Frames and Spherical Codes: where Slepian meets Fourier and Galois

Babak Hassibi

joint work with Matthew Thill

California Institute of Technology

ECE Seminar, UCSD, October 30, 2013
....Lame Attempt at a Bar Joke....
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar

What does the waitress say?
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar

What does the waitress say?

a. Are you a group?
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar

What does the waitress say?

a. Are you a group?
b. Do you come here periodically?
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar.

What does the waitress say?

a. Are you a group?
b. Do you come here periodically?
c. Where’s Jack?
....Lame Attempt at a Bar Joke....

David Slepian, Joseph Fourier and Evariste Galois go to a bar

What does the waitress say?

a. Are you a group?
b. Do you come here periodically?
c. Where’s Jack?
d. ✓ May I see your ID? (Courtesy of Lorenzo Coviello)
Outline

- Introduction
  - applications
  - tight frames, equiangular frames, Harmonic frames, Welch’s bound, difference sets
- Slepian’s construction of frames from groups
- Cyclic groups, dihedral groups, Zadoff-Chu sequences
- Fourier transforms over groups
  - Hadamard frames, new “optimal” frames, representation theory for non Abelian groups
- Conclusion and generalizations
Low Coherence Frames

The coherence of a collection of $n$ unit-norm vectors $v_i \in \mathbb{C}^m$, $i = 1, \ldots, n$, with $m < n$, is defined as

$$\mu = \max_{i \neq j} |v_i^* v_j|.$$ 

We often collect the vectors into an $m \times n$ matrix

$$M = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix}$$

and call it a frame. Furthermore, we are often interested in constructing low-coherence frames and, in particular, solving

$$\min_{\{v_i \in \mathbb{C}^m, \|v_i\|=1\}_{i=1}^n} \max_{i \neq j} |v_i^* v_j| = \mu_{\text{min}}.$$
Applications

Low coherence frames arise in many applications:

- **Spherical codes:**
  - \[ \| v_i - v_j \|^2 = 2(1 - \text{Real}(v_i^* v_j)) \]
- **CDMA:**
  - spreading sequences
- **MIMO communications and SDMA:**
  - quantizing the unit sphere
- **Quantum measurements**
  - designing optimal rank-1 (pure state) measurement operators
- **Compressed sensing:**
  - orthogonal matching pursuit
Frames and spherical codes come up wherever we want to *uniformly* quantize the unit sphere

- uniformly quantizing intervals, rectangles, cubes, etc., is trivial
- the sphere is the simplest shape whose uniform quantization is highly non-trivial

In communication applications, \( n \) is exponentially larger than \( m \):

\[ n = e^{mR} \]

where \( R \) is the rate of the code

- in such setting, random codes perform quite well
- a lot is known about the asymptotics

However, we are not interested in this regime. We are interested in the situation where \( n \) is a constant multiple of \( m \), i.e., coarse quantization

- in this regime, judicious choice of the points can significantly outperform random ones
Frames and spherical codes come up wherever we want to **uniformly** quantize the unit sphere

- uniformly quantizing intervals, rectangles, cubes, etc., is trivial
- the sphere is the simplest shape whose uniform quantization is highly non-trivial

In communication applications, \( n \) is exponentially larger than \( m \):

\[
    n = e^{mR}, \text{ where } R \text{ is the rate of the code}
\]

- in such setting, random codes perform quite well
- a lot is known about the asymptotics
Frames and spherical codes come up wherever we want to uniformly quantize the unit sphere

- uniformly quantizing intervals, rectangles, cubes, etc., is trivial
- the sphere is the simplest shape whose uniform quantization is highly non-trivial

In communication applications, $n$ is exponentially larger than $m$: $n = e^{mR}$, where $R$ is the rate of the code

- in such setting, random codes perform quite well
- a lot is known about the asymptotics

However, we are not interested in this regime. We are interested in the situation where $n$ is a constant multiple of $m$, i.e., coarse quantization

- in this regime, judicious choice of the points can significantly outperform random ones
Tight and Equiangular Frames and Welch’s Bound

Consider the frame

\[ M = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \in C^{m \times n}, \quad \|v_i\| = 1 \]
Tight and Equiangular Frames and Welch’s Bound

Consider the frame

\[ M = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \in \mathbb{C}^{m \times n}, \quad \|v_i\| = 1 \]

\( M \) is called tight if \( MM^* = \frac{n}{m} I_M \)

\( M \) is called equiangular if \( |v_i^* v_j| = c, \forall i \neq j \)

\[ \mu_{\min} \geq \sqrt{n - m} \frac{(n - 1)}{m} \]

with equality iff the frame is tight and equiangular.
Tight and Equiangular Frames and Welch’s Bound

Consider the frame

\[ M = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \in \mathbb{C}^{m \times n}, \quad \|v_i\| = 1 \]

\( M \) is called **tight** if \( MM^* = \frac{n}{m} I_M \)

\( M \) is called **equiangular** if

\[ |v_i^* v_j| = c, \quad \forall i \neq j \]
Tight and Equiangular Frames and Welch’s Bound

Consider the frame

$$M = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \in \mathbb{C}^{m \times n}, \quad \|v_i\| = 1$$

$M$ is called **tight** if $MM^* = \frac{n}{m} I_M$

$M$ is called **equiangular** if

$$|v_i^* v_j| = c, \quad \forall i \neq j$$

**Theorem (Welch’s Bound)**

$$\mu_{\min} \geq \sqrt{\frac{n - m}{m(n - 1)}}$$

with equality iff the frame is tight and equiangular.
Proof of Welch’s Bound

Note that $M^* M$ is the Gram matrix with entries $v_i^* v_j$

$$n(n-1)\mu^2 \geq \sum_{i \neq j} |v_i^* v_j|^2 = \text{trace} \left( (M^* M)^2 \right) - n.$$

Now $\text{trace} M^* M = \sum_{i=1}^m \lambda_i = n$ and $\text{trace} \left( (M^* M)^2 \right) = \sum_{i=1}^m \lambda_i^2$. Thus,

$$\text{trace} \left( (M^* M)^2 \right) \geq \left( \frac{n}{m} \right)^2 \cdot m = \frac{n^2}{m},$$

with equality when $\lambda_1 = \ldots \lambda_m = \frac{n}{m}$. Therefore

$$n(n-1)\mu^2 \geq \sum_{i \neq j} |v_i^* v_j|^2 \geq \frac{n^2}{m} - n,$$

where the first inequality is achieved iff the frame is equiangular, and the second iff it is tight. This gives the Welch bound.
Optimal Frames

- Frames that achieve the Welch bound do not exist for all $n$ and $m$.
Optimal Frames

- Frames that achieve the Welch bound do not exist for all $n$ and $m$
  - for example, they cannot exist for $n > m^2$
Optimal Frames

- Frames that achieve the Welch bound do not exist for all $n$ and $m$
  - for example, they cannot exist for $n > m^2$
- There are a handful of cases where optimal frames are known. Here are a few:
Optimal Frames

- Frames that achieve the Welch bound do not exist for all \( n \) and \( m \)
  - for example, they cannot exist for \( n > m^2 \)
- There are a handful of cases where optimal frames are known. Here are a few:
  - \( n = p^\alpha + 1 \), where \( p \) is an odd prime and \( m = \frac{n}{2} \). The vectors \( v_i \) have 0 and \( \pm 1 \) entries.
  - \( n = 2^\alpha \) and \( m = \frac{n}{2} \). The vectors \( v_i \) have 0 and \( \pm 1 \) entries.
  - \( n = m^2 - m + 1 \), \( m = p^\alpha + 1 \) and the frame is a Harmonic frame, i.e.,
    \[
    v_{i,k} = \frac{1}{\sqrt{m}} e^{j \frac{2\pi f_k i}{n}},
    \]
    for some frequencies \( \{ f_k \}_{k=1}^m \). In other words, \( M \) represents \( m \) rows of the Fourier matrix (corresponding to \( \{ f_k \}_{k=1}^m \)).
Possible Ideas?

Try choosing rows of the DFT matrix? ("Harmonic Frames")

- \( \omega = e^{\frac{2\pi i}{n}} \)

\[
\mathcal{M} = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{k_1 \cdot 2} & \ldots & \omega^{k_1 \cdot (n-1)} \\
1 & \omega^{k_2} & \omega^{k_2 \cdot 2} & \ldots & \omega^{k_2 \cdot (n-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{k_m \cdot 2} & \ldots & \omega^{k_m \cdot (n-1)}
\end{bmatrix}
\]

- Orthogonal rows yield a tight frame.
- How do we choose the frequencies \( k_i \)?
Choosing the $k_i$ Randomly vs. Deterministically

Figure: $n = 499$, $m = 166$, $r = \frac{n-1}{m} = 3$
Possible Ideas

Try choosing rows of the Hadamard matrix?

- $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- $H_{2k} = \begin{bmatrix} H_{2k-1} & H_{2k-1} \\ H_{2k-1} & -H_{2k-1} \end{bmatrix} \in \mathbb{R}^{2^k \times 2^k}$

- All entries are $\pm 1$
- Orthogonal rows $\Rightarrow$ Tight frame
- Each row and column of $H_{2k}$ can be indexed by $k$-bit vectors $a = [a_1 \ a_2 \ \ldots \ a_k]$ and $b = [b_1 \ b_2 \ \ldots \ b_k]$, so that the corresponding entries are given by

$$(-1)^{\sum_{i=1}^{k} \oplus a_i b_i}.$$ 

- How to choose the $a$, i.e., a subset of the rows?
Choosing Hadamard Rows Randomly vs. Deterministically

<table>
<thead>
<tr>
<th>$(n, m)$</th>
<th>Random Hadamard</th>
<th>Deterministic Hadamard</th>
<th>$\sqrt{\frac{n-m}{m(n-1)}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(256, 51)</td>
<td>0.3725</td>
<td>0.2549</td>
<td>0.1256</td>
</tr>
<tr>
<td>(256, 85)</td>
<td>0.2941</td>
<td>0.1294</td>
<td>0.0888</td>
</tr>
<tr>
<td>(512, 73)</td>
<td>0.3425</td>
<td>0.2329</td>
<td>0.1085</td>
</tr>
</tbody>
</table>
Choosing Hadamard Rows Randomly vs. Deterministically

Figure: $n = 256$, $m = 85$, $r = \frac{n-1}{m} = 3$
The Goal

- We would like to devise a **systematic** way of designing low coherence frames.
The Goal

- We would like to devise a *systematic* way of designing low coherence frames
  - as a result, we will come up with many new instances of optimal frames

\[
\binom{n^2}{2} = n(n-1)^2.
\]
The Goal

- We would like to devise a systematic way of designing low coherence frames
  - as a result, we will come up with many new instances of optimal frames

The challenge in designing low coherence frames is that we must control

\[
\binom{n}{2} = \frac{n(n-1)}{2},
\]

inner products.
The Goal

- We would like to devise a *systematic* way of designing low coherence frames
  - as a result, we will come up with many new instances of optimal frames

The challenge in designing low coherence frames is that we must control

$$\binom{n}{2} = \frac{n(n-1)}{2},$$

inner products.

