Reflection Group Codes and their Decoding

Marc Fossorier, J.B. Nation and Wes Peterson

University of Hawai‘i at Mānoa

Ashikaga, August 2010
Background

History.zip

- Basic idea due to David Slepian in 1950s and 1960s: choose a group of orthogonal matrices and a point on a sphere, and use the orbit of that point by that group as a set of signals for communication.
- Refinement by Mittelholzer and Lahtonen in 1996.
- Extension to complex groups by Kim, Shepler, N in 2008-2010.

For comparison
Modulation via nPSK or QAM

First task
Recall a lot of group theory you never knew!
Inner products and transposes

- \((x, y) = x^T y\)
- \((Mx, y) = (x, M^T y) = x^T M^T y\)
- \(\|x\| = \sqrt{(x, x)}\) and \(d(a, b) = \|a - b\|\)

Orthogonal matrices

- **M** is **orthogonal** if \(MM^T = I\), i.e., \(M^T = M^{-1}\)
- If **M** is orthogonal, then

\[
(Mx, y) = (x, M^{-1}y)
\]

\[
(Mx, My) = (x, y)
\]

\[
\|Mx - y\| = \|x - M^{-1}y\|
\]
Groups of orthogonal matrices

All \( n \times n \) orthogonal matrices form a group \( O(n) \).

- \( I \) is orthogonal.
- The inverse of an orthogonal matrix is orthogonal.
- Products of orthogonal matrices are orthogonal.

Examples

- Dihedral groups \( H^k_2 \) generated by the matrices
  \[
  \begin{bmatrix}
  c & -s \\
  s & c
  \end{bmatrix}
  \quad \text{and} \quad
  \begin{bmatrix}
  1 & 0 \\
  0 & -1
  \end{bmatrix}
  \]

  where \( c = \cos \frac{2\pi k}{k} \) and \( s = \sin \frac{2\pi k}{k} \)

- The group \( A_{n-1} \) of all \( n \times n \) permutation matrices

- The group \( B_n \) of all \( n \times n \) permutation matrices with entries \( \pm 1 \)
Basic idea

Let $G$ be a finite group of isometries on $\mathbb{R}^n$.

$G$ acts on the sphere of radius 1.

Choose an initial vector $x_0 \in V$ with $\|x_0\| = 1$.

Associate a group element $g$ with each message $m$.

\[ m \rightarrow x = g^{-1}x_0 \rightarrow r = x + n \rightarrow g'r \approx x_0 \rightarrow m' \]

$G$ acts faithfully and transitively on $Gx_0 = \{gx_0 : g \in G\}$

(or if not, factor out the isotropy group).
2n-PSK: With dihedral groups, use points on the circle to transmit bit-strings of length \( \lceil \log 2n \rceil \).

With the group \( E_6 \), use points on the sphere in \( \mathbb{R}^6 \) to represent bit-strings of length 15.

With the group \( B_{32} \), use points on the sphere in \( \mathbb{R}^{32} \) to represent bit-strings of length 148.

More generally, we can identify the group elements themselves with the (not necessarily binary) message.
Reflection group

...a group $G$ generated by a set of reflections on $\mathbb{R}^n$.

Reflection

For $\alpha$ a unit vector, $S_{\alpha}(x) = x - 2(x, \alpha)\alpha$.

Reflection planes

$N_{\alpha} = \{x : (x, \alpha) = 0\}$ is the set of vectors fixed by $S_{\alpha}$.

Roots

$\Delta(G) = \{\alpha : S_{\alpha} \in G\}$
Example - $A_2$

Notation on whiteboard

\[ A = S_\alpha \]

\[ B = S_\beta \]

\[ G = \{ I, A, B, AB, BA, ABA \} \]
The reflection planes divide the space into **regions**.

Pick one region to be the **fundamental region** $\text{FR}(G)$.

Choose an **initial vector** $\mathbf{x}_0$ in the fundamental region.

A root $\beta$ is **positive** if $(\beta, \mathbf{x}_0) > 0$.

The positive roots whose reflection planes form the walls of the fundamental region are the **fundamental roots**.

$\text{FR}(G) = \{ \mathbf{y} : (\alpha, \mathbf{y}) > 0 \text{ for every fundamental root } \alpha \}$
Generators and length

- **G** is generated by the reflections $S_{\alpha}$ with $\alpha$ a fundamental root.
- The **length** $\ell(g)$ is the minimum number $k$ such that $g$ is a product of $k$ fundamental reflections.
- Roughly speaking, $\|gx_0 - x_0\|$ increases with $\ell(g)$: if $\ell(S_{\alpha}g) = \ell(g) + 1$, then $\|S_{\alpha}gx_0 - x_0\| > \|gx_0 - x_0\|$.

Classification of irreducible reflection groups

$A_n, B_n, D_n, E_6, E_7, E_8, F_4, H_n^2, I_3, I_4$
The action of $G$ on roots

Technical definition
Let $\Delta_G(g)$ denote the set of positive roots for which $g\alpha$ is a negative root.

Theorem
If $\alpha$ is a positive root and $v$ is not on the reflecting plane $N_\alpha$, then $N_\alpha$ is between $v$ and $gv$ if and only if $\alpha \in \Delta_G(g^{-1})$.

Theorem
If $S_\alpha$ is a fundamental reflection, then $S_\alpha \alpha = -\alpha$ and $S_\alpha$ permutes all the other positive roots.

Theorem
If $\alpha$ is any root and $u$ and $v$ are on the same side of the reflection plane $N_\alpha$, then $v$ is closer than $S_\alpha v$ to $u$. If $u$ and $v$ are on opposite sides of $N_\alpha$, then $S_\alpha v$ is closer than $v$ to $u$. 
Theorem

TFAE.

