf{H} \leq \mathbf{K}$ is open-region-minimal if and only if every vector in $\text{FR}(\mathbf{K})$ is closer to the codeword $c^{-1}\mathbf{x}_0$ than to any other code word determined by the coset $c\mathbf{H}$: For any \mathbf{y} in $\text{FR}(\mathbf{K})$,*

$$\|c^{-1}\mathbf{y} - \mathbf{x}_0\| < \|(ch)^{-1}\mathbf{y} - \mathbf{x}_0\|$$

for all h in $\mathbf{H} - \text{Stab}_{\mathbf{H}}(\mathbf{x}_0)$.

Likewise, a coset leader c for $\mathbf{H} \leq \mathbf{K}$ is region-minimal if and only if

$$\|c^{-1}\mathbf{y} - \mathbf{x}_0\| \leq \|(ch)^{-1}\mathbf{y} - \mathbf{x}_0\|$$

for any \mathbf{y} in $\overline{\text{FR}(\mathbf{K})}$ and h in \mathbf{H} .

Note that minimal or open-region-minimal coset leaders may not exist because of ties, i.e., two different codewords may both yield the minimum distance; see Section 12.

A set of coset leaders is compatible with the greedy algorithm if every element in the closure of the larger fundamental region of \mathbf{H} is sent into the closure of the smaller fundamental region of \mathbf{K} by *some* coset leader:

Definition 11. *We call a set of coset leaders CL for groups $\mathbf{H} \leq \mathbf{K}$ greed compatible if*

$$\overline{\text{FR}(\mathbf{H})} \subseteq \bigcup_{c \in \text{CL}} c^{-1}\overline{\text{FR}(\mathbf{K})}.$$

8. COMPARING MINIMAL, REGION MINIMAL, AND GREED COMPATIBLE

In this section, we make a few observations comparing the different geometric notions of minimal coset representatives that will be helpful for the next sections on correct and robust decoding. For example, the definitions immediately imply that

$$\text{open-region-minimal} \Rightarrow \text{region-minimal} \Rightarrow \text{minimal}.$$

If the initial vector has full orbit, we will see in addition that

$$\text{region-minimal} \Leftrightarrow \text{greed compatible}.$$

We record the first fact formally before proceeding to prove the second.

Lemma 12. *Let $\mathbf{H} \leq \mathbf{G}$, and let $\text{CL} = \text{CL}(\mathbf{K}/\mathbf{H})$ be a set of coset leaders for \mathbf{K} over \mathbf{H} . Then*

- (1) *If CL is open-region-minimal, then it is region-minimal.*
- (2) *If CL is region-minimal, then it is minimal.*

We are especially interested in codes whose size equals that of the group.

Proposition 13. *Assume the initial vector \mathbf{x}_0 has full orbit. A set of coset leaders is greed compatible if and only if it is region-minimal.*

Proof. Assume that $\text{CL} = \text{CL}(\mathbf{K}/\mathbf{H})$ is a greed compatible set of coset representatives for \mathbf{K} over \mathbf{H} . Take some $\mathbf{y} \in \text{FR}(\mathbf{K})$ and $c \in \text{CL}$. Find an element $h \in \mathbf{H}$ minimizing $\|hc^{-1}\mathbf{y} - \mathbf{x}_0\|$, so that $hc^{-1}\mathbf{y} \in \overline{\text{FR}(\mathbf{H})}$ by Lemma 5. As CL is greed compatible, there exists $d \in \text{CL}$ with $dhc^{-1}\mathbf{y} \in \overline{\text{FR}(\mathbf{K})}$. Lemma 6 implies that $dhc^{-1} \in \text{Stab}_{\mathbf{K}}(\mathbf{x}_0) = \{I\}$ and thus $d = ch^{-1}$. Then $c = d$ (as c and d are both coset leaders) and $h = I$. Thus $c^{-1}\mathbf{y} \in \overline{\text{FR}(\mathbf{H})}$ and hence $\text{FR}(\mathbf{K}) \subset c\overline{\text{FR}(\mathbf{H})}$. Then as c is an isometry, $\overline{\text{FR}(\mathbf{K})} \subset c\overline{\text{FR}(\mathbf{H})} = c\overline{\text{FR}(\mathbf{H})}$ and CL is minimal.

For the converse, assume that CL is region-minimal and choose some $\mathbf{z} \in \text{FR}(\mathbf{H})$. Choose k minimizing $\|k\mathbf{z} - \mathbf{x}_0\|$ over all k in \mathbf{K} so that $k\mathbf{z} \in \overline{\text{FR}(\mathbf{K})}$. Write $k = ch$ with $c \in \text{CL}$ and $h \in \mathbf{H}$. Since CL is region-minimal, each $h\mathbf{z} = c^{-1}k\mathbf{z}$ lies in $\overline{\text{FR}(\mathbf{H})}$. By Lemma 6, $h = I$, and thus $c\mathbf{z} = ch\mathbf{z} = k\mathbf{z}$ lies in $\overline{\text{FR}(\mathbf{K})}$. Hence \mathbf{z} lies in $c^{-1}\overline{\text{FR}(\mathbf{K})}$ and CL is greed compatible. \square

Lemma 12 and Proposition 13 then imply

Corollary 14. *Assume the initial vector \mathbf{x}_0 has full orbit under \mathbf{G} . Any greed compatible set of coset leaders is also minimal.*

9. ROBUST DECODING: GREED PAYS....

The subgroup decoding procedure uses a greedy algorithm, but greedy algorithms do not always work. We argue in this section that greed compatible coset leaders not only ensure that the subgroup decoding algorithm will decode correctly, but that the algorithm is also robust.

Theorem 15. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} , subgroup sequence, and coset leader sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. If each $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is greed compatible, then the subgroup decoding algorithm decodes robustly.*

Proof. Assume the received vector \mathbf{r} lies in the decoding region $\text{DR}(g)$ for some element g in \mathbf{G} . Set $\mathbf{r}_0 := \mathbf{r} \in V = \overline{\text{FR}(\mathbf{G}_0)}$. Fix k and inductively assume that $\mathbf{r}_{k-1} := d_{k-1} \cdots d_1 \mathbf{r}$ lies in $\overline{\text{FR}(\mathbf{G}_{k-1})}$ with each d_i in $\text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1})$. Since $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is robust, $c\mathbf{r}_{k-1}$ lies in $\overline{\text{FR}(\mathbf{G}_k)}$ for some c in $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. The subgroup decoding algorithm at the k -th step finds a coset leader d_k minimizing $\|d_k\mathbf{r}_{k-1} - \mathbf{x}_0\|$ over all coset leaders

$d \in \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. In particular, $\|d_k \mathbf{r}_{k-1} - \mathbf{x}_0\| \leq \|\mathbf{c} \mathbf{r}_{k-1} - \mathbf{x}_0\|$. Then for any h in \mathbf{G}_k , by Lemma 5,

$$\|hd_k \mathbf{r}_{k-1} - \mathbf{x}_0\| = \|(hd_k c^{-1}) \mathbf{c} \mathbf{r}_{k-1} - \mathbf{x}_0\| \geq \|\mathbf{c} \mathbf{r}_{k-1} - \mathbf{x}_0\| \geq \|d_k \mathbf{r}_{k-1} - \mathbf{x}_0\|$$

as $\mathbf{c} \mathbf{r}_{k-1} \in \overline{\text{FR}(\mathbf{G}_k)}$ and $hd_k c^{-1} \in \mathbf{G}_k$. Thus $d_k \mathbf{r}_{k-1}$ lies in $\overline{\text{FR}(\mathbf{G}_k)}$ as well. At the last step, for $\mathbf{G} = \mathbf{G}_m$, we find that $\mathbf{r}_m = d_m \cdots d_1 \mathbf{r}$ lies in $\overline{\text{FR}(\mathbf{G})}$, and \mathbf{r} decodes as $d_m \cdots d_1 = g'$.

Now $\mathbf{r} = g^{-1} \mathbf{x}$ for some $\mathbf{x} \in \text{FR}(\mathbf{G})$ since $\mathbf{r} \in \text{DR}(g)$. Then $g' g^{-1} \mathbf{x} = g' \mathbf{r}$ lies in $\overline{\text{FR}(\mathbf{G})}$. By Lemma 6, $g' g^{-1} \in \text{Stab}_{\mathbf{G}}(\mathbf{x}_0)$ and g' and g are equivalent, i.e., they define the same codeword. Thus the subgroup decoding algorithm decodes robustly. \square

Corollary 16. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} with full orbit, subgroup sequence, and coset leader sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. If every set $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is greed compatible, then the subgroup decoding algorithm decodes any received vector \mathbf{r} satisfying $\|\mathbf{r} - g^{-1} \mathbf{x}_0\| < \frac{1}{2} d_{\min}$ to g in \mathbf{G} . The corresponding statement is false if we replace $\frac{1}{2} d_{\min}$ by any $\gamma > \frac{1}{2} d_{\min}$.*

Proof. If $\|\mathbf{g} \mathbf{r} - \mathbf{x}_0\| < \frac{1}{2} d_{\min}$, then $\mathbf{g} \mathbf{r} \in \text{FR}(\mathbf{G})$ and $\mathbf{r} \in \text{DR}(g)$. Hence by Theorem 15, the vector \mathbf{r} will decode to the message g . On the other hand, there exists $a \in \mathbf{G}$ such that $\|a^{-1} \mathbf{x}_0 - \mathbf{x}_0\| = d_{\min}$. For any ε with $0 < \varepsilon < \frac{1}{2}$, let $\mathbf{r} = \mathbf{x}_0 + (\frac{1}{2} + \varepsilon)(a^{-1} \mathbf{x}_0 - \mathbf{x}_0)$. Then $\|\mathbf{r} - \mathbf{x}_0\| = (\frac{1}{2} + \varepsilon) d_{\min}$, but \mathbf{r} decodes to a since $\|\mathbf{r} - a^{-1} \mathbf{x}_0\| = (\frac{1}{2} - \varepsilon) d_{\min}$. \square

We will verify in Section 15 that greed compatible coset leaders exist for the complex reflection groups $\mathbf{G}(r, 1, n)$ for an appropriate subgroup sequence and initial vector. In the next section, we show how to salvage correct decoding with small noise even when greed compatible group leaders cannot be found.

Lemma 12, Proposition 13, and Theorem 15 imply that closures are not necessary when the initial vector has full orbit:

Corollary 17. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} , and subgroup sequence. Assume that \mathbf{x}_0 has full orbit. If every coset leader set $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is open-region-minimal, then the subgroup decoding algorithm decodes robustly.*

10. CORRECT DECODING: ...BUT MINIMALITY SUFFICES!

We now turn to the case when \mathbf{x}_0 has full orbit under \mathbf{G} . For example, we choose \mathbf{x}_0 off a reflecting hyperplane if \mathbf{G} is a real or complex reflection group. We show that minimality of induced coset leaders is both necessary and sufficient for the subgroup decoding algorithm to decode correctly, even with some noise. We begin by defining *induced coset leaders* with the following elementary lemma:

Lemma 18. *Fix sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ of coset leaders for each consecutive pair in a subgroup sequence. Then for any $k < \ell$, the set*

$$\text{CL}(\mathbf{G}_\ell/\mathbf{G}_k) = \{c_\ell \cdots c_{k+1} : c_i \in \text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1}) \text{ for } k+1 \leq i \leq \ell\}$$

is a complete set of coset representatives for \mathbf{G}_ℓ over \mathbf{G}_k . We call its elements the induced coset leaders for \mathbf{G}_ℓ over \mathbf{G}_k .

The next theorem explains that, just as coset leaders are chosen to be the codewords of minimum Hamming weight in linear block coding, so too should coset leaders be chosen minimum in a geometric sense in subgroup decoding.

