ISSN 0032-9460, Problems of Information Transmission, 2015, Vol. 51, No. 3, pp. 205–216. © Pleiades Publishing, Inc., 2015.
Original Russian Text © P.S. Rybin, V.V. Zyablov, 2015, published in Problemy Peredachi Informatsii, 2015, Vol. 51, No. 3, pp. 3–14.

CODING THEORY

Asymptotic Bounds on the Decoding Error Probability for Two Ensembles of LDPC Codes[1]

P. S. Rybin and V. V. Zyablov

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia
e-mail: prybin@iitp.ru, zyablov@iitp.ru

Received March 16, 2015; in final form, June 23, 2015

Abstract—Two ensembles of low-density parity-check (LDPC) codes with low-complexity decoding algorithms are considered. The first ensemble consists of generalized LDPC codes, and the second consists of concatenated codes with an outer LDPC code. Error exponent lower bounds for these ensembles under the corresponding low-complexity decoding algorithms are compared. A modification of the decoding algorithm of a generalized LDPC code with a special construction is proposed. The error exponent lower bound for the modified decoding algorithm is obtained. Finally, numerical results for the considered error exponent lower bounds are presented and analyzed.

DOI: 10.1134/S0032946015030011

1. INTRODUCTION

A lower bound on the error exponent (error exponent of the total probability of decoding denial and erroneous decoding), known as Forney's error exponent, for concatenated codes over a binary symmetric channel (BSC) was first obtained in [1]. Then a similar lower bound, known as the Blokh–Zyablov bound, was obtained for generalized concatenated codes in [2]. It should be noted that the decoding complexity of those code constructions is of the order $O(n^4)$, where n is the code length.

Low-density parity-check (LDPC) codes [3] are known to have the minimal decoding complexity growth with the code length. In [4] it was first shown that in the LDPC code ensemble there exist codes capable of correcting a linear portion of errors under a bit-flipping algorithm with complexity of the order $O(n \log n)$. Then in [5] the method developed in [4] was modified for the case of generalized LDPC codes. In [6] the estimates from [4, 5] were improved, and in [7] an estimate for an irregular LDPC code was obtained. In the present paper we use both the estimate from [6] and a slightly modified estimate from [5].

The error exponents of expander codes were investigated in [8,9]. It was shown that in this case there exist codes that attain the capacity of a BSC with positive exponent of error probability under a low-complexity iterative decoding algorithm. In [10] a special code construction in the class of generalized LDPC codes and a low-complexity decoding algorithm were proposed. A lower bound on the error exponent for these codes under the proposed low-complexity decoding algorithm was obtained. It was shown for the first time that an LDPC code with a special construction exists such that the error probability of the low-complexity decoding algorithm exponentially decreases for all code rates below the channel capacity.

[1] The research was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences at the expense of the Russian Science Foundation, project no. 14-50-00150.

In this paper we consider the concatenated code construction with an outer LDPC code proposed in [2, Appendix 6.9, pp. 216–218] and an LDPC code with a special construction proposed in [10]. A low-complexity decoding algorithm is given for each code construction; moreover, a modification of the decoding algorithm for the LDPC code with a special construction is proposed. In this paper we investigate the error decoding probability P over a memoryless BSC with error probability p. The estimation on the error decoding probability will be written in the following way:

$$P \le K(n) \exp\{-nE(\cdot)\},$$

where $K(n)$ is a function slowly (not exponentially) increasing in n, $E(\cdot)$ is the desired error exponent depending on the code construction parameters to be described below and on channel parameters (in particular, on the code rate R and error probability p of the BSC), and n is the code length. The following asymptotic (as $n \to \infty$) properties of the code will be considered in the paper:

- $E(\cdot) > 0$ for some parameters of the code construction and of the channel (e.g., for $R < C$, where C is the channel capacity of a BSC with error probability p);
- $E(\cdot)$ is independent of n.

In this paper we give lower bounds on the error exponent for the considered decoding algorithms. In conclusion, numerical results for the considered error exponent lower bounds are presented and analyzed.

2. LDPC CODES

Let us consider the construction of a parity-check matrix of a Gallager's regular LDPC code. Let $\boldsymbol{H}_b$ denote a block-diagonal matrix with b constituent parity-check matrices $\boldsymbol{H}_0$ of a single-parity-check (SPC) code on the main diagonal:

$$\boldsymbol{H}_b = \begin{pmatrix} \boldsymbol{H}_0 & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H}_0 & \dots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \underbrace{\boldsymbol{0} \quad \boldsymbol{0} \quad \dots \quad \boldsymbol{H}_0}_{b} \end{pmatrix},$$

where b is very large. If the length of SPC code is n_0, then $\boldsymbol{H}_b$ is a $b \times bn_0$ matrix. Let $\pi(\boldsymbol{H}_b)$ denote a random column permutation of $\boldsymbol{H}_b$. Then the matrix

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}_1 \\ \boldsymbol{H}_2 \\ \vdots \\ \boldsymbol{H}_\ell \end{pmatrix} = \begin{pmatrix} \pi_1(\boldsymbol{H}_b) \\ \pi_2(\boldsymbol{H}_b) \\ \vdots \\ \pi_\ell(\boldsymbol{H}_b) \end{pmatrix}$$

constructed using $\ell > 2$ such permutations as layers is a sparse $\ell b \times bn_0$ parity-check matrix $\boldsymbol{H}$, which defines an ensemble of LDPC code with length $n = bn_0$, where $n \gg n_0$. We denote this ensemble by $\mathscr{E}_G$.

