IEICE TRANS. COMMUN., VOL.E90–B, NO.3 MARCH 2007

INVITED SURVEY PAPER

LDPC Codes in Communications and Broadcasting

Tomoaki OHTSUKI[†a)], ***Member***

SUMMARY Low-density parity-check (LDPC) codes are one of the most powerful error correcting codes and are attracting much attention these days. LDPC codes are promising for communications and broadcasting as well where the use of error correcting codes are essential. LDPC codes have been standardized in some communication standards, such as, IEEE802.16e, DVB-S2, IEEE802.3an (10BASE-T), and so on. The performance of LDPC codes largely depend on their code structure and decoding algorithm. In this paper, we present the basics of LDPC codes and their decoding algorithms. We also present some LDPC codes that have good performance and are receiving much attention particularly in communication systems. We also overview some standardized LDPC codes, the LDPC codes standardized in DVB-S2 and the IEEE802.16e standard LDPC codes. Moreover, we present some research on LDPC coded MIMO systems and HARQ using LDPC codes.
key words: *LDPC codes, BP algorithms, LLR, cooperation*

1. Introduction

Communication and broadcasting systems, particularly wireless systems, often incur channel impairments. Thus, the use of error correcting codes is essential. Among error correcting codes, low density parity check (LDPC) codes, proposed by Gallager [1] in the 1960's, and later rediscovered by MacKay and Neal [2], [3], appear as a class of codes that can yield very good performance. An LDPC code is a linear block code defined by a sparse parity-check matrix $\mathbf{H}$ that contains mostly zeros and only a small number of ones, that is, it has a low-density of ones. The excellent performance of LDPC codes can be obtained by being used with belief propagation (BP) algorithm that updates likelihood of each bit with help of other bits as extrinsic information. In general the more the extrinsic information is obtained, the better the performance becomes. The performance of LDPC codes largely depends on their code structure and decoding algorithm. Also there are some constraints on error correcting codes and their decoding, such as complexity, latency, memory, size, rate compatibility, and so on, particularly in communication systems. Therefore, various code construction methods of LDPC codes and their decoding algorithms have been proposed.

It is shown in [4] that appropriately designed LDPC codes have better performance than Turbo codes adopted in the 3rd generation (3G) mobile communication systems. Owing to their excellent performance, LDPC codes are adopted in several communication and broadcasting standards, such as the IEEE802.16e, DVB-S2, IEEE802.3an (10BASE-T), and so on. The LDPC codes in these standards are designed under the above constraints. In addition to the above standards, LDPC codes are expected to be applied to various communication systems, such as multiple-input multiple-output (MIMO) systems. MIMO systems are attracting tremendous attention, because they can yield a significant increase of capacity by exploiting multipath propagation compared to single-input single-output (SISO) systems [5]–[7]. Most practical MIMO systems employ error correcting codes and exploit coding gain as well as diversity gain, which results in a large capacity gain. In LDPC coded MIMO systems detection and decoding cooperate to update log likelihood ratios (LLRs) between them. Owing to the nature of the BP decoding algorithm, LDPC code is a good choice to exploit diversity gain in both spatial and time domains.

In addition to forward error correction (FEC), automatic repeat request (ARQ) is an effective technique for error control. In particular when the feedback channel is available, ARQ is a good choice. The technique combining FEC and ARQ is referred to as Hybrid ARQ (HARQ) and is known to increase the throughput of the system. There are many kinds of codes combined with HARQ. LDPC codes have also been applied to HARQ. For example, in type II HARQ, that is, an incremental redundancy (IR) ARQ scheme, error correcting codes are required to provide good error correction capability over wide range of code rates. Therefore, it is an interesting and important topic how to design LDPC codes for HARQ and also the system itself, considering the nature of LDPC codes.

In this paper, we present the basics of LDPC codes and their decoding algorithms. We also present some LDPC codes that have good performance and are receiving much attention particularly in communication systems because of their characteristics. We also explain some standardized LDPC codes, the LDPC codes standardized in DVB-S2 and the IEEE802.16e standard LDPC codes. Moreover, we present some research on LDPC coded MIMO systems and HARQ using LDPC codes.

The paper is organized as follows. Section 2 presents the basics of LDPC codes. Section 3 presents some iterative decoding algorithms, BP algorithm and its variants. Section 4 explains some LDPC codes receiving much attention particularly in communication systems in terms of both performance and complexity. Sections 5 and 6 present

Manuscript received November 2, 2006.
[†]The author is with the Faculty of Science and Technology, Keio University, Yokohama-shi, 223-8522 Japan.
a) E-mail: ohtsuki@ics.keio.ac.jp
DOI: 10.1093/ietcom/e90–b.3.440

the LDPC codes standardized in DVB-S2 and the IEEE 802.16e. Sections 7 and 8 present some important researches on LDPC coded MIMO systems and HARQ using LDPC codes. Finally, conclusions are drawn in Sect. 9.

2. LDPC Codes

In this paper, we shall consider only binary LDPC codes just for simplicity, although LDPC codes can be generalized to non-binary alphabets [8], [9]. An LDPC code is a linear block code defined by a sparse parity-check matrix **H** that contains mostly zeros and only a small number of ones, that is, it has a low-density of ones. We assume **H** is full rank, unless specified. If the parity-check matrix **H** has N columns and M rows, the codewords consist of sequences **x** of N bits that satisfy a set of M parity checks defined by the parity-check equation $\mathbf{H}\mathbf{x}^T = \mathbf{0}$. The number of message bits is $K = N - M$, and the rate of the code is $R = K/N$. The parity-check matrix **H** is so named because it performs $M = N - K$ separate parity checks on a received codeword. LDPC codes can be classified broadly into two types, regular and irregular LDPC codes. Regular LDPC codes are those for which the parity-check matrix has a uniform column weight w_c as well as a uniform row weight w_r, where the column (row) weight refers to the number of "1s" in a column (row). In regular LDPC codes, the following relationships hold: $w_r = w_c N/M$, $w_c \ll M$, and $R = K/N = 1 - w_c/w_r$. In irregular LDPC codes the number of "1s" in each column or row is not constant.

An (N, K) LDPC code has the block length N and the information length K. A parity-check matrix **H** of a (12, 6) regular LDPC code with the column weight $w_c = 3$ and the row weight $w_r = w_c N/M = 6$ is shown below.

$$\mathbf{H} = \begin{bmatrix} 1&1&1&0&0&1&1&0&0&0&1&0 \\ 1&1&1&1&1&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&1&1&0&1&1&1 \\ 1&0&0&1&0&0&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1&1&0&0&0 \\ 0&0&1&0&1&1&0&0&1&1&1&0 \end{bmatrix} \tag{1}$$

An LDPC code can be represented by a Tanner Graph [10]. The Tanner Graph corresponding to an (N, K) LDPC code consists of N bit nodes, $M = N - K$ check nodes, and a certain number of edges. Each bit node represents a bit of the codeword. Each check node represents a parity check of the code. An edge exists between a bit node and a check node if and only if there is a "1" in the corresponding entry in the parity-check matrix. The Tanner graph thus represents the constraint on codewords, that is, the code itself. The Tanner graph corresponding to the parity-check matrix in Eq. (1) is shown in Fig. 1. In this Tanner graph each bit node has three edge connections and each check node has six edge connections, which accordance with the fact that $w_c = 3$ and $w_r = 6$.

In irregular LDPC codes bit nodes and check nodes are usually specified by degree distribution polynomials, denoted by $\lambda(x)$ and $\rho(x)$, respectively.

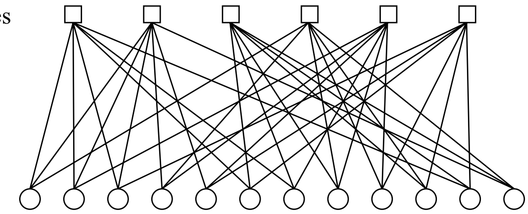

Fig. 1 A Tanner graph: Parity-check matrix of (12, 6) LDPC code with the column weight $w_c = 3$ and the row weight $w_r = 6$.

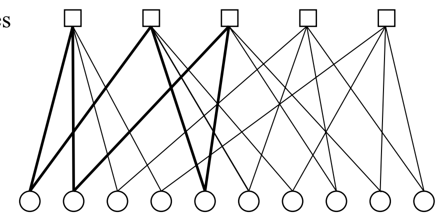

Fig. 2 A Tanner graph: Parity-check matrix of (10, 5) LDPC code with the column weight $w_c = 2$, the row weight $w_r = 4$, and the girth of 6.

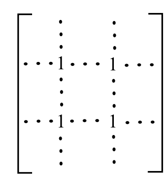

Fig. 3 A parity-check matrix having 4 cycle.

$$\lambda(x) = \sum_{d=1}^{d_v} \lambda_d x^{d-1} \tag{2}$$

$$\rho(x) = \sum_{d=1}^{d_c} \rho_d x^{d-1} \tag{3}$$

where λ_d and ρ_d denote the fractions of all edges connected to degree-d bit nodes and degree-d check nodes, respectively, and d_v and d_c denote the maximum bit node and check node degree, respectively. For instance, the degree distribution polynomials for the regular LDPC code given by Eq. (1) are $\lambda(x) = x^2$ and $\rho(x) = x^5$.

