On the Erasure-Correcting Capabilities of Low-Complexity Decoded LDPC Codes with Constituent Hamming Codes

Victor Zyablov, Pavel Rybin

Inst. for Inform. Transmission Problems
Russian Academy of Sciences
Moscow, Russia

Rolf Johannesson, Maja Lončar

Dept. of Electrical and Inform. Technology
Lund University
Lund, Sweden

ACCT '08, Pamporovo, Bulgaria, June 2008

Outline

- ▷ Hamming code-based low-density parity-check (H-LDPC) codes
- ▷ Erasure correcting capabilities of Hamming codes
- ▷ Iterative erasure-correction algorithm for H-LDPC codes
- ▷ Asymptotic performance
- ▷ Numerical results

Hamming Code-Based LDPC (H-LDPC) Codes

- Parity-check matrix of Gallager's LDPC codes:

$$\boldsymbol{H} = \begin{pmatrix} \pi_1(\boldsymbol{H}_{\mathrm{b}}) \\ \pi_2(\boldsymbol{H}_{\mathrm{b}}) \\ \vdots \\ \pi_\ell(\boldsymbol{H}_{\mathrm{b}}) \end{pmatrix}_{\ell b \times b n_0}$$

where

$$\boldsymbol{H}_{\mathrm{b}} = \begin{pmatrix} 1\,1\,\ldots\,1 & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & 1\,1\,\ldots\,1 & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \ddots & \ddots & & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & 1\,1\,\ldots\,1 \end{pmatrix}_{b \times b n_0}$$

- $(n_0, n_0 - 1)$ single parity-check (SPC) codes are constituent codes
- ℓ random column permutations of $\boldsymbol{H}_{\mathrm{b}}$ form layers of $\boldsymbol{H}$
- Code rate is $R \geq 1 - \frac{\ell b}{b n_0}$

Hamming Code-Based LDPC (H-LDPC) Codes

- Parity-check matrix of H-LDPC codes:

$$\boldsymbol{H} = \begin{pmatrix} \pi_1(\boldsymbol{H}_{\mathrm{b}}) \\ \pi_2(\boldsymbol{H}_{\mathrm{b}}) \\ \vdots \\ \pi_\ell(\boldsymbol{H}_{\mathrm{b}}) \end{pmatrix}_{\ell b(n_0-k_0)\times bn_0}$$

