Algebraic Structures for Multi-Terminal Communications

Dinesh Krithivasan

University of Michigan

Oral Defense

Thesis Outline

1. Lattice codes and Gaussian sources (Chap. 2)

2. Group codes and discrete sources (Chap. 3)

Thesis Outline

1. Lattice codes and Gaussian sources (Chap. 2)
   - Reconstructing linear function of the sources
   - Existence of "good" nested lattice codes
   - New rate region - better for certain parameters
2. Group codes and discrete sources (Chap. 3)

Thesis Outline

1. Lattice codes and Gaussian sources (Chap. 2)
   - Reconstructing linear function of the sources
   - Existence of “good” nested lattice codes
   - New rate region - better for certain parameters
2. Group codes and discrete sources (Chap. 3)
   - Reconstructing arbitrary function of the sources
   - Existence of “good” group codes
   - Unified rate region for many problems

Thesis Outline

1. Lattice codes and Gaussian sources (Chap. 2)
   - Reconstructing linear function of the sources
   - Existence of "good" nested lattice codes
   - New rate region - better for certain parameters
2. Group codes and discrete sources (Chap. 3)
   - Reconstructing arbitrary function of the sources
   - Existence of "good" group codes
   - Unified rate region for many problems

Presentation Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought
  - Try to attain random code performance using them
  - Usually poorer performance. Low complexity

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought
  - Try to attain random code performance using them
  - Usually poorer performance. Low complexity

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought
  - Try to attain random code performance using them
  - Usually poorer performance. Low complexity

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought
  - Try to attain random code performance using them
  - Usually poorer performance. Low complexity

Coding: Structured vs Unstructured

- Information theory - random unstructured codes ubiquitous
  - Shannon's original proofs based on random codes
  - Good performance. Exponential complexity
- Structured codes - usually an afterthought
  - Try to attain random code performance using them
  - Usually poorer performance. Low complexity

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
  - No loss in performance vs unstructured codes in point-to-point setting
  - Performance gains in multi-terminal settings
- Existence proofs for "good" nested structured codes
- One application of this framework

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
    - No loss in performance vs unstructured codes in point-to-point setting
    - Performance gains in multi-terminal settings
- Existence proofs for "good" nested structured codes
- One application of this framework

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
  - No loss in performance vs unstructured codes in point-to-point setting
  - Performance gains in multi-terminal settings
- Existence proofs for “good” nested structured codes
- One application of this framework

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
  - No loss in performance vs unstructured codes in point-to-point setting
  - Performance gains in multi-terminal settings
- Existence proofs for “good” nested structured codes
- One application of this framework
  - Distributed source coding

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
  - No loss in performance vs unstructured codes in point-to-point setting
  - Performance gains in multi-terminal settings
- Existence proofs for "good" nested structured codes
- One application of this framework
  - Distributed source coding

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
  - No loss in performance vs unstructured codes in point-to-point setting
  - Performance gains in multi-terminal settings
- Existence proofs for "good" nested structured codes
- One application of this framework
  - Distributed source coding

Thesis Highlights

- Unified way to use structured codes in many problems
- Nesting of one linear code inside another
    - No loss in performance vs unstructured codes in point-to-point setting
    - Performance gains in multi-terminal settings
- Existence proofs for “good” nested structured codes
- One application of this framework
    - Distributed source coding

Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Information Theory:An Introduction

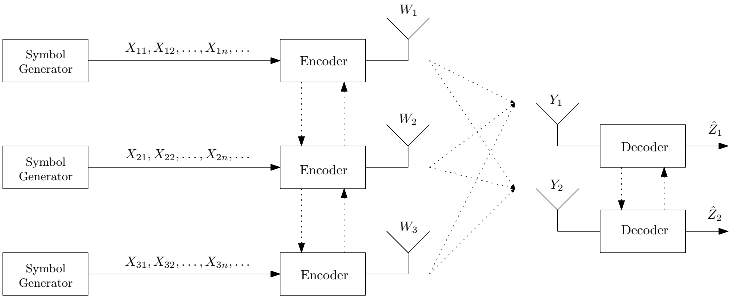
- Mathematical theory of information transmission

Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.

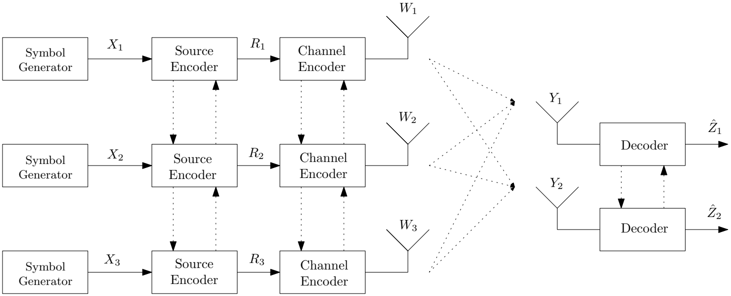
Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.
- Big picture: Transmit stochastic sources over noisy channels



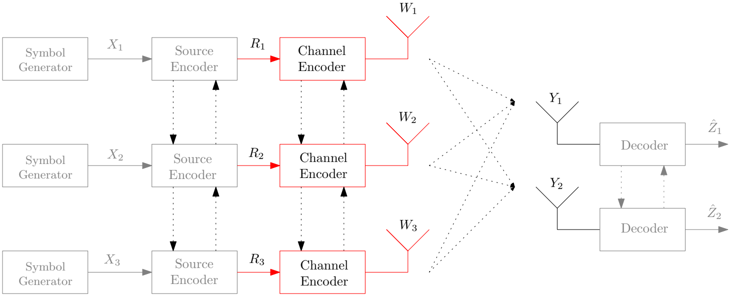
Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.
- Split into modules. Shannon's source channel separation



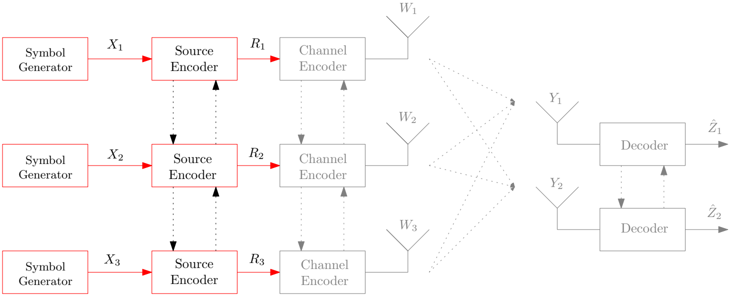
Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.
- Channel coding. Stochastic channels



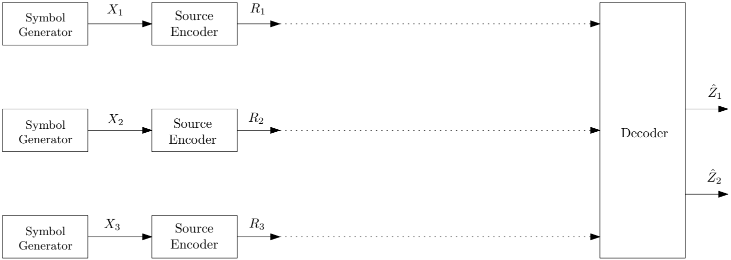
Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.
- Source coding. Stochastic sources.

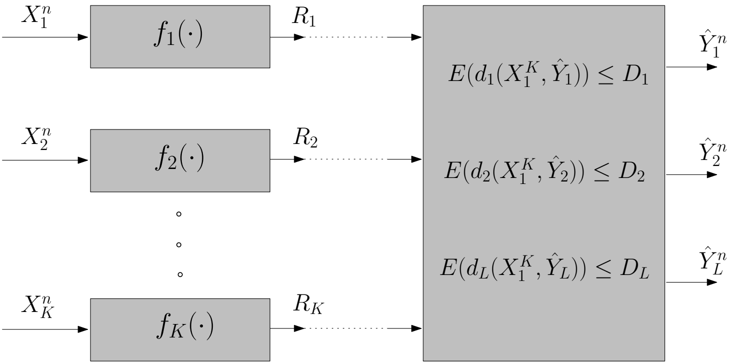


Information Theory:An Introduction

- Mathematical theory of information transmission
- Quantitative measure of information - entropy, mutual information etc.
- Distributed source coding. Sensor networks

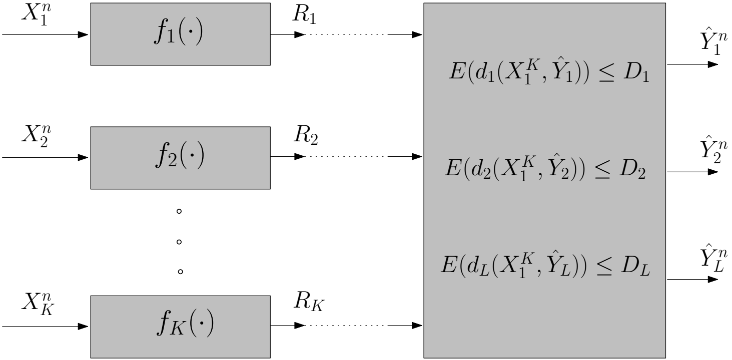


Distributed Source Coding



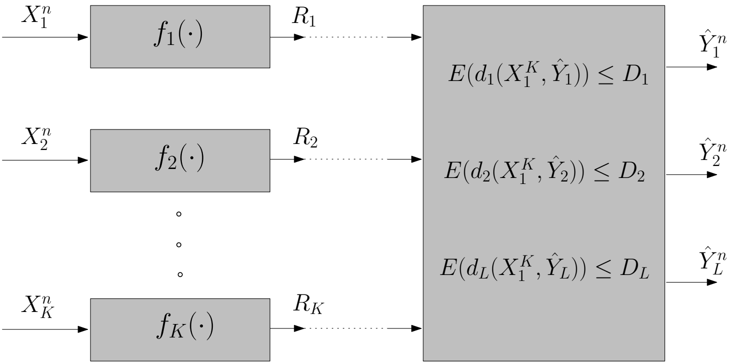
- $X_1, X_2, \ldots, X_K$ - Correlated across space, independent across time

Distributed Source Coding



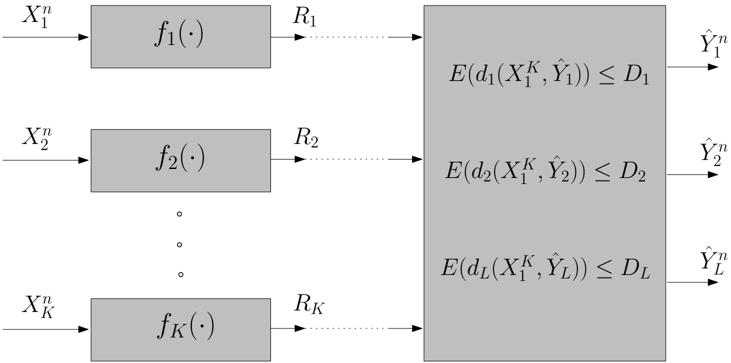
- Encoders $f_i : \mathscr{X}_i^n \to \{1, 2, \ldots, 2^{nR_i}\}, i = 1, \ldots, K$

Distributed Source Coding



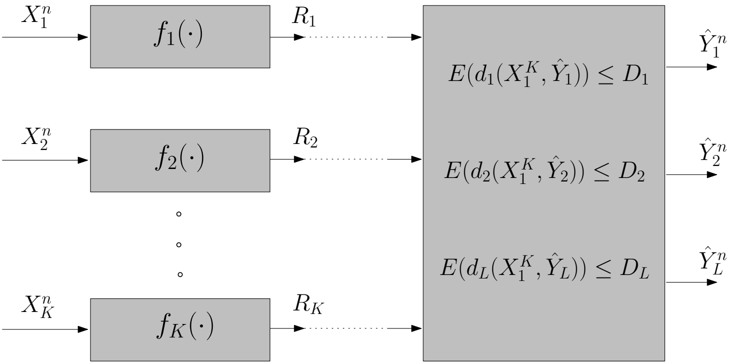
- Rate distortion region $\mathscr{R}\mathscr{D}$: set of achievable $(R_1,\ldots,R_K,D_1,\ldots D_L)$

Distributed Source Coding



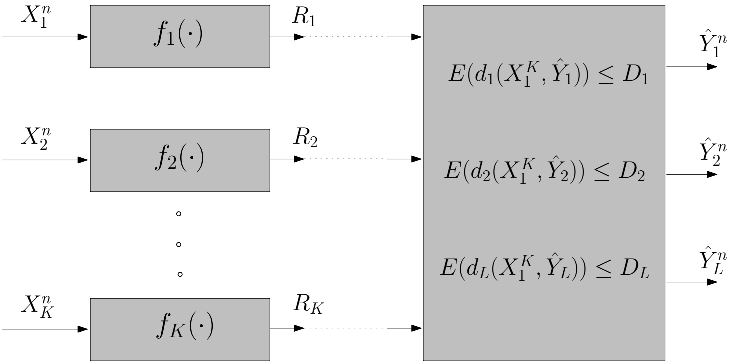
- Goal: Characterize $\mathscr{RD}$ using single-letter information quantities

Distributed Source Coding



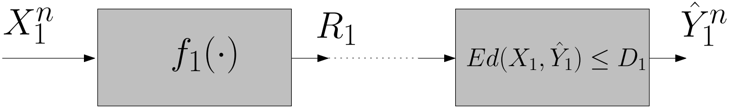
- Goal: Characterize $\mathscr{RD}$ using single-letter information quantities
  - Very hard to solve completely

Distributed Source Coding

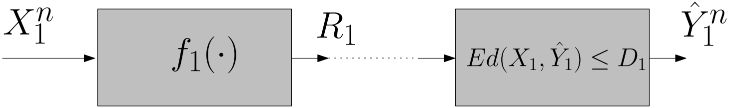


- Goal: Characterize $\mathscr{RD}$ using single-letter information quantities
  - Very hard to solve completely
  - Provide computable inner bounds

Single user source coding



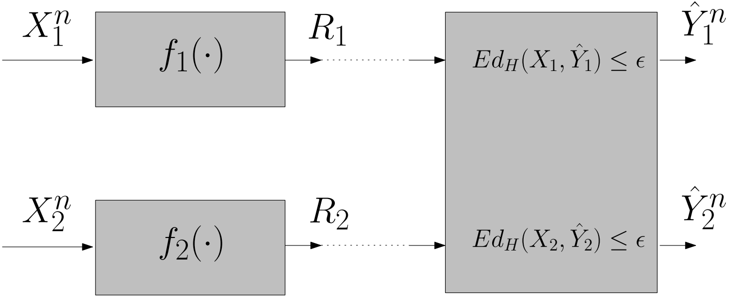
Single user source coding



- Solved completely by Shannon

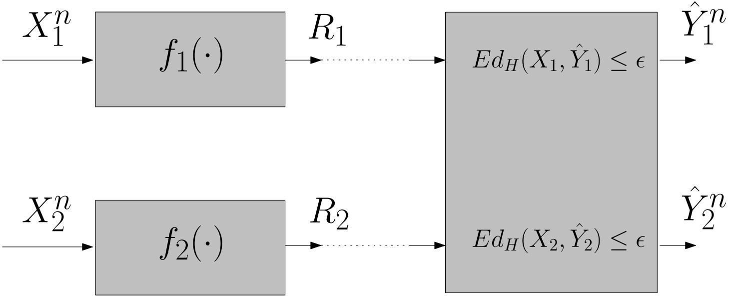
$$R_1 \geq \min_{p_{\hat{Y}_1|X_1} : \, \mathbb{E}d(X_1, \hat{Y}_1) \leq D_1} I(X_1; \hat{Y}_1)$$

