Algebraic Structures for Distributed Source Coding

Dinesh Krithivasan and S. Sandeep Pradhan

University of Michigan

ITA 2009
Introduction

- Random coding - common in information theory
Introduction

- Random coding - common in information theory
- Structured codes - explored mainly for complexity reasons
Random coding - common in information theory

Structured codes - explored mainly for complexity reasons

Structured codes have performance unattainable by random codes
Introduction

- Random coding - common in information theory
- Structured codes - explored mainly for complexity reasons
- Structured codes have performance unattainable by random codes
  - Can achieve expurgated bound on the BSC
Introduction

- Random coding - common in information theory
- Structured codes - explored mainly for complexity reasons
- Structured codes have performance unattainable by random codes
  - Can achieve expurgated bound on the BSC
  - Some works on first order performance gains offered by linear codes
Introduction

- Random coding - common in information theory
- Structured codes - explored mainly for complexity reasons
- Structured codes have performance unattainable by random codes
  - Can achieve expurgated bound on the BSC
  - Some works on first order performance gains offered by linear codes
- This thesis: Unified framework for using structured codes
Random coding - common in information theory

Structured codes - explored mainly for complexity reasons

Structured codes have performance unattainable by random codes
  - Can achieve expurgated bound on the BSC
  - Some works on first order performance gains offered by linear codes

This thesis: Unified framework for using structured codes
  - Attains/Exceeds known performance limits for many problems
**Introduction**

- Random coding - common in information theory
- Structured codes - explored mainly for complexity reasons
- Structured codes have performance unattainable by random codes
  - Can achieve expurgated bound on the BSC
  - Some works on first order performance gains offered by linear codes

This thesis: Unified framework for using structured codes
- Attains/Exceeds known performance limits for many problems
- Suggests practical code constructions
Thesis Overview

- Very general framework - includes many famous problems
Thesis Overview

- Very general framework - includes many famous problems
- Describe avenues for rate gains
Thesis Overview

- Very general framework - includes many famous problems
- Describe avenues for rate gains
- Role of structured codes in obtaining these rate gains
Thesis Overview

- Very general framework - includes many famous problems
- Describe avenues for rate gains
- Role of structured codes in obtaining these rate gains
  - Gaussian sources - Lattice codes
Thesis Overview

- Very general framework - includes many famous problems
- Describe avenues for rate gains
- Role of structured codes in obtaining these rate gains
  - Gaussian sources - Lattice codes
  - Discrete sources - Group codes
Thesis Overview

- Very general framework - includes many famous problems
- Describe avenues for rate gains
- Role of structured codes in obtaining these rate gains
  - Gaussian sources - Lattice codes
  - Discrete sources - Group codes
- Applications to sensor networks, video coding etc.
A Distributed Source Coding Problem

- Set of encoders observe different components of a vector source
- Central decoder receives quantized observations from the encoders
- Decoder interested in minimizing a joint distortion criterion
Joint Distortion Criterion

Distortion criterion depends on all the sources and decoder reconstructions
Joint Distortion Criterion

- Distortion criterion depends on all the sources and decoder reconstructions
- Special cases of this framework
  - Slepian-Wolf problem
  - Wyner-Ziv problem
  - Ahlswede-Korner-Wyner problem
  - Berger-Yeung problem
  - Berger-Tung problem
  - Korner-Marton binary XOR problem
Joint Distortion Criterion

- Distortion criterion depends on all the sources and decoder reconstructions
- Special cases of this framework
  - Slepian-Wolf problem
  - Wyner-Ziv problem
  - Ahlswede-Korner-Wyner problem
  - Berger-Yeung problem
  - Berger-Tung problem
  - Korner-Marton binary XOR problem
- Best known rate region - Berger-Tung based
Motivation for our coding scheme

- Suppose decoder receives auxiliary random variables $U, V$
Motivation for our coding scheme

- Suppose decoder receives auxiliary random variables $U, V$
- Encoders don’t communicate with each other: $V \rightarrow Y \rightarrow X \rightarrow U$
Motivation for our coding scheme

- Suppose decoder receives auxiliary random variables $U, V$
- Encoders don’t communicate with each other: $V - Y - X - U$
- Decoder reconstructs $G(U, V)$

$$G(U, V) \triangleq \arg \min_{G: \hat{Z} = G(U,V)} d(X, Y, \hat{Z})$$
Motivation for our coding scheme