Definition 1. For a given constituent code with parity-check matrix $\boldsymbol{H}_0$, define elements of the ensemble $\mathscr{E}_G$ by sampling the permutations π_l, $l = 1, 2, \dots, \ell$, independently and equiprobably.

Remark 1. It is clear that the construction of a Gallager's LDPC code can easily be generalized by replacing the parity-check matrix $\boldsymbol{H}_0$ of an SPC code with another parity-check matrix of a linear block code with length n_0 and the corresponding code rate R_0. In this case we obtain a generalized LDPC code.

The rate R of code with parity-check matrix $\boldsymbol{H}$ is lower bounded by

$$R \geq 1 - \ell(1 - R_0),$$

where R_0 is the constituent code rate. The equality occurs if and only if the matrix $\boldsymbol{H}$ has full rank.

3. "OPTIMAL" LINEAR CODES

Codes from the ensemble of "optimal" linear codes will be used as constituent codes for the code constructions considered below in this paper. This ensemble contains codes from the ensemble of random linear codes with error exponent that satisfies the lower bound $E_0(\cdot)$ under the maximum likelihood decoding algorithm. The following theorem, proved in [11] in the general form and formulated in [2] in the form given below, yields an estimate $E_0(\cdot)$ on the error exponent of a linear code under maximum likelihood decoding.

Theorem 1. *For any code rate R less than the capacity C of a memoryless BSC there exist binary linear block codes for which the error exponent under maximum likelihood decoding is lower bounded by a function $E_0(R, p)$ defined by the following equations:*

$$E_0(R, p) = -\delta_{VG}(R) \ln(2\sqrt{p(1-p)}) \quad \textit{for} \quad 0 \leq R \leq R_0,$$

where $R_0 = 1 - h\Big(\dfrac{2\sqrt{p(1-p)}}{1 + 2\sqrt{p(1-p)}}\Big)$;

$$E_0(R, p) = (1 - R)\ln 2 - \ln(1 + 2\sqrt{p(1-p)}) \quad \textit{for} \quad R_0 \leq R \leq R_*,$$

where $R_* = 1 - h\Big(\dfrac{\sqrt{p}}{\sqrt{p} + \sqrt{1-p}}\Big)$;

$$E_0(R, p) = \frac{s}{1-s}(1 - R)\ln 2 - \frac{1}{1-s}\ln(p^{1-s} + (1-p)^{1-s}),$$
$$R = 1 - h\Big(\frac{p^{1-s}}{p^{1-s} + (1-p)^{1-s}}\Big), \quad 0 \leq s \leq \frac{1}{2}, \quad \textit{for} \quad R_* \leq R \leq C = 1 - h(p),$$

where $\delta_{VG}(R)$ is the Gilbert–Varshamov bound and $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function.

4. CONCATENATED CODES WITH AN OUTER LDPC CODE

4.1. Description of the Code Construction

Let us consider the concatenated code construction proposed in [2] with an LDPC code as an outer code (in this case concatenated codes of the first order are constructed). The transmitted information, i.e., k_2 binary information symbols, is encoded with an LDPC code of length $n_2 = k_1 b_1$ (where k_1 and b_1 are positive integers) and code rate $R_2 = k_2/n_2$, which will be referred to as an outer code. Represent the obtained codeword as a $k_1 \times b_1$ binary matrix $\boldsymbol{U}$ in any manner (properties of the concatenated code that we are interested in do not depend on a way of representing the LDPC code codeword as a binary matrix $\boldsymbol{U}$):

$$\boldsymbol{U} = (\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^{b_1}),$$

where $\boldsymbol{u}^i$ is a binary column vector of size k_1.

Let $\boldsymbol{G}_0$ be an $n_1 \times k_1$ binary generating matrix of a code selected from the ensemble of "optimal" linear codes with error exponent $E_0(\cdot)$ under maximum likelihood decoding [11] and code rate R_1.

Then a codeword $\boldsymbol{X}$ of the concatenated code, i.e., a matrix of size $n_1 \times b_1$, is obtained as a result of multiplying the matrix $\boldsymbol{G}_0$ and matrix $\boldsymbol{U}$, i.e.

$$\boldsymbol{X} = \boldsymbol{G}_0\boldsymbol{U} = (\boldsymbol{x}^1, \boldsymbol{x}^2, \ldots, \boldsymbol{x}^{b_1}),$$

where $\boldsymbol{x}^i$ is a column vector of size n_1 (a codeword of the inner code).

