Toward a New Approach to Distributed Information Processing: Harnessing Group Structure

S. Sandeep Pradhan
(Joint work with Dinesh Krithivasan)

University of Michigan, Ann Arbor

Distributed Information Processing

- Proliferation of wireless sensor network applications
- Supported by distributed information processing
- Look at distributed source coding problems
- Information-theoretic perspective

Information and Coding theory: Traditional Approach

Information Theory:

- Develop efficient information processing strategies for communication
- Obtain computable performance limits
- Random coding: probability distribution on a collection of communication systems
- Show good average performance
- Encoding and decoding have exponential complexity

Information and Coding theory: Traditional Approach

Information Theory:

- Develop efficient information processing strategies for communication
- Obtain computable performance limits
- Random coding: probability distribution on a collection of communication systems
- Show good average performance
- Encoding and decoding have exponential complexity

Coding Theory:

- Approach these limits using structured codes (Ex: linear codes)
- Fast encoding and decoding algorithms
- Objective: use structured codes for practical implementability

Random Coding in multi-terminal systems

- Prob. distribution on a collection of codebooks (ensemble)
- Lot of bad codebooks in the ensemble
- Average performance significantly affected by these bad 'apples'

Random Coding in multi-terminal systems

- Prob. distribution on a collection of codebooks (ensemble)
- Lot of bad codebooks in the ensemble
- Average performance significantly affected by these bad 'apples'
- Algebraic structure can be used to weed out bad 'apples'
- Better ensemble with better performance

Random Coding in multi-terminal systems

- Prob. distribution on a collection of codebooks (ensemble)
- Lot of bad codebooks in the ensemble
- Average performance significantly affected by these bad 'apples'
- Algebraic structure can be used to weed out bad 'apples'
- Better ensemble with better performance
- Gain barely noticeable in point-to-point communication
  - Improvement in second order performance (error exponents)
  - Binary Symmetric case: almost all linear codes achieve expurgated bound without expurgation

Random Coding in multi-terminal systems

- Prob. distribution on a collection of codebooks (ensemble)
- Lot of bad codebooks in the ensemble
- Average performance significantly affected by these bad 'apples'
- Algebraic structure can be used to weed out bad 'apples'
- Better ensemble with better performance
- Gain barely noticeable in point-to-point communication
  - Improvement in second order performance (error exponents)
  - Binary Symmetric case: almost all linear codes achieve expurgated bound without expurgation
- Gains significant in multi-terminal communication

Linear Codes: Built on Galois Fields

Caution: Even in point-to-point set-up

- Linear codes do not achieve in general
  - Shannon rate-distortion function
  - Shannon capacity-cost function

Linear Codes: Built on Galois Fields

Caution: Even in point-to-point set-up

- Linear codes do not achieve in general
  - Shannon rate-distortion function
  - Shannon capacity-cost function
- Injection of some non-linearity appears to be necessary for optimality

Prior Work: Linear codes for multi-terminal communication

- Linear codes for symmetric source/channel coding problems
- Lattice codes for Gaussian source/channel coding problems

Prior Work: Linear codes for multi-terminal communication

- Linear codes for symmetric source/channel coding problems
- Lattice codes for Gaussian source/channel coding problems
- Examples: (incomplete list)
  - Korner-Marton
  - Han-Kobayashi
  - Ahlswede-Han
  - Forney-Barg
  - Philosof-Zamir-Erez
  - Nazer-Gastpar
  - Krithivasan-Pradhan
  - Viswanath
  - ...

Contributions of the present work

- A unified approach to distributed source coding problem
- Discrete memoryless setting
- Applicable to general source statistics and distortion functions

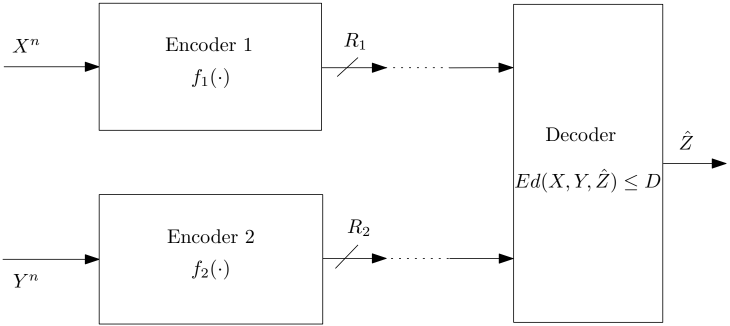
Contributions of the present work

- A unified approach to distributed source coding problem
- Discrete memoryless setting
- Applicable to general source statistics and distortion functions
- Based on abstract abelian groups: groups capture structure
- Nested codes over groups
- New rate-distortion region

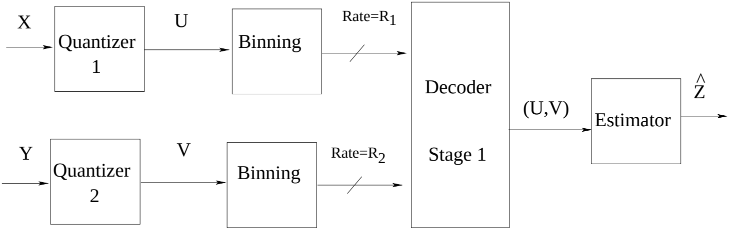
Contributions of the present work

- A unified approach to distributed source coding problem
- Discrete memoryless setting
- Applicable to general source statistics and distortion functions
- Based on abstract abelian groups: groups capture structure
- Nested codes over groups
- New rate-distortion region
- Previously known rate distortion regions can be achieved using nested linear codes