- Suppose decoder receives auxiliary random variables $U, V$
- Encoders don’t communicate with each other: $V - Y - X - U$
- Decoder reconstructs $G(U, V)$

$$G(U, V) \triangleq \arg \min_{G: \hat{Z} = G(U, V)} d(X, Y, \hat{Z})$$

- Decoder not interested in $(U, V)$. Only in $G(U, V)$
Motivation for our coding scheme

- Suppose decoder receives auxiliary random variables $U, V$
- Encoders don’t communicate with each other: $V - Y - X - U$
- Decoder reconstructs $G(U, V)$

$$G(U, V) \triangleq \arg \min_{G: \hat{Z} = G(U,V)} d(X, Y, \hat{Z})$$

- Decoder not interested in $(U, V)$. Only in $G(U, V)$
- Encode such that decoder can only reconstruct what it needs
An Illustrative Example

- $X, Y$ - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
An Illustrative Example

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

- $X, Y$ - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
- Lossless reconstruction of $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- Berger-Tung based coding scheme:
  - Reconstruct sources $X, Y$. Compute $Z = X \oplus_2 Y$
An Illustrative Example

- $X, Y$ - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
- Lossless reconstruction of $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- 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, $d_H(X, Y) \leq 1$
- Lossless reconstruction of $Z = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- 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?
A linear coding scheme:

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

\[ \begin{bmatrix} Z_1 \oplus Z_2 \\ Z_1 \oplus Z_3 \end{bmatrix} \]
A linear coding scheme:

\[
\begin{bmatrix}
X_1 X_2 X_3 \\
Y_1 Y_2 Y_3
\end{bmatrix}
\rightarrow
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix}
\rightarrow
\begin{bmatrix}
X_1 \oplus X_2 \\
X_1 \oplus X_3
\end{bmatrix}
\rightarrow
\begin{bmatrix}
Z_1 \oplus Z_2 \\
Z_1 \oplus Z_3
\end{bmatrix}
\]

\[
\begin{bmatrix}
Y_1 Y_2 Y_3 \\
Y_1 Y_2 Y_3
\end{bmatrix}
\rightarrow
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix}
\rightarrow
\begin{bmatrix}
Y_1 \oplus Y_2 \\
Y_1 \oplus Y_3
\end{bmatrix}
\]

Sum rate: \(2 + 2 = 4 \text{ bits} = 2H(Z)\)
A linear coding scheme:

Sum rate: $2 + 2 = 4$ bits $= 2H(Z)$

Significant features:

- Identical binning at both encoders.
An Illustrative Example contd.

- A linear coding scheme:

\[
\begin{bmatrix}
X_1 & X_2 & X_3 \\
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix}
\]

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

- Significant features:
  - Identical binning at both encoders. Binning performed by Linear codes
An Illustrative Example contd.

- A linear coding scheme:

  \[
  \begin{bmatrix}
  X_1X_2X_3 \\
  Y_1Y_2Y_3
  \end{bmatrix}
  \rightarrow
  \begin{bmatrix}
  1 & 1 & 0 \\
  1 & 0 & 1
  \end{bmatrix}
  \rightarrow
  \begin{bmatrix}
  X_1 \oplus X_2 \\
  X_1 \oplus X_3
  \end{bmatrix}
  \rightarrow
  \begin{bmatrix}
  Z_1 \oplus Z_2 \\
  Z_1 \oplus Z_3
  \end{bmatrix}
  \]

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

- Significant features:
  - Identical binning at both encoders. Binning performed by Linear codes
  - Lossless reconstruction. Entire space is binned
Source \((X_1, X_2)\) is bivariate Gaussian

\[ X_1, X_2 \sim \mathcal{N}(0, 1), \quad \mathbb{E}(X_1 X_2) = \rho > 0 \]
Source \((X_1, X_2)\) is bivariate Gaussian

\[ X_1, X_2 \sim \mathcal{N}(0, 1), \quad \mathbb{E}(X_1 X_2) = \rho > 0 \]

Decoder interested in \(Z = X_1 - cX_2\) with mean square distortion, \(c > 0\)
Jointly Gaussian sources and linear function reconstruction

- Source \((X_1, X_2)\) is bivariate Gaussian
- \(X_1, X_2 \sim \mathcal{N}(0, 1), \mathbb{E}(X_1 X_2) = \rho > 0\)
- Decoder interested in \(Z = X_1 - cX_2\) with mean square distortion, \(c > 0\)
- Berger-Tung based coding scheme
  - Encoders: Quantize \(X_1\) to \(W_1\), \(X_2\) to \(W_2\). Transmit \(W_1, W_2\)
  - Decoder: Reconstruct \(\hat{Z} = \mathbb{E}(Z \mid W_1, W_2)\)
  - Optimal for \(c < 0\) with Gaussian test channels
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
- Need to do quantization first - nested lattice codes
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
- Need to do quantization first - nested lattice codes