Thus, we obtain a first-order concatenated code with length $n = b_1 n_1 = \dfrac{n_2}{R_1}$ and rate $R = R_1 R_2$.

Definition 2. Elements of the ensemble $\mathscr{E}_C$ of concatenated codes of the first order with an outer LDPC code are defined by independently and equiprobably sampling a Gallager's LDPC code from the ensemble $\mathscr{E}_G$ and a code with length n_1 and rate R_1 from the ensemble of "optimal" linear codes.

4.2. Decoding Algorithm

The decoding algorithm $\mathscr{A}_C$ of the above-described concatenated code construction consists of the following two steps:

1. A received sequence is represented as b_1 codewords of a linear code of length n_1, and then each of these b_1 codes is separately decoded by the maximum likelihood decoding algorithm;
2. A $k_1 \times b_1$ matrix is constructed from the sequence obtained on the previous step by selecting k_1 information symbols from each codeword of the linear code, and then the obtained matrix is represented as a sequence of the LDPC code and is decoded with the bit-flipping algorithm.

4.3. Error Exponent

Let us introduce the notation which will be used below in the formulation of theorems:

- Entropy function (note the difference from the binary entropy function $h(p)$)

$$H(\beta) = -\beta \ln \beta - (1-\beta)\ln(1-\beta);$$

- Auxiliary function

$$E^*(R_1, n_1, \omega_t, p, \beta) = \beta E_0(R_1, p) + E_2(\beta, \omega_t, p) - \frac{1}{n_1} H(\beta), \tag{1}$$

where $E_2(\cdot)$ is given by

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

and n_1 satisfies the condition

$$\frac{-\ln \beta_0}{E_0(R_1, p)} \le n_1 \le \frac{1}{R_1}\log_2 \log_2(n). \tag{2}$$

Furthermore, $E^*(\cdot)$ is defined for $R_1 < C$, where C is the capacity of a memoryless BSC with error probability p, for the values of n_1 satisfying condition (2), $0 < \omega_t < 1$, and $\omega_t \le \beta \le \beta_0$, where β_0 is defined for each specific code construction.

In [2] an estimate for the error exponent of the considered concatenated code construction under decoding algorithm $\mathscr{A}_C$ was obtained, which we reformulate in the following way.

Theorem 2. *In the ensemble $\mathscr{E}_C$ there exists (with probability $p_n \to 1$ as $n \to \infty$) a first-order concatenated code with an outer Gallager's LDPC code of length*

$$n = b_1 n_1 = \frac{b n_0}{R_1},$$

where n_0 and n_1 are accordingly selected constants (the lengths of the constituent outer LDPC code and inner linear code, respectively), and $n \to \infty$ ($b \to \infty$ and $b_1 \to \infty$), with rate

$$R = R_1 R_2,$$

such that the error exponent of this code over the memoryless BSC with error probability p under decoding algorithm $\mathscr{A}_C$ with complexity $O(n \log n)$ is lower bounded by

$$E_C(R_1, n_1, \omega_t, p) = \min_{\omega_t \le \beta \le \beta_0} \{E^*(R_1, n_1, \omega_t R_1, p, \beta)\},$$

where ω_t is the fraction of guaranteed errors corrected by a Gallager's LDPC code [6], $\beta_0 = \min\Big(\frac{\omega_t R_1}{2p}, 1\Big)$, *the function $E^*(\cdot)$ is defined in* (1), *and n_1 satisfies condition* (2).

Remark 2. Note that the proof of Theorem 2 (see the Appendix) requires the existence of a Gallager's LDPC code that is capable of correcting any error pattern of weight less than $\lfloor \omega_t n \rfloor$. In [6] it was shown that such a Gallager's LDPC code exists in the ensemble $\mathscr{E}_G$ with probability $p_n \to 1$ as $n \to \infty$. Furthermore, in [12] it was shown that for any code rate $R_2 < 1$ there exists a Gallager's LDPC code such that $\omega_t > 0$. Thus, we can omit the requirement of the existence of such a Gallager's LDPC code in formulations of this theorem and the following ones.

5. LDPC CODES WITH SPECIAL CONSTRUCTION

5.1. Description of the Code Construction

Let us now consider the construction of an LDPC code of a special type proposed in [10]. Let $\boldsymbol{H}_0$ be a parity-check matrix of an SPC code of length n_0 and rate R_0, and let $\boldsymbol{H}_1$ be a parity-check matrix of an "optimal" linear code with length n_1 and rate R_1. We construct the following two block matrices:

$$\boldsymbol{H}_{b_0} = \begin{pmatrix} \boldsymbol{H}_0 & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H}_0 & \dots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \underbrace{\boldsymbol{0} \quad \boldsymbol{0} \quad \dots \quad \boldsymbol{H}_0}_{b_0} \end{pmatrix}$$

and

$$\boldsymbol{H}_{b_1} = \begin{pmatrix} \boldsymbol{H}_1 & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H}_1 & \dots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \underbrace{\boldsymbol{0} \quad \boldsymbol{0} \quad \dots \quad \boldsymbol{H}_1}_{b_1} \end{pmatrix},$$

where b_0 and b_1 satisfy $n_0 b_0 = n_1 b_1$.