Slepian-Wolf problem



- Lossless reconstruction of both sources

Slepian-Wolf problem

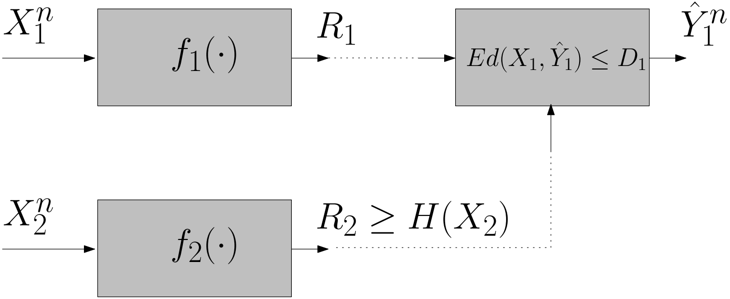


- Lossless reconstruction of both sources

$$R_1 \geq H(X|Y),\ R_2 \geq H(Y|X)$$

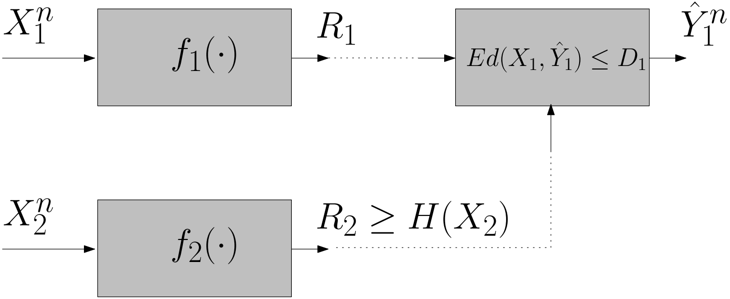
$$R_1 + R_2 \geq H(X, Y)$$

Wyner-Ziv problem



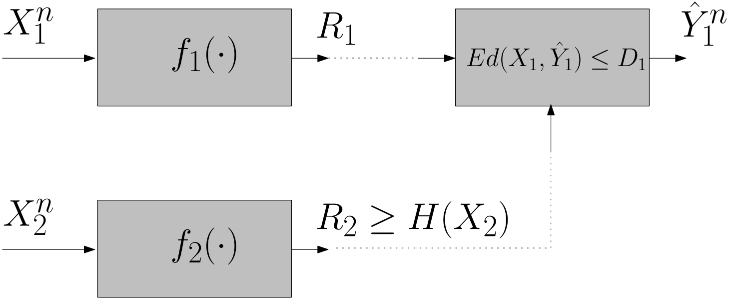
- Lossy reconstruction with decoder side information

Wyner-Ziv problem



- Lossy reconstruction with decoder side information
- Auxiliary random variable U with Markov chain $U - X_1 - X_2$

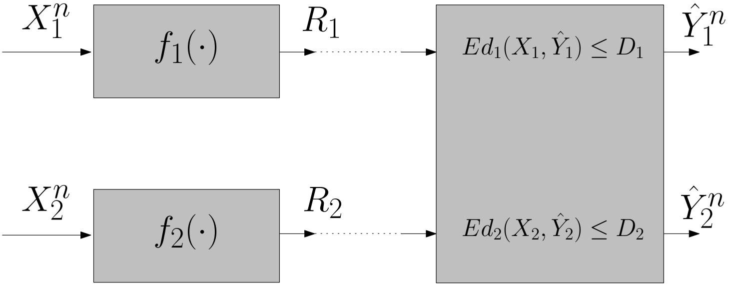
Wyner-Ziv problem



- Lossy reconstruction with decoder side information
- Auxiliary random variable U with Markov chain $U - X_1 - X_2$

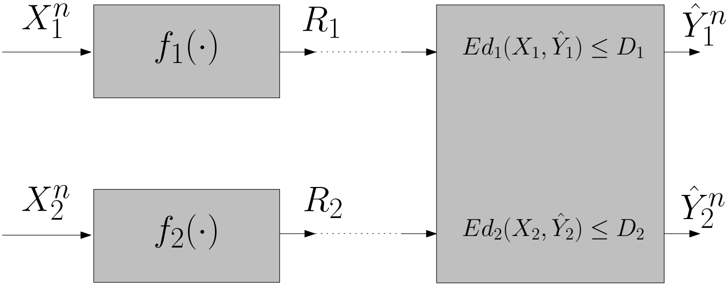
$$R_1 \geq I(X_1; U \mid X_2) = I(X_1; U) - I(X_2; U)$$

Berger-Tung problem



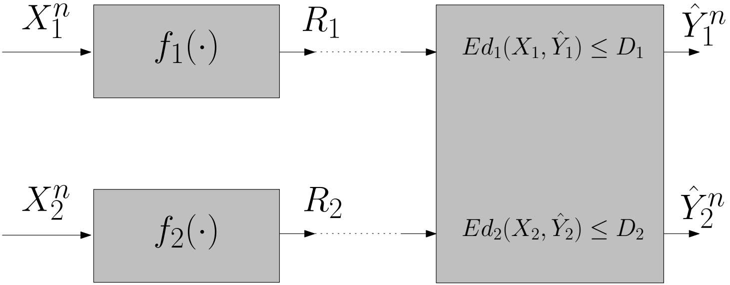
- Independent distortion criteria

Berger-Tung problem



- Auxiliary random variables U, V with $U - X_1 - X_2 - V$

Berger-Tung problem



- Inner bound (tightness not known in general):

$$R_1 \geq I(X_1; U \mid X_2),\ R_2 \geq I(X_2; V \mid X_1)$$

$$R_1 + R_2 \geq I(X_1 X_2; UV)$$

Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Typical proof techniques

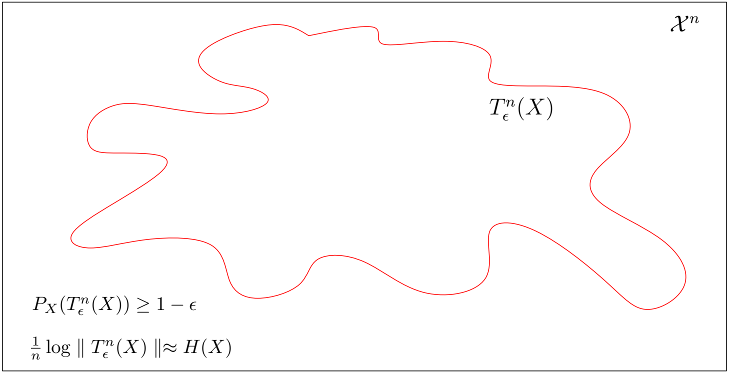
- Two parts to all problems - achievability and converse

Typical proof techniques

- Two parts to all problems - achievability and converse
- Achievability proofs: Operations on the typical set

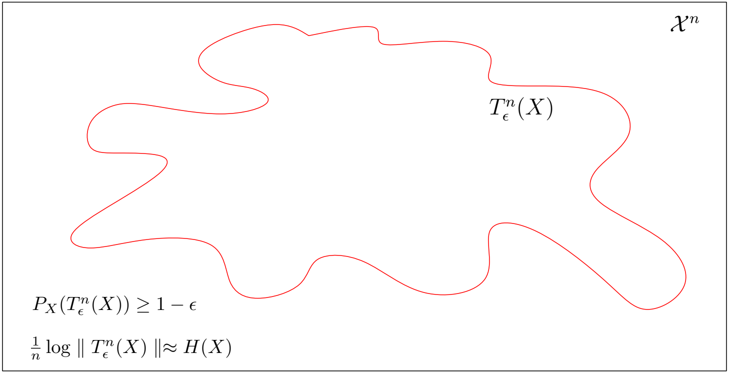
Typical proof techniques

- Two parts to all problems - achievability and converse
- Achievability proofs: Operations on the typical set
- Typical set: Set of probabilistically significant sequences



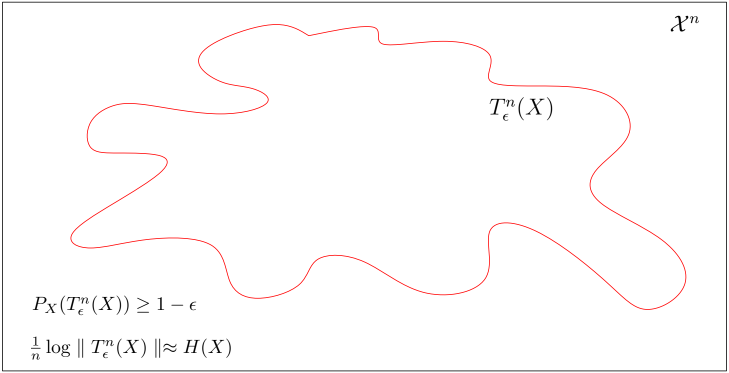
Typical proof techniques

- Two parts to all problems - achievability and converse
- Achievability proofs: Operations on the typical set
- Very complex. No low-dimensional characterization

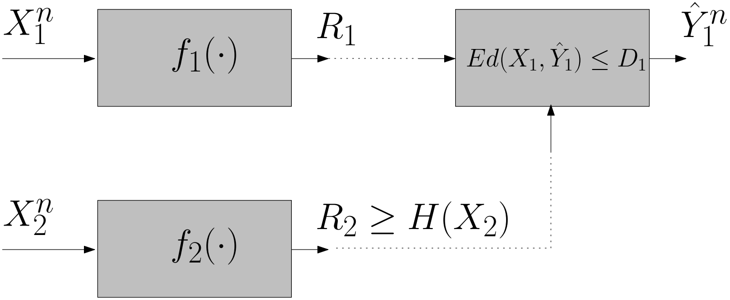


Typical proof techniques

- Two parts to all problems - achievability and converse
- Achievability proofs: Operations on the typical set
- Quantization (source coding) and binning (channel coding)

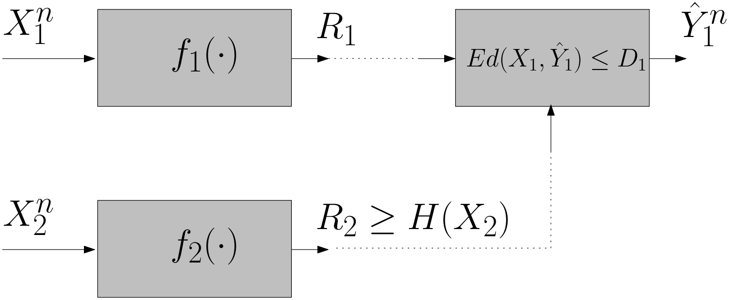


Wyner-Ziv problem - Revisited



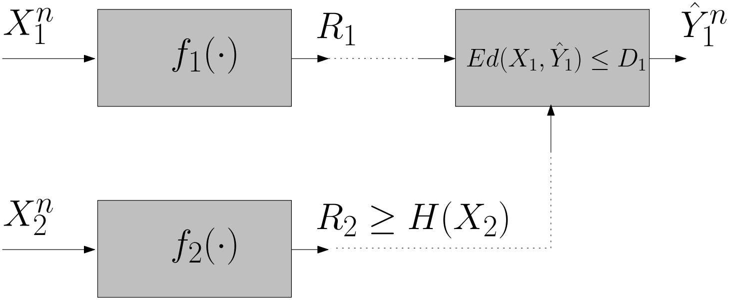
- First to use auxiliary random variable

Wyner-Ziv problem - Revisited



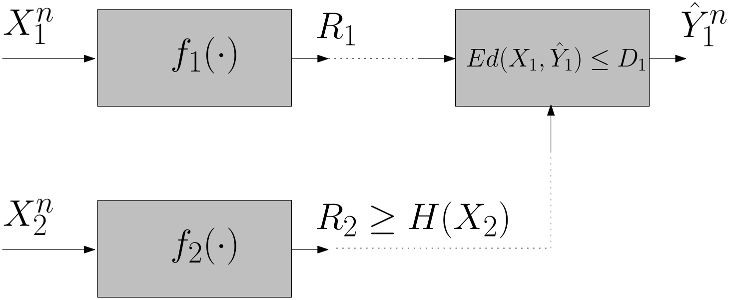
- Encoder does not know X_2: Markov chain $U - X_1 - X_2$

Wyner-Ziv problem - Revisited



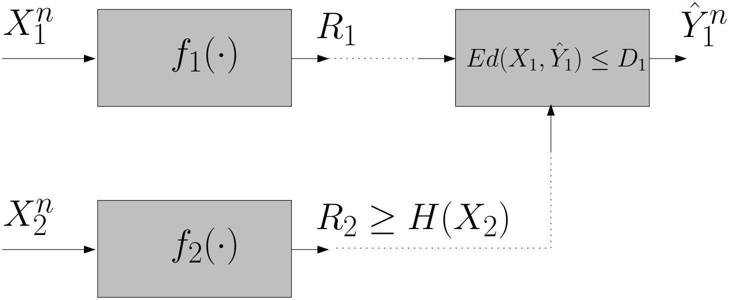
- Encoder does not know X_2: Markov chain $U - X_1 - X_2$
- Combines aspects of both source and channel coding

Wyner-Ziv problem - Revisited



- Encoder does not know X_2: Markov chain $U - X_1 - X_2$
- Combines aspects of both source and channel coding
  - Source coding: Quantize X_1 to U

Wyner-Ziv problem - Revisited



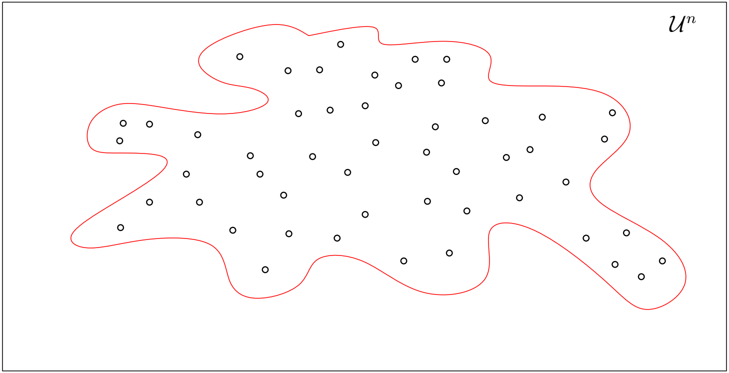
- Encoder does not know X_2: Markov chain $U - X_1 - X_2$
- Combines aspects of both source and channel coding
  - Source coding: Quantize X_1 to U
  - Channel coding: Decode U at decoder using X_2

