Distance Properties of Short LDPC Codes and their Impact on the BP, ML and Near-ML Decoding Performance

Irina E. Bocharova[1,2], Boris D. Kudryashov[1], Vitaly Skachek[2], and Yauhen Yakimenka[2]

[1] St. Petersburg University of Information Technologies,
Mechanics and Optics
St. Petersburg 197101, Russia
`irinaboc@ut.ee, kudryashov_boris@bk.ru`
[2] University of Tartu, Tartu 50409, Estonia
`vitaly@ut.ee, yauhen@ut.ee`

Abstract. Parameters of LDPC codes, such as minimum distance, stopping distance, stopping redundancy, girth of the Tanner graph, and their influence on the frame error rate performance of the BP, ML and near-ML decoding over a BEC and an AWGN channel are studied. Both random and structured LDPC codes are considered. In particular, the BP decoding is applied to the code parity-check matrices with an increasing number of redundant rows, and the convergence of the performance to that of the ML decoding is analyzed. A comparison of the simulated BP, ML, and near-ML performance with the improved theoretical bounds on the error probability based on the exact weight spectrum coefficients and the exact stopping size spectrum coefficients is presented. It is observed that decoding performance very close to the ML decoding performance can be achieved with a relatively small number of redundant rows for some codes, for both the BEC and the AWGN channels.

Keywords: LDPC code, minimum distance, stopping distance, stopping redundancy, BP decoding, ML decoding

1   Introduction

It is well-known that typically binary LDPC codes have minimum distances which are smaller than those of the best known linear codes of the same rate and length. It is not surprising, since minimum distance does not play an important role in iterative (belief propagation (BP)) decoding. On the other hand, a

significant gap in the frame error rate (FER) performance of BP and maximum-likelihood (ML) decoding motivates developing near-ML decoding algorithms for LDPC codes.

There are two main approaches to improving the BP decoding performance. First one is based on post-processing in case of BP decoder failure. Different post-processing techniques for decoding of binary LDPC codes over additive white Gaussian noise (AWGN) channels are studied in [7, 11, 24, 31]. A similar approach to decoding of nonbinary LDPC codes over extensions of the binary Galois field is considered in [2]. Near-ML decoding algorithms for LDPC codes over binary erasure channel (BEC) can be found in [16, 21, 23].

The second approach is based on identifying and destroying specific structural configurations such as trapping and stopping sets of the Tanner graph of the code. In particular, this can be done by adding redundant rows to the code parity-check matrix (see, for example, [14, 17, 19]).

Suboptimality of the above modifications of BP decoding rises the following question: which properties of LDPC codes and to what extent influence their decoding FER performance? In this paper, we are trying to partially answer this question by studying short LDPC codes. We consider both binary LDPC codes and binary images of nonbinary random LDPC codes over extensions of the binary field, as well as quasi-cyclic (QC) LDPC codes constructed by using an optimization technique in [4]. Parameters such as minimum distance, stopping distance, girth of the Tanner graph and estimates on the stopping redundancy are tabulated. Near-ML decoding based on adding redundant rows to the code parity-check matrix is analyzed. Simulated over the BEC and the AWGN channel, the FER performance of the BP, ML and near-ML decoding of these classes of LDPC codes is presented and compared to the improved upper bounds on the performance of ML decoding of regular LDPC codes [5] over the corresponding channels. The presented error probability bounds rely on precise average enumerators for given ensembles which makes these bounds tighter than known bounds (see e.g. [28]). By using an approach similar to that in [5], an improved upper bound on the performance of the BP decoding of binary images of nonbinary regular LDPC codes over BEC is presented.

The paper is organized as follows. In Section 2, all necessary notations and definitions are given. In Section 3, a near-ML decoding method, which is based on adding redundant rows to the code parity-check matrix, is revisited. In Section 4, a recurrent procedure for computing the exact coefficients of the weight and stopping set size spectra is described. The improved upper bound on the ensemble average performance of the BP decoding over BEC is derived. Tables of the computed code parameters along with the simulation results for the BP, ML and near-ML decoding are presented in Section 5. A comparison with the theoretical bounds is done and conclusions are drawn in Section 6.

2 Preliminaries

2.1 Ensembles of binary and binary images of nonbinary regular LDPC codes

For a binary linear $[n, k]$ code $\mathcal{C}$ of rate $R = k/n$ denote by $r = n - k$ its redundancy. We use a notation $\{A_{n,w}\}_{0 \leq w \leq n}$ for a set of code weight enumerators, where $A_{n,w}$ is a number of codewords of weight w. Let $\boldsymbol{H}$ be an $r \times n$ parity-check matrix which defines $\mathcal{C}$.

