Algebraic Structures for Multi-Terminal Communications

Dinesh Krithivasan

University of Michigan

Advisor: Prof. Sandeep Pradhan
Presentation Outline

1. Distributed Source Coding - an Introduction
2. Distributed Source Coding - Discrete Sources
3. Distributed Source Coding - Gaussian Sources
4. Future Work
1. Distributed Source Coding - an Introduction
2. Distributed Source Coding - Discrete Sources
3. Distributed Source Coding - Gaussian Sources
4. Future Work
Distributed Source Coding

\[ f_1(\cdot) \quad R_1 \quad \hat{Y}_1^n \]

\[ f_2(\cdot) \quad R_2 \quad \hat{Y}_2^n \]

\[ \vdots \]

\[ f_K(\cdot) \quad R_K \quad \hat{Y}_L^n \]

\[ E(d_1(X^K_1, \hat{Y}_1)) \leq D_1 \]

\[ E(d_2(X^K_1, \hat{Y}_2)) \leq D_2 \]

\[ E(d_L(X^K_1, \hat{Y}_L)) \leq D_L \]
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
- Encoders $f_i : \mathcal{X}_i^n \rightarrow \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
- Encoders $f_i : X_i^n \rightarrow \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$
- Rate distortion region $\mathcal{RD}$ : set of achievable $(R_1, \ldots, R_K, D_1, \ldots D_L)$
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
- Encoders $f_i : \mathcal{X}_i^n \rightarrow \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$
- Rate distortion region $\mathcal{RD}$: set of achievable $(R_1, \ldots, R_K, D_1, \ldots D_L)$
- Goal: Characterize $\mathcal{RD}$ using single-letter information quantities
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
- Encoders $f_i : \mathcal{X}_i^n \rightarrow \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$
- Rate distortion region $\mathcal{RD}$: set of achievable $(R_1, \ldots, R_K, D_1, \ldots D_L)$
- Goal: Characterize $\mathcal{RD}$ using single-letter information quantities
  - Very hard to solve completely
Distributed Source Coding - Goal

- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time
- Encoders $f_i : \mathcal{X}_i^n \rightarrow \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$
- Rate distortion region $\mathcal{RD}$ : set of achievable $(R_1, \ldots, R_K, D_1, \ldots D_L)$
- Goal: Characterize $\mathcal{RD}$ using single-letter information quantities
  - Very hard to solve completely
  - Provide computable inner bounds
Single user case

\[ X_1^n \xrightarrow{f_1(\cdot)} R_1 \xrightarrow{Ed(X_1, \hat{Y}_1) \leq D_1} \hat{Y}_1^n \]
Single user case

\[ f_1(\cdot) \]

\[ R_1 \]

\[ Ed(X_1, \hat{Y}_1) \leq D_1 \]

- Solved completely by Shannon

\[ R_1 \geq \min_{p_{\hat{Y}_1|x_1} : \mathbb{E}d(X_1, \hat{Y}_1) \leq D_1} I(X_1; \hat{Y}_1) \]
Slepian-Wolf problem

- Lossless reconstruction of both sources
Slepian-Wolf problem

\[ X^n_1 \xrightarrow{f_1(\cdot)} R_1 \xrightarrow{Ed_H(X, \hat{Y}) \leq \epsilon} \hat{Y}^n_1 \]

\[ X^n_2 \xrightarrow{f_2(\cdot)} R_2 \xrightarrow{Ed_H(X, \hat{Y}) \leq \epsilon} \hat{Y}^n_2 \]

- Lossless reconstruction of both sources

\[ R_{SW} = \{(R_1, R_2) : R_1 \geq H(X|Y), R_2 \geq H(Y|X), R_1 + R_2 \geq H(X, Y)\} \]
Lossy reconstruction with decoder side information
Wyner-Ziv problem

- Code built over auxiliary random variable $U$
- Markov chain $U - X_1 - X_2$
Wyner-Ziv problem

Decoder computes $\hat{Y}_1 = G(U, X_2)$ that minimizes $Ed_1(X_1, \hat{Y}_1)$

$$R_1 \geq \min_{U \sim U | X_1, X_2} I(X_1; U | X_2)$$

$$Ed_1(X_1, G(U, X_2)) \leq D_1$$
Berger-Tung problem

\[ X_1^n \xrightarrow{f_1(\cdot)} R_1 \xrightarrow{Ed_1(X_1, \hat{Y}_1) \leq D_1} \hat{Y}_1^n \]

\[ f_2(\cdot) \]

\[ X_2^n \xrightarrow{f_2(\cdot)} R_2 \xrightarrow{Ed_2(X_2, \hat{Y}_2) \leq D_2} \hat{Y}_2^n \]

- Independent distortion criteria
Berger-Tung problem

- Codes built over auxiliary random variables $U, V$
- Markov chain $U - X_1 - X_2 - V$
Berger-Tung problem

\[ X^n_1 \quad \xrightarrow{f_1(\cdot)} \quad R_1 \quad \xrightarrow{\cdot} \quad Ed_1(X_1, \hat{Y}_1) \leq D_1 \]

\[ X^n_2 \quad \xrightarrow{f_2(\cdot)} \quad R_2 \quad \xrightarrow{\cdot} \quad Ed_2(X_2, \hat{Y}_2) \leq D_2 \]

- Inner bound:

\[ R_{BT} = \{(R_1, R_2, D_1, D_2) : R_1 \geq I(X_1; U | X_2), R_2 \geq I(X_2; V | X_1) \} \]

\[ R_1 + R_2 \geq I(X_1X_2; UV), D_1 \geq Ed_1(X_1, g_1(U, V)), D_2 \geq Ed_2(X_2, g_2(U, V)) \]
Berger-Tung problem

\[
X_1^n \xrightarrow{f_1(\cdot)} R_1 \xrightarrow{E_d_1(X_1, \hat{Y}_1) \leq D_1} \hat{Y}_1^n
\]

\[
X_2^n \xrightarrow{f_2(\cdot)} R_2 \xrightarrow{E_d_2(X_2, \hat{Y}_2) \leq D_2} \hat{Y}_2^n
\]