Theorem 19. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} of full orbit, subgroup sequence, and coset leader sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. Minimal coset leaders are necessary for correct decoding: If the subgroup decoding algorithm decodes correctly, then the induced coset leaders $\text{CL}(\mathbf{G}_\ell/\mathbf{G}_k)$ are minimal for all $\ell > k$.*

Proof. Fix some index k and suppose c_k in $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is not minimal. Then there exists some nonidentity element h in \mathbf{G}_{k-1} with

$$(20) \quad \|c_k^{-1}\mathbf{x}_0 - \mathbf{x}_0\| \geq \|(c_k h)^{-1}\mathbf{x}_0 - \mathbf{x}_0\| = \|(c_k c_{k-1} \cdots c_1)^{-1}\mathbf{x}_0 - \mathbf{x}_0\|,$$

where $h = c_{k-1} \cdots c_1$ for some c_i in $\text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1})$. Fix some j with $1 \leq j \leq k-1$ and suppose $\mathbf{r}_j = (c_k c_{k-1} \cdots c_j)^{-1}\mathbf{x}_0$ is a received vector. As \mathbf{r}_j correctly decodes to group element $c_k c_{k-1} \cdots c_j$, the algorithm chooses coset leader c_j among all coset leaders in $\text{CL}(\mathbf{G}_j/\mathbf{G}_{j-1})$, including the coset leader I , at the j -th step. Thus

$$\begin{aligned} \|(c_k c_{k-1} \cdots c_{j+1})^{-1}\mathbf{x}_0 - \mathbf{x}_0\| &= \|c_j(c_k c_{k-1} \cdots c_j)^{-1}\mathbf{x}_0 - \mathbf{x}_0\| \\ &\leq \|I(c_k c_{k-1} \cdots c_j)^{-1}\mathbf{x}_0 - \mathbf{x}_0\|. \end{aligned}$$

This gives a nested sequence of inequalities as j ranges from 1 to $k-1$,

$$\|c_k^{-1}\mathbf{x}_0 - \mathbf{x}_0\| \leq \|(c_k c_{k-1})^{-1}\mathbf{x}_0 - \mathbf{x}_0\| \leq \dots \leq \|(c_k c_{k-1} \cdots c_1)^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$$

with at least one inequality strict as $h \neq I$, contradicting inequality (20) above. We replace c_k by any $c_\ell c_{\ell-1} \cdots c_k$, where each c_i lies in $\text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1})$, in the above argument to see that induced coset leaders are minimal as well. \square

In the last section, we saw that region-minimal coset leaders guarantee robust decoding (Theorem 15). However, it is not always easy to determine the fundamental region of a subgroup \mathbf{G}_k in the subgroup sequence of a complicated group. Even worse, region-minimal coset leaders may fail to exist. The next theorem shows that the decoding algorithm corrects for small noise when we weaken the hypothesis on coset leaders but shrink the region of correct decoding to compensate. We may merely insist that induced coset leaders be minimal, a condition which is straightforward to test but fails for many choices of subgroup sequences (see Section 17).

Theorem 21. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} with full orbit, subgroup sequence, and coset leader sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. If every set of induced coset leaders $\text{CL}(\mathbf{G}, \mathbf{G}_k)$ is minimal (for $1 \leq k < m$), then the subgroup decoding algorithm decodes correctly with some noise.*

Proof. Let $\delta_m = d_{\min}$, the minimum distance of the code, and for $1 \leq k < m$, define

$$\delta_k = \min \{ \|c_m \cdots c_{k+1} h \mathbf{x}_0 - \mathbf{x}_0\| - \|c_m \cdots c_{k+1} \mathbf{x}_0 - \mathbf{x}_0\| \},$$

taking the minimum over all $c_i \in \text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1})$ for $k < i \leq m$ and over all $h \in \mathbf{G}_k - \mathbf{G}_{k-1}$. Set $\delta = \min_{1 \leq k \leq m} \delta_k$. Since each $\text{CL}(\mathbf{G}/\mathbf{G}_k)$ is minimal, each δ_k is strictly positive and thus δ is positive.

Suppose g in \mathbf{G} is a message with transmitted vector $g^{-1} \mathbf{x}_0$. Write g uniquely as $g = c_m \cdots c_1$ with each c_i in $\text{CL}(\mathbf{G}_i/\mathbf{G}_{i-1})$. Assume the received vector \mathbf{r} is within $\delta/2$ of the transmitted vector. Then, for $\mathbf{r}_0 = \mathbf{r}$,

$$\|c_1 \mathbf{r}_0 - (c_m \cdots c_2)^{-1} \mathbf{x}_0\| = \|\mathbf{r}_0 - (c_m \cdots c_1)^{-1} \mathbf{x}_0\| < \delta/2.$$

By the triangle inequality,

$$\begin{aligned} \|c_1 \mathbf{r}_0 - \mathbf{x}_0\| &\leq \|c_1 \mathbf{r}_0 - (c_m \cdots c_2)^{-1} \mathbf{x}_0\| + \|(c_m \cdots c_2)^{-1} \mathbf{x}_0 - \mathbf{x}_0\| \\ &< \frac{\delta}{2} + \|(c_m \cdots c_2)^{-1} \mathbf{x}_0 - \mathbf{x}_0\| \end{aligned}$$

while for $d \in \text{CL}(\mathbf{G}_1/\mathbf{G}_0) - \{c_1\}$,

$$\begin{aligned} \|d \mathbf{r}_0 - \mathbf{x}_0\| &\geq -\|d \mathbf{r}_0 - d(c_m \cdots c_1)^{-1} \mathbf{x}_0\| + \|d(c_m \cdots c_1)^{-1} \mathbf{x}_0 - \mathbf{x}_0\| \\ &= -\|\mathbf{r}_0 - (c_m \cdots c_1)^{-1} \mathbf{x}_0\| + \|(c_m \cdots c_1 d^{-1})^{-1} \mathbf{x}_0 - \mathbf{x}_0\| \\ &> -\delta/2 + \|(c_m \cdots c_2)^{-1} \mathbf{x}_0 - \mathbf{x}_0\| + \delta_1 \\ &\geq \delta/2 + \|(c_m \cdots c_2)^{-1} \mathbf{x}_0 - \mathbf{x}_0\| \end{aligned}$$

because $\delta \leq \delta_1$. Hence the subgroup decoding algorithm, which chooses a coset leader c minimizing $\|c \mathbf{r}_0 - \mathbf{x}_0\|$, will choose $c = c_1$.

Now let $\mathbf{r}_1 = c_1 \mathbf{r}_0$ and note that

$$\|\mathbf{r}_1 - (c_m \cdots c_2)^{-1} \mathbf{x}_0\| = \|\mathbf{r}_0 - (c_m \cdots c_1)^{-1} \mathbf{x}_0\| < \delta/2.$$

An analogous argument shows that the subgroup decoding algorithm will choose the coset leader c_2 (since the product of c_2 with the inverse of any other coset leader in $\text{CL}(\mathbf{G}_2/\mathbf{G}_1)$ lies in $\mathbf{G}_2 - \mathbf{G}_1$) at the second stage. Let $\mathbf{r}_2 = c_2 \mathbf{r}_1$ and note that

$$\begin{aligned} \|\mathbf{r}_2 - (c_m \cdots c_3)^{-1} \mathbf{x}_0\| &= \|c_2 \mathbf{r}_1 - c_3^{-1} \cdots c_m^{-1} \mathbf{x}_0\| = \|\mathbf{r}_1 - c_2^{-1} c_3^{-1} \cdots c_m^{-1} \mathbf{x}_0\| \\ &= \|\mathbf{r}_1 - (c_m \cdots c_2)^{-1} \mathbf{x}_0\| < \delta/2. \end{aligned}$$

Recursively, the algorithm chooses c_3, \dots, c_{m-1} as coset leaders minimizing distance to \mathbf{x}_0 . For the last step, we set $\mathbf{r}_{m-1} = c_{m-1} \cdots c_1 \mathbf{r}_0$ and note that

$$\|c_m \mathbf{r}_{m-1} - \mathbf{x}_0\| < \delta/2$$

while for any other coset leader $d \in \text{CL}(\mathbf{G}_m/\mathbf{G}_{m-1})$,

$$\|d\mathbf{r}_{m-1} - \mathbf{x}_0\| \geq -\|d\mathbf{r}_{m-1} - dc_m^{-1}\mathbf{x}_0\| + \|dc_m^{-1}\mathbf{x}_0 - \mathbf{x}_0\| > -\delta/2 + d_{\min} \geq \delta/2.$$

Hence the algorithm chooses c_m as well and outputs $g' = g$ as the decoded message. \square

The last theorem together with Theorem 19 now gives us necessary and sufficient conditions for correct decoding:

Corollary 22. *Fix any finite group $\mathbf{G} \subset \text{GL}(\mathbf{V})$, initial vector \mathbf{x}_0 in \mathbf{V} with full orbit, subgroup sequence, and coset leader sets $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. Correct subgroup decoding occurs if and only if induced coset leaders $\text{CL}(\mathbf{G}/\mathbf{G}_k)$ are minimal for all k . In this case, subgroup decoding decodes correctly with some noise.*

One can prove directly or appeal to the last corollary to check that very short subgroup sequences always decode correctly with minimal coset leaders:

Corollary 23. *Assume the initial vector has full orbit under \mathbf{G} . Consider a short subgroup sequence $\{I\} < \mathbf{G}_1 < \mathbf{G}$. Then the subgroup decoding algorithm decodes correctly with some noise if and only if the coset leaders for \mathbf{G} over \mathbf{G}_1 are minimal.*

For example, this corollary applies to the octahedral reflection group \mathbf{G}_8 of Section 17.4 with the natural subgroup sequence $\{I\} < \{I, A, A^2, A^3\} < \mathbf{G}_8$. With an appropriate choice of the initial vector, it is straightforward to find minimal coset leaders for \mathbf{G}_8 . Compare with Section 12, though, for difficulties inherent in finding minimal coset leaders in general.

Remark 24. Again, assume that the initial vector \mathbf{x}_0 has full orbit. An easy induction using Lemma 12 together with Corollary 22 shows that

$$\begin{aligned} & \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1}) \text{ region-minimal for all } k \\ & \Rightarrow \text{CL}(\mathbf{G}/\mathbf{G}_j) \text{ region-minimal for all } j \\ & \Rightarrow \text{CL}(\mathbf{G}/\mathbf{G}_j) \text{ minimal for all } j \\ & \Rightarrow \text{correct decoding.} \end{aligned}$$

Although this is directly implied by Proposition 13 and Theorem 15 (as robust decoding implies correct decoding), one might ask if we could merely take minimal coset leaders for consecutive pairs of nested subgroups in this argument. The answer is no, since

$$\begin{aligned} & \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1}) \text{ minimal for all } k \\ & \not\Rightarrow \text{CL}(\mathbf{G}/\mathbf{G}_j) \text{ minimal for all } j. \end{aligned}$$

Indeed, Kim [11] gives an example based on the complex reflection group \mathbf{G}_{25} with each set of coset leaders $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ minimal, but $\text{CL}(\mathbf{G}/\mathbf{G}_j)$ not minimal for some j .

11. ERROR CONTROL

Decoding errors occur with substantial noise: A codeword $g^{-1}\mathbf{x}_0$ may be sent (for some message g in \mathbf{G}) but the received vector \mathbf{r} may land closer to some other codeword. If \mathbf{r} does not lie in the decoding region $\text{DR}(g)$, then it most likely lies in a geometrically neighboring decoding region $\text{DR}(g')$. Can we fine-tune the subgroup decoding algorithm so the decoded message g' is “close” to the sent message g most of the time? In this section, we give properties of a group code that ensure that the decoded message will differ from the sent message in at most one factor when written as a product of coset leaders, provided the received vector lands in a region neighboring the intended one. We assume the initial vector \mathbf{x}_0 has full orbit throughout this section.