Now we construct a parity-check matrix $\boldsymbol{H}$ of a generalized LDPC code of a special type in the following way:

$$\boldsymbol{H} = \begin{pmatrix} \pi_1(\boldsymbol{H}_{b_0}) \\ \pi_2(\boldsymbol{H}_{b_0}) \\ \vdots \\ \pi_\ell(\boldsymbol{H}_{b_0}) \\ \pi_{\ell+1}(\boldsymbol{H}_{b_1}) \end{pmatrix},$$

where, as above, π_i, $i = \overline{1, \ell+1}$, is a random column permutation.

It is easy to see that the first ℓ layers of the parity-check matrix $\boldsymbol{H}$ form a parity-check matrix of a Gallager's LDPC code, which we denote by $\boldsymbol{H}_2$. Then the parity-check matrix $\boldsymbol{H}$ can be written in the following way:

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}_2 \\ \pi_{\ell+1}(\boldsymbol{H}_{b_1}) \end{pmatrix}.$$

Definition 3. The obtained construction of a generalized LDPC code will be called a Gallager's LDPC code with an additional layer composed of random linear codes selected from the ensemble of "optimal" linear codes with error exponent $E_0(\cdot)$ under maximum likelihood decoding [11] and with rate R_1 (LG-LDPC code).

Note that the length of the constructed code is $n = b_0 n_0 = b_1 n_1$, and the code rate R is lower bounded as

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

which, assuming that the rate of the Gallager's LDPC code is R_2, is equivalent to

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

Definition 4. Define elements of the ensemble $\mathscr{E}_{GL}$ are by independently and equiprobably sampling random column permutations π_i, $i = \overline{1, \ell+1}$.

5.2. Decoding Algorithm

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

1. A received sequence is separately decoded with the maximum likelihood decoding algorithm for each of the b_1 linear codes with parity-check matrix $\boldsymbol{H}_1$ from the $(\ell+1)$st layer of $\boldsymbol{H}$;
2. The tentative sequence is decoded using the bit-flipping algorithm by a Gallager's LDPC code with parity-check matrix $\boldsymbol{H}_2$.

It is important to note that algorithm $\mathscr{A}$ is not iterative. Every received sequence is decoded only once with the maximum likelihood algorithm using the linear codes $\boldsymbol{H}_1$ at first, and then the obtained sequence is decoded with the iterative bit-flipping algorithm using Gallger's LDPC code $\boldsymbol{H}_2$.

5.3. Modified Decoding Algorithm

The only difference between the modified decoding algorithm $\mathscr{A}'$ of an LG-LDPC code and the decoding algorithm $\mathscr{A}$ is the second step. On the second step in the modified decoding algorithm for bit-flipping decoding, the whole LG-LDPC code with parity-check matrix $\boldsymbol{H}$ is used, not only the Gallager's LDPC code with parity-check matrix $\boldsymbol{H}_2$. The idea of the bit-flipping algorithm for an LG-LDPC code is (as previously) to reduce the number of unsatisfied checks on each iteration step (i.e., a symbol is inverted if it reduces the number of unsatisfied checks in the LG-LDPC code).

Thus, the modified decoding algorithm $\mathscr{A}'$ consists of the following two steps:

1. A received sequence is decoded with the maximum likelihood decoding algorithm separately for each of the b_1 linear codes with parity-check matrix $\boldsymbol{H}_1$ from the $(\ell+1)$st layer of $\boldsymbol{H}$;
2. The tentative sequence is decoded with the bit-flipping algorithm by the LG-LDPC code with parity-check matrix $\boldsymbol{H}$.

5.4. Error Exponents

At first, let us consider the error exponent for an LG-LDPC code under decoding algorithm $\mathscr{A}$. We formulate the following theorem.

Theorem 3. *In the ensemble $\mathscr{E}_{GL}$ there exists (with probability $p_n \to 1$ as $n \to \infty$) an LG-LDPC code of length*

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

where n_0 and n_1 are accordingly selected constants (the lengths of constituent codes of the LG-LDPC code) and $n \to \infty$ ($b_0 \to \infty$ $b_1 \to \infty$) with rate

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

such that the error exponent of this code over a memoryless BSC with error probability p under decoding algorithm $\mathscr{A}$ with complexity $O(n \log n)$ is lower bounded by

$$E(R_1, n_1, \omega_t, p) = \min_{\omega_t \leq \beta \leq \beta_0} \{E^*(R_1, n_1, \omega_t, p, \beta)\},$$

where ω_t is the fraction of guaranteed errors corrected by a Gallager's LDPC code [6], $\beta_0 = \min\Big(\frac{\omega_t}{2p}, 1\Big)$, *the function $E^*(\cdot)$ is defined in* (1), *and n_1 satisfies condition* (2).