**Main idea:** *We shall look at structures that significantly reduce the number of distinct inner products we must control.*
The Goal

- We would like to devise a *systematic* way of designing low coherence frames
  - as a result, we will come up with many new instances of optimal frames

The challenge in designing low coherence frames is that we must control

\[
\binom{n}{2} = \frac{n(n-1)}{2},
\]

inner products.

**Main idea:** *We shall look at structures that significantly reduce the number of distinct inner products we must control.*

Equiangular frames have only a "single" norm of the inner product.
In 1968 Slepian published the paper, “Group codes for the Gaussian channel”. From the abstract:

“A class of codes for use on the Gaussian channel, called group codes, is defined and investigated. Roughly speaking, all words in a group code are on an equal footing: each has the same error probability and the same disposition of neighbors....Some theorems on distances between words in group codes are demonstrated. The difficult problem of finding group codes with largest nearest neighbor is discussed in some detail.”
Group Structure

Let $G = \{G_1, G_2, \ldots, G_n\}$ be a finite group of $m \times m$ unitary matrices, such that $G_1 = I_m$. 

Choose a unit norm vector $v \in \mathbb{C}^m$ and choose the frame as $M = \begin{bmatrix} G_1 & G_2 & \cdots & G_n \end{bmatrix}$. Note that $v^* i v j = v^* G^{-1} i G^* j v = v^* G_k v$, thus, the number of inner products has gone from $n(n-1)/2$ to $n-1$. 

Babak Hassibi (Caltech)  Frames and Spherical Codes  UCSD, October 30 2013  17 / 62
Let $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ be a finite group of $m \times m$ unitary matrices, such that $G_1 = I_m$.

- any finite group can be *represented* as a set of unitary matrices
Group Structure

Let \( G = \{G_1, G_2, \ldots, G_n\} \) be a finite group of \( m \times m \) unitary matrices, such that \( G_1 = I_m \).

- any finite group can be represented as a set of unitary matrices
- Choose a unit norm vector \( v \in \mathbb{C}^m \) and choose the frame as

\[
M = \begin{bmatrix}
G_1 v & G_2 v & \ldots & G_n v
\end{bmatrix}.
\]
Group Structure

- Let $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ be a finite group of $m \times m$ unitary matrices, such that $G_1 = I_m$.
  - any finite group can be represented as a set of unitary matrices
- Choose a unit norm vector $v \in \mathbb{C}^m$ and choose the frame as
  $$M = \begin{bmatrix} G_1 v & G_2 v & \ldots & G_n v \end{bmatrix}.$$  
  Note that
  $$v_i^* v_j = v^* G_i^{-1} G_j v = v^* G_k v,$$
Group Structure

Let $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ be a finite group of $m \times m$ unitary matrices, such that $G_1 = I_m$.

- any finite group can be represented as a set of unitary matrices

Choose a unit norm vector $v \in \mathbb{C}^m$ and choose the frame as

$$M = \begin{bmatrix} G_1 v & G_2 v & \ldots & G_n v \end{bmatrix}.$$ 

Note that

$$v_i^* v_j = v^* \underbrace{G_i^* G_j v}_{G_k} = v^* G_k v,$$

thus, the number of inner products has gone from $\frac{n(n-1)}{2}$ to $n - 1$.
What Groups to Choose?

- A natural question is what groups to choose
What Groups to Choose?

- A natural question is what groups to choose
  - rather tough, too many groups out there
What Groups to Choose?

- A natural question is what groups to choose
  - rather tough, too many groups out there
  - in fact, to quote from the conclusion of Slepian’s paper: “...The development of this subject is clearly incomplete: we have raised more questions than we have answered....one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance....There is a great abundance of groups of arbitrarily large order that can be examined from the point of generating group codes...”
A natural question is what groups to choose

- rather tough, too many groups out there
- in fact, to quote from the conclusion of Slepian’s paper: “...The development of this subject is clearly incomplete: we have raised more questions than we have answered....one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance....There is a great abundance of groups of arbitrarily large order that can be examined from the point of generating group codes...”
- as a result, there has been scant progress, few follow-up papers (Blake 1972, Biglieri and Elia 1972, Ingmarsson 1989, Rossin and Heegard 1995) and no explicit constructions
A natural question is what groups to choose

- rather tough, too many groups out there
- in fact, to quote from the conclusion of Slepian’s paper: “...The development of this subject is clearly incomplete: we have raised more questions than we have answered....one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance....There is a great abundance of groups of arbitrarily large order that can be examined from the point of generating group codes...”
- as a result, there has been scant progress, few follow-up papers (Blake 1972, Biglieri and Elia 1972, Ingmarsson 1989, Rossin and Heegard 1995) and no explicit constructions

The easiest groups to consider are Abelian
A natural question is what groups to choose

- rather tough, too many groups out there
- in fact, to quote from the conclusion of Slepian’s paper: “…The development of this subject is clearly incomplete: we have raised more questions than we have answered….one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance….There is a great abundance of groups of arbitrarily large order that can be examined from the point of generating group codes…”
- as a result, there has been scant progress, few follow-up papers (Blake 1972, Biglieri and Elia 1972, Ingmarsson 1989, Rossin and Heegard 1995) and no explicit constructions

The easiest groups to consider are Abelian

- every Abelian group is the direct sum of a collection of cyclic groups (of prime power order)
What Groups to Choose?

A natural question is what groups to choose

- rather tough, too many groups out there
- in fact, to quote from the conclusion of Slepian’s paper: “…The development of this subject is clearly incomplete: we have raised more questions than we have answered….one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance….There is a great abundance of groups of arbitrarily large order that can be examined from the point of generating group codes…”
- as a result, there has been scant progress, few follow-up papers (Blake 1972, Biglieri and Elia 1972, Ingmarsson 1989, Rossin and Heegard 1995) and no explicit constructions

The easiest groups to consider are Abelian

- every Abelian group is the direct sum of a collection of cyclic groups (of prime power order)

Let’s therefore start with cyclic groups.
Cyclic Groups

A cyclic group of order $n$ has the simple 1-dimensional representation:

$$g_i = \omega^{k(i-1)}, \quad i = 1, \ldots, n, \quad \omega = e^{i\frac{2\pi}{n}}.$$

If one wants an $m$-dimensional representation then, since the group is Abelian and all matrices can be jointly diagonalized,

$$G_i = \begin{bmatrix} \omega^{k_1(i-1)} & & \\ & \omega^{k_2(i-1)} & \\ & & \ddots \\ & & & \omega^{k_m(i-1)} \end{bmatrix}, \quad i = 1, \ldots, n$$
Cyclic Groups

If we now take
\[ v = [1 \ 1 \ \ldots \ 1]^T \]
we get

\[ M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \ldots & \omega^{k_1(n-1)} \\
1 & \omega^{k_2} & \ldots & \omega^{k_2(n-1)} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \ldots & \omega^{k_m(n-1)}
\end{bmatrix}, \quad \omega = e^{j \frac{2\pi}{n}} \]

for some integers \( \{k_1, \ldots, k_m\} \), which is simply a Harmonic frame. Furthermore,

\[ \mu = \max_{i=1 \ldots, n-1} \frac{1}{m} \left| \sum_{l=1}^{m} \omega^{k_l i} \right| . \]

This looks pretty boring........or is it?
Random Frame vs. Random Harmonic Frame

<table>
<thead>
<tr>
<th>((n, m))</th>
<th>Complex Gaussian</th>
<th>Random Fourier</th>
</tr>
</thead>
<tbody>
<tr>
<td>(251, 125)</td>
<td>.2677</td>
<td>.1996</td>
</tr>
<tr>
<td>(499, 166)</td>
<td>.3559</td>
<td>.1786</td>
</tr>
<tr>
<td>(499, 249)</td>
<td>.2226</td>
<td>.1736</td>
</tr>
<tr>
<td>(503, 251)</td>
<td>.2137</td>
<td>.1533</td>
</tr>
<tr>
<td>(521, 260)</td>
<td>.2208</td>
<td>.1504</td>
</tr>
<tr>
<td>(521, 130)</td>
<td>.3065</td>
<td>.2376</td>
</tr>
<tr>
<td>(643, 321)</td>
<td>.2034</td>
<td>.1627</td>
</tr>
<tr>
<td>(643, 214)</td>
<td>.2274</td>
<td>.1978</td>
</tr>
<tr>
<td>(701, 175)</td>
<td>.2653</td>
<td>.2316</td>
</tr>
<tr>
<td>(701, 350)</td>
<td>.1788</td>
<td>.1326</td>
</tr>
<tr>
<td>(1009, 504)</td>
<td>.1565</td>
<td>.1147</td>
</tr>
<tr>
<td>(1009, 336)</td>
<td>.2086</td>
<td>.1384</td>
</tr>
<tr>
<td>(1009, 252)</td>
<td>.2287</td>
<td>.1631</td>
</tr>
</tbody>
</table>
How to Choose the Frequencies $k_i$?

Recall that we have the following $n - 1$ inner products

$$c_l = \frac{1}{m} \sum_{i=1}^{m} \omega^{k_i l}, \quad l = 1, \ldots, n - 1$$
How to Choose the Frequencies $k_i$?

Recall that we have the following $n - 1$ inner products

$$c_l = \frac{1}{m} \sum_{i=1}^{m} \omega^{k_i l}, \quad l = 1, \ldots, n - 1$$

Thus,

$$|c_l|^2 = \frac{1}{m^2} \left( \sum_{i=1}^{m} \omega^{k_i l} \right) \left( \sum_{j=1}^{m} \omega^{k_j l} \right)^* = \frac{1}{m^2} \sum_{i=1}^{m} \sum_{j=1}^{m} \omega^{(k_i - k_j)l} = \frac{1}{m^2} \sum_{k=0}^{n-1} a_k \omega^{k l}$$

where

$$a_k = |\{(k_i, k_j)|k_i - k_j = k \mod (n)\}|.$$
How to Choose the Frequencies $k_i$?

