3rd BEATS/WIP/CUBAN workshop

Modern Channel Coding Problems: Coding Problems:

an Overview

Giuseppe Caire, Eurecom Joint work with: S. Verdu, S. Shamai, S. Sesia, K. Narayanan

May 23 – 25, 2005

- Almost lossless data compression using block codes.
- Schemes and experimental results.
- Applications: Slepian-Wolf, Bidirectional data exchange, Coding with limited feedback.
- Application to "robust" (lossy) source-channel coding.
- Conclusions.

Fixed-Length (Block) Almost Lossless Compression



Theorem (Shannon-Macmillan) If $\frac{m}{n} > H + \delta$, Probability of block error $\rightarrow 0$.

Example: 7-to-3 code for bias-p coin



- Optimum block source code: encode the 2^3 most probable sourcewords.
- .sould "Block Huffman" code for source with 2^7 values.

Linear Block Source Codes

		u														
		0														
Ч		u	С	ļ	b	K	Μ	ļ	ļ		С	ſ	K	0	n	S
		u	S	ł		q	ļ	Ð	0	λ	Ч	Χ	W	Ð	ł	İ
S		е	X	n	Ð		W	n	K	е		б	Ð			ĺ
n		Ч	K	ļ	Χ	γ	ſ	u	W	ĺ	٨	b	Ð	0	1	Ι
ພ	_	S	ļ	λ	Ζ	n	S	б	б		ļ	λ	С	b	Μ	ł
d	_		r	Ч	Ч	0	Х	Ð	K	Ч	р	Χ	0	ļ	J	С
		ə	λ	0	е	q	Μ	ļ		Ð	ļ	S	ł	ĺ	0	б
0		р	ļ	S		٨	Х	е	q	Х	λ	0	ł	Μ		С
б		n	Ð	u	q	W	Ð		n			С	K		б	S
d		е	ļ	n	Ч	d	ļ	d	ļ	Ζ	Ð	1	b		d	K
	•	 0											$\mathbf{z} = \mathbf{s}$	е Н :	ləbo	SnG

Decoder: Given the linearly encoded vector \mathbf{u} that satisfies $\mathbf{H}\mathbf{u} = \mathbf{z}$. $\mathbf{g}_{\mathbf{H}}(\mathbf{z})$: the most likely source vector \mathbf{u} that satisfies $\mathbf{H}\mathbf{u} = \mathbf{z}$.

Coset partition and source typical set



- Theorem (Elias, 1955; Csiszár-Körner, 1981)
- , H the source is stationary memoryless with entropy H,
- $g + H < \frac{u}{u}$ ■
- the encoding matrix entries are independent,
- $\blacksquare \implies \text{average block error probability} \rightarrow 0.$
- Theorem for general sources [Verdu-Shamai-Caire, 2003]:
- , \overline{H} source has sup-entropy rate \overline{H} ,
- $,\delta+\bar{H}<\frac{m}{m} \blacksquare$
- the encoding matrix entries are independent,
- $\blacksquare \implies average block error probability \rightarrow 0.$

- $\mathbf{u} + \mathbf{x} = \mathbf{v}$:leanned: $\mathbf{v} = \mathbf{v} + \mathbf{u}$
- . Linear channel code with parity-check matrix ${f H}$ inear channel code with parity-check matrix ${f H}$
- The maximum likelihood decoder selects the codeword $y-g_{\mathbf{H}}(\mathbf{H}y),\iff$ it selects the most likely noise realization among those that lead to the same syndrome $\mathbf{H}_y.$
- Random Linear codes (independent equiprobable parity-check

Linear Block Channel Codes As Linear Block Source Codes

Source Encoder = Syndrome Computer:

 $\mathbf{sH} = \mathbf{z}$

where \mathbf{H} is the parity-check matrix of a channel code.

- Maximum likelihood Source decoder: $g_{\mathbf{H}}(\mathbf{z})$ (syndrome decoder)
- Block error probability = Block error probability of the channel code when
- Not a new idea! (Ancheta, 1976) tried syndrome coding for bias-p coins with n = 15,31 Hamming and BCH codes and could beat run-length coding and Cover's enumerative source encoding only for p < 0.07.

