REFLECTION GROUP CODES AND THEIR DECODING

MARC FOSSORIER, J. B. NATION, AND WES PETERSON

This is a working draft.

1. Introduction

In 1968, Slepian introduced “group codes for the gaussian channel” [7]. The idea was to choose a group of orthogonal matrices and a point on a sphere, and then use the orbit of that point by that group as a set of signals for communication. In 1965, he introduced “permutation codes” [6], which were codes derived by choosing a point on a sphere and acting on it with a group of operations consisting of permutations of the coordinates and reversals of the signs of coordinates. Slepian recognized that these two operations can be written as orthogonal matrices, and therefore permutation codes are group codes for the gaussian channel. Furthermore he recognized that these two operations are reflections and therefore the groups are reflection groups.

In a very comprehensive paper in 1996, Mittelholzer and Lahtonen [5] considered the group codes for the gaussian channel generated by all reflection groups, and they were able to characterize all these codes and calculate the optimum initial point for all of them. They also gave efficient decoding algorithms for all these codes—at least all of the codes for which the initial point is not left fixed by any of the group elements.

Some of these codes have better minimum distance than the widely used nPSK modulation, and they compare favorably with QAS modulation. We wondered why they are not used in practical implementations. Our goal is to see how these codes compare in practical situations. This is a progress report. As a first step we have been working on making the implementation more efficient.

2. Reflection groups and reflection group codes

The paper by Mittelholzer and Lahtonen [5] is quite complete and thorough. We will therefore summarize some facts about reflection groups and some of the results of their paper without proofs and build on that material.

A reflection group is a group of orthogonal matrices that is generated by a set of reflections. Each reflection in the group is a reflection in a plane that goes through the origin. One reflection acting on the reflecting plane of another makes a third reflection plane. Certain configurations result in a finite number of reflection planes and hence a finite group. For example, in

Date: May 28, 2007.
two dimensions, there will be a finite reflection group if and only if the angle between reflecting planes divides 360 degrees. There is a list of all possible irreducible reflection groups in the Mittelholzer and Lahtonen paper.

These reflection planes divide the entire space into regions. You can choose any region to be the fundamental region. Then the planes the bound the fundamental region are the fundamental planes and the reflections associated with those planes are the fundamental reflections. For a reflection group that acts irreducibly on an \( n \)-dimensional space, the number of fundamental planes and the number of fundamental reflections is \( n \). Every element of the group can be written as a product of these fundamental reflections. There will be more reflections among the other elements, but not all the elements will be reflections. For the group \( E_6 \), for example, there are six fundamental reflections, 36 reflections in all, and a total of 51840 group elements. Each group element (except the identity element) maps each region into a different region. Thus if \( \mathbf{v} \) is a vector and \( g \neq I \) is a group element, \( \mathbf{v} \) and \( g\mathbf{v} \) are in different regions.

We will consider a unit sphere and instead of talking about points on the sphere we will talk about vectors from the origin to points on the sphere. Let us choose an initial vector that is in the fundamental region. Then the orbit that results from applying all the group elements to the initial vector consists of one vector in each region. You choose one of these vectors and send it, and you receive a vector that differs because of noise. The error probability depends on the exact choice of initial vector. Mittelholzer and Lahtonen showed that the optimum initial vector is a vector that is at the same distance from every bounding plane of the fundamental region—essentially in the very middle of the region. With the choice of initial vector specified by Mittelholzer and Lahtonen, a received vector should be decoded into the code vector that is in the same region. You could do maximum-likelihood decoding by calculating the distance from the received vector to each code vector, but there are much more efficient ways to decode.

For every reflection, there are two unit vectors normal to the plane, one on each side. Those are called roots. The ones that are on the same side of their respective reflection planes as the fundamental region are called positive roots, and the ones on the opposite side are called negative roots. A vector is on the positive side of a reflection plane if its inner product with the positive root is positive, and thus a vector is in the fundamental region if and only if its inner product with every fundamental root is positive.

**Theorem 1.** Every positive root can be written as a linear combination of fundamental roots with all positive coefficients, and every negative root can be written as a linear combination of fundamental roots with all negative coefficients.

It follows from this theorem that if \( \mathbf{v} \) is any vector in the fundamental region, then \( \mathbf{r} \) is a positive root if and only if \( (\mathbf{r}, \mathbf{v}) > 0 \).

**Theorem 2.** If \( g \) is a group element and \( \mathbf{r} \) is a root, then \( g\mathbf{r} \) is also a root.
Here, \( r \) and \( gr \) might both be positive or both negative, or one each. Define \( \Delta(g) \) to be the set of positive roots that are carried into negative roots by \( g \), and let \( |\Delta(g)| \) denote the number of such roots.

**Theorem 3.** Assume that \( v \) is a vector in a region and \( g \) is a group element. The reflecting plane corresponding to positive root \( \alpha \) is between \( v \) and \( gv \) if and only if \( \alpha \in \Delta(g^{-1}) \).

**Proof.** The reflecting plane is between \( v \) and \( gv \) if and only if \((v, \alpha)\) and \((gv, \alpha) = (v, g^{-1}\alpha)\) have opposite signs, which means that \( g^{-1}\alpha \) must be a negative root, and therefore \( \alpha \in \Delta(g) \). \(\square\)

Every group element can be expressed as a product of the fundamental reflections. That product is not unique—several expressions may evaluate to the same group element. For each group element there is a minimum number of factors in the expression. There may even be more than one expression with a minimum number of factors for a group element. The minimum number of factors in expressions for a group element \( g \) is called the length of \( g \), denoted \( \ell(g) \).

**Theorem 4.** If \( S_\alpha \) is a fundamental reflection of \( G \) and \( \alpha \) the corresponding positive root, then \( S_\alpha \alpha = -\alpha \) and \( S_\alpha \) permutes all the other positive roots.

**Theorem 5.** There are three equivalent statements:

1. \( \ell(g) = k \).
2. For any vector \( v \) that is not in any reflecting plane, the number of reflecting planes that separate \( v \) and \( gv \) is \( k \).
3. \( |\Delta(g)| = k \).

Moreover, if \( v \) is a vector in any region, then \( v \) and \( S_\alpha v \) are on opposite sides of the reflection plane for \( \alpha \), but it turns out that \( v \) and \( S_\alpha v \) are on the same side of every other reflecting plane.

We will also use the Matsumoto Cancellation Property, which states that if a product of \( m \) fundamental reflections is equal to a group element \( g \) of length \( \ell(g) < m \), then there must be two factors in that product that can simply be deleted and the result will still equal \( g \).

**Theorem 6.** Let \( g \) be a group element and \( S_\alpha \) be a fundamental reflection, with \( \alpha \) the corresponding positive root of \( S_\alpha \). Then

1. \( \ell(S_\alpha g) = \ell(g) + 1 \) if \( g\alpha \) is a positive root, and
2. \( \ell(S_\alpha g) = \ell(g) - 1 \) if \( g\alpha \) is a negative root.

**Theorem 7.** If \( S \) is any reflection and \( u \) and \( v \) are on the same side of the reflection plane of \( S \), then \( v \) is closer than \( Sv \) to \( u \), and similarly of course, if \( u \) and \( v \) are on opposite sides, then \( Sv \) is closer than \( v \) to \( u \).

These two theorems are the basis for a fairly efficient decoding method for group codes derived from reflection groups. Let \( v_I \) denote the initial vector chosen in the fundamental region. To send a message corresponding to the
group element $g$, we transmit the vector $gv_I$. Suppose $u$ is the received vector. If there is not too much added noise, then $u$ should be in the same region as $gv_I$. Given $u$, we want to find $g$. Let $g^{-1} = g'$. An equivalent statement is that $g'u$ is in the same region as $v_I$, and of course knowledge of $g'$ is equivalent to knowledge of $g$. The outline of a decoding algorithm to find $g'$ is as follows.

The element $g'$ has some finite length, say $\ell(g') = n$. Then by Theorem 5, there are $n$ reflecting planes between $u$ and $v_I$. Let $S_i$ for $i = 1, \ldots, n$ be the fundamental reflections for these planes, in the order in which you would cross them going from $g'u$ to $v_I$. Define a sequence of vectors by $u_0 = u$ and $u_i = S_i u_{i-1}$ for $i = 1, \ldots, n$. There will be one fewer reflecting planes between $u_i$ and $v_I$ than between $u_{i-1}$ and $v_I$, and therefore there will be $n - i$ reflecting planes between $u_i$ and $v_I$. By induction, there will be no reflecting planes between $u_n$ and $v_I$. Therefore, $u_n = S_n S_{n-1} \cdots S_1$ and $g'v_I$ are in the same region, whence $g' = S_n S_{n-1} \cdots S_1$.

Now, how do you know how to choose the fundamental reflections $S_1, S_2, S_3 \ldots S_n$? You use trial and error, and there are two ways to test whether a reflection is a suitable choice as $S_i$. Let $S_\alpha$ be a reflection and $\alpha$ the corresponding root. One way is to calculate the inner product $(u_i, \alpha)$. If this is negative, then $S_\alpha$ is a suitable choice for $S_i$ because then $u_i$ is on the opposite side of the reflection plane for $S_\alpha$ from the fundamental region, where $v_I$ is. The other way is to calculate the distance between $u_i$ and $v_I$ and the distance between $S_\alpha u_i$ and $v_i$. If the latter is smaller, then the reflection plane for $S_\alpha$ must be between $u_i$ and $v_I$, by Theorem 7. Then $S_\alpha$ must be a suitable choice.

3. Subgroups of Reflection Groups - Part 1

Mittelholzer and Lahtonen could improve on this method of decoding by using a subgroup of the reflection group that is a Slepian permutation code. We have found that further refinements are possible, often using a sequence of subgroups, each containing the next.

There are subgroups of reflection groups that are reflection subgroups. Not all subgroups of reflection groups are reflection groups. For example, the subgroup of all matrices whose determinant is 1 contains no reflections. (The determinant of a reflection is $-1$.) There is a subset of reflection subgroups called parabolic subgroups. A parabolic subgroup $H$ of a reflection group $G$ is a group that is generated by a subset of the fundamental reflections of $G$. There exist reflection subgroups that are not parabolic subgroups. Mittelholzer and Lahtonen found that $D_8$ is a subgroup of $E_8$ and $A_7$ is a subgroup of $E_7$, and in neither case is the subgroup a parabolic subgroup. On the other hand, for any reflection group, every subset of the fundamental reflections generates a parabolic subgroup. The dimension of the space acted on by the group is equal to the number of fundamental reflections, so parabolic subgroups always have smaller dimension than the
whole group. So we must distinguish parabolic subgroups, reflection subgroups, and general subgroups. The former ones have nicer properties, but we will have occasion to use all three types.

Let $G$ be a reflection group with $m$ elements and $H$ a reflection subgroup with $k$ elements. Then the whole space is divided into $m$ regions, and one of those regions is chosen to be the fundamental region. Let $v$ be any vector in the fundamental region. Then the positive roots are all the roots $r$ for which $(r, v) > 0$. The subgroup also defines regions, and the whole space is divided into $k$ of these regions. Define the fundamental region for the subgroup to be the region that contains $v$. Then the following theorem holds.

**Theorem 8.** If $H$ is a reflection subgroup of $G$, then the fundamental region for $G$ is contained in the fundamental region for $H$.

