

# On the Performance of Short Forward Error-Correcting Codes

Sheng Tong, Dengsheng Lin, Aleksandar Kavčić, *Senior Member, IEEE*, Li Ping, *Member, IEEE*, and Baoming Bai, *Member, IEEE*

**Abstract**—This letter investigates the performance of short forward error-correcting (FEC) codes. Reed-Solomon (RS) codes and concatenated zigzag codes are chosen as representatives of classical algebraic codes and modern simple iteratively decodable codes, respectively. Additionally, random binary linear codes are used as a baseline reference. Our main results (demonstrated by simulations and ensemble distance spectrum analysis) are as follows: 1) Short RS codes are as good as random binary linear codes; 2) Carefully designed short low-density parity-check (LDPC) codes are almost as good as random binary linear codes; 3) Low complexity belief propagation decoders incur considerable performance loss at short coding lengths. Thus, future work could focus on developing low-complexity (near) optimal decoders for RS codes and/or LDPC codes.

**Index Terms**—Reed-Solomon (RS) codes, concatenated zigzag (CZ) codes, adaptive belief propagation.

## I. INTRODUCTION

THE advent of turbo codes [1] and the rediscovery of low-density parity-check (LDPC) codes [2] revealed that for long code lengths (in the orders of tens of thousands), concatenated codes with iterative decoding can asymptotically approach the capacities of additive white Gaussian noise (AWGN) channels. For short code lengths, however, there is still a considerable gap between the performance of the known practical codes and the theoretical limits, at least when belief propagation (BP) decoding is employed. The gap can be due to deficiencies in both code structures and available decoders.

The work presented in this letter is motivated by the recent progress of decoding techniques that can offer near maximum likelihood (ML) performance. This allows us to examine what is potentially achievable by the available options. We will use the simulation results of random binary linear (RBL) codes as a reference of performance limit. A RBL code is constructed using a randomly generated binary parity check matrix. Following the arguments by Shannon, long RBL codes are asymptotically capacity-approaching and we expect that they also offer nearly optimal performance at relatively short lengths. We will show that if high decoding complexity is

acceptable, some existing short codes such as Reed-Solomon (RS) codes and concatenated zigzag (CZ) codes can perform close to RBL codes. However, this is not the case when a low complexity decoder (such as BP decoding) is used. Our work provides useful insights into the encoding and decoding issues for short codes and points to the necessity of developing more efficient decoding algorithms for available short codes.

## II. ITERATIVE RELIABILITY-BASED DECODING WITH ADAPTIVE BELIEF PROPAGATION

An improved ABP-OSD soft decoding scheme is presented in [4] which combines an adaptive belief propagation (ABP) [3] procedure together with a reliability-based ordered statistics decoding (OSD) [5]. The principles involved are briefly explained below.

ABP is a modified version of belief propagation. Its novelty lies in adaptively modifying the parity-check sub-matrix corresponding to the least reliable bits (LRBs) in the parity check matrix to an identity matrix using Gaussian elimination in each decoding iteration, which prevents error propagation and leads to improved decoding performance.

For an  $(n, k)$  linear block code, the decoding process of OSD( $i$ ) ( $i$  is the order of OSD) can be separated into two stages. The first stage is to determine the positions of  $k$  most reliable bits (that should be linearly independent, forming the most reliable basis (MRB)) by applying Gaussian elimination to the generator matrix. The second stage is to flip at most  $i$  bits in the MRB to construct a codeword list and choose the most likely codeword from the list (i.e., the one leading to lowest mean square error) as the decoder output.

From above, it is seen that both ABP and OSD involve Gaussian elimination and thus two Gaussian eliminations are required per iteration. A low-cost approach is to apply a Gaussian elimination to the parity check matrix  $\mathbf{H}$  and transforms it to a form  $[\mathbf{I}, \mathbf{H}^{MRB}]$ , where  $\mathbf{I}$  (an identity matrix) corresponds to the LRBs and  $\mathbf{H}^{MRB}$  corresponds to the MRB. Then, OSD is performed before ABP using the obtained parity check matrix. Since OSD does not change reliabilities, ABP does not need to perform Gaussian elimination again in the same iteration and thus only one Gaussian elimination is performed per iteration. ABP is used to improve the reliabilities of the LRBs and then OSD is applied to search for the most likely combinations of the MRB. The Gaussian elimination here alleviates the correlation problem for BP decoding and at the same time reduces the complexity involved.