In [10] a corollary of Theorem 3 was obtained, which in this paper is formulated in the following way, omitting one of the conditions (see the Appendix).

Corollary. *We have $E(\cdot) > 0$ if $R \to C$, where C is the capacity of a memoryless BSC with error probability p, in such a way that $R_1 \to C$ and $R_2 < 1$.*

In [12] a novel condition was obtained on the existence of a symbol inverted during iteration of the bit-flipping algorithm. This condition is independent of a type of a constituent code and does not require their uniformity. Hence, using this condition and generalized methods developed in [5], we can obtain an estimate for the fraction ω_t' of guaranteed errors corrected by an LDPC code with the proposed construction (LG-LDPC code). Using this result we can obtain the following estimate for the error exponent of an LG-LDPC code under decoding algorithm $\mathscr{A}'$.

Theorem 4. *In the ensemble $\mathscr{E}_{GL}$ there exists (with probability $p_n \to 1$ when $n \to \infty$) an LG-LDPC code of length*

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

where n_0 and n_1 are accordingly selected constants (the lengths of constituent codes of the LG-LDPC code) and $n \to \infty$ ($b_0 \to \infty$ $b_1 \to \infty$), with rate

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

which is capable of correcting any error pattern of weight less than $\lfloor \omega_t' n \rfloor$, and the error exponent of this code over a memoryless BSC with error probability p under decoding algorithm $\mathscr{A}'$ with complexity $O(n \log n)$ is lower bounded by

$$E'(R_1, n_1, \omega_t', p) = \min_{\omega_t' \leq \beta \leq \beta_0} \{E^*(R_1, n_1, \omega_t', p, \beta)\},$$

where $\beta_0 = \min\Big(\frac{\omega_t'}{2p}, 1\Big)$, the function $E^*(\cdot)$ is defined in (1), *and n_1 satisfies condition* (2).

6. NUMERICAL RESULTS

In Fig. 1, the error exponent estimates $E_C(\cdot)$, $E(\cdot)$, and $E'(\cdot)$ are plotted versus the rate of the linear code R_1 for the fixed parameters $R = 0.5$, $n_1 = 2000$, and $p = 10^{-3}$.

Figure 2 presents plots of maximum achievable values of the error exponent estimates $E_C(\cdot)$, $E(\cdot)$, and $E'(\cdot)$ versus the code construction rate R for the fixed parameters $n_1 = 2000$ and $p = 10^{-3}$.

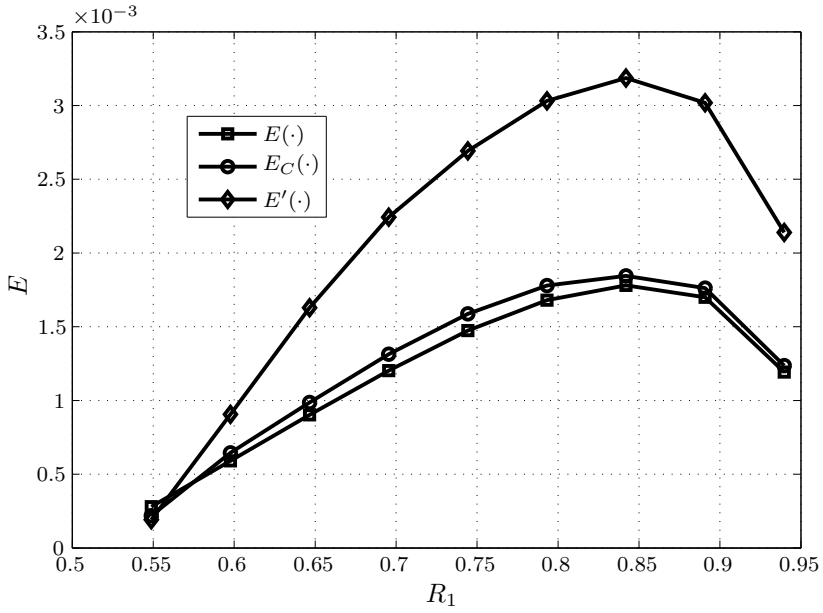

Fig. 1. Error exponent estimates $E_C(\cdot)$, $E(\cdot)$, and $E'(\cdot)$ versus the rate R_1 for the fixed parameters $R = 0.5$, $n_1 = 2000$, and $p = 10^{-3}$.

