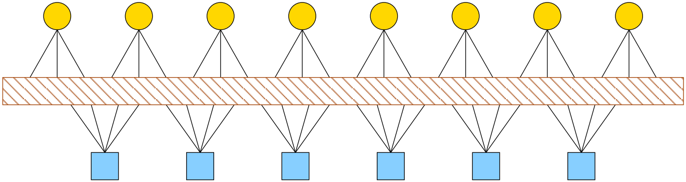
Accumulate-Repeat-Accumulate Codes: Systematic Codes Achieving the Binary Erasure Channel Capacity with Bounded Complexity

Henry D. Pfister (EPFL)
Igal Sason (Technion)

Forty-Third Annual Allerton Conference
on Communication, Control and Computing
September 28–30, 2005

Low-Density Parity-Check (LDPC) Codes (1)



- Irregular ensembles defined by (λ, ρ) or degree distribution (d.d.)
  - where $\lambda(x) = \sum_{i \geq 2} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i \geq 2} \rho_i x^{i-1}$
  - λ_i and ρ_i are the fraction of edges attached to bit and parity-check nodes of degree i
- Capacity-achieving (c.a.) sequences of LDPC codes for the BEC were introduced by Luby et al. and Shokrollahi.

Low-Density Parity-Check (LDPC) Codes (2)

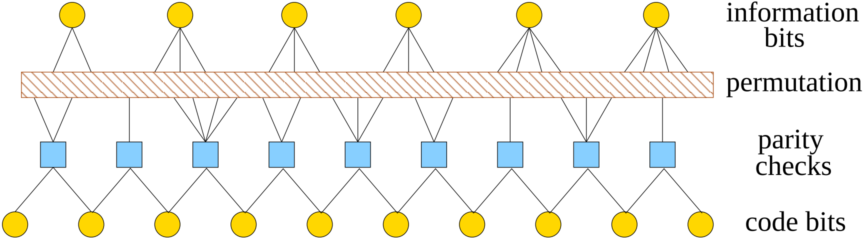
- Consider any sequence $\{(n, \lambda, \rho)\}$ of ensembles of LDPC codes
- Let transmission occur over a binary erasure channel (BEC)
- Assume the sequence achieves asymptotically (i.e., as the block length n tends to infinity) a fraction $1 - \varepsilon$ of the channel capacity with vanishing bit erasure probability

Theorem (1)

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).

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

Irregular Repeat-Accumulate (IRA) Codes



Theorem (2)

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).
$\Rightarrow$ Decoding complexity is *unbounded* as the gap to capacity vanishes !

Can These Results Be Improved ?

Question

What about non-systematic IRA codes whose information bits are punctured before transmission ?

C.A. Codes for the BEC with Bounded Complexity (1)

Two sequences of non-systematic IRA (NSIRA) codes

which asymptotically achieve capacity on the BEC with bounded complexity per information bit. *[PSU, IEEE Trans. on IT, 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, so for small to moderate block lengths, the new codes are not record breaking.

C.A. Codes for the BEC with Bounded Complexity (2)

- We are interested in new code constructions which are better than the previous constructions in terms of convergence speed to capacity as a function of the block length
- From a practical point of view, it would also be nice to have systematic codes

Goal

Construct systematic codes which approach capacity for moderate block lengths and have bounded complexity per information bit

Accumulate-Repeat-Accumulate (ARA) Codes

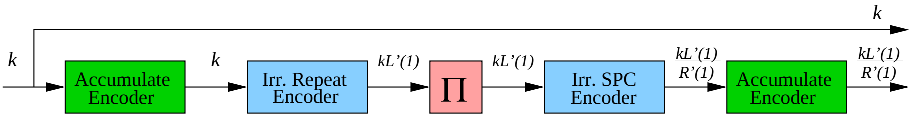
- These codes are a generalization of the IRA codes which were introduced by Abbasfar, Divsalar and Yao (ISIT 2004)
- They have outstanding performance and simple linear-time encoding

Capacity-Achieving Ensembles of ARA Codes?