By viewing $\boldsymbol{H}$ as a biadjacency matrix [1], we obtain a corresponding bipartite Tanner graph. The girth g is the length of the shortest cycle in the Tanner graph.

When decoded over a BEC, the FER performance of the BP decoding is determined by the size of the smallest stopping set called stopping distance d_{stop} (see, for example, [9]). In turn, a stopping set is defined as a subset of indices of columns in a parity-check matrix, such that a matrix constructed from these columns does not have a row of weight one. The asymptotic behavior of a stopping set distribution for ensembles of binary LDPC codes is studied in [22]. In this paper, we study both the average performance of the ensembles of random LDPC codes and of QC LDPC codes widely used in practical schemes.

Two ensembles of random regular LDPC codes are studied below. First we study the Gallager ensemble [13] of (J, K)-regular LDPC codes, where J and K denote the number of ones in each column and in each row of the code parity-check matrix, respectively. Codes of this ensemble are determined by random parity-check matrices $\boldsymbol{H}$, which consist of the strips $\boldsymbol{H}_i$ of width $M = r/J$ rows each, $i = 1, 2, \ldots, J$. All strips are random column permutations of the strip where the jth row contains K ones in positions $(j-1)K+1, (j-1)K+2, \ldots, jK$, for $j = 1, 2, \ldots, n/K$.

Next, we study the ensemble of binary (J, K)-regular LDPC codes, which is a special case of the ensemble described in [26, Definition 3.15]. We refer to this ensemble as the Richardson-Urbanke (RU) ensemble of (J, K)-regular LDPC codes.

For $a \in \{1, 2, \ldots\}$ denote by a^m a sequence $(a, a, \ldots, a)$ of m identical symbols a. In order to construct an $r \times n$ parity-check matrix $\boldsymbol{H}$ of an LDPC code from the RU ensemble, one does the following:

- construct the sequence $\boldsymbol{a} = (1^J, 2^J, \ldots, n^J)$;
- apply a random permutation $\boldsymbol{b} = \pi(\boldsymbol{a})$ to obtain a sequence $\boldsymbol{b} = (b_1, \ldots, b_N)$, where $N = Kr = Jn$;
- set to one the entries in the first row of $\boldsymbol{H}$ in columns $b_1, \ldots, b_K$, the entries in the second row of $\boldsymbol{H}$ in columns $b_{K+1}, \ldots, b_{2K}$, etc. The remaining entries of $\boldsymbol{H}$ are zeros.

In fact, an LDPC code from the RU ensemble is (J, K)-regular if for a given permutation π all elements of subsequences $(b_{iK-K+1}, \ldots, b_{iK})$ are different for all $i = 1, \ldots, r$. It is shown in [20] that the fraction of regular codes among the

RU LDPC codes is roughly

$$\exp\left\{-\frac{1}{2}(K-1)(J-1)\right\}$$

which means that most of the RU codes are irregular. In what follows, we ignore this fact and interpret the RU LDPC codes as the (J, K)-regular codes, and call them "almost regular".

Generally, the design rate $R = 1 - J/K$ is a lower bound on the actual code rate since the rank of randomly constructed parity-check matrix can be smaller than the number of its rows. However, in our study the best generated almost regular RU codes always have the rate equal to the design rate. For this reason, we do not distinguish between the design rate and the actual rate.

In order to construct random binary images of nonbinary (J, K)-regular LDPC codes, we use the standard two-stage procedure. It consists of labeling a proper binary base parity-check matrix by random nonzero elements of the extension of the binary Galois field. In our work, we select a parity-check matrix of a binary LDPC code from the Gallager or the RU ensembles as the base matrix.

In what follows, the Gallager ensembles of binary regular LDPC codes and binary images of nonbinary regular LDPC codes are used only for the theoretical analysis, while for the simulations we use almost regular LDPC codes from the RU ensemble. The reason for this choice is that in the simulations, the RU LDPC ensembles outperform the Gallager LDPC codes with the same parameters.

2.2 QC LDPC codes

The QC LDPC codes represent a class of LDPC codes which is very intensively used in communication standards. Rate $R = b/c$ QC LDPC codes are determined by a $(c - b) \times c$ polynomial parity-check matrix of their parent convolutional code [18]

$$\boldsymbol{H}(D) = \begin{pmatrix} h_{11}(D) & h_{12}(D) & \dots & h_{1c}(D) \\ h_{21}(D) & h_{22}(D) & \dots & h_{2c}(D) \\ \vdots & \vdots & \ddots & \vdots \\ h_{(c-b)1}(D) & h_{(c-b)2}(D) & \dots & h_{(c-b)c}(D) \end{pmatrix} \tag{1}$$

where $h_{ij}(D)$ is either zero or a monomial entry, that is, $h_{ij}(D) \in \{0, D^{w_{ij}}\}$ with w_{ij} being a nonnegative integer, $w_{ij} \leq \mu$, and $\mu = \max_{i,j}\{w_{ij}\}$ is the syndrome memory.