Example: 7-to-3 code for bias-p coin



Optimum code: unique codeword for the 2³ most probable sourcewords.
 Aamming (7,4) parity-check matrix —

Linear Block Source Codes vs. Lempel-Ziv

lNeAu	ed at Decoder	Universal
$\mu \lambda \mid Exp(\mu)$		(u)O
$(u_2)O \mid O(u_2)$		(u)O
somlA	-Fossless	SSƏJSSOJ
рәхіӘ		Variable
p a u i T	$\mathcal{B}lock$	vi Z - ləqmə L

Low-Density Parity-Check (LDPC) Encoding Matrices



stið bəzzərqm07

Belief-Propagation Decoding (Binary Alphabet)

• A priori source log-ratios

$$\{n \dots, 1\} \ni \lambda \quad , \frac{\lambda q - 1}{\lambda q} \operatorname{gol} = \lambda \mathfrak{I}$$

• Bitnode $k \to \mathsf{Checknodes} \in \mathcal{A}_k$

$$\mathcal{V}_{(t)}^{k \to j} = \mathcal{L}_{k} + \sum_{\substack{j' \in \mathcal{A}_{k} - \{j\} \\ \ell^{(t)}}} \mu_{(t-1)}^{j' \to k}$$

$$\mathbf{s}\mathbf{H}=\mathbf{z}$$
 Checknode $j o \mathsf{B}$ itnodes $\in \mathcal{B}_j$ o

$$\begin{pmatrix} (\mathfrak{t}) & \mathfrak{t} \\ \mathfrak{t} \\ \mathfrak{t} \end{pmatrix}^{(\mathfrak{t})} = (-1)^{z_j} \mathfrak{d} \operatorname{tanh}^{-1} \begin{pmatrix} \mathfrak{t} \\ \mathfrak{t} \\ \mathfrak{t} \\ \mathfrak{t} \end{pmatrix}^{(\mathfrak{t})} \operatorname{tanh}(\nu_{\mathfrak{t}'})^{(\mathfrak{t})} \end{pmatrix}^{(\mathfrak{t})}$$

Bitnodes tentative decisions

$$\left\{ \overset{(i)}{\sum}_{\substack{\lambda \leftarrow j, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \sum_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k, \\ \lambda \neq j \in \mathcal{A}_k}} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k}} \mu \overset{(i)}{\sum} \mu \overset{(i)}{\sum}_{\substack{\lambda \in \mathcal{A}_k}} \mu \overset{(i)}{\sum} \mu \overset{$$

$$m, \ldots, 1 = i, \quad j = z_k, \quad j = 1, \ldots, m$$

səbuəllad

- Competing with state-of-the-art data compression (arithmetic coding)
 Lompeting with state-of-the-art data compression (arithmetic coding)
- Arithmetic coding is easily adapted to source with memory (tree sources, Markov sources).
- Arithmetic coding encodes and decodes the source sequence sequentially and can estimate the source statistics parameters (transition probabilities) sequentially (e.g., using the KT estimator).
- Complexity-wise, arithmetic coding is still much simpler and faster than

Partial answers

- Decoding at the encoder: effectively reducing the block-error probability.
- Back to (limited) variable-length: closed-loop iterative doping (CLID) and incremental redundancy (Fountain codes).
- Dealing with memory: incorporating the memory structure of the source in the BP decoder or using a block-sorting transform (BWT).
- Universality: BWT-based minimum description length model and
- Results in Caire-Shamai-Verdu, 2003-2004, Caire-Shokrollahi-Shamai-Verdu, 2004.

Decoding at the Encoder

In contrast to channel decoding, the compressor can run an exact copy of

- Library of Parity-Check Matrices:
 Library of Parity-Check Matrices:
- Closed-loop iterative doping.

Closed Loop Iterative Doping

Every D decoder iterations, the source symbol for which the BP algorithm has accumulated the least reliability is communicated to the decoder:

$$\widehat{\boldsymbol{\lambda}} = \arg \min_{\boldsymbol{\lambda} \leftarrow \widehat{\boldsymbol{\lambda}}} \|\boldsymbol{\nu}_{\boldsymbol{\lambda}}^{(t-1)}\|_{\boldsymbol{\lambda}} + \sum_{\boldsymbol{\lambda} \in \mathcal{A}_{\boldsymbol{\lambda}}} |\boldsymbol{\nu}_{\boldsymbol{\lambda}}^{(t)}|_{\boldsymbol{\lambda}} + \sum_{\boldsymbol{\lambda} \in \mathcal{A}_{\boldsymbol{\lambda}}} |\boldsymbol{\mu}_{\boldsymbol{\lambda}}^{(t-1)}|_{\boldsymbol{\lambda}} = \widehat{\boldsymbol{\lambda}}$$

$$\begin{bmatrix} 0 &= & 3x & 1i & \infty + \\ 1 &= & 3x & 1i & \infty - \end{bmatrix} = \underbrace{\mathfrak{A}}_{\mathcal{A}} \mathfrak{I}$$

- Almost lossless fixed-length version: Fixed number of iterations.
- Lossless variable-length version (zero error probability):
 Dope and iterate until decoded word is correct.
 Choose among the library of H's that leading to the shortest compressed length.