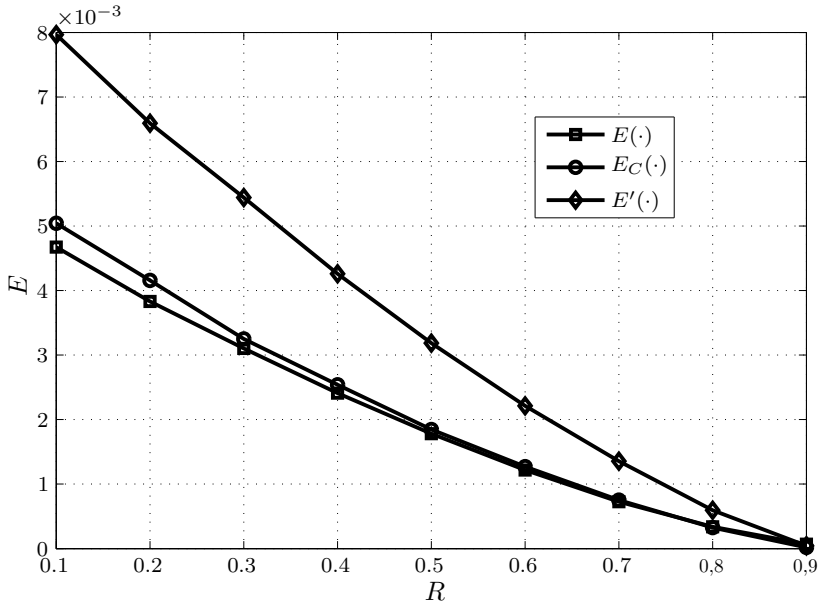

Fig. 2. Maximum achievable values of the error exponent estimates $E_C(\cdot)$, $E(\cdot)$, and $E'(\cdot)$ versus R for the fixed parameters $n_1 = 2000$ and $p = 10^{-3}$.

As one can see from Figs. 1 and 2, the error exponent estimate for the concatenated code construction under decoding algorithm $\mathscr{A}_C$ slightly exceeds the error exponent estimate for an LG-LDPC code under decoding algorithm $\mathscr{A}$. Furthermore, the difference between the estimates increases as the code rate R decreases. Although the code length of an LDPC code in the concatenated code construction is smaller (which is reflected by the factor R_1 at ω_t in the estimate) than the code length of an LDPC code in the LG-LDPC code construction, the observed difference can be explained in the following way. For a fixed code construction rate R and fixed rate R_1 of a linear code, the rate of the LDPC code R_2 can be chosen much lower in the case of the concatenated

code construction than in the case of the LG-LDPC code construction, because in the case of the LG-LDPC code construction the LDPC code contains parity-check symbols of the linear code as information symbols, which increases its code rate. The lower code rate of a Gallager's LDPC yields a larger estimate on ω_t, which in turn increases the estimate on the error exponent. However, the error exponent estimate for an LG-LDPC code under decoding algorithm $\mathscr{A}'$ significantly exceeds both of the estimates, because on the second step of decoding algorithm $\mathscr{A}'$ the redundancy of the linear code is also used (i.e., the total redundancy of the code construction), unlike what is done in $\mathscr{A}$ and $\mathscr{A}_C$.

APPENDIX

Let us proceed to the proofs of the theorems. First, we formulate and prove the following lemma.

Lemma. *The complexity of decoding algorithm $\mathscr{A}$ for an LG-LDPC code with length n is of order $O(n\log n)$ if the length of the linear code satisfies the inequality $n_1 \le \dfrac{1}{R_1}\log_2\log_2(n)$.*

Proof. Since the length of the linear code is n_1 and the code rate is R_1, the complexity of the maximum likelihood decoding algorithm for a single code is of order $O(2^{R_1 n_1})$. The total number of codes is b_1, which is proportional to n, and then the decoding complexity for all codes is of order $O(n2^{R_1 n_1})$.

In [6] it was shown that the complexity of the bit-flipping decoding algorithm for an LDPC code is $O(n\log n)$.

Therefore, the complexity of decoding algorithm $\mathscr{A}$ is of order $O(n\log_2 n)$ if the following condition is satisfied:

$$2^{R_1 n_1} \le n\log_2(n).$$

Hence we find a condition on n_1:

$$n_1 \le \frac{1}{R_1}\log_2\log_2(n). \quad \triangle \tag{3}$$

Remark 3. Similar lemmas can be formulated for algorithms $\mathscr{A}_C$ and $\mathscr{A}'$.

Now we pass to the proofs of Theorem 3 and its corollary.

Proof of Theorem 3. Let on the first step of decoding algorithm $\mathscr{A}$ for the LG-LDPC code the decoding error occur exactly in i linear codes. Since each code contains no more than n_1 errors, the total number of errors W after the first decoding step is not greater than in_1. Let $i = \beta b_1$, where β is the fraction of linear codes in which the decoding failure occurred; then

$$W \le \beta b_1 n_1 = \beta n.$$

According to [6], an LDPC code is capable of correcting any error pattern of weight W such that

$$W < W_0 = \lfloor \omega_t n \rfloor,$$

where ω_t is the fraction of guaranteed errors corrected by a Gallager's LDPC code [6, Theorem 1]. Hence, for $\beta < \omega_t$ the decoding error probability P of the LG-LDPC code under decoding algorithm $\mathscr{A}$ is 0:

$$P = 0, \quad \beta < \omega_t.$$

For $\beta > \omega_t$ the decoding error probability is defined in the following way:

$$P = \sum_{i=\lfloor \omega_t b_1 \rfloor}^{b_1} \binom{b_1}{i} P_2(W \ge W_0 \,|\, i) P_1^i(n_1, R_1, p)\big(1 - P_1(n_1, R_1, p)\big)^{b_1 - i}, \tag{4}$$

where $P_1(n_1, R_1, p)$ is the decoding error probability for the linear code,

$$P_1 \le \exp\{-n_1 E_0(R_1, p)\},$$

and $P_2(W \ge W_0 \,|\, i)$ is the probability of the event that the number of errors after the first step of decoding algorithm $\mathscr{A}$ is not less than W_0 provided that a decoding error occurred in exactly i linear codes.