The polynomial matrix (1) determines an $[Mc, Mb]$ QC LDPC block code using a set of polynomials modulo $D^M - 1$. By tailbiting the parent convolutional

code to length $M > \mu$, we obtain the binary parity-check matrix

$$
\boldsymbol{H}_{\mathrm{TB}} = \begin{pmatrix}
\boldsymbol{H}_0 & \boldsymbol{H}_1 & \ldots & \boldsymbol{H}_{\mu-1} & \boldsymbol{H}_\mu & \boldsymbol{0} & \ldots & \boldsymbol{0} \\
\boldsymbol{0} & \boldsymbol{H}_0 & \boldsymbol{H}_1 & \ldots & \boldsymbol{H}_{\mu-1} & \boldsymbol{H}_\mu & \ldots & \boldsymbol{0} \\
\vdots & & \ddots & \vdots & \vdots & \vdots & \ddots & \\
\boldsymbol{H}_\mu & \boldsymbol{0} & \ldots & \boldsymbol{0} & \boldsymbol{H}_0 & \boldsymbol{H}_1 & \ldots & \boldsymbol{H}_{\mu-1} \\
\vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\boldsymbol{H}_1 & \ldots & \boldsymbol{H}_\mu & \boldsymbol{0} & & \ldots & \boldsymbol{0} & \ldots & \boldsymbol{H}_0
\end{pmatrix},
\tag{2}
$$

of an equivalent (in the sense of column permutation) TB code (see [18, Chapter 2]), where $\boldsymbol{H}_i$, $i = 0, 1, \ldots, \mu$, are binary $(c - b) \times c$ matrices in the series expansion

$$
\boldsymbol{H}(D) = \boldsymbol{H}_0 + \boldsymbol{H}_1 D + \cdots + \boldsymbol{H}_\mu D^\mu,
$$

and $\boldsymbol{0}$ is the all-zero matrix of size $(c - b) \times c$. If each column of $\boldsymbol{H}(D)$ contains J nonzero elements, and each row contains K nonzero elements, the QC LDPC block code is (J, K)-regular. It is irregular otherwise.

Another form of the equivalent $[Mc, Mb]$ binary QC LDPC block code can be obtained by replacing the nonzero monomial elements of $\boldsymbol{H}(D)$ in (1) by the powers of the circulant $M \times M$ permutation matrix $\boldsymbol{P}$, whose rows are cyclic shifts by one position to the right of the rows of the identity matrix.

The polynomial parity-check matrix $\boldsymbol{H}(D)$ (1) can be interpreted as a $(c - b) \times c$ binary base matrix $\boldsymbol{B}$ labeled by monomials, where the entry in $\boldsymbol{B}$ is one if and only if the corresponding entry of $\boldsymbol{H}(D)$ is nonzero, i.e.

$$
\boldsymbol{B} = \boldsymbol{H}(D)|_{D=1}
$$

All three matrices $\boldsymbol{B}$, $\boldsymbol{H}(D)$, and $\boldsymbol{H}$ can be interpreted as bi-adjacency matrices of the corresponding Tanner graphs.

3 Stopping redundancy and convergence to the ML decoding performance

The idea to improve the performance of iterative decoding of linear codes over a BEC by using redundant parity checks was studied, for example, in [27, 34]. This approach was further explored in [29] (for BEC) and in [35] (for BSC and AWGN). The idea of using redundant parity checks was also studied in the context of linear-programming decoding [12], the reader can refer, for example, to [32].

A straightforward method to extend a parity-check matrix of an LDPC code is based on appending a predetermined number of dual codewords to the parity-check matrix. In this approach, the BP decoder uses the redundant matrix instead of the original parity-check matrix. One of the strategies used to extend the parity-check matrix consists of appending dual codewords in the order of their increasing weights starting with the minimum weight d_{dual}. A problem

of searching for low-weight dual codewords has high computational complexity in general, yet for short LDPC codes it is feasible. We apply this approach in the sequel, and study the convergence of the FER of BP decoding of LDPC codes determined by their extended parity-check matrices to the FER of the ML decoding (for both BEC and AWGN channels).

The stopping redundancy is defined as the minimum number of rows in a parity-check matrix required to ensure that the stopping distance of the code d_{stop} is equal to the code minimum distance d_{min}. For a set of the selected LDPC codes, we compute estimates on the minimum number of the rows required in order to ensure removal of stopping sets of a certain size. Next, we describe this approach in more detail. By ℓ-*th stopping redundancy*, ρ_ℓ, we denote the minimum number of rows in any parity-check matrix of the code, such that all ML-decodable stopping sets of size less than or equal to ℓ are removed. In particular, ρ_r is the minimum number of rows in any parity-check matrix of the code, such that there are no ML-decodable stopping sets of size up to r (incl.), i.e. no stopping sets which, if erased, still can be decoded by the ML decoder. Our definition of ℓ-th stopping redundancy is analogous to its counterpart in [15].