In a Tanner graph a cycle or sometimes referred to as a loop of length v is a path comprising v edges that loops back to itself. The minimum length of the cycle is referred to as the girth. The girth of the Tanner graph in Fig. 2 is six. A minimum value of girth of a bipartite graph like a Tanner graph is clearly four. In a parity-check matrix **H** having a length-4 cycle four 1's lie on the corners of a submatrix of **H** as shown in Fig. 3. Superior performance of LDPC codes can be generally obtained by combining with BP decoding algorithm explained later where likelihood of each bit is propagated along edges and used as extrinsic information for other bits. In general the more the extrinsic information is obtained, the better the performance becomes. Thus, the performance of LDPC codes generally depend on the cycle and the girth largely. A small value of girth means that the information of the bit loops back to itself soon and only a small amount of extrinsic information can be exploited. Thus, the likelihood of the bit cannot be improved a lot. Therefore, a girth can be a design parameter of LDPC codes and a lot of papers try to construct LDPC codes with a large girth [11]–[17]. We have to note that with a cycle-free Tanner graph, the BP algorithm terminates in a finite number of steps and yields optimal decoding in terms of symbol error probability [18], [19]. However, cycle-free Tanner graphs have poor bit error rate (BER) performance owing to their small minimum distance: their minimum distance is two at code rates $R > 1/2$ [20]. The reason why the code performance is affected by short cycles is given in [11].

3. Iterative Decoding Algorithms

In this section, we assume BPSK modulation that maps a codeword $\mathbf{c} = (c_1, c_2, \cdots, c_N)$, with $c_n = 0, 1$, into a transmitted sequence $\mathbf{x} = (x_1, x_2, \cdots, x_N)$, according to $x_n = 2c_n - 1$, for $n = 1, 2, \cdots, N$.

The objective of decoding algorithms is computing the a posteriori probability (APP) that a given bit in the transmitted codeword $\mathbf{c}$ equals 1 (or 0), given that the received codeword $\mathbf{y} = (y_1, y_2, \cdots, y_N)$: $\Pr(c_i = 1|\mathbf{x})$. For LDPC codes, the BP decoding algorithm, sometimes referred to as the sum-product algorithm (SPA) or the message passing algorithm based on its applications, is used to calculate the APP $\Pr(c_i = 1|\mathbf{x})$ or APP ratio (likelihood ratio: LR) or log of LR (LLR).

$$l(c_i) = \frac{\Pr(c_i = 0|\mathbf{x})}{\Pr(c_i = 1|\mathbf{x})}$$

$$L(c_i) = \log\left(\frac{\Pr(c_i = 0|\mathbf{x})}{\Pr(c_i = 1|\mathbf{x})}\right)$$

The BP algorithm calculates them iteratively based on the code's Tanner graph. At each iteration of BP decoding, each check node receives messages from all the bit nodes connected to it, and after processing, it sends messages back to these bit nodes. Note that in this process, the information other than it already has is sent back; only extrinsic information is passed. Then a similar procedure is applied to each bit node. We assume all the messages passing between bit and check nodes are in the form of LLR's. Note that they can be in the form of probability or likelihood ratio. However, they include a lot of multiplications of probabilities, which results in high cost and numerically unstable calculation. Thus, LLR is usually preferred.

Moreover, we define the following notations associated with a given iteration:

- F_n: The LLR of the bit n derived from the received value y_n. In an additive white Gaussian nose (AWGN) channel with zero mean and power spectral density $N_0/2$ W/Hz, we initially set $F_n = \frac{4}{N_0} y_n$.
- L^i_{mn}: The LLR of the bit n sent from the check node m to the bit node n in the ith iteration. It is obtained from the information $z^{i-1}_{mn'} : n' \in \{\mathcal{N}(m)\backslash n\}$, where the notation z^{i-1}_{mn} will be introduced next and $\mathcal{N}(m)\backslash n$ is the set of all the bit nodes connected to the check node m with the bit node n excluded.
- z^i_{mn}: The LLR of the bit n sent from the bit node n to the check node m in the ith iteration. It is obtained from the a priori information F_n and the information $\{L_{m'n} : m' \in \mathcal{M}(n)\backslash m\}$, where $\mathcal{M}(n)\backslash m$ is the set of all the check nodes connected to the bit node n with the check node m excluded.
- z^i_n: The a posteriori LLR of the bit n computed in the ith iteration. It is obtained from the a priori information F_n and the information $\{L_{m_j n} : m_j \in \mathcal{M}(n)\}$.

3.1 LLR BP Algorithm

The LLR BP Algorithm [21] can be described as follows.

- Initialization: Set $i = 1$, maximum number of iterations to I_{MAX}. For each n and $m \in \mathcal{M}(n)$, set $z^0_{mn} = F_n$.
- Iterative Decoding:

Step 1: Bit Node to Check Node

For $1 \le n \le N$ and each $m \in \mathcal{M}(n)$, update L^i_{mn} by

$$T^i_{mn} = \prod_{n' \in \mathcal{N}(m)\backslash n} \tanh\left(\frac{z^{i-1}_{mn'}}{2}\right) \tag{4}$$

$$L^i_{mn} = \ln \frac{1 + T^i_{mn}}{1 - T^i_{mn}} \tag{5}$$

Step 2: Check Node to Bit Node

For $1 \le n \le N$ and each $m \in \mathcal{M}(n)$, update z^i_{mn} by

$$z^i_{mn} = F_n + \sum_{m' \in \mathcal{M}(n)\backslash m} L^i_{m'n} \tag{6}$$

Also, for each n, update z^i_n for hard decision by

$$z^i_n = F_n + \sum_{m \in \mathcal{M}(n)} L^i_{mn} \tag{7}$$

Step3: Check Stop Criterion

First, create $\hat{\mathbf{x}}^i = [\hat{x}^i_n]$ such that $\hat{x}^i_n = 1$ if $z^i_n > 0$ and $\hat{x}^i_n = 0$ if $z^i_n < 0$. Next, check $\hat{\mathbf{x}}^i = [\hat{x}^i_n]$.

1. If $\mathbf{H}\hat{\mathbf{x}}^{i^T} = \mathbf{0}$, the decoding algorithm halts, and $\hat{\mathbf{x}}^i$ is considered as a valid decoding result.
2. Otherwise, the algorithm repeats from Step 1.
3. If the algorithm reaches the maximum number of iterations, the algorithm is terminated.

3.2 UMP BP-Based Decoding Algorithm

In LLR BP algorithm the check node calculation is dominant in complexity. That is, the calculations of T^i_{mn} and L^i_{mn} in (4) and (5) require a lot of computations. The uniformly most powerful (UMP) BP-based algorithm is proposed to reduce the complexity of LLR BP algorithm by simplifying the check node calculation [21], [22]. The UMP BP-based algorithm is described below.

- Initialization: Set $i = 1$, maximum number of iterations to I_{MAX}. For each n and $m \in \mathcal{M}(n)$, set $z^0_{mn} = y_n$.
- Iterative Decoding:
  For each iteration, process the following three steps.

Step 1: Bit Node to Check Node
For each m, n,

$$\sigma^i_{mn} = \begin{cases} 1, & \text{if } z^i_{mn} > 0 \\ 0, & \text{if } z^i_{mn} \leq 0 \end{cases} \tag{8}$$

For each m,

$$\sigma^i_m = \sum_{n \in \mathcal{N}(m)} \sigma^i_{mn} \mod 2 \tag{9}$$

For each m, n,

$$L^i_{mn} = (-1)^{\overline{\sigma^i_m \oplus \sigma^i_{mn}}} \min_{n' \in \mathcal{N}(m) \backslash n} |z^i_{mn'}| \tag{10}$$

where $\sigma^i_m \oplus \sigma^i_{mn}$ represents the modulo-2 sum of the hard decisions of all the bits and $\overline{\sigma^i_m \oplus \sigma^i_{mn}}$ denote the binary complement of $\sigma^i_m \oplus \sigma^i_{mn}$.

Step 2: Check Node to Bit Node
For each n and $m \in \mathcal{M}(n)$,

$$z^i_{mn} = y_n + \sum_{m' \in \mathcal{M}(n) \backslash m} L^i_{m'n} \tag{11}$$

For each n

$$z^i_n = y_n + \sum_{m \in \mathcal{M}(n)} L^i_{mn} \tag{12}$$

Step 3: Check Stop Criterion
Same as Step 3 of the LLR BP algorithm.

3.3 Normalized and Offset BP-Based Algorithms

The UMP BP-based algorithm has worse performance than that of the LLR BP algorithm [21], [22]. This is because the calculation of L_{mn} is approximated in the UMP BP-based algorithm. The Normalized BP-based algorithm [21], [22] can improve the performance of the UMP BP-based algorithm by normalizing L_{mn} in the UMP BP-based algorithm with a little bit more computations.

For a given pair of m and n, denote L_1 and L_2 as the value L_{mn} computed by the BP and the UMP BP-based algorithms, respectively. It can be shown that the following two facts hold [21].

1. $\text{sgn}(L_1) = \text{sgn}(L_2)$
2. $|L_2| > |L_1|$

With these two facts, the UMP BP-based algorithm can be improved by dividing L_2 by a scaling factor α greater than 1 to get a much better approximation of L_1. We can determine α by forcing the mean of the normalized magnitude $|L_2|/\alpha$ to equal the mean of the magnitude $|L_1|$, or

$$\alpha = \frac{E(|L_2|)}{E(|L_1|)}. \tag{13}$$

Using α, the check node processing is improved as follows.

$$L^i_{mn} \leftarrow L^i_{mn}/\alpha \tag{14}$$

In the offset BP-based algorithm [23], the check node processing can be improved by offsetting L_{mn} with the offset value β.

$$L^i_{mn} \leftarrow \text{sgn}(L^i_{mn}) \max(L^i_{mn} - \beta, 0). \tag{15}$$

As shown in Eq. (15), the offset BP-based decoding differs from the normalization scheme in that LLR messages smaller in magnitude than β are set to zero to remove their contribution in the next symbol-node-update step.