1. \( \ell(g) = k \).
2. For any vector \( \mathbf{v} \) that is not in any reflecting plane, the number of reflecting planes that separate \( \mathbf{v} \) and \( g\mathbf{v} \) is \( k \).
3. \( |\Delta_G(g)| = k \).
### Types of subgroups

- **parabolic** - generated by fundamental reflections
- **reflection** - generated by reflections
- **other**

### Definition

If $H$ is a reflection subgroup, the **fundamental region** $FR(H)$ is the region containing $x_0$ and bounded by the reflection planes of $H$.

### Theorem

If $H$ is a reflection subgroup of $G$, then $FR(G) \subseteq FR(H)$. 
Let $H$ be a reflection subgroup of $G$.

**Lemma**
- Each left coset $gH$ contains a unique element $c$ of minimal length.
- Choose $c$ as the coset leader.

**Theorem**
If $x \in FR(H)$, then there is a unique coset leader $c$ such that $cx \in FR(G)$ and we have an efficient algorithm to find it.
Summary of group theory background

- group $\mathbf{G}$ of orthogonal matrices
- reflection, reflection group, reflection subgroup
- initial vector $\mathbf{x}_0$
- fundamental regions $\text{FR}(\mathbf{H}) \supseteq \text{FR}(\mathbf{G})$
- coset leader
The algorithm

Setup

- Choose a chain of reflection subgroups

\[ \{ I \} = G_0 < G_1 < \cdots < G_k = G \]

- The fundamental regions are nested in reverse order:

\[ \mathbb{R}^n = FR(I) \supseteq FR(G_1) \supseteq \cdots \supseteq FR(G) \]
The algorithm

**Encode**
- Given a message \( \mathbf{m} \),
- take the corresponding group element \( g \).
- Write it as a product of coset leaders \( g = c_k \ldots c_1 \).
- Transmit \( \mathbf{x} = g^{-1} \mathbf{x}_0 = c_k^{-1} \ldots c_1^{-1} \mathbf{x}_0 \).
The algorithm

\[ r = x + n \]
The algorithm

- $r \in \text{FR}(G_0)$
- Find the coset leader $d_1$ with $d_1 r \in \text{FR}(G_1)$
- Find the coset leader $d_2$ with $d_2 d_1 r \in \text{FR}(G_2)$
- etc.
- to obtain $d_k \ldots d_1 r \in \text{FR}(G)$
- Decode $g' = d_k \ldots d_1 \rightarrow m'$. 

Fossorier, Nation, Peterson  
Reflection Group Codes
Notation for the examples

Coset leaders
The coset leaders are arranged into graphs.

Matrices
\[ \tau_{12} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \sigma_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \]

etc.
Decoding $A_4$

$x_0 = \langle -2, -1, 0, 1, 2 \rangle$
Decoding $A_6$ bent
Decoding $B_4$

$$\sigma_1 \sigma_4 \tau_{14} \sigma_2 \tau_{12} \tau_{24} \sigma_3 \tau_{23} \tau_{34}$$

$$x_0 = \langle 0.707, 1.707, 2.707, 3.707 \rangle$$
Average number of comparisons to decode $A_n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\bar{a}_n$</th>
<th>$\bar{a}'_n$</th>
<th>$\log_2(n + 1)!$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>7.7</td>
<td>7.1</td>
<td>6.9</td>
</tr>
<tr>
<td>8</td>
<td>24.2</td>
<td>19.5</td>
<td>18.4</td>
</tr>
<tr>
<td>16</td>
<td>81.6</td>
<td>57.4</td>
<td>48.3</td>
</tr>
<tr>
<td>32</td>
<td>292.9</td>
<td>182.2</td>
<td>122.7</td>
</tr>
</tbody>
</table>

where

- $\bar{a}_n$ is the average number of comparisons needed to decode $A_n$ using straight coset leader graphs (parabolic subgroups)
- $\bar{a}'_n$ is the average number of comparisons needed to decode $A_n$ using bent coset leader graphs (a different subgroup sequence)
- $\log_2(n + 1)!$ is the theoretical minimum average number of comparisons
### Average number of comparisons to decode $B_n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\bar{b}_n$</th>
<th>$\bar{b'}_n$</th>
<th>$\bar{b''}_n$</th>
<th>$n + \log_2 n!$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>11.0</td>
<td>8.9</td>
<td>8.7</td>
<td>8.6</td>
</tr>
<tr>
<td>8</td>
<td>38.6</td>
<td>27.3</td>
<td>24.0</td>
<td>23.3</td>
</tr>
<tr>
<td>16</td>
<td>142.3</td>
<td>88.6</td>
<td>67.7</td>
<td>60.3</td>
</tr>
<tr>
<td>32</td>
<td>542.0</td>
<td>307.9</td>
<td>204.5</td>
<td>149.7</td>
</tr>
</tbody>
</table>

where

- $\bar{b}_n$ is the average number of comparisons to decode $B_n$ using parabolic subgroups
- $\bar{b'}_n$ is the average number of comparisons to decode $B_n$ using intermediate subgroups with straight CL graphs
- $\bar{b''}_n$ is the average number of comparisons to decode $B_n$ using intermediate subgroups with bent CL graphs
- $n + \log_2 n!$ is the theoretical minimum average number of comparisons
Refinements

**Error control**
- Received vectors from neighboring regions decode to group elements with only one coset leader different.
- A linear block code can be super-imposed.

**Efficiency**
- Choosing the right subgroup sequence can double decoding efficiency.
- Complex permutation groups $G(r, k, n)$ work similarly with large minimum distance.
Use of subgroup decoding may make group coding practical.

Group codes with nontrivial isotropy subgroups can be decoded with this algorithm (though some care is required).

Further testing and analysis is required.

Other groups and other decoding methods should be considered.

Thank you!