On the Error Exponent of Low-Complexity Decoded LDPC Codes with Special Construction

Pavel Rybin and Victor Zyablov

Email: {prybin, zyablov}@iitp.ru

Inst. for Information Transmission Problems
Russian Academy of Sciences

Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 16, 2012

Outline

1. Introduction
2. LDPC codes with special construction
3. Decoding algorithm
4. Main result
5. Numerical results
6. Conclusion

Gallager's LDPC codes

Parity-check matrix of Gallager's LDPC code (G-LDPC code)

$$\mathbf{H_2} = \begin{pmatrix} \pi_1(\mathbf{H}_{b_0}) \\ \pi_2(\mathbf{H}_{b_0}) \\ \vdots \\ \pi_\ell(\mathbf{H}_{b_0}) \end{pmatrix}_{\ell b_0 \times b_0 n_0}$$

where

$$\mathbf{H}_{b_0} = \begin{pmatrix} \mathbf{H_0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H_0} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H_0} \end{pmatrix}_{b_0 \times b_0 n_0}$$

1. $\mathbf{H_0}$ is $1 \times n_0$ parity-check matrix of single parity-check code.
2. ℓ random column permutations of $\mathbf{H}_{b_0}$ form layers of $\mathbf{H_2}$.
3. Code rate is $R_2 \geqslant 1 - \ell/n_0$.

Ensemble of Gallager's LDPC codes

Definition

For a given constituent code with parity-check matrix $\mathbf{H}_0$, the elements of the ensemble $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ are obtained by sampling independently the permutations π_l , $l = 1, 2, ..., \ell$, which are equiprobable.

Ensemble of Gallager's LDPC codes

Definition

For a given constituent code with parity-check matrix $\mathbf{H}_0$, the elements of the ensemble $\mathscr{E}_G(n_0, \ell, b_0)$ are obtained by sampling independently the permutations π_l, $l = 1, 2, ..., \ell$, which are equiprobable.

Remark

It is known[a] *that in ensemble* $\mathscr{E}_G(n_0, \ell, b_0)$ *of G-LDPC codes such code exists which can correct any error pattern with weight up to* $\lfloor \omega_t n \rfloor$ *while decoding with majority algorithm* $\mathscr{A}_M$ *with complexity* $\mathcal{O}(n \log n)$.

[a] P. S. Rybin and V. V. Zyablov, Asymptotic estimation of error fraction corrected by binary LDPC code, *2011 IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2011, 351 – 355.

LDPC codes with special construction

Parity-check matrix of LDPC code with special construction:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_2 \\ \pi\left(\mathbf{H}_{b_1}\right) \end{pmatrix}_{(\ell b_0 m_0 + b_1 m_1) \times b_0 n_0}$$

where

$$\mathbf{H}_{b_1} = \begin{pmatrix} \underbrace{\begin{matrix} \mathbf{H}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_1 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_1 \end{matrix}}_{b_1} \end{pmatrix}_{b_1 m_1 \times b_1 n_1}$$

- $\mathbf{H}_1$ – parity-check matrix of “best” linear code.
- $\mathbf{H}_2$ – parity-check matrix of G-LDPC code from $\mathscr{E}_G\left(n_0, \ell, b_0\right)$.
- $R \geqslant R_1 + R_2 - 1$.

Ensemble of LDPC codes with special construction

Definition

Obtained construction of LDPC code we will call G-LDPC code with added layer composed from linear codes (LG-LDPC code).

Ensemble of LDPC codes with special construction

Definition

Obtained construction of LDPC code we will call G-LDPC code with added layer composed from linear codes (LG-LDPC code).

Definition

For a given linear code with parity-check matrix $\mathbf{H}_1$, the elements of the ensemble $\mathscr{E}_L\left(n_0, \ell, b_0, n_1, 1, b_1\right)$ are obtained by sampling independently the parity-check matrix $\mathbf{H}_2$ from $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ and permutation π.

Decoding algorithm description

Decoding algorithm $\mathscr{A}_C$ consists of the following two steps:

1. Received sequence is decoded with well known maximum likehood algorithm separately by b_1 linear codes with parity-check matrix $\mathbf{H}_1$ from $\ell + 1$ layer of $\mathbf{H}$;

Decoding algorithm description

Decoding algorithm $\mathscr{A}_C$ consists of the following two steps:

1. Received sequence is decoded with well known maximum likehood algorithm separately by b_1 linear codes with parity-check matrix $\mathbf{H}_1$ from $\ell + 1$ layer of $\mathbf{H}$;
2. Tentative sequence is decoded with well known majority decoding algorithm $\mathscr{A}_M$ by G-LDPC code with parity-check matrix $\mathbf{H}_2$.