For the first iteration, the scaling factor α, β on an AWGN channel can either be determined based on Monte Carlo simulations, or obtained theoretically with the formulas derived in [21]. In the normalized BP-based algorithm and the offset BP-based algorithm, scaling factors are not so sensitive to the iteration number and SNR values, though they can be different on an AWGN channel and fading channels. Therefore, one scaling factor can be used for all the iterations and all the SNR values in each decoding algorithm. In [24] normalization factor is derived theoretically on fast Rayleigh fading channel. In [25] LDPC codes are optimized and scaling factors and thresholds are derived by density evolution (DE) [26], [27] for three BP-based decoding algorithms on fast Rayleigh fading channel: the UMP BP-based algorithm, the normalized BP-based algorithm, and the offset BP-based algorithm.

Since the simulation shows the performance remains very good even if we keep the scaling factor of the first iteration for all the subsequent iterations, we choose not to determine the scaling factor after the first iteration. Therefore, we choose one scaling factor for all the iterations and all the SNR values, so that the normalized an offset BP-based algorithms become independent of the SNR value.

Figure 4 shows the BER vs. E_b/N_0 for some decoding algorithms on fast fading channels where (8000, 4000) LDPC code is used. "iter" represents the maximum number of iterations. Although the BER of the UMP BP-based decoding algorithm is degraded compared to that of the BP algorithm, the normalized and offset BP-based algorithms reduce the degradation.

3.4 Shuffled BP Algorithm

As written above, at the ith iteration in the BP algorithm, first all the values of the check-to-bit messages are updated by using the values of the bit-to-check messages obtained at

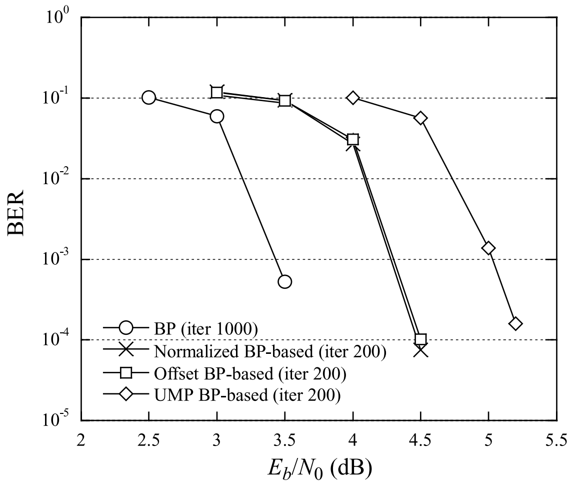

Fig. 4 BER vs. E_b/N_0 for some decoding algorithms on fast fading channels: (8000, 4000) LDPC code. "iter" represents the maximum number of iterations.

the $(i-1)$th iteration. Then all the values of the bit-to-check messages are updated by using the values of the check-to-bit messages newly obtained at the ith iteration. Shuffled BP decoding [28], [29] exploits the fact that for both the check-to-bit messages and bit-to-check messages, the more independent information is used to update the messages, the more reliable they become. As written previously, the design criteria of LDPC codes exploits the same fact: in general the girth should be enlarged. The shuffled BP algorithm is a bit-based serial decoding. In the shuffled BP algorithm the updating process is different from that in the BP algorithm. Other processes, such as, the initialization, stopping criterion test, and output steps are the same as those in the BP algorithm. Equation (4) on the bit-to-check process is modified as follows.

$$T^i_{mn} = \prod_{\substack{n' \in \mathcal{N}(m)\backslash n \\ n'<n}} \tanh\left(\frac{z^i_{mn'}}{2}\right) \prod_{\substack{n' \in \mathcal{N}(m)\backslash n \\ n'>n}} \tanh\left(\frac{z^{i-1}_{mn'}}{2}\right)$$

Note that the standard shuffled BP algorithm is totally serial so that the decoding delay becomes large, though the total number of iterations is reduced and the convergence becomes fast.

To decrease the decoding latency of the shuffled BP algorithm and exploit the parallel implementation of BP algorithm, the group shuffled BP algorithm is also proposed [28]. In the group shuffled BP algorithm the code length is divided into a number of groups. In each group the updating of messages is processed in parallel but the processing of groups remains sequential.

The other implementation of shuffled BP decoding referred to as replica shuffled BP algorithm is proposed in [30]. In the replica shuffled BP algorithm two shuffled BP decoding algorithms are processed simultaneously but in different orders. One updating is processed in ascending order (from bit 1) while the other updating is processed in descending order (from bit N). After each iteration, each subdecoder receives more reliable messages from and sends more reliable messages to another subdecoder. Therefore, the replica shuffled BP algorithm can make decoding convergence faster.

These shuffled BP algorithms make new scheduling on the same graph. Appropriate scheduling leads to fast convergence, low latency, reduced memory requirements, and so on. There are many papers on scheduling for decoding LDPC codes [31]–[33].

4. Some Design of LDPC Codes

The performance of LDPC codes largely depends on the code structure, that is, the code construction, as written above. A large number of design techniques are proposed under different design criteria: Near-capacity performance, efficient encoding and decoding, low error floors, reduced memory requirement, and so on. In wireless communications, efficient encoding and decoding is also an important characteristic. In this section we introduce some of the prominent ones.

4.1 Gallager Codes

First we briefly review Gallager codes [1]. The parity-check matrix $\mathbf{H}$ of an (N, K) Gallager code with column weight w_c and row weight w_r consists of w_c submatrices $\mathbf{H}_i$, $i = 1, 2, \cdots, w_c$, each containing a single 1 in each column and w_r 1's in each row. The first submatrix $\mathbf{H}_1$ contains w_r 1's of its ith row in columns $(i-1)w_r + 1$ to iw_r. That is, each row is obtained by cyclic shifting of the immediately preceding row by w_r positions to the right. The other submatrices $\mathbf{H}_i$ are pseudo-randomly permutated versions of the columns of $\mathbf{H}_1$. The parity-check matrix of a Gallager code is expressed as

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_{w_c} \end{bmatrix}. \qquad (16)$$

4.2 Quasi-Cyclic (QC) LDPC Codes

QC-LDPC codes have an advantage of encoding over other types of LDPC codes as well as other QC codes. They can be simply encoded using feedback-shift registers with complexity linearly proportional to the number of parity bits for serial encoding, and to the code length for parallel encoding [34], [35]. They also have advantages in implementation owing to their cyclic symmetry. QC-LDPC codes are characterized by the parity-check matrix that consists of small square blocks that are a zero matrix or circulants [14], [16], [36]. A circulant is a square matrix in which each row is the cyclic shift (right cyclic shift) of the row above it and the first row is the cyclic shift of the last row. Each column of a circulant is the downward cyclic shift of the column on its left and the first column is the cyclic shift of the last column. Thus, a circulant is fully characterized by its first row or column, which is referred to as the generator of the circulant. For QC-LDPC codes, an $L \times L$ circulant $\mathbf{P}$ over GF(2) is generally made to be full rank and its elements are expressed as

$$P_{i,j} = \begin{cases} 1, & \text{if } i+1 \equiv j \mod L \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

Note that $\mathbf{P}^i$ is the circulant permutation matrix that shifts the identity matrix $\mathbf{I}$ to the right by i times for any integer $i, 0 \leq i \leq L$. Let denote the $L \times L$ zero matrix by $\mathbf{P}^\infty$ for simple notation. For instance, $\mathbf{P}^1 = \mathbf{P} =$ is given by

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & & 0 \end{bmatrix}. \tag{18}$$

Let $\mathbf{H}_{qc}$ be the $mL \times nL$ matrix defined by

$$\mathbf{H}_{qc} = \begin{bmatrix} \mathbf{P}^{\alpha_{11}} & \mathbf{P}^{\alpha_{12}} & \cdots & \mathbf{P}^{\alpha_{1(n-1)}} & \mathbf{P}^{\alpha_{1n}} \\ \mathbf{P}^{\alpha_{21}} & \mathbf{P}^{\alpha_{22}} & \cdots & \mathbf{P}^{\alpha_{2(n-1)}} & \mathbf{P}^{\alpha_{2n}} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \mathbf{P}^{\alpha_{m1}} & \mathbf{P}^{\alpha_{m2}} & \cdots & \mathbf{P}^{\alpha_{m(n-1)}} & \mathbf{P}^{\alpha_{mn}} \end{bmatrix} \tag{19}$$

where $\alpha_{ij} \in \{0, 1, \ldots, L-1, \infty\}$. The QC-LDPC code C with $\mathbf{H}_{qc}$ is quasi-cyclic in the sense that $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1}) \in C$ implies that $\hat{T}^i\mathbf{c} \in C$ for all $i, 0 \leq i \leq L-1$, where

$$\hat{T}^i\mathbf{c} \equiv (T^i\mathbf{c}_0, T^i\mathbf{c}_1, \ldots, T^i\mathbf{c}_{n-1}) \tag{20}$$

$$T^i\mathbf{c}_l \equiv (c_{l,i}, c_{l,i\oplus 1}, \ldots, c_{l,i\oplus L-1}) \tag{21}$$

for $\mathbf{c}_l = (c_{l,0}, c_{l,1}, \ldots, c_{l,L-1})$ where $\oplus$ denotes the modulo-L addition. In QC-LDPC codes, if the locations of 1's in the first row of the ith row block $\mathbf{H}_i \equiv [\mathbf{P}^{\alpha_{i1}} \cdots \mathbf{P}^{\alpha_{in}}]$ is given, the locations of other 1's in $\mathbf{H}_i$ are uniquely determined. Thus, the required memory for storing the parity-check matrix of the QC-LDPC code can be reduced by a factor $1/L$, compared to randomly constructed LDPC codes.

The QC-LDPC code may be regular or irregular depending on the choice of $\alpha_{i,j}$'s of $\mathbf{H}_{qc}$. When $\mathbf{H}_{qc}$ does not contain zero submatrix, it is a regular LDPC code with column weight m and row weight n. Otherwise, it is an irregular LDPC code.

