On Short Forward Error-Correcting Codes for Wireless Communication Systems

Sheng Tong*, Dengsheng Lin*, Aleksandar Kavčić†, Baoming Bai*, and and Li Ping‡

Abstract—For real-time wireless communications, short forward error-correcting (FEC) codes are indispensable due to the strict delay requirement. In this paper we study the performance of short FEC codes. Reed-Solomon (RS) codes and concatenated zigzag (CZ) codes are chosen as representatives of classical algebraic codes and modern simple iterative decodable codes, respectively. Additionally, we use random binary linear codes as a baseline reference for comparison. Our main results (demonstrated by both simulation 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 when high decoding complexity can be tolerated; 3) Low complexity belief propagation decoders incur considerable performance loss at short coding lengths.

Keywords-Reed-Solomon (RS) codes; low-density parity-check (LDPC) codes; Adaptive belief-propagation (ABP)

I. Introduction

The last decade has seen impressive developments in both wireless communications and forward error-correcting (FEC) codes. In particular, the advent of turbo codes [1] and the rediscovery of low-density parity-check (LDPC) codes [2] has demonstrated that for long block lengths (in the order of tens of thousands), concatenated codes with iterative decoding can asymptotically approach the capacities of additive white Gaussian noise (AWGN) channels.

Delay sensitive services e.g., voice and video, still constitute the majority of traffic in current wireless communications. For such services, latency is a serious concern and the coding length can be limited. For example, the WiMax standard permits use of LDPC codes as an optional channel coding scheme, with coding length options covering the range from 576 to 2304 (measured in bits) [13]. The European 3GPP standard uses turbo codes with information block lengths ranging from 40 to 5114 (measured in bits) [14]. However, the performance when using short block lengths is a significant concern since there remains a considerable gap between the performance of practical known short codes and the theoretical limits, at least when belief propagation (BP) decoding is employed. This gap may be associated with deficiencies in both encoder and decoder operation.

This paper provides an overview of the performance of short FEC codes based on state of the art encoding and decoding techniques. We use random binary linear (RBL) codes as a baseline reference. Here, a RBL code is constructed by randomly generating a parity-check matrix. Following the arguments by Shannon, long random codes are asymptotically capacity approaching. Hence, we expect that they could also offer nearly optimal performance at relatively short block lengths.

For more practical codes, we examine Reed-Solomon (RS) and LDPC codes that represent the classical algebraic codes and modern iterative decodable codes respectively. Among the various options for LDPC codes, we focus on the concatenated zigzag (CZ) codes [8] that can offer good performance with very low-cost encoder and decoder structures. We show that with carefully designed linear interleavers, such simple codes can perform very well at short coding lengths.

Our work is motivated by the recent progress of soft decision decoding techniques that offer near maximum likelihood (ML) performance at short block lengths. This allows us to examine what is potentially achievable with the available code options. For code structures, we show that if high decoding complexity is allowed, some existing short FEC codes may perform close to RBL codes. However, this is not the case when low complexity options (such as hard decoding algorithm for RS codes and belief propagation algorithm for CZ codes) are used. Our work provides useful insights into the encoding and decoding issues for short codes applicable to wireless systems and points to the necessity of developing more efficient decoding algorithms for existing short codes.

II. ITERATIVE RELIABILITY-BASED DECODING WITH ADAPTIVE BELIEF PROPAGATION

Recently, an enhanced hybrid soft decoding algorithm for linear block codes is presented [4] which combines a reliability-based decoding algorithm (e.g., ordered statistics decoding (OSD) [5]) and adaptive belief propagation (ABP) [3], denoted as ABP-OSD. This algorithm provides improved soft decision decoding performance. For short block lengths, this algorithm can even approach the ML decoding performance. The basic idea is to use the soft output provided by ABP in each iteration as the input for OSD. During the iterative process, the log-likelihood ratios (LLRs) from ABP will provide improved estimation. Consequently the errors among the most reliable basis (MRB) will reduce and so OSD

^{*}State Key Laboratory of Integrated Service Networks, Xidian University, P. R. China

[#] College of Communication and Information, University of Electronic Science and Technology, P.R. China

[†]Department of Electrical Engineering, University of Hawaii, USA

Department of Electronic Engineering, City University of Hong Kong, Hong Kong

This work was fully supported by a strategic grant from City University of Hong Kong, China [Project No.7001984].

become more efficient. Some details of this hybrid strategy are explained below.