- Tightness of inner bound not known in general
Some observations

- Independent vector quantization followed by independent binning
Some observations

- Independent vector quantization followed by independent binning
- Decoder given excess information
Some observations

- Independent vector quantization followed by independent binning
- Decoder given excess information
  - Decoder given $U, V$
  - Decoder needs only the functions $g_1(U, V), g_2(U, V)$
Some observations

- Independent vector quantization followed by independent binning
- Decoder given excess information
  - Decoder given $U, V$
  - Decoder needs only the functions $g_1(U, V), g_2(U, V)$
- Rate gains possible?
Outline

1. Distributed Source Coding - an Introduction
2. Distributed Source Coding - Discrete Sources
3. Distributed Source Coding - Gaussian Sources
4. Future Work
A Distributed Source Coding Problem

Encoders observe different components of a vector source
A Distributed Source Coding Problem

- Centralized decoder - quantized observations from encoders
A Distributed Source Coding Problem

\[ \begin{align*}
X^n & \quad \rightarrow \quad \text{Encoder 1} \quad f_1(\cdot) \quad \rightarrow \quad R_1 \\
Y^n & \quad \rightarrow \quad \text{Encoder 2} \quad f_2(\cdot) \quad \rightarrow \quad R_2 \\
& \quad \rightarrow \quad \text{Decoder} \\
& \quad \rightarrow \quad \hat{Z}
\end{align*} \]

\[ Ed(X, Y, \hat{Z}) \leq D \]

- Joint distortion criterion to be minimized
A Distributed Source Coding Problem

Encoder 1
$f_1(\cdot)$

$X^n$

Encoder 2
$f_2(\cdot)$

$Y^n$

Decoder

$Ed(X, Y, \hat{Z}) \leq D$

$R_1$

$R_2$

Best known rate region - Berger-Tung based
Distortion $d(X, Y, \hat{Z})$ depends on sources and decoder reconstruction.
Joint Distortion Criterion

- Distortion $d(X, Y, \hat{Z})$ depends on sources and decoder reconstruction
- Special cases of such a distortion criterion:
Distortion $d(X, Y, \hat{Z})$ depends on sources and decoder reconstruction.

Special cases of such a distortion criterion:

- Lossy reconstruction of a function of the sources
Joint Distortion Criterion

Distortion $d(X, Y, \hat{Z})$ depends on sources and decoder reconstruction

Special cases of such a distortion criterion:
- Lossy reconstruction of a function of the sources
- Many famous distributed source coding problems
Joint Distortion Criterion

- Distortion $d(X, Y, \hat{Z})$ depends on sources and decoder reconstruction
- Special cases of such a distortion criterion:
  - Lossy reconstruction of a function of the sources
  - Many famous distributed source coding problems
    - Berger-Tung problem (with multiple distortion criteria)
    - Wyner-Ziv problem
    - Wyner-Ahlswede-Korner problem
    - Yeung-Berger problem
    - Korner-Marton problem
    - Slepian-Wolf problem
Berger-Tung based Coding Scheme

- Independent vector quantization followed by independent binning
Berger-Tung based Coding Scheme

- Independent vector quantization followed by independent binning
- \( X \) quantized to \( U \). \( Y \) quantized to \( V \)
Berger-Tung based Coding Scheme

- Independent vector quantization followed by independent binning
- $X$ quantized to $U$. $Y$ quantized to $V$
- Decoder reconstructs $\hat{Z} = G(U, V)$ that minimizes $d(X, Y, \hat{Z})$
Berger-Tung based Coding Scheme

- Independent vector quantization followed by independent binning
- $X$ quantized to $U$. $Y$ quantized to $V$
- Decoder reconstructs $\hat{Z} = G(U, V)$ that minimizes $d(X, Y, \hat{Z})$

**Theorem**

- $G: U \times V \rightarrow \hat{Z}$ - optimal reconstruction given $U, V$

$$\mathcal{RD}_{BT} \triangleq \{R_1 \geq I(X; U | V), R_2 \geq I(Y; V | U),$$

$$R_1 + R_2 \geq I(XY; UV), D \geq \mathbb{E}d(X, Y, G(U, V))\}$$

Any $(R_1, R_2, D) \in \mathcal{RD}_{BT}^*$ is achievable.
An Illustrative Example

- $X, Y$ - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
- Decoder interested in reconstructing $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
An Illustrative Example

- $X, Y$ - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
- Decoder interested in reconstructing $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- Berger-Tung based coding scheme:
  - Reconstruct sources $X, Y$. Compute $Z = X \oplus_2 Y$
  - Sum rate: $H(X, Y) = 5$ bits
An Illustrative Example

- $X, Y$ - 3 bit correlated binary sources, $d_H(X,Y) \leq 1$
- Decoder interested in reconstructing $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- Berger-Tung based coding scheme:
  - Reconstruct sources $X, Y$. Compute $Z = X \oplus_2 Y$
  - Sum rate: $H(X,Y) = 5$ bits
- Can we do better?
An Illustrative Example contd.

- A linear coding scheme:

  \[
  \begin{bmatrix}
  Z_1 \\ Z_2 \\
  Z_3
  \end{bmatrix}
  \begin{bmatrix}
  X_1 \\ X_2 \\
  X_3
  \end{bmatrix}
  \begin{bmatrix}
  Z_1 \\ Z_2 \\
  Z_3
  \end{bmatrix}
  \]

  Sum rate: \(2 + 2 = 4\) bits
An Illustrative Example contd.