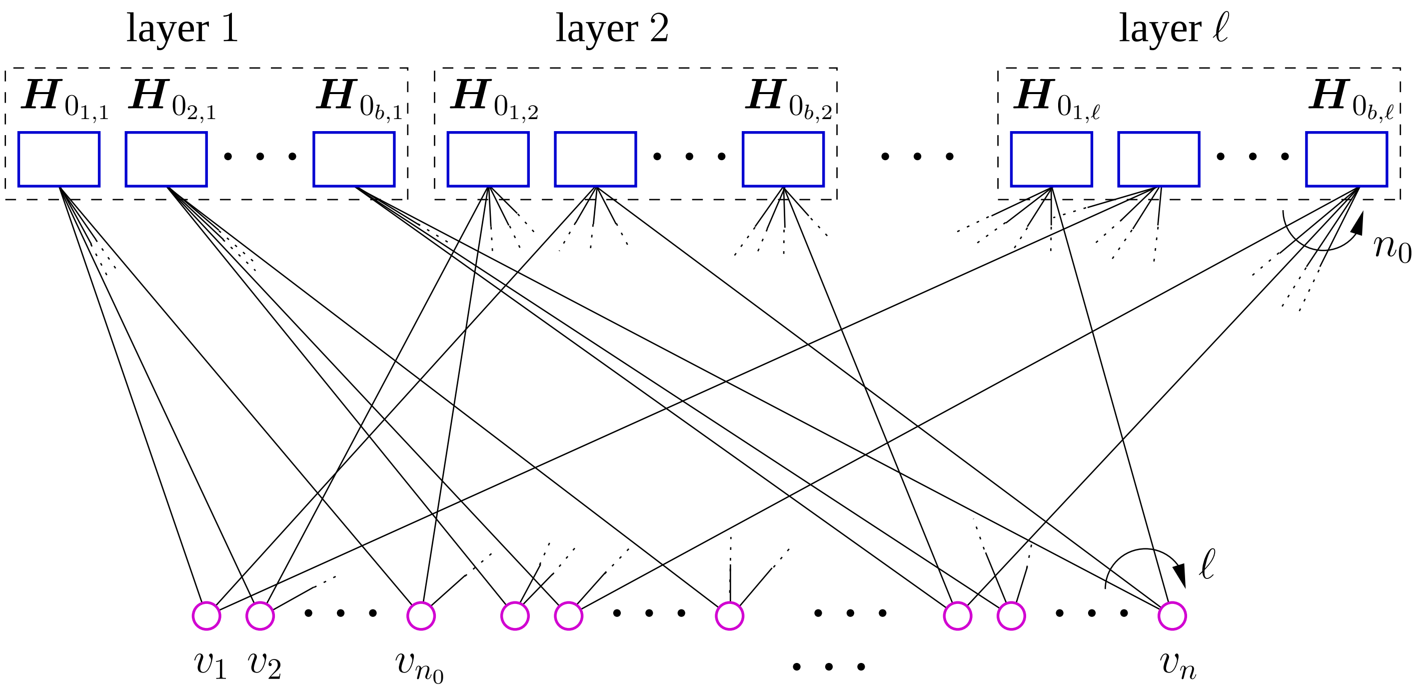
where

$$\boldsymbol{H}_{\mathrm{b}} = \begin{pmatrix} \boldsymbol{H}_0 & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \boldsymbol{H}_0 & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \ddots & \ddots & & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \boldsymbol{H}_0 \end{pmatrix}_{b(n_0-k_0)\times bn_0}$$

- (n_0, k_0) Hamming codes are constituent codes
- ℓ random column permutations of $\boldsymbol{H}_{\mathrm{b}}$ form layers of $\boldsymbol{H}$
- Code rate is $R \geq 1 - \frac{\ell b(n_0-k_0)}{bn_0} \Rightarrow \frac{k_0}{n_0} > 1 - \frac{1}{\ell}$

Hamming Code-Based LDPC (H-LDPC) Codes

- Bipartite Tanner graph of H-LDPC codes:



- Constraint nodes have degree n_0 and represent constituent Hamming codes.
  Constituent parity-check matrices $\boldsymbol{H}_{0_{j,k}}$ are all equal up to column permutations.
- Variable nodes have degree ℓ and represent codesymbols.
  Each variable node is connected to exactly one constraint node in each layer.

Erasure-Correcting Capabilities of Hamming Codes

- Parameters of the (n_0, k_0) Hamming code:
  - $n_0 = 2^m - 1$, $k_0 = n_0 - m$, $m \geq 2$, $d_0 = 3$
  - columns of $\boldsymbol{H}_0$ are all nonzero binary m-tuples
- When communicating over the binary erasure channel (BEC):
  - all erasure patterns with $d_0 - 1 = 2$ or fewer erasures are correctable
  - some erasure patterns with up to m erasures are correctable
- An erasure pattern with $\tau \leq m$ erasures is correctable if the $m \times \tau$ matrix $\boldsymbol{M}$, whose columns are the τ columns of $\boldsymbol{H}_0$ corresponding to the erased positions, has $\operatorname{rank}(\boldsymbol{M}) = \tau$.

  Lemma: The number of correctable erasure patterns with $\tau \leq m$ erasures is

$$\mathcal{M}(\tau, m) = \frac{\prod_{i=0}^{\tau-1} (2^m - 2^i)}{\tau!}$$

  Corollary: The generating function for the number of correctable erasure patterns is

$$g_1(s, n_0) = \sum_{\tau=1}^{m} \mathcal{M}(\tau, m) s^\tau = \binom{n_0}{1} s + \binom{n_0}{2} s^2 + \sum_{\tau=3}^{m} \frac{\prod_{i=0}^{\tau-1} (2^m - 2^i)}{\tau!} s^\tau$$