**Proof.** Let $v$ be any vector in the fundamental region of $G$. Let $r_j$ for $1 \leq j \leq n$ be the fundamental roots of $G$, and let $t_i$ for $1 \leq i \leq q$ be the fundamental roots of $H$. Then each $(r_j, v) > 0$. By Theorem 1, each $t_i$ can be written

$$t_i = \sum c_{ij} r_j$$

with all the coefficients $c_{ij}$ non-negative. Thus

$$(t_i, v) = \sum c_{ij} (r_j, v_j)$$

and that is non-negative because each term is non-negative. Therefore $v$ is in the fundamental region of $H$. \qed

Since a group acts transitively on its regions, and the choice of the fundamental region is arbitrary, it follows that each region of $H$ contains $\frac{|G|}{|H|}$ regions for $G$.

4. **Subgroups - Part II**

Given a reflection group $G$, we would like to choose a sequence of (reflection) subgroups

$$\{I\} = G_0 < G_1 < \cdots < G_{m-1} < G_m = G.$$  

to use in encoding and decoding. The most straightforward way to do so is to first choose a fundamental root system $\Sigma = \{\rho_1, \ldots, \rho_n\}$ for $G$, indexed in some convenient way. For each $i$ let $A_i$ denote the reflection $S_{\rho_i}$. Then, for $1 \leq i \leq n$, let $G_i$ be the subgroup generated by $\{A_1, \ldots, A_i\}$. This gives us a sequence of $n$ parabolic subgroups, where $n$ is the dimension of $G$.

With this setup, there are two issues to consider.

1. The order in which the roots are enumerated makes a difference. We would like the maximum of the indices $[G_i : G_{i-1}]$ not to be too large, and we would prefer that the indices of consecutive subgroups be a power of 2, or just over one, as often as possible. It would be good if the coset leader graph, discussed below, had a simple structure.
(2) It might be possible to refine the sequence of subgroups by inserting intermediate subgroups. This can significantly reduce the number of steps in encoding and decoding, which is roughly proportional to the sum of the indices of consecutive subgroups in the sequence.

4.1. Some Basic Lemmas. Consider a reflection group $G$ acting on $\mathbb{R}^n$, with identity denoted by $I$. For a vector $\alpha$ of unit length, $S_\alpha$ denotes the reflection along $\alpha$, given by

$$S_\alpha(x) = x - 2(x, \alpha)\alpha$$

where $(x, \alpha)$ denotes the standard Euclidean inner product (dot product).

Let $\Delta$ denote the set of roots of $G$, i.e.,

$$\Delta = \{ \alpha \in \mathbb{R}^n : \|\alpha\| = 1 \text{ and } S_\alpha \in G \}.$$

For $\alpha \in \Delta$, let $N_\alpha$ denote the reflecting plane:

$$N_\alpha = \{ x \in \mathbb{R}^n : (x, \alpha) = 0 \}.$$

The projection of a vector onto $N_\alpha$ is given by

$$P_{N_\alpha}(x) = x - (x, \alpha)\alpha.$$

The choice of an initial vector $x_0$ (not on one of the reflecting planes) determines the positive roots $\Delta^+$, the fundamental region $\text{FR}_{x_0}(G)$, and the fundamental root system $\Sigma$. To be precise,

$$\Delta^+ = \Delta^+_G = \{ \alpha \in \Delta : (\alpha, x_0) > 0 \}$$

$$\text{FR}_{x_0}(G) = \{ y \in \mathbb{R}^n : (y, \alpha) > 0 \text{ for all } \alpha \in \Delta^+ \}$$

$$\Sigma = \{ \rho \in \Delta^+ : P_{N_\rho}(x_0) \in \text{FR}_{x_0}(G) \}$$

$$\Sigma = \{ \rho \in \Delta^+ : (P_{N_\rho}(x_0), \alpha) \geq 0 \text{ for all } \alpha \in \Delta^+ \}$$

where $\overline{X}$ denotes the closure of $X$. Since the roots in $\Delta^+$ are positive linear combinations of those in $\Sigma$, we have

$$\text{FR}_{x_0}(G) = \{ y : (y, \alpha) > 0 \text{ for all } \alpha \in \Sigma \}.$$

A straightforward method to find an optimal choice of the initial vector $x_0$ (not on one of the reflecting planes) determines the positive roots $\Delta^+$, the fundamental region $\text{FR}_{x_0}(G)$, and the fundamental root system $\Sigma$. To be precise,

$$\Delta^+ = \Delta^+_G = \{ \alpha \in \Delta : (\alpha, x_0) > 0 \}$$

$$\text{FR}_{x_0}(G) = \{ y \in \mathbb{R}^n : (y, \alpha) > 0 \text{ for all } \alpha \in \Delta^+ \}$$

$$\Sigma = \{ \rho \in \Delta^+ : P_{N_\rho}(x_0) \in \text{FR}_{x_0}(G) \}$$

$$\Sigma = \{ \rho \in \Delta^+ : (P_{N_\rho}(x_0), \alpha) \geq 0 \text{ for all } \alpha \in \Delta^+ \}$$

where $\overline{X}$ denotes the closure of $X$. Since the roots in $\Delta^+$ are positive linear combinations of those in $\Sigma$, we have

$$\text{FR}_{x_0}(G) = \{ y : (y, \alpha) > 0 \text{ for all } \alpha \in \Sigma \}.$$

A straightforward method to find an optimal choice of the initial vector $x_0$, so that it is a unit vector equidistant from the walls of the fundamental region, is given in Mittelholzer and Lahtonen [5].

The following lemma deals with calculating the distance from a vector to $x_0$, which is a measure of how far it is from the fundamental region.

**Lemma 9.** Let $G$ be a reflection group and $\alpha$ a root of $G$.

1. If $a, b \in \mathbb{R}^n$ then $\|S_\alpha a - b\| < \|a - b\|$ if and only if $(\alpha, a)(\alpha, b) < 0$.
2. If $(\alpha, x_0) > 0$ (i.e., $\alpha$ is a positive root), then $\|S_\alpha a - x_0\| < \|a - x_0\|$ if and only if $(\alpha, a) < 0$.
3. For $B \in G$ we have $\|(B - I)x_0\|^2 = 2 - 2(Bx_0, x_0)$.
4. If $B, C \in G$, then $\|(B - I)x_0\| < \|(C - I)x_0\|$ if and only if $(Bx_0, x_0) > (Cx_0, x_0)$. 
Proof. Statements (1) and (3) are straightforward calculations; see, e.g., Kane [3]. Items (2) and (4) are consequences of (1) and (3), respectively. □

The next lemma is simple but crucial to subgroup decoding.

Lemma 10. Fix an initial vector $x_0$ in a reflection group $G$. Let $S \leq T \leq G$ be reflection subgroups, with $S$ having a fundamental system $X$ and $T$ having a fundamental system $Y$. Then

1. $\Delta_S^+ \subseteq \Delta_T^+$,
2. $\text{FR}_{x_0}(S) \supseteq \text{FR}_{x_0}(T)$,
3. the vectors in $X - Y$ are positive roots of $T$, and thus positive linear combinations of the elements of $Y$.

Thus in a sequence of reflection subgroups

$\{I\} = S_0 < S_1 < \cdots < S_n = G$

the fundamental roots of each subgroup are positive roots of all the succeeding subgroups.

Proof. If $S \leq T$ then $\Delta_S^+ \subseteq \Delta_T^+$, whence for a fixed choice of $x_0$ we have $\Delta_S^+ \subseteq \Delta_T^+$. Thus

$$\text{FR}_{x_0}(S) = \{y : (y, \alpha) > 0 \text{ for all } \alpha \in \Delta_S^+\} \supseteq \{y : (y, \alpha) > 0 \text{ for all } \alpha \in \Delta_T^+\} = \text{FR}_{x_0}(T).$$

The last statement is just a useful consequence of $X \subseteq \Delta_S^+ \subseteq \Delta_T^+$.

We conclude this section by compiling some useful basic facts, either from standard textbooks (e.g., Grove and Benson [1], Humphreys [2], Kane [3]) or from calculations.

Lemma 11. Let $Y$ be a fundamental root system for $G$, and let $\alpha$ be a positive root of $G$ with $\alpha \in Y$. Let $\varphi$ be an expression for an element of $G$ that is reduced with respect to $Y$. Then \(\text{length}(S_\alpha \varphi) = \text{length}(\varphi) \pm 1\), and the following are equivalent.

1. $\text{length}(S_\alpha \varphi) = \text{length}(\varphi) + 1$.
2. $S_\alpha \varphi$ is reduced.
3. $(\alpha, \varphi x_0) > 0$.
4. $\varphi^{-1} \alpha$ is a positive root.

Proof. This is a consequence of the Proposition on page 51 of Kane [3]. □

Lemma 12. (1) If $\Sigma$ is a fundamental system and $\alpha, \beta \in \Sigma$ with $\alpha \neq \beta$, then $(\alpha, \beta) \leq 0$.

2. If $T \in G$ and $\alpha \in \Delta$ then $TS_\alpha T^{-1} = S_{T\alpha}$.

3. Let $\alpha, \beta \in \Delta$.

(a) If $(\alpha, \beta) = \frac{1}{2}$ then $S_\alpha \beta = \beta - \alpha$.

(b) If $(\alpha, \beta) = -\frac{1}{2}$ then $S_\alpha \beta = \beta + \alpha$. 
In particular, we may want to replace $\beta$ by $\beta - \alpha$ in finding a fundamental system for a subgroup.

4.2. Generation. In this section we describe how one can efficiently find the reflection subgroups of a reflection group.

The first relevant result is Proposition 1.14 of Humphreys [2]. It tells us that there are no “extra” reflections in $G$.

**Theorem 13.** Let $Y \subseteq \Delta$ be a set of roots of a finite reflection group $G$, and let $S$ be the subgroup generated by $\{S_\alpha : \alpha \in Y\}$. The roots of $S$ are the smallest set $E$ such that

1. $Y \subseteq E$,
2. $\alpha, \beta \in E$ implies $S_\alpha(\beta) \in E$.

Secondly, we have a fundamental theorem of Coxeter; see, e.g., Chapter 6 of Kane [3].

**Theorem 14.** Every finite reflection group is given by a presentation $\langle X, R \rangle$ with generators $X = \{s_1, \ldots, s_n\}$ and relations

1. $s_i^2 = 1$ for all $i$,
2. $(s_is_j)^{m_{ij}} = 1$ for $i < j$.

It is this presentation, of course, that is represented in the *Coxeter graph* of the group.

To this mix we add two more basic facts.

(a) If $Y \subseteq \Delta^+$ is a set of positive roots with the property that $(\alpha, \beta) \leq 0$ whenever $\alpha \neq \beta \in Y$, then $Y$ is linearly independent. (See the proof of Lemma C on page 39 of Kane [3].)

(b) If $\alpha$ and $\beta$ are positive roots with $(\alpha, \beta) = -\cos \frac{\pi}{m}$, then the angle between the vectors is $\pi - \frac{\pi}{m}$, and $(S_\alpha S_\beta)^m = I$.

Now we can describe the algorithm for finding reflection subgroups as follows. We are given a reflections group $G$, with an initial vector $x_0$ and its corresponding fundamental root system $\Sigma$.

1. Determine the set of all roots $\Delta$, and all positive roots $\Delta^+$, for $G$.
   (This is straightforward; see Theorem 13.)
2. Find subsets $Y \subseteq \Delta^+$ with pairwise nonpositive dot products.
3. Find the isomorphism type of the subgroup generated by $\{S_\alpha : \alpha \in Y\}$ using fact (b) above and Theorem 14.

In practice, this yields many subgroups, and one needs to isolate a few that are useful to the purposes at hand, in this case forming subgroup sequences for coding.