Recall that we have the following $n - 1$ inner products

$$c_l = \frac{1}{m} \sum_{i=1}^{m} \omega^{k_i l}, \quad l = 1, \ldots n - 1$$

Thus,

$$|c_l|^2 = \frac{1}{m^2} \left( \sum_{i=1}^{m} \omega^{k_i l} \right) \left( \sum_{j=1}^{m} \omega^{k_j l} \right)^* = \frac{1}{m^2} \sum_{i=1}^{m} \sum_{j=1}^{m} \omega^{(k_i - k_j)l} = \frac{1}{m^2} \sum_{k=0}^{n-1} a_k \omega^{kl}$$

where

$$a_k = |\{(k_i, k_j)|k_i - k_j = k \mod (n)\}|.$$ 

Thus, $|c_l|^2$ and $a_k$ are Fourier pairs.
How to Choose the Frequencies $k_i$?

For an equiangular frame, we have

$$|c_0|^2 = 1 \quad \text{and} \quad |c_l|^2 = c, \quad l = 1, \ldots, n - 1.$$ 

Thus,

$$a_0 = m \quad \text{and} \quad a_k = a, \quad k = 1, \ldots, n - 1.$$
How to Choose the Frequencies $k_i$?

For an equiangular frame, we have

$$|c_0|^2 = 1 \quad \text{and} \quad |c_l|^2 = c, \quad l = 1, \ldots, n - 1.$$

Thus,

$$a_0 = m \quad \text{and} \quad a_k = a, \quad k = 1, \ldots, n - 1.$$

But this means the frequencies $\{k_i\}$ must form a **difference set**.
How to Choose the Frequencies $k_i$?

For an equiangular frame, we have

$$|c_0|^2 = 1 \quad \text{and} \quad |c_l|^2 = c, \quad l = 1, \ldots, n - 1.$$ 

Thus,

$$a_0 = m \quad \text{and} \quad a_k = a, \quad k = 1, \ldots, n - 1.$$ 

But this means the frequencies $\{k_i\}$ must form a difference set:

- $\{k_i\} \subset \{0, 1, \ldots, n - 1\}$
- Each number $k \in \{1, \ldots, n - 1\}$ occurs as a difference $k_i - k_j \mod n$ the same number of times.
Example: For \( n = 7 \), \( \{1, 2, 4\} \) is a difference set.
Example: For $n = 7$, $\{1, 2, 4\}$ is a difference set

- Each of $1, \ldots, 6$ occurs as a difference just once:
  - $1 - 2 \equiv 6 \mod 7$
  - $1 - 4 \equiv 4$
  - $2 - 1 \equiv 1$
  - $2 - 4 \equiv 5$
  - $4 - 1 \equiv 3$
  - $4 - 2 \equiv 2$

Theorem (Xia, Zho and Giannakis (2005))

A harmonic frame is equiangular if and only if the integers $\{k_i\}$ form a difference set in $\{0, 1, \ldots, n-1\}$. 
Difference Sets and Harmonic Frames

Example: For $n = 7$, $\{1, 2, 4\}$ is a difference set

- Each of 1, ..., 6 occurs as a difference just once:
  - $1 - 2 \equiv 6 \mod 7$
  - $1 - 4 \equiv 4$
  - $2 - 1 \equiv 1$
  - $2 - 4 \equiv 5$
  - $4 - 1 \equiv 3$
  - $4 - 2 \equiv 2$

Theorem (Xia, Zho and Giannakis (2005))

A harmonic frame is equiangular if and only if the integers $\{k_i\}$ form a difference set in $\{0, 1, ..., n - 1\}$. 
Difference Sets

Unfortunately, the known difference sets are few and far between

- Singer difference sets
- Quadratic residue difference sets
- Quartic residue difference sets
- Octic difference sets
- Twin-prime difference sets
Difference Sets

- Unfortunately, the known difference sets are few and far between
- There are 5 known families
Difference Sets

- Unfortunately, the known difference sets are few and far between.
- There are 5 known families:
  - Singer difference sets
  - quadratic residue difference sets
  - quartic residue difference sets
  - octic difference sets
  - twin-prime difference sets
Unfortunately, the known difference sets are few and far between.

There are 5 known families:
- Singer difference sets
- quadratic residue difference sets
- quartic residue difference sets
- octic difference sets
- twin-prime difference sets

We therefore need a different approach.
Choosing the $\{k_1, \ldots, k_m\}$

The key is how to choose $\{k_1, \ldots, k_m\}$. 
Choosing the $\{k_1, \ldots, k_m\}$

The key is how to choose $\{k_1, \ldots, k_m\}$.

- Let $n$ be a prime.
Choosing the $\{k_1, \ldots, k_m\}$

The key is how to choose $\{k_1, \ldots, k_m\}$.

- Let $n$ be a prime.
- Consider the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ consisting of all integers \(\{1, 2, \ldots, n - 1\}\).
Choosing the \( \{k_1, \ldots, k_m\} \)

The key is how to choose \( \{k_1, \ldots, k_m\} \).

- Let \( n \) be a prime.
- Consider the multiplicative group \((\mathbb{Z}/n\mathbb{Z})^\times\) consisting of all integers \(\{1, 2, \ldots, n-1\}\). This group has size \(n-1\) and choose an \(m\) such that \(m|n-1\).
Choosing the \( \{k_1, \ldots, k_m\} \)

The key is how to choose \( \{k_1, \ldots, k_m\} \).

- Let \( n \) be a prime.
- Consider the multiplicative group \((\mathbb{Z}/n\mathbb{Z})^\times\) consisting of all integers \(\{1, 2, \ldots, n-1\}\). This group has size \( n - 1 \) and choose an \( m \) such that \( m | n - 1 \).
- Choose \( \{k_1, k_2, \ldots, k_m\} \) to be a subgroup of \((\mathbb{Z}/n\mathbb{Z})^\times\) of size \( m \)
Choosing the \( \{k_1, \ldots, k_m\} \)

The key is how to choose \( \{k_1, \ldots, k_m\} \).

- Let \( n \) be a prime.
- Consider the multiplicative group \( (\mathbb{Z}/n\mathbb{Z})^\times \) consisting of all integers \( \{1, 2, \ldots, n-1\} \). This group has size \( n-1 \) and choose an \( m \) such that \( m|n-1 \).
- Choose \( \{k_1, k_2, \ldots, k_m\} \) to be a subgroup of \( (\mathbb{Z}/n\mathbb{Z})^\times \) of size \( m \).
  - this subgroup is cyclic and unique: choose an \( r \) such that \( m \) is the smallest integer for which \( r^m = 1 \mod(n) \), then

\[
\{k_1, k_2, \ldots, k_m\} = \{1, r, \ldots, r^{m-1}\}
\]
Choosing the \( \{k_1, \ldots, k_m\} \)

What is the point....?
Choosing the \( \{k_1, \ldots, k_m\} \)

What is the point....?

- Let us look at the columns of \( M \) one at a time:

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{2k_1} & \cdots & \omega^{(n-1)k_1} \\
1 & \omega^{k_2} & \omega^{2k_2} & \cdots & \omega^{(n-1)k_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{2k_m} & \cdots & \omega^{k_m(n-1)}
\end{bmatrix}, \quad \omega = e^{j \frac{2\pi}{n}}
\]
Choosing the \( \{k_1, \ldots, k_m\} \)

What is the point....?

- Let us look at the columns of \( M \) one at a time:

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{2k_1} & \ldots & \omega^{(n-1)k_1} \\
1 & \omega^{k_2} & \omega^{2k_2} & \ldots & \omega^{(n-1)k_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{2k_m} & \ldots & \omega^{k_m(n-1)} \\
\end{bmatrix}, \quad \omega = e^{j\frac{2\pi}{n}}
\]

- The first column has all zero exponents
Choosing the \( \{k_1, \ldots, k_m\} \)

What is the point?...

- Let us look at the columns of \( M \) one at a time:

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{2k_1} & \ldots & \omega^{(n-1)k_1} \\
1 & \omega^{k_2} & \omega^{2k_2} & \ldots & \omega^{(n-1)k_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{2k_m} & \ldots & \omega^{k_m(n-1)}
\end{bmatrix}, \quad \omega = e^{j\frac{2\pi}{n}}
\]

- The first column has all zero exponents
- The second column has exponents \( \{k_1, k_2, \ldots, k_m\} \)
Choosing the \( \{k_1, \ldots, k_m\} \)

What is the point....?

- Let us look at the columns of \( M \) one at a time:

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{2k_1} & \ldots & \omega^{(n-1)k_1} \\
1 & \omega^{k_2} & \omega^{2k_2} & \ldots & \omega^{(n-1)k_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{2k_m} & \ldots & \omega^{(n-1)k_m}
\end{bmatrix}, \quad \omega = e^{j\frac{2\pi}{n}}
\]

- The first column has all zero exponents
- The second column has exponents \( \{k_1, k_2, \ldots, k_m\} \)
- The third column has exponents \( \{2k_1, 2k_2, \ldots, 2k_m\} \)
Choosing the \( \{ k_1, \ldots, k_m \} \)

What is the point....?

- Let us look at the columns of \( M \) one at a time:

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{k_1} & \omega^{2k_1} & \ldots & \omega^{(n-1)k_1} \\
1 & \omega^{k_2} & \omega^{2k_2} & \ldots & \omega^{(n-1)k_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{k_m} & \omega^{2k_m} & \ldots & \omega^{k_m(n-1)}
\end{bmatrix}, \quad \omega = e^{j\frac{2\pi}{n}}
\]

- The first column has all zero exponents
- The second column has exponents \( \{ k_1, k_2, \ldots, k_m \} \)
- The third column has exponents \( \{ 2k_1, 2k_2, \ldots, 2k_m \} \)
  - but what is \( \{ 2k_1, 2k_2, \ldots, 2k_m \} \)?
But what is \( \{2k_1, 2k_2, \ldots, 2k_m\} \)?

If \( 2 \in \{k_1, k_2, \ldots, k_m\} \), then

\[
\{2k_1, 2k_2, \ldots, 2k_m\} = \{k_1, k_2, \ldots, k_m\}.
\]
But what is \( \{2k_1, 2k_2, \ldots, 2k_m\} \)?

If \( 2 \in \{k_1, k_2, \ldots, k_m\} \), then

\[
\{2k_1, 2k_2, \ldots, 2k_m\} = \{k_1, k_2, \ldots, k_m\}.
\]
But what is $\{2k_1, 2k_2, \ldots, 2k_m\}$?

