

Capacity-Achieving Accumulate-Repeat-Accumulate Codes for the BEC with Bounded Complexity

Igal Sason¹ and Henry D. Pfister²

Department of Electrical Engineering¹
Techion Institute, Haifa, Israel

School of Computer and Communication Sciences²
Swiss Federal Institute of Technology, Lausanne

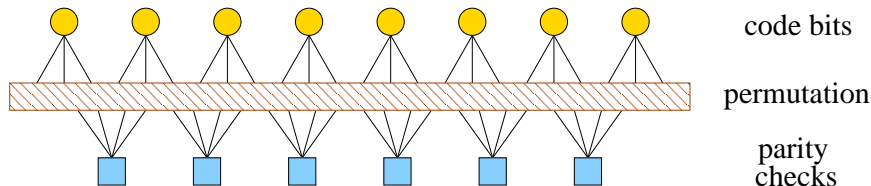
ITA Inaugural Workshop, UC San Diego
February 6–10, 2006

Thanks to Intel Israel for Supporting this Research Work

Outline

- 1 Capacity-Achieving Codes and Complexity
- 2 Accumulate-Repeat-Accumulate Codes
- 3 Simulations
- 4 Symmetry, Duality, and New Ensembles
- 5 Summary

Low-Density Parity-Check (LDPC) Codes

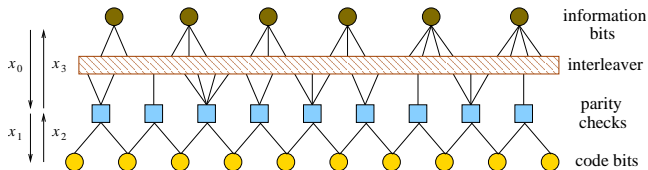


- Irregular Ensembles Defined by Degree Distribution (d.d.)
 - L_i (resp. R_i) is the fraction of bit (resp. check) nodes with degree i
 - λ_i (resp. ρ_i) is the fraction of edges with bit (resp. check) degree i
 - Associated functions: $L(x) = \sum_i L_i x^i$ and $\lambda(x) = \sum_i \lambda_i x^{i-1}$
- Random Permutation Between Bit and Check Nodes
 - Analysis averages over all possible permutations
 - Many results hold for almost all permutations as $n \rightarrow \infty$

Repeat-Accumulate (RA) Type Codes



- IRA Codes: Encoding Point of View
 - Irregular Repeat: fraction L_i of bits repeated i times
 - Irregular Single Parity: fraction R_i checks have degree i
 - Accumulate mapping: $x_1^n \rightarrow y_1^n$ with $y_i = y_{i-1} + x_i$
 - Fraction α of the information bits are sent
- IRA Codes: Decoding Point of View
 - LDPC type decoding graph with added "accumulate" section



Complexity vs. Gap to Capacity

What is the complexity of achieving a rate $(1 - \varepsilon)C$?

Theorem (Sason & Urbanke A)

Under iterative message-passing decoding, the decoding complexity per information bit of LDPC codes, without puncturing, grows at least like $\log \frac{1}{\varepsilon}$ (i.e., the log of the inverse of the gap to capacity).

Theorem (Sason & Urbanke B)

*Under iterative message-passing decoding, the decoding complexity per information bit of **systematic** IRA (SIRA) codes grows at least like $\log \frac{1}{\varepsilon}$ (i.e., the log of the inverse of the gap to capacity).*

Decoding complexity is *unbounded* as the gap to capacity vanishes!

C.A. Codes for the BEC with Bounded Complexity

Two sequences of non-systematic IRA (NSIRA) codes

which asymptotically achieve capacity on the BEC with **bounded complexity per information bit**. [Pfister, Sason & Urbanke, *IEEE Trans. on Information Theory*, July 2005]

This new result was achieved by puncturing bits and thereby allowing a sufficient number of state nodes in the Tanner graph.

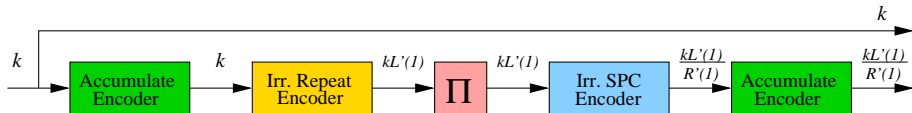
Drawback

The convergence speed to the ultimate performance limit happens to be quite slow in terms of the block length.