Definition 25. *The nearest neighbors of a codeword \mathbf{u} are the codewords \mathbf{v} with $\|\mathbf{u} - \mathbf{v}\| = d_{min}$.*

It is not difficult to see how nearest neighbors of the initial vector determine nearest neighbors of any codeword:

Lemma 26. *For all g in \mathbf{G} , the nearest neighbors of $g\mathbf{x}_0$ are the codewords $g\mathbf{w}$ with \mathbf{w} a nearest neighbor of \mathbf{x}_0 .*

It is useful to identify the group elements yielding nearest neighbors.

Definition 27. *The neighborhood $N_{\mathbf{G}}(\mathbf{x}_0)$ of \mathbf{x}_0 is the set of nearest neighbors of \mathbf{x}_0 , i.e., the points in the orbit of \mathbf{x}_0 closest to \mathbf{x}_0 . We say the corresponding set $N_{\mathbf{G}}$ of group elements realizes the neighborhood:*

$$N_{\mathbf{G}}(\mathbf{x}_0) = \{\mathbf{v} \in \mathbf{G}\mathbf{x}_0 - \{\mathbf{x}_0\} : \|\mathbf{v} - \mathbf{x}_0\| = d_{min}\},$$

$$N_{\mathbf{G}} = \{a \in \mathbf{G} : a\mathbf{x}_0 \in N_{\mathbf{G}}(\mathbf{x}_0)\}.$$

Neighborhoods can be analogously defined for any subgroup \mathbf{G}_k in the subgroup sequence. In the case that \mathbf{G} is a Coxeter group, a set of simple reflections realizes the neighborhood of \mathbf{x}_0 . More generally, the generators for each subgroup may be taken to be a subset of simple reflections so that the group elements realizing the neighborhood for \mathbf{G}_k generate \mathbf{G}_k (see [10]). We seek a similar property for general group codes below.

By Lemma 26, if a codeword $g^{-1}\mathbf{x}_0$ is decoded incorrectly, it will most likely be decoded as a neighbor $(bg)^{-1}\mathbf{x}_0$ with b in $N_{\mathbf{G}}$. To minimize the message error, we would like the canonical form of bg as a product of coset leaders to differ as little as possible from that of g . That is the effect of the next two error control properties for consecutive subgroups in the subgroup sequence, both from [10]. Note that the first property depends on the choice of the initial vector \mathbf{x}_0 . For any subset X of \mathbf{G} , write X^{-1} for the set $\{a^{-1} : a \in X\}$.

Property 28 (Nearest Neighbors). *The Nearest Neighbors Property holds for a fixed set $X_{\mathbf{G}}$ generating \mathbf{G} whenever $N_{\mathbf{G}} \subseteq X_{\mathbf{G}} \cup X_{\mathbf{G}}^{-1}$.*

Property 29 (Error Control). *Let $\mathbf{H} < \mathbf{K}$ be subgroups of \mathbf{G} with a fixed set of coset leaders $\text{CL}(\mathbf{K}/\mathbf{H})$. The Error Control Property holds for sets of generators $X_{\mathbf{H}}$ of \mathbf{H} and $X_{\mathbf{K}}$ of \mathbf{K} whenever*

$$bc \in \text{CL}(\mathbf{K}/\mathbf{H}) \text{ or } c^{-1}bc \in X_{\mathbf{H}} \cup X_{\mathbf{H}}^{-1}$$

for all $b \in X_{\mathbf{K}} \cup X_{\mathbf{K}}^{-1}$ and $c \in \text{CL}(\mathbf{K}/\mathbf{H})$.

Note that the property implies that either bc is the coset leader for the coset $bc\mathbf{H}$, or c is the coset leader for $bc\mathbf{H}$ because bc and c lie in the same coset.

The Error Control Property minimizes small errors:

Theorem 30. *Assume that Error Control Property 29 holds for consecutive pairs of a subgroup sequence $\{I\} = \mathbf{G}_0 < \mathbf{G}_1 < \dots < \mathbf{G}_m = \mathbf{G}$, some choice of generators $X_{\mathbf{G}_k}$ of \mathbf{G}_k , and some choice of coset leaders $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$. Suppose g in \mathbf{G} has canonical form as a product of coset leaders given by*

$$g = c_m \cdots c_1, \text{ each } c_k \in \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1}).$$

Then for any $b \in X_{\mathbf{G}} \cup X_{\mathbf{G}}^{-1}$, the canonical form of bg is

$$bg = c'_m \cdots c'_1, \text{ each } c'_k \in \text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1}),$$

where $c'_i = c_i$ for all but one i . In addition, for that single index j with $c'_j \neq c_j$, the coset leader c'_j is adjacent to c_j in the coset leader graph for \mathbf{G}_j over \mathbf{G}_{j-1} (see Section 13).

Proof. We induct on m . If $m = 1$, then every element is a coset leader, and the conclusion is trivial. Let $m > 1$. Consider $g = c_m \cdots c_1$ and take $b \in X_{\mathbf{G}_m} = X_{\mathbf{G}} \cup X_{\mathbf{G}}^{-1}$. If bc_m is a coset leader, then $bg = (bc_m)c_{m-1} \cdots c_1$ is in canonical form. If not, Property 29 implies that

$$\begin{aligned} bg &= c_m(c_m^{-1}bc_m)c_{m-1} \cdots c_1 \\ &= c_m(b'c_{m-1} \cdots c_1) \end{aligned}$$

with $b' \in X_{\mathbf{G}_{m-1}} \cup X_{\mathbf{G}_{m-1}}^{-1}$. The result follows from applying the induction hypothesis to $b'c_{m-1} \cdots c_1$. \square

The Error Control Property and Nearest Neighbors Properties together imply nice error control:

Corollary 31. *Assume Error Control Property 29 and Nearest Neighbors Property 28 hold for \mathbf{G} with fixed subgroup sequence, initial vector, coset leader sets, and generating sets $X_{\mathbf{G}_k}$ of \mathbf{G}_k . Assume coset leaders are greed compatible. If a received vector lies in the decoding region containing a nearest neighbor of $g^{-1}\mathbf{x}_0$ due to noise, then the subgroup decoding algorithm decodes it to a group element differing from g in only one factor when written as a product of coset leaders.*

Proof. Lemma 26 implies that the received vector \mathbf{r} lies in the decoding region of $g^{-1}b\mathbf{x}_0$ for some b in \mathbf{G} with $b\mathbf{x}_0$ a nearest neighbor of \mathbf{x}_0 . Theorem 15 then implies that the subgroup decoding algorithm will correctly decode \mathbf{r} to $b^{-1}g$. But Property 28 implies that b or b^{-1} lies in $X_{\mathbf{G}}$, and hence $b^{-1}g$ differs from g in only one factor by Theorem 30. \square

12. TIES

Correct decoding requires minimal induced coset leaders by Corollary 22, but they may not exist because of ties. For any subgroup \mathbf{H} of \mathbf{G} , we say that a *tie* occurs when two different codewords encoding elements from the same coset of \mathbf{H} yield the same minimum distance to the initial vector, i.e., when $a\mathbf{H} = b\mathbf{H}$ for some a and b in \mathbf{G} with $\|a^{-1}\mathbf{x}_0 - \mathbf{x}_0\| = \|b^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$ minimizing $\|c^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$ over all c in the coset $a\mathbf{H}$. There are a couple of ways ties occur naturally.

The first is when a and a^{-1} lie in the same coset of \mathbf{H} (i.e., $a^2 \in \mathbf{H} - \{I\}$) and $\|a^{-1}\mathbf{x}_0 - \mathbf{x}_0\| = \|a\mathbf{x}_0 - \mathbf{x}_0\|$ yields a minimum. One has little choice but to change the subgroup sequence in this case, as shown below for the concrete code based on the complex reflection group \mathbf{G}_4 (in the classification of Shephard and Todd [17]).

A second way occurs when the initial vector \mathbf{x}_0 is real and a and b are both symmetric unitary matrices, so that each has inverse equal to its conjugate, with ab and $a^{-1}b^{-1}$ in the same coset. (Such matrices arise in the natural reflection representations of some complex reflection groups where real initial vectors are often a convenient choice.) Then $\|ab\mathbf{x}_0 - \mathbf{x}_0\| = \|a^{-1}b^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$, and this distance could be minimal over the coset. In this case, replacing the initial vector by one that is properly complex will eliminate the tie. Again, see the example of \mathbf{G}_4 below.

Another way to resolve the problem of ties is to allow multiple coset leaders and multiple canonical forms. This worked for the real reflection groups \mathbf{WD}_n in [10] but generally seems to become cumbersome rather quickly.

12.1. Tetrahedral group \mathbf{G}_4 . We give an example of a complex reflection group and choice of initial vector and subgroup sequence for which minimal coset leaders do not exist, and thus the subgroup decoding algorithm does not decode correctly. We then show how to make other choices to recover correct decoding. The group \mathbf{G}_4 of order 24 (with 8 reflections) is generated by the matrices

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{2} + \frac{\sqrt{3}}{2}i \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \frac{1}{\sqrt{3}}i & \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{6}}i \\ \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{6}}i & \frac{1}{2} + \frac{1}{2\sqrt{3}}i \end{bmatrix}$$

which satisfy $A^3 = B^3 = I$ and $ABA = BAB$. As explained in Walker [12], a natural choice for the initial vector is approximately $\mathbf{x}_0 = (0.8881, 0.4597)$.

Suppose we take the subgroup sequence $\{I\} < \{I, A, A^2\} < \mathbf{G}_4$. Set $C = BA^2B$ and $D = CA$, so that C and D are inverse but in the same coset

$\{C, D, CA^2\}$ of \mathbf{G}_1 , with

$$\|C\mathbf{x}_0 - \mathbf{x}_0\| = \|D\mathbf{x}_0 - \mathbf{x}_0\| < \|CA^2\mathbf{x}_0 - \mathbf{x}_0\|.$$

Thus no minimal coset leader exists for this coset because of a tie. Note that $C^2 = A^2 \in \mathbf{H}$.

We could use instead the subgroup sequence $\{I\} < \mathbf{K} < \mathbf{G}_4$ where $\mathbf{K} = \{I, C, C^2, C^3, C^4, C^5\}$. Then \mathbf{K} has index four and minimal coset leaders for \mathbf{K} are I, B, B^2 . A tie prevents choosing AB or $A^2B^2 = A^{-1}B^{-1}$ as a minimal coset leader for the last coset. (Here, A and B are symmetric unitary matrices.) We resolve the tie by choosing a different initial vector. Again consulting Walker [12], we choose $\mathbf{y}_0 = (\frac{1}{\sqrt{2}} + \frac{i}{2}, \frac{1}{2})$ and A^2B^2 becomes the minimal coset leader.

Corollary 23 implies that the subgroup decoding algorithm decodes correctly with some noise for \mathbf{G}_4 with these revised choices.

13. EFFICIENT DECODING USING COSET LEADER GRAPHS

We have thus far discussed mathematical properties that correct for noise and control errors. Before considering explicit construction of group codes, we turn our attention to matters of efficiency. Given a fixed choice of coset leaders, the subgroup decoding algorithm decodes by determining a coset leader at each step in the algorithm that minimizes some distance. If the structure of the group permits, we may avoid looping through *all* the coset leaders in some fixed set $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ at each step.

We may instead use a restriction of the standard Cayley graph to reduce the number of coset leaders considered in subgroup decoding.

Definition 32. *Given a group \mathbf{G} with subgroups $\mathbf{H} \leq \mathbf{K}$ and a set X of generators for \mathbf{K} , the coset leader graph $\Gamma = \Gamma(\mathbf{K}/\mathbf{H})$ for \mathbf{K} over \mathbf{H} with respect to a fixed set $\text{CL}(\mathbf{K}/\mathbf{H})$ of coset leaders is the graph*

- whose vertices are the elements of $\text{CL}(\mathbf{K}/\mathbf{H})$
- with a directed edge (labeled by a) from vertex c to d whenever $c = ad$ for some generator a in X .