Error exponent

- Investigating error probability P under decoding algorithm $\mathscr{A}_C$ of LG-LDPC code we considered memoryless BSC with BER p.
- Estimation on error probability P we wrote in the following way:

$$P \leqslant \exp\left\{-nE\left(R_1, n_1, \omega_t, p\right)\right\},$$

where $E\left(R_1, n_1, \omega_t, p\right)$ is error exponent.

Main result

If $R \to \mathscr{C}$ such, that $R_1 < \mathscr{C}$ and $R_2 < 1$, then $\exists n_1$, that $E\left(R_1, n_1, \omega_t, p\right) > 0$, if $\omega_t > 0$ for $\forall R_2 < 1$.

Main result

If $R \to \mathscr{C}$ such, that $R_1 < \mathscr{C}$ and $R_2 < 1$, then $\exists n_1$, that $E\left(R_1, n_1, \omega_t, p\right) > 0$, if $\omega_t > 0$ for $\forall R_2 < 1$.
Existence conditions:

- Let in the ensemble $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ of G-LDPC codes such code with code rate R_2 exists, which can correct any error pattern of weight up to $\lfloor \omega_t n \rfloor$ while decoding with majority algorithm $\mathscr{A}_M$.
- Let the such linear code exists, which has code length n_1, code rate R_1 and error exponent of this code under maximum likehood decoding is lower-bounded with $E_0\left(R_1, p\right)$.

Theorem

If above conditions are fulfilled then in the ensemble $\mathscr{E}_L\left(n_0, \ell, b_0, n_1, 1, b_1\right)$ of LG-LDPC codes such code exists, which has the code length n:

$$n = n_0 b_0 = n_1 b_1,$$

code rate R:

$$R \geqslant R_1 + R_2 - 1$$

and error exponent of this code over memoryless BSC with BER p under decoding algorithm $\mathscr{A}_C$ with complexity $\mathcal{O}\left(n \log n\right)$ is lower-bounded with:

$$E\left(R_1, n_1, \omega_t, p\right) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ \beta E_0\left(R_1, p\right) + E_2\left(\beta, \omega_t, p\right) - \frac{1}{n_1} H\left(\beta\right) \right\}.$$

Notations

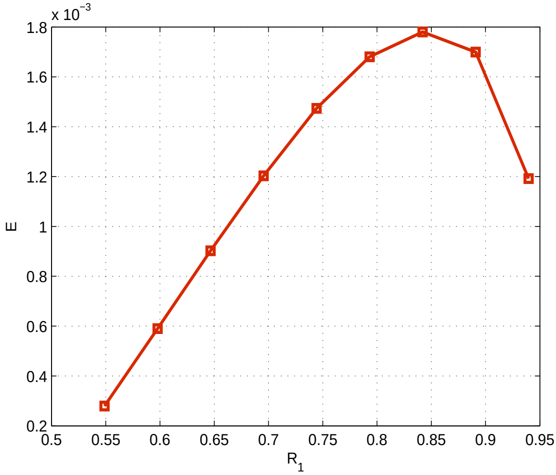
- $\beta_0 = \min\left(\frac{\omega_t}{2p}, 1\right);$
- $H(\beta) = -\beta \ln \beta - (1-\beta)\ln(1-\beta)$ – entropy function;
- $E_2(\beta, \omega_t, p)$ is given by:

$$E_2(\beta, \omega_t, p) = \frac{1}{2}\left(\omega_t \ln \frac{\omega_t}{p} + (2\beta - \omega_t)\ln \frac{2\beta - \omega_t}{1-p}\right) - \beta \ln(2\beta);$$