This motivates our search for new c.a. codes with *bounded complexity*

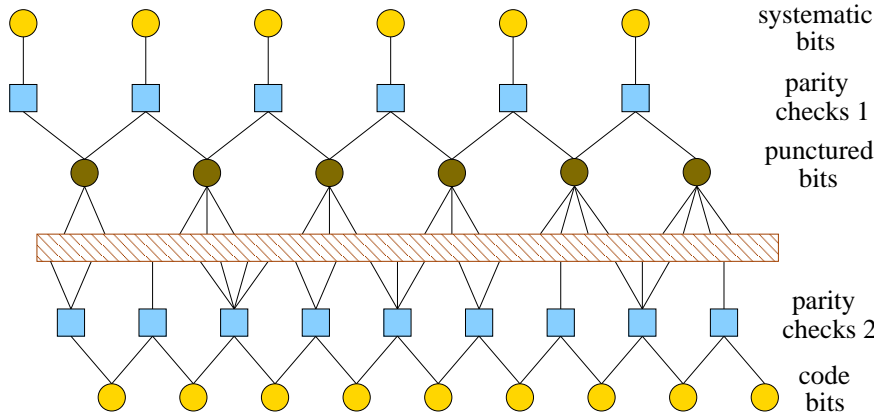
Accumulate-Repeat-Accumulate (ARA) Codes

- These codes are a generalization of the IRA codes; they were introduced by Abbasfar, Divsalar and Yao (ISIT 2004)
- They have good performance and simple linear-time encoding



- Encoder diagram for the systematic ARA ensemble
 - Accumulate block is the rate-1 $\frac{1}{1+D}$ encoder
 - Irregular Repeat: fraction L_i of bits repeated i times
 - Irregular SPC: fraction R_i single parity checks have degree i
 - Block sizes are shown starting with k info bits

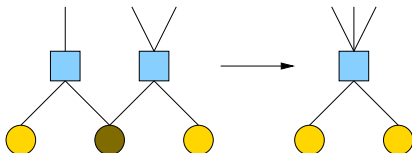
The Decoding Graph for ARA Codes



- Shading is used to denote punctured or erased bits

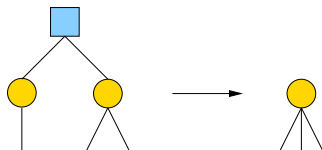
Graph Reduction for Code Bits

- Any “code bit” node whose value is not erased by the BEC can be removed from the graph by absorbing its value into its two “parity-check 2” nodes.
- When the value of a “code bit” node is erased, one can merge the two “parity-check 2” nodes which are connected to it (by summing the equations) and this removes the “code bit” from the graph.
- Merging two “parity-check 2” nodes causes their degrees to be summed.

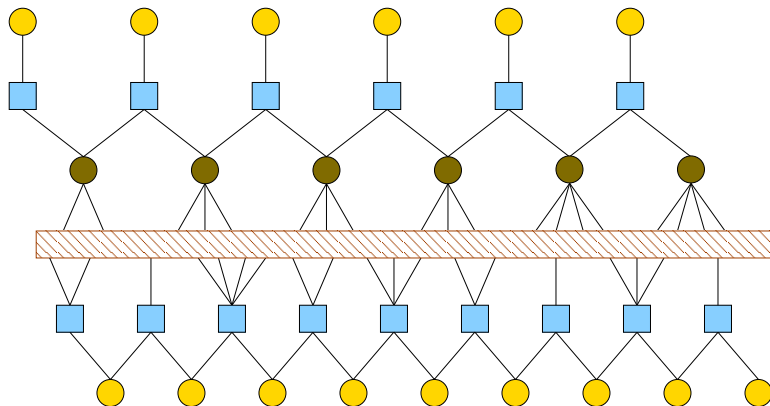


Graph Reduction for Systematic Bits

- The “systematic bit” nodes in the Tanner graph of the systematic ARA codes only provide channel information. Erasures make them worthless, and they can be removed along with their “parity-check 1” nodes without affecting the decoder.
- When the value of a “systematic bit” node is observed (assume the value is zero w.o.l.o.g.), it can be removed leaving a degree 2 parity-check.
- Degree 2 parity-checks imply equality, and allow the connected “punctured bit” nodes to be merged (summing their degrees).