Empirical Distribution of Doped Bits



Biased Coin Experiment: 500-to-303 code



Figure 1: Block error rate of 500-to-303 source codes for a biased coin.

Optimal block coding: (non-constructible) optimal code that assigns a distinct codeword to the most probable 2^{303} source realizations.

Information Spectrum: "Ideal" variable-length coding scheme where the length of the codeword assigned to x_1, \ldots, x_n is equal to $-\log_2 P_{X_1,\ldots,X_n}(x_1,\ldots,x_n)$.

Arithmetic Coding: Nonuniversal, source exactly known.

Code Library: 8 (3,6) regular LDPCs (3 bit overhead).

.etid 02 :poping: 50 bits.

Compression/Decompression Scheme:

G. Caire, S. Shamai, S. Verdú, "Universal Data Compression with LDPC Codes and related topics 3rd International Symposium on Turbo codes and related topics Brest, France, 1 - 5 September 2003

- Pre-processing of the source sequence via the BWT.
- Adaptive Segmentation via MDL principle.
- Communicate to the decoder a quantized version of:
- segmentation
- distributions

Random ensemble of Markov sources



Figure 2: Histogram of redundancies; blocklength = 3000

Random ensemble of Markov sources



Figure 3: Histogram of redundancies; blocklength = 10000

Library of LDPC matrices vs. Fountain Coding



Figure 4: Histogram of redundancies; non-universal p = 0.11, blocklength = 2000



Figure 5: Histogram of redundancies; non-universal p = 0.105, blocklength = 5000

Redundancy (bit/symbol)

CLID versus open-loop incremental redundancy

- Slepian-Wolf separate compression of correlated sources is one of the corner-stones of multiterminal information theory.
- Although known since a long time, it has recently received renewed interest because of new emerging applications (e.g., sensor networks).
- Slepian-Wolf region:

 $(X,X)H \leq {}^{2}\mathcal{A} + {}^{1}\mathcal{R} \quad , (X|X)H \leq {}^{2}\mathcal{A} \quad , (Y|X)H \leq {}^{1}\mathcal{A}$

• Focus on the vertex $R_2 = H(Y)$, $R_1 = H(X|Y)$. Problem: ENC1 must encode X at the conditional entropy without knowing the realization of Y.

Slepian-Wolf random binning

- Randomly partition it into $2^{n(H(X|Y)+1)}$ bins of size $2^{n(I(X)+2\epsilon)}$, $\sim P_X$, and γ randomly partition if into $2^{n(H(X)+1)\epsilon}$.
- Encoding: assuming \mathbf{x} typical, output the index of the bin that contains \mathbf{x} .
- Decoding: the decoder looks into the bin for the \widehat{x} jointly typical with y.
- For any $\epsilon > 0$ and sufficiently large n the probability of encoding and

Slepian-Wolf compression is a channel coding problem

• Assume $\mathcal{X} = \mathbb{F}_q$: S-W operating at $(R_1 = H(X|Y), R_2 = H(Y))$ can be implemented optimally by linear block codes (Wyner scheme).

• Let $\mathbf{H}_1 \in \mathbb{F}_q^{m \times n}$ be a parity-check matrix. A computes the syndrome $\mathbf{s}_1 = \mathbf{H}_1 \mathbf{x}$ and sends it to **B**.

• B has y and s_1 and reconstructs x by ML decoding:

 $(\mathbf{x} | \mathbf{x})_{X|X} \mathbf{f}_{\mathbf{x} = \mathbf{x}_1} \mathbf{h}_{\mathbf{x}} \mathbf{x}_{\mathbf{x}_1 \mathbf{y}} \mathbf{x}_{\mathbf{x}_1 \mathbf{y}} \mathbf{x}_{\mathbf{x}_1 \mathbf{y}} \mathbf{x}_{\mathbf{x}_1 \mathbf{y}} \mathbf{x}_{\mathbf{x}_1 \mathbf{y}_1 \mathbf{x}_1 \mathbf{x}$

- If m/n > H(X|X), for any $\epsilon > 0$ there exist matrices \mathbf{H}_1 such that $P_{\epsilon} < \epsilon$ for sufficiently large n.
- S-W is as hard as achieving channel capacity (with small block error rate!!!).