Iterative Erasure-Correcting Algorithm for H-LDPC Codes

- Consider communication over a BEC using an H-LDPC code of length $n = bn_0$ with constituent Hamming codes of length $n_0 = 2^m - 1$. Let $\boldsymbol{r}$ denote the received sequence.
- Iterative decoding algorithm $\mathscr{A}$: For every iteration $i = 1, 2, ..., i_{\max}$:

  (1) For the tentative sequence $\boldsymbol{r}^{(i)}$ (where $\boldsymbol{r}^{(1)} = \boldsymbol{r}$), select constituent codes $\mathcal{C}_{0j,l}$ with $\tau_{j,l}$ erasures, $j = 1, 2, ..., b$, $l = 1, 2, ..., \ell$, such that:

  Variant $\mathscr{A}_1$: $\tau_{j,l} < d_0 = 3$

  Variant $\mathscr{A}_2$: $\tau_{j,l} \leq m$

  (2) Assuming 0s on the erased positions, compute the syndromes $\boldsymbol{s}_{j,l}$ for the selected constituent codes.

  (3) For each selected constituent code $\mathcal{C}_{0j,l}$, construct the $m \times \tau_{j,l}$ matrix $\boldsymbol{M}_{j,l}$. If $\operatorname{rank}(\boldsymbol{M}_{j,l}) = \tau_{j,l}$, the code is affected by a correctable erasure pattern.

  (4) For every constituent code affected by a correctable erasure pattern find the erased tuple $\boldsymbol{x}_{j,l}$ by solving

$$\boldsymbol{x}_{j,l}\boldsymbol{M}_{j,l}^{\mathrm{T}} = \boldsymbol{s}_{j,l}$$

  Replace the erasures in $\boldsymbol{r}^{(i)}$ with the so-found code symbols. This yields $\boldsymbol{r}^{(i+1)}$.

Iterative Erasure-Correcting Algorithm for H-LDPC Codes

- Decoding complexity:

  Lemma:

  If an erasure pattern is such that in each iteration of the algorithm $\mathscr{A}$, the fraction of constituent codes affected by correctable erasures is

  $$\alpha > 0$$

  then the algorithm $\mathscr{A}$ recovers the transmitted codeword after $\mathcal{O}(\log n)$ iterations.

  Thus, the overall decoding complexity is $\mathcal{O}(n \log n)$.

Asymptotic Performance

- *Theorem:*

In the ensemble $\mathscr{C}(n_0, \ell, b)$ of H-LDPC codes, there exist codes (with probability p, where $\lim_{n\to\infty} p = 1$), which can, with decoding complexity $\mathcal{O}(n \log n)$, correct any erasure pattern with up to $W = \omega_\alpha n$ erasures. The value ω_α is the largest root of the equation

$$h(\omega) - \ell F(\alpha, \omega, n_0) = 0$$

where $h(\omega)$ is the binary entropy function, and the function $F(\alpha, \omega, n_0)$ is given by

$$F(\alpha, \omega, n_0) \triangleq h(\omega) - \frac{h(\alpha\omega n_0)}{n_0} + \max\left\{\omega \log_2 s - \frac{1}{n_0}\log_2(g_0(s, n_0)) - \alpha\omega \log_2\left(\frac{g_1(s, n_0)}{g_0(s, n_0)}\right)\right\}$$