- Quantizer - nearest neighbour
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
- Need to do quantization first - nested lattice codes

- Quantizer - nearest neighbour
- Binning - coset leader of the quantized fine lattice point in the coarse lattice
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
- Need to do quantization first - nested lattice codes

- Quantizer - nearest neighbour
- Binning - coset leader of the quantized fine lattice point in the coarse lattice
- Fine code - Quantizes the source
Nested Lattice codes

- Lattice codes: Equivalent to linear codes for continuous sources
- Lattice code: points in $\mathbb{R}^n$ closed under addition
- Need to do quantization first - nested lattice codes

- Quantizer - nearest neighbour
- Binning - coset leader of the quantized fine lattice point in the coarse lattice
- Fine code - Quantizes the source
- Coarse code - bins fine code
Rate region using nested lattice codes

- Nested lattice codes $\Lambda_2 \subset \Lambda_{11}, \Lambda_2 \subset \Lambda_{12}$
Rate region using nested lattice codes

- Nested lattice codes $\Lambda_2 \subset \Lambda_{11}, \Lambda_2 \subset \Lambda_{12}$
- $\Lambda_{11}, \Lambda_{12}$ - good lattice source codes
Nested lattice codes $\Lambda_2 \subset \Lambda_{11}, \Lambda_2 \subset \Lambda_{12}$

$\Lambda_{11}, \Lambda_{12}$ - good lattice source codes

$\Lambda_2$ - good lattice channel code
Achievable tuples satisfy $2^{-2R_1} + 2^{-2R_2} \leq \left( \frac{\sigma_z^2}{D} \right)^{-1}$
Achievable tuples satisfy \( 2^{-2R_1} + 2^{-2R_2} \leq \left( \frac{\sigma_Z^2}{D} \right)^{-1} \)

For certain sources and distortions: better than Berger-Tung based scheme
Achievable tuples satisfy $2^{-2R_1} + 2^{-2R_2} \leq \left( \frac{\sigma_z^2}{\hat{D}} \right)^{-1}$

For certain sources and distortions: better than Berger-Tung based scheme

Gains based on alignment of $[1, -c]$ with eigenvectors of source covariance matrix
Comparison between the two coding schemes

- **Berger–Tung Sum Rate**
- **Lattice Sum Rate**

- $\rho = 0.95$
- $c = 1$
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: \( P_{XYUV} = P_{XY} P_{U|X} P_{V|Y} \)
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: \( P_{XYUV} = P_{XY} P_{U|X} P_{V|Y} \)
- Decoder interested only in \( G(U, V) \)
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: $P_{XYUV} = P_{XY}P_{U|X}P_{V|Y}$
- Decoder interested only in $G(U, V)$
- Function $G(U, V)$ equivalent to addition in some abelian group $G$
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: $P_{XYUV} = P_{XY}P_U|XP_V|Y$
- Decoder interested only in $G(U, V)$
- Function $G(U, V)$ equivalent to addition in some abelian group $G$
- Abelian groups decomposable into primary cyclic groups $\mathbb{Z}_{p^r}$
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: \( P_{XYUV} = P_{XY}P_{U|X}P_{V|Y} \)
- Decoder interested only in \( G(U, V) \)
- Function \( G(U, V) \) equivalent to addition in some abelian group \( G \)
- Abelian groups decomposable into primary cyclic groups \( \mathbb{Z}_{p^r} \)

\[ g \in G \Leftrightarrow g = (g_1, \ldots, g_k), g_i \in \mathbb{Z}_{p_i^{e_i}} \]
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: \( P_{XYUV} = P_{XY} P_{U|X} P_{V|Y} \)
- Decoder interested only in \( G(U, V) \)
- Function \( G(U, V) \) equivalent to addition in some abelian group \( G \)
- Abelian groups decomposable into primary cyclic groups \( \mathbb{Z}_{p^r} \)

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

- Suffices to build codes over \( \mathbb{Z}_{p^r} \)
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: $P_{XYUV} = P_{XY} P_{U|X} P_{V|Y}$
- Decoder interested only in $G(U, V)$
- Function $G(U, V)$ equivalent to addition in some abelian group $G$
- Abelian groups decomposable into primary cyclic groups $\mathbb{Z}_{p^r}$

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

- Suffices to build codes over $\mathbb{Z}_{p^r}$ - nested group codes
Discrete sources and arbitrary distortions