If $2 \in \{k_1, k_2, \ldots, k_m\}$, then

$$\{2k_1, 2k_2, \ldots, 2k_m\} = \{k_1, k_2, \ldots, k_m\}. $$

But what if $2 \notin \{k_1, k_2, \ldots, k_m\}$?
But what is \( \{2k_1, 2k_2, \ldots, 2k_m\} \)\

If \( 2 \in \{k_1, k_2, \ldots, k_m\} \), then
\[
\{2k_1, 2k_2, \ldots, 2k_m\} = \{k_1, k_2, \ldots, k_m\}.
\]

But what if \( 2 \not\in \{k_1, k_2, \ldots, k_m\} \)?
then \( \{2k_1, 2k_2, \ldots, 2k_m\} \) is a coset of \( \{k_1, k_2, \ldots, k_m\} \)
The Construction

The same is true for every column $l = 2, \ldots, n - 1$: 
The Construction

The same is true for every column $l = 2, \ldots, n - 1$:

- If $l \in \{k_1, k_2, \ldots, k_m\}$, then

$$\{lk_1, lk_2, \ldots, lk_m\} = \{k_1, k_2, \ldots, k_m\}.$$
The Construction

The same is true for every column \( l = 2, \ldots, n - 1 \):

- If \( l \in \{k_1, k_2, \ldots, k_m\} \), then
  \[
  \{lk_1, lk_2, \ldots, lk_m\} = \{k_1, k_2, \ldots, k_m\}.
  \]

- If \( l \notin \{k_1, k_2, \ldots, k_m\} \), then
  \[
  \{lk_1, lk_2, \ldots, lk_m\} \text{ is a coset of } \{k_1, k_2, \ldots, k_m\}
  \]
The Construction

The same is true for every column $l = 2, \ldots, n - 1$:

- If $l \in \{k_1, k_2, \ldots, k_m\}$, then
  \[\{lk_1, lk_2, \ldots, lk_m\} = \{k_1, k_2, \ldots, k_m\}\].

- If $l \notin \{k_1, k_2, \ldots, k_m\}$, then
  \[\{lk_1, lk_2, \ldots, lk_m\}\] is a coset of $\{k_1, k_2, \ldots, k_m\}$.

But there are $\frac{n-1}{m}$ such cosets. Therefore

*The number of distinct inner products is reduced from $\frac{n(n-1)}{2}$ to $n - 1$ to $\frac{n-1}{m}$...*
How does this compare to randomly choosing frequencies?

<table>
<thead>
<tr>
<th>$(n, m)$</th>
<th>Complex Gaussian</th>
<th>Random Fourier</th>
<th>Group Matrix</th>
<th>$\sqrt{\frac{n-m}{m(n-1)}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(251, 125)</td>
<td>.2677</td>
<td>.1996</td>
<td>.0635</td>
<td>.0635</td>
</tr>
<tr>
<td>(499, 166)</td>
<td>.3559</td>
<td>.1786</td>
<td>.0888</td>
<td>.0635</td>
</tr>
<tr>
<td>(499, 249)</td>
<td>.2226</td>
<td>.1736</td>
<td>.0449</td>
<td>.0449</td>
</tr>
<tr>
<td>(503, 251)</td>
<td>.2137</td>
<td>.1533</td>
<td>.0447</td>
<td>.0447</td>
</tr>
<tr>
<td>(521, 260)</td>
<td>.2208</td>
<td>.1504</td>
<td>.0458</td>
<td>.0439</td>
</tr>
<tr>
<td>(521, 130)</td>
<td>.3065</td>
<td>.2376</td>
<td>.1175</td>
<td>.0761</td>
</tr>
<tr>
<td>(643, 321)</td>
<td>.2034</td>
<td>.1627</td>
<td>.0395</td>
<td>.0395</td>
</tr>
<tr>
<td>(643, 214)</td>
<td>.2274</td>
<td>.1978</td>
<td>.0755</td>
<td>.0559</td>
</tr>
<tr>
<td>(701, 175)</td>
<td>.2653</td>
<td>.2316</td>
<td>.0687</td>
<td>.0655</td>
</tr>
<tr>
<td>(701, 350)</td>
<td>.1788</td>
<td>.1326</td>
<td>.0393</td>
<td>.0379</td>
</tr>
<tr>
<td>(1009, 504)</td>
<td>.1565</td>
<td>.1147</td>
<td>.0325</td>
<td>.0315</td>
</tr>
</tbody>
</table>
Example: Finding Coherence when $r = 2$

- Can compute/bound coherence for different values of $r$.
- Often find tighter bounds than for general tight frames.
- Sometimes obtain tight, equiangular frames!

\[
\begin{align*}
\text{m even:} & \quad \mu = \sqrt{n - m - \frac{1}{2}m(n - 1)} + \frac{1}{2}m \\
\text{m odd:} & \quad \mu = \sqrt{n - m - \frac{1}{2}m(n - 1)}
\end{align*}
\]
Example: Finding Coherence when $r = 2$

- Can compute/bound coherence for different values of $r$.
- Often find tighter bounds than for general tight frames.
- Sometimes obtain tight, equiangular frames!

**Theorem ($r = 2$)**

- $m$ even: $\mu = \sqrt{\frac{n-m-\frac{1}{2}}{m(n-1)}} + \frac{1}{2m}$

- $m$ odd: $\mu = \sqrt{\frac{n-m}{m(n-1)}}$
  - Equiangular: Inner products have the same norm
  - $K$ is a difference set.
  - Achieve Welch Bound
Bounding the Coherence When $r = 3$
Bounding the Coherence When $r = 4$
Bounding the Coherence for General $r$

**Theorem (General $r$)**

$$\mu \leq \frac{1}{r} \left( (r - 1) \sqrt{\frac{1}{m} \left( r - \frac{1}{m} \right) + \frac{1}{m}} \right).$$
Bounding the Coherence for General $r$

**Theorem (General $r$)**

$$
\mu \leq \frac{1}{r} \left( (r - 1) \sqrt{\frac{1}{m} \left( r - \frac{1}{m} \right)} + \frac{1}{m} \right).
$$

**Theorem (General $r$, $m$ odd)**

*If $m$ is odd,*

$$
\mu \leq \frac{1}{r} \sqrt{\left( \frac{1}{m} + \left( \frac{r}{2} - 1 \right) \beta \right)^2 + \left( \frac{r}{2} \right)^2 \beta^2},
$$

*where $\beta = \sqrt{\frac{1}{m} \left( r + \frac{1}{m} \right)}$.***
Optimization over Cosets

- Let $n$ be a prime and let $m|n-1$ and $m'|m$ (set $d = \frac{m}{m'}$). Call the unique subgroup of size $m'$ of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ to be $K'$.
- The set of cosets of $K'$ in $G$ form the quotient group $G/K'$. We now construct a $m \times m$ unitary representation of $G$ as follows:
  - choose $d$ cosets of $K'$ in $G$: \{l_1 K', l_2 K', \ldots, l_d K'\}
  - for each $l_i$ define the $m' \times m'$ unitary matrix $D_{l_i} = \text{diag}(\eta_i^{l_i K'})$
    using the exponents in the coset $l_i K'$
  - represent the generator of $G$ as $U = \text{diag}(D_{l_1}, D_{l_2}, \ldots, D_{l_d})$

Optimizing over $m'$ and the cosets $l_i$ can sometimes result in even smaller coherences (note that our current construction is for $m = m'$).
Optimizing Coherence Over Cosets

- Randomly sample different coset choices ($\ell_1 K', ..., \ell_d K'$) for various values of $m'$.
- $n = 491$ and $m = 70$. 

![Graph showing lowest coherence observed for different values of $m'$]
Other Groups

- General Abelian groups can be considered
  - these are products of cyclic groups
  - frames are Kronecker products of the frames described
  - more flexibility in frame dimensions: $n$ need not be a prime
  - difficult to bound the coherence: lower bounded by the coherence associated to any cyclic subgroup
Other Groups

- General Abelian groups can be considered
  - these are products of cyclic groups
  - frames are Kronecker products of the frames described
  - more flexibility in frame dimensions: $n$ need not be a prime
  - difficult to bound the coherence: lower bounded by the coherence associated to any cyclic subgroup

- Need to look at non-Abelian groups
Generalized Dihedral Groups

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau \sigma \tau^{-1} = \sigma^r \rangle \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{D\mathbb{Z}} \]
Generalized Dihedral Groups

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau \sigma \tau^{-1} = \sigma^r \rangle \cong \frac{\mathbb{Z}}{n \mathbb{Z}} \times \frac{\mathbb{Z}}{D \mathbb{Z}} \]

- Nonabelian group of size \( Dn \)
Generalized Dihedral Groups

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau \sigma \tau^{-1} = \sigma^r \rangle \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{D\mathbb{Z}} \]

- Nonabelian group of size \( Dn \)
- Has an irreducible \( D \)-dimensional representation in the form

\[ \sigma \mapsto \mathbf{S} := \text{diag}(\omega, \omega^r, \ldots, \omega^{rD-1}), \]
\[ \tau \mapsto \mathbf{T} := \begin{bmatrix} 1 & \mathbf{I}_{D-1} \end{bmatrix}, \]

where \( \omega = e^{\frac{2\pi i}{n}} \).
Generalized Dihedral Groups (cont.)

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle \]

\[ S := \text{diag}(\omega, \omega^r, \ldots, \omega^{r^{D-1}}), \quad T := \begin{bmatrix} 1 & \mathbf{I}_{D-1} \end{bmatrix} \]

\[ K = \{ k_1, \ldots, k_m \} \text{ unique subgroup of size } m \text{ of } (\mathbb{Z}/n\mathbb{Z})^\times \]

\[ [\sigma] := \text{diag}(S^{k_1}, \ldots, S^{k_m}), \quad [\tau] := \text{diag}(T, \ldots, T) \]
Generalized Dihedral Groups (cont.)