A. Ordered statistics decoding (OSD) [5]

Soft decision decoding of general block linear codes based on OSD is first considered in [5]. Several techniques, including iterative information set reduction [6] and the box and match technique [7], have been developed subsequently to further improve its efficiency.

OSD can be briefly outlined as follows. 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 K most reliable bits, i.e. MRB, which should be chosen to be linearly independent by applying Gaussian elimination on the generator matrix and transforming the K columns corresponding to the K most reliable bits into an identity 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 which is closest to the received signal in Euclidean distance) as the decoder output.

B. Adaptive belief propagation (ABP) [3]

It is well known that the belief propagation algorithm [17] works well for the decoding of linear codes with sparse graph representations. However, the performance of the belief propagation algorithm deteriorates in dense graphs. ABP is a modified version of belief propagation algorithm suitable for dense graphs. Its novelty lies in adaptively modifying the parity-check sub-matrix corresponding to the least reliable bits in the parity-check matrix to an identity matrix using a Gaussian elimination in each decoding iteration (see Fig.1), which prevents error propagation. ABP applies to and greatly improves soft decoding performance of general linear block codes.

Both OSD and ABP involve Gaussian elimination and so two Gaussian eliminations are required per iteration, each with complexity $O((n-k)^3)$. A low-cost technique is to perform OSD over the parity check matrix; i.e., apply Gaussian elimination to the parity check matrix and transform the sub-block corresponding to the least reliable bits to an identity matrix. After this Gaussian elimination, the MRB can be obtained from the bit positions that do not correspond to the identity submatrix. Since OSD doesn't change bit reliabilities, ABP does not need to perform Gaussian elimination again in the same

Figure 1. Illustration of ABP decoding on a parity check matrix of an (N,K) linear block code obtained by using Gaussian elimination. The columns, with indices i_1 , i_2 , ..., i_{N-K} , correspond to the (N-K) least reliable bits, forming an identity matrix

iteration. This leads to reduced cost since only one Gaussian elimination is involved per iteration.

III. PERFORMANCE COMPARISON OF SHORT CODES

It has been shown that ABP-OSD can achieve near ML decoding performance [4]. We now employ it as a useful tool for evaluating various coding schemes.

A. Simulation based ML lower bound on FER

We assume an AWGN channel with BPSK modulation. The simulation based approach discussed in [12] is used to evaluate the ML performance for short codes. The basic principles are as follows. For a decoder, if its output is the same as the transmitted codeword, then decoding is successful. Otherwise, we compare the distances between the decoder output, the received sequence and the transmitted codeword. If the decoder output is closer to the received sequence (than the transmitted codeword), then even an ML decoder will make an error. Thus the ratio of the number of this class of error events to the total number of transmitted codewords provides a lower bound on frame error rate (FER) by ML decoding (referred to as the ML lower bound hereafter). The better the decoder performance, the tighter the simulation-based ML lower bound. Base on this technique, we have examined some well known short codes and made observations as summarized below.

B. High-rate short RS codes are as good as random binary linear codes

Fig.s 2 and 3 show the FER performance of RS(31,25), RS(63,55), respectively. The RBL codes of the same lengths and rates are also shown for reference. (The RBL codes are constructed randomly and we speculate that the performance based on random samples is close to the ensemble performance).

From Fig.s 2 and 3, it is seen that hard decision decoding of RS codes incurs a power efficiency loss of about 2-3dB in comparison to the ML lower bounds (generated using the

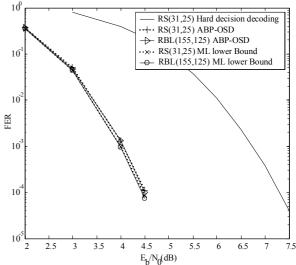


Figure 2. Frame error rate (FER) performance of RS(31,25) code and a (155,125) RBL code on an AWGN channel. The number of iterations for ABP is 20 and the order of OSD is 1.