A Distributed Source Coding Problem

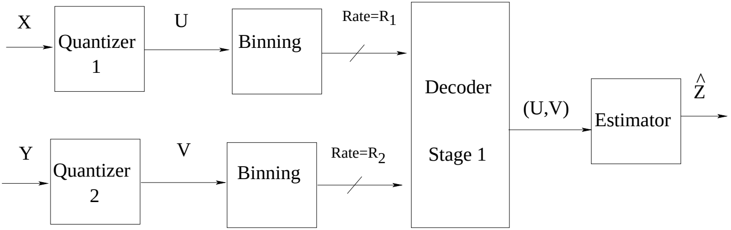


- Set of encoders observe different components of a vector source
- Central decoder receives quantized observations from the encoders
- Best known rate region - Berger-Tung based



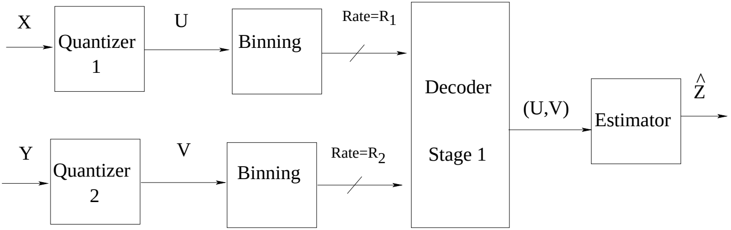
- For given distortion D
- Quantize X to U and quantize Y to V

Berger-Tung Based Rate Region: Known Results



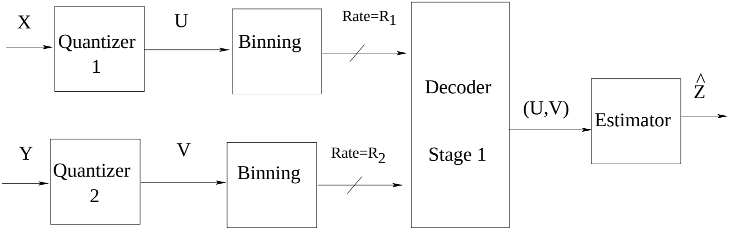
- For given distortion D
- Quantize X to U and quantize Y to V
- Find two quantizer transformations $p_{U|X}$ and $p_{V|Y}$ such that
  - best estimator $\hat{Z} = F(U, V)$ from (U, V) satisfies distortion D.

Berger-Tung Based Rate Region: Known Results



- For given distortion D
- Quantize X to U and quantize Y to V
- Find two quantizer transformations $p_{U|X}$ and $p_{V|Y}$ such that
  - best estimator $\hat{Z} = F(U, V)$ from (U, V) satisfies distortion D.
- Rates incurred in quantization $= I(X; U)$ and $I(Y; V)$

Berger-Tung Based Rate Region: Known Results



- For given distortion D
- Quantize X to U and quantize Y to V
- Find two quantizer transformations $p_{U|X}$ and $p_{V|Y}$ such that
  - best estimator $\hat{Z} = F(U, V)$ from (U, V) satisfies distortion D.
- Rates incurred in quantization $= I(X; U)$ and $I(Y; V)$
- Rate rebate by exploiting correlation between U and $V = I(U; V)$

Berger-Tung Based Rate Region contd.

- Hence

$$
\begin{aligned}
R_1 &\geq I(X;U) - I(U;V) \\
R_2 &\geq I(Y;V) - I(U;V) \\
R_1 + R_2 &\geq I(X;U) + I(Y;V) - I(U;V)
\end{aligned}
$$

- Achieved using random quantization and random binning

Berger-Tung Based Rate Region contd.

- Hence

$$
\begin{aligned}
R_1 &\geq I(X;U) - I(U;V) \\
R_2 &\geq I(Y;V) - I(U;V) \\
R_1 + R_2 &\geq I(X;U) + I(Y;V) - I(U;V)
\end{aligned}
$$

- Achieved using random quantization and random binning
- Observations:
  - Estimator $\hat{Z} = F(U,V)$ may be an information lossy transformation
  - Is it possible to reconstruct directly $\hat{Z}$ at the decoder?
  - Can we get a rate rebate that is greater than $I(U;V)$?

Berger-Tung Based Rate Region contd.

- Hence

$$\begin{aligned} R_1 &\geq I(X;U) - I(U;V) \\ R_2 &\geq I(Y;V) - I(U;V) \\ R_1 + R_2 &\geq I(X;U) + I(Y;V) - I(U;V) \end{aligned}$$

- Achieved using random quantization and random binning
- Observations:
  - Estimator $\hat{Z} = F(U,V)$ may be an information lossy transformation
  - Is it possible to reconstruct directly $\hat{Z}$ at the decoder?
  - Can we get a rate rebate that is greater than $I(U;V)$?
  - Can a joint design of quantizer and binning get better performance?