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau \sigma \tau^{-1} = \sigma^r \rangle \]

\[ S := \text{diag}(\omega, \omega^r, \ldots, \omega^{r^{D-1}}), \quad T := \begin{bmatrix} I_{D-1} \\ \vdots \end{bmatrix} \]

\[ K = \{ k_1, \ldots, k_m \} \text{ unique subgroup of size } m \text{ of } (\mathbb{Z}/n\mathbb{Z})^\times \]

\[ [\sigma] := \text{diag}(S^{k_1}, \ldots, S^{k_m}), \quad [\tau] := \text{diag}(T, \ldots, T) \]

- Need to find \( \mathbf{v} \), and form

\[ \mathcal{M} = \ldots [\sigma]^a[\tau]^b\mathbf{v} \ldots \in \mathbb{C}^{Dm \times Dn}, \quad a = 0, \ldots, n-1 \quad b = 0, \ldots, D-1 \]
Generalized Dihedral Groups (cont.)

\[ G_{n,r} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^D = 1, \tau \sigma \tau^{-1} = \sigma^r \rangle \]

\[ \mathbf{S} := \text{diag}(\omega, \omega^r, \ldots, \omega^{r^{D-1}}), \quad \mathbf{T} := \begin{bmatrix} 1 & \mathbf{I}_{D-1} \end{bmatrix} \]

\[ K = \{ k_1, \ldots, k_m \} \] unique subgroup of size \( m \) of \((\mathbb{Z}/n\mathbb{Z})^\times\)

\[ [\sigma] := \text{diag}(\mathbf{S}^{k_1}, \ldots, \mathbf{S}^{k_m}), \quad [\tau] := \text{diag}(\mathbf{T}, \ldots, \mathbf{T}) \]

- Need to find \( \mathbf{v} \), and form

\[ \mathcal{M} = [\ldots [\sigma]^a[\tau]^b\mathbf{v} \ldots] \in \mathbb{C}^{Dm \times Dn}, \quad a = 0, \ldots, n-1 \quad b = 0, \ldots D-1 \]

- Choice of \( \mathbf{v} \) is tricky: “all-one vector” does not make the frame tight

(“....one outstanding problem is that of finding a tractable method of choosing the initial vector to maximize the nearest neighbor distance....” (Slepian 1968))
The dihedral frame is tight iff $v = \begin{bmatrix} w^T & \ldots & w^T \end{bmatrix}^T$ and $w = [w_1, \ldots, w_D]^T$ is a Zadoff-Chu sequence, i.e., one for which $w$ is orthogonal to its circular shifts.
Theorem

The dihedral frame is tight iff \( \mathbf{v} = [\mathbf{w}^T \ldots \mathbf{w}^T]^T \) and \( \mathbf{w} = [w_1, \ldots, w_D]^T \) is a Zadoff-Chu sequence, i.e., one for which \( w \) is orthogonal to its circular shifts.

The Zadoff-Chu sequence

\[
\begin{align*}
    w_d &= e^{\frac{i \pi d^2}{D}} \quad \text{if } D \text{ is even} \\
    w_d &= e^{\frac{i \pi d(d+1)}{D}} \quad \text{if } D \text{ is odd.}
\end{align*}
\]
The dihedral frame is tight iff $v = [w^T \ldots w^T]^T$ and $w = [w_1, \ldots, w_D]^T$ is a Zadoff-Chu sequence, i.e., one for which $w$ is orthogonal to its circular shifts.

The Zadoff-Chu sequence

$$w_d = e^{\frac{i\pi d^2}{D}} \text{ if } D \text{ is even}$$

$$w_d = e^{\frac{i\pi d(d+1)}{D}} \text{ if } D \text{ is odd}.$$
Dihedral Coherence

Figure: Coherences arising from dihedral representations for $r = \frac{n-1}{m} = 4$
This was rather unsatisfactory
Discussion

This was rather unsatisfactory

- we had to work hard and exploit the specific structure of the group
- we lucked out on finding a good $\mathbf{v}$
- do we have to do a new analysis for every different group?
Discussion

This was rather unsatisfactory

- we had to work hard and exploit the specific structure of the group
- we lucked out on finding a good $v$
- do we have to do a new analysis for every different group?

Or is there a better more natural way?
Representation Theory
Representation Theory

- $G$ a finite group, $|G| = n$
Fourier Transforms over Groups

Representation Theory

- $G$ a finite group, $|G| = n$
- a representation $\rho(\cdot)$ of $G$ is a homomorphism to $d \times d$ unitary matrices,
Fourier Transforms over Groups

Representation Theory

- \( G \) a finite group, \( |G| = n \)
- a representation \( \rho(\cdot) \) of \( G \) is a homomorphism to \( d \times d \) unitary matrices, i.e.,
  \[
  \rho(g_1)\rho(g_2) = \rho(g_1g_2).
  \]
Representation Theory

- $G$ a finite group, $|G| = n$
- a representation $\rho(\cdot)$ of $G$ is a homomorphism to $d \times d$ unitary matrices, i.e.,
  \[
  \rho(g_1)\rho(g_2) = \rho(g_1g_2).
  \]
- a representation is \textit{irreducible} if all of the matrices in the representation cannot be simultaneously block-diagonalized
Representation Theory

- $G$ a finite group, $|G| = n$
- a representation $\rho(\cdot)$ of $G$ is a homomorphism to $d \times d$ unitary matrices, i.e.,

$$\rho(g_1)\rho(g_2) = \rho(g_1g_2).$$

- a representation is **irreducible** if all of the matrices in the representation cannot be simultaneously block-diagonalized
- every finite group admits irreducible representations
Fourier Transforms over Groups

Representation Theory

- $G$ a finite group, $|G| = n$
- a representation $\rho(\cdot)$ of $G$ is a homomorphism to $d \times d$ unitary matrices, i.e.,
  \[ \rho(g_1)\rho(g_2) = \rho(g_1g_2). \]

- a representation is *irreducible* if all of the matrices in the representation cannot be simultaneously block-diagonalized
- every finite group admits irreducible representations
Let’s start by focusing on the Abelian case.
Fourier Transforms over Groups - The Abelian Case

Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
Fourier Transforms over Groups - The Abelian Case

Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
- **No.** All the irreducible representations are scalar.
Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
- **No.** All the irreducible representations are scalar.
- **Fact:** *The number of non-equivalent irreducible representations of an Abelian group is $n$*
Fourier Transforms over Groups - The Abelian Case

Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
- **No.** All the irreducible representations are scalar.
- **Fact:** The number of non-equivalent irreducible representations of an Abelian group is $n$
- Label these $\rho_0(\cdot), \ldots, \rho_{n-1}$
Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
- **No.** All the irreducible representations are scalar.
- **Fact:** The number of non-equivalent irreducible representations of an Abelian group is $n$
- Label these $\rho_0(\cdot), \ldots, \rho_{n-1}$
- **Example:** For the group of integers with addition mod $n$, we have

$$\rho_k(l) = e^{i2\pi kl}.$$
Fourier Transforms over Groups - The Abelian Case

Let’s start by focusing on the Abelian case

- Can an Abelian group have a $d \times d$ irreducible representation for $d > 1$?
- **No.** All the irreducible representations are scalar.
- **Fact:** The number of non-equivalent irreducible representations of an Abelian group is $n$
- Label these $\rho_0(\cdot), \ldots, \rho_{n-1}$
- **Example:** For the group of integers with addition mod $n$, we have
  \[ \rho_k(l) = e^{j2\pi kl}. \]
  The $\rho_i(\cdot)$ also form a group (the Pontryagin dual group)
  \[ \rho_i(g_1)\rho_j(g_1)\rho_i(g_2)\rho_j(g_2) = \rho_i(g_1)\rho_i(g_2)\rho_j(g_1)\rho_j(g_2) = \rho_i(g_1g_2)\rho_j(g_1g_2). \]
Using these facts, we can write down a square $n \times n$ matrix with $(k, l)$ entry $\rho_{k-1}(g_l)$.
Using these facts, we can write down a square $n \times n$ matrix with $(k, l)$ entry $\rho_{k-1}(g_l)$, i.e,

$$F_G = \frac{1}{\sqrt{n}} \begin{bmatrix}
\rho_0(g_1) & \rho_0(g_2) & \cdots & \rho_0(g_n) \\
\rho_1(g_1) & \rho_1(g_2) & \cdots & \rho_1(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \cdots & \rho_{n-1}(g_n)
\end{bmatrix}$$

Every column corresponds to a group element, and every row to an irreducible representation.
Fourier Transforms over Groups - The Abelian Case

Using these facts, we can write down a square $n \times n$ matrix with $(k, l)$ entry $\rho_{k-1}(g_l)$, i.e.,

$$\mathcal{F}_G = \frac{1}{\sqrt{n}} \begin{bmatrix}
\rho_0(g_1) & \rho_0(g_2) & \ldots & \rho_0(g_n) \\
\rho_1(g_1) & \rho_1(g_2) & \ldots & \rho_1(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \ldots & \rho_{n-1}(g_n)
\end{bmatrix}$$

Every column corresponds to a group element, and every row to an irreducible representation.

- Let’s call this a Fourier matrix
Fourier Transforms over Groups - The Abelian Case

Using these facts, we can write down a square $n \times n$ matrix with $(k, l)$ entry $\rho_{k-1}(g_l)$, i.e,

$$
F_G = \frac{1}{\sqrt{n}} \begin{bmatrix}
\rho_0(g_1) & \rho_0(g_2) & \ldots & \rho_0(g_n) \\
\rho_1(g_1) & \rho_1(g_2) & \ldots & \rho_1(g_n) \\
\vdots & \vdots & & \vdots \\
\rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \ldots & \rho_{n-1}(g_n)
\end{bmatrix}
$$

Every column corresponds to a group element, and every row to an irreducible representation.

- Let’s call this a Fourier matrix
- **Example:** For the group of integers with addition mod $n$, it is the usual Fourier matrix.
Some Properties

\[ \mathcal{F}_G = \frac{1}{\sqrt{n}} \begin{bmatrix} \rho_0(g_1) & \rho_0(g_2) & \ldots & \rho_0(g_n) \\ \rho_1(g_1) & \rho_1(g_2) & \ldots & \rho_1(g_n) \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \ldots & \rho_{n-1}(g_n) \end{bmatrix} \]

The rows and columns are orthonormal.
Some Properties

\[
\mathcal{F}_G = \frac{1}{\sqrt{n}} \begin{bmatrix}
\rho_0(g_1) & \rho_0(g_2) & \cdots & \rho_0(g_n) \\
\rho_1(g_1) & \rho_1(g_2) & \cdots & \rho_1(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \cdots & \rho_{n-1}(g_n)
\end{bmatrix}
\]

The rows and columns are orthonormal. Let's look at the inner product of the \( l_1 \) and \( l_2 \) columns

\[
\sum_{k=0}^{n-1} \rho_k(g_{l_1}) \rho_k(g_{l_2})^* = \sum_{k=0}^{n-1} \rho_k(g_{l_1}) (\rho_k(g_{l_2}))^{-1} = \sum_{k=0}^{n-1} \rho_k(g_{l_1}) \rho_k(g_{l_2}^{-1}) = \sum_{k=0}^{n-1} \rho_k(g_{l_1} g_{l_2}^{-1}) = S.
\]
Some Properties

\[ \mathcal{F}_G = \frac{1}{\sqrt{n}} \begin{bmatrix}
\rho_0(g_1) & \rho_0(g_2) & \cdots & \rho_0(g_n) \\
\rho_1(g_1) & \rho_1(g_2) & \cdots & \rho_1(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{n-1}(g_1) & \rho_{n-1}(g_2) & \cdots & \rho_{n-1}(g_n)
\end{bmatrix} \]

The rows and columns are orthonormal.