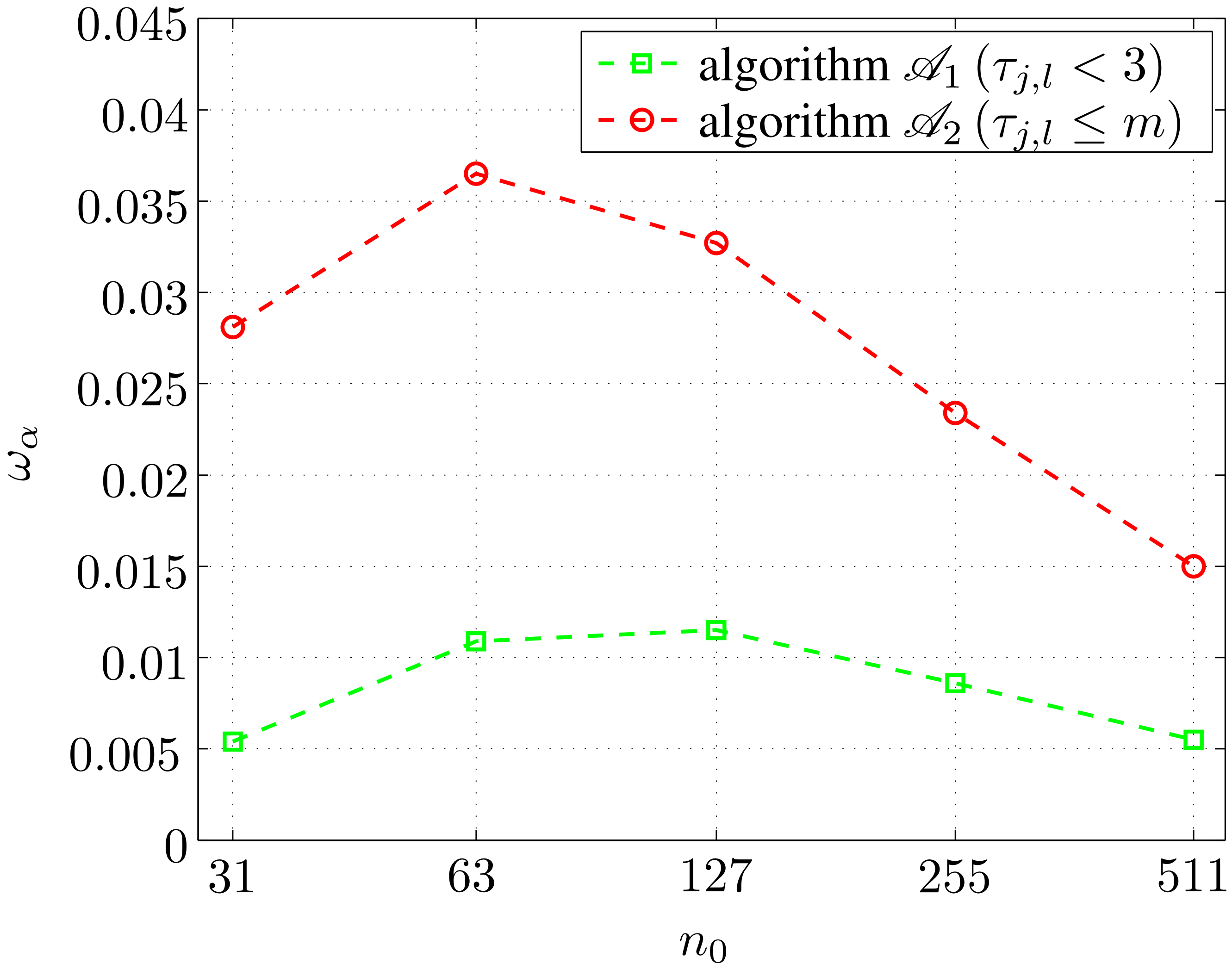
where $\alpha > 0$ and the maximization is performed over all s such that

$$\frac{\alpha\omega n_0}{1 - \alpha\omega n_0} \leq \frac{g_1(s, n_0)}{g_0(s, n_0)}.$$

The function $g_1(s, n_0)$ is the generating function of all the erasure patterns that are correctable by the constituent Hamming codes, and $g_0(s, n_0)$ is the generating function of the uncorrectable erasure patterns, $g_0(s, n_0) = (1 + s)^{n_0} - g_1(s, n_0)$.

