On the error exponent of low-complexity decoded LDPC codes with special construction

Pavel Rybin prybin@iitp.ru
Victor Zyablov zyablov@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Science, Moscow 101447, Russia

Abstract. In this paper we consider low-density parity-check (LDPC) codes with special construction. We obtain the lower-bound on error exponent for these codes under low-complexity decoding algorithm. We show that such LDPC code with special construction exists, that error probability of decoding algorithm exponentially decreases for all code rates below channel capacity. The error exponent is computed numerically for different code parameters.

1 Introduction

Low-density parity-check code were proposed by R. G. Gallager (G-LDPC codes) in [1]. The error-correcting capabilities of G-LDPC codes for the binary symmetric channel (BSC) were studied in [2], where it was shown that such G-LDPC codes exist that capable of correcting a portion of errors that grows linearly with the code length n, with decoding complexity $\mathcal{O}(n \log n)$. Then in [3] this lower-bound on guaranteed corrected error fraction was improved.

The lower-bound on code distance of G-LDPC codes was obtained by R. G. Gallager in [1]. In [4] and [5] the upper and lower-bound on error exponent under maximum likehood decoding of G-LDPC codes was obtained. In [5] it was shown that lower-bound on error exponent under maximum likehood decoding of G-LDPC codes meets the lower-bound on error exponent under maximum decoding of good linear codes obtained in [6]. It is important to note that the complexity of maximum likehood decoding is $\mathcal{O}(2^n)$.

In this paper we consider LDPC codes with special construction and low-complexity decoding algorithm for these codes. We obtain the lower-bound on error exponent for these codes under decoding with complexity $\mathcal{O}(n \log n)$. We show for the first time that such LDPC code with special construction exists, that error probability of decoding algorithm with complexity $\mathcal{O}(n \log n)$ exponentially decreases for all code rates below channel capacity. The error exponent is computed numerically for different code parameters.

2 Construction description

At first consider the construction of parity-check matrix $\mathbf{H}_2$ of Gallagers LDPC code (G-LDPC code) with constituent single parity check (SPC) code with parity-check matrix $\mathbf{H}_0$. Let $\mathbf{H}_{b_0}$ denote a block-diagonal matrix with the b_0 constituent parity-check matrices $\mathbf{H}_0$ on the main diagonal, that is,

$$\mathbf{H}_{b_0} = \left(\underbrace{\begin{matrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{matrix}}_{b_0} \right),$$

where b_0 is very large. If the length of SPC code is n_0, then matrix $\mathbf{H}_{b_0}$ is of size $b_0 \times b_0 n_0$. Let $\pi\left(\mathbf{H}_{b_0}\right)$ denote a random column permutation of $\mathbf{H}_{b_0}$. Then the matrix constructed using $\ell > 2$ such permutations as layers,

$$\mathbf{H}_2 = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_\ell \end{pmatrix} = \begin{pmatrix} \pi_1\left(\mathbf{H}_{b_0}\right) \\ \pi_2\left(\mathbf{H}_{b_0}\right) \\ \vdots \\ \pi_\ell\left(\mathbf{H}_{b_0}\right) \end{pmatrix}$$

is a sparse $\ell b_0 \times b_0 n_0$ parity-check matrix which characterizes the ensemble of G-LDPC codes of length $n = b_0 n_0$, where $n \gg n_0$. Let $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ denote this ensemble.

Definition 1. *For a given SPC 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.*

The rate of a G-LDPC code from $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ is lower-bounded [7] by

$$R_2 \geqslant 1 - \ell\left(1 - R_0\right), \tag{1}$$

where $R_0 = \frac{n_0 - 1}{n_0}$ is code rate of SPC code. The equality is achieved iff matrix $\mathbf{H}_2$ has full rank.