Quantization - Good source codes

- Quantize X_1 to U for a fixed $P_{U|X_1}$

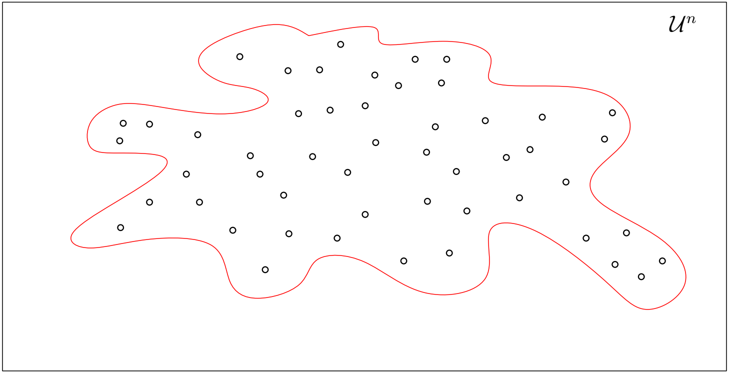
Quantization - Good source codes

- Quantize X_1 to U for a fixed $P_{U|X_1}$
- Codebook $\mathscr{C}$ built from typical set of U



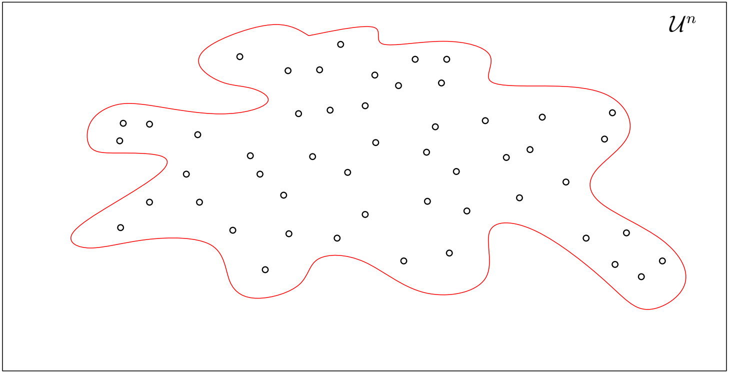
Quantization - Good source codes

- Quantize X_1 to U for a fixed $P_{U|X_1}$
- Code must "cover" typical set of X_1 well



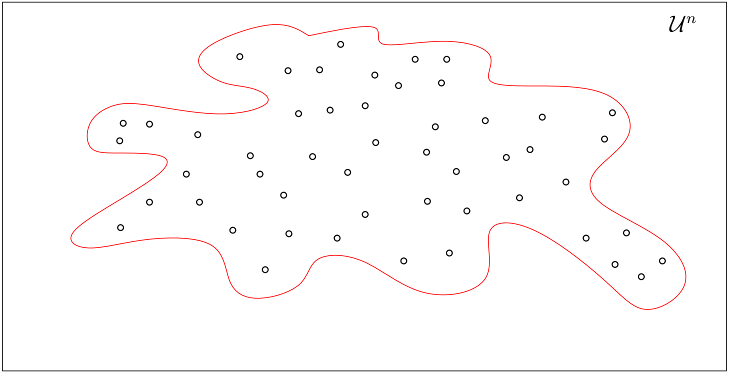
Quantization - Good source codes

- Quantize X_1 to U for a fixed $P_{U|X_1}$
- Size of good code book: $I(X_1;U)$



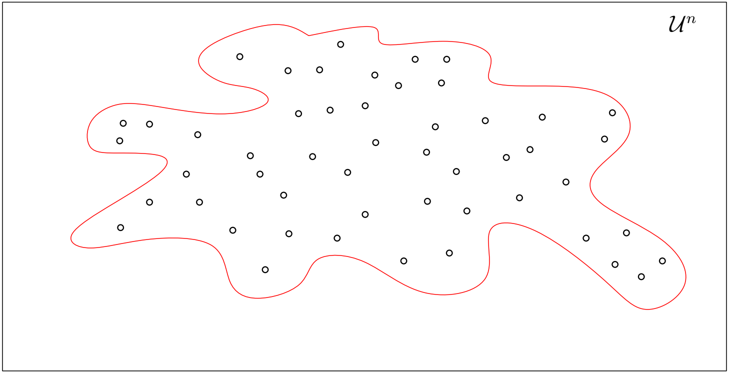
Quantization - Good source codes

- Quantize X_1 to U for a fixed $P_{U|X_1}$
- Codewords chosen at random. No structure.



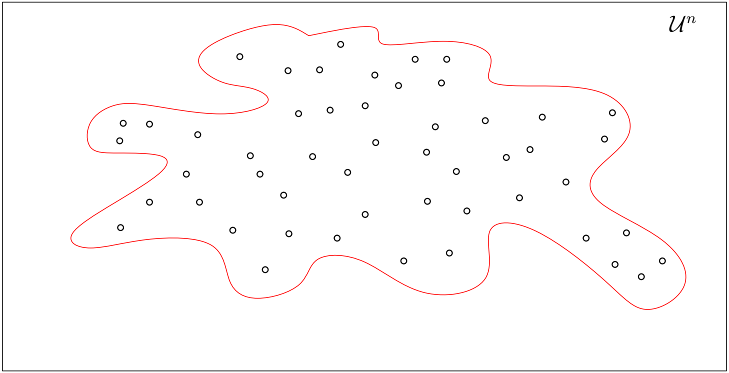
Binning - Good channel codes

- Suppose X_1 already quantized to U



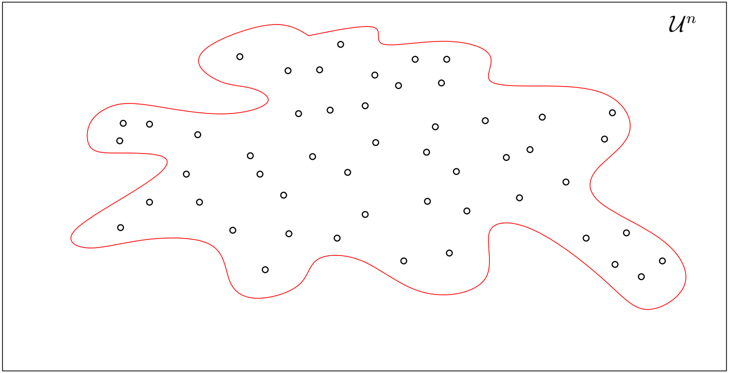
Binning - Good channel codes

- Decoder knows X_2 correlated to U



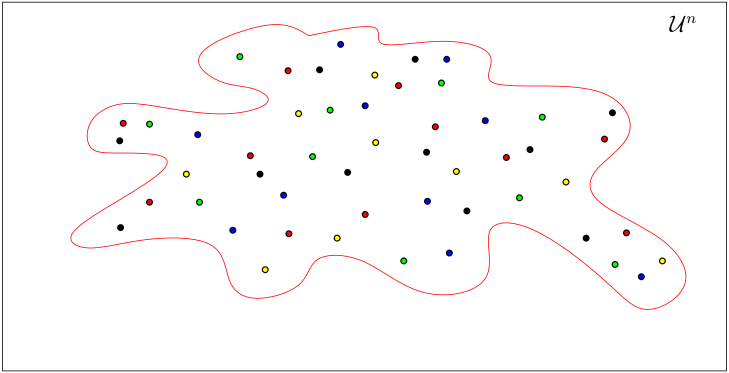
Binning - Good channel codes

- Can this side information be exploited?



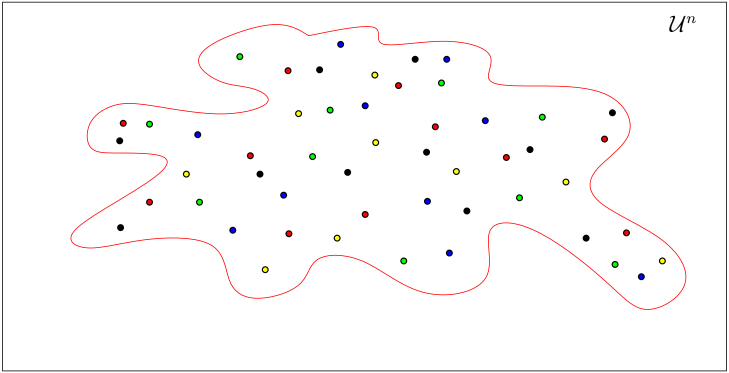
Binning - Good channel codes

- Bin the codewords - Transmit only bin index



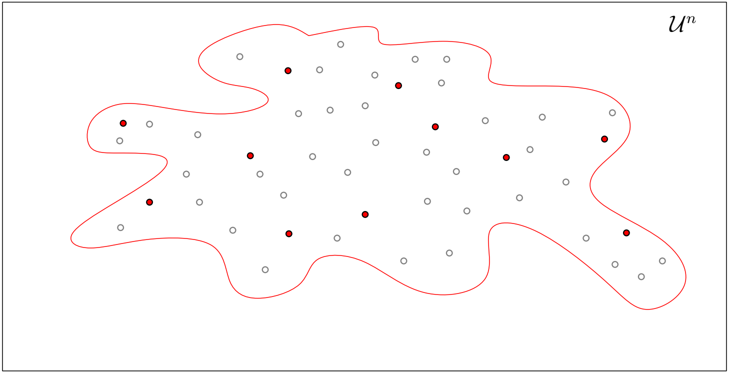
Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Each bin:



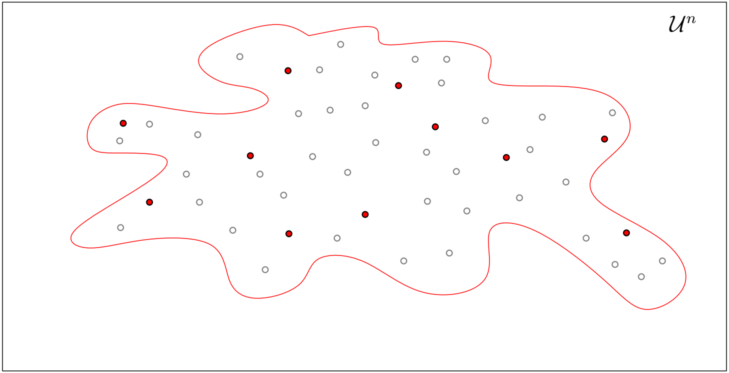
Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Each bin: Channel code for channel $P_{X_2|U}$ with input U, output X_2



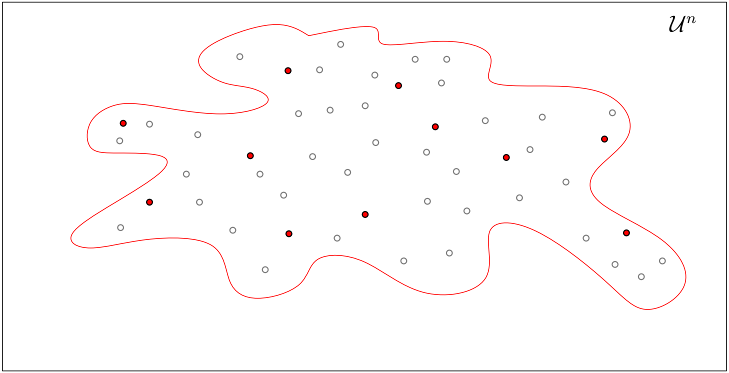
Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Code must "pack" the typical set of X_2 well



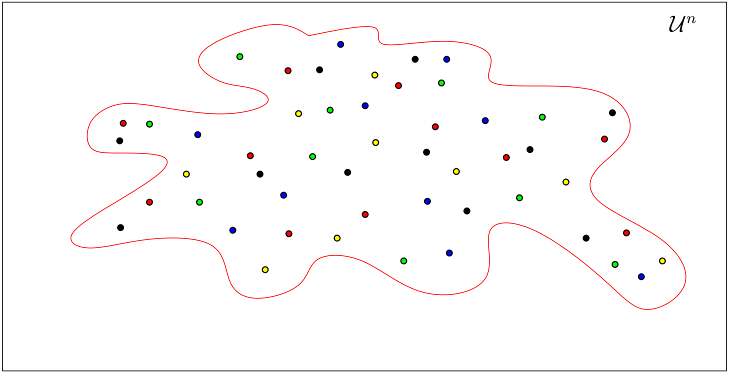
Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Size of each bin $I(U; X_2)$. Binning done randomly



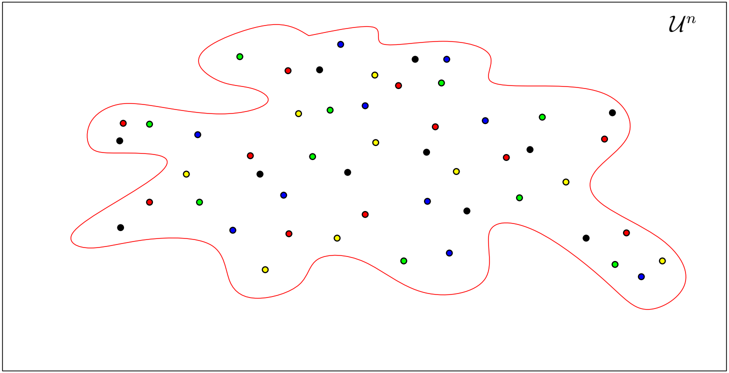
Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Overall transmission rate $R = I(X_1;U) - I(U;X_2)$



Binning - Good channel codes

- Bin the codewords - Transmit only bin index
- Nesting of a "good" channel code in a "good" source code



Random coding: Some observations

- Random coding for distributed source coding

Random coding: Some observations

- Random coding for distributed source coding
    - Unstructured ensembles drawn from typical sets

Random coding: Some observations

- Random coding for distributed source coding
  - Unstructured ensembles drawn from typical sets
  - Independent quantization followed by independent binning

Random coding: Some observations

- Random coding for distributed source coding
  - Unstructured ensembles drawn from typical sets
  - Independent quantization followed by independent binning
- Decoder given excess information

Random coding: Some observations

- Random coding for distributed source coding
  - Unstructured ensembles drawn from typical sets
  - Independent quantization followed by independent binning
- Decoder given excess information
  - First reconstructs auxiliary random variables U, V

Random coding: Some observations

- Random coding for distributed source coding
  - Unstructured ensembles drawn from typical sets
  - Independent quantization followed by independent binning
- Decoder given excess information
  - First reconstructs auxiliary random variables U, V
  - Then computes $\hat{Y}_1 = g_1(U, V)$, $\hat{Y}_2 = g_2(U, V)$

Random coding: Some observations

- Random coding for distributed source coding
  - Unstructured ensembles drawn from typical sets
  - Independent quantization followed by independent binning
- Decoder given excess information
  - First reconstructs auxiliary random variables U, V
  - Then computes $\hat{Y}_1 = g_1(U, V)$, $\hat{Y}_2 = g_2(U, V)$
- Rate gains possible?