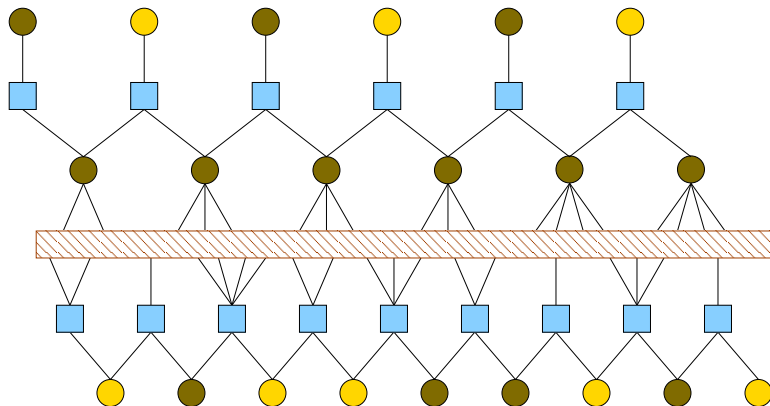


Example of Graph Reduction



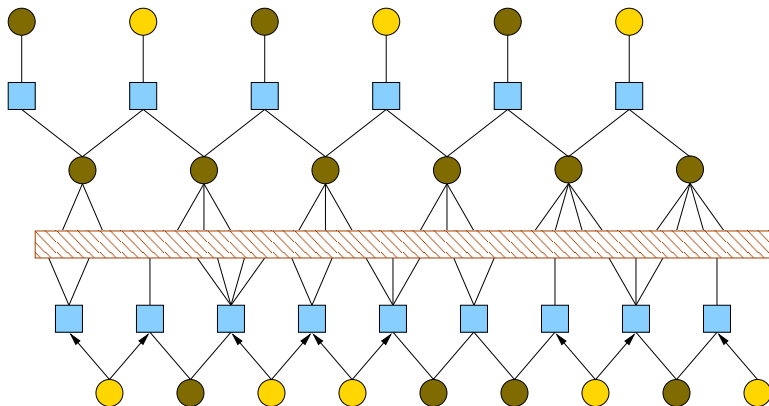
Original Tanner graph

Example of Graph Reduction



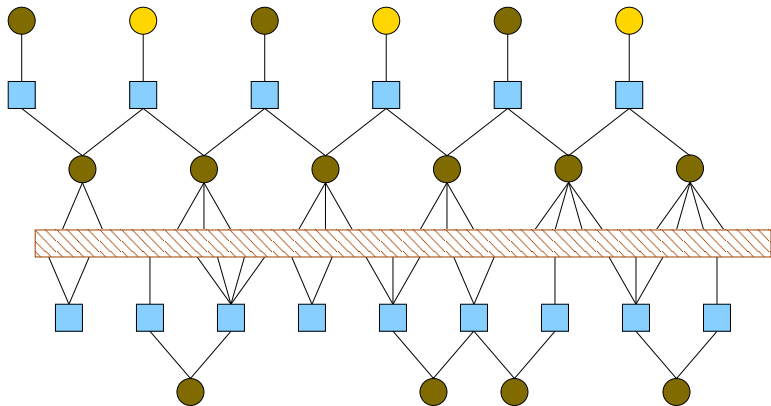
Add erasures from channel

Example of Graph Reduction



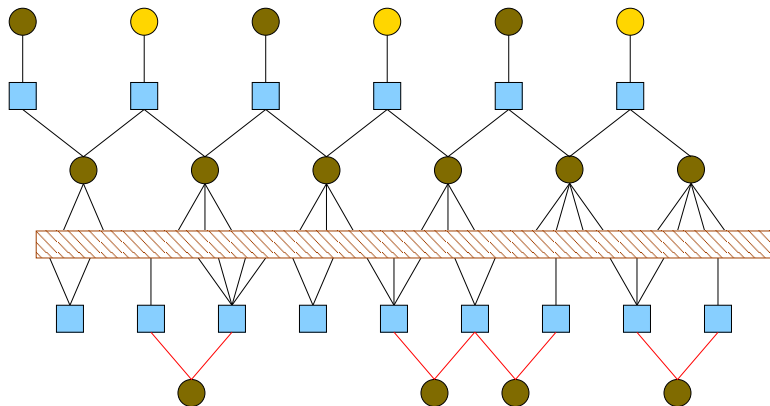
Mark known code bits

Example of Graph Reduction



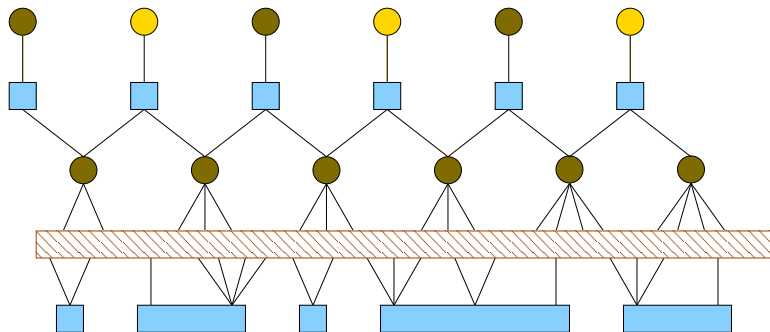
Merge values into checks

Example of Graph Reduction



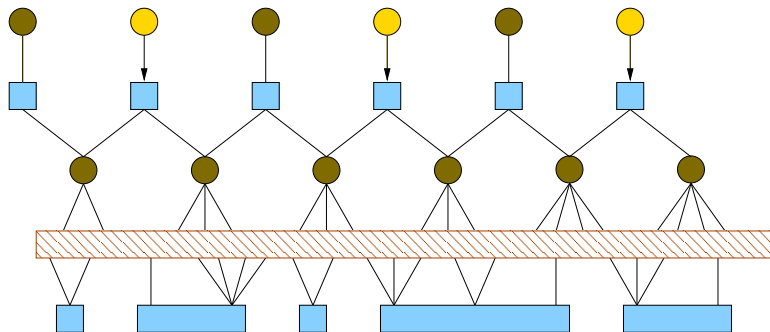
Mark unknown code bits

Example of Graph Reduction



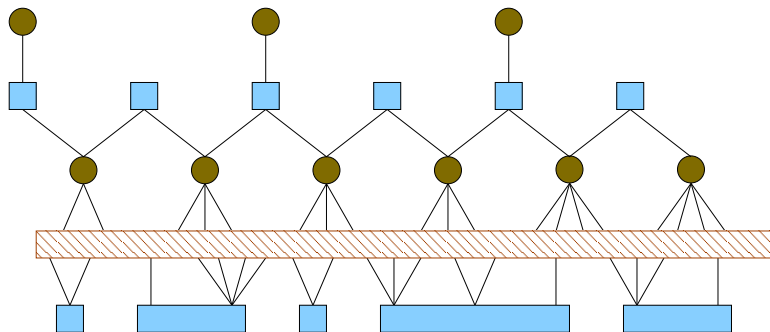
Sum check equations to remove

Example of Graph Reduction



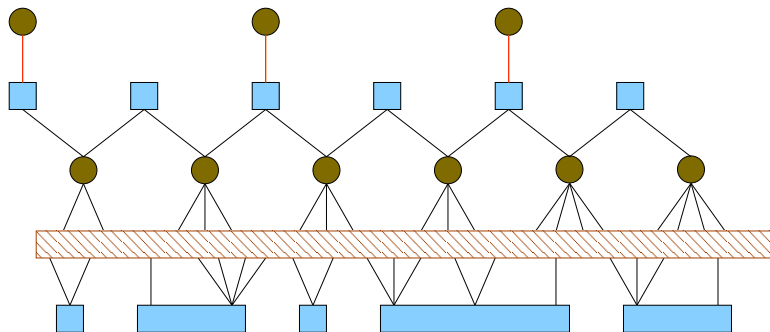
Mark known systematic bits

Example of Graph Reduction



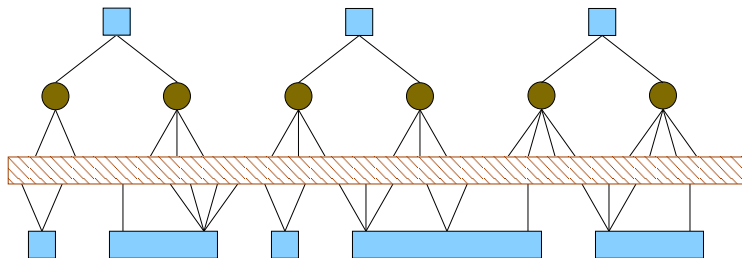
Merge values into checks

Example of Graph Reduction