Example 1

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

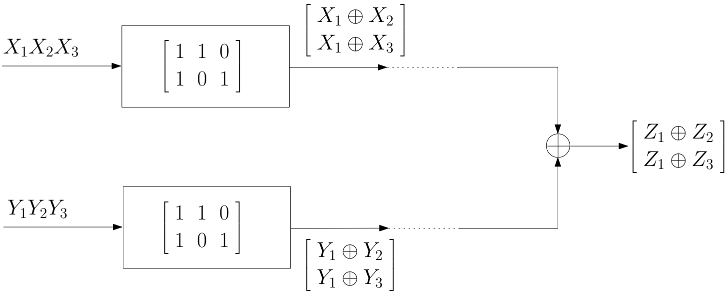
Example 1

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

Example 1

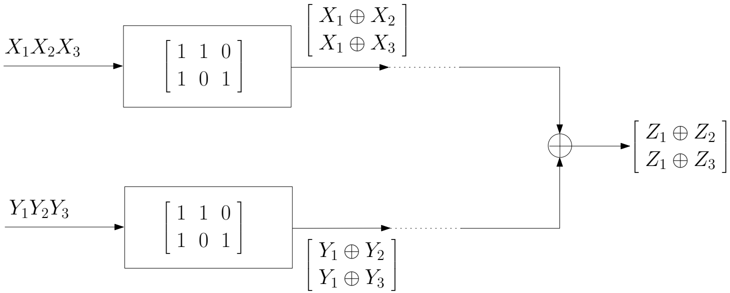
- X, Y - 3 bit correlated binary sources, $d_H(X, Y) \leq 1$
- Decoder interested in reconstructing
  $\hat{Z} = X \oplus_2 Y \in \{000, 001, 010, 100\}$
- Berger-Tung based coding scheme:
  - Reconstruct sources X, Y. Compute $\hat{Z} = X \oplus_2 Y$
  - Sum rate: $H(X, Y) = 5$ bits
- Can we do better?

Example 1: Linear Coding Scheme



- $X_1 \oplus X_2 \oplus Y_1 \oplus Y_2 = X_1 \oplus Y_1 \oplus X_2 \oplus Y_2 = \hat{Z}_1 \oplus \hat{Z}_2$
- Sum rate: $2 + 2 = 4$ bits

Example 1: Linear Coding Scheme



- $X_1 \oplus X_2 \oplus Y_1 \oplus Y_2 = X_1 \oplus Y_1 \oplus X_2 \oplus Y_2 = \hat{Z}_1 \oplus \hat{Z}_2$
- Sum rate: $2 + 2 = 4$ bits
- Significant features:
  - encoding function commutes with function $\hat{Z} = X \oplus Y$
  - Identical binning at both encoders
  - Linear codes

Example 2: Reconstruct the pair (X, Y) (Slepian-Wolf)

- (X, Y) - binary correlated sources

Example 2: Reconstruct the pair (X, Y) (Slepian-Wolf)

- (X, Y) - binary correlated sources
- Can be thought of as addition in $\mathbb{F}_4$

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

- Map binary sources into $\mathbb{F}_4$

Example 2: Reconstruct the pair (X, Y) (Slepian-Wolf)

- (X, Y) - binary correlated sources
- Can be thought of as addition in $\mathbb{F}_4$

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

- Map binary sources into $\mathbb{F}_4$
- Encode sequentially one digit at a time
- Previously decoded digits $=$ side information at the decoder

Example 3: Reconstruct the function $X \vee Y$

- (X, Y) - binary correlated sources

Example 3: Reconstruct the function $X \vee Y$

- (X, Y) - binary correlated sources
- Can be embedded in the addition table in $\mathbb{F}_3$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- Map binary sources into $\mathbb{F}_3$

Example 3: Reconstruct the function $X \vee Y$

- (X, Y) - binary correlated sources
- Can be embedded in the addition table in $\mathbb{F}_3$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- Map binary sources into $\mathbb{F}_3$
- Construct linear codes over $\mathbb{F}_3$
- Can do better than Slepian-Wolf coding

Overview of our Coding Scheme

- Fix test channel $p_{U|X}, p_{V|Y}$

Overview of our Coding Scheme

- Fix test channel $p_{U|X}, p_{V|Y}$
- Function to be reconstructed $F(U, V)$ - embed in the addition table of some abelian group
- Abelian groups decomposable into primary cyclic groups

Overview of our Coding Scheme

- Fix test channel $p_{U|X}, p_{V|Y}$
- Function to be reconstructed $F(U, V)$ - embed in the addition table of some abelian group
- Abelian groups decomposable into primary cyclic groups
- Encode sequentially using nested group codes
- All codes used in encoding have the same algebraic structure

Overview of our Coding Scheme

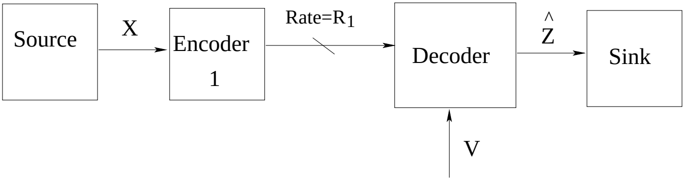
- Fix test channel $p_{U|X}, p_{V|Y}$
- Function to be reconstructed $F(U, V)$ - embed in the addition table of some abelian group
- Abelian groups decomposable into primary cyclic groups
- Encode sequentially using nested group codes
- All codes used in encoding have the same algebraic structure
- Two quantizers and the binning operation is designed jointly
- A framework applicable to arbitrary source statistics and distortion measures

Overview of our Coding Scheme

- Fix test channel $p_{U|X}, p_{V|Y}$
- Function to be reconstructed $F(U, V)$ - embed in the addition table of some abelian group
- Abelian groups decomposable into primary cyclic groups
- Encode sequentially using nested group codes
- All codes used in encoding have the same algebraic structure
- Two quantizers and the binning operation is designed jointly
- A framework applicable to arbitrary source statistics and distortion measures

- We looked at linear codes for binning.
- How to do quantization using structured codes?

