On the Error-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

Maja Lončar, Rolf Johannesson

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
- Generalized syndrome of H-LDPC codes
- Iterative decoding 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:

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

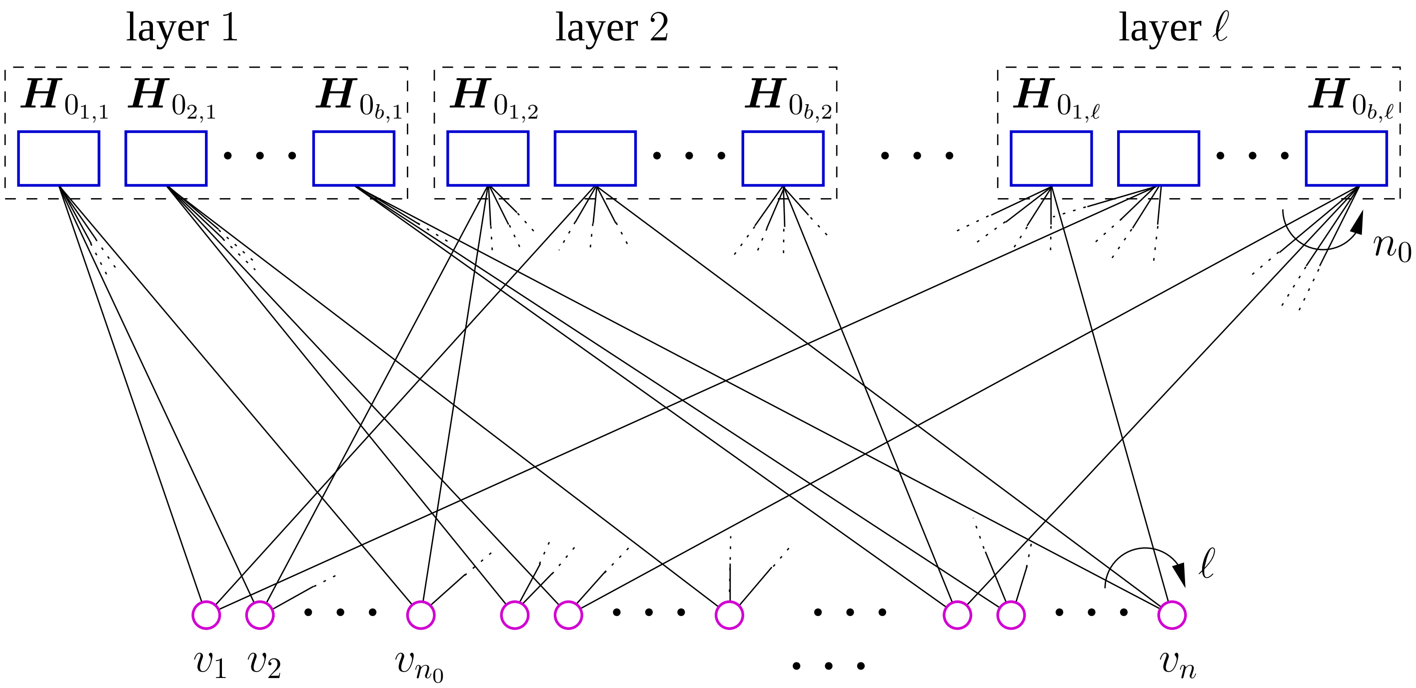
where

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

- (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.

Generalized Syndrome of H-LDPC Codes

- Parameters of (n_0, k_0) Hamming code:
  - $n_0 = 2^m - 1$, $k_0 = n_0 - m$, $m \geq 2$, $d_0 = 3$
  - Hamming codes are perfect single-error correcting codes
  - The columns of $\boldsymbol{H}_0$ are all nonzero binary m-tuples
- Consider communication over the binary symmetric channel (BSC).
  - The received sequence is $\boldsymbol{r} = \boldsymbol{v} + \boldsymbol{e}$. The error pattern has weight $|\boldsymbol{e}| = W = \omega n$.
  - The syndrome vector is the ℓbm-tuple

$$\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}^{\mathrm{T}} = (\boldsymbol{s}_1\, \boldsymbol{s}_2 \ldots \boldsymbol{s}_\ell)$$

where the lth layer syndrome $\boldsymbol{s}_l$ consists of b constituent-code syndromes $\boldsymbol{s}_{j,l}$, $j = 1, \ldots, b$