- A linear coding scheme:

\[
\begin{bmatrix}
Z_1 \\
Z_2 \\
Z_3
\end{bmatrix} \oplus 
\begin{bmatrix}
X_1 \\
X_2 \\
X_3
\end{bmatrix}
\]

- Sum rate: \(2 + 2 = 4\) bits

- Significant features:
A linear coding scheme:

\[
\begin{bmatrix}
X_1 \oplus X_2 \\
X_1 \oplus X_3
\end{bmatrix}
\]

\[
\begin{bmatrix}
Y_1 \oplus Y_2 \\
Y_1 \oplus Y_3
\end{bmatrix}
\]

Sum rate: \(2 + 2 = 4\) bits

Significant features:

- Identical binning at both encoders
A linear coding scheme:

\[
\begin{align*}
\begin{bmatrix}
X_1 \\
X_2 \\
X_3
\end{bmatrix} & \oplus \\
\begin{bmatrix}
Z_1 \\
Z_2 \\
Z_3
\end{bmatrix} \\
\begin{bmatrix}
Y_1 \\
Y_2 \\
Y_3
\end{bmatrix} & \oplus
\end{align*}
\]

\[
\begin{align*}
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix} & \begin{bmatrix}
X_1 \\
X_2 \\
X_3
\end{bmatrix} \\
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix} & \begin{bmatrix}
Y_1 \\
Y_2 \\
Y_3
\end{bmatrix}
\end{align*}
\]

Sum rate: \(2 + 2 = 4 \text{ bits}\)

Significant features:
- Identical binning at both encoders
- Linear codes
Korner-Marton Coding Scheme

- Correlated binary random variables \((X_1, X_2)\)
Korner-Marton Coding Scheme

- Correlated binary random variables \((X_1, X_2)\)
- Decoder interested in lossless reconstruction of \(Z = X_1 \oplus_2 X_2\)
Korner-Marton Coding Scheme

- Correlated binary random variables \((X_1, X_2)\)
- Decoder interested in lossless reconstruction of \(Z = X_1 \oplus_2 X_2\)
Correlated binary random variables \((X_1, X_2)\)

Decoder interested in lossless reconstruction of \(Z = X_1 \oplus_2 X_2\)

Matrix \(A\): puts different typical \(z^n\) in different bins. \(\frac{k}{n} \approx H(Z)\)
Correlated binary random variables \((X_1, X_2)\)

Decoder interested in lossless reconstruction of \(Z = X_1 \oplus_2 X_2\)

Matrix \(A\): puts different typical \(z^n\) in different bins. \(\frac{k}{n} \approx H(Z)\)

Associated code: Good channel code for additive noise \(Z\)
Function to be reconstructed \( F(X, Y) = (X, Y) \).
Function to be reconstructed $F(X, Y) = (X, Y)$.

Reconstruction of binary sources equivalent to addition in $\mathbb{F}_4$. 
Slepian-Wolf Coding

- Function to be reconstructed $F(X, Y) = (X, Y)$.
- Reconstruction of binary sources equivalent to addition in $\mathbb{F}_4$.

<table>
<thead>
<tr>
<th>+4</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>00</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>10</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>

**Table:** Addition in $\mathbb{F}_4$
Slepian-Wolf Coding

- Function to be reconstructed $F(X, Y) = (X, Y)$.
- Reconstruction of binary sources equivalent to addition in $\mathbb{F}_4$.

<table>
<thead>
<tr>
<th>$\oplus_4$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>00</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>10</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>

Table: Mapping for SW-coding

- Treat binary sources as $\mathbb{F}_4$ sources.
Slepian-Wolf Coding

- Function to be reconstructed $F(X, Y) = (X, Y)$.
- Reconstruction of binary sources equivalent to addition in $\mathbb{F}_4$.

\[
\begin{array}{cccccc}
\oplus_4 & 00 & 01 & 10 & 11 \\
00 & 00 & 01 & 10 & 11 \\
01 & 01 & 00 & 11 & 10 \\
10 & 10 & 11 & 00 & 01 \\
11 & 11 & 10 & 01 & 00 \\
\end{array}
\]

**Table:** Mapping for SW-coding

- Treat binary sources as $\mathbb{F}_4$ sources.
- Function to be reconstructed is $Z = \tilde{X} \oplus_4 \tilde{Y}$. 
Digit Decomposition Approach

- We encode the vector function one component at a time.
We encode the vector function one component at a time.

Table: First Digit of $\tilde{Z}$

\[
\begin{array}{ccc}
\oplus_2 & 0 & 0 \\
0 & 0 & 0 \\
1 & 1 & 1 \\
\end{array}
\]

Table: Second Digit of $\tilde{Z}$

\[
\begin{array}{ccc}
\oplus_2 & 0 & 1 \\
0 & 0 & 1 \\
0 & 0 & 1 \\
\end{array}
\]
Digit Decomposition Approach

- We encode the vector function one component at a time.

\[ \oplus_2 0 0 \]
\[
0 0 0
\]
\[
1 1 1
\]

Table: First Digit of $\tilde{Z}$

\[ \oplus_2 0 1 \]
\[
0 0 1
\]
\[
0 0 1
\]

Table: Second Digit of $\tilde{Z}$

- Use KM encoding for each “digit”
Digit Decomposition Approach

- We encode the vector function one component at a time.

\[
\begin{array}{ccc}
\oplus_2 & 0 & 0 \\
0 & 0 & 0 \\
1 & 1 & 1 \\
\end{array}
\]

- Use KM encoding for each “digit”
- First digit can be encoded at rate \( H(\tilde{X}_1) = H(X) \)
- Second digit can be encoded at rate \( H(\tilde{Y}_2|\tilde{X}_1) = H(Y|X) \)
Overview of our Coding Scheme

- Fix test channel $P_{XYUV} = P_{XY}P_{U|X}P_{V|Y}$
Overview of our Coding Scheme

- Fix test channel $P_{XYUV} = P_{XYP_{U|X}P_{V|Y}}$
- Function to be reconstructed $G(U, V)$ - equivalent to addition in some abelian group
Overview of our Coding Scheme