We consider the suitability of systematic irregular ARA codes for the construction of capacity-achieving ensembles for the BEC with bounded complexity.

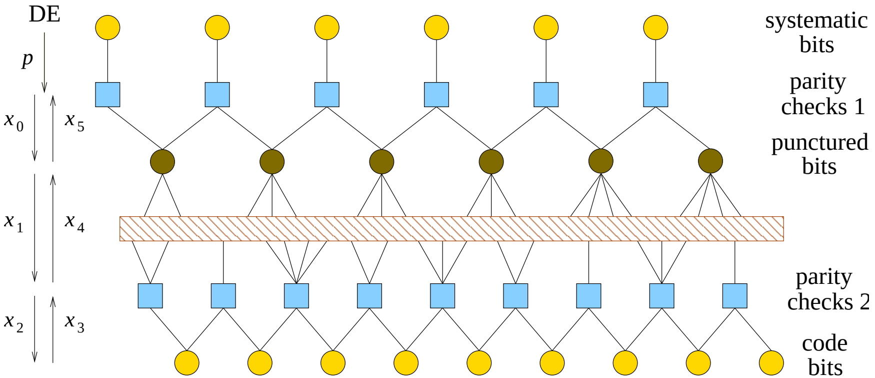
We also examine by computer simulations their performance for moderate to large block length.

Systematic ARA Codes: Encoder



- Encoder diagram for the systematic ARA ensemble
  - "Accumulate" block is the standard rate-1 $\frac{1}{1+D}$ encoder
  - "Irr. Repeat" block repeats each bit a different number of times
  - "Irr. SPC" block groups bit in different size blocks and outputs a single parity bit for each block
  - Block sizes are shown on each arrow for k information bits

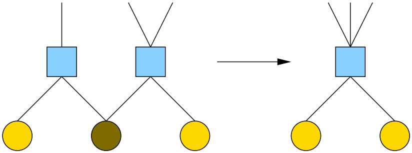
Systematic ARA Codes: Tanner Graph



- Shading is used to denote punctured or erased bits

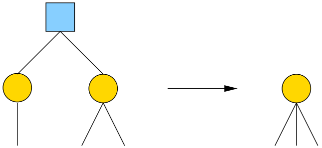
Graph Reduction for Code Bits

- 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.

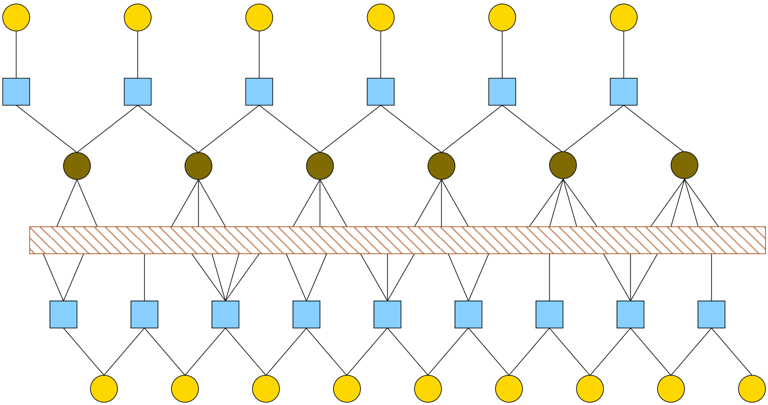


Graph Reduction for Systematic Bits

- 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).