- Arbitrary discrete sources and arbitrary distortions
- Fix test channels: \( P_{XYUV} = P_{XY} P_{U|X} P_{V|Y} \)
- Decoder interested only in \( G(U, V) \)
- Function \( G(U, V) \) equivalent to addition in some abelian group \( G \)
- Abelian groups decomposable into primary cyclic groups \( \mathbb{Z}_{p^r} \)

\[
g \in G \iff g = (g_1, \ldots, g_k), \quad g_i \in \mathbb{Z}_{p_i^{e_i}}
\]

- Suffices to build codes over \( \mathbb{Z}_{p^r} \) - nested group codes
- Extension to arbitrary groups through sequential coding
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 $\mathcal{C}_2 \subset \mathcal{C}_1$
Nested Group codes

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

- Group code over $\mathbb{Z}_{p^r}^n$: $C < \mathbb{Z}_{p^r}^n$
- $C = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$
- $(C_1, C_2)$ nested if $C_2 \subset C_1$
- We need:
  - $C_1 < \mathbb{Z}_{p^r}^n$: “good” source code
    - Can find $u^n \in C_1$ jointly typical with source $x^n$
  - $C_2 < \mathbb{Z}_{p^r}^n$: “good” channel code
Nested Group codes

- Group code over $\mathbb{Z}_{pr}^n$: $\mathcal{C} < \mathbb{Z}_{pr}^n$
- $\mathcal{C} = \ker(\phi)$ for some homomorphism $\phi: \mathbb{Z}_{pr}^n \rightarrow \mathbb{Z}_{pr}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ nested if $\mathcal{C}_2 \subset \mathcal{C}_1$
- We need:
  - $\mathcal{C}_1 < \mathbb{Z}_{pr}^n$: “good” source code
    - Can find $u^n \in \mathcal{C}_1$ jointly typical with source $x^n$
  - $\mathcal{C}_2 < \mathbb{Z}_{pr}^n$: “good” channel code
    - Can distinguish between typical channel noise sequences
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$
Group source codes: Example

- Consider \( \mathbb{Z}_4 = \{0, 1, 2, 3\} \)
- One non-trivial subgroup \( 2\mathbb{Z}_4 = \{0, 2\} \)
- Good group source code for \( (\mathcal{X}, \mathcal{U}, P_{XU}) \)
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

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

Assume $\mathcal{U} = \mathbb{Z}_4$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

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

Assume $\mathcal{U} = \mathbb{Z}_4$

Exists for large $n$ if $\frac{1}{n} \log |\mathcal{C}_1| \geq \log 4 - \min\{H(U|X), 2|H(U|X) - 1|\}$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

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

Assume $\mathcal{U} = \mathbb{Z}_4$

Exists for large $n$ if $\frac{1}{n} \log |\mathcal{C}_1| \geq \log 4 - \min\{H(U|X), 2|H(U|X) - 1|^+\}$

Optimal random code’s size: $H(U) - H(U|X) = I(X; U)$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

Good group source code for $(X, U, P_{XU})$

Assume $U = \mathbb{Z}_4$

Exists for large $n$ if $\frac{1}{n} \log |C_1| \geq \log 4 - \min\{H(U|X), 2|H(U|X) - 1|\}$

Optimal random code’s size: $H(U) - H(U|X) = I(X; U)$

Penalty for imposing group structure
Group Channel codes: Example

- Consider \( \mathbb{Z}_4 = \{0, 1, 2, 3\} \)
- One non-trivial subgroup \( 2\mathbb{Z}_4 = \{0, 2\} \)
Group Channel codes: Example

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$
- Good group channel code for $(\mathcal{I}, \mathcal{J}, P_{ZS})$
Group Channel codes: Example

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$
- Good group channel code for $(\mathcal{I}, \mathcal{I}, P_{\mathcal{I} \mathcal{S}})$
- Assume $\mathcal{I} = \mathbb{Z}_4$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

Good group channel code for $(\mathcal{I}, \mathcal{J}, P_{ZS})$

Assume $\mathcal{I} = \mathbb{Z}_4$

Exists for large $n$ if

$$\frac{1}{n} \log |\mathcal{C}_2| \leq \log 4 - \max\{H(Z|S), 2(H(Z|S) - H([Z]_1|S))\}$$
Group Channel codes: Example