- Fix test channel $P_{XYUV} = P_{XY}P_{U|X}P_{V|Y}$
- Function to be reconstructed $G(U, V)$ - equivalent to addition in some abelian group
- Abelian groups decomposable into primary cyclic groups
Overview of our Coding Scheme

- Fix test channel $P_{XYUV} = P_{XY}P_{U|X}P_{V|Y}$
- Function to be reconstructed $G(U, V)$ - equivalent to addition in some abelian group
- Abelian groups decomposable into primary cyclic groups
- Encode sequentially using nested group codes
Groups - An Introduction

- $G$ - a finite abelian group of order $n$
$G$ - a finite abelian group of order $n$

$G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$

$G$ isomorphic to direct sum of possibly repeating primary cyclic groups
Groups - An Introduction

- $G$ - a finite abelian group of order $n$

- $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$

- $G$ isomorphic to direct sum of possibly repeating primary cyclic groups

$$g \in G \Leftrightarrow g = (g_1, \ldots, g_k), \ g_i \in \mathbb{Z}_{p_i^{e_i}}$$
Groups - An Introduction

- $G$ - a finite abelian group of order $n$
- $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- $G$ isomorphic to direct sum of possibly repeating primary cyclic groups

$$g \in G \Leftrightarrow g = (g_1, \ldots, g_k), \ g_i \in \mathbb{Z}_{p_i^{e_i}}$$

- Enough to prove coding theorems for primary cyclic groups
- Extension to arbitrary abelian groups through digit decomposition
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
- Cosets bin the entire space.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
- Lossy coding: Need to quantize first.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
- Lossy coding: Need to quantize first.
  - Dilute the coset density -
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
- Lossy coding: Need to quantize first.
  - Dilute the coset density - Nested group codes.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
- Lossy coding: Need to quantize first.
  - Dilute the coset density - Nested group codes.
  - Fine code - Quantizes the source.
Nested Group Codes - Motivation

- Codes used in KM, SW - good linear channel codes.
  - Cosets bin the entire space.
  - Suitable for lossless coding.
- Lossy coding: Need to quantize first.
  - Dilute the coset density - Nested group codes.
  - Fine code - Quantizes the source.
  - Coarse code - bins only the fine code.
Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathcal{C} < \mathbb{Z}_{p^r}^n$
Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathcal{C} < \mathbb{Z}_{p^r}^n$
- $\mathcal{C} = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$
Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathcal{C} \leq \mathbb{Z}_{p^r}^n$
- $\mathcal{C} = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ nested if $\mathcal{C}_2 \subset \mathcal{C}_1$
Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathcal{C} < \mathbb{Z}_{p^r}^n$
- $\mathcal{C} = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ nested if $\mathcal{C}_2 \subset \mathcal{C}_1$
- We need:
  - $\mathcal{C}_1 < \mathbb{Z}_{p^r}^n$: “good” source code
  - $\mathcal{C}_2 < \mathbb{Z}_{p^r}^n$: “good” channel code
Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathcal{C} < \mathbb{Z}_{p^r}^n$
- $\mathcal{C} = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ nested if $\mathcal{C}_2 \subset \mathcal{C}_1$
- We need:
  - $\mathcal{C}_1 < \mathbb{Z}_{p^r}^n$: “good” source code
    - Can find $u^n \in \mathcal{C}_1$ jointly typical with source $x^n$
  - $\mathcal{C}_2 < \mathbb{Z}_{p^r}^n$: “good” channel code
    - Can find unique typical $z^n$ given the coset of $\mathcal{C}_2$ in $\mathbb{Z}_{p^r}^n$
Good Group Source Codes

- Good group source code \( C_1 \) for the triple \((\mathcal{X}, U, P_{XU})\)
Good group source code $C_1$ for the triple $(X, U, P_{XU})$

Assume $U = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$
Good Group Source Codes

- Good group source code $C_1$ for the triple $(X, U, P_{X \cup U})$
- Assume $U = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

*Exists for large $n$ if $\frac{1}{n} \log |C_1| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\}**
Good Group Source Codes

- Good group source code $\mathcal{C}_1$ for the triple $(\mathcal{X}, \mathcal{U}, P_{XU})$
- Assume $\mathcal{U} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

*Exists for large $n$ if $\frac{1}{n} \log |\mathcal{C}_1| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}\}^+$*

- Compare with optimal random code’s size: $H(U) - H(U|X) = I(X; U)$
Good Group Source Codes

- Good group source code $\mathcal{C}_1$ for the triple $(\mathcal{X}, \mathcal{U}, P_{XU})$
- Assume $\mathcal{U} = \mathbb{Z}_p^r$ for some prime $p$ and exponent $r > 0$

Lemma

*Exists for large $n$ if* \[ \frac{1}{n} \log |\mathcal{C}_1| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\} \]

- Compare with optimal random code’s size: $H(U) - H(U|X) = I(X; U)$
- Not good in Shannon sense
Good group source code $C_1$ for the triple $(X, U, P_{X|U})$

Assume $U = \mathbb{Z}_p^r$ for some prime $p$ and exponent $r > 0$

Lemma

Exists for large $n$ if $\frac{1}{n} \log |C_1| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}\}$

- Compare with optimal random code’s size: $H(U) - H(U|X) = I(X; U)$
- Not good in Shannon sense
- Penalty for imposing group structure
Good group channel code $C_2$ for the triple $(Z, I, P_{ZS})$
Good group channel code $C_2$ for the triple $(\mathcal{I}, \mathcal{J}, P_{ZS})$

Assume $\mathcal{I} = \mathbb{Z}_p^r$ for some prime $p$ and exponent $r > 0$
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(\mathcal{Z}, \mathcal{I}, P_{ZS})$
- Assume $\mathcal{Z} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

*Exists for large $n$ if* $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H(Z_i|S))$
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(\mathcal{Z}, \mathcal{S}, P_{ZS})$
- Assume $\mathcal{Z} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