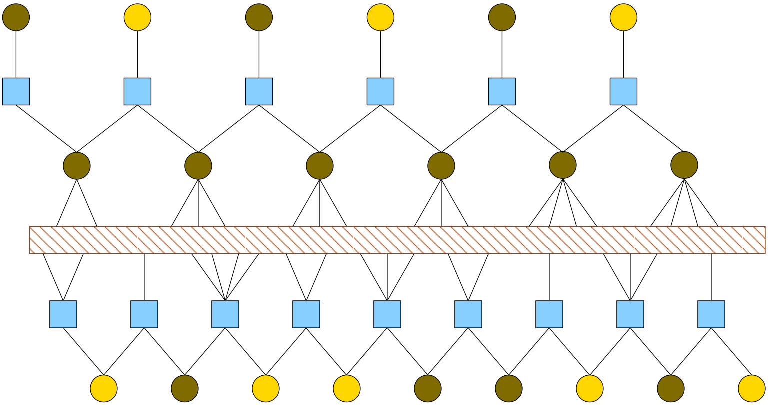


Example of Graph Reduction



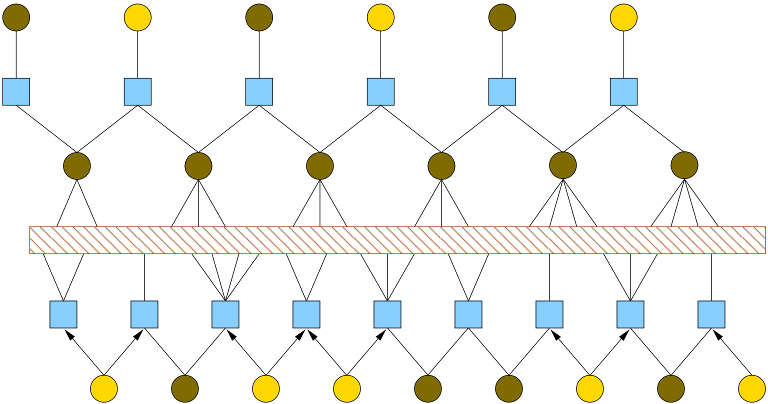
Original Tanner graph

Example of Graph Reduction



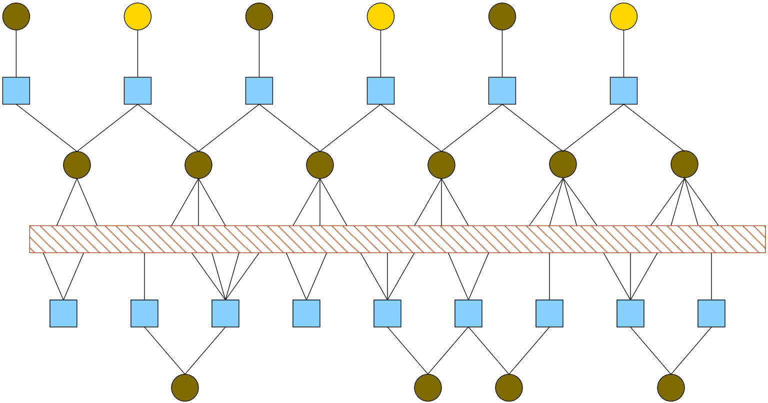
Add erasures from channel

Example of Graph Reduction



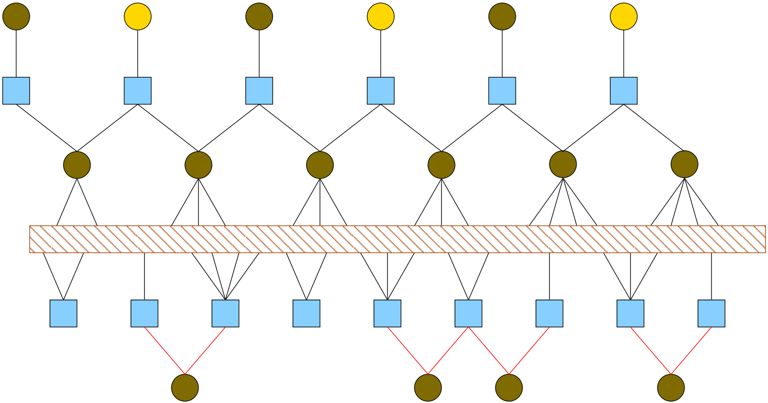
Mark known code bits

Example of Graph Reduction