4.3 Array LDPC Codes

Array LDPC codes are structured LDPC codes based on "array codes" that are two-dimensional codes proposed for detecting and correcting burst errors [36]–[39]. The array code can be seen as a regular QC-LDPC code. The array LDPC code is constructed by submatrices constructed by cyclic shift of the $L \times L$ identity matrix. The parity check matrix of the array LDPC code is defined for a prime q and a positive integer $j \leq q$ by

$$\mathbf{H}_\mathrm{A} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} & \cdots & \mathbf{I} \\ \mathbf{I} & \mathbf{P}^1 & \cdots & \mathbf{P}^{j-1} & \cdots & \mathbf{P}^{k-1} \\ \mathbf{I} & \mathbf{P}^2 & \cdots & \mathbf{P}^{2(j-1)} & \cdots & \mathbf{P}^{2(k-1)} \\ \vdots & \vdots & & \vdots & & \vdots \\ \mathbf{I} & \mathbf{P}^{(j-1)} & \cdots & \mathbf{P}^{(j-1)(j-1)} & \cdots & \mathbf{P}^{(j-1)(k-1)} \end{bmatrix} \tag{22}$$

Thus, the array LDPC code is a QC-LDPC code with $L = q, n = q$, and $m = j$ where the column and row weights of the array LDPC code are j and q, respectively. Note that q has to be a prime to achieve good performance. It is shown that for $j \geq 3$, the girth of the Tanner graph is 6 [37], [38].

For efficient encoding of array LDPC codes, [36] proposed a modified array code with the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} & \cdots & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \mathbf{P} & \cdots & \mathbf{P}^{j-2} & \cdots & \mathbf{P}^{k-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{P}^{2(j-3)} & \cdots & \mathbf{P}^{2(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{P}^{(j-1)(k-j)} \end{bmatrix}$$

where k and j are two integers such that $j \leq k \leq q$ where q denotes a prime number. $\mathbf{I}$ is a $q \times q$ identity matrix, $\mathbf{0}$ the $q \times q$ null matrix, and $\mathbf{P}$ a $q \times q$ permutation matrix representing a single left- or right-cyclic shift. The modified array LDPC code is an irregular QC-LDPC code with $L = q, n = k, m = j$ whose $\mathbf{H}$ has zero submatrix. Owing to the upper triangular form of $\mathbf{H}$, it can be efficiently encoded, that is, linear encoding complexity with codeword length. As can be seen from the structure of $\mathbf{H}$, there are no cycle of length 4 in the corresponding Tanner graph. Thus, the modified array LDPC codes have very low error floors.

4.4 Irregular Repeat Accumulate (IRA) Codes

Irregular repeat accumulate (IRA) codes [40] are a generalization of the repeat accumulate (RA) codes in [41]. IRA codes are shown to have the same performance with reduced encoding complexity as the standard LDPC codes: IRA codes have a linear-time encoding algorithm and can be decoded in linear time using the BP algorithms. There are two versions of the IRA codes, the nonsystematic and the systematic versions. In [42] the systematic versions of IRA codes are referred to as LDPC codes with semi-random parity-check matrix. The Tanner graph for the IRA code is shown in Fig. 5. The bit nodes are classified into two subclasses, the information bit nodes and the parity bit nodes. The information bits that are repeated i times are represented by the bit nodes with degree i, and thus they participate in i parity-check equations. Each check node is connected to n_a information bit nodes and two parity bit nodes. The connections between check nodes and information bit nodes are determined randomly, while those between check nodes and parity bit nodes are arranged in a regular zig-zag pattern so that the encoding can be implemented with simple accumulator. In the following we present an overview of the systematic versions of IRA codes.

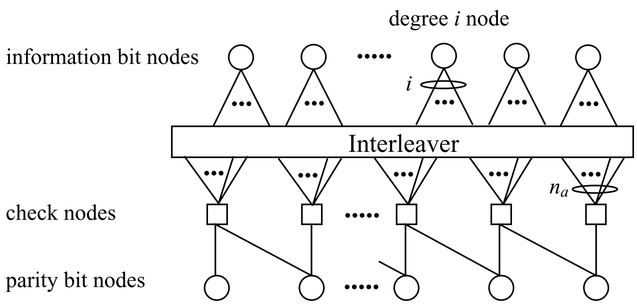

Fig. 5 A Tanner graph of IRA code.

The parity check matrix of the IRA code **H** consists of two parts. One part is deterministic, and the other part is generated randomly. Therefore, the parity check matrix **H** is described by

$$\mathbf{H}_{M\times N} = \left[\begin{array}{c|ccccc} & 1 & 0 & 0 & \cdots & 0 \\ & 1 & 1 & 0 & \cdots & 0 \\ \mathbf{A}_{M\times K} & 0 & 1 & 1 & \cdots & 0 \\ & \vdots & \vdots & \ddots & \ddots & \vdots \\ & 0 & \cdots & 0 & 1 & 1 \end{array} \right] \tag{23}$$

where $\mathbf{A}_{M\times K}$ is the random structure of the regular LDPC code. We denote the codeword by $\mathbf{c} = (u_1, \cdots, u_K, p_1, \cdots, p_M)$ where u_k is the information bit for $1 \leq k \leq K$ and p_m is the parity bit for $1 \leq m \leq M$. Then, using this parity check matrix, the fast encoding can be carried out by

$$p_1 = \sum_{k=1}^{K} u_k h_{1,k} \tag{24}$$

$$p_m = p_{m-1} + \sum_{k=1}^{K} u_k h_{m,k}, \quad 2 \leq m \leq M \tag{25}$$

where $h_{i,j}$ is the (i, j)th element of parity check matrix **H**, $1 \leq i \leq M$ and $1 \leq j \leq N$. Equations (24) and (25) show that the parity bits are determined from the information bits and the random part of parity check matrix without any need of computing the generator matrix.

In [43] IRA codes are optimized with DE for binary-input symmetric channels in the large block-length limit. In [25] IRA codes are optimized with DE for three BP-based algorithms, UMP BP based, normalized BP-based, and offset BP-based algorithms, on fast Rayleigh fading channels. In [44] IRA codes are optimized with Extrinsic information transfer (EXIT) charts for OFDM systems with partial channel state information. In [45] IRA codes are optimized with DE and EXIT charts for MIMO systems with iterative receivers.

5. LDPC Codes for DVB-S2

DVB-S2 is the second-generation specification for satellite broadband applications, such as TV and sound broadcasting, internet access, and professional services like TV contribution links and digital satellite news gathering [46], [47]. The first-generation specification, DVB-S, uses QPSK modulation and concatenated convolutional and Reed-Solomon (RS) codes. DVB-S2 employs LDPC codes that can realize 35% throughput increase compared to DVB-S.

In broadcasting like DVB-S2, ARQ is not a practical solution. Thus, generally, error correcting codes with large code length are used. The LDPC codes standardized in DVB-S2 are tens of thousands bits long. The LDPC codes are standardized with considering both performance and encoding complexity. In general encoding complexity of LDPC codes is high. In DVB-S2 a submatrix of the parity check matrix is of the form, $\mathbf{H}_{(N-K)\times N} = [\mathbf{A}_{(N-K)\times K}\mathbf{B}_{(N-K)\times(N-K)}]$ where **A** is a submatrix corresponding to information and **B** is a staircase lower triangular submatrix corresponding to parity as same as that of the IRA code in Eq. (23). Encoding procedure is also the same as that of the IRA codes, like Eqs. (24) and (25). Calculating each parity bit recursively, we can obtain the whole codeword **c**. Owing to this construction, we can encode information bits using the parity check matrix directly, that is, without using the generator matrix. Also, since the submatrix **A** is sparse, encoding has linear complexity with respect to the block length N. Thus, it is easy to encode. In addition it facilitates description of the code, which is particularly good for broadcasting applications where long codes are used. It is reported in [47] that performance loss due to the above construction compared to general one is smaller than 0.1 dB and negligible for the use of DVB-S2.

The parity check matrix specified in DVB-S2 is designed to have a small storage and to be specified easily. Thus, the following restriction is imposed on the submatrix **A**. The connectivity of the information bit nodes and the check nodes is defined as follows. First initialize all the parity information bits $(p_0, p_1, \cdots, p_{N-K-1})$. Second accumulate the first information bit i_0 at the parity bit addresses p_j specified in the DVB-S2 standard for each rate, $p_j = p_j \oplus i_0$. Third, for the next 359 information bits, $i_m, m = 1, 2, \cdots, 359$, accumulate i_m at the parity bit addresses p_j as follows.

$$p_j = p_j \oplus i_m, j = (x + q(m \bmod 360)) \bmod (N - K) \tag{26}$$

where x denotes the address of the parity bit accumulator corresponding to the first bit i_0, and q is a code rate dependent constant specified in the DVB-S2 standard for each rate. In a similar manner, for every group of 360 new information bits, the connectivity is defined.

In DVB-S2, to avoid error floors at low error rates, BCH codes are introduced as an outer codes, with the same block length as the LDPC code and an error correction capability of 8 to 12 bits, depending on the inner LDPC code.

The block length of concatenated code of outer BCH code and inner LDPC code is 64800 bits for applications not so critical for delays, 16200 bits otherwise. 10 different code rates and 4 different modulation schemes are available: (1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10) and QPSK, 8PSK, 16APSK and 32-APSK. Within a frame, FEC

Table 1 Degree distribution in terms of the number of nodes of the DVB-S2 LDPC codes.