For example, if we take $G = A_n$, the reflection subgroups are all isomorphic to direct products of groups $A_j$ with $j \leq n$, which is not very exciting.
For the groups $B_n$, however, we obtain an interesting subgroup sequence. A standard fundamental root system for $B_n$ is the set of vectors

\[
\begin{align*}
\alpha_1 &= (1, 0, 0, \ldots, 0) \\
\alpha_2 &= (-1, 1, 0, \ldots, 0) \\
\alpha_3 &= (0, -1, 1, 0, \ldots, 0) \\
\vdots \\
\alpha_n &= (0, \ldots, 0, -1, 1)
\end{align*}
\]

We also have the positive roots

\[
\begin{align*}
\beta_2 &= (0, 1, 0, \ldots, 0) \\
\beta_3 &= (0, 0, 1, 0, \ldots, 0) \\
\vdots \\
\beta_n &= (0, \ldots, 0, 1)
\end{align*}
\]

Then the subgroup generated by $\{S_{\alpha_1}, \ldots, S_{\alpha_k}\}$ is $B_k$, and between $B_k$ and $B_{k+1}$ we have the subgroup generated by $\{S_{\alpha_1}, \ldots, S_{\alpha_k}, S_{\beta_{k+1}}\}$. If we denote this subgroup by $M_{k+1}$, then $M_{k+1} \cong B_k \times A_1$, and we have the subgroups sequence

\[
\{I\} < B_1 < M_2 < B_2 < M_3 < B_3 < \cdots < M_n < B_n.
\]

This will play a role in efficiently encoding and decoding using $B_n$.

It is interesting to look at this situation syntactically. The reflections $S_{\beta_j}$ correspond to the longest coset leader of $[B_j : B_{j-1}]$. So if we denote $S_{\alpha_1} = A$, $S_{\alpha_2} = B$, $S_{\alpha_3} = C$, etc., then $S_{\beta_2} = BAB$, $S_{\beta_3} = CBABC$, $S_{\beta_4} = DCBABCD$, etc. The coset leaders for $[B_j : M_j]$ correspond to building terms from $I$, or reducing them from $S_{\beta_j}$, depending on whether their length is more or less than half that of the longest expression.

A similar situation occurs in the groups $D_n$, except that

1. the reflections $A$ and $B$ commute, so the longest coset leader for $[D_5 : D_4]$ looks like $EDCABCDE$ for example, and
2. the longest coset leader still has order 2, but it is not a reflection.

(Note that its determinant is $+1$.)

So the intermediate subgroups in this case are not reflection subgroups, but they work similarly for coding purposes. (See the section on the groups $D_n$ for a discussion of the minor adjustments that are required.)

Recall that a fundamental root system $\Sigma$ has the following properties.

1. $\Sigma$ is linearly independent.
2. Every root in $\Delta$ is a linear combination of elements of $\Sigma$ with coefficients all nonnegative or all nonpositive.

It would be nice if the algorithm given above always yielded a fundamental root system for the subgroup in question. This seems to usually be the case,
but not always. In the dihedral group $H^7_2$, consider the vectors
\[ \alpha = (1, 0) \]
\[ \beta = (\cos\left(\frac{2\pi}{7}2\right), \sin\left(\frac{2\pi}{7}2\right)) \]
\[ \gamma = (\cos\left(\frac{2\pi}{7}3\right), \sin\left(\frac{2\pi}{7}3\right)). \]

Then the dot product $(\alpha, \beta)$ is negative, and indeed $\{S_\alpha, S_\beta\}$ generate the group, but for a fundamental system you want $\{\alpha, \gamma\}$.

It seems to be the case that this problem can be remedied by restricting the dot products that can occur, but we have been unable to complete the proof of the following conjecture.

**Conjecture 15.** Let $Z \subseteq \Delta$ be any set of roots such that
1. $\alpha \in Z$ implies $-\alpha \notin Z$,
2. $\alpha, \beta \in Z$ distinct implies $(\alpha, \beta) = 0$ or $-1 \leq (\alpha, \beta) \leq -\frac{1}{2}$.

Then there are a subgroup $S \leq G$ and a choice of the fundamental region such that $Z$ is a fundamental system for $S$.

If this is true, it would have the following consequence.

**Conjecture 16.** Let $G$ be a finite reflection group with the property that $(\alpha, \beta) = 0$ or $|\langle \alpha, \beta \rangle| \geq \frac{1}{2}$ for all roots $\alpha \neq \beta$. Then there is a one-to-one correspondence between reflection subgroups of $G$ and subsets $Z \subseteq \Delta^+$ with pairwise nonpositive dot products. Moreover, if $Sg(Z)$ denotes the subgroup generated by $\{S_\alpha : \alpha \in Z\}$, then
\[ Sg(Z_1) \leq Sg(Z_2) \text{ if and only if } Z_1 \subseteq \text{Span}(Z_2). \]

4.3. **Subgroup tables.** Table 1 lists some reflection subgroups of small index in various reflection subgroups. These subgroups were found by finding sets of positive roots with pairwise nonpositive direct products, which is quite efficient and includes the parabolic subgroups. Subgroups of a particular type can occur in multiple copies. The table is far from complete.

The length column gives the length of the longest coset leader for a subgroup, which is a parameter in determining the complexity of encoding and decoding. This will also be the length of the directed graph $\Gamma$ of coset leaders described below. (These graphs have no cycles. The length of such a graph is the maximum number of edges in a path.) By the analysis of length given in the standard textbooks, the maximum length of an element in a reflection group is the number of positive roots. So for parabolic subgroups the length of the longest coset leader will be the difference between the number of positive roots of the group and its subgroup. These, in turn, can be found in a table in Mittelholzer and Lahtonen [5], or computed directly.

Nonparabolic subgroups, on the other hand, involve generators of length greater than 1. There does not appear to be a general formula for the length of coset leaders for nonparabolic subgroups. For these cases, we just wrote simple programs to determine the graph $\Gamma$. 

<table>
<thead>
<tr>
<th>Group</th>
<th>Subgroup</th>
<th>Index</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_n$</td>
<td>$A_{n-1}$</td>
<td>$n + 1$</td>
<td>$n$</td>
</tr>
<tr>
<td>$B_n$</td>
<td>$B_{n-1} \times A_1$</td>
<td>$n$</td>
<td>$n - 1$</td>
</tr>
<tr>
<td>$D_n$</td>
<td>$D_{n-1}$</td>
<td>$2n$</td>
<td>$2n - 2$</td>
</tr>
<tr>
<td>$E_6$</td>
<td>$D_5$</td>
<td>27</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>$A_5 \times A_1$</td>
<td>36</td>
<td>10</td>
</tr>
<tr>
<td>$E_7$</td>
<td>$E_6$</td>
<td>56</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>$D_6 \times A_1$</td>
<td>63</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>$A_7$</td>
<td>72</td>
<td>15</td>
</tr>
<tr>
<td>$E_8$</td>
<td>$E_7 \times A_1$</td>
<td>120</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>$D_8$</td>
<td>135</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>$A_8$</td>
<td>1920</td>
<td>42</td>
</tr>
<tr>
<td>$F_4$</td>
<td>$B_4$</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1. Reflection Subgroups

5. Coset leaders, graphs and normal form

Now suppose we are given a sequence of reflection subgroups of a reflection group $G$, say

$$\{I\} = G_0 < G_1 < \cdots < G_{m-1} < G_m = G.$$ 

First we describe an algorithm to find a set of coset leaders for $[G_i : G_{i-1}]$ consisting of minimal length terms, so that when combined they will yield a canonical expression for an arbitrary element of $G$ as a product of coset leaders. Then we describe how to construct a graph $\Gamma_i$ for each extension $[G_i : G_{i-1}]$. These graphs encode the algebraic structure of $G$ in terms of the sequence of subgroups, and will be crucial to our encoding and decoding algorithms.

Let $G$ be a finite reflection group, $A, B, C, \ldots$ be the $n$ fundamental reflections, and let $H$ be an arbitrary subgroup of $G$. Define an expression to be a finite sequence of fundamental reflections. If you multiply the reflections in an expression, in sequence, you get a group element. More than one expression can result in the same group element. An expression is called reduced if it has minimum length. Define order for expressions as follows: $E_1 < E_2$ if the number of factors in $E_1$ is less than the number of factors in $E_2$, or if both have the same number of factors and $E_1$ precedes $E_2$ in dictionary order. Since the elements of $G$ are transformations, they are composed from right to left, and expressions should be read in the same way. Thus, for example, $BAC < ABC$ in the dictionary order. The relation $<$ on expressions is of course a linear order: you can compare any two expressions.

Consider the left cosets $XH$ of $H$ in $G$. Define the coset leader of a coset to be the smallest expression that evaluates to an element of the coset. By the usual definition, the coset leader is an element of the coset. This is
slightly different—what we call the coset leader evaluates to an element of the coset. Since the order is simple, this uniquely defines the coset leader. Note also that this requires that the coset leader be a reduced expression, because otherwise there is a shorter expression that evaluates to an element of the same coset.

We will say that two expressions are in the same coset if they evaluate to group elements that are in the same coset. You can determine whether $E_1$ and $E_2$ are in the same coset by determining whether $E_1^{-1}E_2$ is in $H$. If $H$ is a reflection group, then you can do this by decoding $E_1^{-1}E_2$ in $H$ and seeing whether the result is the initial vector of $H$.

Next we will define an algorithm for making a list of expressions. (We will prove that this is a list of all coset leaders.) Initially the list contains only the identity element, an expression with no elements. For each expression $E$ in the list, in order, multiply it on the left by each fundamental reflection $R$ in order, and then check whether the result is in the same coset as any expression on the list. If it is not, then add $RE$ to the list.

**Lemma 17.** If $E_1$ and $E_2$ are expressions on this list, and if $E_1$ precedes $E_2$ on the list, then $E_1 < E_2$.

**Proof.** The algorithm starts testing expressions of the form $RE$ where $E$ is an expression and $R$ is a fundamental reflection. It starts with $E$ of length zero and tests expressions $RE$ of length 1. After exhausting $E$’s of length $k$ from the list and testing $RE$’s of length $k+1$, it continues with $E$’s of length $k+1$ testing $RE$’s of length $k+2$. Thus the length is non-decreasing in the list, and if $E_1$ precedes $E_2$ on the list and they have different lengths, then $E_1 < E_2$. If $R_1E_1$ and $R_2E_2$ are on the list and have the same length, and $E_1 < E_2$, then $R_1E_1$ would have been tested before $R_2E_2$ and hence would come earlier on the list. Since $E_1 < E_2$ and they have the same length, then $E_1$ precedes $E_2$ alphabetically, and then it will also be true that $R_1E_1$ precedes $R_2E_2$ alphabetically. Finally, it might be that two expressions $R_1E$ and $R_2E$ being compared are derived from the same expression $E$ on the list. In that case, since we try fundamental reflections in order alphabetically, if $R_1E$ appears first on the list, it must have been tested before $R_2E$ and therefore $R_1 < R_2$ and it follows that $R_1E < R_2E$ alphabetically. □

**Theorem 18.** Coset leaders for all cosets are on this list.

**Proof.** The proof is by induction on the length $k$ of the expressions. All coset leaders of length $k = 1$ are on the list, because all expressions of length 1 are tested, and the ones that are coset leaders will be put on the list. Assume that all coset leaders of length less than $k$ are on the list. Suppose that $RE$ is a coset leader of length $k$ and $R$ is the last reflection in the expression $RE$. Then since $RE$ is a coset leader, its length is the number of factors, $k$. Then $E$ has $k−1$ factors, and must have length no greater than $k − 1$. It must be in a coset whose coset leader has length no greater than $k − 1$. Therefore, by the induction hypothesis, its coset leader $E_0$ is in the list. Both $E_0$ and
$E$ are in the same coset $E_0H = EH$, and $E_0$ being the coset leader, it must be that $E_0 \leq E$. Then also $RE_0H = REH$. Since $RE$ is the coset leader of this coset, $RE \leq RE_0$, and therefore $E \leq E_0$. Thus $E = E_0$, and the coset leader $RE$ can be gotten by multiplying a coset leader on the list, $E_0$, by a reflection $R$, and therefore the coset leader $RE$ will be on the list.  