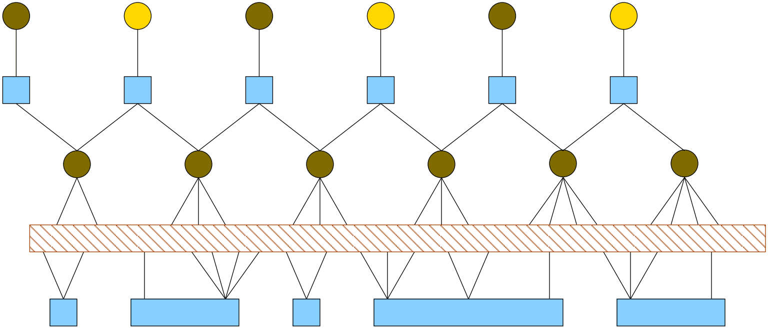
Merge values into checks

Example of Graph Reduction



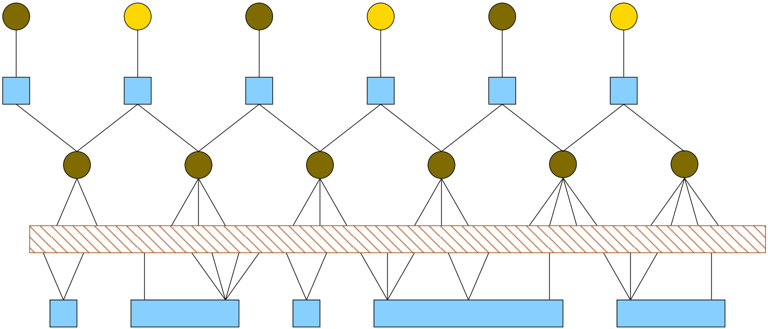
Mark unknown code bits

Example of Graph Reduction



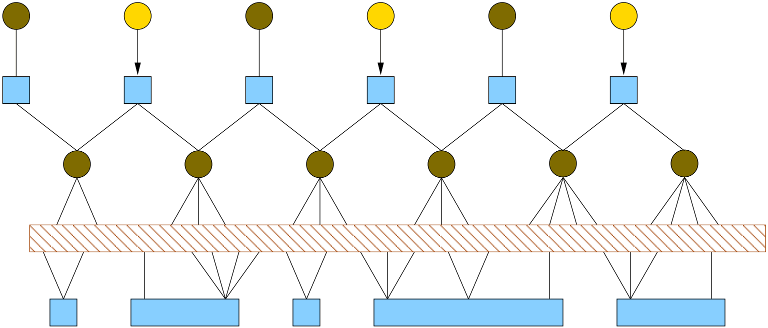
Sum check equations to remove

Example of Graph Reduction



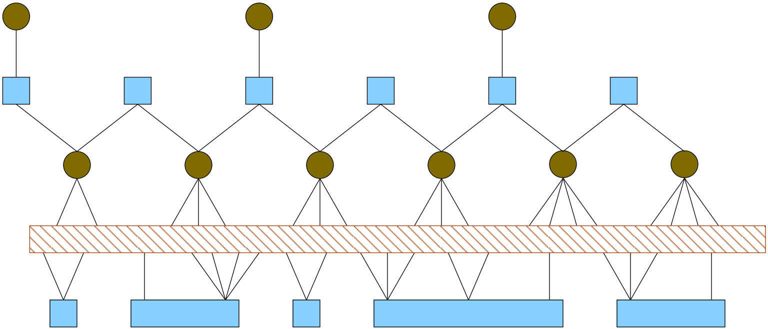
Tanner graph after check node graph reduction