Outline

1 Thesis Overview

2 Information Theory: An Introduction

3 Random Codes for Distributed Source Coding

4 Nested Group Codes

5 Distributed Source Coding : An Inner Bound

6 Conclusions

A Distributed source coding example

- Alice has the outcome of three fair coin tosses. She copies them and sends the copy to Bob

A Distributed source coding example

- Alice has the outcome of three fair coin tosses. She copies them and sends the copy to Bob
- She makes at most one error while copying

A Distributed source coding example

- Alice has the outcome of three fair coin tosses. She copies them and sends the copy to Bob
- She makes at most one error while copying
- Charlie wants to know only the location of the error (if any)

A Distributed source coding example

- Alice has the outcome of three fair coin tosses. She copies them and sends the copy to Bob
- She makes at most one error while copying
- Charlie wants to know only the location of the error (if any)
- Alice and Bob talk to Charlie but not to each other

A Distributed source coding example

- Alice has the outcome of three fair coin tosses. She copies them and sends the copy to Bob
- She makes at most one error while copying
- Charlie wants to know only the location of the error (if any)
- Alice and Bob talk to Charlie but not to each other
- What is the minimum amount of information (bits) Charlie needs from them?

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob
- A better scheme: Alice sends her 3 bits with no compression

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob
- A better scheme: Alice sends her 3 bits with no compression
- Bob bins his sequence as

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob
- A better scheme: Alice sends her 3 bits with no compression
- Bob bins his sequence as

00	01	10	11
000	001	010	100
111	110	101	011

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob
- A better scheme: Alice sends her 3 bits with no compression
- Bob bins his sequence as

00	01	10	11
000	001	010	100
111	110	101	011

- Suppose Alice sends 001 and Bob sends 10, error in first location

Distributed source coding example contd.

- Straightforward scheme - 3 bits each from Alice and Bob
- A better scheme: Alice sends her 3 bits with no compression
- Bob bins his sequence as

00	01	10	11
000	001	010	100
111	110	101	011

- Suppose Alice sends 001 and Bob sends 10, error in first location
- Can we do even better?

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- Ex: Alice sends 10, Bob sends 01
- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- Ex: Alice sends 10, Bob sends 01
- Possible pairs: $(001, 010), (001, 101), (110, 010), (110, 101)$
- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- Ex: Alice sends 10, Bob sends 01
- Possible pairs: $\cancel{(001,010)}, (001,101), (110,010), \cancel{(110,101)}$
- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- Ex: Alice sends 10, Bob sends 01
- Possible pairs: $\cancel{(001,010)}, (001,101), (110,010), \cancel{(110,101)}$
- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

Distributed source coding example contd.

- What if Alice also does the same binning?

00	01	10	11
000	001	010	100
111	110	101	011

- Ex: Alice sends 10, Bob sends 01
- Possible pairs: $\cancel{(001, 010)}, (001, 101), (110, 010), \cancel{(110, 101)}$
- In both cases, error in first location
- Charlie doesn't know the toss outcomes but he also doesn't care

The coding strategy explained

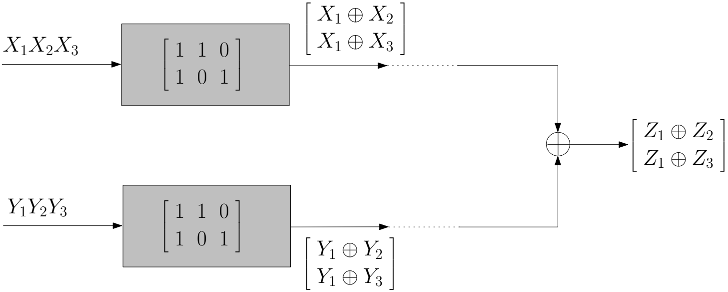
- Two 3 bit sources $X = X_1 X_2 X_3, Y = Y_1 Y_2 Y_3$. Correlation $w_H(X, Y) \leq 1$

The coding strategy explained

- Two 3 bit sources $X = X_1 X_2 X_3, Y = Y_1 Y_2 Y_3$. Correlation $w_H(X, Y) \leq 1$
- Encoding using identical linear codes:

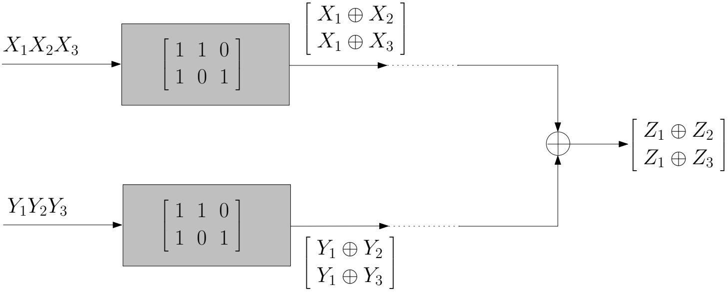
The coding strategy explained

- Two 3 bit sources $X = X_1X_2X_3, Y = Y_1Y_2Y_3$. Correlation $w_H(X, Y) \leq 1$
- Encoding using identical linear codes:



The coding strategy explained

- Two 3 bit sources $X = X_1X_2X_3, Y = Y_1Y_2Y_3$. Correlation $w_H(X, Y) \le 1$
- Encoding using identical linear codes:



- Significant feature: Identical linear binning

Korner-Marton Coding Scheme

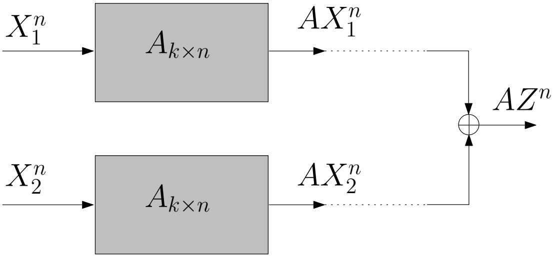
- Correlated binary random variables (X_1, X_2)

Korner-Marton Coding Scheme

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

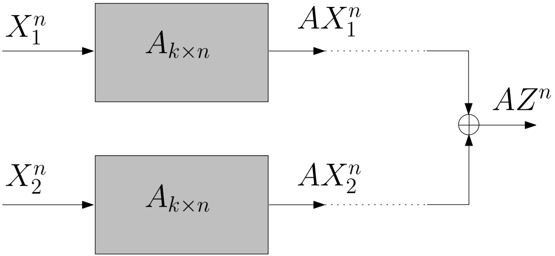
Korner-Marton Coding Scheme

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



Korner-Marton Coding Scheme

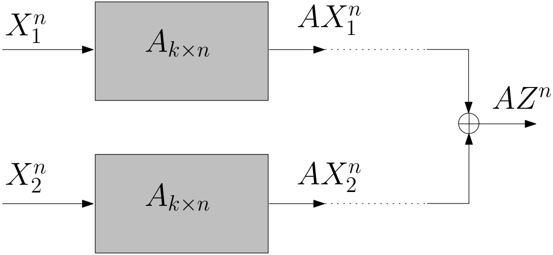
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



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

Korner-Marton Coding Scheme

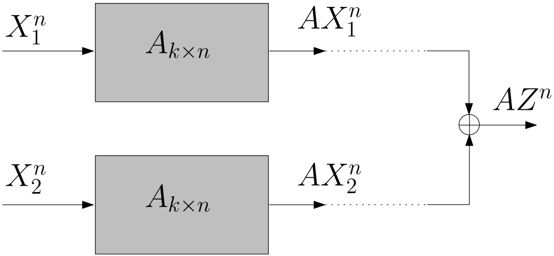
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- 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

Korner-Marton Coding Scheme

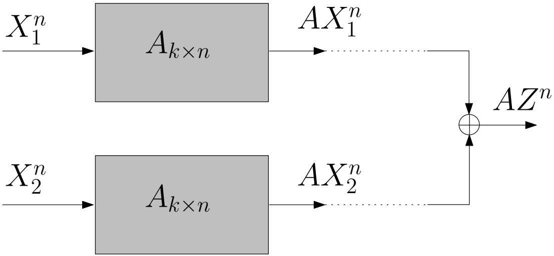
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Centralized encoder:

Korner-Marton Coding Scheme

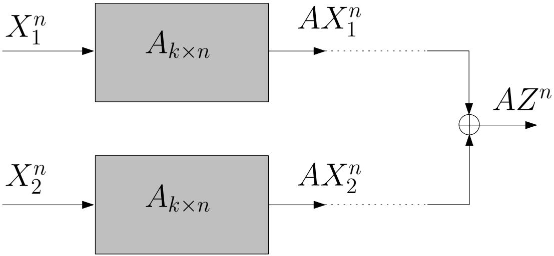
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Centralized encoder:
  - Compute $Z = X_1 \oplus X_2$. Compress to $f(z^n)$

Korner-Marton Coding Scheme

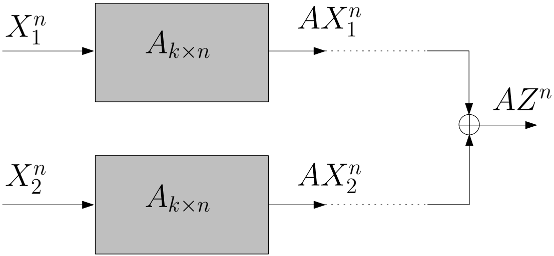
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Centralized encoder:
  - Compute $Z = X_1 \oplus X_2$. Compress to $f(z^n)$
  - Transmit $f(z^n)$ to decoder. Decoder recovers z^n

Korner-Marton Coding Scheme

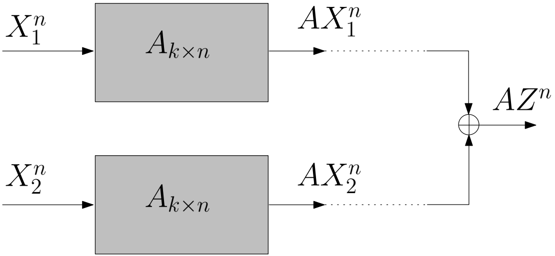
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Decentralized encoders:

Korner-Marton Coding Scheme

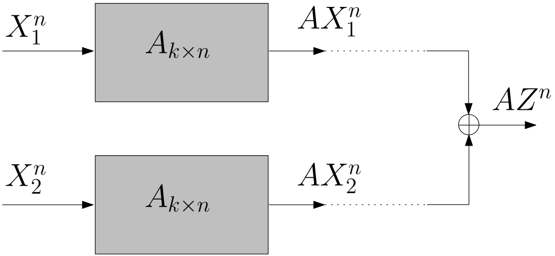
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Decentralized encoders:
  - Compress x_1^n and x_2^n and transmit

Korner-Marton Coding Scheme

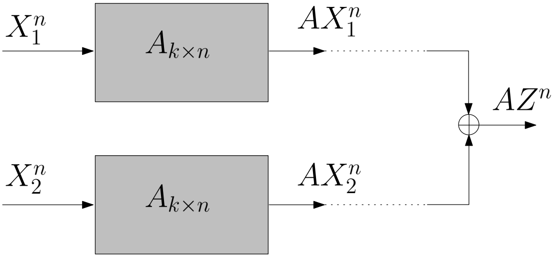
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Decentralized encoders:
  - Compress x_1^n and x_2^n and transmit
  - Decoder estimates z^n from $f_1(x_1^n)$, $f_2(x_2^n)$

Korner-Marton Coding Scheme

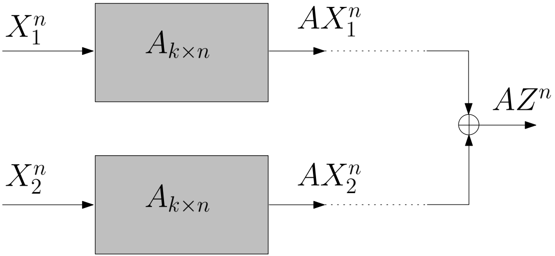
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Identical linear binning:

Korner-Marton Coding Scheme

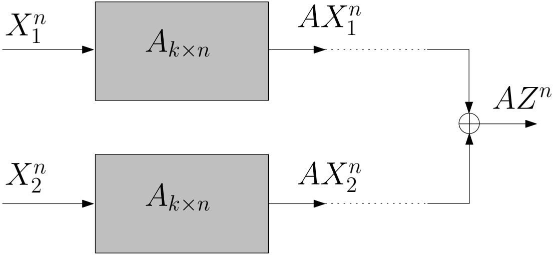
- Correlated binary random variables (X_1, X_2)
- Decoder interested in lossless reconstruction of $Z = X_1 \oplus_2 X_2$



- Identical linear binning:
  - Mimics centralized encoding

Korner-Marton Coding Scheme

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



- Identical linear binning:
  - Mimics centralized encoding
  - Correlated binning better than independent binning

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Korner Marton coding scheme

- Possible extensions:
  - Lossy coding
    - Will involve nesting of a good channel code in a good source code
    - Nesting to be done while maintaining linearity of channel code
    - Good nested linear codes
  - What about reconstructing $Z = X \oplus_4 Y$
    - Example worked because $\oplus_2$ is the group operation of the field $\mathbb{F}_2$
    - No field exists with group operation $\oplus_4$
    - Group codes

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword
- Traditionally, linear codes built over Galois fields, ex. $\mathbb{F}_2 = \{0, 1\}$

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword
- Traditionally, linear codes built over Galois fields, ex. $\mathbb{F}_2 = \{0, 1\}$
- More general: linear codes over Abelian groups $\mathbb{Z}_{p^r}$

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword
- Traditionally, linear codes built over Galois fields, ex. $\mathbb{F}_2 = \{0, 1\}$
- More general: linear codes over Abelian groups $\mathbb{Z}_{p^r}$
- Pros: Linear code ensembles have fewer bad codebooks
  - Improvement in second order performance (error exponents)
  - More dramatic gains in multi terminal settings

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword
- Traditionally, linear codes built over Galois fields, ex. $\mathbb{F}_2 = \{0, 1\}$
- More general: linear codes over Abelian groups $\mathbb{Z}_{p^r}$
- Pros: Linear code ensembles have fewer bad codebooks
  - Improvement in second order performance (error exponents)
  - More dramatic gains in multi terminal settings
- Cons: Even in single user setting, bad first order performance
  - do not achieve Shannon rate-distortion function
  - do not achieve Shannon capacity cost function

Linear codes: An Introduction

- Linear code $\mathscr{C}$: Sum of any two codewords is another codeword
- Traditionally, linear codes built over Galois fields, ex. $\mathbb{F}_2 = \{0, 1\}$
- More general: linear codes over Abelian groups $\mathbb{Z}_{p^r}$
- Pros: Linear code ensembles have fewer bad codebooks
  - Improvement in second order performance (error exponents)
  - More dramatic gains in multi terminal settings
- Cons: Even in single user setting, bad first order performance
  - do not achieve Shannon rate-distortion function
  - do not achieve Shannon capacity cost function
- Injection of some non-linearity seems necessary for optimality

Group codes: Codes over primary cyclic groups

- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality

Group codes: Codes over primary cyclic groups

- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality
- Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo-4 group operation

Group codes: Codes over primary cyclic groups

- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality
- Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo-4 group operation
- Any abelian group G decomposable into primary cyclic groups

Group codes: Codes over primary cyclic groups

- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality
- Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo-4 group operation
- Any abelian group G decomposable into primary cyclic groups
- Suffices to prove coding theorems for $\mathbb{Z}_{p^r}$