- Caire-Shamai-Verdu, 2004.
- Let A and B have data vectors $\mathbf{x} \in \mathcal{X}^n$ and $\mathbf{y} \in \mathcal{Y}^n$, respectively.
- . \mathbf{X}, \mathbf{Y} are generated according to some known joint pmf $P_{X,Y}$.
- A and B are connected by a bidirectional lossless channel.
- Goal: make x known to B and y known to B with minimal rate.

Proposition:

 $(X|Y) H \leq {}^{2}\mathcal{H} (X|X), \quad \mathcal{R}_{2} \geq H(Y|X)$

- Achievability: use Slepian-Wolf in both directions.
- Converse: let a genie give y to the encoder in A, the minimum rate to communicate x to B is still H(X|Y). The same argument holds in the reverse direction.

Zhe Slepian-Wolf and data exchange regions



- A is a server that sends a source file x to a client B via an unreliable high.
 A is a server that sends a source file x to a client B via an unreliable high.
- After demodulation/decoding, B has y = x + e, a corrupted version of x.
- A and B are also connected by a bidirectional reliable data link (e.g., GPRS, UMTS, Wired Internet).
- The bidirectional reliable link has low throughput (or high-cost).
- We wish to use efficiently the reliable link to transfer x to B in a fully reliable way by exploiting the fact that B has already received y.

- Suppose that $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ are linked by a BEC with erasure probability p.
- Using a Fountain Code, A produces m > np parity bits ${\bf s}_1$ and sends them to B via the reliable link.
- With high probability, **B** is able to decode **x** since it has received $\approx (1-p)$ symbols via y and additional > np symbols via \mathbf{s}_1 .
- Communication $A \to B$ and zero in the reverse direction.
- Problem: very heavy demand on the performance of the Fountain Code.

- Idea! The bidirectional link affords significant simplification.
- B encodes the erasure pattern using standard data compression and sends it to A.
- A just sends the erased symbols to B.
- No encoding/decoding is needed, and communication take place at rate $\Rightarrow B$. $\Rightarrow B$.
- In the BEC "correlation" case, we achieve the S-W rates in both directions for data exchange and avoid complicated coding and decoding.

- . A of $\mathbf{Y}\mathbf{H}={}_{2}\mathbf{s}$ sbnas **B** ons ,**B** of $\mathbf{x}\mathbf{H}={}_{1}\mathbf{s}$ sbnas **A** . I qat **C** \bullet
- Step 2. Both terminals have $\mathbf{s} = \mathbf{s}_1 \mathbf{s}_2 = \mathbf{H}(\mathbf{x} \mathbf{y})$: they run locally to recover e exact copies of the BP decoder and use CLID over the bidirectional link to recover e exactly.
- At each CLID round, d symbols of x are exchanged in direction $A \rightarrow B$ and d symbols of y in the same positions are exchanged in direction $B \rightarrow A$, such that both terminals can compute the value of e in the doped positions.

Rate of the scheme.

- This scheme achieves $H(X_i Y_i) + \Delta$ in both directions, where Δ is due to CLID and to the suboptimality (gap from capacity) of the LDPC code.
- In general, $\max\{H(X|Y), H(Y|X)\} \ge H(X_i Y_i)$ unless X and Y are non-redundant and e = x y is i.i.d..
- Remark: this is the case where x is a compressed source and y is the result of channel decoding with sufficient interleaving (e.g., multicast of compressed video).

Numerical experiment

- Let x be a binary i.i.d. uniform vector and y = x + e, with e i.i.d. Bernoulli-...
- . Iodmys/fid $4\partial \Phi_{0.0} = (i \Im)H = (i Y i X)H$ gnibleif, $\partial G = 0.0454$ bit/symbol.
- We used an irregular LDPC ensemble with block length n = 60000 and degree sequences optimized using approximated density evolution and

 $^{801}x\ddot{\mathbf{d}}.0+^{701}x\ddot{\mathbf{d}}.0 = (x)q \quad ,^{15}x7\ddot{\mathbf{d}}\mathbf{62}.0+^{05}x3850.0+^{9}x871\pounds.0+^{2}x67\pounds\pounds.0 = (x)\Lambda$

- The compression coding rate is 0.0583, corresponding to 28%
 The compression coding rate is 0.0583, corresponding to 28%
- At each CLID round, a block of d CLID bits are sent. We considered the cases d = 1, 10, 50, 100, 200.