Berger-Tung Rate Region: Closer Look



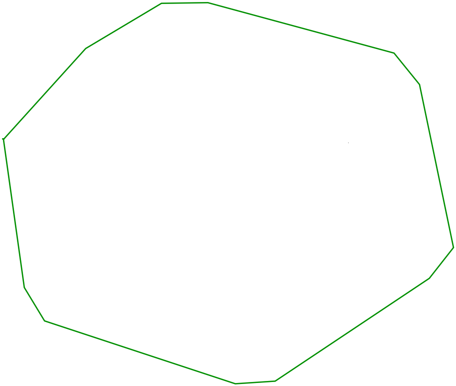
- $R_2 = I(Y;V)$, $\quad R_1 = I(X;U) - I(U;V)$
- Source X: alphabet $\mathcal{X}$, distribution p_X
- Side Information V: alphabet $\mathcal{V}$, distribution $p_{V|X}$.
- Reconstruction: alphabet $\hat{\mathcal{Z}}$.
- Compress X into bits to achieve a target distortion.

Berger-Tung Rate Region Contd.

Encoding: Quantization + Binning

- Quantize X to U with rate $I(X;U)$
- Partition the quantizer into bins of rate $I(U;V)$
- Each bin is a good channel code for the channel $p_{V|U}$.
- Send the bin index to the decoder
- Recover the quantizer codeword from the bin using V.

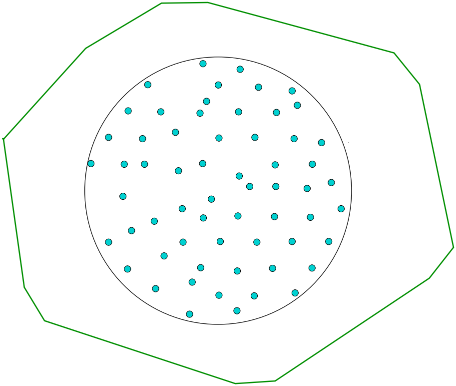
Space in which quantizer is built



- Space: $\mathcal{U}^n$
- Quantizer : X to U

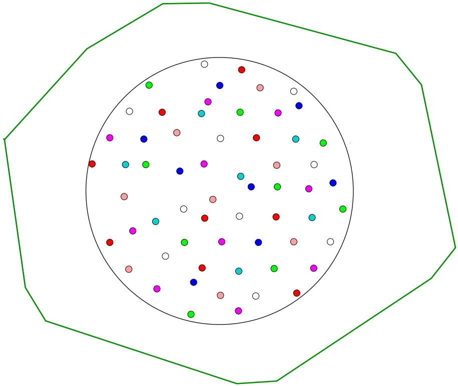
- Joint histogram of source word and its quantized version $\approx p_{XU}$

Good Quantizer



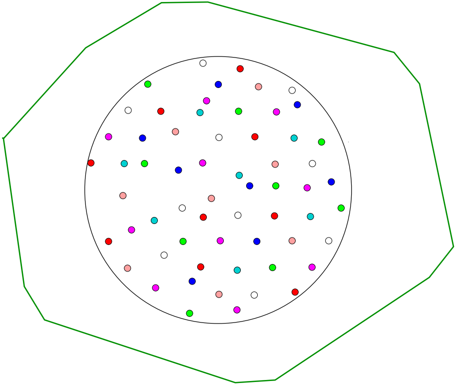
- Quantize X to U
- Must cover a specific region
- Typical set with respect to p_U.
- Rate: $I(X;U)$.
- Shannon source code

Quantizer Partition into bins



- Partition into bins

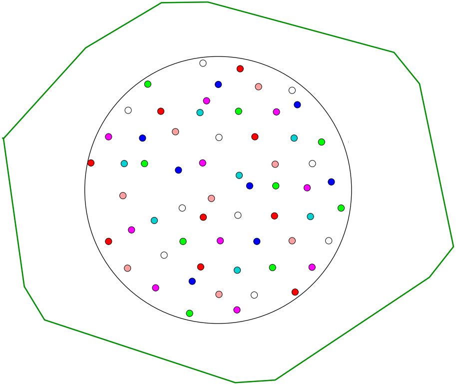
Quantizer Partition into bins



- Partition into bins
- Bin = Good channel code
- Fictitious channel
- 

- I/P Distribution: P_U
- Conditional distribution: $p_{V|U}$.

Quantizer Partition into bins

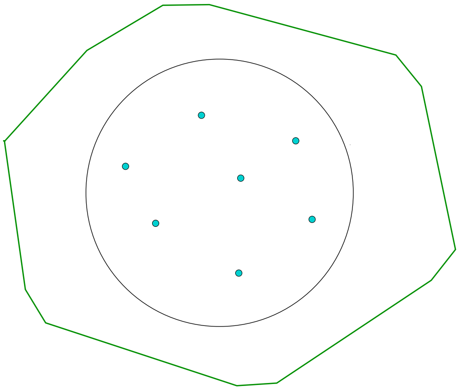


- Partition into bins
- Bin = Good channel code
- Fictitious channel
- 

- I/P Distribution: P_U
- Conditional distribution: $p_{V|U}$.
- Bin Rate: $I(U;V)$.
- Bin density rate:

  $= I(X;U) - I(U;V)$

Good Channel Code



- Each bin is a good channel code
- Pack codewords in the region
- Typical set with respect to U
- Rate: $I(U; V)$.
- Shannon channel code