For a unitary group with a given subgroup sequence and initial vector, Theorem 19 tells us that the coset leaders should be chosen minimal. If we also specify a generating set X_k for each subgroup \mathbf{G}_k , then the coset leader graphs are determined. See Figure 15.7 for an example.

In [10], navigation through spanning trees of coset leader graphs for Coxeter groups played an important role in efficient decoding of group codes built on real reflection groups. On an *ad hoc* basis, we have applied similar methods to decode group codes based on some specific complex reflection groups, e.g., \mathbf{G}_4 and \mathbf{G}_8 . However, as yet there is no general theory of how this is best done. For most of the groups considered in this paper, the coset leader graphs are trees and cycles, and the complications that occur when navigating the more complex coset leader graphs associated with exceptional reflection groups do not arise. Indeed, for the complex reflection

groups $\mathbf{G}(r, 1, n)$, the correct coset leader can be chosen in one step; see Remark 39. (Kriloff and Lay [16] give a more detailed analysis of the Cayley graphs for $\mathbf{G}(r, 1, n)$.)

For the purposes of this paper, let us suppress the particular methods of navigating coset leader graphs used in constructing our examples, but the reader should be aware that some such scheme is required for efficient decoding. We hope to address navigation schemes in a future report.

14. DECODING WITH WREATH PRODUCTS

In this section, we consider some wreath products that act as isometries on finite dimensional complex space and show that a natural subgroup sequence and choice of coset leaders produce codes that not only decode correctly, but also robustly. These ideas allow one to expand a successful group code of small size into a successful group code of arbitrarily large size. We will apply the results to the infinite family $\mathbf{G}(r, 1, n)$ of complex reflection groups in Section 15 and also to construct codes in Table 17.2.1).

Let $\mathbf{H} \subset \mathrm{GL}_m(\mathbb{C})$ be a finite unitary group acting on the vector space \mathbb{C}^m . Let \mathbf{G} be the wreath product of \mathbf{H} with the symmetric group Sym_n ,

$$\mathbf{G} = \mathbf{H} \wr \mathrm{Sym}_n = \mathrm{Sym}_n \times \mathbf{H}^n.$$

Then \mathbf{G} acts on $\mathbf{V} = \mathbb{C}^{mn}$ as the unitary group of all $mn \times mn$ block permutation matrices with each block a matrix in \mathbf{H} . We adopt a standard left notation for wreath products and write each element of \mathbf{G} as the product of a permutation in Sym_n and an n -tuple of matrices from \mathbf{H} ,

$$\mathbf{G} = \{\sigma(h_1, \dots, h_n) : h_i \in \mathbf{H}, \sigma \in \mathrm{Sym}_n\},$$

so that

$$g(x_1, \dots, x_n) = (h_{\sigma(1)}x_{\sigma(1)}, \dots, h_{\sigma(n)}x_{\sigma(n)})$$

for $g = \sigma^{-1}(h_1, \dots, h_n)$, where each x_i lies in \mathbb{C}^m . (This choice makes later computations easier.)

Define a subgroup sequence

$$\{I\} = \mathbf{G}_0 < \mathbf{G}_1 < \dots < \mathbf{G}_{2n-1} = \mathbf{G}$$

by setting

$$\begin{aligned} \mathbf{G}_{2\ell-1} &= \{\sigma(h_1, \dots, h_\ell, 1, \dots, 1) : \sigma \in \mathrm{Sym}_\ell\} && \text{for } \ell = 1, \dots, n, \\ \mathbf{G}_{2\ell} &= \{\sigma(h_1, \dots, h_{\ell+1}, 1, \dots, 1) : \sigma \in \mathrm{Sym}_\ell\} && \text{for } \ell = 1, \dots, n-1 \end{aligned}$$

(viewing Sym_ℓ as a subset of Sym_n) so that the subgroups \mathbf{G}_k give block diagonal matrix groups:

$$\begin{aligned} \mathbf{G}_{2\ell-1} &= (\mathbf{H} \wr \mathrm{Sym}_\ell) \oplus \{I_{m(n-\ell)}\} && \text{for } \ell = 1, \dots, n, \\ \mathbf{G}_{2\ell} &= (\mathbf{H} \wr \mathrm{Sym}_\ell) \oplus \mathbf{H} \oplus \{I_{m(n-\ell-1)}\} && \text{for } \ell = 1, \dots, n-1, \end{aligned}$$

with I_k the $k \times k$ identity matrix. An obvious choice of coset leaders for pairs of consecutive subgroups arises. We select block diagonal matrices with one

block from \mathbf{H} and the rest the identity, or we choose cycles in the symmetric group ending at a fixed index: Set

$$\begin{aligned} \text{CL}(\mathbf{G}_{2\ell}/\mathbf{G}_{2\ell-1}) &= \{(1, \dots, 1, h, 1, \dots, 1) : h \in \mathbf{H} \text{ in the } (\ell + 1)\text{-th slot}\}, \\ \text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell}) &= \{(j \ j + 1 \ \dots \ \ell + 1) \in \text{Sym}_{\ell+1} : 1 \leq j \leq \ell + 1\}. \end{aligned}$$

Fix a unit vector \mathbf{v}_0 in \mathbb{C}^m suitable for \mathbf{H} ; this determines the stabilizer group $\text{Stab}_{\mathbf{H}}(\mathbf{v}_0)$. Extend \mathbf{v}_0 to a initial vector \mathbf{x}_0 for \mathbf{G} by setting

$$\mathbf{x}_0 = (u_1 \mathbf{v}_0, u_2 \mathbf{v}_0, \dots, u_n \mathbf{v}_0)$$

in \mathbf{V} for some real numbers u_i with $0 < u_1 < \dots < u_n$ such that \mathbf{x}_0 has unit length. Note that $\text{Stab}_{\mathbf{G}}(\mathbf{x}_0) = (\text{Stab}_{\mathbf{H}}(\mathbf{v}_0))^n$.

Theorem 33. *Let \mathbf{H} be a finite unitary group and let $\mathbf{G} = \mathbf{H} \wr \text{Sym}_n$ with the above subgroup sequence and initial vector. The above choice of coset leaders is greed compatible.*

Proof. We first note conditions that minimize a distance $\|g\mathbf{x} - \mathbf{x}_0\|$ over g in \mathbf{G} . Fix $\mathbf{x} = (x_1, \dots, x_n)$ in $\mathbf{V} = \mathbb{C}^{mn}$ with each x_i in \mathbb{C}^m and write an arbitrary g in \mathbf{G} as a product $\sigma^{-1}(h_1, \dots, h_n)$ with each h_i in \mathbf{H} and σ in Sym_n . Then using the (\mathbf{G} -invariant) standard inner product,

$$\|g\mathbf{x} - \mathbf{x}_0\|^2 = \|\mathbf{x}_0\|^2 + \|\mathbf{x}\|^2 - 2 \sum_{1 \leq j \leq n} u_j \text{Re}(\mathbf{v}_0^H h_{\sigma(j)} x_{\sigma(j)})$$

where the superscript H denotes conjugate transpose. The distance $\|g\mathbf{x} - \mathbf{x}_0\|^2$ is minimal when the summation over j in the last expression is maximal. But recall that for any two strictly increasing sequences of positive real numbers $0 < \alpha_1 < \dots < \alpha_k$ and $0 < \beta_1 < \dots < \beta_k$, the sum $\sum a_j b_{\tau(j)}$ is maximized over all τ in Sym_k by $\tau = I$. Hence $\|g\mathbf{x} - \mathbf{x}_0\|$ is minimal over all g in \mathbf{G} when

- (a) h_i maximizes $\text{Re}(\mathbf{v}_0^H h_i x_i)$ over all elements in \mathbf{H} for $i = 1, \dots, n$, and
- (b) σ in Sym_n is chosen so that

$$\text{Re}(\mathbf{v}_0^H h_{\sigma(1)} x_{\sigma(1)}) \leq \dots \leq \text{Re}(\mathbf{v}_0^H h_{\sigma(n)} x_{\sigma(n)}).$$

Note that if each h_i in (a) above is unique and the inequalities in (b) are strict, then a unique group element g minimizes $\|g\mathbf{x} - \mathbf{x}_0\|$. We apply this observation to the subgroups \mathbf{G}_k in the subgroup sequence and conclude that

$$\begin{aligned} \text{FR}(\mathbf{G}_{2\ell-1}) &= \{(w_1, \dots, w_n) : w_i \in \mathbb{C}^m, \text{Re}(\mathbf{v}_0^H w_1) < \dots < \text{Re}(\mathbf{v}_0^H w_\ell), \\ &\quad \text{Re}(\mathbf{v}_0^H w_i) > \text{Re}(\mathbf{v}_0^H h w_i) \text{ for all } I \neq h \in \mathbf{H}, 1 \leq i \leq \ell\}, \\ \text{FR}(\mathbf{G}_{2\ell}) &= \{(w_1, \dots, w_n) : w_i \in \mathbb{C}^m, \text{Re}(\mathbf{v}_0^H w_1) < \dots < \text{Re}(\mathbf{v}_0^H w_\ell), \\ &\quad \text{Re}(\mathbf{v}_0^H w_i) > \text{Re}(\mathbf{v}_0^H h w_i) \text{ for all } I \neq h \in \mathbf{H}, 1 \leq i \leq \ell + 1\}. \end{aligned}$$

The closures of the fundamental regions are obtained by changing all the strict inequalities in the above descriptions to nonstrict inequalities.

We show that if $\mathbf{x} \in \overline{\text{FR}(\mathbf{G}_k)}$, then there exists a coset leader d such that $d\mathbf{x} \in \overline{\text{FR}(\mathbf{G}_{k+1})}$ by treating the even and odd cases separately.

Suppose \mathbf{x} lies in some $\overline{\text{FR}(\mathbf{G}_{2\ell})}$. Choose a coset leader d from $\text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell})$ with $d\mathbf{x} = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$ and

$$\text{Re}(\mathbf{v}_0^H x_{\sigma^{-1}(1)}) \leq \dots \leq \text{Re}(\mathbf{v}_0^H x_{\sigma^{-1}(\ell+1)}).$$

That is, d is the cyclic permutation $\sigma = (j \ j+1 \ \dots \ \ell+1) \in \text{Sym}_{\ell+1}$ such that application of d results in the insertion of $\text{Re}(\mathbf{v}_0^H x_{\ell+1})$ into its proper place in the order. Then $d\mathbf{x}$ lies in $\overline{\text{FR}(\mathbf{G}_{2\ell+1})}$.

Now suppose \mathbf{x} instead lies in $\overline{\text{FR}(\mathbf{G}_{2\ell-1})}$ and choose an element h in \mathbf{H} maximizing $\text{Re}(\mathbf{v}_0^H h x_{\ell+1})$. Let d in $\text{CL}(\mathbf{G}_{2\ell}/\mathbf{G}_{2\ell-1})$ be the corresponding coset leader (i.e., $d = I_\ell \oplus h \oplus I_{nm-\ell-1}$). Then $d\mathbf{x}$ lies in $\overline{\text{FR}(\mathbf{G}_{2\ell})}$.