Exists for large $n$ if $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H([Z]_i|S))$

- $[Z]_i$ - random variable taking values over distinct cosets of $p^i \mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(\mathcal{I}, \mathcal{S}, P_{ZS})$
- Assume $\mathcal{I} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

_exists for large $n$ if $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H([Z]_i|S))$

- $[Z]_i$ - random variable taking values over distinct cosets of $p^i \mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$
- Suppose $\mathcal{I} = \mathbb{Z}_8$. Then $[Z]_1$ - binary random variable
Good Group Channel Codes

- Good group channel code $\mathcal{C}_2$ for the triple $(\mathcal{I}, \mathcal{J}, P_{Z\mathcal{S}})$
- Assume $\mathcal{I} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

*Exists for large $n$ if $\frac{1}{n} \log |\mathcal{C}_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) \left( H(Z|S) - H([Z]_i|S) \right)\*

- $[Z]_i$ - random variable taking values over distinct cosets of $p^i \mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$
- Suppose $\mathcal{I} = \mathbb{Z}_8$. Then $[Z]_1$ - binary random variable
- Symbol probabilities - $(p_0 + p_2 + p_4 + p_6)$ and $(p_1 + p_3 + p_5 + p_7)$
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(\mathcal{Z}, \mathcal{I}, P_{ZS})$
- Assume $\mathcal{Z} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

Exists for large $n$ if $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H([Z]_i|S))$

- Compare with optimal random code’s size $\log p^r - H(Z|S)$
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(Z, J, P_{ZS})$
- Assume $Z = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

Exists for large $n$ if $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H([Z]_i|S))$

- Compare with optimal random code’s size $\log p^r - H(Z|S)$
- Not good in Shannon sense
Good Group Channel Codes

- Good group channel code $C_2$ for the triple $(\mathcal{F}, \mathcal{I}, P_{ZS})$
- Assume $\mathcal{F} = \mathbb{Z}_{p^r}$ for some prime $p$ and exponent $r > 0$

**Lemma**

*Exists for large $n$ if $\frac{1}{n} \log |C_2| \leq \log p^r - \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z|S) - H([Z]_i|S))$*

- Compare with optimal random code's size $\log p^r - H(Z|S)$
- Not good in Shannon sense
- Penalty for presence of subgroups
Proof Techniques - Group Channel Codes

- Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^k$
Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^k$

Good group channel codes: Recover $z^n$ from $\phi(z^n)$. 
Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$

Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e = P \left( \bigcup_{\tilde{z}^n \in A_c^n(Z)} (\phi(\tilde{z}^n) = \phi(z^n)) \right)$$
• Existence proofs by ensemble averaging \( P_e \) over all \( \phi: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^k \)

• Good group channel codes: Recover \( z^n \) from \( \phi(z^n) \)

\[
P_e \leq \sum_{\tilde{z}^n \in A^*_n(Z)} P\left( \phi(\tilde{z}^n - z^n) = 0^k \right)
\]
Proof Techniques - Group Channel Codes

- Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$

- Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e \leq \sum_{\tilde{z}^n \in A^{|n|}_{\phi}(Z) \atop \tilde{z}^n \neq z^n} P\left(\phi(\tilde{z}^n - z^n) = 0^k\right)$$

- Depends on which subgroup $p^i \mathbb{Z}_{p^r}$ the term $(\tilde{z}^n - z^n)$ belongs to
Proof Techniques - Group Channel Codes

- Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^r$
- Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$
P_e \leq \sum_{\tilde{z}^n \in \mathcal{A}_c^n(Z) \atop \tilde{z}^n \neq z^n} P\left(\phi(\tilde{z}^n - z^n) = 0^k\right)
$$

- Depends on which subgroup $p^i \mathbb{Z}_p^n$ the term $(\tilde{z}^n - z^n)$ belongs to

- Suppose $\mathcal{I} = \mathbb{Z}_8$
Proof Techniques - Group Channel Codes

- Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$

- Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e \leq \sum_{\tilde{z}^n \in A^n(Z)} P\left(\phi(\tilde{z}^n - z^n) = 0^k\right)$$

- Depends on which subgroup $p^i \mathbb{Z}_{p^r}$ the term $(\tilde{z}^n - z^n)$ belongs to

- Suppose $\mathcal{I} = \mathbb{Z}_8$
  
  - $\tilde{z}^n - z^n \in 4\mathbb{Z}_8^n \implies \phi(\tilde{z}^n - z^n) \in 4\mathbb{Z}_8^k \implies$ probability $= \left(\frac{1}{2}\right)^k$
Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_p^n \to \mathbb{Z}_p^k$

Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e \leq \sum_{\tilde{z}^n \in A^n_{\phi}(Z)} P \left( \phi(\tilde{z}^n - z^n) = 0^k \right)$$

- Depends on which subgroup $p^i \mathbb{Z}_p^n$ the term $(\tilde{z}^n - z^n)$ belongs to

Suppose $\mathcal{Z} = \mathbb{Z}_8$

- $\tilde{z}^n - z^n \in 4\mathbb{Z}_8^n \implies \phi(\tilde{z}^n - z^n) \in 4\mathbb{Z}_8^k \implies$ probability $= \left(\frac{1}{2}\right)^k$
- $\tilde{z}^n - z^n \in 2\mathbb{Z}_8^n \implies \phi(\tilde{z}^n - z^n) \in 2\mathbb{Z}_8^k \implies$ probability $= \left(\frac{1}{4}\right)^k$
Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_{pr}^n \rightarrow \mathbb{Z}_{pr}^k$

Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e \leq \sum_{\tilde{z}^n \in A^n_c(Z)} P\left(\phi(\tilde{z}^n - z^n) = 0^k\right)$$

- Depends on which subgroup $p^i \mathbb{Z}_{pr}^n$ the term $(\tilde{z}^n - z^n)$ belongs to