Illustration of Encoding

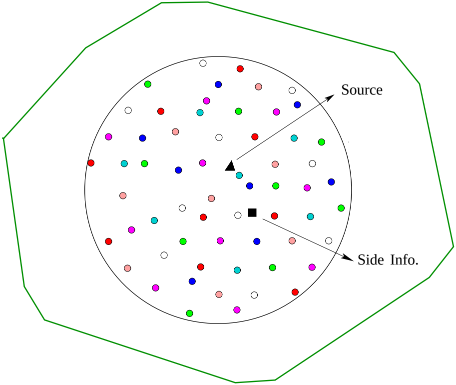


Illustration of Decoding

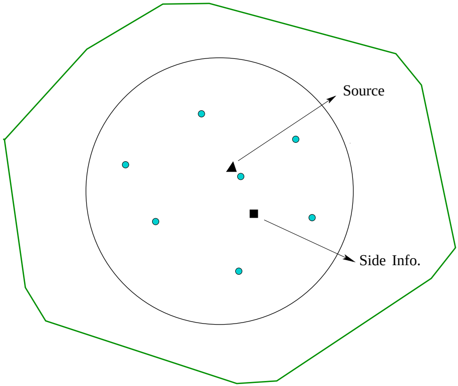
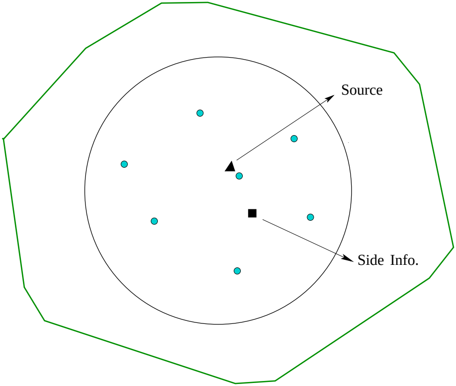


Illustration of Decoding



- None of the codes used here have any algebraic structure

Try this with linear codes

RECALL

- Linear Codes do not achieve
  - Shannon rate-distortion function
  - Shannon capacity-cost function
- Linear code do not achieve
  - the source rate $I(X;U)$
  - the channel rate $I(U;V)$

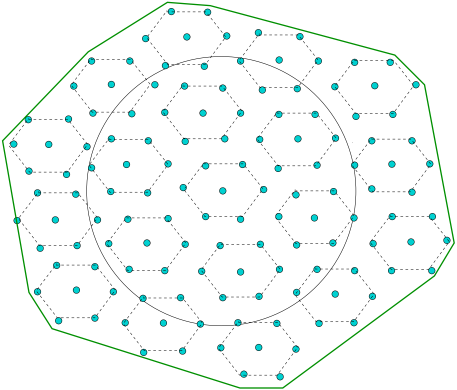
Try this with linear codes

RECALL

- Linear Codes do not achieve
  - Shannon rate-distortion function
  - Shannon capacity-cost function
- Linear code do not achieve
  - the source rate $I(X;U)$
  - the channel rate $I(U;V)$

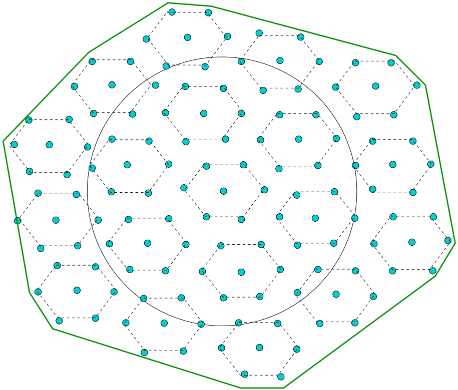
Q: How to achieve $I(X;U) - I(U;V)$ using linear codes?

Linear code as a Quantizer: Lemma 1



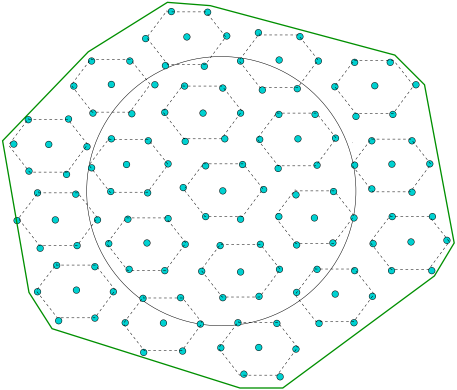
- Linear code $\mathcal{C}_1$

Linear code as a Quantizer: Lemma 1



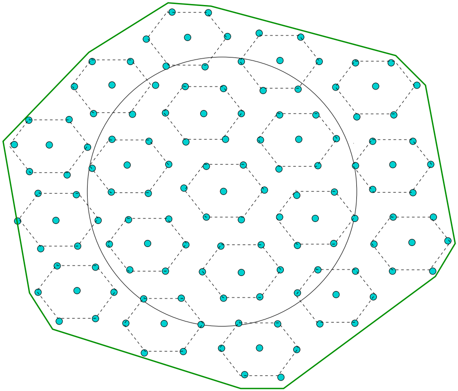
- Linear code $\mathcal{C}_1$
- Contains a good quantizer
- True for arbitrary $(\mathcal{X}, \mathcal{U}, p_{XU})$

Linear code as a Quantizer: Lemma 1



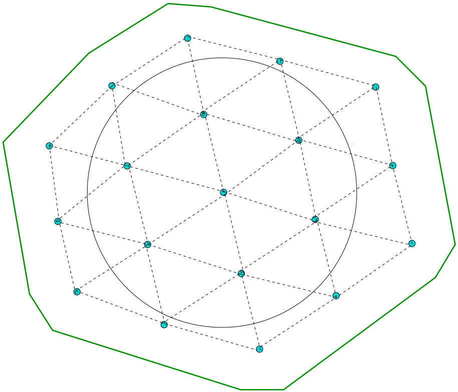
- Linear code $\mathcal{C}_1$
- Contains a good quantizer
- True for arbitrary $(\mathcal{X}, \mathcal{U}, p_{XU})$
- Codeword density as before
- Expand beyond typical set