However, we stress the difference between the updated definition of the ℓ-th stopping redundancy for $\ell \geq d$ and its counterpart in [15]. In fact, the stopping sets of size $\ell \geq d$ that are *not* ML-decodable, are exactly the supports of the codewords.

In order to calculate the upper bounds on the ℓ-th stopping redundancy with a method based on [33], we first estimate by sampling u_i, the number of ML-decodable stopping sets of size i in a particular parity-check matrix. Then, we use the estimates on u_i ($i = 1, 2, \ldots, r$) with the method similar to [33, Thm. 1,2] in order to obtain the approximate upper bounds on the *stopping redundancy hierarchy*, i.e. the stopping redundancies $\rho_1, \rho_2, \ldots, \rho_r$.

In Table 1, we present estimates on ρ_ℓ, $\ell = d_{\text{min}}, d_{\text{min}} + 1, d_{\text{min}} + 2$, and $\ell = r$, along with $d_{\text{min}}, d_{\text{stop}}, d_{\text{dual}}$ and g, for a set of selected LDPC codes. In Section 5, we also present the simulated FER performance of the BP and ML decoding over the BEC for this set of codes with varying number of redundant rows. The same set of LDPC codes with varying number of redundant rows in their parity-check matrices is also simulated over the AWGN channel.

The LDPC codes from the following four families were selected:

- Random regular LDPC codes from the RU ensemble (rows 2 and 3 in Table 1)
- QC LDPC codes (row 4)
- Binary images of nonbinary regular LDPC codes (row 5)
- Linear codes represented in a "sparse form" (row 1)

Two random RU codes were selected by an exhaustive search among 100000 code candidates. As a search criteria, we used the minimum distance and the first spectrum coefficient $A_{d_{\text{min}},n}$. The QC LDPC code was obtained by optimization of lifting degrees for a constructed base matrix in order to guarantee the best possible minimum distance under a given restriction on the girth value of the

---

We recall that a support of a codeword is a stopping set.

code Tanner graph. For comparison, we simulated the best linear code with the same length and dimension determined by a parity-check matrix with the lowest possible correlation between its rows. Next, we refer to this form of the parity-check matrix as a "sparse form". Parameters of the selected codes are presented in Table 1. Here we use the notations 'RU' for random LDPC codes, 'L' for the best linear code with parity-check matrix in 'sparse form', 'NB' for the binary image of nonbinary regular LDPC code and 'QC' for QC LDPC code, respectively.

Table 1. Parameters of studied [48.24] codes

Code	$d_{\min}$	$A_{d_{\min},n}$	d_{stop}	d_{dual}	g	J,K	$\rho_{d_{\min}}, \rho_{d_{\min}+1}, \rho_{d_{\min}+2}$	ρ_r	Type
1	12	17296	4	12	4	6,12	6240,12151,23468	13 761 585	'L'
2	8	13	4	6	4	6,12	261,581,1254	13 683 513	'RU'
3	7	1	5	5	4	4,8	83,175,380	12 549 204	'RU'
4	7	8	7	5	6	3,6	58,130,274	9 876 964	'QC'
5	8	7	4	7	4	3,6	355,751,1551	13 819 276	'NB'

4 Upper bounds on ML and BP decoding error probability for ensembles of LDPC codes

In this section, we analyze the Gallager ensembles of binary and binary images of nonbinary (J,K)-regular LDPC codes. By following the approach in [5] we derive estimates on the decoding error probability of the ML and BP decoding by using precise coefficients of the average weight spectrum and average stopping set size spectrum, respectively. Additionally to the bounds on the performance of the ML decoding obtained in [5], in this paper we derive the improved bounds on the performance of BP decoding for both binary LDPC codes and binary images of nonbinary regular LDPC codes.

The main idea behind the approach in [5] is computing the average spectra coefficients recurrently with complexity linear in n. The resulting coefficients are substituted into the union-type upper bound on the error probability of the ML decoding over a BEC [3]

$$P_e \leq \sum_{i=d}^{n} \min \left\{ \binom{n}{i}, \sum_{w=d}^{i} S_w \binom{n-w}{i-w} \right\} \epsilon^i (1-\epsilon)^{n-i} \tag{3}$$

where S_w is the w-th weight (stopping set size) spectrum coefficient, ε is the erasure probability and d denotes the minimum distance (stopping distance). In order to upper-bound the error probability of the ML decoding over an AWGN channel, the average weight spectrum coefficients are substituted into the tangential-sphere bound [25].