  - The generalized syndrome is the ℓb-tuple

$$\boldsymbol{S} = (\boldsymbol{S}_1\, \boldsymbol{S}_2 \ldots \boldsymbol{S}_\ell) = (S_{1,1}\, S_{2,1} \ldots S_{b,1}\;\; S_{1,2}\, S_{2,2} \ldots S_{b,2}\;\; \ldots\;\; S_{1,\ell}\, S_{2,\ell} \ldots S_{b,\ell})$$

whose elements are indicators whether the constituent codes have detected errors or not:

$$S_{j,l} = \begin{cases} 0, & \boldsymbol{s}_{j,l} = \boldsymbol{0} \\ 1, & \boldsymbol{s}_{j,l} \neq \boldsymbol{0} \end{cases} \qquad j = 1, 2, \ldots, b, \quad l = 1, 2, \ldots, \ell$$

Generalized Syndrome of H-LDPC Codes

- Let a_1 be the number of constituent Hamming codes affected by exactly one error. Then

$$a_1 \leq |\boldsymbol{S}| \leq \ell W \tag{1}$$

with equalities if the W errors all affect different constituent codes.

- *Lemma 1 (Bounds on the number of errors):*

For an arbitrary error pattern with W errors, let

$$a_1 \geq \frac{\ell W}{2}. \tag{2}$$

Then, if the number of constituent codes affected with one error is a_1, the number of errors is bounded by the inequalities

$$\frac{a_1}{\ell} \leq W \leq \frac{2a_1}{\ell}.$$

Proof:

Follows immediately from (1) and (2).

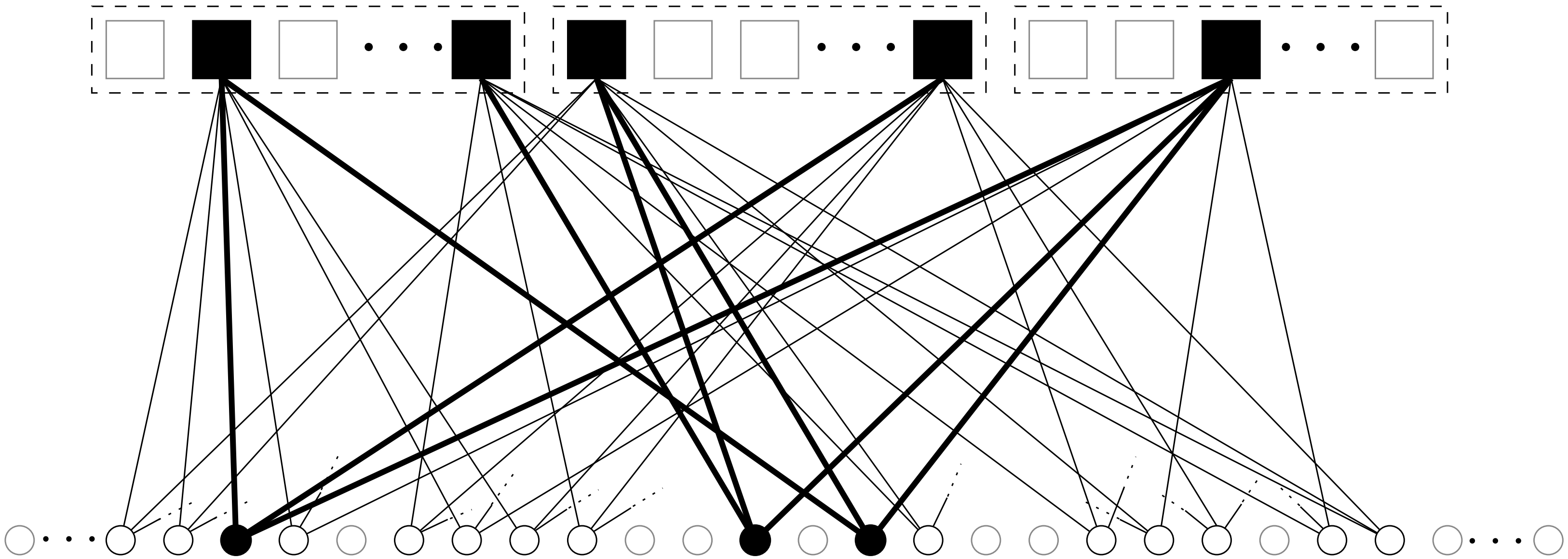
Generalized Syndrome of H-LDPC Codes

- Example:

  H-LDPC code with $\ell = 3$ layers and $(7, 4)$ Hamming constituent codes.

$$(|\boldsymbol{S}_1|\ |\boldsymbol{S}_2|\ |\boldsymbol{S}_3|) = (2\ 2\ 1) \text{ or } (2\ 2\ 0)$$

$$a_1 = 2$$



$$W = 3$$

Iterative Decoding Algorithm for H-LDPC Codes

- Algorithm $\mathscr{A}$: For every iteration $i = 1, 2, ..., i_{\max}$

(1) For the tentative sequence $\boldsymbol{r}^{(i)}$ (where $\boldsymbol{r}^{(1)} = \boldsymbol{r}$), ML-decode independently the ℓb constituent Hamming codes using syndrome decoding.

If all the constituent codes have zero syndrome, output $\hat{\boldsymbol{v}} = \boldsymbol{r}^{(i)}$ and stop.

Otherwise, proceed to step (2).

(2) For every symbol $r_k^{(i)}$, $k = 1, 2, ..., n$, in the sequence $\boldsymbol{r}^{(i)}$, for which at least one of the ℓ decisions requires that the symbol is changed, check if changing the symbol reduces the weight of the generalized syndrome.

If so, flip the symbol value, otherwise, leave it unchanged.

This yields the updated sequence $\boldsymbol{r}^{(i+1)}$.

If $\boldsymbol{r}^{(i+1)} = \boldsymbol{r}^{(i)}$, declare the decoding failure and stop.

Otherwise, return to step (1).

Iterative Decoding Algorithm for H-LDPC Codes

- *Lemma 2 (Reduction of the generalized syndrome weight):*

  For an arbitrary error pattern with W errors, if the number of constituent Hamming codes affected by a single error satisfies the condition

  $$a_1 > \frac{\ell W}{2}$$

  then when decoding the constituent codes there exists a symbol such that flipping its value results in a reduction of the generalized syndrome weight.

  Proof:

  Hint: Each received symbol is connected to exactly ℓ constituent codes. If more than $\ell/2$ of them is affected by exactly one error, then flipping this symbol results in a reduction of the generalized syndrome weight.

Iterative Decoding Algorithm for H-LDPC Codes

- *Lemma 3 (Error-correcting capability of algorithm $\mathscr{A}$):*

  Let W_α be the largest weight of the error pattern such that, for any $W \leq W_\alpha$, the number of constituent codes affected by a single error satisfies the condition

  $$a_1 > \frac{\ell W}{2}. \tag{3}$$

  Then, if the number of errors is such that

  $$W < \frac{W_\alpha}{2} \tag{4}$$

  these errors will be corrected by algorithm $\mathscr{A}$. Furthermore, the maximum number of errors that may be introduced during the decoding process (until reaching the correct decision) is smaller than the initial number of errors.

  Proof:

  Follows from Lemmas 1 and 2.

Iterative Decoding Algorithm for H-LDPC Codes

- *Lemma 4 (Decoding complexity):*

  If an error pattern is such that in each iteration of the algorithm $\mathscr{A}$, the number of corrected errors is larger than the number of introduced errors, then the algorithm $\mathscr{A}$ yields a correct decision after $\mathcal{O}(\log n)$ iterations.

From Lemma 4 follows that 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 correct any error pattern with up to $\omega_\alpha n/2$ errors, with decoding complexity $\mathcal{O}(n \log n)$. 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 $\alpha > 1/2$ and the maximization is performed over all s such that