## III. PERFORMANCE COMPARISON OF VARIOUS SHORT CODES

It has been shown that ABP-OSD can achieve near ML decoding performance. We now use it as a useful tool to evaluate

Manuscript received May 10, 2007. The associate editor coordinating the review of this letter and approving it for publication was Dr. Vladimir Stankovic. This work was supported by a strategic grant from City University of Hong Kong [Project No. 7001812].

S. Tong and B. Bai are with the State Key Lab of ISN, Xidian University, Xi'an, 710071, P. R. China (email: ts\_xd@163.com, bm-bai@mail.xidian.edu.cn).

D. Lin is with the College of Communication and Information, University of Electronic Science and Technology, P.R. China (email: linds@uestc.edu.cn).

A. Kavčić is with the Department of Electrical Engineering, University of Hawaii, USA (email: kavcic@hawaii.edu).

L. Ping is with the Department of Electronic Engineering, City University of Hong Kong, Hong Kong (email: eelping@cityu.edu).

Digital Object Identifier 10.1109/LCOMM.2007.070746.

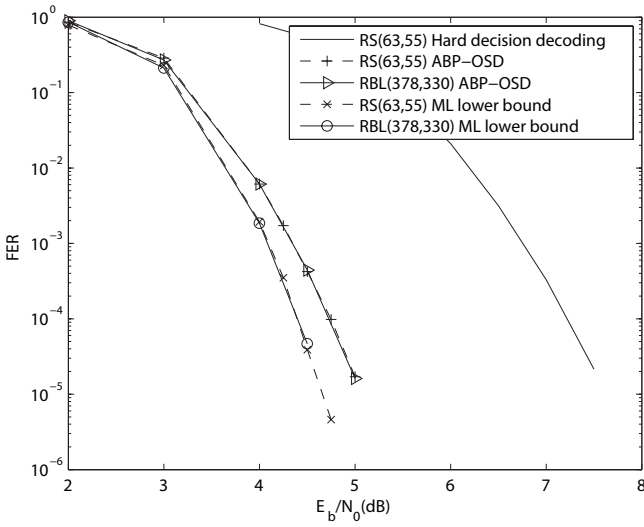


Fig. 1. Frame error rate (FER) performance of RS(63,55) code and a (378,330) random binary linear code on an AWGN channel.

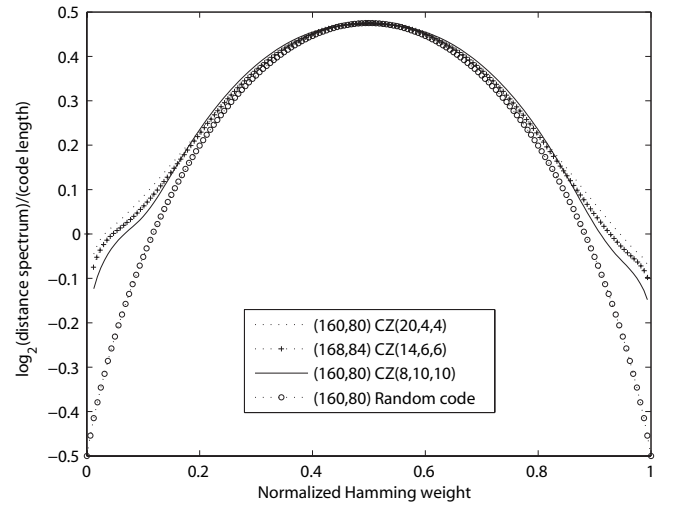


Fig. 3. The average ensemble distance spectra of concatenated zigzag codes and random codes.