Let’s look at the inner product of the \( l_1 \) and \( l_2 \) columns

\[
\sum_{k=0}^{n-1} \rho_k(g_{l_1}) \rho_k(g_{l_2})^* = \sum_{k=0}^{n-1} \rho_k(g_{l_1})(\rho_k(g_{l_2}))^{-1} = \sum_{k=0}^{n-1} \rho_k(g_{l_1}) \rho_k(g_{l_2}^{-1})
\]

\[
= \sum_{k=0}^{n-1} \rho_k(g_{l_1} g_{l_2}^{-1}) = S.
\]

But

\[
\rho_{k'}(g) S = \sum_{k=0}^{n-1} \rho_{k'}(g) \rho_k(g) = \sum_{k=0}^{n-1} \rho_{k'k}(g) = S \implies S = 0.
\]
Thus, rather than frequencies, we can choose a set of irreducible representations \( \{ \rho_{k_1}(\cdot), \ldots, \rho_{k_m}(\cdot) \} \) to construct a frame

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
\rho_{k_1}(g_1) & \rho_{k_1}(g_2) & \cdots & \rho_{k_1}(g_n) \\
\rho_{k_2}(g_1) & \rho_{k_2}(g_2) & \cdots & \rho_{k_2}(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{k_m}(g_1) & \rho_{k_m}(g_2) & \cdots & \rho_{k_m}(g_n)
\end{bmatrix}
\]
Thus, rather than frequencies, we can choose a set of irreducible representations \( \{ \rho_{k_1}(\cdot), \ldots, \rho_{k_m}(\cdot) \} \) to construct a frame

\[
M = \frac{1}{\sqrt{m}} \begin{bmatrix}
\rho_{k_1}(g_1) & \rho_{k_1}(g_2) & \cdots & \rho_{k_1}(g_n) \\
\rho_{k_2}(g_1) & \rho_{k_2}(g_2) & \cdots & \rho_{k_2}(g_n) \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{k_m}(g_1) & \rho_{k_m}(g_2) & \cdots & \rho_{k_m}(g_n)
\end{bmatrix}
\]

Let us again look at the inner product of the \( l_1 \) and \( l_2 \) columns

\[
\sum_{i=1}^{m} \rho_{k_i}(g_{l_1}) \rho_{k_i}(g_{l_2})^* = \sum_{i=1}^{m} \rho_{k_i}(g_{l_1}^{-1} g_{l_2}^{-1}),
\]

so that there are again only \( n - 1 \) inner products (one for each non-identity group element).
The result of Xia, Zhou and Giannakis generalizes
The result of Xia, Zhou and Giannakis generalizes

- A set of representations \( \{ \rho_{k_1}(\cdot), \ldots, \rho_{k_m}(\cdot) \} \) is called a \textit{generalized difference set} if each representation \( \rho_k(\cdot) \in \{ \rho_0(\cdot), \ldots, \rho_{n-1}(\cdot) \} \) occurs as \( \rho_{k_i}(\cdot)\rho_{k_j}^{-1}(\cdot) \) the same number of times.
The result of Xia, Zhou and Giannakis generalizes

- A set of representations \( \{\rho_{k_1}(\cdot), \ldots, \rho_{k_m}(\cdot)\} \) is called a generalized difference set if each representation \( \rho_k(\cdot) \in \{\rho_0(\cdot), \ldots, \rho_{n-1}(\cdot)\} \)
occurs as \( \rho_{k_i}(\cdot)\rho_{k_j}^{-1}(\cdot) \) the same number of times

**Theorem**

A frame constructed from the representations \( \{\rho_{k_1}(\cdot), \ldots, \rho_{k_m}(\cdot)\} \) achieves the Welch bound iff it is a generalized difference set.
But What About Beyond Difference Sets?

Let's start with an example.

The group we considered earlier, \( \mathbb{Z} / n \mathbb{Z} \), for \( n = p \) a prime, is really the additive group of \( \text{GF}(p) \).

Can we do this with \( \text{GF}(p^k) \)?

Let \( \omega = e^{2\pi i/p} \).

For every \( a \in \text{GF}(p^k) \), there corresponds an irreducible representation \( \rho_a(x) = \omega \text{tr}(ax) \).

For \( x \in \text{GF}(p^k) \), \( \text{tr}(x) \) is the trace of \( x \) over \( \text{GF}(p^k) \):

\[
\text{tr}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{k-1}} \in \text{GF}(p).
\]

If one views \( \text{GF}(p^k) \) as a \( k \)-dimensional vector space over \( \text{GF}(p) \), then the field element \( x \) can be represented as a \( k \times k \) matrix with entries in \( \text{GF}(p) \).

\( \text{trace}(x) \) is the trace of this matrix and hence takes values in \( \text{GF}(p) \), the integers \( \{0, 1, \ldots, p-1\} \).
But What About Beyond Difference Sets?

Let’s start with an example.
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, \( \mathbb{Z}/n\mathbb{Z} \), for \( n = p \) a prime, is really the additive group of \( GF(p) \).
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, $\mathbb{Z}/n\mathbb{Z}$, for $n = p$ a prime, is really the additive group of $GF(p)$.

- **Can we do this with $GF(p^k)$?**
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, \( \mathbb{Z}/n\mathbb{Z} \), for \( n = p \) a prime, is really the additive group of \( GF(p) \).

- **Can we do this with** \( GF(p^k) \)?
  - Let \( \omega = e^{\frac{2\pi i}{p}} \)
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, $\mathbb{Z}/n\mathbb{Z}$, for $n = p$ a prime, is really the additive group of $GF(p)$.

- Can we do this with $GF(p^k)$?

  - Let $\omega = e^{\frac{2\pi i}{p}}$
  - For every $a \in GF(p^k)$, there corresponds an irreducible representation

$$\rho_a(x) = \omega^{\text{tr}(ax)}$$
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, $\mathbb{Z}/n\mathbb{Z}$, for $n = p$ a prime, is really the additive group of $GF(p)$.

- **Can we do this with $GF(p^k)$?**
  - Let $\omega = e^{2\pi i / p}$
  - For every $a \in GF(p^k)$, there corresponds an irreducible representation
    \[ \rho_a(x) = \omega^{\text{tr}(ax)} \]
  - For $x \in GF(p^k)$, $\text{tr}(x)$ is the *trace* of $x$ over $GF(p)$:
    \[ \text{tr}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{k-1}} \in GF(p) \]
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, $\mathbb{Z}/n\mathbb{Z}$, for $n = p$ a prime, is really the additive group of $GF(p)$.

Can we do this with $GF(p^k)$?

- Let $\omega = e^{\frac{2\pi i}{p}}$
- For every $a \in GF(p^k)$, there corresponds an irreducible representation
  $$\rho_a(x) = \omega^{\text{tr}(ax)}$$

- For $x \in GF(p^k)$, $\text{tr}(x)$ is the trace of $x$ over $GF(p)$:
  $$\text{tr}(x) = x + x^p + x^{p^2} + ... + x^{p^{k-1}} \in GF(p)$$

- If one views $GF(p^k)$ as a $k$-dimensional vector space over $GF(p)$, then the field element $x$ can be represented as a $k \times k$ matrix with entries in $GF(p)$. 

Babak Hassibi (Caltech) Frames and Spherical Codes UCSD, October 30 2013 49 / 62
But What About Beyond Difference Sets?

Let’s start with an example. The group we considered earlier, \( \mathbb{Z}/n\mathbb{Z} \), for \( n = p \) a prime, is really the additive group of \( GF(p) \).

**Can we do this with \( GF(p^k) \)?**

- Let \( \omega = e^{\frac{2\pi i}{p}} \)
- For every \( a \in GF(p^k) \), there corresponds an irreducible representation

\[
\rho_a(x) = \omega^{\text{tr}(ax)}
\]

- For \( x \in GF(p^k) \), \( \text{tr}(x) \) is the *trace* of \( x \) over \( GF(p) \):

\[
\text{tr}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{k-1}} \in GF(p)
\]

- If one views \( GF(p^k) \) as a \( k \)-dimensional vector space over \( GF(p) \), then the field element \( x \) can be represented as a \( k \times k \) matrix with entries in \( GF(p) \). \( \text{trace}(x) \) is the trace of this matrix and hence takes values in \( GF(p) \), the integers \( \{0, 1, \ldots, p - 1\} \).
Frames from $GF(p^k)$

We get a new matrix:

$$\omega = e^{\frac{2\pi i}{p}}$$

$$\mathcal{M} = \frac{1}{\sqrt{m}} \begin{bmatrix} 1 & \omega \text{tr}(k_1 \cdot \alpha_1) & \omega \text{tr}(k_1 \cdot \alpha_2) & \ldots & \omega \text{tr}(k_1 \cdot \alpha_{p^k-1}) \\ 1 & \omega \text{tr}(k_2 \cdot \alpha_1) & \omega \text{tr}(k_2 \cdot \alpha_2) & \ldots & \omega \text{tr}(k_2 \cdot \alpha_{p^k-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega \text{tr}(k_m \cdot \alpha_1) & \omega \text{tr}(k_m \cdot \alpha_2) & \ldots & \omega \text{tr}(k_m \cdot \alpha_{p^k-1}) \end{bmatrix}$$

- $GF(p^k) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{p^k-1}\}$

$\omega$ is now an element of $GF(p^k)$.