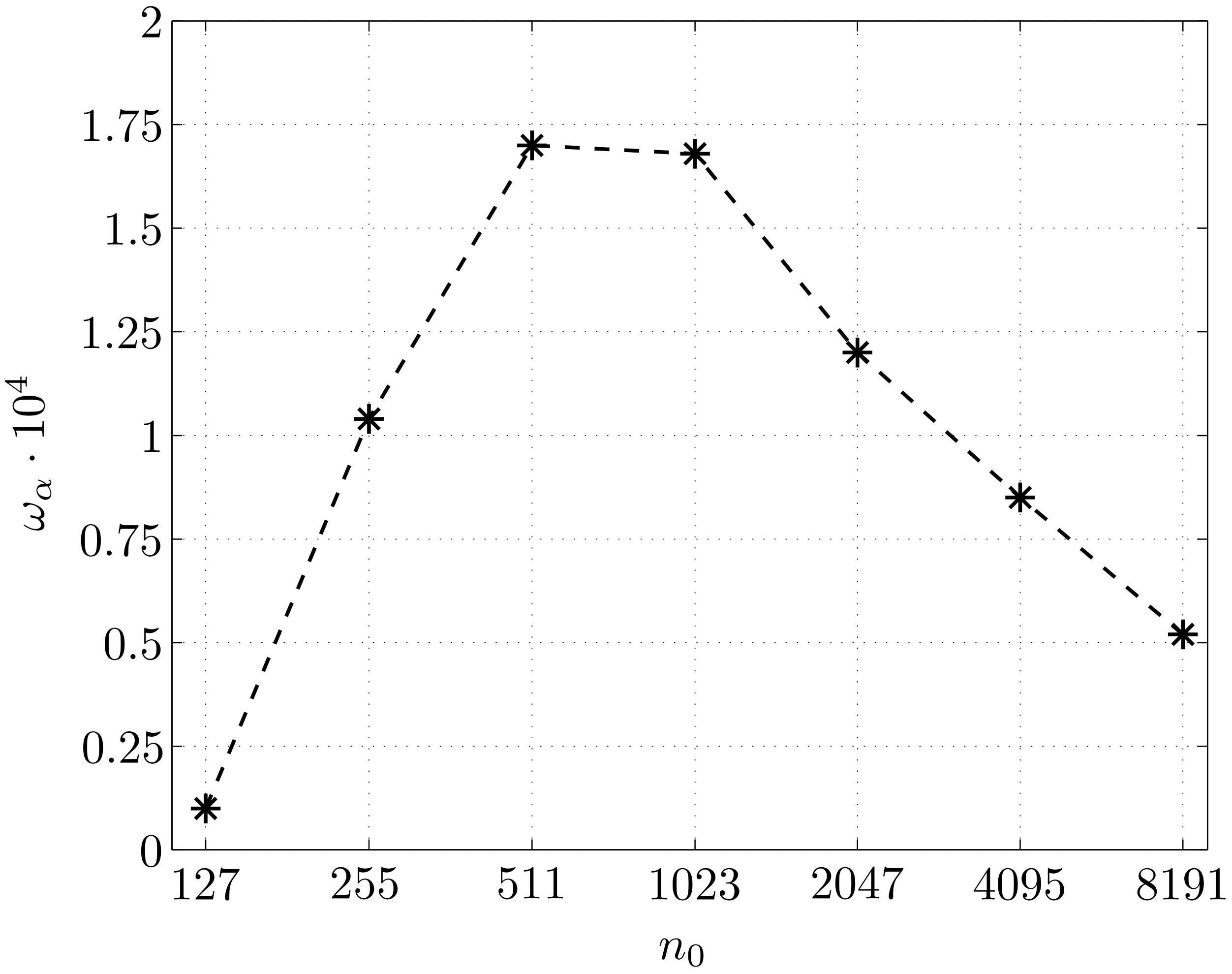
  $$\frac{\alpha\omega n_0}{1 - \alpha\omega n_0} \leq \frac{g_1(s, n_0)}{g_0(s, n_0)}.$$

  The function $g_1(s, n_0)$ is the generating function of all the single-error patterns that are correctable by the constituent Hamming codes, and $g_0(s, n_0)$ is the generating function of the remaining n_0-tuples:

  $$\begin{aligned} g_1(s, n_0) &= n_0 s \\ g_0(s, n_0) &= (1 + s)^{n_0} - n_0 s. \end{aligned}$$