Group codes: Codes over primary cyclic groups

- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality
- Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo-4 group operation
- Any abelian group G decomposable into primary cyclic groups
- Suffices to prove coding theorems for $\mathbb{Z}_{p^r}$
- Group code defined via parity check matrix

$$\mathscr{C} = \left\{ x^n \in \mathbb{Z}_{p^r}^n : H x^n = 0^k \right\} \text{ for some } k \times n \text{ matrix } H$$

Group codes: Codes over primary cyclic groups

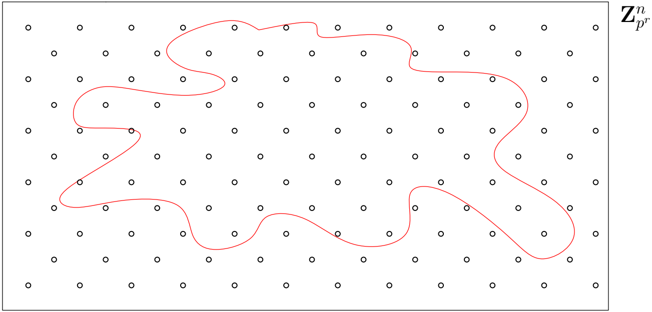
- Primary cyclic group $\mathbb{Z}_{p^r}$ - cyclic group of prime power cardinality
- Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo-4 group operation
- Any abelian group G decomposable into primary cyclic groups
- Suffices to prove coding theorems for $\mathbb{Z}_{p^r}$
- Group code defined via parity check matrix

$$\mathscr{C} = \left\{ x^n \in \mathbb{Z}_{p^r}^n : Hx^n = 0^k \right\} \text{ for some } k \times n \text{ matrix } H$$

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

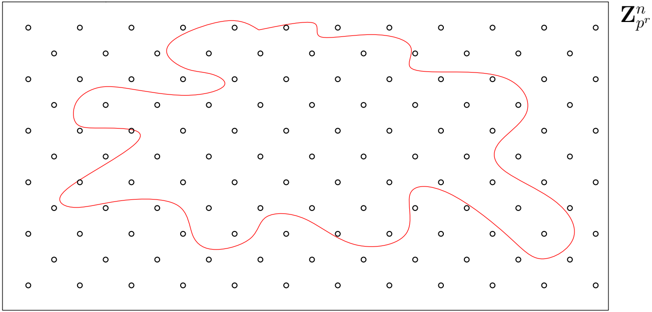
Good Group Source Codes

- Good group source code $\mathscr{C}_1$ for the triple $(\mathscr{X}, \mathscr{U}, P_{XU})$



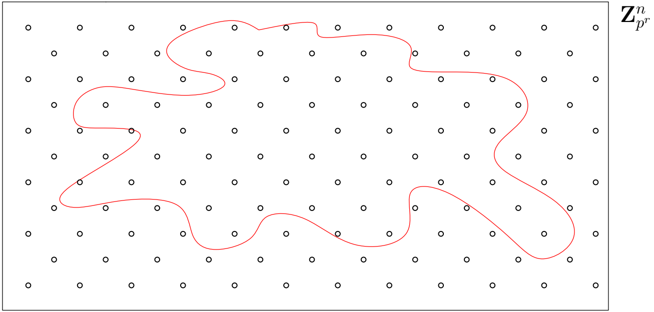
Good Group Source Codes

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



Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n

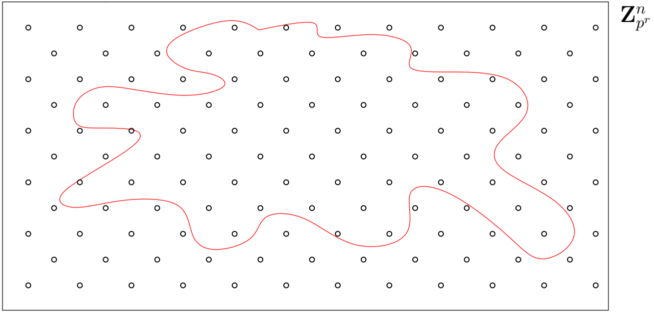


Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n
- We showed:

Good group source codes

Exist for large n if $\frac{1}{n}\log|\mathscr{C}_1| \geq \log p^r - r|H(U|X) - \log p^{r-1}|^+$

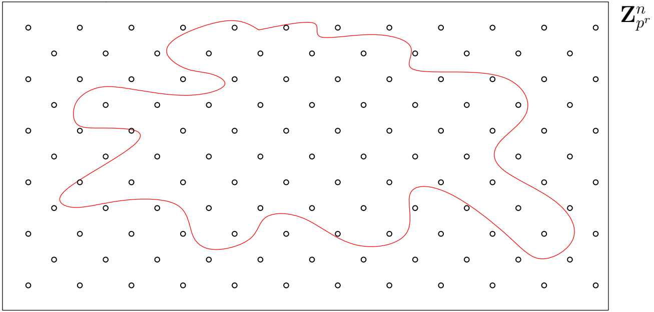


Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n
- No good source code in ensemble if $H(U|X) < \log p^{r-1}$

Good group source codes

Exist for large n if $\frac{1}{n}\log|\mathscr{C}_1| \geq \log p^r - r|H(U|X) - \log p^{r-1}|^+$

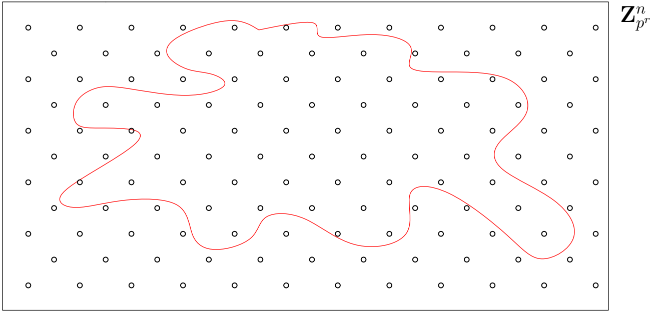


Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n
- Else: Bad performance

Good group source codes

Exist for large n if $\frac{1}{n}\log|\mathscr{C}_1| \geq r(\log p^r - H(U|X))$

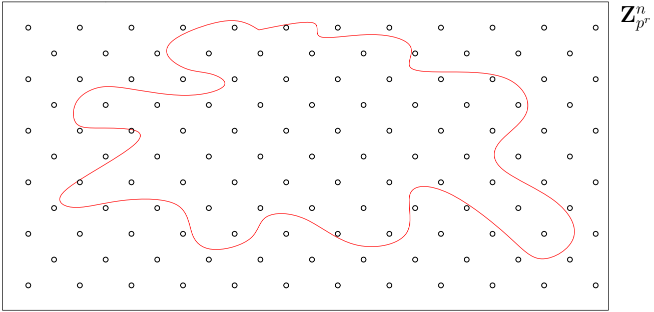


Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n
- Linear code $(r = 1)$: Still not very good

Good linear source codes

Exist for large n if $\frac{1}{n} \log |\mathscr{C}_1| \geq (\log p - H(U|X))$

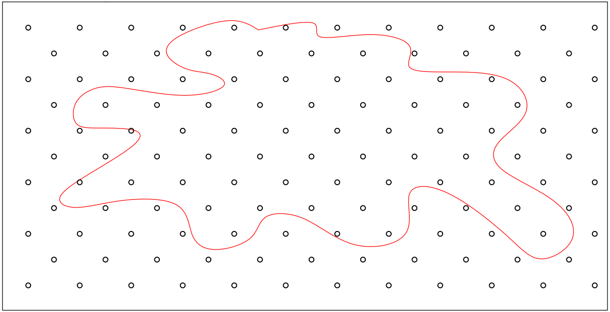


Good Group Source Codes

- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with x^n
- Larger than optimal code size: $H(U) - H(U|X)$

Good linear source codes

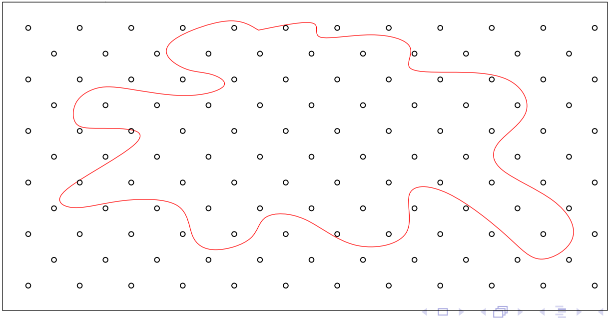
Exist for large n if $\frac{1}{n}\log|\mathscr{C}_1| \geq (\log p - H(U|X))$



$\mathbf{Z}_{p^r}^n$

Good Group Source Codes contd.

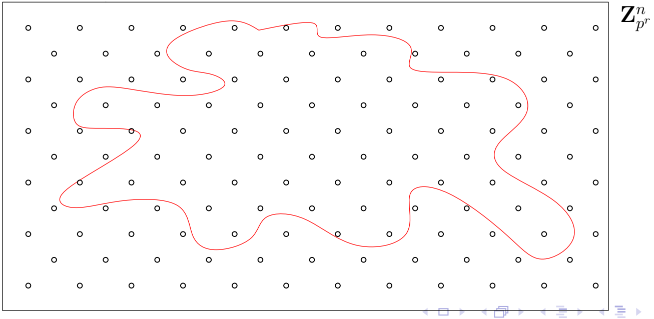
- Linear code not Shannon-good for source coding



$\mathbf{Z}_{p^r}^n$

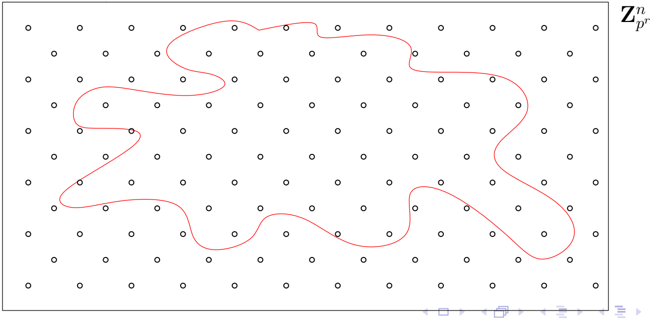
Good Group Source Codes contd.

- Linear code not Shannon-good for source coding
- But contains a Shannon-good source code



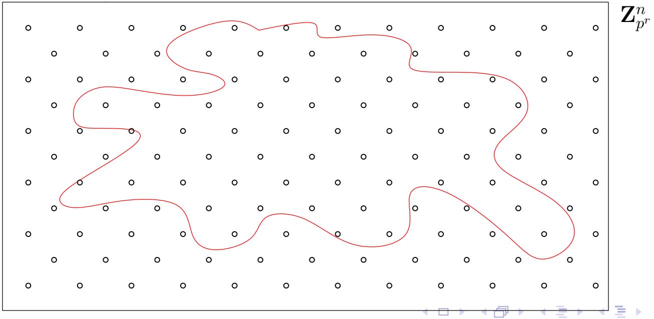
Good Group Source Codes contd.

- Linear code not Shannon-good for source coding
- But contains a Shannon-good source code
- Larger codebook due to binning entire space



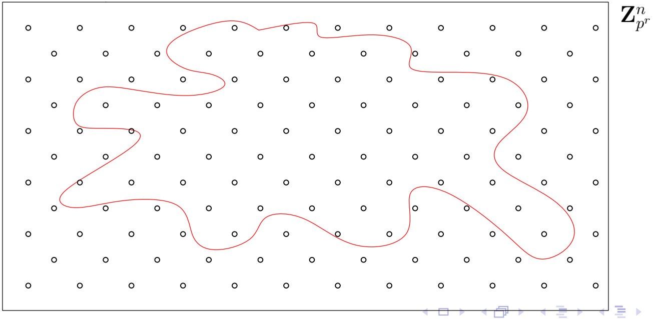
Good Group Source Codes contd.

- Linear code not Shannon-good for source coding
- But contains a Shannon-good source code
- Penalty for imposing structure



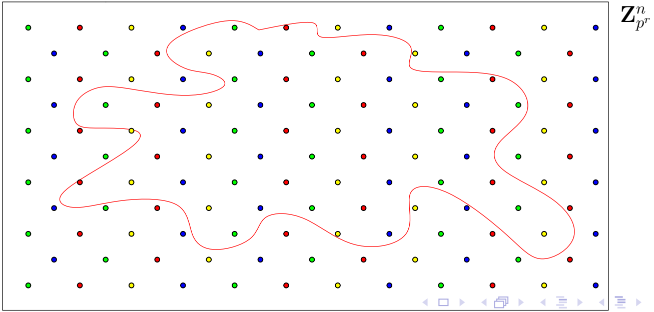
Good Group Source Codes contd.

- Linear code not Shannon-good for source coding
- But contains a Shannon-good source code
- Group codes $(r > 1)$: more penalties for subgroups



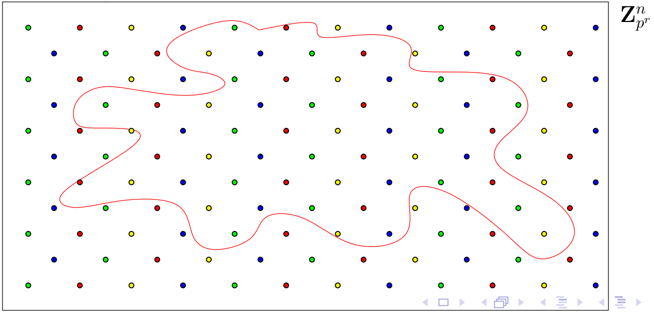
Good Group Channel Codes

- Good group channel code $\mathscr{C}_2$ for the triple $(\mathscr{Z}, \mathscr{S}, P_{ZS})$



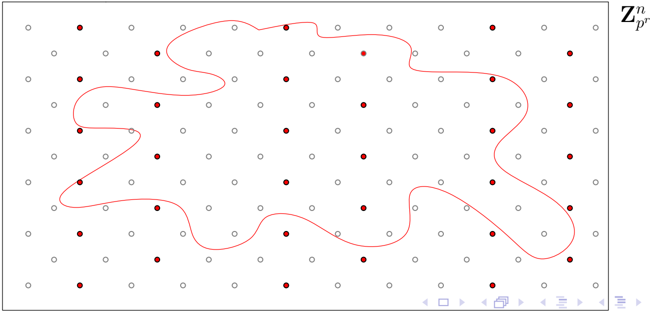
Good Group Channel Codes

- Assume $\mathcal{Z} = \mathbb{Z}_{p^r}$ for some prime p and exponent $r > 0$



Good Group Channel Codes

- Good: Can find z^n given its coset(color) and s^n

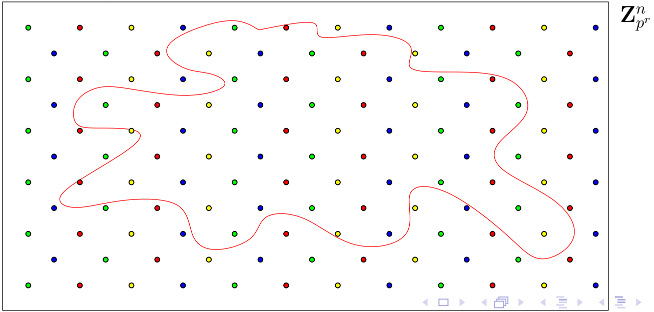


Good Group Channel Codes

- Good: Can find z^n given its coset(color) and s^n
- We showed:

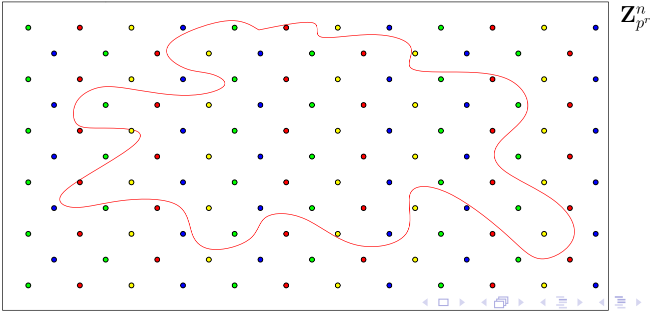
Good group channel codes

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



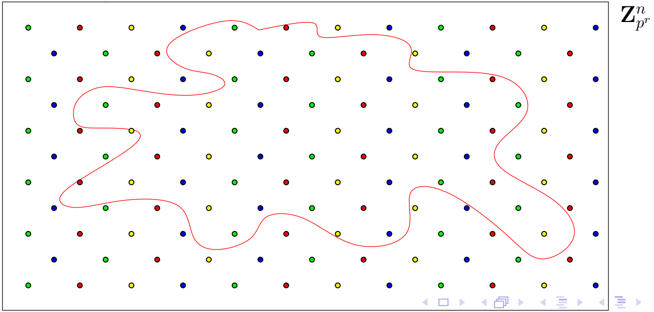
Good Group Channel Codes

- Good: Can find z^n given its coset(color) and s^n
- $[Z]_i$ - random variable taking values over distinct cosets of $p^i\mathbb{Z}_{p^r}$ in $\mathbb{Z}_{p^r}$



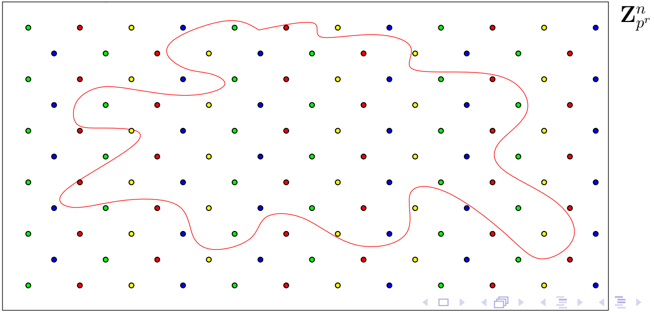
Good Group Channel Codes

- Good: Can find z^n given its coset(color) and s^n
- Suppose $\mathcal{Z} = \mathbb{Z}_8$. $[Z]_1$ - binary random variable



Good Group Channel Codes

- Good: Can find z^n given its coset(color) and s^n
- Suppose $\mathcal{Z} = \mathbb{Z}_8$. $[Z]_1$ - binary random variable
- Symbol probabilities: $(p_0 + p_2 + p_4 + p_6, p_1 + p_3 + p_5 + p_7)$



Good Group Channel Codes contd.

- Each subgroup of $\mathbb{Z}_{p^r}$: one term in maximization

Good group channel codes

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

Good Group Channel Codes contd.

- Each subgroup of $\mathbb{Z}_{p^r}$: one term in maximization
- 0th term corresponds to $H(Z|S)$

Good group channel codes

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

Good Group Channel Codes contd.

- Each subgroup of $\mathbb{Z}_{p^r}$: one term in maximization
- 0th term corresponds to $H(Z|S)$
- Penalty for presence of subgroups

Good group channel codes

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

Good Group Channel Codes contd.

- Each subgroup of $\mathbb{Z}_{p^r}$: one term in maximization
- 0th term corresponds to $H(Z|S)$
- Penalty for presence of subgroups
- Linear code $(r = 1)$: Still not good

Good linear channel codes

Exist for large n if $\frac{1}{n}\log|\mathscr{C}_2| \leq \log p - H(Z|S)$

Good Group Channel Codes contd.

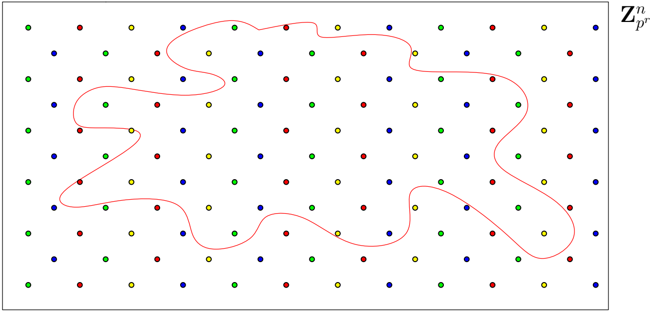
- Each subgroup of $\mathbb{Z}_{p^r}$: one term in maximization
- 0th term corresponds to $H(Z|S)$
- Penalty for presence of subgroups
- Linear code $(r = 1)$: Still not good
- Larger than optimal code size: $H(Z) - H(Z|S)$

Good linear channel codes

Exist for large n if $\frac{1}{n}\log|\mathscr{C}_2| \leq \log p - H(Z|S)$

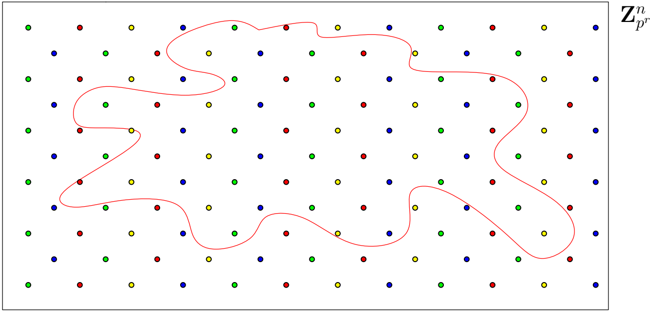
Good Group Channel Codes contd.

- Linear code not Shannon-good for channel coding



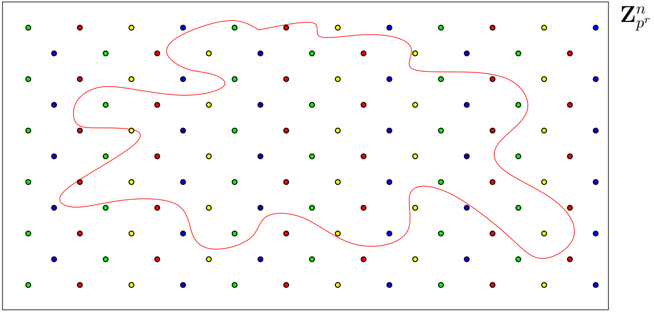
Good Group Channel Codes contd.

- Linear code not Shannon-good for channel coding
- But every coset (color) contains a Shannon-good channel code



Good Group Channel Codes contd.

- Linear code not Shannon-good for channel coding
- But every coset (color) contains a Shannon-good channel code
- Larger codebook for binning entire space



Why bother with group codes?

- Nesting one code within another helps overall performance

Why bother with group codes?

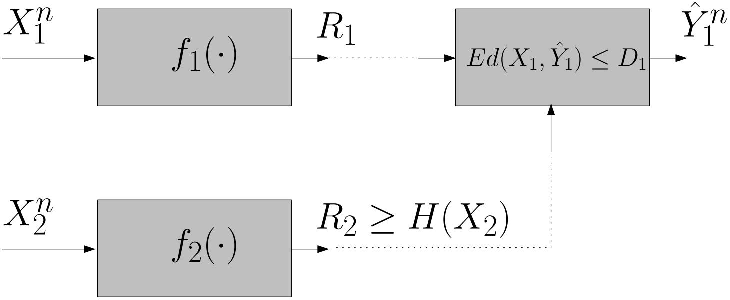
- Nesting one code within another helps overall performance
- $(\mathscr{C}_1, \mathscr{C}_2)$ nested if $\mathscr{C}_2 \subset \mathscr{C}_1$

Why bother with group codes?

- Nesting one code within another helps overall performance
- $(\mathscr{C}_1, \mathscr{C}_2)$ nested if $\mathscr{C}_2 \subset \mathscr{C}_1$
- Example: Wyner-Ziv problem using nested group codes

Why bother with group codes?

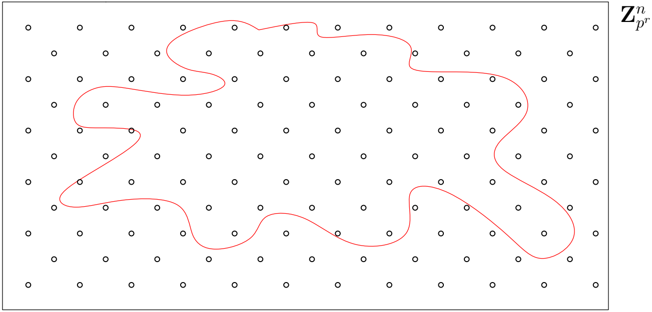
- Nesting one code within another helps overall performance
- $(\mathscr{C}_1, \mathscr{C}_2)$ nested if $\mathscr{C}_2 \subset \mathscr{C}_1$
- Example: Wyner-Ziv problem using nested group codes



$$R_1 \geq I(X_1; U \mid X_2) = I(X_1; U) - I(X_2; U)$$

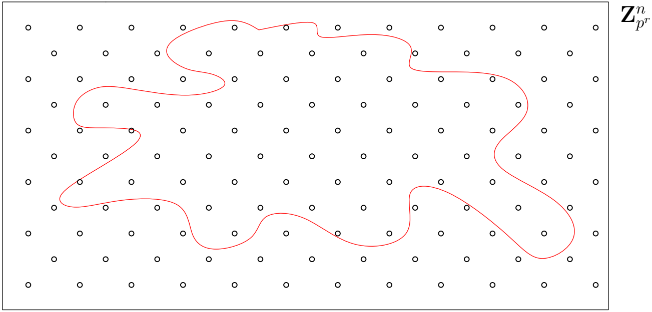
Wyner-Ziv via group codes: Quantization

- Group code good for $(\mathscr{X}_1, \mathscr{U}, P_{X_1 U})$



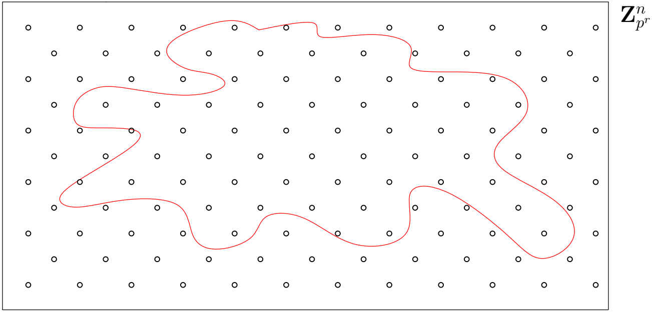
Wyner-Ziv via group codes: Quantization

- Group code good for $(\mathscr{X}_1, \mathscr{U}, P_{X_1 U})$
- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with source x^n



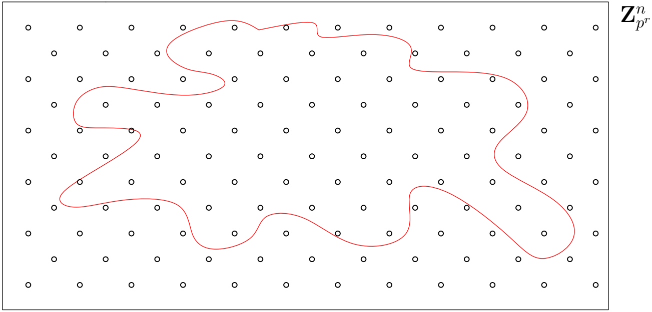
Wyner-Ziv via group codes: Quantization

- Group code good for $(\mathscr{X}_1, \mathscr{U}, P_{X_1U})$
- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with source x^n
- Rate of the code: $R = \log p^r - r|H(U|X_1) - \log p^{r-1}|^+$



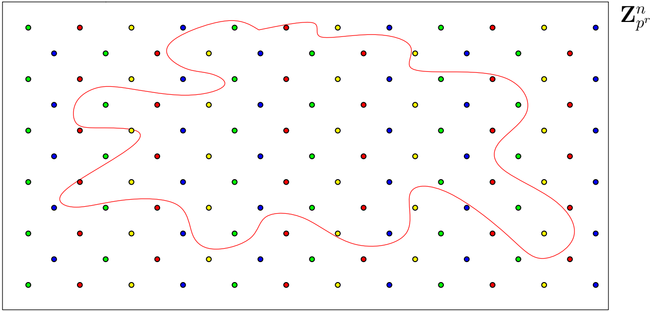
Wyner-Ziv via group codes: Quantization

- Group code good for $(\mathscr{X}_1, \mathscr{U}, P_{X_1U})$
- Good: Can find $u^n \in \mathscr{C}_1$ jointly typical with source x^n
- Rate of the code: $R = \log p^r - r|H(U|X_1) - \log p^{r-1}|^+$
- Code over Galois field: $R = \log p - H(U|X_1)$



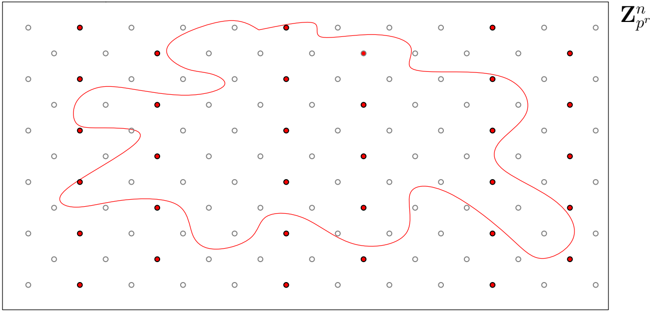
Wyner-Ziv via group codes: Binning

- Every coset (color) good channel code for $(\mathscr{U}, \mathscr{X}_2, P_{UX_2})$



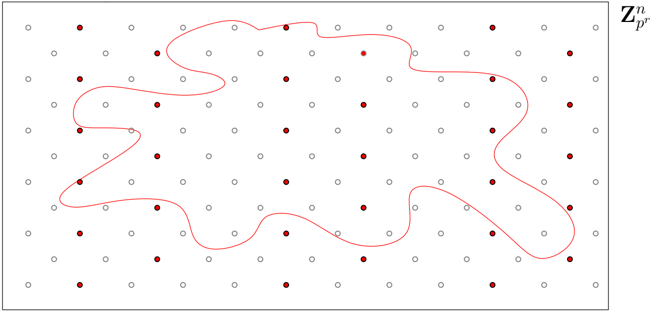
Wyner-Ziv via group codes: Binning

- Every coset (color) good channel code for $(\mathscr{U}, \mathscr{X}_2, P_{UX_2})$
- Good: Can find unique typical u^n given x_2^n and coset (color)