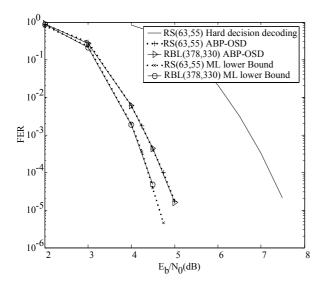


Figure 3. Frame error rate (FER) performance of RS(63,55) code and a (378,330) RBL code on an AWGN channel. The number of iterations for ABP is 20 and the order of OSD is 3.

technique outlined in III.A). This means that there is significant room for potential performance improvement for short RS codes if an efficient soft decoding algorithm is available. Another interesting observation 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.

C. Carefully designed LDPC codes perform close to random binary linear codes

For simplicity we consider CZ codes [8,9] that is a special case of LDPC codes. The reason for choosing CZ codes as the representative of LDPC codes is due to its simplicity. The dual-diagonal structure of CZ codes allows fast and low-cost encoder as well as decoder operations. Such structures has now been adopted in many applications, e.g., the LDPC codes specified in IEEE 802.16e standard (see Fig.4 for FER performance comparison of CZ codes and codes proposed for IEEE 802.16e under belief propagation decoding). In the following, we will show that carefully designed CZ codes can achieve performance close to RBL codes under ML decoding.

Denote the code length and information block length of a CZ code as N and K, respectively. Decompose the codeword c as $c = [p^T, d^T]$, where p and d contain the parity and information bits respectively and T denotes the matrix transposition operation. Accordingly, decompose the parity check matrix H (size: (N-K) by N) into $H = [H^p, H^d]$. Then,

$$(H^p, H^d) \begin{pmatrix} p \\ d \end{pmatrix} = 0$$
 (1)

Let M be a preset integer constrained by (i) M divides N-K and (ii) N-K divides KM. We construct H^P in the following block diagonal form with M non-zero blocks (each denoted by L) on its diagonal line as

$$H^{p} = \begin{pmatrix} L & 0 & 0 \\ 0 & L & \ddots & \\ & \ddots & \ddots & 0 \\ 0 & & 0 & L \end{pmatrix}$$
 (2)

where each L is of size $((N-K)/M)\times((N-K)/M)$ with the following dual diagonal structure,

$$\boldsymbol{L} = \begin{pmatrix} 1 & & 0 \\ 1 & 1 & \\ & \ddots & \ddots \\ 0 & & 1 & 1 \end{pmatrix} \tag{3}$$

We adopt the following rules to create \mathbf{H}^d . Partition \mathbf{H}^d and \mathbf{p} (both having N-K rows) into M equal sub-blocks as

$$\boldsymbol{H}^{d} = \begin{pmatrix} \boldsymbol{H}^{d1} \\ \vdots \\ \boldsymbol{H}^{dM} \end{pmatrix}$$
 (4a)

and

$$\boldsymbol{p} = \begin{pmatrix} \boldsymbol{p}^1 \\ \vdots \\ \boldsymbol{p}^M \end{pmatrix} \tag{4b}$$

Note that \mathbf{H}^{dm} , \mathbf{p}^m and \mathbf{L} have the same number, (N-K)/M, of rows. Due to the special form of the \mathbf{H}^p , the encoding process for a CZ code is much simpler than a general LDPC code. Based on (1) to (4), $\mathbf{p}^m = \{p^m(i)\}$ (m=1,2,...,M, i=1,2,...,(N-K)/M) can be easily calculated from $d=\{d_i\}$ as follows

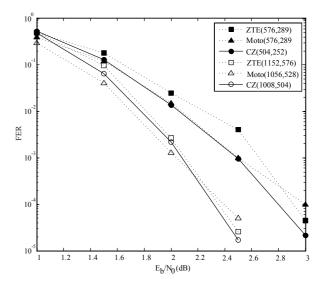


Figure 4. FER performance comparison of CZ codes with linear interleavers and two LDPC codes proposed in 802.16e under belief propagation decoding. The ZTE codes and Moto codes are proposed in [15] and [16], respectively.