Now let us construct the graph $\Gamma$ of (left) coset leaders for $[G : H]$. The vertices of $\Gamma$ are the coset leaders of $G$ over $H$, say $v_0, \ldots, v_{k-1}$ where $v_0 = I$ and $k = |G|/|H|$. There is a directed edge from $v_i$ to $v_j$ if $v_j = Rv_i$ for a fundamental reflection $R$ and $\text{length}(v_j) = \text{length}(v_i) + 1$. We label such an edge by $R$, so that the transformation $v_j$ can be reconstructed by tracing a path from $v_0 (= I)$ to $v_j$ and reading the edge labels in order. Such a path need not be unique, due to the presence of commuting reflections, but in the next section we will indicate how a canonical path can be chosen.

We also need the following observation.

**Theorem 19.** Let $G$ be a group, and

$$\{I\} = G_0 < G_1 < \cdots < G_{m-1} < G_m = G$$

a sequence of subgroups. Choose (left) coset leaders for each $G_i$ over $G_{i-1}$, with $I$ as the coset leader for $G_{i-1}$. Then every element of $G$ has a unique expression as a product of coset leaders, $g = c_m \ldots c_1$, with each $c_i$ a coset leader for $[G_i : G_{i-1}]$.

**Proof.** If $g \in G_i$, then $g \in G_k$ for some minimal $k \leq m$. The claim is proved by induction on $k$. If $k = 0$, then $g = I$ and we take $c_j = I$ for all $j$. So, assuming that every $h \in G_{k-1}$ has a unique expression as a product of coset leaders, let $g \in G_k$. Then $g = c_kh$ for some unique coset leader $c_k$ and unique $h = c_k^{-1}g$ in $G_{k-1}$. For larger indices $\ell > k$ we have $g \in G_{\ell-1}$, so we must choose $c_\ell = I$, and thus the whole expression is uniquely determined.  

In practice, we will number the vertices of each $\Gamma_i$, and rather than explicitly writing the transformation $g = c_m \ldots c_1$, we will identify $g$ by a sequence of integers $d = d_1 \ldots d_m$ with each $d_j$ being the number labelling the vertex $c_j$. (So the sequence is read left to right while the group elements, being transformations, are composed right to left. With a little care, this need not cause confusion.)

The results on coset leaders in this section (Lemma 17, Theorems 18 and 19) apply to an arbitrary subgroup $H$ of a group $G$ with a given linearly ordered set of generators $A, B, C, \ldots$.

### 6. The Spanning Tree

Now find a spanning tree for each graph $\Gamma_i$, that is, a subset $T_i$ of the edges of $G_i$ such that for each vertex $v \in \Gamma_i$, there is a unique path in $T_i$ from 0 to $v$. (The tree should have an additional technical property, described below.) Note that the spanning tree determines a unique expression for each coset leader as a product of fundamental reflections, and hence a canonical
representation of each group element as a product of fundamental reflections. This will be one of the possibly several such expressions of minimal length (corresponding to the different paths from 0 to \(v\)).

We will use spanning trees for navigating through the group in encoding and decoding, so for programming purposes we need to describe some functions on the vertices. Each vertex \(j\) in \(\Gamma_i\) has a unique predecessor in the tree, which we denote by \(\text{pred}(i,j)\). The edge from \(\text{pred}(i,j)\) to \(j\) is labelled by a fundamental reflection \(R\), and we set \(\text{lm}(i,j) = R\). There may be several edges in the tree emanating from \(j\). Let \(\text{breadth}(i,j)\) be the number of these, and let \(\text{succ}(i,j,k)\) for \(1 \leq k \leq \text{breadth}(i,j)\) denote the successor vertices to \(j\) in the tree \(T_i\).

The order in which the branches are listed does matter. In decoding, we will navigate through the tree by testing the branches out of vertex \(j\) in \(T_i\) in the order \(\text{succ}(i,j,1), \text{succ}(i,j,2), \text{succ}(i,j,3), \ldots\) and refer to this as the branch order of the successors of \(j\). The technical condition that must be satisfied in order for the decoding to work is the following.

Let \(j, v\) be vertices in \(\Gamma_i\), and let \(k, \ell\) be two successors of \(j\) in \(T_i\) with \(k\) preceding \(\ell\) in the branch order. If there are paths in \(\Gamma_i\) going from \(j\) to \(v\) through both \(k\) and \(\ell\), then the (unique) path from \(j\) to \(v\) in \(T_i\) must go through \(k\).

At this point, the reader should ask whether such a tree exists, and if so, how to find it. In fact, the algorithm which we used in the previous section to list all the coset leaders in alphabetical order (reading from right to left) determines such a tree. That is, our tree consists of the edges \((E, RE)\) of \(\Gamma_i\) where \(RE\) is the alphabetically least expression for the corresponding element: if \(RE = SF\) with \(R\) and \(S\) fundamental reflections, then \(R\) precedes \(S\) alphabetically.

7. Who is my neighbor?

Our group coding scheme is based on the premise that there is a direct connection between Euclidean distance and word length. The group code consists of \(\{Tx_0 : T \in G\}\). It is not that \(\|Tx_0 - x_0\| < \|T'x_0 - x_0\|\) whenever \(T\) is shorter than \(T'\) - that is too simple-minded to be true, and it is easy to find examples. The operative fact is the following.

**Theorem 20.** Let \(H\) be a subgroup of a reflection group \(G\), and let \(x_0\) be an initial vector for \(G\). Consider two elements \(T\) and \(T'\) of \(G\) with reduced expressions \(T = Lh\) and \(T' = L'h\), where \(L, L'\) are coset leaders and \(h \in H\). If \(L\) precedes \(L'\) in the graph \(\Gamma\) of coset leaders for \([G : H]\), i.e., the reduced expression for \(L'\) is \(\phi L\), then \(\|Tx_0 - x_0\| < \|T'x_0 - x_0\|\).

**Proof.** Recall that (by construction) \(x_0\) has the property that \((\alpha, x_0) > 0\) for every fundamental root \(\alpha\) of \(G\), where \((x, y)\) denotes the standard Euclidean inner product. On the other hand, a straightforward calculation shows that, for arbitrary vectors \(a, b, \alpha\) we have

\[
\|S_\alpha a - b\| < \|a - b\| \quad \text{iff} \quad (a, \alpha)(b, \alpha) < 0.
\]
Therefore \( \|S_\alpha Tx_0 - x_0\| < \|Tx_0 - x_0\| \) iff \((\alpha, Tx_0) < 0\). But by Lemma 11 we know that length\((S_\alpha T) < \text{length}(T)\) if and only if \((\alpha, Tx_0) < 0\). The length condition certainly applies when \(L\) is an immediate predecessor of \(L' = S_\alpha L\) in \(\Gamma\), and the statement of the theorem follows by induction. \(\square\)

The preceding theorem does not tell the whole story, because it does not apply when \(S_\alpha L\) is not reduced. To describe the closest geometric neighbors of \(Tx_0\) in \(\{Ux_0 : U \in G\}\) requires a more careful analysis. Because the transformations in \(G\) are isometries, \(\|Tx_0 - T'x_0\| = \|T'^{-1}Tx_0 - x_0\|\). Also, the closest neighbors of \(x_0\) are exactly the set of elements \(Rx_0\) with \(R = S_\alpha\) a fundamental reflection, all of which attain the minimum distance. The next result shows that the canonical form of \(T'\), where \(T'x_0\) is a geometric neighbor of \(Tx_0\), is closely related to the canonical form of \(T\).

**Theorem 21.** Let \(G\) be a reflection group with initial vector \(x_0\). Fix a sequence of parabolic subgroups

\[
\{I\} = G_0 < G_1 < \cdots < G_{n-1} < G_n = G.
\]

If the canonical form of \(T\) as a product of coset leaders is \(c_n \ldots c_1\) and \(T'x_0\) is a neighbor of \(Tx_0\), i.e., \(\|T'x_0 - Tx_0\|\) is the minimal distance for \(G\), then the canonical form of \(T'\) is \(c'_n \ldots c'_1\) where \(c'_i = c_i\) for all but one \(i\), and for that index \(c'_j\) is an immediate predecessor or successor of \(c_j\) in \(\Gamma_j\).

Our proof (following the proof of Theorem 22) depends primarily on the following three facts about reflection groups, which can be found in Kane [3] or the other standard texts on reflection groups.

1. By Lemma C on page 59 of Kane and the remark that follows, if \(G\) is a reflection group and \(H\) is a parabolic subgroup, every coset has a unique element of minimum length. (We will consider that to be the coset leader.) Furthermore, every element of the coset can be written uniquely as a product \(Lh\) where \(L\) is the coset leader and \(h\) is an element of the subgroup. Moreover, the length of \(Lh\) is equal to the sum of the lengths of \(L\) and \(h\).

2. By Lemma 11, if \(\phi\) is an element of \(G\) and \(\alpha\) is a fundamental reflection, then the length of \(\alpha\phi\) is either \(\text{length}(\phi) - 1\) or \(\text{length}(\phi) + 1\).

3. The Matsumoto cancellation property, found on page 51 of Kane, states that if \(\phi\) is an element of length \(m\) in a reflection group and you have an expression \(L\) for \(\phi\) as a product of more than \(m\) fundamental reflections, then there exist two factors in \(L\) such that if they are eliminated from \(L\) giving \(L'\), then \(\phi = L = L'\) when evaluated in \(G\).

**Theorem 22.** If \(G\) is a reflection group and \(H\) is a parabolic subgroup, and \(L\) is the coset leader of the coset \(LH\), and if \(S_\alpha\) is a fundamental reflection, then the coset leader of the coset \(S_\alpha LH\) is either \(S_\alpha L\), or else it is \(L\). Note that in the latter case, the length is the length of \(L\), and in the former case it could be either one more or one less than that.
A simple example will illustrate the various cases that arise in the proof. Consider the group $A_4$ with the sequence of parabolic subgroups

$$I < A_1 < A_2 < A_3 < A_4$$

where $A_1$ is the subgroup generated by $\{A\}$, the subgroup $A_2$ is generated by $\{A, B\}$, etc. Then $L = CD$ is a coset leader for $A_4$ over $A_3$, and we want to write the elements $XL$ with $X = A, B, C, D$ as products of coset leaders. We have

$$ACD = CD \cdot A$$
$$BCD = BCD$$
$$CCD = D$$
$$DCD = CD \cdot C$$

because $A$ commutes with $CD$, $BCD$ is a coset leader, $C^2 = I$, and $(CD)^3 = I$, respectively.

**Proof.** Denote the length of $L$ by $m$. Then by (1) above, every other element of the coset $LH$ has length greater than $m$. By (3), the length of $S_\alpha L$ is either $m - 1$ or $m + 1$ and the length of every other element of the coset $S_\alpha LH$ is greater than $m - 1$. Now consider three cases.

(A) If the length of $S_\alpha L$ is $m - 1$, it is the shortest element in the coset, so it is the coset leader.