Hence each $\text{CL}(\mathbf{G}_k/\mathbf{G}_{k-1})$ is a set of greed compatible coset leaders for k even or odd. \square

Theorem 15 implies that the subgroup decoding algorithm decodes wreath product codes robustly:

Corollary 34. *Let \mathbf{H} be a finite unitary group and let $\mathbf{G} = \mathbf{H} \wr \text{Sym}_n$ with the above natural choice of subgroup sequence, coset leaders, and initial vector. Then the subgroup decoding algorithm decodes robustly.*

We now investigate error control for wreath products. We fix a set of generators X_k for each subgroup \mathbf{G}_k in the subgroup sequence: If k is odd, we choose block diagonal matrices that are the identity except first block from \mathbf{H} together with a set of consecutive transpositions in Sym_n ; if k is even, we add on block diagonal matrices that are the identity except for a single block from \mathbf{H} . Set

$$\begin{aligned} X_{2\ell-1} &= \{(h, 1, \dots, 1), h \in X_{\mathbf{H}}\} \cup \{(1 \ 2), (2 \ 3), \dots, (\ell-1 \ \ell)\}, \\ X_{2\ell} &= X_{2\ell-1} \cup \{(1, \dots, 1, h, 1, \dots, 1) : h \in \mathbf{H} \text{ in the } (\ell+1)\text{-th slot}\}. \end{aligned}$$

With these choices, we have good error control:

Proposition 35. *Let \mathbf{H} be a finite unitary group and let $\mathbf{G} = \mathbf{H} \wr \text{Sym}_n$. The above natural choice of subgroup sequence, coset leaders, initial vector, and generators for each subgroup in the subgroup sequence satisfies Error Control Property 29.*

Proof. Fix a pair of nested subgroups with smaller group of odd index, say $\mathbf{G}_{2\ell-1} < \mathbf{G}_{2\ell}$. Take any b in $X_{2\ell}$ and any $c = (1, \dots, 1, h, 1, \dots, 1)$ in $\text{CL}(\mathbf{G}_{2\ell}/\mathbf{G}_{2\ell-1})$, with $h \in \mathbf{H}$. If b lies in $X_{2\ell-1}$, then b and c commute and $c^{-1}bc = b \in X_{2\ell-1}$. If $b \notin X_{2\ell-1}$, then $bc \in \text{CL}(\mathbf{G}_{2\ell}/\mathbf{G}_{2\ell-1})$. Thus Error Control Property 29 is satisfied.

Now fix a pair of nested subgroups with smaller group of even index, say $\mathbf{G}_{2\ell} < \mathbf{G}_{2\ell+1}$. Take any b in $X_{2\ell+1}$ and any $c = (j \ j+1 \ \dots \ \ell+1)$ in $\text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell})$. First suppose $b = (h, 1, \dots, 1)$ with h in \mathbf{H} . If $j > 1$, then $c^{-1}bc = b \in X_{2\ell}$ (as c and b commute), while if $j = 1$, then $c^{-1}bc =$

$(1, \dots, 1, h, 1, \dots, 1) \in X_{2\ell}$. Now suppose that $b = (i-1 \ i)$ for some $i \leq \ell+1$. If $i < j$, then $c^{-1}bc = b \in X_{2\ell}$ as c and b commute; if $i = j$, then bc is the coset leader $(i-1 \ \dots \ \ell+1) \in \text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell})$; if $i = j+1$, then bc is the coset leader $(i \ \dots \ \ell+1) \in \text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell})$; and if $j+1 < i$, then $c^{-1}bc = (i-2 \ i-1) \in X_{2\ell}$. Thus Error Control Property 29 is satisfied in this case as well. \square

Theorem 30 then implies that errors can be controlled when they occur:

Corollary 36. *Let \mathbf{H} be a finite unitary group and let $\mathbf{G} = \mathbf{H} \wr \text{Sym}_n$ with the above natural choice of subgroup sequence, coset leaders, initial vector, and generating sets $X_k \subset \mathbf{G}$ for each \mathbf{G}_k . Assume the Nearest Neighbors Property 28 holds. If a received vector lands in the decoding region containing a nearest neighbor of $g^{-1}\mathbf{x}_0$ due to noise, then the subgroup decoding algorithm decodes it to a group element differing from g in only one factor when written as a product of coset leaders.*

Remark 37. One may interpolate a sequence of subgroups of \mathbf{H} to refine the above process and improve the decoding efficiency. At the even stages, one could splice a fixed subgroup sequence for \mathbf{H} into the $(l+1)$ -st coordinate and replace $\mathbf{G}_{2\ell}$ with a new sequence. One should take robust coset leaders for the subgroup sequence of \mathbf{H} and fix generators satisfying the Error Control Property 29 for \mathbf{H} so that the wreath product $\mathbf{G} = \mathbf{H} \wr \text{Sym}_n$ with the refined subgroup sequence would also inherit robust decoding with error control. But one could also use other methods to decode \mathbf{H} at the even steps. That is the process envisioned in the decoding of wreath products in Nation and Walker [13], where the Snowflake Algorithm is used to decode \mathbf{H} at the even steps.

15. INFINITE FAMILY OF COMPLEX REFLECTION GROUPS $\mathbf{G}(r, 1, n)$

We apply the above decoding program to the complex reflection groups $\mathbf{G}(r, 1, n)$ for arbitrary integers $n, r \geq 1$ in this section. We obtain efficient codes with good error control properties that resist channel noise. These groups are wreath products acting by isometries on \mathbb{C}^n , specifically, extensions of $(\mathbb{Z}/r\mathbb{Z})^n$ by the symmetric group Sym_n :

$$\mathbf{G}(r, 1, n) \cong \text{Sym}_n \ltimes (\mathbb{Z}/r\mathbb{Z})^n \quad \text{and} \quad |\mathbf{G}(r, 1, n)| = n! r^n.$$

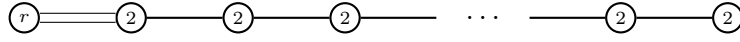
Let ξ be the primitive complex r -th root-of-unity $e^{\frac{2\pi i}{r}}$, so that $\mathbf{G}(r, 1, n)$ is the set all matrices with a single nonzero entry in each row and in each column, that entry being a power of ξ .

Consider the diagonal transformations a_i ($1 \leq i \leq n$) that multiply the i -th entry of a vector by ξ and the transpositions b_j for $1 \leq j < n$ that switch the j -th and $(j+1)$ -st coordinates. Then b_1, \dots, b_{n-1} generate the symmetric group $\mathbf{G}(1, 1, n) \leq \mathbf{G}(r, 1, n)$ and every element of $\mathbf{G}(r, 1, n)$ can be written uniquely as a product of a permutation matrix (generated by the b_i) and a diagonal matrix (generated by the a_i). Fix an initial vector $\mathbf{x}_0 = (u_1, \dots, u_n)$ with $0 < u_1 < \dots < u_n$ real.

15.1. $\mathbf{G}(r, 1, n)$: **Defining relations.** We will use the Coxeter-like abstract presentation for $\mathbf{G}(r, 1, n)$ in terms of generators and canonical braid relations:

$$\begin{aligned} \mathbf{G}(r, 1, n) = \langle a_1, b_1, \dots, b_{n-1} : & a_1^r = 1 = b_i^2, \\ & b_i b_j = b_j b_i \text{ for } |i - j| > 1, a_1 b_j = b_j a_1 \text{ for } 1 \neq j \neq 2, \\ & b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}, a_1 b_1 a_1 b_1 = b_1 a_1 b_1 a_1 \rangle. \end{aligned}$$

In other words, the following Coxeter-Dynkin diagram gives the abstract group structure for $\mathbf{G}(r, 1, n)$:



15.2. $\mathbf{G}(r, 1, n)$: **Subgroup sequence, coset leaders, and generators.** Consider the nested sequence of subgroups

$$\{I\} = \mathbf{G}_0 < \mathbf{G}_1 < \dots < \mathbf{G}_{2n-1} = \mathbf{G}$$

given as block diagonal matrix groups

$$\begin{aligned} \mathbf{G}_{2\ell-1} &= \mathbf{G}(r, 1, \ell) \oplus \{I_{n-\ell}\} && \text{for } \ell = 1, \dots, n, \\ \mathbf{G}_{2\ell} &= \mathbf{G}(r, 1, \ell) \oplus \mathbf{G}(r, 1, 1) \oplus \{I_{n-\ell-1}\} && \text{for } \ell = 1, \dots, n-1 \end{aligned}$$

where I_ℓ is the $\ell \times \ell$ identity matrix. Fix coset leaders for \mathbf{G}_k over \mathbf{G}_{k-1} by setting

$$\begin{aligned} \text{CL}(\mathbf{G}_{2\ell}/\mathbf{G}_{2\ell-1}) &= \{I, a_{\ell+1}, a_{\ell+1}^2, \dots, a_{\ell+1}^{r-1}\}, \\ \text{CL}(\mathbf{G}_{2\ell+1}/\mathbf{G}_{2\ell}) &= \{I, b_\ell, b_{\ell-1} b_\ell, \dots, b_2 b_3 \cdots b_\ell, b_1 b_2 \cdots b_\ell\}. \end{aligned}$$

We choose generators $X_k \subset \mathbf{G}$ for the subgroups \mathbf{G}_k to reflect the fact that (at the even steps) \mathbf{G}_{2k} is obtained by adding adding a generator $a_{\ell+1}$ that commutes with the elements of \mathbf{G}_{2k-1} and (at the odd steps) $\mathbf{G}_{2\ell+1}$ is obtained by adding adding the transposition b_ℓ : Set

$$\begin{aligned} X_{2\ell-1} &= \{a_1, b_1, b_2, \dots, b_{\ell-1}\}, \\ X_{2\ell} &= \{a_1, b_1, b_2, \dots, b_{\ell-1}, a_{\ell+1}\}. \end{aligned}$$

15.3. $\mathbf{G}(r, 1, n)$: **Correct and Robust Decoding.** The above choices coincide with the natural choice of subgroup sequence, coset leaders, and initial vector for general wreath products given in Section 14. Thus Corollary 34 implies

Corollary 38. *With the above choice of subgroup sequence, coset leaders, and initial vector, the subgroup decoding algorithm for $\mathbf{G}(r, 1, n)$ (for any r and any n) decodes robustly: For all g in $\mathbf{G}(r, 1, n)$, any received vector in the decoding region of g decodes to g .*

TABLE 15.2.1. Subgroup sequence for $\mathbf{G}(r, 1, n)$

k	Generating set X_k for \mathbf{G}_k	Coset leaders for \mathbf{G}_k over \mathbf{G}_{k-1}
0	I	
1	a_1	$a_1, a_1^2, \dots, a_1^r = I$
2	a_1, a_2	$a_2, a_2^2, \dots, a_2^r = I$
3	a_1, b_1	I, b_1
4	a_1, b_1, a_3	$a_3, a_3^2, \dots, a_3^r = I$
5	a_1, b_1, b_2	$I, b_2, b_1 b_2$
\vdots	\vdots	\vdots
$2n - 2$	$a_1, b_1, \dots, b_{n-2}, a_n$	$a_n, a_n^2, \dots, a_n^r = I$
$2n - 1$	a_1, b_1, \dots, b_{n-1}	$I, (b_j \cdots b_{n-1})$ for $1 \leq j \leq n - 1$

15.4. $\mathbf{G}(r, 1, n)$: Implementing the Decoding Algorithm Explicitly.

Although the last corollary shows that the algorithm decodes correctly, it is helpful to point out explicitly how one implements the algorithm by hand using the ideas in the proof of Theorem 33. Suppose $\mathbf{r} = (x_1, \dots, x_n)$ is a received vector in \mathbb{C}^n , and recall that $\mathbf{x}_0 = (u_1, \dots, u_n)$ with $0 < u_1 < \dots < u_n$ real. Consider the sequence

$$\begin{aligned}
& \|\mathbf{r} - \mathbf{x}_0\| \\
& \|a_1^k \mathbf{r} - \mathbf{x}_0\| \\
& \|a_2^\ell a_1^k \mathbf{r} - \mathbf{x}_0\| \\
& \|b_1^\delta a_2^\ell a_1^k \mathbf{r} - \mathbf{x}_0\| \\
& \|a_3^m b_1^\delta a_2^\ell a_1^k \mathbf{r} - \mathbf{x}_0\| \\
& \|ca_3^m b_1^\delta a_2^\ell a_1^k \mathbf{r} - \mathbf{x}_0\| \\
& \vdots
\end{aligned}$$

where c is a coset leader for \mathbf{G}_5 over \mathbf{G}_4 , thus one of $\{I, b_2, b_1 b_2\}$. First k is chosen to maximize $\operatorname{Re}(\xi^k x_1)$, then ℓ to maximize $\operatorname{Re}(\xi^\ell x_2)$. Now since $u_1 < u_2$, an easy calculation shows that if $\operatorname{Re}(\xi^k x_1) > \operatorname{Re}(\xi^\ell x_2)$, then we should apply b_1 , switching the values, to minimize the distance; otherwise not (so that δ is 0 or 1). Next m is chosen to maximize $\operatorname{Re}(\xi^m x_3)$. Then, since $u_1 < u_2 < u_3$, we apply the correct coset leader c (a permutation) to put $\operatorname{Re}(\xi^k x_1)$, $\operatorname{Re}(\xi^\ell x_2)$, $\operatorname{Re}(\xi^m x_3)$ into increasing order (an insertion sort). Continue until pau.