Now consider the proposing special construction of parity-check matrix of LDPC code. Let $\mathbf{H}_1$ is parity-check matrix of linear code with code length n_1 and code rate R_1. Consider a block-diagonal matrix $\mathbf{H}_{b_1}$ with the b_1 paritychecks matrices on the main diagonal

$$\mathbf{H}_{b_1} = \left(\underbrace{\begin{array}{cccc} \mathbf{H}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_1 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_1 \end{array}}_{b_1} \right),$$

where b_1 is so, that $b_1 n_1 = b_0 n_0$. Then the following matrix

$$\mathbf{H} = \left(\begin{array}{c} \pi_1(\mathbf{H}_{b_0}) \\ \pi_2(\mathbf{H}_{b_0}) \\ \vdots \\ \pi_\ell(\mathbf{H}_{b_0}) \\ \pi_{\ell+1}(\mathbf{H}_{b_1}) \end{array} \right),$$

is the parity-check matrix of proposing LDPC code with special construction. It is easy to see that the first ℓ layers of matrix $\mathbf{H}$ form parity-check matrix of G-LDPC code. So, we can write the matrix $\mathbf{H}$ in the following way:

$$\mathbf{H} = \left(\begin{array}{c} \mathbf{H}_2 \\ \pi_{\ell+1}(\mathbf{H}_{b_1}) \end{array} \right).$$

Matrix $\mathbf{H}$ characterizes the ensemble of G-LDPC codes with added layer composed from linear codes (LG-LDPC codes). Let $\mathscr{E}_{LG}(n_0, \ell, b_0, n_1, 1, b_1)$ denote this ensemble.

Definition 2. *For a given SPC code with parity-check matrix $\mathbf{H}_0$ and for a given linear code with parity-check matrix $\mathbf{H}_1$, the elements of the ensemble $\mathscr{E}_{LG}(n_0, \ell, b_0, n_1, 1, b_1)$ are obtained by sampling independently the permutations π_l , $l = 1, 2, ..., \ell + 1$, which are equiprobable.*

The length of constructed LG-LDPC code is $n = b_0 n_0 = b_1 n_1$ and code rate R is lower-bounded by

$$R \geqslant R_1 - \ell(1 - R_0),$$

and according to (1):

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

3 Algorithm description

We will decode described LG-LDPC code like concatenated code, that is on the first step we decoded received sequence using linear codes with parity-check matrix $\mathbf{H}_1$ from $\ell + 1$ layer of $\mathbf{H}$, on the second step we decode sequence, obtained on previous step, using G-LDPC code with parity-check matrix $\mathbf{H}_2$.

In this paper we will consider the algorithm $\mathscr{A}_C$, which consist of the following two steps:

1. received sequence 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 decoded with well known majority decoding algorithm $\mathscr{A}_M$ by G-LDPC code with parity-check matrix $\mathbf{H}_2$.

It is important to note that algorithm $\mathscr{A}_C$ is not iterative. Every received sequence is decoded only once with maximum likehood decoding algorithm using linear codes $\mathbf{H}_1$ at first, and then obtained sequence decoded with iterative majority algorithm $\mathscr{A}_M$ using G-LDPC code $\mathbf{H}_2$.

4 Main result

Investigating error probability P under decoding algorithm $\mathscr{A}_C$ of LG-LDPC code we will consider memoryless binary-symmetric channel (BSC) with bit error rate (BER) p. Estimation on error probability P we will write 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 required error exponent.

In [3] it was shown that in ensemble $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ 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 algorithm $\mathscr{A}_M$ with complexity $\mathcal{O}\left(n \log n\right)$. In [6] it was shown that such linear code exist, which error exponent under maximum likehood decoding is lower-bounded with such $E_0\left(R, p\right)$ that $E_0\left(n \log n\right) > 0$ for $\forall R < C$, where C – is channel capacity of BSC with BER p. Take into consideration these results we can formulate the following:

Theorem 1. *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 $E_0\left(R_1, p\right)$.