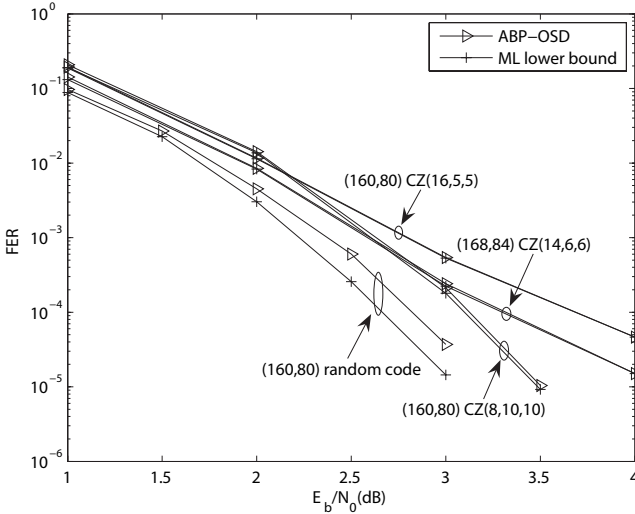


Fig. 2. Frame error rate (FER) performance of CZ codes with different numbers of component codes and a (160,80) random binary linear code.

various coding schemes. We will assume an AWGN channel with BPSK modulation. The number of iterations for ABP is 20 and the order of OSD is 3. A simulation-based approach to ML decoding lower bound on frame error rate (FER) is used [10]. Note that the better the decoder performance, the tighter the simulation-based ML lower bound. Our preliminary investigation (via simulation and ensemble distance spectrum analysis) shows the following:

#### A. High-rate short RS codes are as good as random binary linear codes [3,11]

Fig. 1 shows the FER performance of the RS(63,55) code and a RBL code of the same length and rate. From Fig. 1, it is seen that hard decision decoding incurs a coding gain loss of about 2-3dB when compared to the near ML decoding performance. This means that the potential coding gain of short RS codes is significant and should be exploited fully. A more interesting phenomenon is that short RS codes perform

similarly to RBL codes, which suggests that short RS codes have good error correcting performance. Moreover, due to their algebraic structure, hardware implementations of short RS codes are preferred for practical applications.

#### B. Carefully designed LDPC codes perform close to random binary linear codes

Concatenated zigzag (CZ) codes is a special class of LDPC codes, which are obtained by combining several parallel concatenated zigzag codes linked by interleavers [6]. Fig. 2 depicts the near ML decoding FER performance of several rate-1/2 short CZ codes with different numbers of component codes, together with a length-160 rate-1/2 RBL code. A CZ code is denoted by  $CZ(m, J, K)$ , where  $m$  is the number of segments contained in each zigzag code,  $J$  is the information block length of each segment, and  $K$  is the number of component zigzag codes. Hence, a  $CZ(m, J, K)$  code is a length- $m(K+J)$  rate- $J/(J+K)$  block code constructed by a turbo-type parallel concatenation. Jointly optimized linear interleavers [8] are adopted for CZ codes, which are specified by angular coefficient vectors. The angular coefficient vectors for  $CZ(16,5,5)$ ,  $CZ(14,6,6)$ , and  $CZ(8,10,10)$  are (1, 30, 24, 56, 21), (1, 23, 52, 22, 74, 34), and (1, 11, 37, 49, 66, 70, 56, 48, 43, 4), respectively. It is seen from Fig.3 that, when  $K$  is large, the CZ code ensemble weight distribution (computed using the algorithm outlined in [6]) approaches a binomial distribution. This implies that a CZ code with a large  $K$  has a similar weight distribution as a RBL code, which further verifies the observation in Fig.2 that the near ML decoding performance of CZ codes improves when  $K$  increases. The gap between the CZ (8,10,10) code and the (160,80) RBL code is only a fraction of a dB. Incidentally, a CZ code can also be viewed as a special case of LDPC or repeat-accumulate (RA) codes based on a semi-random parity check matrix [7]. However, CZ codes have faster convergence speeds using a serial belief propagation decoder [6] than general LDPC codes. For short block lengths, due to their layered structure, CZ codes can also outperform RA codes.