Example of Graph Reduction



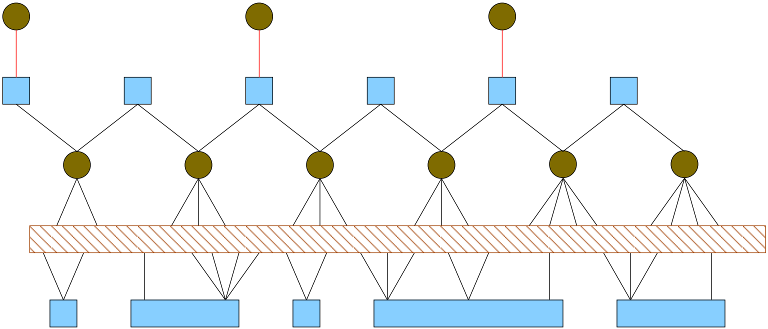
Mark known systematic bits

Example of Graph Reduction



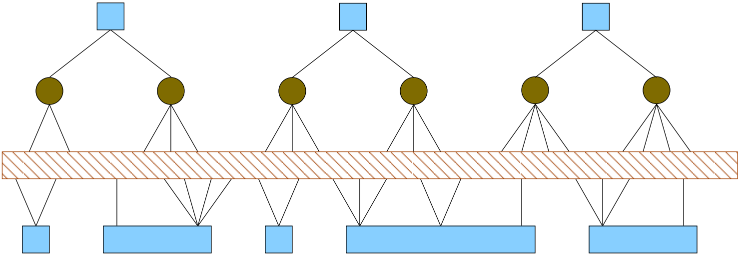
Merge values into checks

Example of Graph Reduction



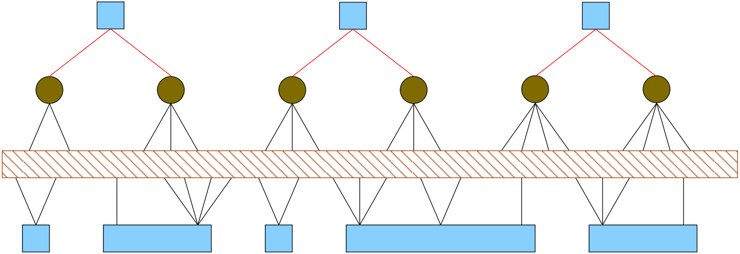
Mark unknown systematic bits

Example of Graph Reduction



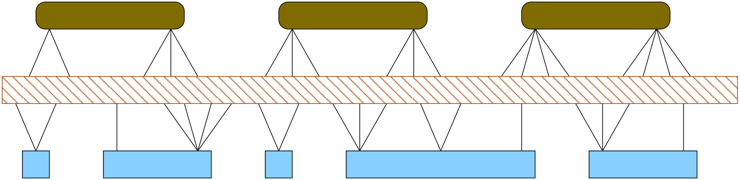
Remove unknown systematic bits

Example of Graph Reduction



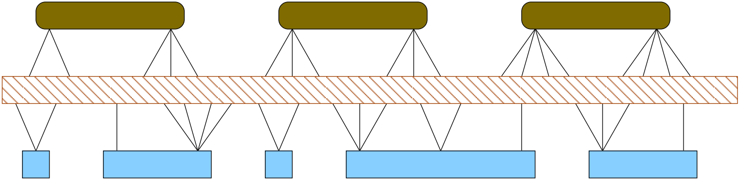
Mark degree 2 check nodes

Example of Graph Reduction



Combine bit nodes to remove

Example of Graph Reduction



Tanner graph of residual LDPC

Density Evolution via Graph Reduction (1)

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

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

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

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

Density Evolution via Graph Reduction (2)

After the graph reduction, all the “systematic bit" nodes and “code bit" nodes are removed.