- Estimate cardinality of $(z^n + p^i \mathbb{Z}_{pr}^n) \cap A^n_c(Z)$
Existence proofs by ensemble averaging $P_e$ over all $\phi: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^k$

Good group channel codes: Recover $z^n$ from $\phi(z^n)$

$$P_e \leq \sum_{\tilde{z}^n \in A_\epsilon^n(Z)} \sum_{\tilde{z}^n \neq z^n} P\left(\phi(\tilde{z}^n - z^n) = 0^k\right)$$

- Depends on which subgroup $p^i \mathbb{Z}_p^n$ the term $(\tilde{z}^n - z^n)$ belongs to

Estimate cardinality of $(z^n + p^i \mathbb{Z}_p^n) \cap A_\epsilon^n(Z)$

- Equivalent to entropy maximization under affine constraints
Good group source code:
Good group source code:

\[ P \left( \sum_{u^n \in A^n(x^n)} 1_{\{u^n \in C\}} \right) = 0 \]

Group structure introduces dependencies
Good group source code:

\[ P \left( \left[ \sum_{u^n \in A^n_c(x^n)} 1_{\{u^n \in \mathcal{C}\}} \right] = 0 \right) \]

Group structure introduces dependencies

Suen’s inequality from random graph literature
Suen’s Inequality

- Bounds on sum of “sparsely” dependent indicator random variables
Suen’s Inequality

- Bounds on sum of “sparsely” dependent indicator random variables

\[ I_1 \quad I_3 \quad I_4 \quad I_5 \]

- Each indicator is a node
Suen’s Inequality

- Bounds on sum of “sparsely” dependent indicator random variables

- Edges between dependent indicators

\[ I_1, I_2, I_3, I_4, I_5 \]
Suen’s Inequality

- Bounds on sum of “sparsely” dependent indicator random variables

\[ \lambda = \sum_i \mathbb{E}I_i \]
\[ \Delta = \frac{1}{2} \sum_i \sum_{j \sim i} \mathbb{E}(I_i I_j) \]
\[ \delta = \max_i \sum_{k \sim i} \mathbb{E}I_k \]
Suen’s Inequality

- Bounds on sum of “sparsely” dependent indicator random variables

\[ I_1 \quad I_2 \quad I_3 \quad I_4 \quad I_5 \]

- \( \lambda = \sum_i \mathbb{E}[I_i] \)
- \( \Delta = \frac{1}{2} \sum_i \sum_{j \sim i} \mathbb{E}[I_i I_j] \)
- \( \delta = \max_i \sum_{k \sim i} \mathbb{E}[I_k] \)

\[ P \left( \sum_i I_i = 0 \right) \leq \exp \left\{ -\min \left( \frac{\lambda^2}{8\Delta}, \frac{\lambda}{2}, \frac{\lambda}{6\delta} \right) \right\} \]
Need to evaluate $P(u^n \in \mathcal{C})$ and $P(u^n_1, u^n_2 \in \mathcal{C})$
Need to evaluate \( P(u^n \in \mathcal{C}) \) and \( P(u_1^n, u_2^n \in \mathcal{C}) \)

\( P(u^n \in \mathcal{C}) \) easy to evaluate
Need to evaluate $P(u^n \in C)$ and $P(u^n_1, u^n_2 \in C)$

$P(u^n \in C)$ easy to evaluate

$P(u^n_1, u^n_2 \in C)$
Need to evaluate $P(u^n \in \mathcal{C})$ and $P(u^n_1, u^n_2 \in \mathcal{C})$

$P(u^n \in \mathcal{C})$ easy to evaluate

$P(u^n_1, u^n_2 \in \mathcal{C})$

- Depends on number of solutions in $(\alpha, \beta)$ to $\alpha u^n_1 + \beta u^n_2 = 0$
Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathcal{C})$ and $P(u^n_1, u^n_2 \in \mathcal{C})$

- $P(u^n \in \mathcal{C})$ easy to evaluate

- $P(u^n_1, u^n_2 \in \mathcal{C})$
  - Depends on number of solutions in $(\alpha, \beta)$ to $\alpha u^n_1 + \beta u^n_2 = 0$
  - $P(u^n_1, u^n_2 \in \mathcal{C}) = \frac{\text{Number of solution pairs}(\alpha, \beta)}{p^{2r}}$
Proof Techniques - Group Source Codes contd.

- Need to evaluate \( P(u^n \in \mathcal{C}) \) and \( P(u^n_1, u^n_2 \in \mathcal{C}) \)

- \( P(u^n \in \mathcal{C}) \) easy to evaluate

- \( P(u^n_1, u^n_2 \in \mathcal{C}) \)
  - Depends on number of solutions in \((\alpha, \beta)\) to \( \alpha u^n_1 + \beta u^n_2 = 0 \)
  - \( P(u^n_1, u^n_2 \in \mathcal{C}) = \frac{\text{Number of solution pairs}(\alpha, \beta)}{p^{2r}} \)

- Have to estimate the degree of each vertex in the dependency graph
Notation

- Fix $P_{U|X}, P_{V|Y}$ such that $\mathbb{E}d(X, Y, G(U, V)) \leq D$
Notation

- Fix $P_{U|X}, P_{V|Y}$ such that $E d(X, Y, G(U, V)) \leq D$
- Suppose $G(U, V)$ equivalent to group operation in abelian group $G$
Notation

- Fix $P_{U|X}, P_{V|Y}$ such that $\exists d(X, Y, G(U, V)) \leq D$
- Suppose $G(U, V)$ equivalent to group operation in abelian group $G$
- Decompose $G$ into primary cyclic groups. Encode one digit at a time
Fix $P_{U \mid X}, P_{V \mid Y}$ such that $Ed(X, Y, G(U, V)) \leq D$

Suppose $G(U, V)$ equivalent to group operation in abelian group $G$

Decompose $G$ into primary cyclic groups. Encode one digit at a time

Decoder: At the $b$th stage, previously decoded digits as side information
Coding Strategy