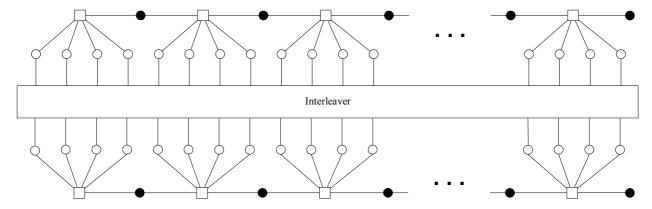


Figure 5. Factor graph of a 2-dimensional concatenated zigzag code, CZ(I,4,2). Open and filled circles represent information bits and parity check bits, respectively, and open squares represent parity check nodes. Note that the lower row of open circles is just an interleaved version of the upper row of open circles

$$p^{m}(1) = \sum_{j} h_{1j}^{dm} d_{j} \pmod{2}$$

and

$$p^{m}(i) = p^{m}(i-1) + \sum_{j} h_{ij}^{dm} d_{j} \pmod{2}, \tag{5}$$

We restrict each \mathbf{H}^{dm} to have exactly one 1 per column and J 1's per row, where J=KM/(N-K). More precisely, we construct \mathbf{H}^{d1} in a staircase form as follows.

$$\boldsymbol{H}^{d1} = \begin{bmatrix} 1 & \cdots & 1 & & & & 0 \\ & & 1 & \cdots & 1 & & & \\ & & & & \ddots & & \\ 0 & & & & & 1 & \cdots & 1 \\ & & & & & J & & \end{bmatrix}_{(N-K)/M \times K}$$

The other sub-matrices \mathbf{H}^{dm} 's are obtained by pseudo randomly permuting the columns of \mathbf{H}^{d1} . Thus, the positions of the 1's in $\{\mathbf{H}^{dm}, m=1,2,...,M\}$ can be determined by M interleavers. Similar to turbo codes, interleaver design plays an important role in the construction of CZ codes, especially for short to moderate block lengths. In the following, we adopt the jointly optimized linear interleavers considered in [10]. Let

$$(q^{(1)}, q^{(2)}, ..., q^{(m)}, ..., q^{(M)})$$
 (6)

be M integers. We call these integers as angular coefficients below. We construct M interleavers using the following equation:

$$\pi_i = iq^{(m)} \pmod{K}$$
 for $i = 0, 1, ..., K$ (7)

The position of the only non-zero entry in the *i*th column of \mathbf{H}^{dm} is then determined by π_i . Thus, the overall CZ code is completely specified by M angular coefficients defined in (6). We always choose $q^{(1)} = 1$ that gives \mathbf{H}^{d} . The other M-1 angular coefficients are selected from integers prime to K following the sum-distance criterion discussed in [10].

A CZ code can also be interpreted either as a parallel concatenation of several component codes or as a semi-

random LDPC code with a certain structure. For the first interpretation, the graphical representation of a component code was drawn using a "zigzag" graph in [8]. Hence, it was named a zigzag code. Each zigzag code can be defined by a block row in H, i.e., $[L, H^{dm}]$. Following the notations in [8], a CZ code is denoted by CZ(I, J, M), where I (= (N-N)M) is the number of segments (each segment forming a single parity check (SPC) code) contained in each zigzag code, J (=KM/(N-K)) is the information block length of each segment, and M is the number of component zigzag codes. Hence, a CZ(I, J, M) code is a length-I(J+M) (=N) rate-J/(J+M) (=K/N) block code constructed by a turbo-type parallel concatenation. For the second interpretation, the factor graph representation of a CZ(I,4,2) code is shown in Fig.5.

Incidentally, CZ codes are also closely related to repeat-accumulate (RA) codes [11]. The latter can be generated based on the partitioned parity check matrix in (1) using the following structures for the parity and information parts. The parity part is given by

$$\mathbf{H}^p = \mathbf{L} \tag{8}$$

where L has the dual diogonal structure defined in (3) with a proper size (a similar structure was discussed in [9].) The information part is obtained by restricting each column of H^d to have exactly M non-zero entries (i.e., 1's) and the positions of these non-zero entries are randomly generated. Here M is the repetition index in an RA code and the dual-diagonal structure in (8) provides the accumulation nature of the code. Clearly, the RA code defined above bears close similarity to the CZ code defined in (2)-(5). In general, the partition of H^d as shown in (4) leads to better error-floor performance for CZ codes. This can also be seen from the weight distribution analysis outlined below.