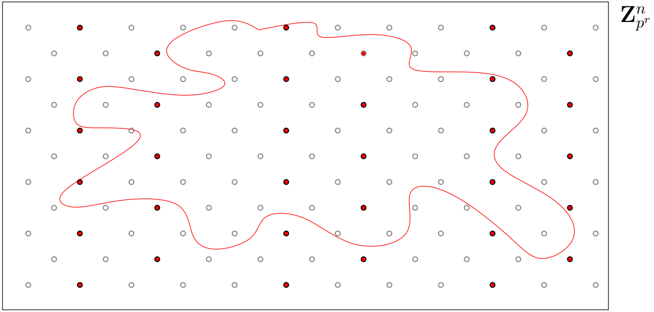
Wyner-Ziv via group codes: Binning

- Every coset (color) good channel code for $(\mathscr{U}, \mathscr{X}_2, P_{UX_2})$
- Good: Can find unique typical u^n given x_2^n and coset (color)
- Bin size: $R = \log p^r - \max_{0 \le i < r} \left(\frac{r}{r-i}\right) (H(U|X_2) - H([U]_i \mid X_2))$



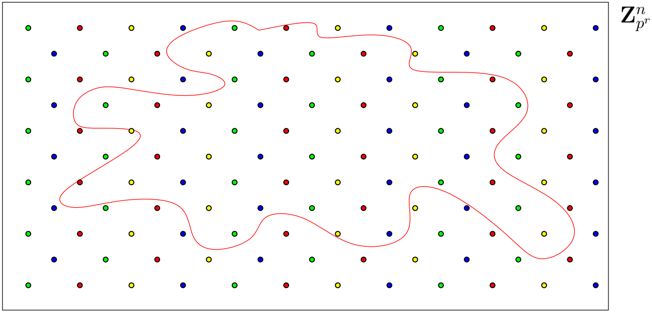
Wyner-Ziv via group codes: Binning

- Every coset (color) good channel code for $(\mathscr{U}, \mathscr{X}_2, P_{UX_2})$
- Good: Can find unique typical u^n given x_2^n and coset (color)
- Bin size: $R = \log p^r - \max_{0 \le i < r} \left(\frac{r}{r-i}\right)(H(U|X_2) - H([U]_i \mid X_2))$
- Code over Galois field: $R = \log p - H(U|X_2)$



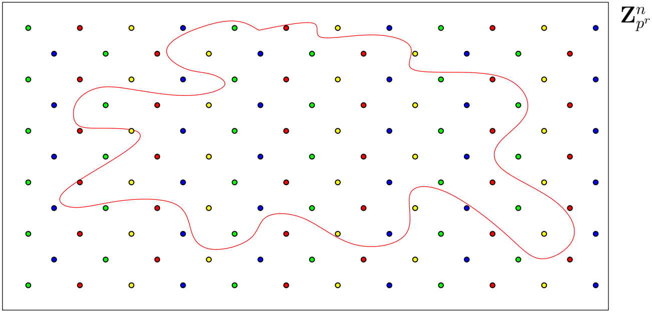
Wyner-Ziv via group codes: Rate Region

- Only coset leaders (colors) get transmitted



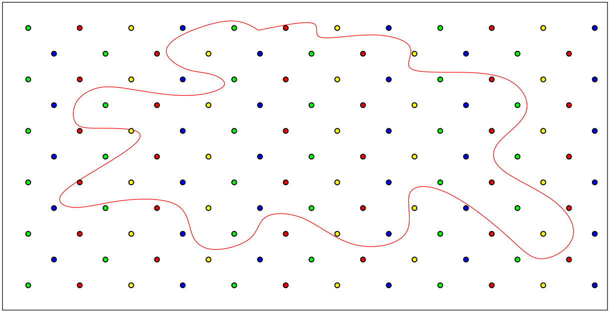
Wyner-Ziv via group codes: Rate Region

- Only coset leaders (colors) get transmitted
- Number of colors : $(\log p - H(U|X_1)) - (\log p - H(U|X_2))$



Wyner-Ziv via group codes: Rate Region

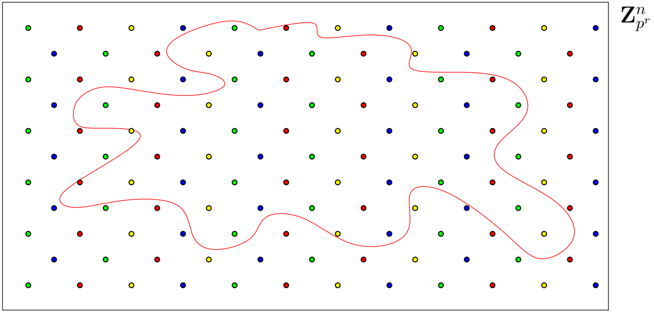
- Only coset leaders (colors) get transmitted
- Number of colors : $H(U|X_2) - H(U|X_1)$



$\mathbf{Z}_{p^r}^n$

Wyner-Ziv via group codes: Rate Region

- Only coset leaders (colors) get transmitted
- Number of colors : $I(X_1;U) - I(U;X_2)$



Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 UV} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U,V)$
  - $g(U,V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U,V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 U V} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U, V)$
  - $g(U, V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U, V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 UV} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U, V)$
  - $g(U, V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U, V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 UV} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U,V)$
  - $g(U,V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U,V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 UV} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U, V)$
  - $g(U, V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U, V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \leq i \leq k$

Overview of the coding scheme

- Fix test channels $P_{X_1 X_2 UV} = P_{X_1 X_2} P_{U|X_1} P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U,V)$
  - $g(U,V)$ group operation in abelian group G: Nested group codes
  - What if it isn't?
  - "Embed" $g(U,V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Overview of the coding scheme

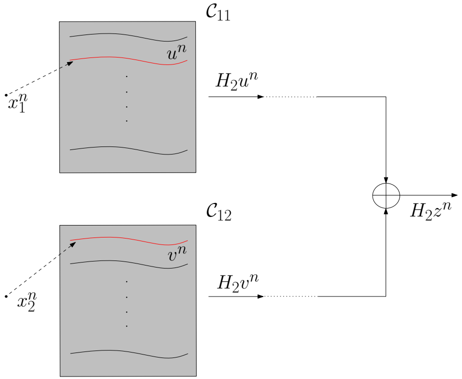
- Fix test channels $P_{X_1X_2UV} = P_{X_1X_2}P_{U|X_1}P_{V|X_2}$
- Decoder interested in some reconstruction function $g(U,V)$
    - $g(U,V)$ group operation in abelian group G: Nested group codes
    - What if it isn't?
    - "Embed" $g(U,V)$ in a suitable abelian group
- Decompose G into primary cyclic groups $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$
- Encode sequentially using codes over $\mathbb{Z}_{p_i}^{e_i}$, $1 \le i \le k$

Coding Strategy

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

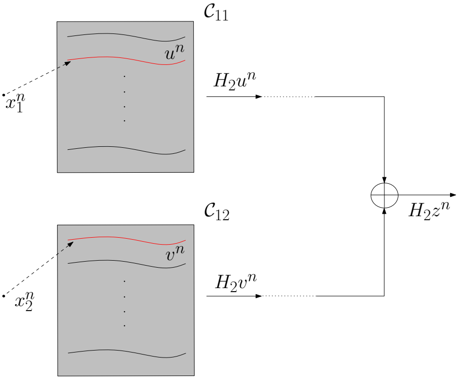
Coding Strategy

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



Coding Strategy

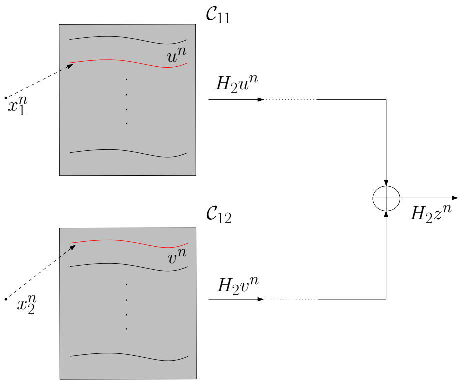
- Nested group codes $\mathscr{C}_2 < \mathscr{C}_{11}, \mathscr{C}_{12}$



- $\frac{1}{n}\log|\mathscr{C}_{11}| \geq \log p^r - r|H(U|X_1) - \log p^{r-1}|^+$

Coding Strategy

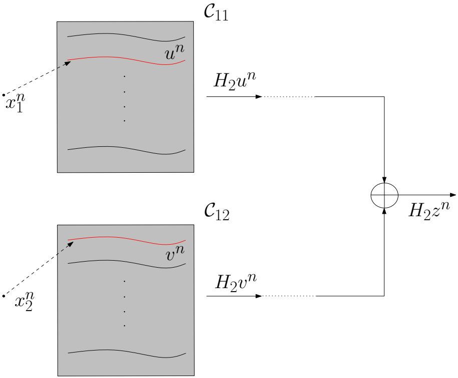
- Nested group codes $\mathscr{C}_2 < \mathscr{C}_{11}, \mathscr{C}_{12}$



- $\frac{1}{n}\log|\mathscr{C}_{11}| \geq$
  $\log p^r - r|H(U|X_1) - \log p^{r-1}|^+$
- $\frac{1}{n}\log|\mathscr{C}_{12}| \geq$
  $\log p^r - r|H(V|X_2) - \log p^{r-1}|^+$

Coding Strategy

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



- $\frac{1}{n}\log|\mathscr{C}_{11}| \geq \log p^r - r|H(U|X_1) - \log p^{r-1}|^+$
- $\frac{1}{n}\log|\mathscr{C}_{12}| \geq \log p^r - r|H(V|X_2) - \log p^{r-1}|^+$
- $\frac{1}{n}\log|\mathscr{C}_{2}| \leq \log p^r - \max_{0\leq i<r}\left(\frac{r}{r-i}\right)(H(Z) - H([Z]_i))$

Achievable Rates

Achievable rates

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

$$R_1 \geq \max_{0 \leq i < r} \left(\frac{r}{r-i}\right) (H(Z) - H([Z]_i)) - r|H(U|X) - \log p^{r-1}|^+$$
$$R_2 \geq \max_{0 \leq i < r} \left(\frac{r}{r-i}\right) (H(Z) - H([Z]_i)) - r|H(V|Y) - \log p^{r-1}|^+$$
$$D \geq \mathbb{E} d(X, Y, g(U, V))$$

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy - Encode (U, V) instead of Z

Achievable Rates

Achievable rates

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

$$R_1 \geq \max_{0 \leq i < r} \left(\frac{r}{r-i} \right) (H(Z) - H([Z]_i)) - r|H(U|X) - \log p^{r-1}|^+$$
$$R_2 \geq \max_{0 \leq i < r} \left(\frac{r}{r-i} \right) (H(Z) - H([Z]_i)) - r|H(V|Y) - \log p^{r-1}|^+$$
$$D \geq \mathbb{E} d(X, Y, g(U, V))$$

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy - Encode (U, V) instead of Z

Achievable Rates

Achievable rates

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

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

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

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

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy - Encode (U, V) instead of Z

Achievable Rates

Achievable rates

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

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

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

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

are achievable.

- More general rate region possible by
  - Embedding in general groups and using digit decomposition
  - Alternative coding strategy - Encode (U, V) instead of Z

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

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

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

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

A Lossless Reconstruction Example

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

A Lossless Reconstruction Example

- X, Y, Z - Quaternary random variables
- Quaternary rvs: X, Y. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- Group based scheme in $\mathbb{Z}_4$ achieves

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

A Lossless Reconstruction Example

- X, Y, Z - Quaternary random variables
- Quaternary rvs: X, Y. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- Group based scheme in $\mathbb{Z}_4$ achieves

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

- Can be lower than $H(X, Y)$

A Lossless Reconstruction Example

- X, Y, Z - Quaternary random variables
- Quaternary rvs: X, Y. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- Group based scheme in $\mathbb{Z}_4$ achieves

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

- Can be lower than $H(X, Y)$
- Function can also be "embedded" in $\mathbb{Z}_4, \mathbb{Z}_7, \mathbb{Z}_2^3, \mathbb{Z}_4^2$

A Lossless Reconstruction Example

- X, Y, Z - Quaternary random variables
- Quaternary rvs: X, Y. Correlation: $Y = X \oplus_4 Z$
- Decoder: lossless reconstruction of $Z = (X - Y) \mod 4$
- Group based scheme in $\mathbb{Z}_4$ achieves

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

- Can be lower than $H(X, Y)$
- Function can also be "embedded" in $\mathbb{Z}_4, \mathbb{Z}_7, \mathbb{Z}_2^3, \mathbb{Z}_4^2$
  - For every group : P_X, P_Z such that that group gives best embedding

P_X	P_Z	$R_{\mathbb{Z}_4}$	$R_{\mathbb{Z}_7}$	$R_{\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2}$	$R_{\mathbb{Z}_4\oplus\mathbb{Z}_4}$
$[\frac{1}{4}\,\frac{1}{4}\,\frac{1}{4}\,\frac{1}{4}]$	$[\frac{1}{2}\,0\,\frac{1}{4}\,\frac{1}{4}]$	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.

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

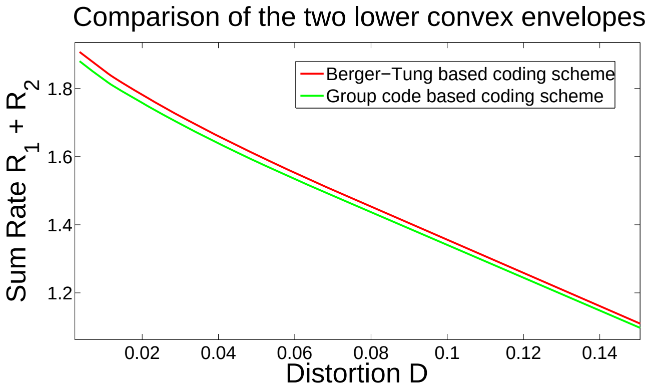
Lossy Reconstruction of binary XOR

- 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

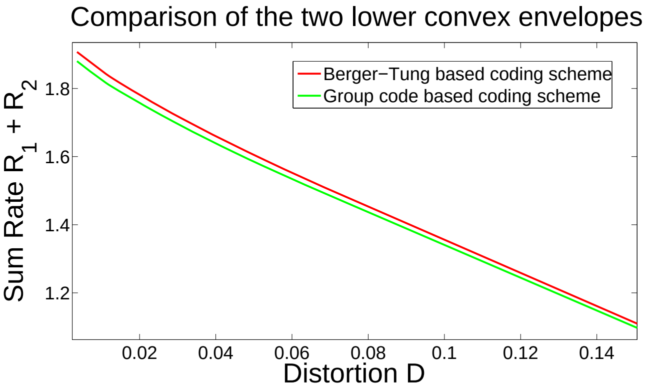
- Correlated binary sources (X, Y)
- Reconstruct $Z = X \oplus_2 Y$ within Hamming distortion D
- U, V - binary auxiliary random variables
- $G(U, V)$ - one of 16 possibilities depending on $(P_{U|X}, P_{V|Y})$

Lossy Example contd.



- Rate gains over the Berger-Tung based scheme

Lossy Example contd.