Remark 39. An observation in the proof of Theorem 33 can be used to speed up the algorithm considerably. Writing $x = |x|e^{i\theta}$, we maximize the

real part of $\xi^k x = |x|e^{(\frac{2\pi k}{r} + \theta)i}$ by making $\frac{2\pi k}{r} + \theta$ as close to 2π as possible. Thus k should be chosen as the nearest integer to $r - \frac{r\theta}{2\pi}$.

15.5. $\mathbf{G}(r, 1, n)$: Initial vector. We refine our choice of initial vector so that neighbors of \mathbf{x}_0 are just its images under the natural generating set a_1, b_1, \dots, b_{n-1} in order to control errors. We mimic construction of an optimal vector for the Coxeter group \mathbf{WB}_n . If we take a real vector \mathbf{x}_0 of the form

$$\mathbf{x}_0 = (\alpha, \alpha + \beta, \alpha + 2\beta, \dots, \alpha + (n-1)\beta)$$

and require that

$$\|a_1\mathbf{x}_0 - \mathbf{x}_0\| = \|b_1\mathbf{x}_0 - \mathbf{x}_0\| = \dots = \|b_{n-1}\mathbf{x}_0 - \mathbf{x}_0\|,$$

then a straightforward computation gives

$$\frac{\beta}{\alpha} = \sqrt{1 - \cos \frac{2\pi}{r}}$$

which yields $\sqrt{2}\beta$ as the minimum distance of the code. Initially we set $\alpha = 1$, and then normalize so that $\|\mathbf{x}_0\| = 1$. Note that $\|a_i\mathbf{x}_0 - \mathbf{x}_0\|$ will be greater than $\sqrt{2}\beta$ for $i > 1$. This choice gives an initial vector with full orbit under \mathbf{G} , and the minimum distances of the code defined by this choice of \mathbf{x}_0 (for various r and n) have a reasonable order of magnitude. Table 15.5.1 gives the values achieved for small values of r and n .

TABLE 15.5.1. Actual d_{min} obtained for some $\mathbf{G}(r, 1, n)$

r	$n = 2$	$n = 3$	$n = 4$
3	.71	.41	.27
4	.63	.38	.26
5	.56	.35	.24
6	.51	.32	.23
7	.46	.30	.21
8	.42	.28	.20

15.6. $\mathbf{G}(r, 1, n)$: Controlling Errors. The above choices of subgroup sequence, coset leaders, and initial vector for $\mathbf{G}(r, 1, n)$ are consistent with those from Section 14 for general wreath products. Thus Proposition 35 implies Error Control Property 29 for $\mathbf{G}(r, 1, n)$.

We now check directly that Nearest Neighbors Property 28 holds as well, i.e., we check that if $g\mathbf{x}_0$ is any nearest neighbor of \mathbf{x}_0 , then g lies in $X_{\mathbf{G}} \cup X_{\mathbf{G}}^{-1}$. We argue that if $g \neq I, a_1, a_1^{-1}$ or some b_j , then $\|g\mathbf{x}_0 - \mathbf{x}_0\|^2 > 2\beta^2 = d_{min}$. This distance squared is the sum of terms of the form

$$|\xi^t(\alpha + j\beta) - (\alpha + \ell\beta)|^2$$

for integers j and ℓ . One may verify that if $j = \ell$ and $t \neq 0$, then this expression is at least $2\beta^2$, while if $j \neq \ell$, then it is at least β^2 and there are at least two such terms.

Corollary 31 then implies error control for the groups $\mathbf{G}(r, 1, n)$:

Corollary 40. *For $\mathbf{G} = \mathbf{G}(r, 1, n)$, assume the above natural choice for subgroup sequence, initial vector, coset leaders, and generating sets $X_k \subset \mathbf{G}$ for each \mathbf{G}_k . If a received vector lands in the decoding region containing a nearest neighbor of $g^{-1}\mathbf{x}_0$ due to noise, then the subgroup decoding algorithm decodes it to a group element differing from g in only one factor when written as a product of coset leaders.*

15.7. $\mathbf{G}(r, 1, n)$: Efficient Decoding. We argue that the above choices for $\mathbf{G}(r, 1, n)$ also yield efficient decoding using navigation through the coset leader graphs as described in Section 13. One can check directly that each coset leader graph is connected (see Definition ??) for $\mathbf{G}(r, 1, n)$. The graphs for $\mathbf{G}(4, 1, 4)$ are given in Figure 15.7. (Note that Kriloff and Lay [16] show existence of Hamiltonian cycles for the Cayley graphs of $\mathbf{G}(r, 1, n)$.) We use Remark 39 and the explicit decoding process described after Corollary 38. At stages $1, 2, 4, \dots, 2k$ where the coset leader graphs are cyclic, we can choose in one step the coset leader that moves the received vector closest to the initial vector. For the permutation stages $3, 5, \dots, 2k+1$, the graph gives an insertion sort. As in [10], a modified insertion sort could also be used to shorten the decoding somewhat. Hence the coset leader graphs for $\mathbf{G}(r, 1, n)$ are particularly easy to navigate, compared to most unitary groups.

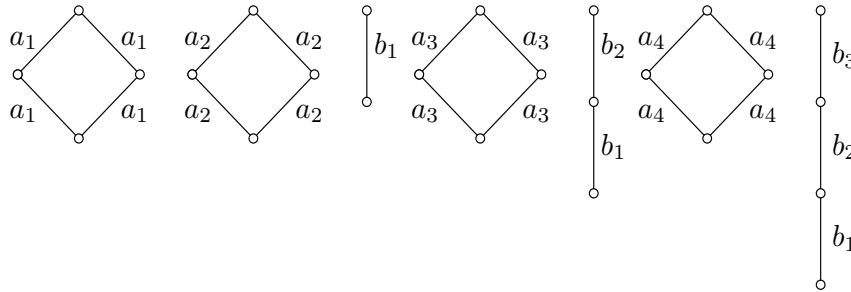


FIGURE 15.7.1. Coset leader graphs for $\mathbf{G}(4, 1, 4)$

15.8. $\mathbf{G}(r, 1, n)$: Number of Steps in the Algorithm. Assuming that we use the method indicated in the last subsection to navigate the cyclic coset leader graphs, the analysis of the average number of steps to decode using $\mathbf{G}(r, 1, n)$ is identical to that given for the Weyl group $\mathbf{WB}_n = \mathbf{G}(2, 1, n)$ in

Fossorier, Nation and Peterson [10]. In other words, for any $r \geq 2$, one can decode $\mathbf{G}(r, 1, n)$ just as fast as $\mathbf{G}(2, 1, n)$. Moreover, exactly as in [10], one can speed up the sorting by using a slightly different subgroup sequence, which amounts to using an improved insertion sort. We omit the details and give the results.

Asymptotically, the number of steps in decoding is $\frac{n^2}{4}$ for the subgroup sequence given here, and $\frac{n^2}{8}$ for the modified sort. But for moderate values of n , the number of steps is fewer than that would indicate, and in fact close to the theoretical minimum. Some of these numbers are given in Table 15.8.1, where

- γ_n is the average number of comparisons to decode using intermediate subgroups with a standard insertion sort,
- γ'_n is the average number of comparisons to decode using intermediate subgroups with a modified insertion sort,
- $n + \log_2 n!$ is the theoretical minimum average number of comparisons; see Knuth [21].

TABLE 15.8.1. Average number of comparisons to decode $\mathbf{G}(r, 1, n)$

n	γ_n	γ'_n	$n + \log_2 n!$
4	8.9	8.7	8.6
8	27.3	24.0	23.3
16	88.6	67.7	60.3
32	307.9	204.5	149.7

16. REMARKS ON INITIAL VECTOR AND MINIMAL DISTANCE OF THE CODE

How does choice of initial vector determine the effectiveness of an arbitrary group code? We discuss factors influencing the choice of initial vector under subgroup decoding. In the next section, we give some experimental data comparing minimal distance of group codes and their decoding complexity.

16.1. Suboptimal minimal distance. The choice of initial vector determines the minimal distance d_{min} of the code; one usually regards the largest possible minimal distance as optimal in coding theory, as decoding errors are minimized when codewords are as far away from each other as possible. Mittelholzer and Lahtonen [9] gave an elegant and simple solution to the problem of choosing the initial vector in the case \mathbf{G} is a Coxeter group: Any unit vector in the fundamental region can be taken for the initial vector, some work better than others, and there is a straightforward algorithm to find the optimal choice.

The geometry of arbitrary groups acting on complex space prevents a clean generalization. In the last section, we gave some explicit minimal distances for the codes built on $\mathbf{G}(r, 1, n)$. The choice of initial vector gives robust decoding and good error control. But this choice does not yield the optimal minimum distance of the code (although it approaches the optimum value as r increases). In some examples, for small values of r and n , an initial vector \mathbf{x}_0 for $\mathbf{G}(r, 1, n)$ which yields the optimal minimal distance of the code can come at a price: greed-compatible coset leaders may not exist and thus subgroup decoding does not work. Thus in practical applications, we often settle for an initial vector giving less than the optimal minimal distance in order to gain robust decoding.

16.2. Geometric uniformity. The following simple observations on “geometric uniformity” (discussed by Forney [5] for Euclidean spaces) nevertheless can be useful in choosing an initial vector.

Observation 41. *Fix an initial vector \mathbf{x}_0 .*

- (1) *If c is a complex number with $|c| = 1$, and $\mathbf{y}_0 = c\mathbf{x}_0$, then the code $\mathbf{G}\mathbf{y}_0$ has the same minimum distance as $\mathbf{G}\mathbf{x}_0$. The nearest neighbors of \mathbf{y}_0 are the vectors $a\mathbf{y}_0$ with $a \in N_{\mathbf{G}}$.*
- (2) *If $h \in \mathbf{G}$ and $\mathbf{z}_0 = h\mathbf{x}_0$, then the code $\mathbf{G}\mathbf{z}_0$ also has the same minimum distance as $\mathbf{G}\mathbf{x}_0$. In this case, the nearest neighbors of \mathbf{z}_0 are the vectors $b\mathbf{z}_0$ with $b \in hN_{\mathbf{G}}h^{-1}$.*

The first part of the lemma suggests that the first entry of \mathbf{x}_0 may be taken to be real (or imaginary), which can be useful. Although we often choose the initial vector \mathbf{x}_0 to be a *real* unit vector, note that occasionally it is crucial for the minimality of coset leaders that the initial vector *not* be real. In either case, we usually adjust the entries to make neighbors realized by a preferred set of generators (for example, reflections). The preceding observation gives us some guidance in making these adjustments.

17. EXPERIMENTS AND COMPARISONS OF GROUP CODES

What is the trade-off in group coding when choosing a large minimum distance over a low decoding complexity? We give some experimental data comparing group codes in this section. We also report on ideas for group coding over the quaternions and experimental attempts for successful decoding using exceptional complex reflection groups.