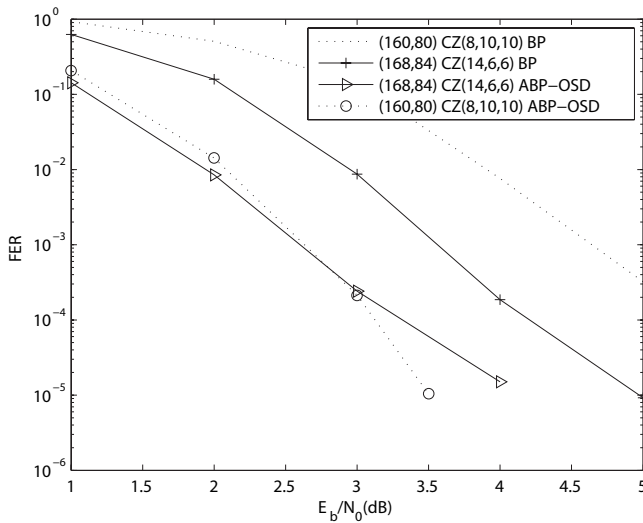


Fig. 4. Frame error rate (FER) performance of CZ codes (the same codes used in Fig.2) under BP decoding and near ML decoding on an AWGN channel.

*C. For short block lengths, there is still a considerable gap between the performances by belief propagation and ML decoders*

Both the belief propagation decoding performance and near ML decoding performance (via ABP-OSD) of a length-168 rate-1/2 CZ(14,6,6) code and a length-160 rate-1/2 CZ(8,10,10) code are shown in Fig.4. From Fig.4, it is seen that the gap between near ML decoding performance (involving very high complexity) and belief propagation decoding performance (involving much lower complexity) increases as  $K$  increases. The gap is about 2dB for the CZ(8,10,10) code at a FER of  $10^{-3}$ .

#### IV. CONCLUSIONS

In summary, good short RS codes and carefully designed short LDPC codes perform similarly to random binary linear codes. This provides useful insights into the encoding and

decoding issues for short FEC codes and provides interesting directions for future work, such as developing low-complexity (near) ML decoders for short RS codes and short LDPC codes, or searching for good short codes that allow efficient (near) ML decoders.

#### ACKNOWLEDGMENT

The first author is grateful for the great help from Keying Wu and Jing Jiang. We would also like to thank the anonymous reviewers for their valuable comments.

#### REFERENCES

- [1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," in *Proc. IEEE Int. Conf. Communications*, pp. 1064-1070, May 1993.
- [2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, pp. 1645-1646, Aug. 1996.
- [3] J. Jiang and K. R. Narayanan, "Iterative soft input soft output decoding of Reed-Solomon codes by adapting the parity check matrix," *IEEE Trans. Inf. Theory*, vol. 8, pp. 3746-3756, Aug. 2006.
- [4] A. Kothiyal, O. Y. Takeshita, W. Jin, and M. Fossorier, "Iterative reliability-based decoding of linear block codes with adaptive belief propagation," *IEEE Commun. Lett.*, vol. 9, pp. 1067-1069, Dec. 2005.
- [5] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 41, pp. 1379-1396, Sept. 1995.
- [6] L. Ping, X. Huang, and N. Phamdo, "Zigzag codes and concatenated zigzag codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 800-807, Feb. 2001.
- [7] L. Ping, W. K. Leung, and N. Phamdo, "Low density parity check codes with semi-random parity check matrix," *Electron. Lett.*, vol. 35, pp. 38-39, Jan. 1999.
- [8] C. He, M. Lentmaier, D. J. Costello, Jr., and K. S. Zigangirov, "Joint permutator analysis and design for multiple turbo codes," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4068-4083, Sept. 2006.
- [9] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. 36th Allerton Conf. on Communication, Control, and Computing*, pp. 201-210, Sept. 1998.
- [10] R. Lucas, M. Bossert, M. Breitbart, "On iterative soft-decision decoding of linear binary block codes and product codes," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 276-296, Feb. 1998.
- [11] M. Fossorier and A. Valembois, "Reliability-based decoding of Reed-Solomon codes using their binary image," *IEEE Commun. Lett.*, vol. 8, pp. 452-454, July 2004.