- Nested group codes $\mathcal{C}_2 < \mathcal{C}_{11}, \mathcal{C}_{12}$
Coding Strategy

- Nested group codes $\mathcal{C}_2 < \mathcal{C}_{11}, \mathcal{C}_{12}$
Coding Strategy

- Nested group codes $\mathcal{C}_2 < \mathcal{C}_{11}, \mathcal{C}_{12}$

\[
\frac{1}{n} \log |\mathcal{C}_{11}| \geq \log p^r - \min \{ H(U|X), r | H(U|X) - \log p^{r-1} \}^+
\]
Coding Strategy

- Nested group codes $\mathcal{C}_2 < \mathcal{C}_{11}, \mathcal{C}_{12}$

\[
\frac{1}{n} \log |\mathcal{C}_{11}| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^r-1|^+\}
\]

\[
\frac{1}{n} \log |\mathcal{C}_{12}| \geq \log p^r - \min\{H(V|Y), r|H(V|Y) - \log p^r-1|^+\}
\]
Coding Strategy

- Nested group codes $\mathcal{C}_2 < \mathcal{C}_{11}, \mathcal{C}_{12}$

\[
\frac{1}{n} \log |\mathcal{C}_{11}| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\}
\]

\[
\frac{1}{n} \log |\mathcal{C}_{12}| \geq \log p^r - \min\{H(V|Y), r|H(V|Y) - \log p^{r-1}|^+\}
\]

\[
\frac{1}{n} \log |\mathcal{C}_2| \leq \log p^r - \max_{0 \leq i < r} \left(\frac{r}{r-i}\right) (H(Z) - H([Z]_i))
\]
Achievable Rates

Theorem

The set of tuples $(R_1, R_2, D)$ that satisfy

\[ R_1 \geq \max_{0 \leq i < r} \left( \frac{r}{r - i} \right) \left( H(Z) - H([Z]_i) \right) - \min \{ H(U|X), r|H(U|X) - \log p^{r-1} \} \]

\[ R_2 \geq \max_{0 \leq i < r} \left( \frac{r}{r - i} \right) \left( H(Z) - H([Z]_i) \right) - \min \{ H(V|Y), r|H(V|Y) - \log p^{r-1} \} \]

\[ D \geq \mathbb{E}d(X, Y, G(U, V)) \]

are achievable.
Theorem

The set of tuples \((R_1, R_2, D)\) that satisfy

\[
R_1 \geq \max_{0 \leq i < r} \left( \frac{r}{r - i} \right) (H(Z) - H([Z]_i)) - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\}
\]

\[
R_2 \geq \max_{0 \leq i < r} \left( \frac{r}{r - i} \right) (H(Z) - H([Z]_i)) - \min\{H(V|Y), r|H(V|Y) - \log p^{r-1}|^+\}
\]

\[
D \geq \mathbb{E}d(X, Y, G(U, V))
\]

are achievable.

- More general rate region possible by D. Krithivasan (U of M)
Achievable Rates

Theorem

The set of tuples \((R_1, R_2, D)\) that satisfy

\[
R_1 \geq \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z) - H([Z]_i)) - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\}
\]

\[
R_2 \geq \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) (H(Z) - H([Z]_i)) - \min\{H(V|Y), r|H(V|Y) - \log p^{r-1}|^+\}
\]

\[
D \geq \mathbb{E}d(X, Y, G(U, V))
\]

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
Achievable Rates

**Theorem**

The set of tuples \((R_1, R_2, D)\) that satisfy

\[
R_1 \geq \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) \left( H(Z) - H([Z]_i) \right) - \min \{ H(U|X), r | H(U|X) - \log p^{r-1} \}^+
\]

\[
R_2 \geq \max_{0 \leq i < r} \left( \frac{r}{r-i} \right) \left( H(Z) - H([Z]_i) \right) - \min \{ H(V|Y), r | H(V|Y) - \log p^{r-1} \}^+
\]

\[
D \geq Ed(X, Y, G(U, V))
\]

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy at \(b\)th stage - Encode \((U_b, V_b)\) instead of \(Z_b\)
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
- Recovers known rate regions (using nested linear codes) of
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
- Recovers known rate regions (using nested linear codes) of Berger-Tung problem
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
- Recovers known rate regions (using nested linear codes) of
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
  - Yeung-Berger problem
Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
- Recovers known rate regions (using nested linear codes) of
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
  - Yeung-Berger problem
  - Slepian-Wolf problem, Korner-Marton problem
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables
- Sources: $X, Y$. Correlation: $Y = X \oplus_4 Z$
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables

- Sources: $X, Y$. Correlation: $Y = X \oplus_4 Z$

- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables
- Sources: $X, Y$. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- No linear code over $\mathbb{F}_4$ - KM not possible
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables
- Sources: $X, Y$. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- No linear code over $\mathbb{F}_4$ - KM not possible
- Group based scheme achieves

$$R_{sum} = 2 \max\{H(Z), 2(H(Z) - H([Z]_1))\}$$
A Lossless Reconstruction Example

- $X, Y, Z$ - Quaternary random variables
- Sources: $X, Y$. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- No linear code over $\mathbb{F}_4$ - KM not possible
- Group based scheme achieves

$$R_{sum} = 2 \max\{H(Z), 2(H(Z) - H([Z]_1))\}$$

- Can be lower than $H(X, Y)$
Lossy Reconstruction of binary XOR

- Correlated binary sources \((X, Y)\)
Lossy Reconstruction of binary XOR

- Correlated binary sources \((X, Y)\)
- Reconstruct \(Z = X \oplus_2 Y\) within Hamming distortion \(D\)
Lossy Reconstruction of binary XOR