- The residual LDPC code effectively sees a BEC whose erasure probability is 1
- Therefore, the DE fixed point equation is given by

$$\widetilde{\lambda}_{1-p}\big(1-\widetilde{\rho}_p(1-x)\big) = x,$$

where

$$\widetilde{f}_p(x) \triangleq \frac{(1-p)^2 f(x)}{\left(1-\frac{p\int_0^x f(t)dt}{\int_0^1 f(t)dt}\right)^2}.$$

Symmetry Properties of Capacity-Achieving Codes

- In the following, we discuss the symmetry between the bit and check degree distributions of c.a. ensembles for the BEC.
- First, we describe this relationship for LDPC codes, and then we extend it to ARA codes.
- The extension is based on combining the DE analysis of LDPC codes with graph reduction analysis of ARA codes.

Symmetry Properties of C.A. LDPC Codes (1)

The relationship between the bit d.d. and check d.d. of c.a. ensembles of LDPC codes can be expressed in a number of ways. Starting with the DE fixed point equation

$$p\lambda\big(1-\rho(1-x)\big) = x \qquad (1)$$

where p designates the erasure probability of the BEC, we see that picking either the d.d. λ or ρ determines the other d.d. exactly.

Symmetry Properties of C.A. LDPC Codes (2)

A few definitions are needed to discuss things properly. Following the notation by Oswald and Shokrollahi (IT, Dec. 2002), let

$$\mathcal{P} \triangleq \left\{ f : f(x) = \sum_{k=1}^{\infty} f_k x^k,\ x \in [0,1], \quad f_k \geq 0,\ f(0) = 0,\ f(1) = 1 \right\}.$$

Let the operator $\mathcal{T}$ transform invertible functions $f : [0,1] \rightarrow [0,1]$ to

$$\mathcal{T}f(x) \triangleq 1 - f^{-1}(1-x)$$

Let $\mathcal{A}$ be the set of all functions $f \in \mathcal{P}$ such that $\mathcal{T}f \in \mathcal{P}$, i.e.,

$$\mathcal{A} \triangleq \left\{ f : f \in \mathcal{P}\ ,\ \mathcal{T}f \in \mathcal{P} \right\}.$$

Symmetry Properties of C.A. LDPC Codes (3)

The set of capacity-achieving LDPC codes for $p = 1$

The first step towards proving (λ, ρ) is a c.a. d.d. pair is showing that $\lambda \in \mathcal{A}$. For $p = 1$, this is almost the only step. So, we define the set of d.d. pairs which satisfy the DE fixed point equation by

$$\begin{aligned} \mathcal{C}_{\text{LDPC}} &\triangleq \left\{ (\lambda, \rho) \in \mathcal{P} \times \mathcal{P} \mid \lambda\big(1 - \rho(1-x)\big) = x \right\} \\ &= \left\{ (\lambda, \rho) \mid \lambda \in \mathcal{A},\ \rho = \mathcal{T}\lambda \right\}. \end{aligned}$$

The *symmetry property* of c.a. LDPC codes with rate 0

$$(\lambda, \rho) \in \mathcal{C}_{\text{LDPC}} \xleftrightarrow{\text{symmetry}} (\rho, \lambda) \in \mathcal{C}_{\text{LDPC}}$$

Symmetry Properties of C.A. ARA Codes

The set of capacity-achieving ARA degree distributions

$$\mathcal{C}_{\text{ARA}}(p) \triangleq \left\{ (\lambda, \rho) \in \mathcal{P} \times \mathcal{P} \;\middle|\; \widetilde{\lambda}_{1-p}\big(1 - \widetilde{\rho}_p(1-x)\big) = x \right\}$$

Symmetry diagram for LDPC and ARA codes

$$\begin{tikzcd}
(\lambda, \rho) \in \mathcal{C}_{\text{ARA}}(p) \arrow[r, leftrightarrow, "\text{ARA symmetry}"] \arrow[d, shift right, "\mathcal{G}_{\text{ARA}}"'] & (\rho, \lambda) \in \mathcal{C}_{\text{ARA}}(1-p) \arrow[d, shift left, "\mathcal{G}_{\text{ARA}}"] \\
(\widetilde{\lambda}_{1-p}, \widetilde{\rho}_p) \in \mathcal{C}_{\text{LDPC}} \arrow[r, leftrightarrow, "\text{LDPC symmetry}"] \arrow[u, dashed, shift right] & (\widetilde{\rho}_p, \widetilde{\lambda}_{1-p}) \in \mathcal{C}_{\text{LDPC}} \arrow[u, dashed, shift left]
\end{tikzcd}$$