Then in the ensemble $\mathscr{E}_{LG}(n_0, \ell, b_0, n_1, 1, b_1)$ *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* $\mathcal{O}(n \log n)$ *is lower-bounded with* E*:*

$$E(R_1, n_1, \omega_t, p) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ \beta E_0(R_1, p) + E_2(\beta, \omega_t, p) - \frac{1}{n_1} H(\beta) \right\}, \qquad (2)$$

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

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

herewith n_1 *satisfies the following conditions:*

$$\frac{-\ln \beta_0}{E_0(R_1, p)} \leq n_1 \leq \frac{1}{R_1} \log_2 \log_2(n). \qquad (3)$$

Let $R \to C$ in the such way, that $R_1 < C$ and $R_2 < 1$. Then according to (2) there exist such n_1 that satisfies condition (3) and $E(R_1, n_1, \omega_t, p) > 0$, if $\omega_t > 0$ for $\forall R_2 < 1$.

5 Numerical results

Let consider the maximum of $E(R_1, n_1, \omega_t, p)$ for fixed $n_1 = 2000$, $p = 10^{-3}$ and given R of LG-LDPC code in the following way:

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

Figure 1 illustrates the values of $E(R, p)$ computed for several code rates R of LG-LDPC codes. Figure 2 illustrates the values $E(R, p)$ and $E_0(R, p)$ computes for several code rates R (in first case for LG-LDPC codes and in the second for linear codes).

As it seen on figure 2 the value of $E(R, p)$ is about two degree less than value of $E_0(R, p)$. But it is important to note that value $E_0(R, p)$ meets only with decoding complexity $\mathcal{O}(2^n)$ and value $E(R, p)$ meets with decoding complexity $\mathcal{O}(n \log n)$.

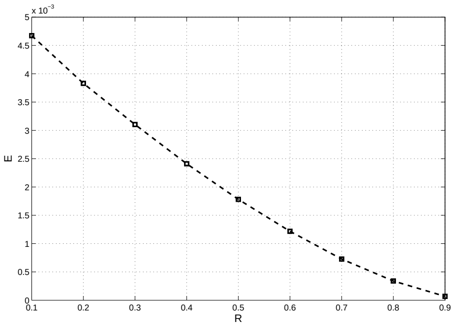

Figure 1: Values of $E\,(R,p)$ according to R of G-LDPC code and for fixed $p = 10^{-3}$

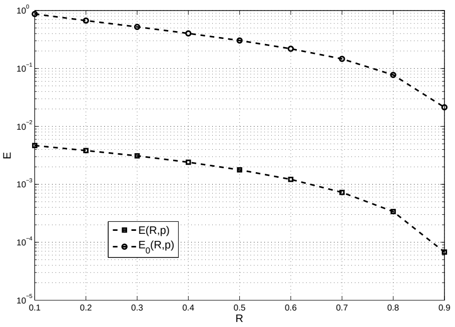

Figure 2: Values of $E\,(R,p)$ and $E_0\,(R,p)$ according to R and for fixed $p = 10^{-3}$

References

[1] R. G. Gallager, Low-Density Parity-Check Codes, Massachusetts: MIT Press, 1963.

[2] V. V. Zyablov and M. S. Pinsker, Estimation of the error-correction complexity for Gallager low-density codes, *Problems of Inform. Transmission*, **11**, 23–26, 1975.

[3] 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.

[4] D. Burshtein, O. Barak, Upper Bounds on the Error Exponents of LDPC Code Ensembles, *2006 IEEE International Symposium on Information Theory (ISIT)*, 2006, 401 – 405.

[5] O. Barak, D. Burshtein, Lower Bounds on the Error Rate of LDPC Code Ensembles, *IEEE Trans. Inform. Theory*, **53**, 4225 – 4236, 2007.

[6] R. G. Gallager, Information theory and reliable communication, Springer-Verlag, 1970.

[7] M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inform. Theory*, **27**, 533–547, 1981.