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

Outline

1. Thesis Overview
2. Information Theory: An Introduction
3. Random Codes for Distributed Source Coding
4. Nested Group Codes
5. Distributed Source Coding : An Inner Bound
6. Conclusions

Summary

- Unified framework using structured codes

Summary

- Unified framework using structured codes
    - Nesting makes them atleast as good as unstructured codes

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of “goodness”
- Distributed coding of discrete sources
  - Existence of “good” group codes
  - Recovers rate regions for many problems

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes
  - Recovers rate regions for many problems
  - Improves rate regions for certain distortion functions

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes
  - Recovers rate regions for many problems
  - Improves rate regions for certain distortion functions
- Jointly Gaussian sources

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes
  - Recovers rate regions for many problems
  - Improves rate regions for certain distortion functions
- Jointly Gaussian sources
  - Lattice codes analogous to group codes

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes
  - Recovers rate regions for many problems
  - Improves rate regions for certain distortion functions
- Jointly Gaussian sources
  - Lattice codes analogous to group codes
  - Within 1 bit of optimal rate-distortion region

Summary

- Unified framework using structured codes
  - Nesting makes them atleast as good as unstructured codes
  - Can be plugged into many multi-terminal problems
  - Existence results for appropriate notions of "goodness"
- Distributed coding of discrete sources
  - Existence of "good" group codes
  - Recovers rate regions for many problems
  - Improves rate regions for certain distortion functions
- Jointly Gaussian sources
  - Lattice codes analogous to group codes
  - Within 1 bit of optimal rate-distortion region
  - Arbitrarily large gains over unstructured codes

Codes over Non-Abelian Groups

- Group codes built over abelian groups

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?
    - Normal subgroup of G^n

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?
  - Normal subgroup of G^n
  - Too stringent. No good codes exist.

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?
  - Normal subgroup of G^n
  - Too stringent. No good codes exist.
- Ensemble of subgroups of G^n

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?
    - Normal subgroup of G^n
    - Too stringent. No good codes exist.
- Ensemble of subgroups of G^n
    - Trellis based characterization (from control theory literature)

Codes over Non-Abelian Groups

- Group codes built over abelian groups
- Proofs used underlying ring structure
- Codes over a non-abelian group G
- Codebook : Kernel of homomorphism from G^n to G^k?
  - Normal subgroup of G^n
  - Too stringent. No good codes exist.
- Ensemble of subgroups of G^n
  - Trellis based characterization (from control theory literature)
  - More sophisticated tools from group theory

Other Extensions

- Distributed source coding - only one example

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels
  - Might want to decode a function of interfering users' messages

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels
  - Might want to decode a function of interfering users' messages
  - Structured codes will lead to better rate regions

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels
  - Might want to decode a function of interfering users' messages
  - Structured codes will lead to better rate regions
- Practical nested linear code constructions

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels
  - Might want to decode a function of interfering users' messages
  - Structured codes will lead to better rate regions
- Practical nested linear code constructions
  - Rich theory of LDPC, LDGM codes

Other Extensions

- Distributed source coding - only one example
- Multi-terminal channel coding
  - Broadcast channels, interference channels
  - Might want to decode a function of interfering users' messages
  - Structured codes will lead to better rate regions
- Practical nested linear code constructions
  - Rich theory of LDPC, LDGM codes
  - Sub-optimal but fast decoding

Thank You

Questions?

Slepian-Wolf Coding

- Function to be reconstructed $F(X, Y) = (X, Y)$.

Slepian-Wolf Coding

- 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 $\mathbb{F}_4$.

$\oplus_4$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

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 $\mathbb{F}_4$.

$\oplus_4$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

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 $\mathbb{F}_4$.

$\oplus_4$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

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.

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 $\tilde{Z}$

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.

$\oplus_2$	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"
- First digit can be encoded at rate $H(\tilde{X}_1) = H(X)$
- Second digit can be encoded at rate $H(\tilde{Y}_2|\tilde{X}_1) = H(Y|X)$

Proof Techniques - Group Channel Codes

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

Proof Techniques - Group Channel Codes

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

Proof Techniques - Group Channel Codes

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

$$P_e = P\left(\bigcup_{\substack{\tilde{z}^n \in A_\epsilon^n(Z) \\ \tilde{z}^n \neq z^n}} (\phi(\tilde{z}^n) = \phi(z^n)) \right)$$

Proof Techniques - Group Channel Codes

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

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

Proof Techniques - Group Channel Codes

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

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

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

Proof Techniques - Group Channel Codes

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

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

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

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

Proof Techniques - Group Channel Codes

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

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

  - Depends on which subgroup $p^i \mathbb{Z}_{p^r}^n$ 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 $= \left(\frac{1}{2}\right)^k$

Proof Techniques - Group Channel Codes

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

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

  - Depends on which subgroup $p^i \mathbb{Z}_{p^r}^n$ 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 $= \left(\frac{1}{4}\right)^k$

Proof Techniques - Group Channel Codes

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

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

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

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

Proof Techniques - Group Channel Codes

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

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

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

- Estimate cardinality of $(z^n + p^i\mathbb{Z}_{p^r}^n) \cap A_\epsilon^n(Z)$
  - Equivalent to entropy maximization under affine constraints

Proof Techniques - Group Source Codes

- Good group source code:

Proof Techniques - Group Source Codes

- Good group source code:

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

- Group structure introduces dependencies

Proof Techniques - Group Source Codes

- Good group source code:

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

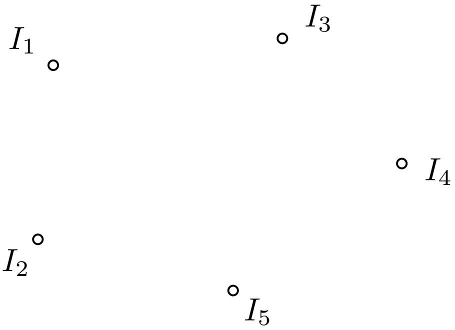
- Group structure introduces dependencies
- Suen's inequality from random graph literature

Suen's Inequality

- Bounds on sum of "sparsely" dependent indicator random variables

Suen's Inequality

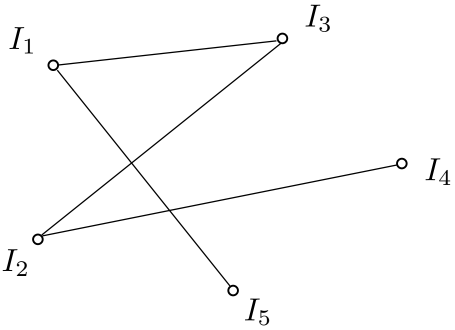
- Bounds on sum of "sparsely" dependent indicator random variables



- Each indicator is a node

Suen's Inequality

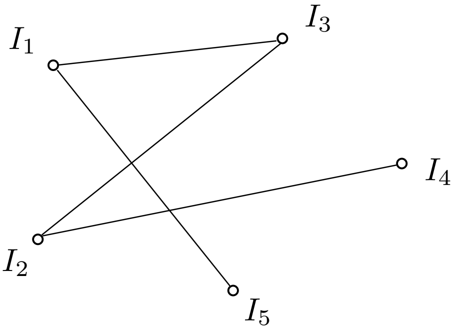
- Bounds on sum of "sparsely" dependent indicator random variables



- Edges between dependent indicators

Suen's Inequality

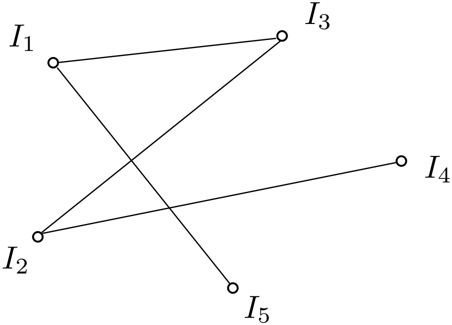
- Bounds on sum of "sparsely" dependent indicator random variables



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

Suen's Inequality

- Bounds on sum of "sparsely" dependent indicator random variables



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

$$P\left(\sum_i I_i = 0\right) \leq \exp\left\{-\min\left(\frac{\lambda^2}{8\Delta}, \frac{\lambda}{2}, \frac{\lambda}{6\delta}\right)\right\}$$

Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$

Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$
- $P(u^n \in \mathscr{C})$ easy to evaluate

Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$
- $P(u^n \in \mathscr{C})$ easy to evaluate
- $P(u_1^n, u_2^n \in \mathscr{C})$

Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$
- $P(u^n \in \mathscr{C})$ easy to evaluate
- $P(u_1^n, u_2^n \in \mathscr{C})$
    - Depends on number of solutions in (α, β) to $\alpha u_1^n + \beta u_2^n = 0$

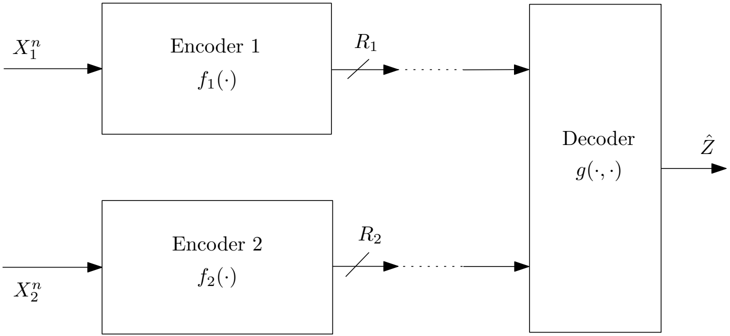
Proof Techniques - Group Source Codes contd.

- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$
- $P(u^n \in \mathscr{C})$ easy to evaluate
- $P(u_1^n, u_2^n \in \mathscr{C})$
  - Depends on number of solutions in (α, β) to $\alpha u_1^n + \beta u_2^n = 0$
  - $P(u_1^n, u_2^n \in \mathscr{C}) = \frac{\text{Number of solution pairs}_{(\alpha,\beta)}}{p^{2r}}$

Proof Techniques - Group Source Codes contd.

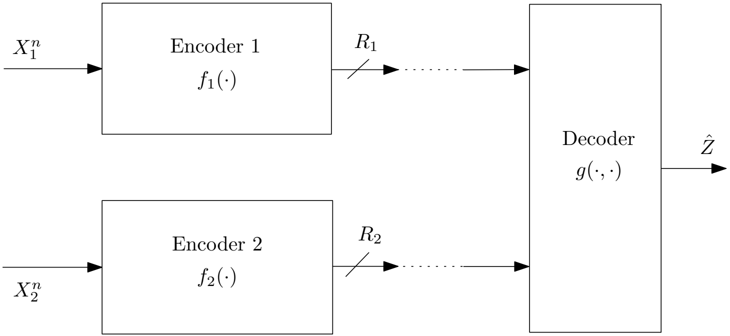
- Need to evaluate $P(u^n \in \mathscr{C})$ and $P(u_1^n, u_2^n \in \mathscr{C})$
- $P(u^n \in \mathscr{C})$ easy to evaluate
- $P(u_1^n, u_2^n \in \mathscr{C})$
  - Depends on number of solutions in (α, β) to $\alpha u_1^n + \beta u_2^n = 0$
  - $P(u_1^n, u_2^n \in \mathscr{C}) = \frac{\text{Number of solution pairs}_{(\alpha,\beta)}}{p^{2r}}$
  - Have to estimate the degree of each vertex in the dependency graph

Highlights of the work



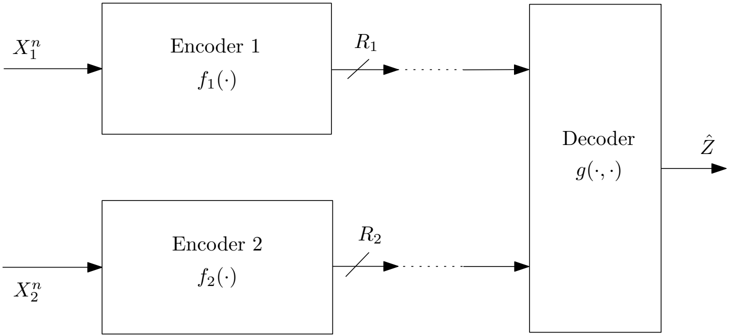
- $X_1, X_2 \sim \mathcal{N}(0,1), \mathbb{E}(X_1 X_2) = \rho > 0$

Highlights of the work



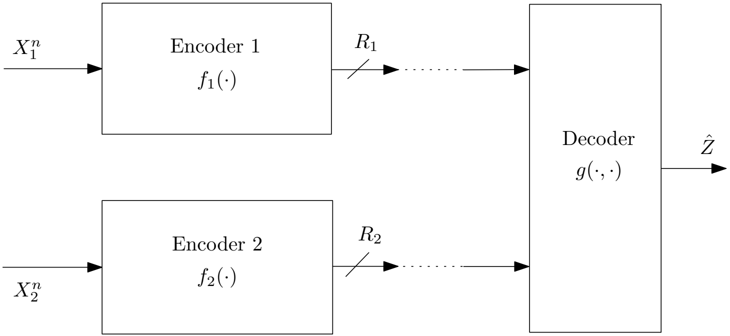
- $\hat{Z} = X_1 - cX_2$, $c > 0$

Highlights of the work



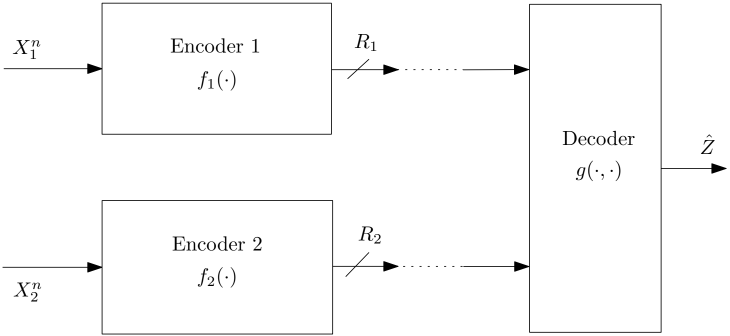
- $\mathbb{E}d(X_1, X_2, \hat{Z}) = \mathbb{E}(X_1 - cX_2 - \hat{Z})^2$

Highlights of the work



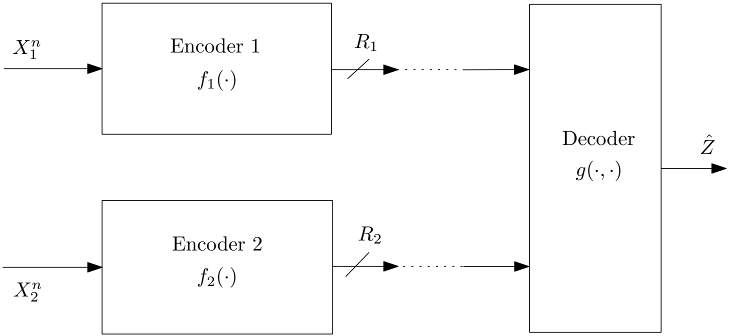
- Objective: Achievable rates (R_1, R_2) at distortion D

Highlights of the work



- Achievable rate region using nested lattice codes

Highlights of the work



- Showed achievability of (R_1, R_2, D) when

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