(B) If the length of $S_\alpha L$ is $m + 1$ and there is no element of the coset $S_\alpha LH$ that has length $m$, then $S_\alpha L$ is the unique element of minimal length in the coset, and thus is the coset leader.

(C) The only remaining case is the case in which the length of $S_\alpha L$ is $m + 1$ and there is an element of the coset $S_\alpha LH$ of length $m$. Let us denote that element as $S_\alpha Lh$, where $h$ is an element of the subgroup $H$. Let us denote the length of $h$ by $k$. By (1) the length of $Lh$ is $k + m$. By (2) the length of $S_\alpha Lh$ is either the length of $Lh$ plus one or the length of $Lh$ minus $1$. Therefore we have $m = k + m + 1$ or $m = k + m - 1$. The first of these is impossible, and the second is possible only if $k = 1$. That means that $h$ has length one and is therefore a fundamental reflection. Also, $\ell(S_\alpha Lh) = m$.

Continuing with case (C), we have that the length of $S_\alpha Lh$ is $m$, and the length of $L$ is $m$, and both $h$ and $S_\alpha$ are fundamental reflections. Now let us represent $L$ as the product of $m$ fundamental reflections. Then $S_\alpha Lh$ is the product of $m + 2$ fundamental reflections, but it has length $m$, so Matsumoto’s theorem applies. There must be two of the $m + 1$ factors that can simply be deleted without changing the value of the product. There are four possibilities. The two factors might be in $L$, one might be $S_\alpha$ and the other in $L$, one might be $h$ and the other in $L$, or they might be $h$ and $S_\alpha$. We will show that the first three are impossible. Therefore the two factors that can be dropped must be $h$ and $S_\alpha$, and as a result, the coset leader is $S_\alpha Lh = L$. 

If both the factors that can be dropped are in $L$, resulting in $L' = L$, then $L'$ has $m - 2$ factors and its length is less than $m$ contrary to the assumption that $L$ has length $m$ and therefore cannot be expressed as a product of fewer than $m$ fundamental reflections.

If one of the factors that can be dropped is $S_\alpha$ and the other is in $L$ and if dropping that factor in $L$ gives $L'$, then $S_\alpha L h = L' h$, and therefore $S_\alpha L = L'$. We assumed that $S_\alpha L$ had length $m + 1$, but $L'$ has length $m - 1$ so this case is impossible.

If one of the factors that can be dropped is $h$, and the other is in $L$ and if dropping that factor in $L$ gives $L'$, then $S_\alpha L h = S_\alpha L'$ and therefore, $L h = L'$. But $L'$ has length $m - 1$, and since $L$ is assumed to be the coset leader of its coset, $L'$ cannot be in the same coset as $L$.

The only remaining possibility is that the two factors that can be dropped are $h$ and $S_\alpha$, and the coset leader is $S_\alpha L h = L$. □

We can now complete the proof of Theorem 21 as follows. If $T$ and $T'$ are as in the theorem, then $T' = S_\alpha T$ for some fundamental reflection $S_\alpha$. If $c'_n = S_\alpha c_n$, then it has length either one more or less than the length of $c_n$, and the conclusion follows. But if $c'_n = c_n$, then by the last case of the preceding analysis $S_\alpha c_n = c_n h$ for some fundamental reflection $h$ that is in $G_{n-1}$, and the conclusion follows by induction.

8. Binary schemes

The basic idea of this section is that we should establish a correspondence between binary messages and group elements. That is, we will take bit strings of length $x$, where $x \leq \lceil \log_2 |G| \rceil$, and map them one-to-one to a subset consisting of some $2^x$ elements of $G$. We typically begin the process with a sequence of parabolic subgroups

$$\{I\} = G_0 < G_1 < G_2 < \cdots < G_n = G$$

and write each element $T$ of $G$ as a product of coset leaders. Letting $\gamma : 2^x \rightarrow G$ denote the assignment map, we want the following property to hold: if $T x_0$ and $T' x_0$ are geometric neighbors in $G x_0$, then $\gamma^{-1}(T)$ and $\gamma^{-1}(T')$ differ by as few bits as possible. It may not be possible to arrange that geometric closest neighbors always differ by one bit, but in fact it is practical to get the average difference fairly close to one bit.

Now geometric neighbors are described by Theorem 21; their expressions differ by exactly one coset leader, and the differing pair are neighbors in some $\Gamma_j$. So the initial plan would be to partition the bit strings into sections corresponding to the coset leader graphs $\Gamma_1, \ldots, \Gamma_n$. If we do this directly, then we can encode only bit strings of length $\sum_{j=1}^n \lceil \log_2 |\Gamma_j| \rceil$, which is generally less than the capacity of the group $\lceil \log_2 |G| \rceil$. In order to gain extra bits, we will combine various pairs of indices. The details of this modification will be described later.
The motivation for the condition above is that we will be sending messages in the form of vectors $Tx_0$ with $T \in G$. Decoding will be done by finding the transformation $T \in G$ whose inverse moves the received vector $r$ closest to the initial vector $x_0$, i.e., the $T$ that minimizes $\|T^{-1}r - x_0\|$. The most like error will be to incorrectly decode $Tx_0$ as one of its neighbors $T'x_0$. If the corresponding bit strings differ by only a few bits, then super-imposing an error-correcting code will correct most of these errors.

For the purposes of this correspondence, we must use a sequence of parabolic subgroups in making the assignment. Theorems 21 and 22 are only valid for parabolic subgroups. Intermediate subgroups can and will be used freely in the process of encoding and decoding, but not in this part of the setup.

9. Setup

In order to implement encoding and decoding for a specific group $G$ acting on $\mathbb{R}^n$ with a given subgroup sequence, we begin by choosing a fundamental root system $\mathbf{r}_1, \ldots, \mathbf{r}_n$. If there are intermediate subgroups, then we also need to identify roots, say $\mathbf{s}_1, \ldots, \mathbf{s}_k$ corresponding to those transformations.

Next we find an appropriate initial vector $x_0$, lying in the middle of a fundamental region. An algorithm for this process is described in Mittelholzer and Lahtonen [5]. First form the matrix $R$ whose rows are the normalized root vectors $\frac{\mathbf{r}_i}{\|\mathbf{r}_i\|}$. Find the inverse matrix $R^{-1}$, and let $\mathbf{v}$ be the vector whose $j$-th entry is the sum of the $j$-th row of $R^{-1}$. Then let $x_0 = \frac{\mathbf{v}}{\|\mathbf{v}\|}$.

At this point we also write the procedures to implement the reflections $S_{\mathbf{v}}(\mathbf{x}) = \mathbf{x} - 2\frac{\mathbf{x} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\mathbf{v}$ for $\mathbf{v} = \mathbf{r}_1, \ldots, \mathbf{r}_n, \mathbf{s}_1, \ldots, \mathbf{s}_k$. These transformations are given by orthogonal matrices, but most oft times they will be permutation matrices or permutations with sign changes. It is clearly advantageous to apply those transformations to the vector directly, reserving matrix multiplication for those few cases where the matrix is not sparse.

10. Encoding: message to coset leaders

Now assume that we are given a binary message $\mathbf{m} = m_1 \ldots m_x$ of length $x$. Using our predetermined scheme, we invoke a procedure to convert $\mathbf{m}$ to a string of coset leaders $d_1 \ldots d_n$, which in turn corresponds uniquely to an element of $G$. In the simple case where we are not combining subgroups, just break $\mathbf{m}$ into blocks so that

$$m_1 \ldots m_r \mapsto d_1$$
$$m_{r+1} \ldots m_s \mapsto d_2$$
$$\ldots$$
$$m_{t+1} \ldots m_X \mapsto d_n.$$
If we are combining subgroups, then some substrings will correspond to pairs \(\langle d_i, d_j \rangle\). This procedure may be fairly involved and may incorporate look-up tables, but the theoretical content is all in choosing the correspondence (discussed earlier), not in implementing it. The output is the string \(d\) of coset leaders.

If we are including intermediate subgroups, at this point we now convert \(d\) to a string \(e = e_1 \ldots e_m\) of coset leaders for the refined chain of subgroups. This is primarily a consideration for the groups \(B_n\) or the related group \(F_4\). In the case of \(B_n\), \(e_1 = d_1\) and each of \(d_2, \ldots, d_n\) is replaced by a pair of coset leaders. The details of this conversion are discussed in another section. Then proceed as below with \(e_1 \ldots e_m\) instead of \(d_1 \ldots d_n\).

11. Encoding: coset leaders to vector

Now we have a transformation \(T = T_{nd_n} \ldots T_{1d_1}\) where \(T_{ij}\) denotes the coset leader labeled \(j\) for in the graph \(\Gamma_i\) for \(S_i/S_{i-1}\). This group element is a product of a long string of fundamental reflections, applied to a vector from right to left. The vector that we want to transmit is

\[ x = T^{-1}x_0 = T_{1d_1}^{-1} \cdots T_{nd_n}^{-1}x_0 \]

which is obtained by applying to \(x_0\) the same sequence of fundamental in the opposite order, i.e., reading the reflections from left to right as they appear in the canonical expression for \(T\).

In practice, then, to encode we first apply the reflection corresponding to the vertex \(d_n\) in the graph \(\Gamma_n\) to \(x_0\), and then move to its predecessor \(\text{pred}(d_n)\) in the spanning tree for \(\Gamma_n\) and apply its reflection, continuing until we reach the root 0 of \(\Gamma_n\) (which corresponds to the identity \(I\)). Then we move to the vertex \(d_{n-1}\) in the graph \(\Gamma_{n-1}\) and apply its reflection and move to its predecessor, and so on until we reach the root of \(\Gamma_1\).

Then we transmit the vector \(x\) thus obtained.

12. Noise

Presumably, at this point the vector goes through a noisy channel, so that the received vector is \(r = x + n\). In testing, we simulate this by adding to each component of \(x\) separately a value generated by pseudo-random generator for a Gaussian distribution with mean 0 and variance \(s^2\), for various values of \(s\).

13. Decoding: vector to coset leaders

Upon receiving the vector \(r\), we call a procedure to find the transformation \(S\) that will take \(r\) into the fundamental region of \(x_0\), i.e., find \(S\) that will minimize \(\|Sr - x_0\|\). Since \(r = x + n \approx T^{-1}x_0\), hopefully this will be \(T\), or if not then perhaps a neighbor of \(T\). First assume that each subgroup \(G_i\) is a reflection subgroup.
We begin with the vector $r$ at the vertex 0 in the graph $\Gamma_1$, and proceed through the spanning tree. At each vertex $i$, we have a vector $x$ and we consider in the proper order the successor nodes to $i$. Each of these successor nodes has a corresponding fundamental reflection, $R$ say. If $\|Rx - x_0\| < \|x - x_0\|$ then we move to that node and start considering its successors. If not, then we move to the next successor node of $i$, if there is one, until we exhaust the successors of $i$. When we reach a vertex $j$ where no successor node yields an improvement, or the last vertex of $\Gamma_1$, then we record that vertex as $d'_1$.

Then with the vector $x$ we move to the vector in $\Gamma_2$, and proceed to work our way through it, and so forth through $\Gamma_n$. Thus we obtain the vector $d' = d'_1 \ldots d'_n$ corresponding to the coset leaders of $S$.

If there are intermediate subgroups, we follow the same steps but there are more than $n$ graphs to consider in finding $e' = e'_1 \ldots e'_m$. Then, using the given correspondence, transform $e'$ into $d'$.