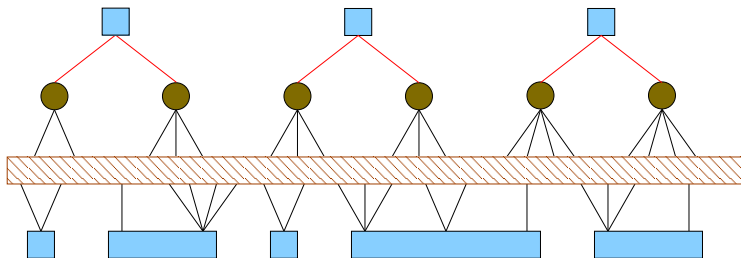
Mark unknown systematic bits

Example of Graph Reduction



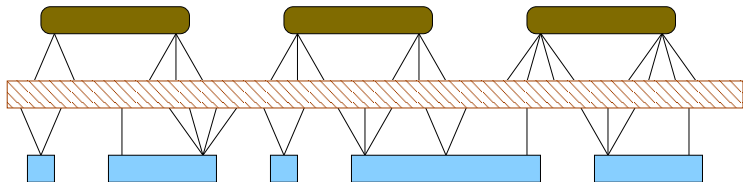
Remove unknown systematic bits

Example of Graph Reduction



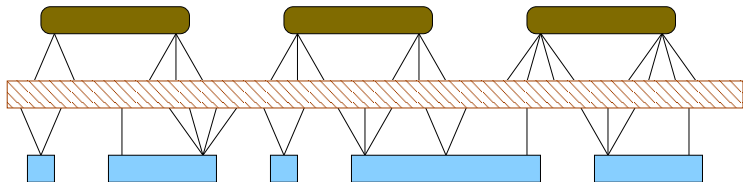
Mark degree 2 check nodes

Example of Graph Reduction



Combine bit nodes to remove

Example of Graph Reduction



Tanner graph of residual LDPC

Density Evolution via Graph Reduction for ARA Codes

After the graph reduction, we are left with a standard LDPC ensemble whose new edge-perspective degree distributions are given by

$$\tilde{\rho}(x) = \frac{\tilde{R}'(x)}{\tilde{R}'(1)} = \frac{(1-p)^2 \rho(x)}{(1-pR(x))^2}$$

$$\tilde{\lambda}(x) = \frac{\tilde{L}'(x)}{\tilde{L}'(1)} = \frac{p^2 \lambda(x)}{(1-(1-p)L(x))^2}$$

- Swapping p with $1-p$ exposes a nice symmetry between the information and parity bits