	The Number of Nodes							
Code Rate\Degree	13	12	11	8	4	3	2	1
1/4		5400				10800	48599	1
1/3		7200				14400	43199	1
1/2				12960		19440	32399	1
3/5		12960				25920	25919	1
2/3	4320					38880	21599	1
3/4		5400				43200	16199	1
4/5			6480			45360	12959	1
5/6	5400					48600	10799	1
8/9					7200	50400	7199	1
9/10					6480	51840	6479	1

and modulation modes are constant but may change frame by frame. For 8PSK, 16APSK, and 32APSK modulation schemes, that is, other than QPSK modulation scheme, the output of the LDPC encoder shall be bit interleaved using a block interleaver. Data is serially written into the interleaver column-wise, and serially read-out row-wise. Degree distribution (represented by the number of nodes) of the LDPC codes are listed in Table 1. In [47], [48] the good DVB-S2 FEC performance in the AWGN channel is shown for various code rates and modulation schemes: Within 0.6–0.8 dB to Shannon limit.

6. IEEE 802.16e Standard LDPC Codes

The IEEE 802.16 standard specifies the air interface of fixed and mobile broadband wireless access (BWA) systems. The IEEE 802.16e is a standard for mobile access where orthogonal frequency division multiple access (OFDMA) is adopted. In OFDMA the subcarriers are divided among the users to form sub channels. For each subchannel, the coding and modulation are adapted independently to optimize the use of spectrum resources and enhance the indoor coverage by assigning a robust scheme. Scalable OFDMA (SOFDMA) is an enhanced version of OFDMA that scales the number of subcarriers in a channel with possible values of 128, 512, 1024, and 2048. WiBro (Wireless Broadband) is a Korean standard based on SOFDMA.

In the following we present a summary of the IEEEE 802.16e standard LDPC code in [49]. In the IEEE 802.16e standard LDPC codes are adopted to the OFDMA physical layer. The LDPC codes standardized in IEEE 802.16e is based on a set of one or more fundamental LDPC codes. Each fundamental code is a systematic linear block code. Using the methods described later, the fundamental codes can accommodate various code rates (1/2, 2/3A, 2/3B, 3/4A, 3/4B, and 5/6) and code lengths (from $n = 576$ to 2304). The matrix $\mathbf{H}$ is defined by the following $m \times n$ matrix:

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{0,0} & \mathbf{P}_{0,1} & \mathbf{P}_{0,2} & \cdots & \mathbf{P}_{0,n_b-2} & \mathbf{P}_{0,n_b-1} \\ \mathbf{P}_{1,0} & \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{1,n_b-2} & \mathbf{P}_{1,n_b-1} \\ \mathbf{P}_{2,0} & \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \cdots & \mathbf{P}_{2,n_b-2} & \mathbf{P}_{2,n_b-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{P}_{m_b-1,0} & \mathbf{P}_{m_b-1,1} & \mathbf{P}_{m_b-1,2} & \cdots & \mathbf{P}_{m_b-1,n_b-2} & \mathbf{P}_{m_b-1,n_b-1} \end{bmatrix} = \mathbf{P}^{H_b} \quad (27)$$

where $\mathbf{P}_{i,j}$ is one of a set of $z \times z$ permutation matrices or a $z \times z$ zero matrix. The matrix $\mathbf{H}$ is expanded from a binary base matrix $\mathbf{H}_b$ of size $m_b \times n_b$, where $n = z \cdot n_b$ and $m = z \cdot m_b$, with an integer > 1. The base matrix is expanded by replacing each 1 in the base matrix with a $z \times z$ permutation matrix, and each 0 with a $z \times z$ zero matrix. The base matrix size n_b is $n_b = 24$.

The permutations used are circular right shifts, and the set of permutation matrices contains the $z \times z$ identity matrix and circular right shifted version of the identity matrix. In the binary base matrix $\mathbf{H}_b$ each 0 is replaced by a blank or negative value (e.g., by -1) to denote a $z \times z$ all-zero matrix and each 1 is replaced by a circular shift size $p(i, j) \geq 0$ so that the model matrix $\mathbf{H}_{bm}$ is generated. $\mathbf{H}_{bm}$ can be directly expanded to $\mathbf{H}$.

$\mathbf{H}_b$ consists of two submatrices, $m_b \times k_b$ submatrix $\mathbf{H}_{b1}$ corresponding to the systematic bits and $m_b \times m_b$ submatrix $\mathbf{H}_{b2}$ corresponding to the parity bits: $\mathbf{H} = [\mathbf{H}_{b1}|\mathbf{H}_{b2}]$. $\mathbf{H}_{b2}$ is partitioned into two sections, where the vector $\mathbf{h}_b$ has odd weight and $\mathbf{H}'_{b2}$ has a dual-diagonal structure with matrix elements at row i, column j equal to 1 for $i = j$, 1 for $i = j + 1$, and 0 elsewhere. The base matrix has $h_b(0) = 1$, $h_b(m_b - 1) = 1$, and $h_b(j) = 1$ for $0 < j < m_b - 1$.

$$\mathbf{H} = [\mathbf{h}_b|\mathbf{H}'_{b2}] = \begin{bmatrix} h_b(0) & 1 & & & & \\ h_b(1) & 1 & 1 & & 0 & \\ \cdot & & 1 & \vdots & & \\ \cdot & & & \vdots & 1 & \\ \cdot & & 0 & & 1 & 1 \\ h_b(m_b-1) & & & & & 1 \end{bmatrix} \quad (28)$$

When expanding to $\mathbf{H}$, each 1 in $\mathbf{H}'_{b2}$ is assigned a shift size of 0 and is replaced by a $z \times z$ identity matrix.

A base model matrix is defined for the largest code length $n = 2304$ of each code rate. For all other code lengths of the same code rate, the set of shifts $\{p(i, j)\}$ in the base model matrix are used to determine the shift sizes. For code rates 1/2, 2/3, 3/4, and 5/6, the shift sizes $\{p(f, i, j)\}$ for a code size corresponding to expansion factor z_f are derived from $\{p(i, j)\}$ as follows.

$$p(f, i, j) = \begin{cases} p(i, j), & p(i, j) \leq 0 \\ \left\lfloor \frac{p(i,j) z_f}{z_0} \right\rfloor, & p(i, j) > 0 \end{cases} \quad (29)$$

where $\lfloor x \rfloor$ is a floor function that returns the largest integer less than or equal to x. For code rate 2/3A, the shift sizes $\{p(f, i, j)\}$ for a code size corresponding to expansion factor

z_f are derived from $\{p(i, j)\}$ as follows.

$$p(f, i, j) = \begin{cases} p(i, j), & p(i, j) \leq 0 \\ \text{mod } (p(i, j), z_f), & p(i, j) > 0 \end{cases} \quad (30)$$

The IEEEE 802.16e standard LDPC code supports different block sizes for each code rate through the use of an expansion factor. Each base model matrix has $n_b = 24$ columns, and the expansion factor is equal to $n/24$ for code length n.

7. LDPC Coded MIMO Systems

MIMO wireless systems offer high date rate transmission [50], [51]. In a MIMO system, since the transmitter transmits different signals at the same time from each transmit antenna, these signals interfere with each other. This means that the MIMO receiver must detect each transmitted signal from among the signals received.

Iterative signal detection with error correcting can achieve a good performance in MIMO systems particularly with soft-decision decoding and soft-interference cancellation. Figure 6 shows the receiver of a MIMO system with iterative signal detection. In iterative signal detection schemes [52], [53] signal detection (*ex.* Maximum Likelihood Detection (MLD), Minimum Mean Square Error (MMSE), and so on) is performed in the first iteration. When decoding yields a valid codeword, both iterative signal detection and iterative decoding stop, and the valid codeword is output. On the other hand, if no valid codeword is obtained up to the maximum number of decoding iterations, iterative signal detection is then performed. In the second or later signal detection iteration, the decoder output is processed to realize signal detection.

In Iterative Interference Cancellation (IIC), the decoder output is used to make an interference replica. Iterative detection uses the decoder output as a priori information for signal detection. In the iterative MMSE Soft Interference Cancellation (SIC) [54] a posterior probability LLR is used to make a soft replica. Interference cancellation is performed by subtracting the soft replica from the received signal to suppress the interference. The resulting signal is then input to the detector module, the MMSE module in MMSE-SIC. The detected signal is decoded by the soft decision decoder again.

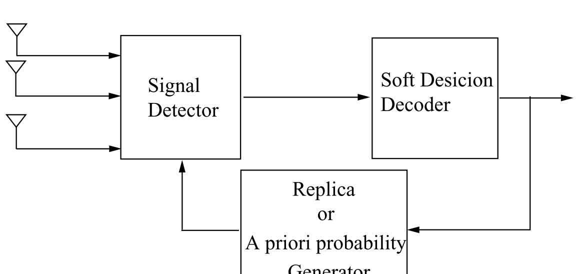

Fig. 6 Receiver block diagram of a MIMO system with iterative signal detection.

As error correcting codes in iterative detection with error correction, a turbo code and an LDPC code together with BP algorithm are used because of excellent error rate performance with linear processing time. In [55] LDPC codes are employed in a space-time coded OFDM systems over correlated frequency- and time-selective fading channels where both regular and irregular LDPC codes are examined. In [56] LDPC codes are optimized for AWGN channels and MIMO channels by performing a curve fitting on EXIT charts. In [57] LDPC codes are employed in MIMO-OFDM systems with turbo iterative receiver that consists of a soft maximum a posteriori (MAP) demodulator and a BP LDPC decoder, and with linear MMSE-SIC (LMMSE-SIC) demodulator and a BP decoder. LDPC codes are optimized for the systems both in AWGN channels and in specific MIMO channels by approximating the LLR output of the detector as a mixture of symmetric Gaussian variables, and using the Gaussian-approximated density evolution developed in [58]. It is shown that the MIMO-OFDM system with optimized LDPC codes and the MAP-based optimum receiver can perform within 1 dB from the ergodic capacity of the MIMO-OFDM systems under consideration. It is also shown that the suboptimum LMMSE-SIC based receiver has a small performance loss compared to the MAP-based optimum receiver. Note that the soft MAP demodulator has a complexity of $O(|\Omega|^{N_t})$, while the LMMSE-SIC demodulator has a complexity of $O(|\Omega|^2)$ where Ω is a signal constellation and N_t is the number of transmit antennas. The other interesting result shown in the paper is that the channel specific gain obtained by optimizing the code for the channel is not so large in the systems under the channel considered in the paper.