Consider the Gallager ensemble of q-ary LDPC codes, where $q = 2^m$, $m \geq 1$ is an integer. The weight generating function of q-ary sequences of length n satisfying the nonzero part of one q-ary parity-check equation is given in [13] as

$$g(s) = \frac{(1 + (q-1)s)^K + (q-1)(1-s)^K}{q} \ .$$

(4)

It is easy to derive the weight generating function of q-ary sequences of length K and q-ary weight not equal to 1:

$$g_{\text{stop}}(s) = \sum_{w=0,2,3,\ldots,K} \binom{K}{w}(q-1)^w s^w = (1 + (q-1)s)^K - K(q-1)s.$$

(5)

Each q-ary symbol can be represented as a binary sequence (image) of length m. It is easy to see that different representations of a finite field of characteristic two will lead to different generating functions of binary images for the same ensemble of nonbinary LDPC codes. Following the techniques in [10], we study an average binary weight spectrum for the ensemble of m-dimensional binary images. By assuming uniform distribution on the m-dimensional binary images of the non-zero q-ary symbols, we obtain the generating function of the average binary weights of a q-ary symbol in the form

$$\phi(s) = \frac{1}{q-1}\sum_{w=1}^{m}\binom{m}{w}s^w = \frac{(1+s)^m - 1}{q-1} \ .$$

(6)

The average binary weight generating function for one strip is given by

$$G(s) = \big(g(\phi(s))\big)^M = \sum_{w=0}^{nm} N_{nm,w}s^w \ ,$$

where $N_{nm,w}$ denotes the average number of binary sequences $\boldsymbol{\beta}$ of weight w and of length nm satisfying $\boldsymbol{\beta}\mathcal{B}_i^{\mathrm{T}} = \mathbf{0}$. Here, $\mathcal{B}_i$ denotes the average binary image of $\boldsymbol{H}_i$. We obtain the average binary weight enumerator of nonbinary regular LDPC code as

$$\mathrm{E}\{A_{nm,w}\} = \binom{nm}{w}\big(p(w)\big)^J = \binom{nm}{w}^{1-J} N_{nm,w}^J,$$

(7)

where $p(w) = \binom{nm}{w}^{-1} N_{nm,w}$. By substituting (6) into (5), similarly to (7), we obtain the average binary stopping set size spectrum coefficient.

It is known that if the generating function is represented as a degree of another generating function it can be easily computed by applying a recurrent procedure. Details of the recurrent procedure for computing coefficients of the average weight spectra can be found in [5]. We proceed by computing $N_{nm,w}$ recursively.

5 Simulation results

We simulate the BP and ML decoding over the BEC and AWGN channel for the five LDPC codes whose parameters are presented in Table 1. In Fig. 1, the FER performance of the BP and ML decoding over the BEC and the AWGN channel is compared. It is easy to see that the best BP decoding performance both over the BEC and over the AWGN channel (and at the same time the worse ML decoding performance) is shown by the QC LDPC code with the most sparse parity-check matrix and the largest girth value of its Tanner graph. We remark that the best linear [48,24,12] code determined by a parity-check matrix in a "sparse form", as expected, has the best ML decoding performance over the both channels. Its BP decoding performance is worse than that of the selected LDPC codes except for the binary image of nonbinary LDPC code.