Capacity-Achieving ARA Codes (1)

- Suppose we choose the d.d. after graph reduction to be

$$\tilde{\lambda}(x) = \tilde{\rho}(x) = \frac{(1-b)x}{1-bx} \quad 0 < b < 1.$$

- Since $\tilde{\lambda}(1 - \tilde{\rho}(1 - x)) = x$, this choice gives a c.a. LDPC ensemble after graph reduction
- Inverting the graph reduction to get the original d.d. gives

$$L(x) = \frac{bx + \ln(1 - bx)}{p [b + \ln(1 - b)] + (1 - p) [bx + \ln(1 - bx)]}$$

$$R(x) = \frac{bx + \ln(1 - bx)}{(1 - p) [b + \ln(1 - b)] + p [bx + \ln(1 - bx)]}.$$

Capacity-Achieving ARA Codes (2)

Theorem (Self-Matched ARA Codes)

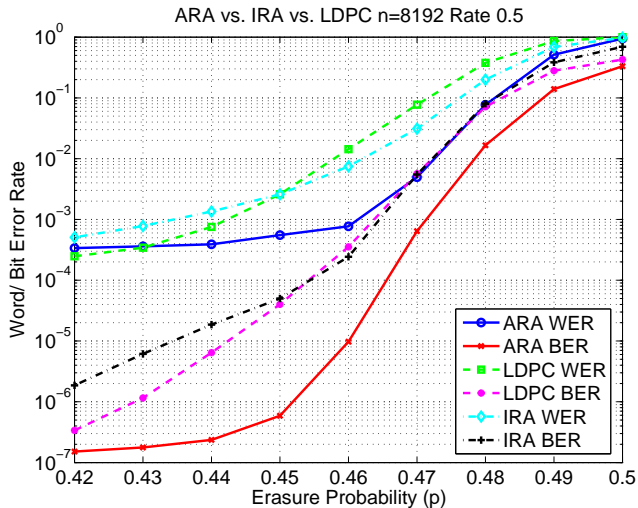
The power series expansions of $L(x)$ and $R(x)$ are non-negative for $p \in (0, 1)$ if b is chosen (in terms of Lambert W -function) to be

$$b = W \left(-e^{-\frac{13+\sqrt{61}}{12} \frac{1+|1-2p|}{1-|1-2p|} - 1} \right) + 1.$$