The preceding discussion depends on Theorem 20, which is valid only for reflection subgroups. (And in practice, rather than check $\|Rx - x_0\| < \|x - x_0\|$ directly, we can test the equivalent condition $(\alpha, x) < 0$ where $\alpha$ is the positive root with $R = S_\alpha$.) Nor is there an obvious modification that applies to arbitrary intermediate subgroups. However, there is one important situation, which arises repeatedly, that we can handle. This involves an intermediate subgroup generated by a set of reflections and an element $R$ satisfying $R^2 = I$. In this case, it can happen that there are transformations $S \in G$ such that $\|RSx_0 - x_0\| = \|Sx_0 - x_0\|$, making it impossible to decide which coset leader to choose. Rather than discuss this situation abstractly, we will illustrate it in the section on the groups $D_n$, which are typical.

14. Decoding: coset leaders to received message

Then we reverse the encoding process to obtain the received message $m' = m'_1 \ldots m'_X$ from the coset leaders $d'_1 \ldots d'_n$. This means applying the inverses of the functions used in encoding, and hence probably look-up tables, but in principle this step is straightforward. (In practice, it can get a bit messy, especially when the coset leaders are combined for sections of the message.)

15. Decoding works for parabolic sequences

We would like to show that the decoding algorithm works: given a vector $x$, it finds a transformation $T \in G$ such that $Tx$ is in the closure of the fundamental region $\overline{FR_{x_0}(G)}$. Suppose we decode using a sequence of parabolic subgroups

$$\{I\} = G_0 < G_1 < \cdots < G_{n-1} < G_n = G.$$ 

The first step is to find a group element $T_1 \in G_1$ such that $T_1x \in \overline{FR_{x_0}(G_1)}$. We will verify below that this can be done by going through the coset leader graph $\Gamma_1$. Then we proceed to $\Gamma_2$ and repeat the process, keeping in mind
that the fundamental regions are nested by Lemma 10. By induction, after going through the graph $\Gamma_k$ we obtain a transformation $T_k \in G_k$ such that $T_k \ldots T_1x \in \text{FR}_{x_0}(G_k)$.

Let us first consider the following simplified form of the algorithm, which works for sequences of reflection subgroups (not just parabolic ones). At each stage, we have a vector $y_i$ and a transformation $V_i \in G$ with $y_i = V_ix$. The initial values are $y_0 = x$ and $V_0 = I$. If there is a fundamental root $\alpha$ such that $(y_i, \alpha) < 0$, then choosing one such we let $y_{i+1} = S_\alpha y_i$ and $V_{i+1} = S_\alpha V_i$. If there is no such $\alpha$, then $y_i$ is in the closure of the fundamental region, and we terminate with $T = V_i$. We only need to show that this algorithm does indeed terminate.

The argument uses the length of $T$ as a product fundamental reflections. This must be interpreted as meaning the length of $T$ in terms of fundamental reflections for $G_k$. These can change as we proceed through the sequence. On the other hand, we will show below that the algorithm does not work for sequences of arbitrary subgroups, at least not without modification.

Recall that a reflection group $G$ acts transitively on its Weyl chambers. Thus, for each vector $x$, there are a vector $x_1$ in the closure of the fundamental region and an element $U \in G$ with $x = Ux_1$. Now $(y_i, \alpha) = (V_i Ux_1, \alpha) < 0$. Applying Lemma 11, we conclude that $\text{length}(S_\alpha VU) = \text{length}(VU) - 1$. Thus the process stops after at most $\text{length}(U)$ steps. (Unless $x_1$ is on the boundary, the algorithm terminates after $\text{length}(U)$ steps with $y_k = x_1 = VUx_1$, so that $V = U^{-1}$.)

The preceding version of the algorithm tests every fundamental root $\alpha$ (for the subgroup) at every step. This is the procedure described in Mitteholzer [4]. Our refinement is to test only the successors of each vertex in the spanning tree of coset leaders, thus eliminating the redundancies of the original method. It remains to verify that, at least for parabolic subgroups sequences, the refinement does not miss the desired transformation.

There are two issues to consider. We terminate the search when no successor of the current vertex in the spanning tree yields a vector that is closer to the initial vector $x_1$ than the one we have. Offhand, we should consider all the successors of the vertex in the graph $\Gamma$. Reduction to the spanning tree is merely a way to avoid redundancies due to group relations such as commutativity and $ABA = BAB$. But to ensure that every candidate has been considered, it is essential that the tree satisfy the technical condition given in that section. Again, the natural way to achieve that condition is to use the alphabetical ordering.

The second issue is that not every neighbor of the current vector is represented by an edge in $\Gamma_k$; some are represented by edges in some $\Gamma_j$ with $j < k$. Theorem 22 gives the possibilities (for parabolic subgroups). The following argument shows that, in the context of our algorithm, only successors of the current vertex in $\Gamma_k$ represent legitimate candidates for the next move. Let us phrase it in terms of decoding from the fundamental region of a subgroup $S$ to that of $T$. The argument is to be applied inductively,
with $S = G_{k-1}$ and $T = G_k$. The vector $u$ represents the vector found by decoding the received vector into the fundamental region of $S$.

Let $G$ be a reflection group and $\{I\} \leq S \leq T \leq G$ with $S$ a parabolic subgroup of $T$. Let $u$ be a vector in the fundamental region of $S$. Then $u = Ux_1$ for some vector $x_1$ in the fundamental region of $T$ and transformation $U \in T$. Assume that we have found an element $L \in T$ such that

1. $L$ is a coset leader for $T$ over $S$, and
2. $\ell(UL) = \ell(U) - \ell(L)$.

Thus $L$ is a product of $\ell(L)$ reflections, each of which reduces the length of the product by one. (Lengths are computed with respect to the fundamental system of $T$.)

Assuming that $u \neq x_1$, let $\beta$ be a fundamental root of $T$ such that $(\beta, Lu) < 0$. Then $S_\beta LU$ will have length $\ell(U) - \ell(L) - 1$. We want to show that the coset leader $K$ for $S_\beta LS$ is a neighbor (necessarily a successor) of $L$ in $\Gamma$. Thus we must eliminate the possibility that $K = L$.

Suppose to the contrary that $S_\beta L \in LS$. Then $L^{-1}S_\beta L = S_{L^{-1}\beta} \in S$ and $S_\beta L U = LS_{L^{-1}\beta} U$. We claim that $\ell(S_{L^{-1}\beta} U) > \ell(U)$ by virtue of Theorems 4 and 5. Thus we count (very carefully) the number of sign changes effected on the positive roots of $T$ by $U$ and $S_{L^{-1}\beta} U$.

First, consider those $\alpha \in \Delta^+ T$ such that $U \alpha \notin \Delta S$. Now $S_{L^{-1}\beta}$ is a product of fundamental reflections of $S$. By Lemma 25, each of these changes the sign of one positive root of $S$, permutes the remaining positive roots of $S$, and permutes the positive roots of $T$ that are not roots of $S$ amongst themselves. (This is not true for nonparabolic subgroups.) So for these roots we have $(U \alpha, x_1) > 0$ if $(S_{L^{-1}\beta} U \alpha, x_1) > 0$.

Now consider those $\alpha \in \Delta^+ T$ with $U \alpha \in \Delta S$. Because $x_1 \in FR(T) \subseteq FR(S)$, for these roots we have

$$(U \alpha, x_1) > 0 \text{ iff } (U \alpha, u) > 0$$

iff $$(U \alpha, Ux_1) > 0$$

iff $(\alpha, x_1) > 0$

which in fact holds. Thus $U$ effects zero sign changes on these roots. On the other hand, $(\beta, Lu) = (L^{-1}\beta, u) < 0$, so $L^{-1}\beta \in \Delta \bar{S}$. Let $\delta = -L^{-1}\beta \in \Delta \bar{S}$. By the preceding calculation, $\delta = U \xi$ for some $\xi \in \Delta^+ T$. Then

$$S_{L^{-1}\beta} U \xi = -\delta = L^{-1}\beta \in \Delta \bar{S} \subseteq \Delta \bar{T}.$$  

Thus $S_{L^{-1}\beta} U$ effects at least one sign change on these roots, and therefore $\ell(S_{L^{-1}\beta} U) > \ell(U)$.

We conclude the argument that $K \neq L$ by noting that consequently $\ell(LS_{L^{-1}\beta} U) > \ell(U)$. But $LS_{L^{-1}\beta} U = S_\beta LU$, and we calculated earlier that $\ell(S_\beta LU) = \ell(U) - \ell(L) - 1$. This contradiction invalidates the assumption that $K = L$.

Thus decoding using the coset leader graphs for a sequence of parabolic subgroups considers all the legitimate candidates, as claimed.
16. Another proof that decoding works

In this section we present a second proof that decoding works for sequences of parabolic subgroups, one which in some respects provides more details.

For every $g \in G$, let us define $\Delta_G(g)$ to be the set of positive roots $\alpha$ in $G$ for which $g\alpha$ is a negative root, and for a reflection subgroup $H$ define $\Delta_H(g)$ to be the set of positive roots $\alpha$ of $H$ for which $g\alpha$ is a negative root. Fixing the subgroup $H$, let us define $\Delta^*_G(g)$ to be the set of positive roots $\alpha$ in $G$ that are not roots of $H$ and for which $g\alpha$ is a negative root. However, length with respect to $G$ may not be the same as length with respect to $H$. We will define $\ell_G(g)$ to mean the length with respect to $G$ and $\ell_H(h)$ to be length with respect to $H$. Note that length with respect to $H$ has meaning only for elements of $H$. Also, $\ell_G(h) = \ell_H(h)$ for parabolic subgroups.

**Theorem 23.** Every coset of a reflection subgroup $H$ of a reflection group $G$ contains a unique element $g_0$ for which $\Delta_H(g_0)$ is empty.

**Proof.** Suppose that $\Delta(g)$ contains a root $\alpha$ that is in $H$, and let $S_\alpha$ denote the corresponding reflection. Let $g_1 = gs_\alpha$. Then by Theorem 5, $g_1$ carries $\alpha$ into a positive root and all the other roots of $H$ are permuted. That means that $\Delta_H(g_1)$ contains one fewer element than $\Delta_H(g)$, and $g_1$ is in the same coset as $g$. In other words, if $\Delta_H(g)$ is not empty, then there is another element $g_1$ of the coset $gH$ with one fewer root. It follows that there must be an element $g_0$ in the coset $gH$ for which $\Delta_H(g_0)$ is empty. □

Now let us consider whether there could be two such elements, $g_0$ and $g_0h$, where $h$ is not the identity element. $\Delta_H(h)$ must not be empty, because if it were empty, that would imply that $\ell_H(h) = 0$, which in turn implies that $h$ is the identity element. Assume that $g_0$ carries no positive roots of $H$ into negative roots, and note that this implies that no negative roots of $H$ are carried into positive roots. However, $h$ carries some positive roots of $H$ into negative roots of $H$. (Note that $h$ carries every root of $H$ into a root of $H$.) Now for $g_0h$, the positive roots of $H$ that are carried into negative roots of $H$ by $h$ will be carried into negative roots by $g_0$, with the result that $g_0h$ carries some positive roots of $H$ into negative roots. Therefore if $|\Delta_H(g_0)| = 0$ and $h$ is an element of $H$, but not the identity element, then $|\Delta_H(g_0h)| \neq 0$. □

Let us choose this element $g_0$ as the coset leader of the coset $gH$.

**Theorem 24.** Let $G$ be a reflection group and $H$ a reflection subgroup, and let $g$ be an element of shortest length in the coset $gH$. If $S$ is a fundamental reflection in $G$ such $\ell_G(Sg) = \ell_G(g) - 1$, then $Sg$ is a minimum-length element in its coset.