In [59] binary and nonbinary LDPC codes of quasi-regular structure are employed in space-time wireless transmission. It is shown through simulation that when applied to multiple antenna systems with large diversity order, LDPC codes of quasi-regular construction can achieve higher coding gain than previously proposed space-time trellis codes, turbo codes, and convolutional codes in quasi-static fading channels. [59] also extends the work of [60] regarding threshold analysis of nonbinary codes (2^p-ary LDPC codes where p equals the number of encoded bits transmitted by the transmit antenna array during each signaling interval) by incorporating a channel adapter to force symmetry into the MIMO channels. The technique of how to track DE of nonbinary SP decoding under Gaussian approximation for static multiple-antenna channels is shown, and then the threshold analysis is applied to quasi-singular codes under quasi-static fading. It is also shown that on fast fading channels, 2^p-ary irregular LDPC codes, designed for static channels, have superior performance to nonbinary quasi-regular codes and binary irregular codes designed for fast fading channels.

As shown above, LDPC-MIMO systems together with BP algorithm can achieve excellent error rate performance with linear processing time. However, since BP algorithm with LDPC codes can not realize exact MAP decoding, decoding is not guaranteed to converge within a fixed number of iterations. To achieve a reasonable degree of convergence, BP demands quite a few detection and decoding iterations. Increasing the number of iterations yields improved error rate performance but the improvements tend to saturate with iteration number. Unfortunately, in practical systems, the numbers of detection and decoding iterations are restricted to minimize latency, receiver size, and so on. In addition, BP needs several decoding iterations to propagate the LLR. Sequential BP can, at the cost of higher decoding latency, converge with a fewer decoding iterations than parallel BP [28], [61]. Since one bit carries all the other bits' information, LLR propagation is faster with sequential updating than with parallel updating. In particular, sequential BP can achieve better BER performance than the parallel BP with small numbers of decoding iterations.

In [62] a convergence acceleration (CA) technique is proposed for MIMO systems with BP algorithm. The CA technique performs signal detection and decoding alternately, whereas the conventional approach is to perform signal detection and decoding for all coded bits simultaneously. Moreover, the CA technique divides the coded bits into several groups based on transmit time. While it performs decoding in the same fashion as the conventional approach, only one group is detected in each signal detection iteration. The CA technique performs iterative group-based signal detection with decoding. For the same number of detection iterations per symbol, the CA technique and the conventional approach yield the same detection complexity, but the former provides a larger number of detection iterations. At the same maximum numbers of detection iterations per symbol and decoding iterations, the former requires fewer decoding iterations than the latter. Thus, the CA technique offers higher signal detection and LLR update frequencies than the conventional approach. In addition, in BP, the improvement of some LLRs leads to the improvement of the decoder performance. Since the CA technique updates initial LLRs more frequently than the conventional approach, at the same maximum numbers of detection iterations and decoding iterations, the CA technique improves the BP performance more than the conventional approach.

Figure 7 shows the BER of the conventional and CA iterative signal detection techniques for 4×4 MIMO system using MMSE-SIC where the irregular LDPC code with the code length 8000 and the code rate 0.5, and QPSK modulation are used. Figure 8 shows the average number of detections per coded bit and decoding iterations of the conventional and CA iterative signal detection techniques for the same system. All simulations assume that channel estimation is perfect and that the channel gain varies independently symbol by symbol. "Conv." represents the BER of the conventional iterative signal detection technique. In Fig. 7 the maximum number of detections per coded bit D_{max} is set to 5 for the CA technique and 5, 10, and 100 for the conventional technique. The maximum number of decoding iterations B_{max} is set to 20. For the CA technique, G is set to 1, 2, 4 and 10. Note that $G = 1$ is equivalent to the conventional iterative signal detection.

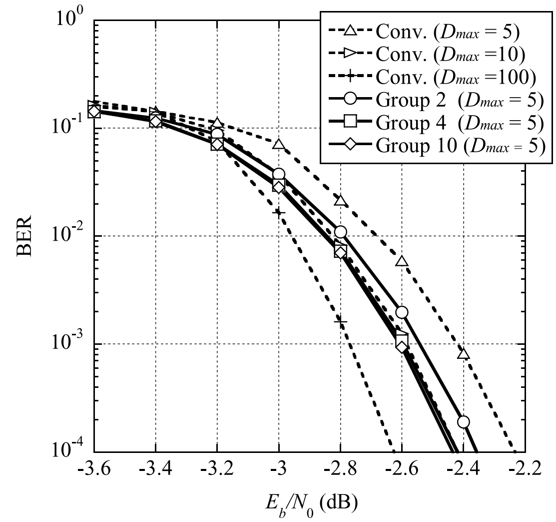

Fig. 7 BER versus E_b/N_0 dB for 4 × 4 MIMO system with QPSK and irregular LDPC codes using MMSE-SIC: B_{max} = 20, and D_{max} = 5, 10 and 100 for conventional approach and D_{max} = 5 for the CA technique.

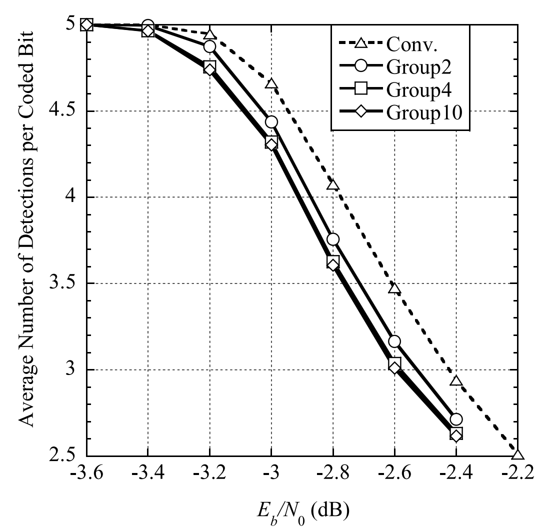

Fig. 8 Average number of detections per coded bit versus E_b/N_0 dB for 4 × 4 MIMO system with QPSK and irregular LDPC codes using MMSE-SIC: B_{max} = 20, and D_{max} = 5.

It can be seen that for the same D_{max} value, $D_{max} = 5$, the CA technique offers better BER than the conventional approach. Since the CA technique updates the initial LLRs more frequently than the conventional approach, the CA technique offers better decoding performance than the conventional approach. The BER of the CA technique is improved with increasing the number of groups. As the number of groups increases, the initial LLR is updated more frequently. In addition, at a low number of decoding iterations, even if the soft replica is wrong, the effect of error propagation is likely to be small, since the LLR of each bit is likely to be small. It can also be seen that the BER of the CA technique with $G = 4$ and 10 match that of the conventional approach with $D_{max} = 10$. Note that the conventional approach with D_{max} = 10 needs 5 more detections per coded bit and 100 more decoding iterations than the CA technique with G = 4 and 10. In addition, the conventional approach with D_{max} = 100 achieves better BER than the CA technique with G = 4 and 10. However, the conventional approach with D_{max} = 100 uses 95 more detections per coded bit and 1900 more decoding iterations than the CA technique. Moreover, it can be seen that the BER is improved with increasing the number of detection and decoding iterations.

Figure 8 confirms that the CA technique needs fewer (average) detections per coded bit and decoding iterations than the conventional approach. Since LDPC codes can realize error detection, the average numbers of detections per coded bit and decoding iterations fall as the decoder performance is improved. Since the CA technique can achieve better BER than the conventional approach even though it uses fewer (average) detection and decoding iterations with G = 4 and 10, the CA technique converges faster than the conventional approach.

8. Hybrid ARQ Using LDPC Codes

For error control, there are two kinds of well-known techniques: FEC and ARQ. When the feedback channel is available, ARQ is a good technique. The technique combining FEC and ARQ is referred to as Hybrid ARQ (HARQ) and is known to increase the throughput. There are three types of HARQ schemes. The first one is Type I HARQ where cyclic redundancy check (CRC) is appended to data and is encoded. The second one is Type II HARQ. Type II HARQ is an incremental redundancy (IR) ARQ scheme that transmits different coded bits in different transmissions. Type III HARQ is also an IR ARQ scheme. The difference between type II and III is that in type III the redundancy information is self-decodable.

There are many kinds of codes combined with HARQ. LDPC codes have also been applied to HARQ. In [63] IR HARQ schemes based on LDPC codes are proposed where LDPC codes are constructed based on the multiedge construction [64]; it deterministically arranges the edges adjacent to degree-2 bit nodes into a big cycle involving only degree-2 bit nodes. In [65] type-I HARQ based on LDPC codes is considered where a two-dimensional type-I cyclic $(0, s)$th order Euclidean Geometry LDPC code (EG-LDPC) is employed for error correction. In [66] HARQ scheme using LDPC codes are considered for satellite communication where protograph based LDPC codes and Go-back-N protocols are used.