Linear code as a Quantizer: Lemma 1



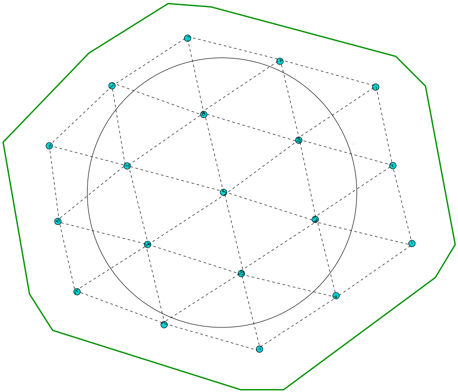
- Linear code $\mathcal{C}_1$
- Contains a good quantizer
- True for arbitrary $(\mathcal{X}, \mathcal{U}, p_{XU})$
- Codeword density as before
- Expand beyond typical set
- Rate of the code:
  $\log |\mathcal{U}| - H(U|X)$
- Penalty for linearity:
  $\log |\mathcal{U}| - H(U)$.
- Refer: Good linear source code

Linear code as a channel code: Lemma 2



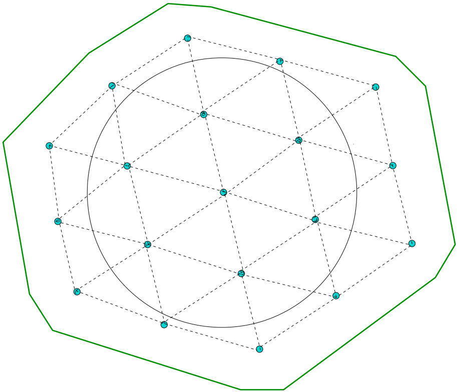
- Linear code $\mathcal{C}_2$
- Every coset contains a good channel code

Linear code as a channel code: Lemma 2



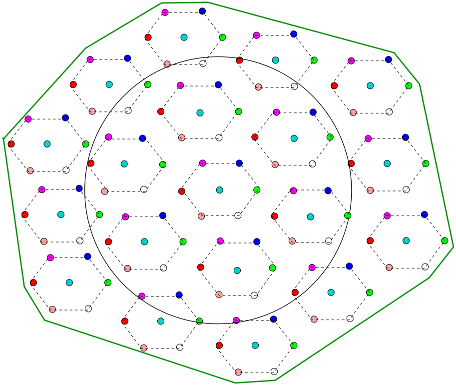
- Linear code $\mathcal{C}_2$
- Every coset contains a good channel code
- True for arbitrary $(\mathcal{U}, \mathcal{V}, p_{UV})$
- Codeword density as before
- Expand beyond typical set

Linear code as a channel code: Lemma 2



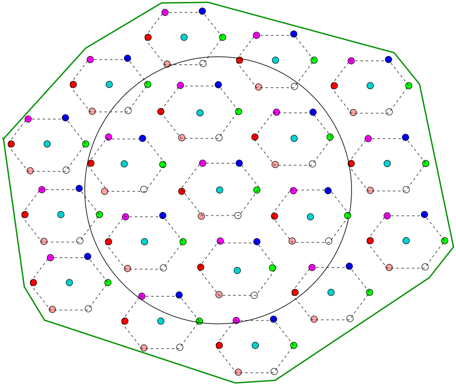
- Linear code $\mathcal{C}_2$
- Every coset contains a good channel code
- True for arbitrary $(\mathcal{U}, \mathcal{V}, p_{UV})$
- Codeword density as before
- Expand beyond typical set
- Rate of the code: $\log|\mathcal{U}| - H(U|V)$
- Penalty for linearity: $\log|\mathcal{U}| - H(U)$
- Refer: Good linear channel code

Linear code Partition



- Partition $\mathcal{C}_1$ into cosets of $\mathcal{C}_2$
- Coset density as before

Linear code Partition



- Partition $\mathcal{C}_1$ into cosets of $\mathcal{C}_2$
- Coset density as before

- Coset density rate

$$= \log|\mathcal{U}| - H(U|X) - \log|\mathcal{U}| + H(U|V)$$
$$= I(X;U) - I(U;V)$$

Linear Codes: Upshot

- Built on Galois fields
- Nested linear codes can achieve Berger-Tung bound
- Good nested linear codes can achieve Shannon limit
  - Take V=constant
  - Source Code Rate: $\log|\mathcal{U}| - H(U|X)$
  - Channel Code Rate: $\log|\mathcal{U}| - H(U)$
- A specific form of non-linearity

Linear Codes: Upshot

- Built on Galois fields
- Nested linear codes can achieve Berger-Tung bound
- Good nested linear codes can achieve Shannon limit
  - Take V=constant
  - Source Code Rate: $\log|\mathcal{U}| - H(U|X)$
  - Channel Code Rate: $\log|\mathcal{U}| - H(U)$
- A specific form of non-linearity

Next: extension to arbitrary abelian groups

Groups - An Introduction

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

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

- Call g_i as the ith digit of g

Groups - An Introduction

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

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

- Call g_i as the ith digit of g
- Enough to prove coding theorems for primary cyclic groups
- Extension to arbitrary abelian groups through digit decomposition

Example 4:

- Let group size be 36
- $36 = 2^2 \times 3^2$
- Abelian groups of order 36:
  - $\mathbb{Z}_4 \times \mathbb{Z}_9$: Two digits
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$: Three digits
  - $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$: Three digits
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$: Four digits

Embedding a function in a group G

A function $F : \mathcal{U} \times \mathcal{V} \to \hat{\mathcal{Z}}$ can be embedded in G if