17.1. Quaternions. There is an obvious generalization of the reflection groups $\mathbf{G}(r, 1, n)$ that will have the same good decoding properties. These are the groups $\mathbb{P}(\mathbf{K}, n)$ of all $n \times n$ permutation matrices whose nonzero entries are from a group \mathbf{K} of complex numbers z with $|z| = 1$, or more generally, quaternions w with $|w| = 1$. For example, we could take

$$\mathbf{K} = \{z \in \mathbb{C} : z^{2^k} = 1 \text{ for some } k \geq 1\} .$$

This is an infinite group, but for any given application we would only use a finite part of it, although without a predetermined bound. Likewise, there are a few finite multiplicative subgroups of unit quaternions that could be used as entries in the permutation matrices; see Kranek [22] or Lehrer and Taylor [23]. As an exercise, we programmed a simulation of coding with $\mathbb{P}(\mathbb{H}, 3)$ with \mathbb{H} the 8-element quaternion group.

17.2. Comparing group codes. We now give a table comparing some group codes of similar sizes. We include two Coxeter groups, two complex reflection groups in the family $\mathbf{G}(r, 1, n)$, the wreath product of an exceptional complex reflection group with a symmetric group, and the wreath product of the quaternion group \mathbb{H} with a symmetric group. We include the exceptional complex reflection group and quaternion group individually in the table for comparison.

We measure the decoding complexity by counting the average number of comparisons required to decode a received vector, i.e., the number of comparisons of lengths of vectors or distances between vectors. We used the decoding methods described in this paper, except that for \mathbf{G}_4 and $\mathbf{G}_4 \wr \text{Sym}_4$ we used the Snowflake algorithm (discussed in the next section) to illustrate how methods can be mixed with wreath products (see Remark 37).

The first column names the acting group \mathbf{G} , the second column gives the size of the group code, the third column gives the length of the code (the dimension of \mathbf{V} in terms of the base field \mathbb{R} , \mathbb{C} or \mathbb{H}), the fourth column gives the minimum distance d_{min} of the code, and the last column gives the approximate average number of comparisons in decoding.

TABLE 17.2.1. Size, length, minimum distance, and average number of comparisons to decode for various group codes

Group	$ \mathbf{G} $	length	d_{min}	comparisons
Sym_{10}	$10! = 3,628,800$	10	.156	23.3
$\mathbf{WB}_8 = \mathbf{G}(2, 1, 8)$	$2^8 8! = 1,032,092$	8	.104	24.0
$\mathbf{G}(4, 1, 6)$	$4^6 6! = 2,932,120$	6	.148	15.7
$\mathbf{G}(8, 1, 5)$	$8^5 5! = 3,932,160$	5	.154	12.1
\mathbf{G}_4	24	2	.866	4.21
$\mathbf{G}_4 \wr \text{Sym}_4$	$(24)^4 4! = 7,962,624$	8	.213	21.5
\mathbb{H}	8	1	1.414	1
$\mathbb{H} \wr \text{Sym}_5$	$8^5 5! = 3,932,160$	5	.191	12.1

17.3. Subgroups of $\mathbf{G}(r, 1, n)$. For any divisor p of r , recall that $\mathbf{G}(r, p, n)$ is a reflection subgroup of $\mathbf{G}(r, 1, n)$. The properties that make subgroup decoding work well for the groups $\mathbf{G}(r, 1, n)$ seem not to hold for the groups

$\mathbf{G}(r, p, n)$ with $p > 1$, except for the real group $\mathbf{WD}_n = \mathbf{G}(2, 2, n)$ (see [10]). A general choice of subgroup sequence, initial vector, and coset leaders that is greed compatible seems elusive. In addition, we have not been able to find choices giving the Error Control Property 11. This leaves the question: *Is there any good decoding scheme for the groups $\mathbf{G}(r, p, n)$ with $p > 1$?*

17.4. Tetrahedral group \mathbf{G}_4 , Octahedral \mathbf{G}_8 , Icosahedral \mathbf{G}_{16} . In Section 12.1 we saw that subgroup decoding worked for codes based on the tetrahedral group \mathbf{G}_4 using a careful choice of the subgroup sequence and initial vector. There are two other reflection groups of this type, the octahedral group \mathbf{G}_8 and the icosahedral group \mathbf{G}_{16} . These groups are generated by matrices A and B satisfying the equations $A^k = B^k = I$ and $ABA = BAB$ for $k = 3, 4$ and 5 respectively:

- $k = 3$ gives \mathbf{G}_4 with 24 elements.
- $k = 4$ gives \mathbf{G}_8 with 96 elements.
- $k = 5$ gives \mathbf{G}_{16} with 600 elements.

For the octahedral group, if we take the natural subgroup sequence $\{I\} < \{I, A, A^2, A^3\} < \mathbf{G}_8$ and a *nonreal* unit vector \mathbf{x}_0 such that $\|A^{-1}\mathbf{x}_0 - \mathbf{x}_0\| = \|B^{-1}\mathbf{x}_0 - \mathbf{x}_0\|$, then coset leaders can be chosen minimal and the subgroup decoding algorithm decodes correctly with some noise.

On the other hand, we have not been able to find a combination of subgroup sequence and initial vector that gives minimal coset leaders for a code based on the icosahedral group \mathbf{G}_{16} . For example, for a standard matrix representation and subgroup sequence $\{I\} < \{I, A, A^2, A^3, A^4\} < \mathbf{G}_{16}$, ties arise in a rather unexpected way:

$$B^3A^4B^3 = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \quad \text{and} \quad B^3A^4B^3A^4 = \begin{bmatrix} c & 0 \\ 0 & \bar{c} \end{bmatrix}$$

where $c = e^{\frac{\pi}{5}i}$.

17.5. Hessian groups \mathbf{G}_{25} and \mathbf{G}_{26} . We have not found a subgroup decoding scheme that works for the complex reflection groups \mathbf{G}_{25} and \mathbf{G}_{26} . Despite repeated attempts, using computerized search programs (testing all subgroup sequences), we have been unable to find a subgroup sequence and initial vector yielding greed compatible coset leaders for these groups.

18. CONCLUSIONS

Subgroup decoding works well for codes based on the groups $\mathbf{G}(r, 1, n)$, which are wreath products of cyclic groups, thus generalizing codes based on the real reflection groups $\mathbf{WA}_n \cong \text{Sym}_n$ and \mathbf{WB}_n . Codes based on these groups decode robustly, have good error control, and decode in few steps relative to the size of the group. There are problems with error control (Property 29) for the groups $\mathbf{G}(r, p, n)$ with $p > 1$ that generalize \mathbf{WD}_n . Subgroup decoding works on some of the exceptional unitary groups, but not others, and this seems to be inherent in the structure of the groups. In

general, good coding properties are preserved by wreath products, allowing us to build large codes from small ones.

This suggests that other decoding methods should be considered. Walker, building on the work of Kim [11], has designed an alternative algorithm for arbitrary unitary groups called the *Snowflake Algorithm*; see [12, 13]. The efficiency of this other decoding method varies from pretty good to very good, depending on the group action, in ways that we do not yet totally understand. In the Snowflake algorithm, the basic algorithm of group coding, transmitting $g^{-1}\mathbf{x}_0$ and decoding with $g'(\mathbf{r}) \approx \mathbf{x}_0$, remains unchanged. However, the use of a subgroup sequence is abandoned, so that the greedy aspect of the algorithm is no longer a factor. Rather, a set of generators is chosen for \mathbf{G} so that each group element will have a relatively short expression as a product of the generators. This expression may not be unique, but one such expression can be chosen as a canonical form for the element and tables of equivalent minimal expressions calculated. Using these, one can decode *correctly* with some noise, and for some groups it can be done *efficiently*. For those groups where the algorithm can be made efficient, including wreath products of the complex reflection groups \mathbf{G}_4 , \mathbf{G}_5 , \mathbf{G}_8 and \mathbf{G}_{20} , the Snowflake algorithm might provide an alternative method of decoding group codes.

19. APPENDIX I: A PRIMITIVE GROUP DECODING ALGORITHM

This paper has focused on subgroup decoding, which works very well for codes based on real reflection groups or the groups $\mathbf{G}(r, 1, n)$. These group codes may prove useful in certain practical situations. The same probably cannot be said for codes based on arbitrary unitary groups, though there may be applications which we cannot yet envision, e.g., in cryptography. Often, a choice of initial vector and subgroup sequence yielding an effective decoding algorithm (or one that even decodes correctly) remains elusive. In this appendix, we describe a very general type of decoding algorithm. Then we give an analog of Theorem 21: If a weak necessary condition is satisfied, then the algorithm decodes correctly when the received vector is sufficiently close to the sent codeword. The appendix is based on Kim [11]; a refined version is given in Walker [12].

The parameters for this type of decoding are

- a finite unitary group \mathbf{G} ,
- an initial unit vector \mathbf{x}_0 ,
- a generating set X for \mathbf{G} .

Again, the codewords are elements of the orbit $\mathbf{G}\mathbf{x}_0$, a codeword $\mathbf{x} = g^{-1}\mathbf{x}_0$ is transmitted, and the received vector is $\mathbf{r} = \mathbf{x} + \mathbf{n}$ where \mathbf{n} represents noise. The *primitive decoding algorithm* decodes as follows. We fix some predetermined $\varepsilon > 0$. Let $\mathbf{r}_0 = \mathbf{r}$. Recursively, given \mathbf{r}_k , find a transformation

$c_{k+1} \in X$ such that the vector $\mathbf{r}_{k+1} = c_{k+1}\mathbf{r}_k$ satisfies

$$\|\mathbf{r}_{k+1} - \mathbf{x}_0\| < \|\mathbf{r}_k - \mathbf{x}_0\| - \varepsilon .$$

If no such c_{k+1} exists, terminate and decode \mathbf{r} as $c_k \cdots c_1$.

For example, if \mathbf{G} is a reflection group, we might take X to be all reflections or a minimal generating set of reflections or anything in between. (Walker has shown that it may be necessary to include some nonreflections in the set X to obtain the condition (\ddagger) below.)

Let us assume that the pair X, \mathbf{x}_0 satisfies the condition that every non-trivial codeword is sent closer to the initial vector by some element of X :

(\ddagger) For any $\mathbf{w} \in \mathbf{G}\mathbf{x}_0$ with $\mathbf{w} \neq \mathbf{x}_0$, $\|c\mathbf{w} - \mathbf{x}_0\| < \|\mathbf{w} - \mathbf{x}_0\|$ for some $c \in X$.

(This is a condition satisfied by simple reflections in a Coxeter group: Every group element factors as a product of a minimum number of simple reflections generating the group, multiplying by the first factor decreases length, and length corresponds to distance back to some initial vector.)

We want to show that the procedure terminates and decodes correctly, i.e., at termination $c_k \cdots c_1 \in \mathbf{S}\mathbf{g}$ where $\mathbf{S} = \text{Stab}(\mathbf{x}_0)$. Clearly (\ddagger) is necessary for correct decoding, for if \mathbf{w} witnesses a failure of (\ddagger) , then \mathbf{w} cannot be decoded correctly even with no noise. For each codeword \mathbf{w} , let $\text{MG}(\mathbf{w})$ be the set of “minimal generators” c that minimize the distance from $c\mathbf{w}$ back to \mathbf{x}_0 over all c in $X \cup \{I\}$:

$$\text{MG}(\mathbf{w}) = \{c \in X \cup \{I\} : \|c\mathbf{w} - \mathbf{x}_0\| \leq \|d\mathbf{w} - \mathbf{x}_0\| \text{ for all } d \in X \cup \{I\}\}.$$

Then (\ddagger) is equivalent to the condition that $I \notin \text{MG}(\mathbf{w})$ whenever codeword $\mathbf{w} \neq \mathbf{x}_0$. Define

$$\delta = \min_{\substack{\mathbf{w} \in \mathbf{G}\mathbf{x}_0 - \{\mathbf{x}_0\} \\ c \in \text{MG}(\mathbf{w})}} \|\mathbf{w} - \mathbf{x}_0\| - \|c\mathbf{w} - \mathbf{x}_0\|$$

so that $\|\mathbf{w} - \mathbf{x}_0\| \geq \|c\mathbf{w} - \mathbf{x}_0\| + \delta$ for any $c \in \text{MG}(\mathbf{w})$. There are two versions of the algorithm. At each step, either

- (A) choose c_{k+1} to minimize $\|c_{k+1}\mathbf{r}_k - \mathbf{x}_0\|$, or
- (B) choose the first c_{k+1} such that $\|c_{k+1}\mathbf{r}_k - \mathbf{x}_0\| < \|\mathbf{r}_k - \mathbf{x}_0\| - \frac{1}{3}\delta$.