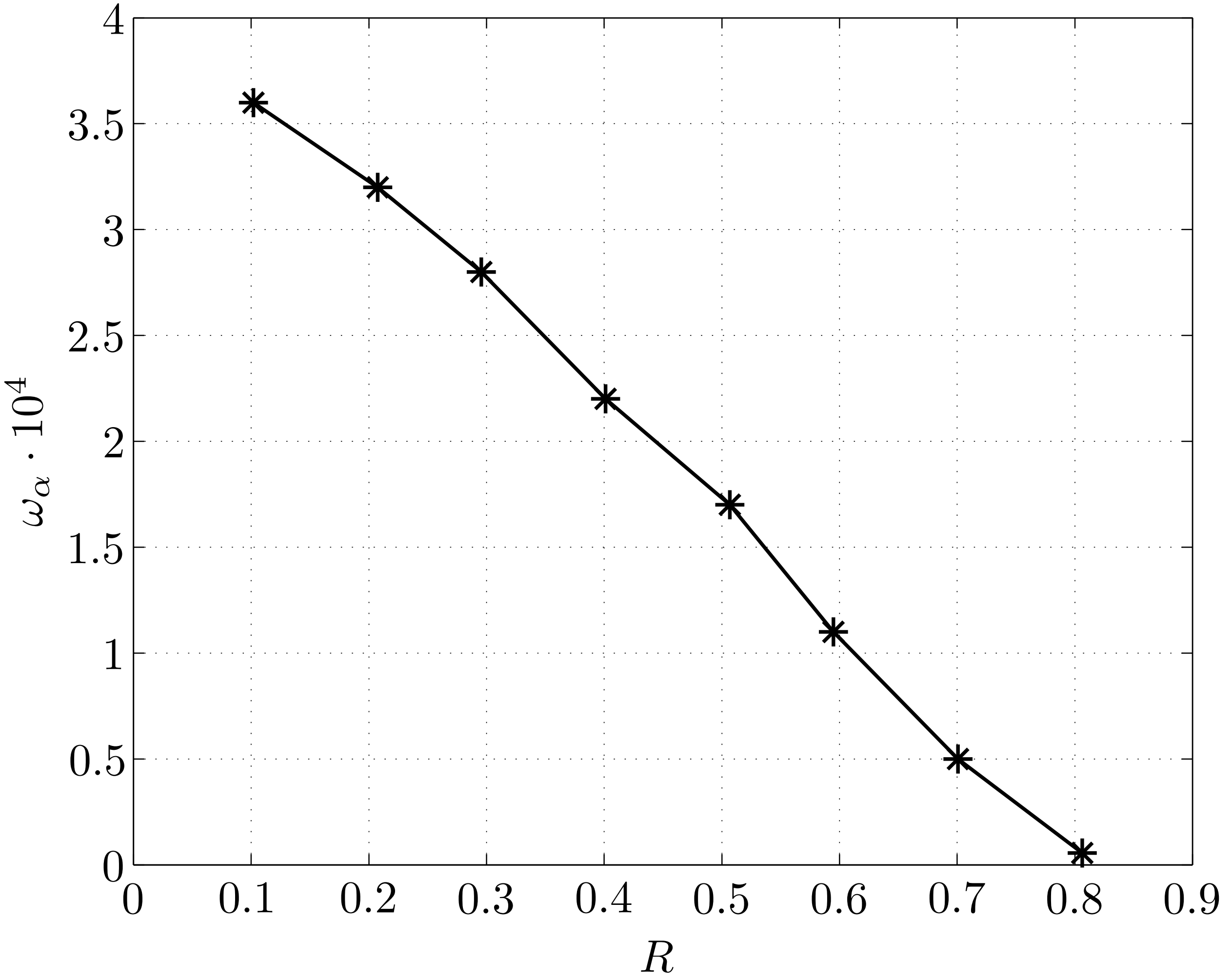
Numerical Results

- Code ensembles of rates $R \approx \frac{1}{2}$, with $\ell \in \{9,\ 16,\ 28,\ 51,\ 93,\ 171,\ 315\}$ layers



Numerical Results

- Code ensembles of variable rates with fixed constituent Hamming code of length $n_0 = 511$



Conclusions

- Random Hamming code-based LDPC codes were used over the binary symmetric channel
- Simple iterative decoding algorithm with complexity $\mathcal{O}(n \log n)$ was considered, where
  - constituent Hamming codes are decoded independently
  - symbols are flipped only if this reduces the generalized syndrome weight (GSW)
- Conditions for reducing the GSW and for correcting errors were formulated
- Existence of H-LDPC codes capable of correcting $\mathcal{O}(n)$ errors with complexity $\mathcal{O}(n \log n)$ was proved and verified numerically for several code ensembles