Fig. 2 shows the BP decoding performance over the BEC and AWGN channel of the codes 'QC' and 'L' from Table 1, when their parity-check matrices are extended. We call the corresponding decoding technique "redundant parity check" (RPC) decoding. The number next to "RPC" in Fig. 2 indicates the number of redundant rows that was added. The best convergence of the FER performance of the BP decoding over the BEC to that of the ML decoding is demonstrated by the QC LDPC code, while the best linear code has the slowest convergence of its BP performance to the ML decoding performance. We observe that the obtained simulation results are consistent with the estimates on the stopping redundancy hierarchy given in Table 1. Surprisingly, similar behavior can also be observed for the FER performance of RPC decoding over the AWGN channel.
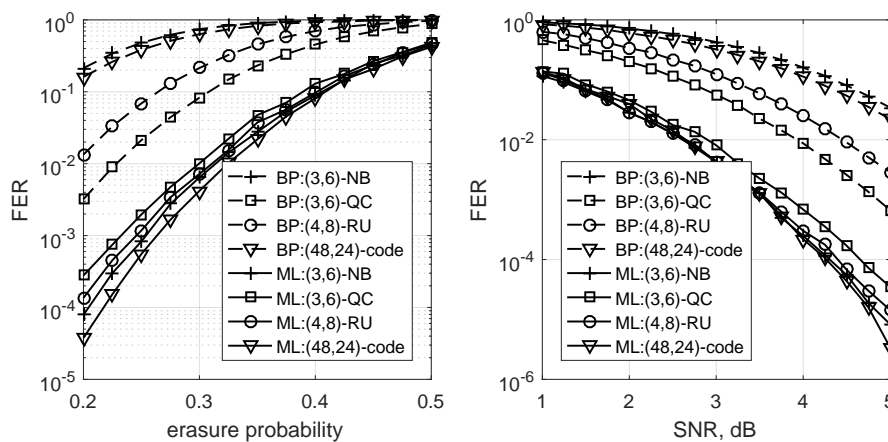
Fig. 1. Comparison of the FER performance of BP and ML decoding over the BEC and the AWGN channel for LDPC codes of length $n = 48$ and rate $R = 1/2$
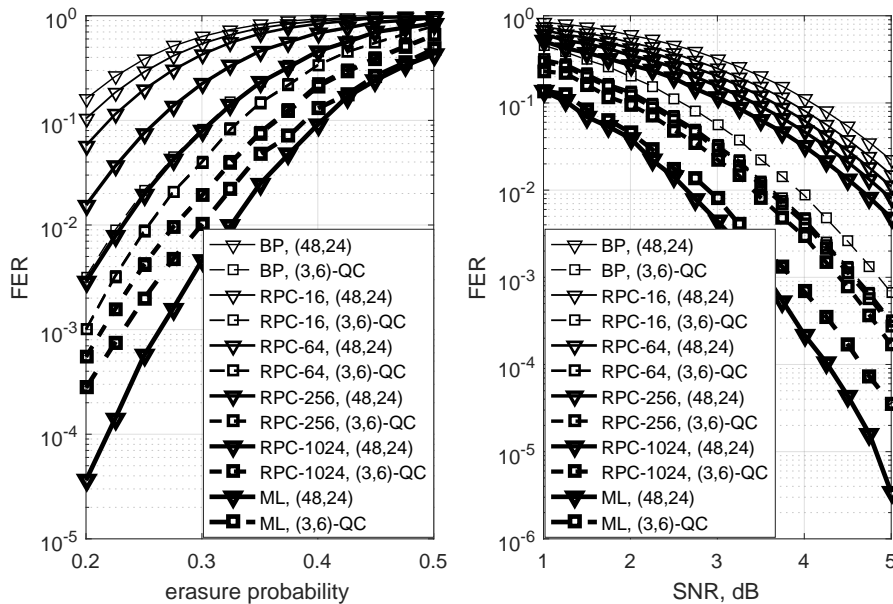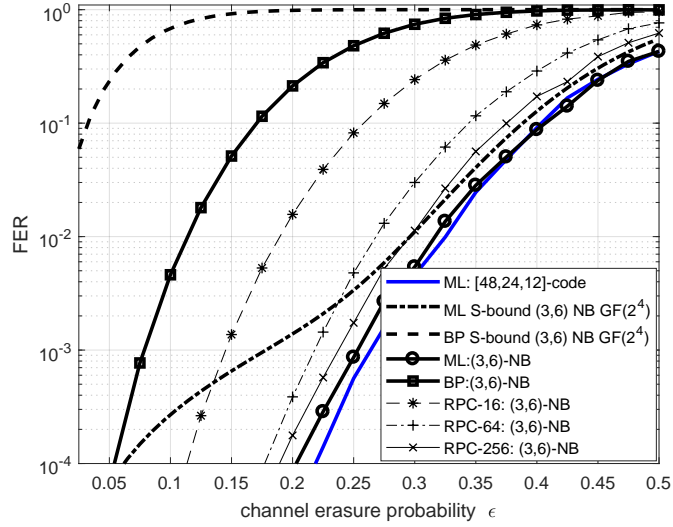
Fig. 2. FER performance of RPC decoding over the BEC and the AWGN channel for 'L' and 'QC' codes.

6 Discussion

In this section, we compare the simulated FER performance of the BP, ML and near-ML (RPC) decoding over the BEC and the AWGN channel with improved bounds on the ML and BP decoding performance. In Fig. 3, the FER performance over the BEC for the binary image of nonbinary $(3, 6)$-regular LDPC code over $GF(2^4)$ ('NB' code in Table 1) and the corresponding bounds are shown.

As it is shown in the presented plots, the ML performance of the 'NB' code is rather close to the ML performance of the 'L' code, but the convergence of the FER performance of the RPC decoding to the performance of the ML decoding for the 'NB' code is much faster than for the 'L' code.