The overall parity weight of a CZ code is the sum of the parity weights of the M component codes. These component parity weights can be approximately regarded as independent random variables if the M interleavers are random. (We will assume that this assertion approximately holds for linear interleavers defined in (7).) Then, according to the central limit theorem, when M is large, the distribution of the overall parity

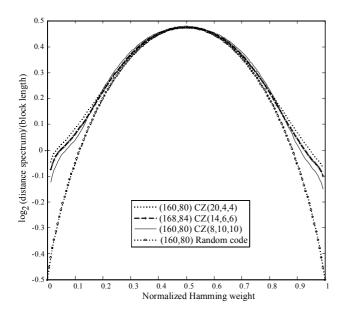


Figure 6. Average ensemble distance spectra of concatenated zigzag codes and random codes.

weight approaches Gaussian, implying that a CZ code with a large M has a similar weight distribution as an RBL code. This is illustrated in Fig.6. With increased M, the average ensemble distance spectra of CZ codes (computed using the algorithm outlined in [8]) approach to that of an RBL code.

Fig. 7 shows the ML lower bound for the FER performance of several rate-1/2 short concatenated zigzag (CZ) codes with different number of component codes, together with that for a length-160 rate-1/2 RBL code. The gap between the CZ (8,10,10) code and the (160,80) RBL code performance is only a fraction of a dB, which further verifies the observation in Fig.6 that the near ML decoding performance of CZ codes improves when K increases.

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

Both the belief propagation decoding performance and ABP-OSD performance 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.8. From Fig.8, it is seen that the gap between the belief propagation decoding performance (with low computational complexity) and the ABP-OSD performance (with much higher computational complexity) increases as the number of component zigzag codes, M, increases. The gap is about 2dB for the CZ(8,10,10) code at a FER of 10^{-3} . Although CZ(8,10,10) exhibits a better FER performance than CZ(14,6,6) when a high complexity ABP-OSD decoder is employed, the opposite observation can be made when a low-complexity belief propagation decoder is used.

In the above discussions, we have compared the performance of various short block linear codes. To be more comprehensive, we also provide a comparison between the performance of CZ codes and a convolutional code. Fig. 9

shows the belief propagation decoding performance of two rate-1/2 CZ codes and the Viterbi decoding performance of a rate-1/2 convolutional code with a constraint length of 9 used in the IS-95 CDMA system forward link. The numbers of information bits and parity bits of the convolutional code are 416 and 200 respectively, so its rate is actually slightly lower than $\frac{1}{2}$ (≈ 0.48), which is a result of the extra 16 bits used for termination. We can see from Fig.9 that the convolutional code performs slightly better than the CZ(14,6,6) code (with 84 information bits) under belief propagation decoding. However, Fig. 7 shows that the ABP-OSD performance of the CZ(14,6,6) code is better than the ML performance of the convolutional code. Note that for simplicity, the length of the convolutional code is fixed at 200 information bits and its performance with 84 information bits is similar (except the rate loss due to the termination bits is higher).

However, the BP performance of the CZ(34,6,6) code (with a longer length of 204 information bits) is better than that of the convolutional code, as can be observed in Fig.9.

IV. CONCLUSIONS

We have presented an overview on the performance of available short FEC coding schemes for wireless communication systems based on the recent developments in soft decision decoding techniques. We have shown that at short coding lengths, good RS codes and carefully designed LDPC codes can perform close to ideal RBL codes if high decoding complexity is allowed. However, if decoding complexity is an issue, then there is still a considerable gap between the performance of practical codes and the ideal RBL codes. It is still a challenging task to close this gap which can bring about

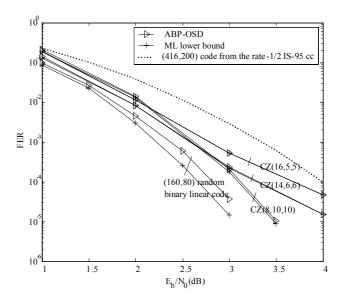


Figure 7. Frame error rate (FER) performance of CZ codes with different numbers of component codes and a (160,80) random binary linear code. The angular coeffi-cient vectors for CZ(16,5,5), CZ(14,6,6), and CZ(8,10,10) are (1, 30, 24, 56, 21), (1, 23, 52, 22, 74, 34), and (1,11, 37, 49,66,70,56, 48, 43, 4), respectively. The number of iterations for ABP is 20 and the order of OSD is 3.