To realize type II HARQ, rate-compatible (RC) codes can offer an efficient framework, because they can easily realize IR transmission by using only simple encoder and decoder: In response to negative acknowledgment (NACK) from the receiver, incremental parity bits of the next lower late code are transmitted. Several RC codes are designed based on convolutional codes and block codes. RC punctured turbo (RCPT) codes [67]–[69] and RC-LDPC codes [67] were also introduced. It is shown in [67] that puncturing alone cannot provide a sequence of well-performing LDPC codes with a wide range of rates. The problem can be found at higher rates where the large percentage of punctured bits (erasures) paralyzes the iterative soft-decision decoder. To solve this problem, RC-LDPC codes based on both puncturing and extending are proposed [67], [70], [71]. In [70] RC-LDPC codes are constructed based on progressive edge growth (PEG) construction [72]. The PEG method is a general non-algebraic method for constructing the Tanner graph with a large average cycle length. In constructing a graph with a given variable node degree distribution, the PEG method starts with the edge-selection procedure so that the placement of a new edge on the graph has the smallest impact on the cycle length of the graph. [71] points out the problem of RC-LDPC code based on the PEG method. That is, in the RC-LDPC code based on the PEG method, most of the large local cycles are not necessarily connected to the column elements with the lower weights. In applying puncturing, it is necessary to puncture the column elements with the lower weights that are combined with the large local cycles to avoid the performance loss. However, the column elements with the lower weights in the parity check matrix based on the PEG method consist of both large and short local cycles uniformly. Thus, it is difficult to avoid the performance degradation owing to puncturing in the RC-LDPC codes based on the PEG method. To overcome the above issue, [71] proposes a construction method using the progressively increased column weights (PICW) order to reduce the performance loss due to puncturing, where most of the lower weight column weights are combined with the large local cycles.

Recently, the other type of ARQ referred to as Reliability-Based Hybrid ARQ (RB-HARQ) scheme is attracting much attention. The RB-HARQ scheme uses error correcting codes with soft-input soft-output (SISO) decoder, where the receiver decides the retransmission bits based on the LLRs of the bits. The RB-ARQ schemes using convolutional codes and turbo codes have been proposed [73]–[75]. The RB-HARQ scheme using turbo code is shown to offer throughput close to capacity. However, in the RB-HARQ scheme the receiver must feed back the indices of unreliable bits to the transmitter. Therefore, the number of feedback bits can potentially be quite large. For instance, if the code length is approximately 1000 bits, each bit position can be represented by a 10-bit index. If 100 bits are to be retransmitted, the number of feedback bits will be 1000 bits if no source coding is applied. In [74] the RB-HARQ scheme that exploits the time-correlation properties of convolutional codes to reduce the number of feedback bits was proposed. In [75] a source coding is applied for the feedback bits of RB-HARQ scheme. In [76] the RB-HARQ scheme using LDPC codes was proposed. [76] also proposes the RB-HARQ scheme that reduces the number of feedback bits by utilizing the code structure of LDPC codes where the feedback bits are specified by the retransmission bits by each row that contains the unreliable bit. It is shown in [76] that the RB-HARQ scheme has high throughput with reduced amount of feedback.

9. Conclusions

We present the basics of LDPC codes and their decoding algorithms. We also present some LDPC codes having good performance and receiving much attention particularly in communication systems. We also overview two standardized LDPC codes, the LDPC codes standardized in DVB-S2 and the IEEE802.16e standard LDPC codes. Moreover, we present some researches on LDPC coded MIMO systems and HARQ using LDPC codes. As written above, the performance of LDPC codes largely depend on the code structure and decoding algorithms. It also depends on its channel, code rate, code length, and so on. In addition there are some constraints particularly in wireless communications and broadcasting, such as memory size, hardware, latency, and so on. Therefore, we have to carefully discuss the performance of LDPC codes.

In communication systems communication channels may often be time-varying and with memory, that is, with intersymbol interference (ISI). Some papers consider the design of LDPC code together with channel estimation. There are some papers considering code design and/or decoding algorithm over the ISI channels as well. The performance of communication systems, such as throughput depends on not only physical layer but also other layers. Therefore, the cross-layer design with considering practical constraints and the channel can improve the performance of LDPC coded communication and broadcasting systems.

Recently, cooperative communication is one of the hottest topics in communications. LDPC codes and BP algorithm are also based on the cooperation among bit nodes through the constraint, that is, the code. Cooperation is a key concept for communications and their elemental technologies, such as error correction coding and decoding.

References

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

[2] D.J.C. MacKay, “Good error-correcting codes based on very sparse matrices,” IEEE Trans. Inf. Theory, vol.45, no.2, pp.339–431, March 1999.

[3] 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.

[4] 3GPP, “Comparison of structured LDPC codes and 3GPP turbo codes,” 3GPP TSG RAN WG1 #43, R1-051360, Nov. 2005.

[5] G.J. Foschini and M.J. Gans, “On limits of wireless communications in a fading environment when using multiple antennas,” Wirel. Pers. Commun., vol.6, pp.311–335, March 1998.

[6] I.E. Telatar, “Capacity of multiantenna Gaussian channels,” Bell Laboratories, Tech. Memo., June 1995.

[7] I.E. Telatar, “Capacity of multiantenna Gaussian channels,” Eur. Trans. Commun., vol.10, no.6, pp.585–595, Nov./Dec. 1999.

[8] A. Bennatan and D. Burshtein, “Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels,” IEEE Trans. Inf. Theory, vol.52, no.2, pp.549–583, Feb. 2006.

[9] V. Rathi and R. Urbanke, “Density evolution, thresholds and the stability condition for non-binary LDPC codes,” IEE Proc., Commun., vol.152, no.6, pp.1069–1074, Dec. 2005.

[10] R.M. Tanner, “A recursive approach to low complexity codes,” IEEE Trans. Inf. Theory, vol.27, no.5, pp.533–547, Sept. 1981.

[11] J.M.F. Moura, J. Lu, and H. Zhang, “Structured low-density parity-check codes,” IEEE Signal Process. Mag., vol.21, no.1, pp.42–55, Jan. 2004.

[12] J. Lu and J.M.F. Moura, “Structured LDPC codes for high-density recording: Large girth and low error floor,” IEEE Trans. Magn., vol.42, no.2, pp.208–213, Feb. 2006.

[13] J.L. Kim, U.N. Peled, I. Perepelista, V. Pless, and S. Friedland, “Explicit construction of families of LDPC codes with no 4-cycles,” IEEE Trans. Inf. Theory, vol.50, no.10, pp.2378–2388, Oct. 2004.

[14] M.P.C. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices,” IEEE Trans. Inf. Theory, vol.50, no.8, pp.1788–1793, Aug. 2004.

[15] X.Y. Hu, E. Eleftheriou, and D.M. Arnold, “Regular and irregular edge-growth Tanner graphs,” IEEE Trans. Inf. Theory, vol.51, no.1, pp.386–398, Jan. 2005.

[16] S. Myung, K. Yang, and Y. Kim, “Lifting methods for quasi-cyclic LDPC codes,” IEEE Trans. Commun. Lett., vol.10, no.6, pp.489–491, June 2006.

[17] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, “Construction of low-density parity-check codes based on balanced incomplete block designs,” IEEE Trans. Inf. Theory, vol.50, no.6, pp.1257–1269, June 2004.

[18] E.R. Kschiischang, B.J. Frey, and H.A. Loeliger, “Factor graphs and the sum-product algorithm,” IEEE Trans. Inf. Theory, vol.47, no.2, pp.498–519, Feb. 2001.

[19] E.R. Kschiischang, B.J. Frey, and H.A. Loeliger, “Iterative decoding of compound codes by probability propagation in graphical models,” IEEE J. Sel. Areas Commun., vol.16, no.2, pp.219–230, Feb. 1998.

[20] T. Etzion, A. Trachtenberg, and A. Vardy, “Which codes have cycle-free Tanner graphs?,” IEEE Trans. Inf. Theory, vol.45, no.6, pp.2173–2181, Sept. 1999.

[21] J. Chen and M.P.C. Fossorier, “Near optimum universal belief propagation based decoding of low-density parity check codes,” IEEE Trans. Commun., vol.50, no.3, pp.406–414, March 2002.

[22] M.P.C. Fossorier, M. Mihaljevic, and H. Imai, “Reduced complexity iterative decoding of low density parity check codes based on belief propagation,” IEEE Trans. Commun., vol.47, no.5, pp.673–680, May 1999.

[23] J. Chen and M. Fossorier, “Density evolution for two improved BP-based decoding algorithms of LDPC codes,” IEEE Commun. Lett., vol.6, no.5, pp.208–210, May 2002.

[24] A. Ohhashi and T. Ohtsuki, “Regular low-density parity-check (LDPC) code with normalized and UMP BP-based algorithms on fast Rayleigh fading channel,” IEEE VTC 2004-Fall, vol.4, pp.2520–2524, Sept. 2004.

[25] A. Ohhashi and T. Ohtsuki, “Performance analysis of BP-based algorithms for irregular low-density parity-check codes on fast Rayleigh fading channel,” IEEE VTC 2004-Fall, vol.4, pp.2530–2534, Sept. 2004.

[26] S.Y. Chung, On the construction of some capacity-approaching coding schemes, Ph.D. Dissertation, MIT, Sept. 2000.

[27] T.J. Richardson and R. Urbanke, “The capacity of low-density parity-check codes under message-passing decoding,” IEEE Trans. Inf. Theory, vol.47, no.2, pp.599–618, Feb. 2001.

[28] J. Zhang and M.P.C. Fossorier, “Shuffled iterative decoding,” IEEE Trans. Commun., vol.53, no.2, pp.209–213, Feb. 2005.

[29] H. Kefir and I. Kanter, “Parallel versus sequential updating for belief propagation decoding,” Physica A, vol.330, pp.259–270, 2003.

[30] J. Zhang, Y. Wang, and M.P.C. Fossorier, “Replica shuffled iterative decoding,” IEEE ISIT2005, pp.454–458, Sept. 2005.

[31] H. Xiao and A.H. Banihashemi, “Graph-based message-passing schedules for decoding LDPC codes,” IEEE Trans. Commun., vol.52, no.12, pp.2098–2105, Dec. 2004.

[32] Y. Mao and A.H. Banihashemi, “Decoding low-density parity-check

codes with probabilistic schedule," IEEE Commun. Lett., vol.5, no.10, pp.414–416, Oct. 2001.