Since in the case of erroneous decoding of the maximum likelihood decoding algorithm the number of errors in a block can at most become twice as large, there must be more than $\frac{W_0}{2}$ errors before the first step in i erroneous blocks in order to have more than W_0 errors after the first step of decoding algorithm $\mathscr{A}$. Then we can write $P_2(W \ge W_0 \,|\, i)$ in the following way:

$$P_2(W \ge W_0 \,|\, i) = \sum_{j=\lfloor \frac{\omega_t n}{2} \rfloor}^{in_1} \binom{in_1}{j} p^j (1-p)^{in_1 - j}.$$

Using the Chernov bound, we obtain

$$P_2(W \ge W_0 \,|\, i) \le \exp\{-nE_2(\beta, \omega_t, p)\},$$

where

$$E_2(\beta, \omega_t, p) = \begin{cases} \dfrac{1}{2}\left(\omega_t \ln \dfrac{\omega_t}{p} + (2\beta - \omega_t) \ln \dfrac{2\beta - \omega_t}{1-p}\right) - \beta \ln 2\beta, & \beta < \beta_0, \\ 0, & \beta \ge \beta_0. \end{cases} \tag{5}$$

Here $\beta = \dfrac{i}{b_1} > \omega_t$, and

$$\beta_0 = \min\Big(\frac{\omega_t}{2p}, 1\Big),$$

because $\beta > 1$ has no sense.

According to (5), the probability $P_2(W \ge W_0 \,|\, i)$ can be replaced with a trivial estimate $P_2(W \ge W_0 \,|\, i) \le 1$ for $i \ge \lceil \beta_0 b_1 \rceil$; then the sum (4) is upper bounded as follows:

$$P \le \sum_{i=\lfloor \omega_t b_1 \rfloor}^{\lfloor \beta_0 b_1 \rfloor} \binom{b_1}{i} P_2(W \ge W_0 \,|\, i) P_1^i(n_1, R_1, p) \big(1 - P_1(n_1, R_1, p)\big)^{b_1 - i} + \sum_{i=\lceil \beta_0 b_1 \rceil}^{b_1} \binom{b_1}{i} P_1^i(n_1, R_1, p) \big(1 - P_1(n_1, R_1, p)\big)^{b_1 - i}.$$

Let P_{II} denote the first sum on the right-hand side of this inequality and P_{I} denote the second. Let us consider each of the sums separately.

The sum P_{I} is easily estimated as a tail of the binomial distribution with probability P_1 using the Chernov bound:

$$P_{\mathrm{I}} \le \exp\{-nE_{\mathrm{I}}(R_1, n_1, \omega_t, p)\},$$

where

$$E_{\mathrm{I}}(R_1, n_1, p) = \beta_0 E_0(R_1, p) - \frac{1}{n_1} H(\beta_0)$$

and P_1 satisfies the condition

$$P_1(n_1, R_1, p) \le \beta_0,$$

whence

$$n_1 \ge \frac{-\ln \beta_0}{E_0(R_1, p)}. \tag{6}$$

Now consider the sum P_{II}:

$$P_{\mathrm{II}} \le \lceil(\beta_0-\omega_t)b_1\rceil \max_{\omega_t\le\beta\le\beta_0}\left\{\binom{b_1}{\beta b_1}P_2(W\ge W_0\,|\,\beta b_1)P_1^{\beta b_1}(1-P_1)^{(1-\beta)b_1}\right\}.$$

Hence, as $n\to\infty$ ($b_1\to\infty$ and $b_0\to\infty$), we obtain

$$E_{\mathrm{II}}(R_1,n_1,\omega_t,p)=\min_{\omega_t\le\beta\le\beta_0}\left\{E_2(\beta,\omega_t,p)+\beta E_0(R_1,p)-\frac{1}{n_1}H(\beta)\right\}. \tag{7}$$

Note that if the minimum on the right-hand side of (7) is attained at β_0, then according to (5) we obtain $E_{\mathrm{II}}=E_{\mathrm{I}}$. Consequently, $E_{\mathrm{II}}\le E_{\mathrm{I}}$.

It is easily seen that, as $n\to\infty$, the inequality

$$P\le\exp\{-nE(R_1,n_1,\omega_t,p)\}$$

is satisfied, where $E(R_1,n_1,\omega_t,p)=\min\{E_{\mathrm{II}}(R_1,n_1,\omega_t,p),E_{\mathrm{I}}(R_1,n_1,p)\}=E_{\mathrm{II}}(R_1,n_1,\omega_t,p)$.