**Proof.** Suppose there is a shorter element $f$ than $Sg$ in $SgH$. Then by Theorem 6, $\ell(Sf) \leq \ell(f) + 1 < \ell(g)$, whence $g$ is not a minimum-length element of $gH$, contrary to hypothesis. □
Lemma 25. Let $\alpha$ be a fundamental root of the parabolic subgroup $H$ and $S_\alpha$ the corresponding reflection. Then $S_\alpha$

(a) reverses the sign of $\alpha$,
(b) permutes all the other positive roots of $H$ among themselves, and
(c) permutes the positive roots of $G$ that are not roots of $H$ among themselves.

Proof. Items (a) and (b) follow from Theorem 4 and the fact that $H$ is a group. Because $G$ is a group, all its positive roots except $\alpha$ are permuted, but if every root of $H$ is carried into another root of $H$, each root of $G$ that is not a root of $H$ must be carried into another root that is not a root of $H$. \hfill \square

Theorem 26. If $h$ is an element of the subgroup $H$, then $|\Delta^*_G(h)| = 0$.

Proof. If $\alpha$ is a root and $S_\alpha$ a reflection of $H$, then by the lemma above, the roots of $G$ that are not in $H$ are permuted, and therefore $|\Delta^*_G(h)| = |\Delta^*_G(S_\alpha h)|$. Every element of $H$ can be written as a product of fundamental reflections of $H$, while $|\Delta^*_G(I)| = 0$. The theorem follows by induction on the number of factors in $h$. \hfill \square

For parabolic subgroups, we can prove some stronger results.

Theorem 27. If $G$ is a reflection group and $H$ is a parabolic subgroup, then the coset leader of every coset is the unique shortest element in the coset.

Proof. If $g$ is any group element and $S$ is any fundamental reflection in $H$, then by the lemma above, $|\Delta^*_G(gS)| = |\Delta^*_G(g)|$. Every element of $H$ can be expressed as a product of fundamental reflections of $H$. Applying the previous result for each factor of $h$ shows that for any $h$ we have $|\Delta^*_G(gh)| = |\Delta^*_G(g)|$, so that $|\Delta^*_G(gh)|$ is the same for all elements of the coset $gH$. The length of $gh$ is equal to $|\Delta^*_G(g)| + |\Delta_H(g)|$. The smallest possible value for the length occurs for the unique coset leader for which $|\Delta_H(g)| = 0$, and this length is $|\Delta^*_G(g)|$. \hfill \square

Corollary 28. Let $G$ be a reflection group and $H$ a parabolic subgroup, and let $g0$ be a coset leader and $h \in H$. Then $\ell(g0h) = \ell(g0) + \ell(h)$.

Proof. By the lemma above, for any fundamental reflection $S$ in $H$, we have $|\Delta^*_G(g0S)| = |\Delta^*_G(g0)|$. It follows that $|\Delta^*_G(g0h)| = |\Delta^*_G(g0)|$ for any $h \in H$. Also, since $|\Delta_H(g0)| = 0$, then $|\Delta_H(g0h)| = |\Delta_H(h)|$. Therefore, by Theorem 3,

$$\ell(g0h) = |\Delta^*_G(g0h)| + |\Delta_H(g0h)| = |\Delta^*_G(g0)| + |\Delta_H(h)| = \ell(g0) + \ell(h).$$

\hfill \square

In what follows, we will assume that the coset leader is the unique element $g$ of the coset for which $|\Delta_H(g)| = 0$ and that this is the unique element of the coset for which the length is minimum. Theorems 23 and 27 show that
this is true for parabolic subgroups, and we have found this to be true for all the reflection subgroups that are not parabolic subgroups that we have examined carefully.

For a given coset, there may be more than one expression for the coset leader as a product of fundamental reflections. We want to choose a unique expression to use in what follows. For that purpose we define an order for the expressions. We define $e_1 < e_2$ if written in reverse order, $e_1$ comes before $e_2$ in dictionary order. (Note that if $e$ is an expression for a group element $g$, then the reverse of $e$ is an expression for $g^{-1}$ because each reflection is its own inverse.)

With those assumptions, it is possible to build a tree from the cosets. Make the identity element the root of the tree and make a node for each coset leader. If both $e$ and $S_\alpha e$ are expressions for coset leaders, where $S_\alpha$ is a fundamental reflection of $G$, then connect those two nodes with a branch labeled $S_\alpha$. Each coset leader corresponds to a node in this graph, because of Theorem 24, and if you write the names of all the fundamental reflections on the path from the root node to that node, in reverse order, you get the expression for that coset leader. Thus among the expressions defined by this tree there is one expression for each coset leader.

This tree can be used for decoding. Assume again that $v_I$ is the initial vector and $u$ is the received vector. There is a group element $g'$ such that $g'u$ is in the same region as $v_I$. This $g'$ is essentially the information that we require. Then $g'$ can be expressed uniquely as $g'_0 h$ where $g'_0$ is a coset leader and $h$ is an element of the subgroup. What we propose is to find $g'_0$ and $h$ as separate steps in the decoding process.

Here is the algorithm for finding $g'_0$.

1. Start at the root of the tree, with vector $w = u$.
2. At each node test the branches in alphabetic order.
3. If the label on the branch is $S_\alpha$ and $w$ is on the opposite side of the reflection plane for $S_\alpha$ from $v_I$, then multiply $w$ by $S_\alpha$, move to the node at the end of this branch, and repeat step (2).
4. If no branch passes the test, then this is the node corresponding to $g'_0$ and the path from the root to this node gives an expression for $g'_0$ (in reverse order).

Let $S_\alpha$ be a reflection and $\alpha$ the corresponding root. Again there are two ways to test whether $w$ and $v_I$ are on opposite sides of the reflection plane of $S_\alpha$. One way is to calculate $w \cdot \alpha$ and if this is negative, then $w$ is on the opposite side of the reflection plane from the fundamental region, where $v_I$ is. The other way is to calculate the distance between $w$ and $v_I$ and the distance between $S_\alpha w$ and $v_I$ and if the latter is smaller, then the reflection plane for $S_\alpha$ must be between $u_i$ and $v_I$, by Theorem 7.

Here is a proof that this will work. Suppose you receive vector $u$. Then there exists a group element $g'$ such that $g'u$ is in the same region as $v_I$. Then there exists a coset leader $g_0$ such that $g' = g_0 h$. Let $m = \ell(g_0)$. We
want to determine $g_0$. $g_0$ is a node in the tree and the path from the root of the tree to this node gives an expression with $m$ factors for this coset leader. Starting with $w = u$ and multiplying by those factors results in $g_0u$. Following the above procedure and testing the branches at each node in alphabetic order, you will reach the node that corresponds to $g_0$, because the tree was built with the alphabetically lowest representation of each coset leader as a product of fundamental reflections. The question is, how do you know that you must stop at that node, because you do not know $n$ when you start decoding.

The remaining question is, how do you know when you have reached the node that corresponds to $g_0$, because when you start this algorithm, you do not know $n$. Suppose you are at that node. If there are no branches going out from that node, you have no choice but to quit there. Suppose there is a branch and it is labeled $S_\alpha$. Then the node that it leads to corresponds to $S_\alpha g_0$ which must be a coset leader, but not the correct one. Note that $\ell(S_\alpha g_0) = \ell(g_0)+1$. On the other hand, $|\Delta_H(S_\alpha g_0)| = |\Delta_H(g_0)| = 0$, because both are coset leaders. Therefore, multiplying $u$ by $S_\alpha$ puts the result on the opposite side of the plane corresponding to $S_\alpha$ and since $|\Delta_H(g_0)| = 0$, the plane must be a reflection in $G$ that is not in $H$, and afterwards $S_\alpha u$ is on the opposite side of that reflection plane from $v_I$, so it fails the test. Since every branch will fail the test in this way, the algorithm will stop here at the correct place.

17. Specific groups

17.1. $A_n$. The groups $A_n$ have a particularly simple structure, making them a good example with which to begin. $A_n$ is isomorphic to the symmetric group on $n + 1$ letters, and it is convenient to represent it as acting on the subspace $\sum x_i = 0$ of $\mathbb{R}^{n+1}$. In particular, $A_n$ has size $(n + 1)!$.

For a concrete example, we consider $A_4$, which has order $5! = 120$. The Coxeter graph for $A_4$ is given in Figure 1.

```
A  B  C  D
```

**Figure 1.** Coxeter graph for $A_4$

Now we take the subgroups sequence

$I < A_1 < A_2 < A_3 < A_4$

where $A_1$ is the subgroup generated by $\{A\}$, the subgroup $A_2$ is generated by $\{A, B\}$, etc. Note that our ordering of the parabolic subgroups is implicit in the labelling of the Coxeter graph, and this choice is not unique.
The coset leader graphs $\Gamma_1$ to $\Gamma_4$ are given in Figure 2. The vertices of $\Gamma_k$ are labelled 0, \ldots, k; to avoid cluttering the figure we have labelled only $\Gamma_4$. Also it is understood that the edges are always directed downward, from vertex $j$ to $j + 1$.

\begin{center}
\begin{tikzpicture}
    \node (A) at (0,0) {A};
    \node (B) at (1,0) {B};
    \node (C) at (2,0) {C};
    \node (D) at (3,0) {D};
    \node (E) at (0,1) {A};
    \node (F) at (1,1) {B};
    \node (G) at (2,1) {C};
    \node (H) at (3,1) {D};
    \node (I) at (0,2) {A};
    \node (J) at (1,2) {B};
    \node (K) at (2,2) {C};
    \node (L) at (3,2) {D};
    \node (M) at (0,3) {A};
    \node (N) at (1,3) {B};
    \node (O) at (2,3) {C};
    \node (P) at (3,3) {D};
    \node (Q) at (0,4) {A};
    \node (R) at (1,4) {B};
    \node (S) at (2,4) {C};
    \node (T) at (3,4) {D};

    \draw[->] (A) -- (B);
    \draw[->] (B) -- (C);
    \draw[->] (C) -- (D);
    \draw[->] (D) -- (E);
    \draw[->] (E) -- (F);
    \draw[->] (F) -- (G);
    \draw[->] (G) -- (H);
    \draw[->] (H) -- (I);
    \draw[->] (I) -- (J);
    \draw[->] (J) -- (K);
    \draw[->] (K) -- (L);
    \draw[->] (L) -- (M);
    \draw[->] (M) -- (N);
    \draw[->] (N) -- (O);
    \draw[->] (O) -- (P);
    \draw[->] (P) -- (Q);
    \draw[->] (Q) -- (R);
    \draw[->] (R) -- (S);
    \draw[->] (S) -- (T);

    \node at (0,5) {0};
    \node at (1,5) {1};
    \node at (2,5) {2};
    \node at (3,5) {3};
    \node at (4,5) {4};
\end{tikzpicture}
\end{center}

\textbf{Figure 2.} Coset leader graphs $\Gamma_k$ for $A_4$

The elements of the group $A_n$ are then identified by sequences $d = (d_1, d_2, d_3, d_4)$ with each $d_i$ a vertex in $\Gamma_i$. For example, the sequence $(1,0,2,2)$ corresponds to the product (from right to left) $CD \cdot BC \cdot I \cdot A = CDBCA$.