Still a tight frame

If $p = 2$, all entries are $\pm 1 \Rightarrow$ rows of Hadamard matrix

How do we choose the $k_i$?
Frames from $GF(p^k)$

We get a new matrix:

$$\omega = e^{\frac{2\pi i}{p}}$$

$$\mathcal{M} = \frac{1}{\sqrt{m}}\begin{bmatrix}
1 & \omega^\text{tr}(k_1 \cdot \alpha_1) & \omega^\text{tr}(k_1 \cdot \alpha_2) & \ldots & \omega^\text{tr}(k_1 \cdot \alpha_{p^k-1}) \\
1 & \omega^\text{tr}(k_2 \cdot \alpha_1) & \omega^\text{tr}(k_2 \cdot \alpha_2) & \ldots & \omega^\text{tr}(k_2 \cdot \alpha_{p^k-1}) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^\text{tr}(k_m \cdot \alpha_1) & \omega^\text{tr}(k_m \cdot \alpha_2) & \ldots & \omega^\text{tr}(k_m \cdot \alpha_{p^k-1})
\end{bmatrix}$$

- $GF(p^k) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{p^k-1}\}$
- The $i^{th}$ row corresponds to the representation $\rho_{k_i}(x) = \omega^\text{tr}(k_i x)$.
  - $k_i$ is now an element of $GF(p^k)$. 
Frames from $GF(p^k)$

We get a new matrix:

$$
\omega = e^{\frac{2\pi i}{p}}
$$

$$
\mathcal{M} = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega \text{tr}(k_1 \cdot \alpha_1) & \omega \text{tr}(k_1 \cdot \alpha_2) & \cdots & \omega \text{tr}(k_1 \cdot \alpha_{p^k-1}) \\
1 & \omega \text{tr}(k_2 \cdot \alpha_1) & \omega \text{tr}(k_2 \cdot \alpha_2) & \cdots & \omega \text{tr}(k_2 \cdot \alpha_{p^k-1}) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega \text{tr}(k_m \cdot \alpha_1) & \omega \text{tr}(k_m \cdot \alpha_2) & \cdots & \omega \text{tr}(k_m \cdot \alpha_{p^k-1})
\end{bmatrix}
$$

- $GF(p^k) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{p^k-1}\}$
- The $i^{th}$ row corresponds to the representation $\rho_{k_i}(x) = \omega \text{tr}(k_i x)$.
  - $k_i$ is now an element of $GF(p^k)$.
- Still a tight frame
Frames from $GF(p^k)$

We get a new matrix:

$$\omega = e^{\frac{2\pi i}{p}}$$

$$\mathcal{M} = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^{\text{tr}(k_1 \cdot \alpha_1)} & \omega^{\text{tr}(k_1 \cdot \alpha_2)} & \cdots & \omega^{\text{tr}(k_1 \cdot \alpha_{p^k-1})} \\
1 & \omega^{\text{tr}(k_2 \cdot \alpha_1)} & \omega^{\text{tr}(k_2 \cdot \alpha_2)} & \cdots & \omega^{\text{tr}(k_2 \cdot \alpha_{p^k-1})} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{\text{tr}(k_m \cdot \alpha_1)} & \omega^{\text{tr}(k_m \cdot \alpha_2)} & \cdots & \omega^{\text{tr}(k_m \cdot \alpha_{p^k-1})}
\end{bmatrix}$$

- $GF(p^k) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{p^k-1}\}$
- The $i^{th}$ row corresponds to the representation $\rho_{k_i}(x) = \omega^{\text{tr}(k_i x)}$.
  - $k_i$ is now an element of $GF(p^k)$.
- Still a tight frame
- If $p = 2$, all entries are $\pm 1 \Rightarrow$ rows of Hadamard matrix
Frames from $GF(p^k)$

We get a new matrix:

$$
\omega = e^{\frac{2\pi i}{p}}
$$

$$
\mathcal{M} = \frac{1}{\sqrt{m}} \begin{bmatrix}
1 & \omega^\text{tr}(k_1 \cdot \alpha_1) & \omega^\text{tr}(k_1 \cdot \alpha_2) & \cdots & \omega^\text{tr}(k_1 \cdot \alpha_{p^k-1}) \\
1 & \omega^\text{tr}(k_2 \cdot \alpha_1) & \omega^\text{tr}(k_2 \cdot \alpha_2) & \cdots & \omega^\text{tr}(k_2 \cdot \alpha_{p^k-1}) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^\text{tr}(k_m \cdot \alpha_1) & \omega^\text{tr}(k_m \cdot \alpha_2) & \cdots & \omega^\text{tr}(k_m \cdot \alpha_{p^k-1})
\end{bmatrix}
$$

- $GF(p^k) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{p^k-1}\}$
- The $i^{th}$ row corresponds to the representation $\rho_{k_i}(x) = \omega^\text{tr}(k_i \cdot x)$.
  - $k_i$ is now an element of $GF(p^k)$.
- Still a tight frame
- If $p = 2$, all entries are $\pm 1 \Rightarrow$ rows of Hadamard matrix

**How do we choose the $k_i$?**
Frames from $GF(p^k)$

- The nonzero elements of $GF(p^k)$ form a group under multiplication
  - $GF(p^k)^\times$
  - Cyclic group
  - Size $p^k - 1$
Frames from $GF(p^k)$

- The nonzero elements of $GF(p^k)$ form a group under multiplication
  - $GF(p^k)^\times$
  - Cyclic group
  - Size $p^k - 1$

- Let $m$ divide $p^k - 1$. 
Frames from $GF(p^k)$

- The nonzero elements of $GF(p^k)$ form a group under multiplication
  - $GF(p^k)^\times$
  - Cyclic group
  - Size $p^k - 1$

- Let $m$ divide $p^k - 1$.

- $K = \{k_1, \ldots, k_m\} \Rightarrow$ unique subgroup of $GF(p^k)^\times$ of size $m$. 
Frames from $GF(p^k)$

- The nonzero elements of $GF(p^k)$ form a group under multiplication
  - $GF(p^k)^\times$
  - Cyclic group
  - Size $p^k - 1$

- Let $m$ divide $p^k - 1$.

- $K = \{k_1, ..., k_m\} \Rightarrow$ unique subgroup of $GF(p^k)^\times$ of size $m$.

- What do our inner products look like?
Frames from $GF(p^k)$

$$M = \frac{1}{\sqrt{m}} \begin{bmatrix} 1 & \omega \text{tr}(k_1 \cdot \alpha_1) & \omega \text{tr}(k_1 \cdot \alpha_2) & \ldots & \omega \text{tr}(k_1 \cdot \alpha_{p^k-1}) \\ 1 & \omega \text{tr}(k_2 \cdot \alpha_1) & \omega \text{tr}(k_2 \cdot \alpha_2) & \ldots & \omega \text{tr}(k_2 \cdot \alpha_{p^k-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega \text{tr}(k_m \cdot \alpha_1) & \omega \text{tr}(k_m \cdot \alpha_2) & \ldots & \omega \text{tr}(k_m \cdot \alpha_{p^k-1}) \end{bmatrix}$$

Our inner product between columns $\ell_1, \ell_2 \in GF(p^k)$ is:

$$\frac{1}{m} \left[ \omega \text{tr}(k_1 \cdot \ell_1) \quad \omega \text{tr}(k_2 \cdot \ell_1) \quad \ldots \quad \omega \text{tr}(k_m \cdot \ell_1) \right] \cdot \left[ \omega \text{tr}(k_1 \cdot \ell_2) \quad \omega \text{tr}(k_2 \cdot \ell_2) \quad \ldots \quad \omega \text{tr}(k_m \cdot \ell_2) \right] = \frac{1}{m} \sum_{i=1}^{m} \omega \text{tr}((\ell_2 - \ell_1) \cdot k_i).$$

Note: $\text{tr}(x_1) + \text{tr}(x_2) = \text{tr}(x_1 + x_2)$
Generalized FT Matrix

\[ \frac{1}{m} \sum_{i=1}^{m} \omega \text{tr}((\ell_2 - \ell_1) \cdot k_i) \]

- Set \( \ell := \ell_2 - \ell_1 \in GF(p^k) \).
- Inner products are:
  \[ c_\ell = \frac{1}{m} \sum_{i=1}^{m} \omega \text{tr}(\ell \cdot k_i) \]
- One inner product value per coset \( \ell K \)
- Number of inner products is \( r = \frac{p^k - 1}{m} \).
Choosing Hadamard Rows Randomly vs. Deterministically

Figure: \( n = 256, m = 85, r = \frac{n-1}{m} = 3 \)
Frames from $GF(p^k)$

Since $GF(p^k)$ is cyclic, the same results from the Harmonic case hold:

**Theorem (General $r$)**

\[
\mu \leq \frac{1}{r} \left( (r - 1) \sqrt{\frac{1}{m} \left( r - \frac{1}{m} \right)} + \frac{1}{m} \right).
\]

**Theorem (General $r$, $m$ odd)**

*If $m$ is odd,*

\[
\mu \leq \frac{1}{r} \sqrt{\left( \frac{1}{m} + \left( \frac{r}{2} - 1 \right) \beta \right)^2 + \left( \frac{r}{2} \right)^2 \beta^2},
\]

*where $\beta = \sqrt{\frac{1}{m} \left( r + \frac{1}{m} \right)}$.*
We can also get new tight, equiangular frames!

**Theorem \((r = 2)\)**

- \(m\) even: \(\mu = \sqrt{\frac{n-m-\frac{1}{2}}{m(n-1)}} + \frac{1}{2m}\)

- \(m\) odd: \(\mu = \sqrt{\frac{n-m}{m(n-1)}}\)
  - Equiangular \(\Rightarrow\) Achieve Welch Bound
  - \(K\) is a “generalized” difference set.
What About Non-Abelian Groups?

- $G$ a finite group, $|G| = n$

$\sqrt{d_i} \text{vec}(\rho_i(g))$
What About Non-Abelian Groups?

- $G$ a finite group, $|G| = n$
- The irreducible representations $\rho_i(\cdot)$ can be $d_i \times d_i$ unitary matrices with different values of $d_i$
What About Non-Abelian Groups?

- $G$ a finite group, $|G| = n$
- The irreducible representations $\rho_i(\cdot)$ can be $d_i \times d_i$ unitary matrices with different values of $d_i$
- **Fact**: Let there be $s$ nonequivalent irreducible representations, each with dimension $d_i$. Then

$$\sum_{i=1}^{s} d_i^2 = n.$$
What About Non-Abelian Groups?

- $G$ a finite group, $|G| = n$
- The irreducible representations $\rho_i(\cdot)$ can be $d_i \times d_i$ unitary matrices with different values of $d_i$
- **Fact:** Let there be $s$ nonequivalent irreducible representations, each with dimension $d_i$. Then
  \[ \sum_{i=1}^{s} d_i^2 = n. \]

- This is perfect for making a square $n \times n$ matrix!

\[ \mathcal{F} = \frac{1}{\sqrt{n}} \begin{bmatrix} \sqrt{d_1} \text{vec}(\rho_1(g_1)) & \sqrt{d_1} \text{vec}(\rho_1(g_2)) & \ldots & \sqrt{d_1} \text{vec}(\rho_1(g_n)) \\ \sqrt{d_2} \text{vec}(\rho_2(g_1)) & \sqrt{d_2} \text{vec}(\rho_2(g_2)) & \ldots & \sqrt{d_2} \text{vec}(\rho_2(g_n)) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{d_s} \text{vec}(\rho_s(g_1)) & \sqrt{d_s} \text{vec}(\rho_s(g_2)) & \ldots & \sqrt{d_s} \text{vec}(\rho_s(g_n)) \end{bmatrix} \]
What About Non-Abelian Groups?