In either version, when there is no $c \in X$ such that $\|c\mathbf{r}_k - \mathbf{x}_0\| < \|\mathbf{r}_k - \mathbf{x}_0\| - \frac{1}{3}\delta$, we terminate and decode \mathbf{r} as $c_k \cdots c_1$.

We verify that either version of the primitive decoding algorithm works with some noise:

Theorem 42. *Assume that the pair X, \mathbf{x}_0 satisfies the condition (\ddagger) . Define δ as above. If $\|\mathbf{r} - g^{-1}\mathbf{x}_0\| < \delta/3$, then the procedure terminates in at most $\lceil 6/\delta \rceil$ steps and outputs $c_k \cdots c_1 \in g\mathbf{S}$.*

Proof. We show that each step of the algorithm moves us at least $\delta/3$ closer to the initial vector. Hence the process terminates in at most

$$(3/\delta) \max \|\mathbf{w} - \mathbf{x}_0\| \leq (3/\delta) 2 = 6/\delta$$

steps (not counting a possible terminal step of choosing I), where the max is taken over all codewords \mathbf{w} (on the unit sphere).

At step k , set $g' = c_k \cdots c_1$, $\mathbf{w} = g'g^{-1}\mathbf{x}_0$, and $\mathbf{r}_k = g'\mathbf{r}$. Suppose $\mathbf{w} \neq \mathbf{x}_0$. Note that $\|\mathbf{r}_k - \mathbf{w}\| = \|g'\mathbf{r} - g'g^{-1}\mathbf{x}_0\| < \delta/3$. By (‡) and the definition of δ , there exists $c \in \text{MG}(\mathbf{w})$ with

$$\begin{aligned} \|\mathbf{r}_k - \mathbf{x}_0\| &\geq \|\mathbf{w} - \mathbf{x}_0\| - \|\mathbf{r}_k - \mathbf{w}\| \\ &> \|c\mathbf{w} - \mathbf{x}_0\| + \delta - \delta/3 \\ &= \|c\mathbf{w} - \mathbf{x}_0\| + 2\delta/3 \end{aligned}$$

whilst

$$\begin{aligned} \|c\mathbf{r}_k - \mathbf{x}_0\| &\leq \|c\mathbf{w} - \mathbf{x}_0\| + \|c\mathbf{r}_k - c\mathbf{w}\| \\ &< \|c\mathbf{w} - \mathbf{x}_0\| + \delta/3. \end{aligned}$$

Thus

$$\|c\mathbf{r}_k - \mathbf{x}_0\| < \|\mathbf{r}_k - \mathbf{x}_0\| - \delta/3$$

making $c\mathbf{r}_k$ closer than \mathbf{r}_k to \mathbf{x}_0 by a step of length at least $\delta/3$ as desired. \square

20. APPENDIX II: PARTIAL GROUP CODES BASED ON $\mathbf{G}(r, 1, n)$

It can be advantageous to use a group code based on a proper subset of the codewords, $\mathbf{W} \subset \mathbf{G}\mathbf{x}_0 = \{g\mathbf{x}_0 : g \in \mathbf{G}\}$. In this appendix, we briefly indicate how this can be done to yield a significant improvement in codes based on $\mathbf{G}(r, 1, n)$.

Although the code based on $\mathbf{G}(r, 1, n)$ in Section 15 has good error control properties, a problem arises: the distance between adjacent codewords is not uniform, which makes the decoded “bits” not uniformly reliable. (Errors are more likely in the parts of the received vector corresponding to smaller components of the initial vector.) This stems from the fact that the initial vector,

$$\mathbf{x}_0 = (\alpha, \alpha + \beta, \alpha + 2\beta, \dots, \alpha + (n-1)\beta),$$

gives $d_{\min} = \sqrt{2}\beta$ as the minimal distance of the code where $0 < \beta < \alpha$ and $\beta/\alpha = (1 - \cos \frac{2\pi}{r})^{1/2}$. For the generators a_i and b_j of $\mathbf{G}(r, 1, n)$, this choice implies that

$$\|a_1\mathbf{x}_0 - \mathbf{x}_0\| = \|b_1\mathbf{x}_0 - \mathbf{x}_0\| = \dots = \|b_{n-1}\mathbf{x}_0 - \mathbf{x}_0\| = d_{\min}$$

and $\|a_j\mathbf{x}_0 - \mathbf{x}_0\| > \sqrt{2}\beta$ for $j > 1$.

One solution to this problem is the following. Recall that any group element $g \in \mathbf{G}(r, 1, n)$ can be written as a product of coset leaders in the form

$$g = \tau_{\ell_n} a_n^{k_n} \cdots \tau_{\ell_3} a_3^{k_3} \tau_{\ell_2} a_2^{k_2} a_1^{k_1}$$

where each τ_{ℓ_j} is a permutation and each $k_i \in \mathbb{N}$. Choose integers m_j for $1 \leq j \leq n$ with m_j dividing m_{j+1} ,

$$1 = m_n | m_{n-1} | \dots | m_2 | m_1 | r.$$

Then use only codewords $g\mathbf{x}_0$ (as above) with $m_j | k_j$ for $1 \leq j \leq n$. Although this code is a proper subset of the full code for $\mathbf{G}(r, 1, n)$, it does not correspond to a subgroup. Note that the size of the code is

$$|W| = \frac{n! r^n}{\prod_{1 \leq j \leq n} m_j} .$$

The decoding algorithm is unchanged, except that the received vector is interpreted to be the nearest *codeword*.

Now the object is to adjust the parameters m_1, \dots, m_{n-1} and the initial vector \mathbf{x}_0 to make as uniform as possible the distances $\|b_j\mathbf{x}_0 - \mathbf{x}_0\|$ for $1 \leq j \leq n-1$, and $\|a_k^{m_k}\mathbf{x}_0 - \mathbf{x}_0\|$ for $1 \leq k \leq n$, while increasing the minimum distance of the code in the process. In practice this can be done rather effectively by *ad hoc* adjustments, but an interesting problem arises: *Find a good algorithm to adjust these parameters.*

For example, consider the code based on $\mathbf{G}(16, 1, 4)$. The original subgroup decoding scheme takes $m_1 = m_2 = m_3 = m_4 = 1$ and an initial vector of the form

$$\mathbf{x}_0 = (\alpha, \alpha + \beta, \alpha + 2\beta, \dots, \alpha + (n-1)\beta)$$

with $\beta/\alpha = .2759$. The size of the code is $16^4 \cdot 4! = 2^{16} \cdot 24$. One can calculate that the variation in the distances $\|g\mathbf{x}_0 - \mathbf{x}_0\|$ with $g \in \{a_1, a_2, a_3, a_4, b_1, b_2, b_3\}$ is $\max/\min = 1.83$, and the normalized d_{min} is .169.

If instead we take $m_1 = 4, m_2 = 2, m_3 = m_4 = 1$ and $\beta/\alpha = 1.0$, then we obtain a code with only $2^{13} \cdot 24$ codewords. However, the variation in the distances is then $\max/\min = 1.36$, and the minimum distance d_{min} becomes .280, giving a considerable improvement.

REFERENCES

- [1] D. Slepian, *Permutation modulation*, Proc. IEEE, **53** (1965), 228–236.
- [2] D. Slepian, *Group codes for the Gaussian channel*, Bell Syst. Tech. J., **47** (1968), 575–602.
- [3] I. Ingemarsson, *Group codes for the Gaussian channel*, in Topics in Coding Theory (Lecture Notes in Control and Information Theory), vol. **128**, New York, Springer-Verlag (1989), 73–108.
- [4] T. Ericson, *Permutation codes*, Rapport de Recherche INRIA, no. 2109, Nov. 1993.
- [5] G. David Forney, Jr., *Geometrically Uniform Codes*, IEEE Trans. Inform. Theory, vol. 37, no. 5 (1991), 1241–1260.
- [6] A. Jiang, R. Matescu, M. Schwartz, and J. Bruck, *Rank modulation for flash memory*, Proceedings IEEE ISIT (2008), 1731–1735.
- [7] A. Jiang, M. Schwartz, and J. Bruck, *Error correcting codes for rank modulation*, Proceedings IEEE ISIT (2008), 1736–1740.
- [8] A. Barg and A. Mazumdar, *Codes in permutations and error correction for rank modulation*, IEEE Trans. on Information Theory 56 (2010), 6273–6293.
- [9] T. Mittelholzer and J. Lahtonen, *Group codes generated by finite reflection groups*, IEEE Trans. on Information Theory, **42** (1996), 519–528.
- [10] M. Fossorier, J. Nation and W. Peterson, *Reflection group codes and their decoding*, IEEE Trans. on Information Theory, **56** (2010), 6273–6293.
- [11] H.J. Kim, *Decoding Complex Reflection Groups*, Master’s project, University of Hawaii, 2011. Available at scholarspace.manoa.hawaii.edu.

- [12] C. Walker, The Snowflake Decoding Algorithm, Master's project, University of Hawaii, 2012. Available at scholarspace.manoa.hawaii.edu.
- [13] J.B. Nation and C. Walker, *The Snowflake Decoding Algorithm*, submitted, preprint available at math.hawaii.edu/~jb.
- [14] T. Wadayama and M. Hagiwara, *LP-Decodable Permutation Codes Based on Linearly Constrained Permutation Matrices*, IEEE Trans. Inform. Theory, vol. 58, no. 6 (2012), 5454–5470.
- [15] M. Hagiwara and J. Kong, *Comparing Euclidean, Kendall tau metrics toward extending LP decoding*, Proceedings ISITA (2012), 91–95.
- [16] C. Kriloff and T. Lay, “Hamiltonian cycles in Cayley graphs of imprimitive complex reflection groups”, arXiv: 1303.4147.
- [17] G.C. Shephard and J.A. Todd, *Finite unitary reflection groups*, Canad. J. Math., **6** (1954), 274–304.
- [18] L.C. Grove and C.T. Benson, *Finite Reflection Groups (GTM 99)*, New York, Springer-Verlag, 1985.
- [19] J.E. Humphreys, *Reflection Groups and Coxeter Groups (Cambridge Studies in Advanced Mathematics, vol. 29)*, Cambridge, UK, Cambridge Univ. Press, 1990. Springer-Verlag, 1985.
- [20] R. Kane, *Reflection Groups and Invariant Theory*, CMS Books in Mathematics, New York, Springer-Verlag, 2001.
- [21] D. Knuth, *Searching and Sorting, the Art of Computer Programming*, vol. 3, Reading, MA, Addison-Wesley, 1973.
- [22] W. Kranek, *Finite subgroups of the quaternions* (2003), available at www.math.virginia.edu/~ww9c/kranek.pdf.
- [23] G.I. Lehrer and D.E. Taylor, *Unitary Reflection Groups*, Australian Math. Soc. Lecture Series (no. 20), Cambridge, UK, Cambridge Univ. Press, 2009.
- [24] G.D. Forney, *Geometrically uniform codes*, IEEE Trans. on Information Theory 37 (1991), 1241–1260.

DEPT. OF MATHEMATICS, UNIVERSITY OF HAWAI'I-WEST O'AHU, KAPOLEI, HI 96707, USA

E-mail address: hyejungkimkim@gmail.com

DEPT. OF MATHEMATICS, UNIVERSITY OF HAWAI'I, HONOLULU, HI 96822, USA

E-mail address: jb@math.hawaii.edu

DEPT. OF MATHEMATICS, UNIVERSITY OF NORTH TEXAS, DENTON, TX 76203, USA

E-mail address: ashepler@unt.edu