Now we assign binary sequences to the first $2^x$ vertices of $\Gamma_k$, where $x = \lceil \log_2(|\Gamma_k|) \rceil = \lceil \log_2(k + 1) \rceil$, which is the first two vertices of $\Gamma_1$ and $\Gamma_2$, and the first four vertices of $\Gamma_3$ and $\Gamma_4$. If we do this using a Gray Map, so that neighboring vertices have binary sequences differing in only one bit, we obtain the assignment shown in Figure 3.

\begin{center}
\begin{tikzpicture}
    \node (00) at (0,0) {0};
    \node (01) at (0,1) {0};
    \node (10) at (1,0) {1};
    \node (11) at (1,1) {1};
    \node (00) at (2,0) {00};
    \node (01) at (2,1) {01};
    \node (10) at (3,0) {10};
    \node (11) at (3,1) {11};
    \node (00) at (4,0) {00};
    \node (01) at (4,1) {01};

    \draw[->] (00) -- (01);
    \draw[->] (01) -- (10);
    \draw[->] (10) -- (11);
    \draw[->] (11) -- (00);
\end{tikzpicture}
\end{center}

\textbf{Figure 3.} Binary sequence assignments for $A_4$

Then we can use 64 elements of our 120-element group to encode six-bit messages. We think of a message as being broken into four parts

\[ m_1 \ m_2 \ m_3 m_4 \ m_5 m_6 \]
associated with the four graph labellings. For example, the message \( m = 101111 \) corresponds to the vertex sequence \((1, 0, 2, 2)\), which as we saw above represents the element \(CDBCA\).

Of course, the choice \( n = 4 \) gives us a rather “toy” example, but in practice it is not much harder to do larger \( n \). The only complication is that in order to encode at or near the maximum number of bits \( \lfloor \log_2(|G|) \rfloor \), we must combine the binary assignments for pairs of graphs, as discussed previously. But for the permutation groups \(A_n, B_n\) and \(D_n\) this process is also quite straightforward, and we have written the programs for \( n \) a power of 2 up to \( n = 2^5 = 32 \), without much difficulty.

For the permutation groups \(A_n, B_n\) and \(D_n\) we can compare our method (using coset leaders) with Slepian’s method (using sorting methods for the permutation). There are, of course, very efficient sorting algorithms available. Using coset leaders for the permutations is not bad, but certainly not as fast as the best sorting algorithms. On the other hand, the coset leaders give us a natural way to represent and keep track of the permutations, which for large \( n \) is a real issue.

17.2. \(B_n\). The groups \(B_n\) have larger size for the same dimension \( (2^n n! \) versus \((n + 1)! \) for \(A_n\)) and a refined subgroup sequence, making them a better candidate for group coding, especially for larger \( n \). Again, to make a specific example we choose \( n = 4 \). The Coxeter graph for \(B_4\) is given in Figure 4.

\[
\begin{array}{cccc}
A & 4 & B & C & D \\
\end{array}
\]

**Figure 4.** Coxeter graph for \(B_4\)

The coset leader graph for the sequence of parabolic subgroups

\[
I < B_1 < B_2 < B_3 < B_4
\]

is given in Figure 5. Again, elements of \(B_n\) are identified by sequences \(d = (d_1, d_2, d_3, d_4)\) with each \(d_i\) in \(\Gamma_i\). Likewise, we can assign bit-strings to 256 of the 384 group elements using Gray codes.

For the actual dirty work of encoding and decoding, we want to use the refined subgroup sequence

\[
I < B_1 < M_2 < B_2 < M_3 < B_3 < M_4 < B_4
\]

where \(M_k\) is the subgroup generated by \(B_{k-1}\) and the longest coset leader \(R_k\) for \([B_k : B_{k-1}]\). In fact, \(R_k\) is a reflection, so \(R_k^2 = I\), and it commutes with the elements of \(B_{k-1}\), whence \(M_k \cong B_{k-1} \times A_1\). (See the examples below.) For this subgroup sequence we have another coset leader sequence \(e\), so we also need a translation between the \(d\) and \(e\) sequences.
Using the reflections $R_2 = BAB$, $R_3 = CBABC$ and $R_4 = DCBABC\!\!D$ the coset leader graph for the refined sequence is given in Figure 6.

The sequence $e = (e_1, \ldots, e_7)$ translates into $d$ by the correspondence

\[
\begin{align*}
    d_1 &= e_1 \\
    d_2 &= e_3 & \text{if } e_2 = 0 \\
    &= 3 - e_3 & \text{if } e_2 = 1 \\
    d_3 &= e_5 & \text{if } e_4 = 0 \\
    &= 5 - e_5 & \text{if } e_4 = 1 \\
    d_4 &= e_7 & \text{if } e_6 = 0 \\
    &= 7 - e_7 & \text{if } e_6 = 1
\end{align*}
\]

Finally, for $n \geq 6$ we will again want to combine the cosets in assigning the bit-strings, but this can be done at the $d$-sequence level.

17.3. $D_n$. The groups $D_n$ are in many ways similar, but introduce a few new features. They are also useful as building blocks for the groups $E_6$, $E_7$ and $E_8$. The cardinality of $D_n$ is $2^{n-1}n!$, so for the same dimension we lose
a bit and gain a little in terms of distance. The structure of $D_4$ is atypically symmetric, so we illustrate with $D_5$. The Coxeter graph for $D_5$ is given in Figure 7.

![Figure 7. Coxeter graph for $D_5$](image)

Figure 8. Coset leader graphs $\Gamma_k$ for $D_5$

The corresponding coset leader graphs for the sequence of parabolic subgroups is in Figure 8. The fact that $AB = BA$ makes the graph nonlinear. In this event, we do not label the lower edges, which carry the same value as their opposite (transposed) edge. The spanning trees $T_k$ are indicated by darker lines.

Similar to the case with $B_n$, the group $D_n$ has a refining subgroup sequence. For $D_5$ this is

$$I < D_1 < D_2 < N_3 < D_3 < N_4 < D_4 < N_5 < D_5$$

where $N_k$ is the subgroup generated by $D_{k-1}$ and the longest coset leader $R_k$ for $[D_k : D_{k-1}]$. Since $A$ and $B$ commute, the refinement starts with dimension 3. The longest coset leaders $R_k$ in $\Gamma_k$ for our case are $R_3 = CABC$, $R_4 = DCABCD$, and $R_5 = EDCABCDE$. They satisfy $R_2^k = I$, but they are rotations rather than reflections, being the product of an even number of reflections. Nor do they commute with the elements of $D_{k-1}$. For example,

$$AR_3 = ACABC = CACBC = CABCB = R_3B.$$
So $N_k$ is not a direct product. Nonetheless, they work fine for encoding and decoding purposes, once we make a minor adjustment. Figure 9, which labels the vertices rather than the edges of $\Gamma_4$, illustrates pretty well what is going on. Figure 10 gives the coset leaders for the refined sequence, ignoring the dashed lines temporarily.

Figure 9. Example with $\Gamma_4$ for $D_4$

Consider the vector $x = DCAx_0 = (ACD)^{-1}x_0$ which we would use to encode the element $ACD = BCDR_4$, the latter being the representation as
a product of coset leaders. However,
\[ \| x - x_0 \| = \| DCAx_0 - x_0 \| \]
\[ = \| DCBx_0 - x_0 \| \quad \text{by symmetry} \]
\[ = \| R_4DCAx_0 - x_0 \| \]
\[ = \| R_4x - x_0 \|. \]

So in decoding \( x \), even with exact arithmetic, you wouldn’t know whether
to take \( R_4 \) as part of the coset leader or not. Indeed, the scheme indicated
by Figure 10 would use \( BCD \) and \( BCDR_4 \) for elements that could also
be represented as \( ACDR_4 \) and \( ACD \), respectively. Adding roundoff error
and noise just make the situation worse. The easy solution is to allow both
representations for all such middle elements. Thus we have added the \textit{faux}
coset leaders, indicated by dashed lines.

The sequence \( e = (e_1, \ldots, e_7) \) translates into \( d \) by a correspondence similar
to the one used for \( B_n \), except that we must account for the dual representation.

The refined sequence for \( D_n \) has an unexpected advantage. It is not hard
to see, using parity considerations, that for \( k \geq 3 \) odd one cannot assign bit
strings to the top \( 2^x \) elements of \( \Gamma_k \) in such a way that adjacent vertices differ
by one bit (because of the split). With the refined sequence, we wind up
using the top and bottom \( 2^{x-1} \) elements, avoiding the middle and removing
the parity problem. (For \( n = 2^x \) we use the middle elements, but there is
no parity problem.)

Finally, for larger \( n \) we must as usual combine cosets.

17.4. \( F_4 \). The exceptional group \( F_4 \) has size \( 2^{7}3^2 = 1152 \), and exhibits a
little more structure than the preceding groups. The Coxeter graph for \( F_4 \)
is given in Figure 11. For encoding and decoding \( F_4 \) we use the sequence of
reflection subgroups
\[ I < B_1 < M_2 < B_2 < M_3 < B_3 < M_4 < B_4 < F_4 \]
where the first part of the sequence, through \( B_3 = \text{Sg}(A, B, C) \), is the standard
sequence for \( B_3 \). The latter subgroups are given by
\[ M_4 = \text{Sg}(A, B, C, X) \]
\[ B_4 = \text{Sg}(A, B, C, Y) \]
\[ F_4 = \text{Sg}(A, B, C, D) \]
where \( X \) and \( Y \) are the reflections
\[ X = DABACBADABCABAD \]
\[ Y = DABAD. \]

The coset leader graph for \( F_4 \) over \( B_3 \) is given in Figure 12. This is the graph
we use for determining the binary assignments (neighbors should differ by
few bits), but the spanning tree is not indicated because for encoding and
decoding we will use instead the coset leader graphs for the intermediate subgroups, shown in Figure 13.

\[
\begin{array}{cccc}
D & A & 4 & B & C \\
\end{array}
\]

**Figure 11.** Coxeter graph for $F_4$

\[
D \\
A \\
B \\
A \\
D \\
C \\
A \\
B \\
D \\
A \\
B \\
A \\
D \\
C
\]

**Figure 12.** Coset leader graphs for $F_4$ over $B_3$

17.5. $E_6$, $E_7$ and $E_8$. The group $E_6$ has cardinality $2^73^45 = 51,840$. Depending on how we index the generators, it can be considered to be an extension of either $D_5$ or $A_5$. Both these possibilities are indicated in Figure 14. The coset leader graph is simpler for the former case, and that is given in Figure 15. The coset leader graph for $E_6$ over $A_5$ is not planar.
The group $E_7$ has size $2^{10} \cdot 3^4 \cdot 5 \cdot 7 = 2,903,040$. Its parabolic subgroup $D_6$ has index 126, almost optimally bad for coding purposes. So instead we used the subgroup $E_6$ with index 57, which is somewhat better. Implementing coding and decoding in this case was straightforward; the coset leader graph is not included here.

The group $E_8$ with cardinality $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7 = 696,729,600$ is another matter. Jiajia Seffrood and the authors drew the coset leader graph for $E_8$ over $E_7$, which has 240 elements (and is not reproduced here). The problem is how to find a good binary assignment for this graph, and we have not yet implemented the coding scheme.

**REFERENCES**

Figure 15. Coset leader graph for $E_6$ over $D_5$


ELECTRICAL ENGINEERING DEPARTMENT, UNIVERSITY OF HAWAI'I, HONOLULU, HI 96822, USA
E-mail address: marc@aravis.eng.hawaii.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAI'I, HONOLULU, HI 96822, USA
E-mail address: jb@math.hawaii.edu

DEPARTMENT OF INFORMATION AND COMPUTER SCIENCE, UNIVERSITY OF HAWAI'I, HONOLULU, HI 96822, USA
E-mail address: wes@hawaii.edu