$\mathcal{G}_{ARA}$ is the graph reduction mapping from (λ, ρ) to $(\widetilde{\lambda}_{1-p}, \widetilde{\rho}_p)$

Matched Functions

Definition

The functions f and g are said to be matched if

$$\mathcal{T}f = g.$$

Note that $\mathcal{T}^2 f = f$ for any function f, so

$$\mathcal{T}f = g \Longleftrightarrow \mathcal{T}g = f.$$

Example (Self-Matched Function)

$$f(x) = \frac{(1-b)x}{1-bx} \quad 0 < b < 1$$

is a function matched to itself (i.e., $\mathcal{T}f = f$), and it also has a non-negative power series expansion around zero.

Construction of C.A. ARA codes for the BEC (1)

The algorithm proceeds as follows:

- Choose a function $f \in \mathcal{A}$, and set the pair of tilted d.d. from the edge perspective (after graph reduction) to

$$\widetilde{\lambda} = f, \quad \widetilde{\rho} = \mathcal{T}f.$$

- Calculate the pair of tilted d.d. from the node perspective

$$\widetilde{L}(x) = \frac{\int_0^x \widetilde{\lambda}(t)\, dt}{\int_0^1 \widetilde{\lambda}(t)\, dt}, \quad \widetilde{R}(x) = \frac{\int_0^x \widetilde{\rho}(t)\, dt}{\int_0^1 \widetilde{\rho}(t)\, dt}.$$

Construction of C.A. ARA codes for the BEC (2)

- Calculate the original d.d. pair w.r.t. the nodes (i.e., the original d.d. pair before the graph reduction) by the equations

$$L(x) = \frac{\widetilde{L}(x)}{p + (1-p)\widetilde{L}(x)}\,, \quad R(x) = \frac{\widetilde{R}(x)}{1 - p + p\widetilde{R}(x)}$$

- Critical Point: Check if L and R have non-negative power series expansions around zero.
- If this is indeed the case, calculate d.d. pair w.r.t. the edges

$$\lambda(x) = \frac{L'(x)}{L'(1)}\,, \qquad \rho(x) = \frac{R'(x)}{R'(1)}.$$

Construction of C.A. ARA codes for the BEC (3)

Construction of a capacity-achieving systematic ARA codes for the BEC with bounded complexity per information bit

- Recall the self-matched function, and let

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

- According to the algorithm, this gives

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

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

Construction of C.A. ARA codes for the BEC (4)

Condition for power series expansions to be non-negative

It has been observed empirically, that the expansions of both L and R are non-negative if and only if p satisfies

$$\frac{1}{1-\frac{13-\sqrt{61}}{9}\left(b+\ln(1-b)\right)} \leq p \leq 1-\frac{1}{1-\frac{13-\sqrt{61}}{9}\left(b+\ln(1-b)\right)}$$

and

$$b \in [b^*, 1), \quad b^* \triangleq W(-e^{-\frac{25+\sqrt{61}}{12}})+1 \approx 0.9304$$

where W designates the Lambert W-function.

Construction of C.A. ARA codes for the BEC (5)

Asymptotic behavior of the d.d. coefficients

$$L_k, R_k = O\left(\frac{b^k}{k\ln^2(k)}\right), \qquad \lambda_k, \rho_k = O\left(\frac{b^k}{\ln^2(k)}\right).$$

Advantage of this ensemble

We believe the performance advantage of this ensemble over other c.a. ensembles is due to the *exponential* decay of the d.d. coefficients.