Rate cumulative distribution



Rate cumulative distribution (detail)



I = b , sbrund CLID rounder of protocol CLID rounds, d = 1



Histogram of the number of protocol CLID rounds, d = 100



- It is well-known that feedback does not increase capacity of memoryless
- Nevertheless, feedback may achieve a target P_e with much smaller block
 Nevertheless, feedback may achieve a target P_e with much smaller block
- Shannon's feedback: the encoder at time k knows the channel output
- Burnashev's exponent:

 $(\mathfrak{O}/\mathfrak{A} - \mathfrak{l})\overline{\mathcal{O}} = (\mathfrak{A})_{\ell}\mathfrak{A}$

where \boldsymbol{C} is the channel capacity and

$$({}^{q=X|X} d \|_{p=X|X} d) d \underset{X \ni d, p}{\operatorname{xcm}} = \overline{d}$$

freed scheme achieving Burnashev's exponent

- Step 1: the information message is transmitted using a good nearcapacity achieving code for the underlying DMC (without feedback).
- Step 2: now the encoder knows exactly the state of the decoder and repeating L times the letter a (accept) or b (deny) where a and b are chosen to achieve \overline{D} .
- If "deny" is decoded, the whole block is re-transmitted. If "accept" is decoded, transmission of the current block stops.
- An error occurs when "accept" is decoded while "deny" was transmitted.

- АВQ
- Hybrid-ARQ
- Essentially based on ACK/NACK: performance dominated by the ability of the decoder to detect its error status.
- A problem of practical interest: devise schemes that attain both high reliability and low complexity for given fixed feedback rate $R_{\rm f}$ (ratio of feedback symbols over forward channel symbols).

Proposed scheme

- Caire, Shamai, Verdu 2005.
- Serial concatenation of two LDPC codes: outer coding $b\mapsto x_1,$ inner coding $x_1\mapsto x_2.$
- Step 1: upon reception of the channel output y, the decoder runs BP over the joint Tanner graph and obtains \widehat{x}_1 , such that, assuming interleaving, $e_1 = \widehat{x} x_1 \sim Bernoulli-p$.
- Main feedback: the decoder computes the syndrome $\mathbf{z}_1 = \mathbf{H}_1 \hat{\mathbf{x}}_1 = \mathbf{H}_1 \hat{\mathbf{x}}_1$. If $\mathbf{z}_1 = 0$, the receiver declares the subvector of $\hat{\mathbf{x}}_1$ as the output. If $\mathbf{z}_1 \neq 0$, \mathbf{z}_1 is sent over the feedback link.
- The encoder knows \mathbf{x}_1 and \mathbf{z}_1 and the decoder knows $\hat{\mathbf{x}}_1$ and \mathbf{z}_1 , but

- Step 2: both encoder and decoder run BP simultaneously on the Tanner graph of the outer code with syndrome equal to z1, and variable nodes associated to the elements of e1.
- Problem: similar to the bidirectional data exchange, but CLID cannot be
- Answer: we use a noisy version of the CLID algorithm ... the "dirty CLID".

• Let ℓ the position of the least reliable symbol at a given doping iteration, then the encoder sends $x_{1,\ell}$ through the forward channel which outputs $y_{1,\ell}$. The decoder computes the MAP estimates $\widetilde{x}_{1,\ell}$ and $\widetilde{e}_{1,\ell} = \widetilde{x}_{1,\ell} - \widehat{x}_{1,\ell}$, and the forward channel which outputs and $\psi_{1,\ell}$.

 Both encoder and decoder have the same noisy observation of e1,8 and can update their BP algorithm by incorporating the additional message

 $\Im\operatorname{sol}{}^{\mathfrak{I},\mathfrak{I}^{\mathfrak{H}}}(\mathfrak{I}-)$

for the ℓ -th variable node.

The BP algorithms at the encoder and decoder remain synchronized.
 The decoding process stops at an iteration when its guess ê1 satisfies the parity-check equations, i.e.,

 $\mathbf{I}\widehat{\mathbf{O}}_{1}\mathbf{H}=\mathbf{I}\widehat{\mathbf{O}}_{1}$

Design options

- The outer code must be optimized for a BSC with probability of error p.
- rate is given by $\mathbb{E}[d]$ the expected number of doped bits, the resulting feedback

$$\eta_{f} = \frac{\pi r_{2}(1-r_{1}) + \mathbb{E}[d]}{[n] + \mathbb{E}[d]} \approx r_{2}(1-r_{1}) + \eta$$

.(vonsbruber gridob) llsms si η eradundancy).