- Correlated binary sources \((X, Y)\)
- Reconstruct \(Z = X \oplus_2 Y\) within Hamming distortion \(D\)
- \(U, V\) - binary auxiliary random variables
Lossy Reconstruction of binary XOR

- Correlated binary sources \((X, Y)\)
- Reconstruct \(Z = X \oplus_2 Y\) within Hamming distortion \(D\)
- \(U, V\) - binary auxiliary random variables
- \(G(U, V)\) - one of 16 possibilities depending on \((P_{U|X}, P_{V|Y})\)
Comparison of the two lower convex envelopes

Rate gains over the Berger-Tung based scheme
Rate gains over the Berger-Tung based scheme

Implies Berger-Tung inner bound not tight for three-user case
Outline

1. Distributed Source Coding - an Introduction
2. Distributed Source Coding - Discrete Sources
3. Distributed Source Coding - Gaussian Sources
4. Future Work
Highlights of the work

\[ X_1^n, X_2^n \sim \mathcal{N}(0, 1), \mathbb{E}(X_1 X_2) = \rho > 0 \]
Highlights of the work

\[ \hat{Z} = X_1 - cX_2, \quad c > 0 \]
Highlights of the work

\[ X_1^n \rightarrow \text{Encoder 1} \rightarrow R_1 \rightarrow \cdots \rightarrow \text{Decoder} \rightarrow \hat{Z} \]

- \[ f_1(\cdot) \]
- \[ f_2(\cdot) \]

\[ \mathbb{E}d(X_1, X_2, \hat{Z}) = \mathbb{E}(X_1 - cX_2 - \hat{Z})^2 \]
Objective: Achievable rates \((R_1, R_2)\) at distortion \(D\)
Achievable rate region using nested lattice codes
Showed achievability of $(R_1, R_2, D)$ when

$$2^{-2R_1} + 2^{-2R_2} \leq \left(\frac{\sigma_Z^2}{D}\right)^{-1}$$
Outline

1. Distributed Source Coding - an Introduction
2. Distributed Source Coding - Discrete Sources
3. Distributed Source Coding - Gaussian Sources
4. Future Work
Abelian group code $C = \ker(\phi)$ for homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$
Abelian group code $\mathcal{C} = \ker(\phi)$ for homomorphism $\phi: \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$.

Proofs use underlying ring structure of $\mathbb{Z}_{p^r}$. 
Abelian group code \( \mathcal{C} = \ker(\phi) \) for homomorphism \( \phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k \).

Proofs use underlying ring structure of \( \mathbb{Z}_{p^r} \):
- \( \phi(\cdot) \) equivalent to multiplication by \( k \times n \) matrix \( \Phi \).
Codes over Non-Abelian Groups

- Abelian group code \( \mathcal{C} = \ker(\phi) \) for homomorphism \( \phi: \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k \)
- Proofs use underlying ring structure of \( \mathbb{Z}_{p^r}^n \)
  - \( \phi(\cdot) \) equivalent to multiplication by \( k \times n \) matrix \( \Phi \)
  - Ensemble average \( P_e \) over all matrices \( \Phi \in \mathbb{Z}_{p^r}^{k \times n} \)
Abelian group code $C = \ker(\phi)$ for homomorphism $\phi: \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$

Proofs use underlying ring structure of $\mathbb{Z}_{p^r}$

- $\phi(\cdot)$ equivalent to multiplication by $k \times n$ matrix $\Phi$
- Ensemble average $P_e$ over all matrices $\Phi \in \mathbb{Z}_{p^r}^{k \times n}$

Non-abelian $G$
Abelian group code \( C = \ker(\phi) \) for homomorphism \( \phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k \).

Proofs use underlying ring structure of \( \mathbb{Z}_{p^r} \):
- \( \phi(\cdot) \) equivalent to multiplication by \( k \times n \) matrix \( \Phi \)
- Ensemble average \( P_e \) over all matrices \( \Phi \in \mathbb{Z}_{p^r}^{k \times n} \)

Non-abelian \( G \):
- Not many homomorphisms from \( G^n \) to \( G^k \)
Abelian group code $\mathcal{C} = \ker(\phi)$ for homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$

Proofs use underlying ring structure of $\mathbb{Z}_{p^r}$
- $\phi(\cdot)$ equivalent to multiplication by $k \times n$ matrix $\Phi$
- Ensemble average $P_e$ over all matrices $\Phi \in \mathbb{Z}_{p^r}^{k \times n}$

Non-abelian $G$
- Not many homomorphisms from $G^n$ to $G^k$
- No underlying ring structure
Abelian group code $C = \ker(\phi)$ for homomorphism $\phi: \mathbb{Z}_{p^r}^n \rightarrow \mathbb{Z}_{p^r}^k$

Proofs use underlying ring structure of $\mathbb{Z}_{p^r}$

- $\phi(\cdot)$ equivalent to multiplication by $k \times n$ matrix $\Phi$
- Ensemble average $P_e$ over all matrices $\Phi \in \mathbb{Z}_{p^r}^{k \times n}$

Non-abelian $G$

- Not many homomorphisms from $G^n$ to $G^k$
- No underlying ring structure
- Ensemble of all subgroups? (not necessarily normal)
Other Extensions

- All ideas applicable to multi-terminal channel coding problems
Other Extensions

- All ideas applicable to multi-terminal channel coding problems
- Lattice scheme works only for Gaussian sources
Other Extensions

- All ideas applicable to multi-terminal channel coding problems
- Lattice scheme works only for Gaussian sources
  - Extension to arbitrary continuous sources and functions
Other Extensions

- All ideas applicable to multi-terminal channel coding problems
- Lattice scheme works only for Gaussian sources
  - Extension to arbitrary continuous sources and functions
  - Information theoretic characterization of rate region
Other Extensions

- All ideas applicable to multi-terminal channel coding problems
- Lattice scheme works only for Gaussian sources
  - Extension to arbitrary continuous sources and functions
  - Information theoretic characterization of rate region

Thank You