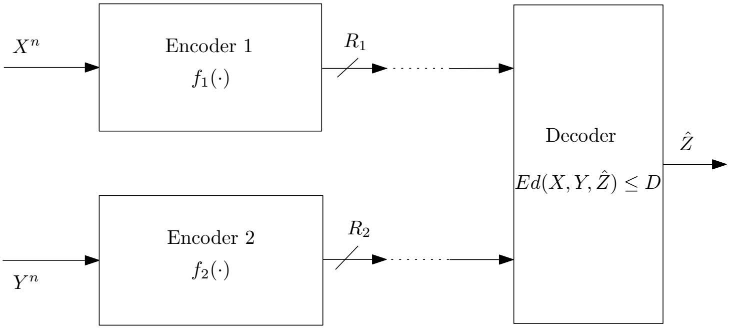
Toward a New Approach to Distributed Source Coding: Harnessing Group Structure

Dinesh Krithivasan and S. Sandeep Pradhan

University of Michigan

ITA 2009

A Distributed Source Coding Problem



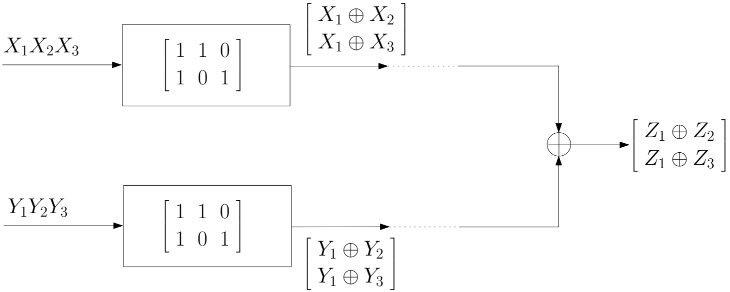
- Set of encoders observe different components of a vector source
- Central decoder receives quantized observations from the encoders
- Best known rate region - Berger-Tung based

An Illustrative Example

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

An Illustrative Example contd.

- A linear coding scheme:



- Sum rate: $2 + 2 = 4$ bits
- Significant features:
  - Identical binning at both encoders
  - Linear codes

Slepian-Wolf coding

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

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

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

Overview of our Coding Scheme

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

Groups - An Introduction

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

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

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

Nested Group Codes - Motivation

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

Nested Group Codes

- Group code over $\mathbb{Z}_{p^r}^n$: $\mathscr{C} < \mathbb{Z}_{p^r}^n$
- $\mathscr{C} = \ker(\phi)$ for some homomorphism $\phi \colon \mathbb{Z}_{p^r}^n \to \mathbb{Z}_{p^r}^k$
- $(\mathscr{C}_1, \mathscr{C}_2)$ nested if $\mathscr{C}_2 \subset \mathscr{C}_1$
- We need:
    - $\mathscr{C}_1 < \mathbb{Z}_{p^r}^n$: "good" source code
        - Can find $u^n \in \mathscr{C}_1$ jointly typical with source x^n
    - $\mathscr{C}_2 < \mathbb{Z}_{p^r}^n$: "good" channel code
        - Can distinguish between typical channel noise sequences

Good Group Source Codes

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

Lemma

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

- Compare with optimal random code's size: $H(U) - H(U|X) = I(X;U)$
- Not good in Shannon sense
- Penalty for imposing group structure

Good Group Channel Codes

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

Lemma

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

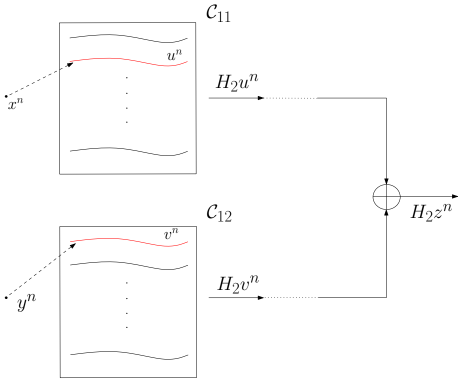
- Compare with optimal random code's size: $\log p^r - H(Z|S)$
- Not good in Shannon sense
- Penalty for presence of subgroups

Notation

- Fix $P_{U|X}, P_{V|Y}$ such that $\mathbb{E}d(X, Y, G(U, V)) \leq D$
- Suppose $G(U, V)$ equivalent to group operation in abelian group G
- Decompose G into primary cyclic groups. Encode one digit at a time
- Decoder: At the bth stage, previously decoded digits as side information

Coding Strategy

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



- $\frac{1}{n}\log|\mathscr{C}_{11}| \geq \log p^r - \min\{H(U|X), r|H(U|X) - \log p^{r-1}|^+\}$.
- $\frac{1}{n}\log|\mathscr{C}_{12}| \geq \log p^r - \min\{H(V|Y), r|H(V|Y) - \log p^{r-1}|^+\}$.
- $\frac{1}{n}\log|\mathscr{C}_2| \leq \log p^r - \max_{0 \leq i < r}\left(\frac{r}{r-i}\right)(H(Z) - H([Z]_i))$.

Achievable Rates

Theorem

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

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

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

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

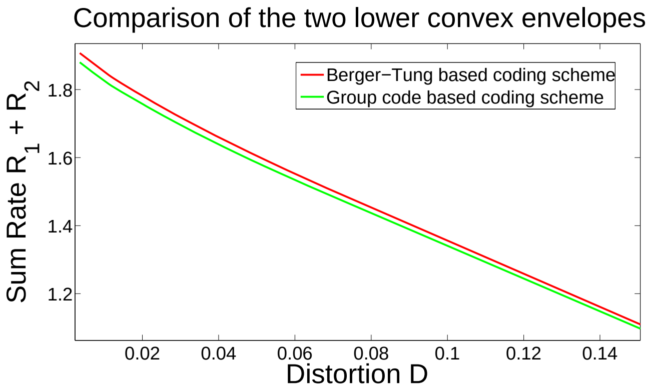
are achievable.

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

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

Special cases

- Lossless compression using group codes - achievable rates
- Lossy compression for arbitrary sources and distortion measures using group codes
- Nested linear codes - Shannon rate-distortion bound for arbitrary sources and additive distortion measures
- 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
- Function computation - Lossless reconstruction of $Z = X \oplus_4 Y$

Conclusions

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