Embedding a function in a group G

A function $F : \mathcal{U} \times \mathcal{V} \rightarrow \hat{\mathcal{Z}}$ can be embedded in G if

- $\exists$ a one-to-one mapping $F_1 : \mathcal{U} \rightarrow G$
- $\exists$ a one-to-one mapping $F_2 : \mathcal{V} \rightarrow G$
- $\exists$ a mapping $F_3 : G \rightarrow \hat{\mathcal{Z}}$
- such that $F(U, V) = F_3 \left[F_1(U) \oplus_G F_2(V) \right]$

Embedding a function in a group G

A function $F : \mathcal{U} \times \mathcal{V} \to \hat{\mathcal{Z}}$ can be embedded in G if

- $\exists$ a one-to-one mapping $F_1 : \mathcal{U} \to G$
- $\exists$ a one-to-one mapping $F_2 : \mathcal{V} \to G$
- $\exists$ a mapping $F_3 : G \to \hat{\mathcal{Z}}$
- such that $F(U,V) = F_3\left[F_1(U) \oplus_G F_2(V)\right]$

Example: $\hat{Z} = U \vee V$ can be embedded in $\mathbb{Z}_3$

Nested Group Codes - Motivation

- Codes used in KM,SW - good channel codes
  - Cosets bin the entire space
  - Suitable for lossless coding

Nested Group Codes - Motivation

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

Nested Group Codes

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

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 $\phi\colon \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ 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 $\phi\colon \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$
- $(\mathcal{C}_1, \mathcal{C}_2)$ nested if $\mathcal{C}_2 \subset \mathcal{C}_1$
- 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 distinguish between typical channel noise sequences

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 $r > 0$

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

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

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: $H(U) - H(U|X) = I(X;U)$
- Compare with linear code: $\log p^r - H(U|X)$
- Not good in Shannon sense
- Extra penalty for imposing group structure beyond linearity

Good Group Channel Codes

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

Good Group Channel Codes

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

Lemma

Exists for large n if

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

Good Group Channel Codes

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

Lemma

Exists for large n if

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

- $[U]_i$ is a function of U.
- Compare with optimal random code: $H(U) - H(U|V)$
- Compare with linear code: $\log p^r - H(U|V)$
- Not good in Shannon sense
- Extra penalty for imposing group structure beyond linearity

Proof Technique

- Matrix characterization of subgroups of direct product of a group
- random coding over subgroups
- Suen's inequality [1998]

Coding Approach: 5 steps

Fix $p_{U|X}, p_{V|Y}$ such that $\mathbb{E}d(X, Y, F(U, V)) \leq D$

Coding Approach: 5 steps

Fix $p_{U|X}, p_{V|Y}$ such that $\mathbb{E}d(X, Y, F(U, V)) \leq D$

- Step 1: Embed $F(U, V)$ in an abelian group G
- Step 2: Decompose G into primary cyclic groups: $G_1, \ldots, G_K$
  - Represent $U = (U_1, \ldots, U_K)$ and $V = (V_1, \ldots, V_K)$

Coding Approach: 5 steps

Fix $p_{U|X}, p_{V|Y}$ such that $\mathbb{E}d(X, Y, F(U, V)) \leq D$

- Step 1: Embed $F(U, V)$ in an abelian group G
- Step 2: Decompose G into primary cyclic groups: $G_1, \ldots, G_K$
  - Represent $U = (U_1, \ldots, U_K)$ and $V = (V_1, \ldots, V_K)$
- Step 3: Group source code over G_i for every i: $\mathcal{C}_{11}(i)$, $\mathcal{C}_{12}(i)$
- Step 4: Group channel code over G_i for every i: $\mathcal{C}_2(i)$

Coding Approach: 5 steps

Fix $p_{U|X}, p_{V|Y}$ such that $\mathbb{E}d(X, Y, F(U, V)) \leq D$

- Step 1: Embed $F(U, V)$ in an abelian group G
- Step 2: Decompose G into primary cyclic groups: $G_1, \ldots, G_K$
  - Represent $U = (U_1, \ldots, U_K)$ and $V = (V_1, \ldots, V_K)$
- Step 3: Group source code over G_i for every i: $\mathcal{C}_{11}(i)$, $\mathcal{C}_{12}(i)$
- Step 4: Group channel code over G_i for every i: $\mathcal{C}_2(i)$
- Step 5: Nest the channel code inside the source codes
  - $\mathcal{C}_2(i) < \mathcal{C}_{11}(i)$ and $\mathcal{C}_2(i) < \mathcal{C}_{12}(i)$
  - Identical binning of quantizers

Encoding and Decoding

Encoders: at the ith stage

- Encode the sources X and Y to digits U_i and V_i sequentially
  - quantize + bin

Encoding and Decoding

Encoders: at the ith stage

- Encode the sources X and Y to digits U_i and V_i sequentially
  - quantize + bin