- Two extreme cases.
- Choosing a trivial inner code and an outer code optimized for the forward value of the formark of $\epsilon > 0$. channel, we get $r_2 = 1$ and $r_1 = C - \epsilon$, with some gap-to-capacity $\epsilon > 0$. which is a code design parameter. This choice yields $R_f \approx 1 - C + \epsilon + \eta$.

• Choosing an inner code optimized for the forward channel yields $r_2 = 1 - \delta(p) - \epsilon = 1$. This yields

$$\mathcal{U}^{\dagger} = (\mathcal{O} + (\mathcal{O})\mathcal{U})(\mathbf{v} - \mathcal{O}) = {}^{f}\mathcal{U}$$

which can be made as small as desired.

- Data compression via linear block codes, from the pure data compression
 Data compression via linear block codes, from the pure data compression
- ON THE BAD SIDE: residual error probability, complexity of BP decoding.
- ON THE GOOD SIDE: linear mapping has generally a well conditioned inverse (non-catastrophic!): a small Hamming distance between encoded sequences reflects into a small Hamming distance of the source reconstructed sequence.
- Standard state-of-the-art data compression has generally catastrophic inverse: one bit error yields a random reconstructed sequence, almost independent of the independent sequence.

Option 1: \approx optimal quantization with clever indexing



Option 2: Suboptimal quantization with entropy coding



Option 1: Multistage TCQ + standard LDPC coding



Option 2: ECSQ + LDPC coding for data compression



Comparison with successive refinement scalar

noitezitneup



Design tradeoffs

- Multistage TCQ based on binary CC (typically, rate 1/4, 128 states) yields an efficient successive refinement quantization scheme, yet, suboptimal at high rates.
- Binary CC yields directly a non-catastrophic binary indexing (directly following from non-catastropic property of the CC encoder).
- Soft-reconstruction (softbits) yields just minor improvement w.r.t. hard
- Entropy-Constrained Scalar Quantization is much simpler but not generally succesively refinement.
- It requires careful mapping of M-ary indices onto binary: we have investigated multi-level coding, by exploiting the entropy chain rule:

 $({}_{1}d, \ldots, {}_{1-m}d|_{m}d)H \cdots + ({}_{1}d|_{2}d)H + ({}_{1}d)H = (\eta)H$

- Pleasant reminiscence of the "bit-plane" structure of practical source
 Pleasant reminiscence (e.g., JPEG2000).
- It is expected that ECTCQ + carefully designed LDPC yields the best
 performance (to be optimized and demonstrated ...).

- Concatenation of predictive quantization for images, followed by adaptive probability estimation/identification and compression by multi-level Turbo
 Codes [Kim, Sesia, Ramstad and Caire, 2005].
- In this work we exploit the fact that the quantized source after predictive quantization looks like a non-stationary but independent M discrete source.
- Concatenation of Wavelet transform, quantization and Markov (context) model estimation of JPEG2000 with multi-level Turbo-Codes [on-going work with M. Fresia].
- In this work we exploit the fact that JPEG2000 models the bitplanes as non-stationary binary Markov-Chains, whose structure can be incorporated into the BP decoder.

A numerical experiment



Conclusions

- Data compression via linear coding $\mathbf{z} = \mathbf{H} \mathbf{x}$ is theoretically an optimal fixed-to-fixed length data compression scheme.
- . Because of complexity, we use sparse ${\bf H}$ and BP decoding.
- Good performances in the non-universal and universal case can be obtained by decoding at the encoder, using a library of matrices, CLID, BWT, MDL probability model estimation.
- Although competing with state-of-the art is very hard for the pure data (lossless) compression case, linear block coding has unique "noncatastrophic" features that make it a key building block for robust JSCC.
- Distributed data compression (Slepian-Wolf) is a channel coding

Open problems

- Open problem 1: using modern (sparse-graph based) techniques for lossy compression. This is a totally different approach, linear maps cannot be optimal for lossy coding!.
- Preliminary results in special cases: Zecchina, Mezard et al., building on the analogy with the K-SAT problem and using techniques such as Survey Propagation.
- Open problem 2: lossy transmission for a compound/broadcast channel, achievable distortion region.
- Very important for future DAB/DVB, and MM broadcasting for 3G+.
- Best known performances are obtained by Hybrid analog-digital