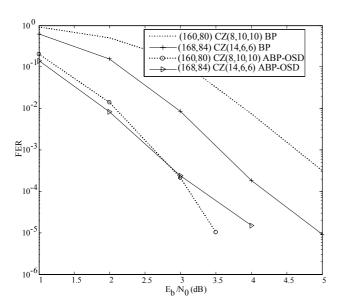


Figure 8. Frame error rate (FER) performance of CZ codes (which have been used in Fig.7) under BP decoding and near ML decoding on an AWGN channel. The number of iterations for ABP is 20 and the order of OSD is 3.

valuable coding gain for future wireless systems.

An interesting observation can be made from Fig. 8 that opposite conclusions can be made for the performance comparison of two codes when different decoding methods are used. This suggests that code design should carefully take into consideration the potential decoding capability. The decoder structure can be improved even after a standard on an encoder structure is finalized. With the ever growing processing power, the performance offered by the ABP-OSD algorithm as shown in Fig.7 may become practical in the future. It is thus worthwhile to prepare for such improvement when we select suitable coding schemes for future wireless communication systems.

ACKNOWLEDGMENT

The first author is grateful for the valuable help received from Keying Wu and Jing Jiang.

REFERENCES

- C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," in *Proc. IEEE Int. Conf. Communications*, Geneva, Switzerland, pp.1064-1070, May 1993.
- [2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *IEE 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. on Inform. 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. Inform. Theory*, vol. 41, pp. 1379-1396, Sept. 1995.

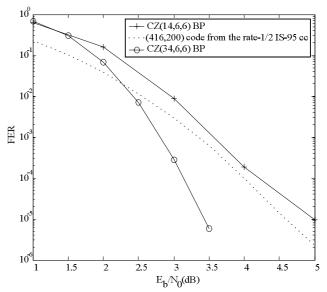


Figure 9. Frame error rate (FER) performance of CZ codes under BP decoding, and a (416,200) block code derived from the rate-1/2 IS-95 convolutional code (cc) under the Viterbi decoding on an AWGN channel. CZ(14,6,6) has been used in Fig.s 7 and 8, and CZ(34,6,6) is specified by the angular coefficient vector (1,97,35,143,167,113).

- [6] M. Fossorier, "Reliability-based soft-decision decoding with iterative information set reduction," *IEEE Trans. Inform. Theory*, vol. 48, pp. 3101–3106, Dec 2002.
- [7] A. Valembois and M. Fossorier, "Box and match techniques applied to soft-decision decoding," *IEEE Trans. Inform. Theory*, vol.50, pp.796-810, May 2004.
- [8] L. Ping, X. Huang, and N. Phamdo, "Zigzag codes and concatenated zigzag codes," *IEEE Trans. Inform. Theory*, vol.47, pp.800-807, Feb.2001.
- [9] L. Ping; W. K. Leung, and N. Phamdo, "Low density parity check codes with semi-random parity check matrix," *IEE Electronics Lett.*, vol.35, pp.38-39, Jan. 1999.
- [10] C. He, M. Lentmaier, D. J. Costello, Jr., and K. Sh. Zigangirov, "Joint permutor analysis and design for multiple turbo codes," *IEEE Trans. Inform. Theory*, vol.52, pp.4068-4083, Sept. 2006.
- [11] 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.
- [12] R. Lucas, M. Bossert, M. Breitbach, "On iterative soft-decision decoding of linear binary block codes and product codes," *IEEE Journal Selected Areas in Communications*, vol.16, pp. 276-296, Feb. 1998.
- [13] IEEE P802.16e/D8, Draft IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Sys-tems, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, May, 2005.
- [14] C. B. Schlegel and L. C. Perez, Trellis and Turbo Coding, IEEE Press and Wiley-Interscience, 2004, p.322.
- [15] R. Xu, L.Q. Yuan, "High girth LPDC coding for OFDMA PHY," IEEE C802 16e-04/423
- [16] B. Classon, Y.F. Blankenship, "High girth LPDC coding for OFDMA PHY," IEEE C80216e-04/423.
- [17] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm", *IEEE Trans. Inform. Theory*, vol.47, pp.498-519, Feb. 2001