Decoder: at the ith stage

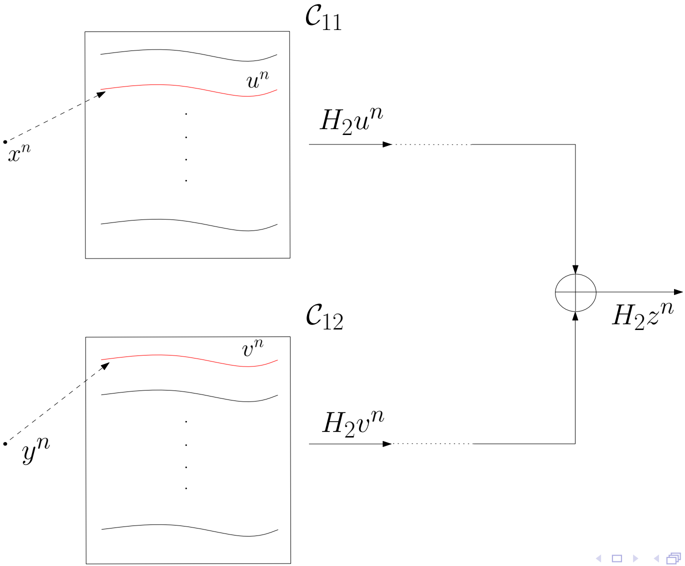
- Recover $\hat{Z}_i = U_i \oplus_{G_i} V_i$
- Use previously decoded digits as side information

Example 5

Suppose we embed $F(U, V)$ in $\mathbb{Z}_4 \times \mathbb{Z}_7$

- We have two digits: $(U_1, V_1, \hat{Z}_1)$ and $(U_2, V_2, \hat{Z}_2)$
- Two stages
- Stage 1: $\mathbb{Z}_4$ operation
- Stage 2: $\mathbb{Z}_7$ operation

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



Achievable Rates

Theorem

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

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

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

$$D \geq \mathbb{E} d(X, Y, F(U, V))$$

are achievable.

Achievable Rates

Theorem

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

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

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

$$D \geq \mathbb{E} d(X, Y, F(U, V))$$

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy at ith stage - Encode (U_i, V_i) instead of $\hat{Z}_i$

Example 6: Lossless reconstruction of quaternary function

- X and Y take values in $\{0, 1, 2, 3\}$
- Lossless reconstruction of $\hat{Z} = X - Y \mod 4$

Example 6: Lossless reconstruction of quaternary function

- X and Y take values in $\{0, 1, 2, 3\}$
- Lossless reconstruction of $\hat{Z} = X - Y \bmod 4$
- Can be embedded in abelian groups of order ≤ 16
- $\mathbb{Z}_4,\ \mathbb{Z}_7,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4 \oplus \mathbb{Z}_4$ give non-trivial performance

Example 6: Lossless reconstruction of quaternary function

- X and Y take values in $\{0, 1, 2, 3\}$
- Lossless reconstruction of $\hat{Z} = X - Y \mod 4$
- Can be embedded in abelian groups of order ≤ 16
- $\mathbb{Z}_4, \mathbb{Z}_7, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_4 \oplus \mathbb{Z}_4$ give non-trivial performance

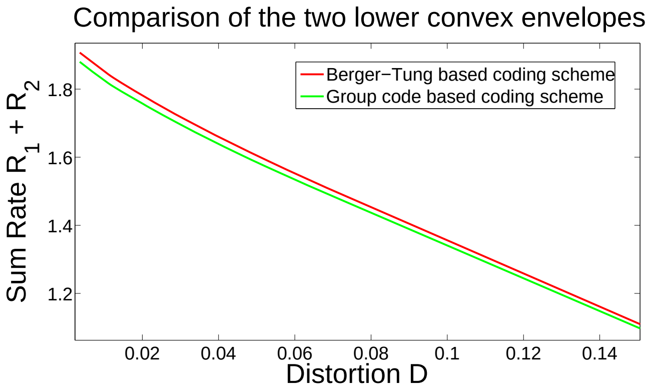
p_X	p_E	$R_{\mathbb{Z}_4}$	$R_{\mathbb{Z}_7}$	$R_{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2}$	$R_{\mathbb{Z}_4 \oplus \mathbb{Z}_4}$
$[\frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}]$	$[\frac{1}{2}\ 0\ \frac{1}{4}\ \frac{1}{4}]$	3	3.9056	3.1887	3.5
$[\frac{3}{10}\ \frac{6}{10}\ \frac{1}{10}\ 0]$	$[0\ \frac{4}{5}\ \frac{1}{20}\ \frac{3}{20}]$	2.3911	2.0797	2.4529	2.1796
$[\frac{1}{3}\ \frac{1}{10}\ \frac{1}{2}\ \frac{1}{15}]$	$[\frac{3}{7}\ \frac{1}{7}\ \frac{1}{7}\ \frac{2}{7}]$	3.6847	4.5925	3.3495	3.4633
$[\frac{9}{10}\ \frac{1}{30}\ \frac{1}{30}\ \frac{1}{30}]$	$[\frac{3}{20}\ \frac{3}{4}\ \frac{1}{20}\ \frac{1}{20}]$	2.308	2.7065	1.9395	1.7815

Table: Example distributions for which embedding in a given group gives the lowest sum rate.

Example 7: Lossy Reconstruction of binary XOR

- Correlated binary sources (X, Y)
- Reconstruct $\hat{Z} = X \oplus_2 Y$ within Hamming distortion D
- U, V - binary auxiliary random variables
- $F(U, V)$ - one of 16 possibilities depending on $(p_{U|X}, p_{V|Y})$

Lossy Example contd.



- Rate gains over the Berger-Tung based scheme
- Implies Berger-Tung inner bound not tight for three-user case

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
  - Berger-Tung problem
  - Wyner-Ziv problem, Wyner-Ahlswede-Korner problem
  - Yeung-Berger problem
  - Slepian-Wolf problem, Korner-Marton problem

Conclusions

- Presented a nested group codes based coding scheme
- Recovered known rate regions of several distributed source coding problems
- Offers rate gains over the Berger-Tung based coding scheme
- Extensions:
  - Codes over groups for multi-user channel coding problems
  - Codes over non-abelian groups