According to the lemma proved above, the complexity of decoding algorithm $\mathscr{A}$ is of order $O(n\log n)$ if condition (3) is satisfied, but for the obtained estimate to hold, condition (6) must also be satisfied. Thus,

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

which completes the proof. △

Remark 4. The proof of Theorem 4 differs from that of Theorem 3 only in the fact that W_0 is set to be $\lfloor\omega_t' n\rfloor$, where ω_t' is the fraction of guaranteed error correcteds by the LG-LDPC code. It should be noted that the dependence of errors and their positions are not important for the proof; important is only the number of errors.

Remark 5. The proof of Theorem 2 differs from the proof of Theorem 3 only in the fact that W_0 is set to be $\lfloor\omega_t R_1 n\rfloor$, because the length of the Gallager's LDPC code in the concatenated code construction is $n_2=nR_1$.

Proof of the corollary. The correctness of the corollary is easily checked by noting that $E_0(\cdot)>0$ for $R_1<C$ [11] and $E_2(\cdot)\ge 0$, which follows from (5), and that we can always select n_1 in a such way that $\frac{1}{n_1}H(\beta)<\beta E_0(\cdot)+E_2(\cdot)$, because n_1 can be arbitrarily large according to condition (2). Furthermore, as was noted above, in [12] it was shown that for any code rate $R_2<1$ there exists a construction of a Gallager's LDPC code with $\omega_t>0$, which allowed us to omit this condition in the assertion of the corollary (unlike the assertion of a similar corollary in [10]). △

REFERENCES

1. Forney, G.D., Jr., *Concatenated Codes*, Cambridge: MIT Press, 1966. Translated under the title *Kaskadnye kody*, Moscow: Mir, 1970.
2. Blokh, E.L. and Zyablov, V.V., *Lineinye kaskadnye kody* (Linear Concatenated Codes), Moscow: Nauka, 1982.
3. Gallager, R.G., *Low-Density Parity-Check Codes*, Cambridge: MIT Press, 1963. Translated under the title *Kody s maloi plotnost'yu proverok na chetnost'*, Moscow: Mir, 1966.
4. Zyablov, V.V. and Pinsker, M.S., Estimation of the Error-Correction Complexity for Gallager Low-Density Codes, *Probl. Peredachi Inf.*, 1975, vol. 11, no. 1, pp. 23–36 [*Probl. Inf. Trans.* (Engl. Transl.), 1975, vol. 11, no. 1, pp. 18–28].

5. Zyablov, V.V., Johannesson, R., and Lončar, M., Low-Complexity Error Correction of Hamming-Code-Based LDPC Codes, *Probl. Peredachi Inf.*, 2009, vol. 45, no. 2, pp. 25–40 [*Probl. Inf. Trans.* (Engl. Transl.), 2009, vol. 45, no. 2, pp. 95–109].

6. Zyablov, V.V. and Rybin, P.S., Analysis of the Relation between Properties of LDPC Codes and the Tanner Graph, *Probl. Peredachi Inf.*, 2012, vol. 48, no. 4, pp. 3–29 [*Probl. Inf. Trans.* (Engl. Transl.), 2012, vol. 48, no. 4, pp. 297–323].

7. Rybin, P., On the Error-Correcting Capabilities of Low-Complexity Decoded Irregular LDPC codes, in *Proc. 2014 IEEE Int. Sympos. on Information Theory (ISIT'2014), Honolulu, HI, USA, June 29 – July 4, 2014*, pp. 3165–3169.

8. Barg, A. and Zémor, G., Error Exponents of Expander Codes, *IEEE Trans. Inform. Theory*, 2002, vol. 48, no. 6, pp. 1725–1729.

9. Barg, A. and Zémor, G., Error Exponents of Expander Codes under Linear-Complexity Decoding, *SIAM J. Discret. Math.*, 2004, vol. 17, no. 3, pp. 426–445.

10. Zyablov, V.V. and Rybin, P.S., Estimation of the Exponent of the Decoding Error Probability for a Special Generalized LDPC Code, *Inform. Protsessy*, 2012, vol. 12, no. 1, pp. 84–97 [*J. Commun. Technol. Electron.* (Engl. Transl.), 2012, vol. 57, no. 8, pp. 946–952].

11. Gallager, R.G., *Information Theory and Reliable Communication*, New York: Wiley, 1968. Translated under the title *Teoriya informatsii i nadezhnaya svyaz'*, Moscow: Sov. Radio, 1974.

12. Frolov, A.A. and Zyablov, V.V., Asymptotic Estimation of the Fraction of Errors Correctable by q-ary LDPC Codes, *Probl. Peredachi Inf.*, 2010, vol. 46, no. 2, pp. 47–65 [*Probl. Inf. Trans.* (Engl. Transl.), 2010, vol. 46, no. 2, pp. 142–159].