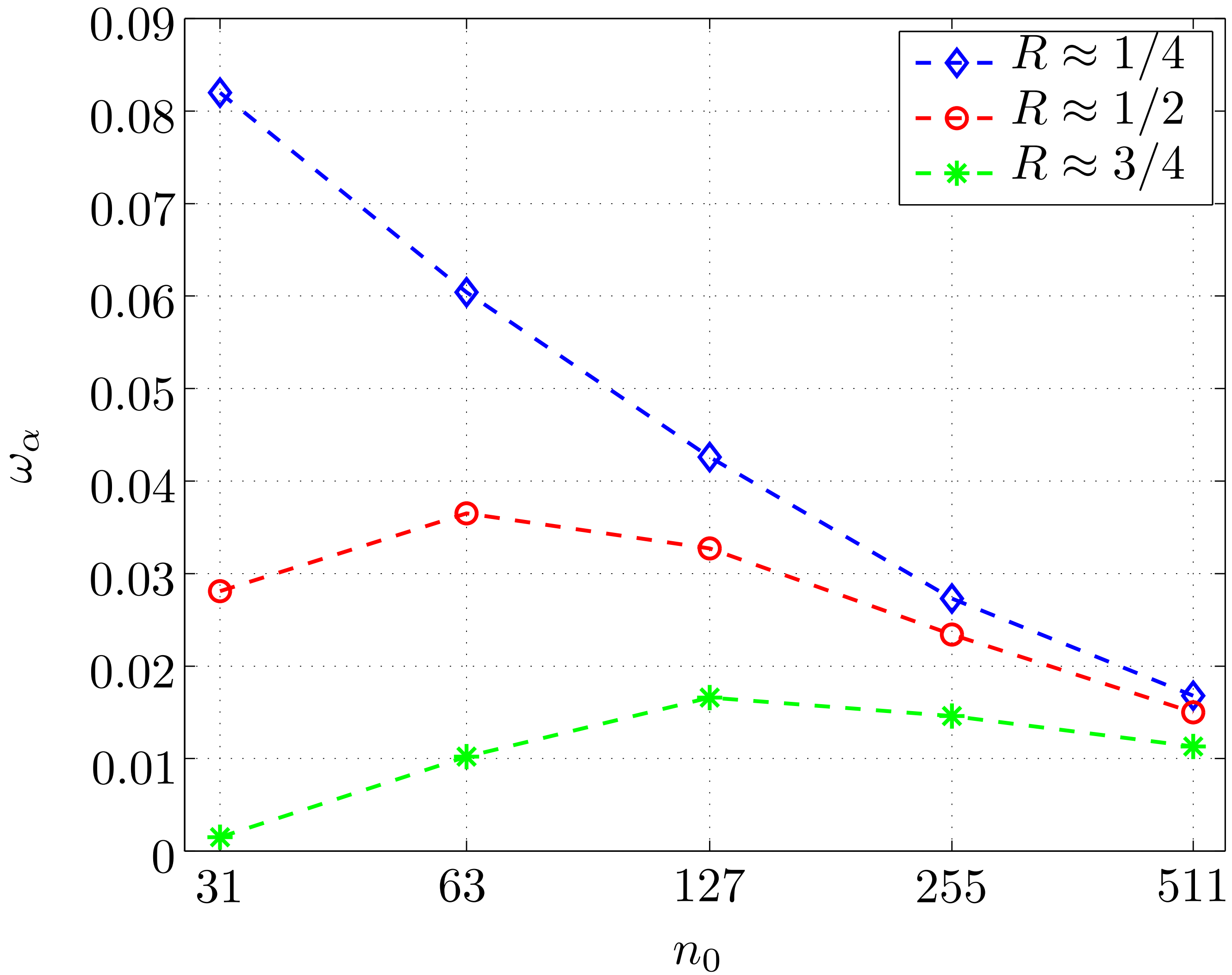
Numerical Results

- Code ensembles of rates $R \approx \frac{1}{2}$, $\alpha = 10^{-4}$, decoded with $\mathscr{A}_1$ and $\mathscr{A}_2$



Numerical Results

- Code ensembles of rates $R \approx \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$, $\alpha = 10^{-4}$, decoded with $\mathscr{A}_2$



Conclusions

- ▷ Random Hamming code-based LDPC codes were used over the binary erasure channel.
- ▷ Constituent Hamming codes of length $n_0 = 2^m - 1$ can correct up to m erasures (if the corresponding columns of the parity-check matrix are linearly independent).
- ▷ Simple iterative decoding algorithm of complexity $\mathcal{O}(n \log n)$ was considered.
- ▷ Existence of H-LDPC codes capable of correcting $\mathcal{O}(n)$ erasures with complexity $\mathcal{O}(n \log n)$ was proved and verified numerically for several code ensembles.