- Consider $\mathbb{Z}_4 = \{0,1,2,3\}$
- One non-trivial subgroup $2\mathbb{Z}_4 = \{0,2\}$
- Good group channel code for $(\mathcal{I}, \mathcal{J}, P_{ZS})$
- Assume $\mathcal{I} = \mathbb{Z}_4$
- Exists for large $n$ if
  \[ \frac{1}{n} \log |\mathcal{C}_2| \leq \log 4 - \max\{H(Z|S), 2(H(Z|S) - H([Z]_1|S))\} \]
- Optimal random code’s size: $\log 4 - H(Z|S)$
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

One non-trivial subgroup $2\mathbb{Z}_4 = \{0, 2\}$

Good group channel code for $(\mathcal{I}, \mathcal{S}, P_{ZS})$

Assume $\mathcal{I} = \mathbb{Z}_4$

Exists for large $n$ if

$$\frac{1}{n} \log |\mathcal{C}_2| \leq \log 4 - \max\{H(Z|S), 2(H(Z|S) - H([Z]_1|S))\}$$

Optimal random code’s size: $\log 4 - H(Z|S)$

Penalty for presence of non-trivial subgroups
Coding Strategy

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

\begin{align*}
\frac{1}{n} \log |\mathcal{C}_{11}| &\geq \log 4 - \\
&\min\{H(U|X), 2|H(U|X) - 1|\} \\
\frac{1}{n} \log |\mathcal{C}_{12}| &\geq \log 4 - \\
&\min\{H(V|Y), 2|H(V|Y) - 1|\} \\
\frac{1}{n} \log |\mathcal{C}_2| &\leq \log 4 - \\
&\max\{H(Z), 2(H(Z) - H([Z]_1))\}
\end{align*}
Achievable Rates

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

\[
R_1 \geq \max\{H(Z), 2(H(Z) - H([Z]_1))\} - \min\{H(U|X), 2|H(U|X) - 1|^+\}
\]

\[
R_2 \geq \max\{H(Z), 2(H(Z) - H([Z]_1))\} - \min\{H(V|Y), 2|H(V|Y) - 1|^+\}
\]

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

are achievable.
Achievable Rates

The set of tuples $\langle R_1, R_2, D \rangle$ that satisfy

$$R_1 \geq \max\{H(Z), 2(H(Z) - H([Z]_1))\} - \min\{H(U|X), 2|H(U|X) - 1|^+\}$$

$$R_2 \geq \max\{H(Z), 2(H(Z) - H([Z]_1))\} - \min\{H(V|Y), 2|H(V|Y) - 1|^+\}$$

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

are achievable.

- More general rate region possible
Group codes vs Berger-Tung based coding

Comparison of the two lower convex envelopes

Reconstruction of XOR with Hamming distortion
Reconstruction of XOR with Hamming distortion

Implies Berger-Tung bound not tight for more than 2 users
Existence of “good” nested lattices - arbitrary finite levels of nesting
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
- Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
- Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
- Nested linear codes recover known rate regions of

D. Krithivasan & S.S. Pradhan (U of M)
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
- Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
- Nested linear codes recover known rate regions of
  - Berger-Tung problem
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
- Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
- Nested linear codes recover known rate regions of
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
Existence of “good” nested lattices - arbitrary finite levels of nesting
Lossless and lossy compression using abelian group codes - achievable rates
Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
Nested linear codes recover known rate regions of
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
  - Yeung-Berger problem
Other results

- Existence of “good” nested lattices - arbitrary finite levels of nesting
- Lossless and lossy compression using abelian group codes - achievable rates
- Nested linear codes achieve Shannon rate-distortion bound for arbitrary discrete sources and additive distortions
- Nested linear codes recover known rate regions of
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
  - Yeung-Berger problem
  - Slepian-Wolf problem, Korner-Marton problem
Future research directions

- Extension of lattice coding schemes to arbitrary continuous sources
Future research directions

- Extension of lattice coding schemes to arbitrary continuous sources
- Construction of practical group codes using LDPC/LDGM codes with iterative decoding
Future research directions

- Extension of lattice coding schemes to arbitrary continuous sources
- Construction of practical group codes using LDPC/LDGM codes with iterative decoding
- Use of structured codes in multi-terminal channel coding problems
Future research directions

- Extension of lattice coding schemes to arbitrary continuous sources
- Construction of practical group codes using LDPC/LDGM codes with iterative decoding
- Use of structured codes in multi-terminal channel coding problems
- Connections between information theory (typicality) and abstract algebra (subgroups)
Future research directions

- Extension of lattice coding schemes to arbitrary continuous sources
- Construction of practical group codes using LDPC/LDGM codes with iterative decoding
- Use of structured codes in multi-terminal channel coding problems
- Connections between information theory (typicality) and abstract algebra (subgroups)
- Codes over non-abelian groups