- $G$ a finite group, $|G| = n$
- The irreducible representations $\rho_i(\cdot)$ can be $d_i \times d_i$ unitary matrices with different values of $d_i$
- **Fact:** Let there be $s$ nonequivalent irreducible representations, each with dimension $d_i$. Then
  \[
  \sum_{i=1}^{s} d_i^2 = n.
  \]
  This is perfect for making a square $n \times n$ matrix!

- $F = \frac{1}{\sqrt{n}} \begin{bmatrix}
  \sqrt{d_1} \text{vec}(\rho_1(g_1)) & \sqrt{d_1} \text{vec}(\rho_1(g_2)) & \cdots & \sqrt{d_1} \text{vec}(\rho_1(g_n)) \\
  \sqrt{d_2} \text{vec}(\rho_2(g_1)) & \sqrt{d_2} \text{vec}(\rho_2(g_2)) & \cdots & \sqrt{d_2} \text{vec}(\rho_2(g_n)) \\
  \vdots & \vdots & \ddots & \vdots \\
  \sqrt{d_s} \text{vec}(\rho_s(g_1)) & \sqrt{d_s} \text{vec}(\rho_s(g_2)) & \cdots & \sqrt{d_s} \text{vec}(\rho_s(g_n))
\end{bmatrix}$

- $F$ is unitary. We will call it a Fourier matrix.
Frames from NonAbelian Groups

- To get a tight frame, we will choose subset of the irreducible representations (block rows)

\[
\begin{bmatrix}
\sqrt{d_1} \text{vec}(\rho_1(g_1)) & \sqrt{d_1} \text{vec}(\rho_1(g_2)) & \ldots & \sqrt{d_1} \text{vec}(\rho_1(g_n)) \\
\sqrt{d_2} \text{vec}(\rho_2(g_1)) & \sqrt{d_2} \text{vec}(\rho_2(g_2)) & \ldots & \sqrt{d_2} \text{vec}(\rho_2(g_n)) \\
\vdots & \vdots & \ddots & \vdots \\
\sqrt{d_k} \text{vec}(\rho_k(g_1)) & \sqrt{d_k} \text{vec}(\rho_k(g_2)) & \ldots & \sqrt{d_k} \text{vec}(\rho_k(g_n))
\end{bmatrix}
\]

- What is the inner product between columns \(i\) and \(j\)?

\[
\sum_{t=1}^{k} d_t \text{vec}(\rho_t(g_i)) \ast \text{vec}(\rho_t(g_j)) = \sum_{t=1}^{k} d_t \text{trace} \rho_t(g_i) \ast \rho_t(g_j) = \sum_{t=1}^{k} d_t \chi_t(g_{i-1} g_{j-1}) \chi_t(g) = \text{trace} \rho_t(g)
\]

\(\chi_t\) are the characters of \(G\). (Well-studied)
To get a tight frame, we will choose subset of the irreducible representations (block rows)

$$
\begin{bmatrix}
\sqrt{d_1} \text{vec}(\rho_1(g_1)) & \sqrt{d_1} \text{vec}(\rho_1(g_2)) & \ldots & \sqrt{d_1} \text{vec}(\rho_1(g_n)) \\
\sqrt{d_2} \text{vec}(\rho_2(g_1)) & \sqrt{d_2} \text{vec}(\rho_2(g_2)) & \ldots & \sqrt{d_2} \text{vec}(\rho_2(g_n)) \\
\vdots & \vdots & \ddots & \vdots \\
\sqrt{d_k} \text{vec}(\rho_k(g_1)) & \sqrt{d_k} \text{vec}(\rho_k(g_2)) & \ldots & \sqrt{d_k} \text{vec}(\rho_k(g_n))
\end{bmatrix}
$$

What is the inner product between columns $i$ and $j$?

$$
\sum_{t=1}^{k} d_t \text{vec}(\rho_t(g_i))^* \text{vec}(\rho_t(g_j)) = \sum_{t=1}^{k} d_t \text{trace} \rho_t(g_i)^* \rho_t(g_j)
$$

$$
= \sum_{t=1}^{k} d_t \text{trace} \rho_t(g_i^{-1} g_j) = \sum_{t=1}^{k} d_t \chi_t(g_i^{-1} g_j)
$$
Frames from NonAbelian Groups

To get a tight frame, we will choose subset of the irreducible representations (block rows)

\[
\begin{bmatrix}
\sqrt{d_1} \text{vec}(\rho_1(g_1)) & \sqrt{d_1} \text{vec}(\rho_1(g_2)) & \ldots & \sqrt{d_1} \text{vec}(\rho_1(g_n)) \\
\sqrt{d_2} \text{vec}(\rho_2(g_1)) & \sqrt{d_2} \text{vec}(\rho_2(g_2)) & \ldots & \sqrt{d_2} \text{vec}(\rho_2(g_n)) \\
\vdots & \vdots & \ddots & \vdots \\
\sqrt{d_k} \text{vec}(\rho_k(g_1)) & \sqrt{d_k} \text{vec}(\rho_k(g_2)) & \ldots & \sqrt{d_k} \text{vec}(\rho_k(g_n))
\end{bmatrix}
\]

What is the inner product between columns \(i\) and \(j\)?

\[
\sum_{t=1}^{k} d_t \text{vec}(\rho_t(g_i))^* \text{vec}(\rho_t(g_j)) = \sum_{t=1}^{k} d_t \text{trace} \rho_t(g_i)^* \rho_t(g_j)
\]

\[
= \sum_{t=1}^{k} d_t \text{trace} \rho_t(g_i^{-1} g_j) = \sum_{t=1}^{k} d_t \chi_t(g_i^{-1} g_j)
\]

\(\chi_t(g) = \text{trace} \rho_t(g)\) are the characters of \(G\). (Well-studied)
Character Table for $SL_2(q)$, $q$ even

<table>
<thead>
<tr>
<th>Class Representative:</th>
<th>$\begin{bmatrix} 1 &amp; 0 \ 0 &amp; 1 \end{bmatrix}$</th>
<th>$\begin{bmatrix} 1 &amp; 1 \ 0 &amp; 1 \end{bmatrix}$</th>
<th>$\begin{bmatrix} a &amp; 0 \ 0 &amp; a^{-1} \end{bmatrix}$</th>
<th>$B \begin{bmatrix} s &amp; 0 \ 0 &amp; s^{-1} \end{bmatrix} B^{-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of such classes:</td>
<td>1</td>
<td>1</td>
<td>$\frac{1}{2}(q-2)$</td>
<td>$\frac{1}{2}q$</td>
</tr>
<tr>
<td>Size of class:</td>
<td>1</td>
<td>$q^2-1$</td>
<td>$q(q+1)$</td>
<td>$q(q-1)$</td>
</tr>
<tr>
<td>$1_G$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$St_G$</td>
<td>$q$</td>
<td>0</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>$\rho_\chi$</td>
<td>$q+1$</td>
<td>1</td>
<td>$\chi(a) + \chi(a^{-1})$</td>
<td>0</td>
</tr>
<tr>
<td>$\pi_\eta$</td>
<td>$q-1$</td>
<td>$-1$</td>
<td>0</td>
<td>$-\eta(s) - \eta(s^{-1})$</td>
</tr>
</tbody>
</table>

- $a \in GF(q)^\times$
- $s \in GF(q^2)^\times$ such that $N(s) = s^{q+1} = 1$ (‘‘norm 1’’)
- $B \in SL_2(q^2)$ such that $B \begin{bmatrix} s & 0 \\ 0 & s^{-1} \end{bmatrix} B^{-1} \in SL_2(q)$
- $\chi$ a representation of $GF(q)^\times$
- $\eta$ a representation of the group of norm 1 elements
Choosing the Representations

We can now generalize the method of choosing the rows of our original Fourier matrix to form our harmonic frame.

- Let $\rho$ be an irreducible representation of a group $H$
- $G \leq Aut(H)$
- For any $g \in G$, $\rho_g(h) := \rho(gh)$ is an irreducible representation.
- $g' \in G$ acts on the set $\{\rho_g\}_{g \in G}$ as $g'\rho_g = \rho_{gg'}$.
- Similarly, $G$ acts on the corresponding characters as $g'\chi_g = \chi_{gg'}$. 
Choosing the Representations

- Let \( K = \{ k \in G \mid \chi(kh) = \chi(h), \forall h \in H \} \), the stabilizer of \( \chi \) under the \( G \)-action.
- Let \( A \leq G \) such that the set product \( KA \) is a group.
  - Equivalently, \( KA = AK \).
- We will require that \( A \cap K = 1 \).
- Choose the rows of the Generalized FT matrix corresponding to the representations \( \{ \rho_a \mid a \in A \} \).
Summary and Discussion

- Studied the construction of low coherence frames using Slepian’s approach
  - cyclic groups, harmonic frames, difference sets, choice of frequencies to reduce the distinct inner products from \( \frac{n(n-1)}{2} \) to \( \frac{n-1}{m} \)
  - dihedral groups, Zadoff-Chu sequences, hard to generalize to other non-Abelian groups, choice of initial vector complicated

- Claimed that more natural approach is to use Fourier transforms over groups
  - generalized difference sets, optimal frames from \( \text{GF}(p^k) \), key role of irreducible representations, no need for initial vector
  - generalization to non-Abelian groups, characters and character table play a key role
  - work is on-going
Summary and Discussion

- Studied the construction of low coherence frames using Slepian’s approach
  - cyclic groups, harmonic frames, difference sets, choice of frequencies to reduce the distinct inner products from $\frac{n(n-1)}{2}$ to $\frac{n-1}{m}$
  - dihedral groups, Zadoff-Chu sequences, hard to generalize to other non-Abelian groups, choice of initial vector complicated

- Claimed that more natural approach is to use Fourier transforms over groups
  - generalized difference sets, optimal frames from $GF(p^k)$, key role of irreducible representations, no need for initial vector
  - generalization to non-Abelian groups, characters and character table play a key role
  - work is ongoing

Cool math helps!