In Fig. 4, the FER performance of the BP, ML and RPC decoding over the BEC and the AWGN channel is compared to the corresponding upper and lower bounds on the performance of the ML decoding. In particular, for comparison of the performance over the BEC, we use the improved upper bound (3) computed for the precise ensemble average spectrum coefficients for both random linear code and $(3, 6)$-regular random binary LDPC code. As a lower bound, we consider the tighten sphere-packing bound in [6]. For comparison of the performance over the AWGN channel, we show the tangential-sphere upper bound [25] computed with the precise ensemble average spectrum coefficients for the same two ensembles and the Shannon lower bound [30].

Fig. 3. Comparison of the FER performance of BP and RPC decoding over the BEC with improved union-type bounds (3) on the ML and BP decoding performance.
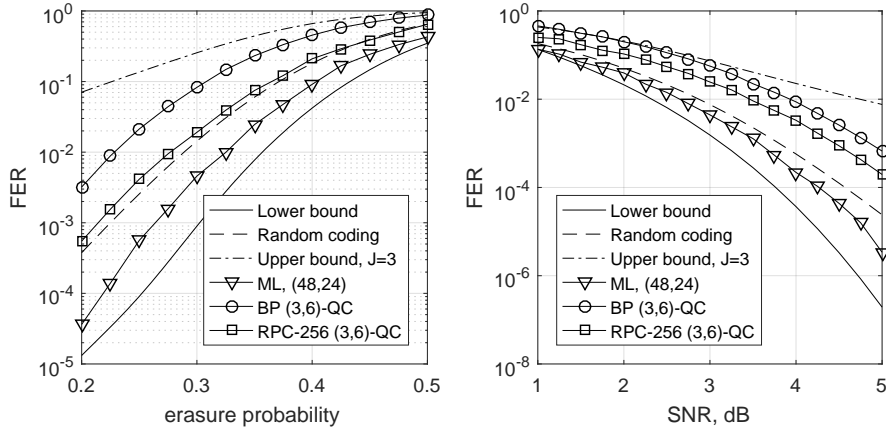
Fig. 4. Comparison of the FER performance of BP, ML and RPC decoding with upper and lower bounds on the ML decoding performance.

Based on the presented results, we conclude the following:

- Although it is commonly believed that the stopping sets influence the BP decoding performance over the BEC only, the behavior of the analyzed codes over the BEC and the AWGN channel is very similar. In particular, for short codes, the FER performance of the BP decoding over the AWGN channel can be significantly improved by adding redundant rows to the parity-check matrix.
- Convergence of the RPC decoding performance to the ML decoding performance is faster for those codes which are most suitable for iterative decoding, that is, codes with large girth of the Tanner graph.
- RPC decoding has a decoding threshold. When a small number of redundant rows is added, the FER performance rapidly improves, but after adding a certain number of redundant rows, the performance improvement becomes practically unjustified due to growing complexity.
- The FER performance of the RPC decoding achieves the FER performance of the ML decoding over the BEC with exponential (in length) complexity. However, a significant reduction in the FER compared to the FER of BP decoding can be achieved with a significantly lower complexity than that of the ML decoding.
- Binary images of nonbinary LDPC codes with RPC decoding demonstrate good FER performance over the BEC. In order to apply RPC decoding to these codes over the AWGN channel it is required to add q-ary parity-checks to their parity-check matrices. This method looks promising and is subject of our future research.

References

1. A. S. Asratian, *Bipartite Graphs and Their Applications*. Cambridge University Press, 1998, no. 131.
2. M. Baldi, F. Chiaraluce, N. Maturo, G. Liva, and E. Paolini, "A hybrid decoding scheme for short non-binary LDPC codes," *IEEE Commun. Letters*, vol. 18, no. 12, pp. 2093–2096, 2014.
3. E. R. Berlekamp, "The technology of error-correcting codes," *Proc. of the IEEE*, vol. 68, no. 5, pp. 564–593, 1980.
4. I. E. Bocharova, B. Kudryashov, and R. Johannesson, "Searching for binary and nonbinary block and convolutional LDPC codes," *IEEE Trans. Inform. Theory*, vol. 62, no. 1, pp. 163–183, Jan. 2016.
5. I. E. Bocharova, B. D. Kudryashov, and V. Skachek, "Performance of ML Decoding for Ensembles of Binary and Nonbinary Regular LDPC Codes of Finite Lengths," in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, 2017, pp. 794–798.
6. I. E. Bocharova, B. D. Kudryashov, and V. Skachek, "ML and Near-ML decoding Performance of LDPC Codes over BEC: Bounds and Decoding algorithms," submitted for publication.
7. I. E. Bocharova, B. D. Kudryashov, V. Skachek, and Y. Yakimenka, "Low complexity algorithm approaching the ML decoding of binary LDPC codes," in *Proc. IEEE Int. Symp. on Inform. Theory(ISIT)*, 2016, pp. 2704–2708.