Encoding and decoding complexity per information bit

The number of edges in the Tanner graph is given by

$$\chi_{\mathrm{E}}, \chi_{\mathrm{D}} = \frac{3-p}{1-p} - \frac{b^2 p}{(1-b)[b+\ln(1-b)]}.$$

Construction of C.A. NSIRA codes for the BEC (1)

By graph reduction for NSIRA codes, the same algorithm for ARA codes applies, except that for NSIRA codes $\widetilde{\lambda} = \lambda$.

- Starting with the self-matched function, we find the fraction of “information bit" nodes with degree i is given by

$$L_i = -\frac{b^i}{i} \frac{1}{b + \ln(1-b)}, \quad i = 2, 3, \ldots$$

- The non-negativity of the sequence $\{L_i\}$ holds when $0 < b < 1$ (so $b + \ln(1-b) < 0$). Notice there is no constraint on p.
- The d.d. R is the same as for the ARA ensemble

Construction of C.A. NSIRA codes for the BEC (2)

Condition for non-negative power series expansions

Since L is always non-negative, only one condition must be satisfied. It has been empirically observed that the expansion of R is non-negative if and only if p satisfes

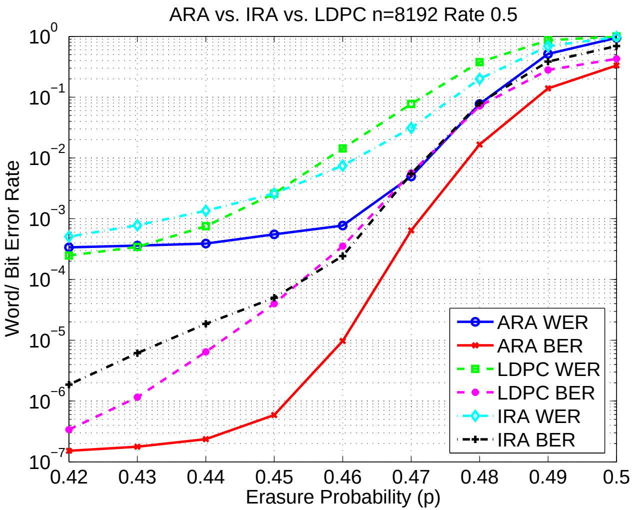
$$p \leq 1 - \frac{1}{1 - \frac{13-\sqrt{61}}{9}\left[b + \ln(1-b)\right]} .$$

We note this is a strictly weaker condition than for the ARA ensemble.

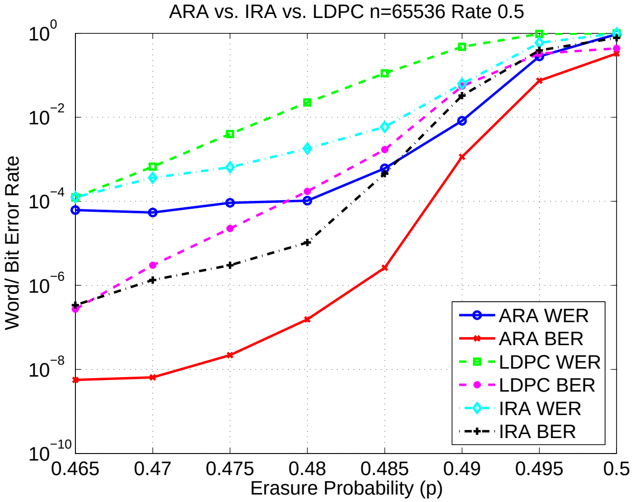
Encoding and decoding complexity per information bit

$$\chi_{\mathrm{E}} = \chi_{\mathrm{D}} = \frac{2}{1-p} - \frac{b^2}{(1-b)\left[b + \ln(1-b)\right]}$$

Computer Simulations (1)



Computer Simulations (2)



Summary

- Introduced capacity-achieving ARA codes for the BEC
  - Systematic codes whose decoding complexity per information bit is bounded as the gap to capacity vanishes
  - Simulations show improved performance over 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