[33] Y. Chen and K.K. Parhi, "Overlapped message passing for quasi-cyclic low-density parity check codes," IEEE Trans. Circuits Syst. I, vol.51, no.6, pp.1106–1113, June 2004.

[34] Z. Li, L. Chen, L. Zeng, S. Lin, and W.H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," IEEE Trans. Commun., vol.54, no.1, pp.71–81, Jan. 2006.

[35] L. Chen, J. Xu, I. Djurdjevic, and S. Lin, "Near-Shannon-limit quasi-cyclic low-density parity-check codes," IEEE Trans. Commun., vol.52, no.7, pp.1038–1042, July 2004.

[36] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," IEEE Trans. Inf. Theory, vol.51, no.8, pp.2894–2901, Aug. 2005.

[37] J. Fan, "Array codes as LDPC codes," Proc. 2nd Int. Symp. Turbo Codes and Related Topics, pp.543–546, 2000.

[38] K. Yang and T. Helleseth, "On the minimum distance of array codes as LDPC codes," IEEE Trans. Inf. Theory, vol.49, no.12, pp.3268–3271, Dec. 2003.

[39] E. Elefttheriou and S. Ölçer, "Low-density parity-check codes for digital subscriber lines," IEEE ICC, pp.1752–1757, April/May 2002.

[40] H. Jin, A. Khandekar, and R. McEliece, "Irregular repeat-accumulate code," 2nd Int. Symp. on Turbo Codes and Related Topics, pp.1–8, Sept. 2000.

[41] D. Divsalar, H. Jin, and R. McEliece, "Coding theorems for 'turbo-like' codes," 36th Allerton Conf. on Communication, Control, and Computing, pp.201–210, Sept. 1998.

[42] 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.

[43] A. Roumy, S. Guemghar, G. Caire, and S. Verudú, "Design methods for irregular repeat-accumulate codes," IEEE Trans. Inf. Theory, vol.50, no.8, pp.1711–1727, Aug. 2004.

[44] H. Sankar and K.R. Narayanan, "Design of irregular repeat accumulate codes for OFDM systems with partial channel state information," IEEE Trans. Wireless Commun., vol.4, no.5, pp.2491–2497, Sept. 2005.

[45] G. Yue and X. Wang, "Optimization of irregular repeat accumulate codes for MIMO systems with iterative receivers," IEEE Trans. Wireless Commun., vol.4, no.6, pp.2843–2855, Nov. 2005.

[46] Digital video broadcasting (DVB); second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broad-band satellite applications, EN 302 307, European Telecommunications Standards Institute (ETSI).

[47] A. Morello and V. Mignone, "DVB-S2: The second generation standard for satellite broad-band services," Proc. IEEE, vol.94, pp.210–227, Jan. 2006.

[48] M. Eroz, F.W. Sun, and L.N. Lee, "DVB-S2 low density parity check codes with near Shannon limit performance," Int. J. Satell. Commun. Network, vol.22, pp.269–279, May-June 2004.

[49] IEEE Std 802.16e, "Draft IEEE standard for local and metropolitan area networks, Part 16: Air interface for fixed and mobile broadband wireless access systems," Feb. 2006.

[50] G. Foschini and J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," Wirel. Pers. Commun., vol.6, pp.311–355, March 1998.

[51] G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," Wirel. Pers. Commun., vol.1, pp.41–59, 1996.

[52] B. Steingrimsson, Z.Q. Luo, and K.M. Wong, "Soft quasi-maximum-likelihood detection for multiple-antenna wireless channels," IEEE Trans. Signal Proc., vol.51, no.11, pp.2710–2719, Nov. 2003.

[53] B. Lu, G. Yue, and X. Wang, "Performance analysis and design optimization of LDPC-coded MIMO OFDM system," IEEE Trans. Signal Proc., vol.52, no.2, pp.348–361, Feb. 2004.

[54] X. Wang and H.V. Poor, "Iterative (turbo) soft interference cancellation and decoding for coded CDMA," IEEE Trans. Commun., vol.47, no.7, pp.1046–1061, July 1999.

[55] B. Lu, X. Wang, and K.R. Narayanan, "LDPC-based space-time coded OFDM systems over correlated fading channels: Performance analysis and receiver design," IEEE Trans. Commun., vol.50, no.1, pp.74–80, Jan. 2002.

[56] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," IEEE Trans. Commun., vol.52, no.4, pp.670–678, April 2004.

[57] B. Lu, G. Yue, and X. Wang, "Performance analysis and design optimization of LDPC-coded MIMO OFDM systems," IEEE Trans. Commun., vol.52, no.2, pp.348–361, Feb. 2004.

[58] S. Chung, G.D. Forney, T.J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," IEEE Commun. Lett., vol.5, no.2, pp.58–60, Feb. 2001.

[59] G. Li, J. Fair, and W.A. Krzymień, "Low-density parity-check codes for space-time wireless transmission," IEEE Trans. Wireless Commun., vol.5, no.2, pp.312–322, Feb. 2006.

[60] J. Hou, P.H. Siegel, L.B. Milstein, and H.D. Pfister, "Capacity-approaching bandwidth-efficient coded modulation schemes based on low-density parity-check codes," IEEE Trans. Inf. Theory, vol.49, no.9, pp.2141–2155, Sept. 2005.

[61] H. Kfir and I. Kanter, "Parallel versus sequential updating for belief propagation decoding," Physica A, vol.330, pp.259–270, 2003.

[62] S. Gounai and T. Ohtsuki, "Convergence acceleration of iterative signal detection for MIMO system with belief propagation," Proc. IEEE GLOBECOM2006, Nov.–Dec. 2006.

[63] S. Sesia, G. Caire, and G. Vivier, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," IEEE Trans. Commun., vol.52, no.8, pp.1311–1321, Aug. 2004.

[64] T. Richardson and R. Urbanke, "Multi-edge type LDPC codes," http://lthcwww.epfl.ch/

[65] J. Liang, Z. Ding, and S. Lin, "Receiver design for type-I hybrid ARQ scheme in frequency-selective fading channels," 35th Asilomar Conf. on Signals, Systems, and Computers, vol.2, pp.959–963, Nov. 2001.

[66] S. Shambayati, C.R. Jones, and D. Divsalar, "Maximizing throughput for satellite communication in a hybrid FEC/ARQ scheme using LDPC codes," IEEE MILCOM, vol.5, pp.3289–3298, Oct. 2005.

[67] J. Li and K. Narayanan, "Rate-compatible low density parity check codes for capacity-approaching ARQ scheme in packet data communications," Int. Conf. on Comm., Internet, and Info. Tech. (CIIT), pp.201–206, Nov. 2002.

[68] R. Mantha and F.R. Kschischang, "A capacity-approaching hybrid ARQ scheme using turbo codes," IEEE GLOBECOM, vol.5, pp.2341–2345, 1999.

[69] D.N. Rowitch and L.B. Milstein, "On the performance of hybrid FEC/ARQ systems using rate compatible punctured turbo (RCPT) codes," IEEE Trans. Commun., vol.48, no.6, pp.948–959, June 2000.

[70] M.R. Yazdani and A.H. Banihashemi, "On construction of rate-compatible low-density parity-check codes," IEEE Commun. Lett., vol.8, no.3, pp.159–161, March 2004.

[71] C. Zheng, N. Miyazaki, and T. Suzuki, "Rate compatible low-density parity-check codes based on progressively increased column weights," IEICE Trans. Fundamentals, vol.E89-A, no.10, pp.2493–2500, Oct. 2006.

[72] X.Y. Hu, E. Eleftheriou, and D.M. Arnold, "Progressive edge-growth Tanner graphs," IEEE GLOBECOM, vol.2, pp.995–1001, Nov. 2001.

[73] H. Kim and J.M. Shea, "New turbo-ARQ techniques based on estimated reliabilities," IEEE WCNC 2003, vol.2, pp.843–848, March 2003.

[74] A. Roongta and J.M. Shea, "Reliability-based hybrid ARQ using

convolutional codes," IEEE ICC 2003, vol.4, pp.2889–2893, May 2003.

[75] A. Roongta and J.M. Shea, "Reliability-based hybrid ARQ and rate-compatible punctured convolutional (RCPC) codes," IEEE WCNC 2004, vol.4, pp.2105–2109, March 2004.

[76] Y. Inaba, T. Saito, and T. Ohtsuki, "Reliability-based hybrid ARQ (RB-HARQ) schemes using low-density parity-check (LDPC) codes," IEICE Trans. Commun., vol.E89-B, no.4, pp.1170–1177, April 2006.

Tomoaki Ohtsuki received the B.E., M.E., and Ph.D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1990, 1992, and 1994, respectively. From 1994 to 1995 he was a Post Doctoral Fellow and a Visiting Researcher in Electrical Engineering at Keio University. From 1993 to 1995 he was a Special Researcher of Fellowships of the Japan Society for the Promotion of Science for Japanese Junior Scientists. From 1995 to 2005 he was with Science University of Tokyo. In 2005 he joined Keio University. He is now an Associate Professor at Keio University. From 1998 to 1999 he was with the department of electrical engineering and computer sciences, University of California, Berkeley. He is engaged in research on wireless communications, optical communications, signal processing, and information theory. Dr. Ohtsuki is a recipient of the 1997 Inoue Research Award for Young Scientist, the 1997 Hiroshi Ando Memorial Young Engineering Award, Ericsson Young Scientist Award 2000, 2002 Funai Information and Science Award for Young Scientist, IEEE the 1st Asia-Pacific Young Researcher Award 2001, and the 5th International Communication Foundation (ICF) Research Award. He is a Vice Chair of Editorial Board, IEICE Communications Society and a Technical Editor of IEEE Wireless Communications Magazine. He is a senior member of the IEEE and a member of the SITA.