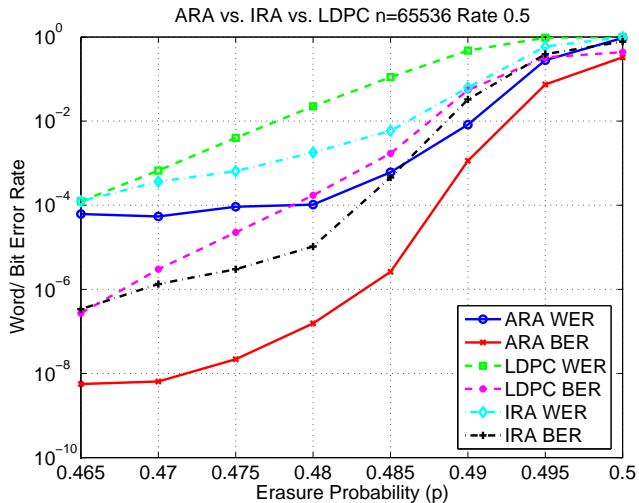
Therefore, the ARA ensemble defined by (L, R) achieves capacity on the BEC under iterative decoding for $p \in (0, 1)$.

*Moreover, the tails of the d.d. **decay exponentially** fast and the encoding/decoding complexity is bounded.*

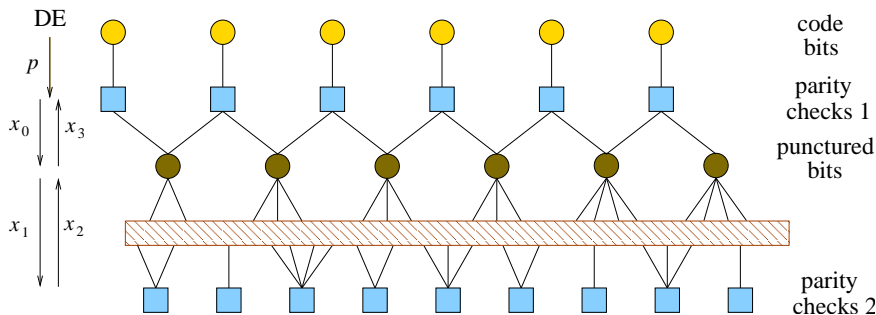
Computer Simulations (1)



Computer Simulations (2)

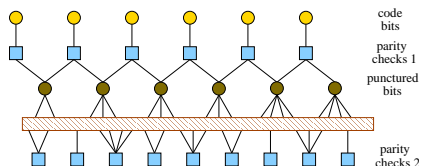
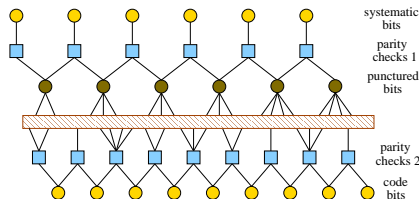


Accumulate LDPC (ALDPC) Codes



- After "accumulate", code bit sequence belongs to an LDPC code
- Natural image of NSIRA codes under the duality transformation
- Graph reduction only on bit d.d. (versus check d.d. for NSIRA)

Summary



- How would you like your LDPC codes served?
 - With a little accumulate on top? on the bottom? or both?
- On the left: Accumulate-Repeat-Accumulate (ARA) Codes
 - LDPC + Accumulate on top and bottom
 - Self-dual ensemble unchanged under bit/check swap
- On the right: Accumulate-LDPC (ALDPC) Codes
 - LDPC + Accumulate on top
 - Natural dual of NSIRA ensemble under bit/check swap

Summary (Cont.)

- Introduced Various Capacity-Achieving (C.A.) Codes with Bounded Complexity
 - ARA Codes: Systematic codes with bounded complexity
 - LDPC Codes: Good minimum distance and bounded complexity
 - Simulations show ARA superior to other c.a. ensembles
- Introduced Density Evolution Via Graph Reduction
 - Exposes natural symmetry between LDPC, ARA and NSIRA codes
 - Allows c.a. LDPC codes to be mapped onto other code structures
- **Full paper:** H. Pfister and I. Sason, "Capacity-achieving ensembles of accumulate-repeat-accumulate codes for the erasure channel with bounded complexity", submitted to *IEEE Trans. on Information Theory*, December 1st, 2005.
[Online]. Available:
<http://arxiv.org/abs/cs.IT/0512006>.