8. I. E. Bocharova, B. D. Kudryashov, V. Skachek, and Y. Yakimenka, "Average spectra for ensembles of LDPC codes and their applications," in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, 2017, pp. 361–365.

9. C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, 2002.

10. M. El-Khamy and R. J. McEliece, "Bounds on the average binary minimum distance and the maximum likelihood performance of Reed Solomon codes," in *Proc. 42nd Allerton Conf. on Communication, Control and Computing*, 2004.

11. Y. Fang, J. Zhang, L. Wang, and F. Lau, "BP-Maxwell decoding algorithm for LDPC codes over AWGN channels," in *6th Int. Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, 2010, pp. 1–4.

12. J. Feldman, M.J. Wainwright, and D.R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inform. Theory,* vol. 51, no. 3, pp. 954-972, 2005.

13. R. G. Gallager, *Low-Density Parity-Check Codes.* M.I.T. Press: Cambridge, MA, 1963.

14. T. Hehn, J. B. Huber, and S. Laendner, "Improved iterative decoding of LDPC codes from the IEEE WiMAX standard," in *Proc. International ITG Conference on Source and Channel Coding (SCC),* 2010, pp. 1–6.

15. T. Hehn, O. Milenkovic, S. Laendner, and J. B. Huber, "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5308–5331, 2008.

16. G. Hosoya, T. Matsushima, and S. Hirasawa, "A decoding method of low-density parity-check codes over the binary erasure channel," in *Proc. 27th Symposium on Information Theory and its Applications (SITA)*, 2004, pp. 263–266.

17. M. Jianjun, J. Xiaopeng, L. Jianguang, and S. Rong, "Parity-check matrix extension to lower the error floors of irregular LDPC codes," *IEICE Trans. on Commun.*, vol. 94, no. 6, pp. 1725–1727, 2011.

18. R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding.* John Wiley & Sons, 2015, vol. 15.

19. S. Laendner, T. Hehn, O. Milenkovic, and J. B. Huber, "When does one redundant parity-check equation matter?" in *Global Telecommunications Conference (Globecom),* 2006, pp. 1–6.

20. S. Litsyn and V. Shevelev, "On ensembles of low-density parity-check codes: asymptotic distance distributions," *IEEE Trans. Inform. Theory*, vol. 48, no. 4, pp. 887–908, 2002.

21. P. M. Olmos, J. J. Murillo-Fuentes, and F. Pérez-Cruz, "Tree-structure expectation propagation for decoding LDPC codes over binary erasure channels," in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, 2010, pp. 799–803.

22. A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 929–953, 2005.

23. H. Pishro-Nik and F. Fekri, "On decoding of low-density parity-check codes over the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 439–454, 2004.

24. H. Pishro-Nik and F. Fekri, "Results on punctured low-density parity-check codes and improved iterative decoding techniques," *IEEE Trans. Inform. Theory*, vol. 53, no. 2, pp. 599–614, 2007.

25. G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1284–1292, 1994.

26. T. Richardson and R. Urbanke, *Modern Coding Theory.* Cambridge University Press, 2008.

27. N. Santhi and A. Vardy, "On the effect of parity-check weights in iterative decoding," in *Proc. IEEE Intern. Symp. on Inform. Theory (ISIT),* Chicago, IL, 2004, p. 322.

28. I. Sason and S. Shamai, "Improved upper bounds on the ensemble performance of ML decoded low density parity check codes," *IEEE Commun. Letters*, vol. 4, no. 3, pp. 89–91, 2000.

29. M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 922–932, 2006.

30. C. E. Shannon, "Probability of Error for Optimal Codes in a Gaussian channel," *Bell System Technical Journal,* vol. 38, no. 3, pp. 611–656, 1959.

31. N. Varnica, M. P. Fossorier, and A. Kavcic, "Augmented belief propagation decoding of low-density parity check codes," *IEEE Trans. Commun.*, vol. 55, no. 7, pp. 1308–1317, 2007.

32. P. O. Vontobel and R. Kötter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," arXiv preprint cs/0512078, 2005.

33. Y. Yakimenka and V. Skachek, "Refined upper bounds on stopping redundancy of binary linear codes," in *Proc. IEEE Information Theory Workshop (ITW)*, 2015, pp. 1–5.

34. J. S. Yedidia, J. Chen, and M. Fossorier, "Generating code representations suitable for belief propagation decoding," in *Proc. 40-th Allerton Conf. Commun., Control, and Computing,* Monticello, IL, 2002.

35. J. Zumbrägel, M. F. Flanagan, and V. Skachek, "On the pseudocodeword redundancy of binary linear codes," *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4848-4861, 2012.