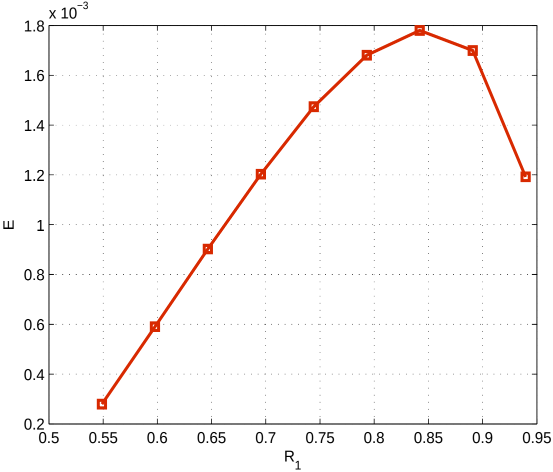
- n_1 satisfies the following conditions:

$$\frac{-\ln \beta_0}{E_0(R_1, p)} \leq n_1 \leq \frac{1}{R_1}\log_2\log_2(n).$$

Values of $E\left(R_1, n_1, \omega_t, p\right)$ according to R_1 of linear code and for fixed $R = 0.5$, $n_1 = 2000$ and $p = 10^{-3}$:

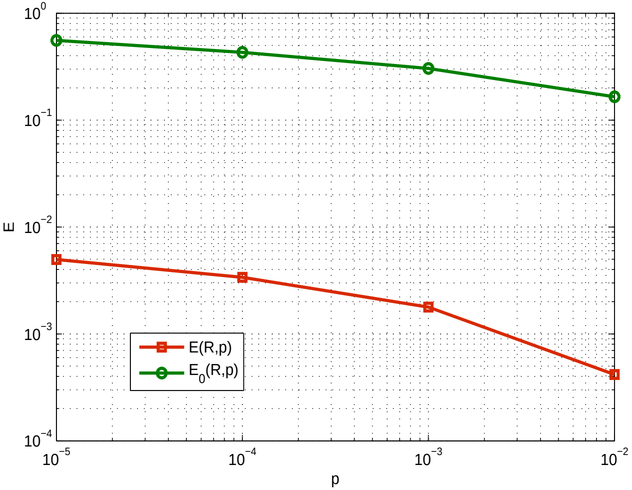


Values of $E\left(R_1, n_1, \omega_t, p\right)$ according to R_1 of linear code and for fixed $R = 0.5,\ n_1 = 2000$ and $p = 10^{-3}$:

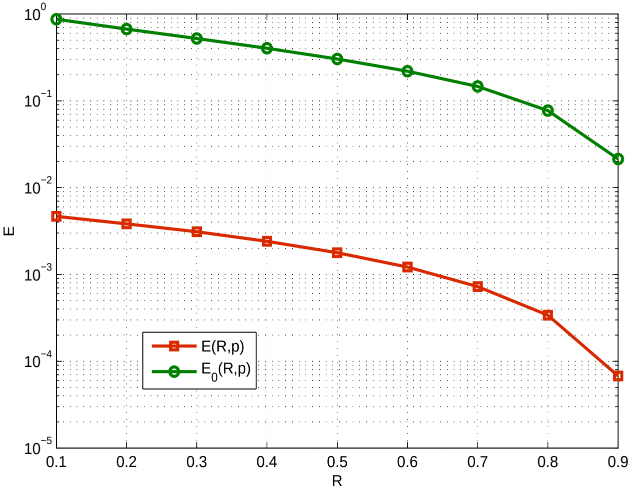


$$E\left(R, p\right) = \max_{R_1, R_2 : R_1 + R_2 - 1 = R} E\left(R_1, n_1, \omega_t, p\right).$$

Values of $E(R,p)$ and $E_0(R,p)$ according to p and for fixed $R = 0.5$:



Values of $E(R,p)$ and $E_0(R,p)$ according to R and for fixed $p = 10^{-3}$:



Conclusion

- Construction of LG-LDPC codes was proposed.

Conclusion

- Construction of LG-LDPC codes was proposed.
- Decoding algorithm $\mathscr{A}_C$ with low complexity was developed.

Conclusion

- Construction of LG-LDPC codes was proposed.
- Decoding algorithm $\mathscr{A}_C$ with low complexity was developed.
- Lower-bound of error exponent for LG-LDPC codes under decoding algorithm $\mathscr{A}_C$ was obtained.

Conclusion

- Construction of LG-LDPC codes was proposed.
- Decoding algorithm $\mathscr{A}_C$ with low complexity was developed.
- Lower-bound of error exponent for LG-LDPC codes under decoding algorithm $\mathscr{A}_C$ was obtained.
- It was proved, that for any code rate less than channel capacity such LG-LDPC code exists, that under decoding algorithm $\mathscr{A}_C$ with low-complexity $\mathcal{O}\left(n \log n\right)$ the error probability decreases exponentially.

Thank you for the attention!