Chapter 10 Quasi-Cyclic Low-Density Parity-Check Codes

10.1 Introduction to Quasi Cyclic Low-Density Parity-Check Codes

It is well known that low-density parity-check (LDPC) codes, decoded with iterative decoding based on belief propagation (BP) or various BP-based algorithms as introduced in the preceding chapters, can achieve excellent performance that is quite close to Shannon limit. Ever since the rediscovery of LDPC codes, design, construction, efficient encoding and decoding, performance analysis, and applications of these powerful error-correction codes in digital communication and storage systems have always become the central points of research in the past decade. To date, various methods for constructing LDPC codes have been proposed, however based on the methods of construction, LDPC codes can be generally classified into two broad categories: (1) random (or random-like) codes generated by computer search based on certain design guidelines and required structural constraints in their Tanner graphs, such as the girth and degree distributions for the variable and check nodes, etc.; (2) structured LDPC codes designed based on algebraic and combinatorial methods, such as quasi-cyclic (QC) LDPC codes, LDPC codes based on finite geometry and BIBD (balanced incomplete block design) that will be introduced in this chapter.

Although iterative decoding of long LDPC codes constructed randomly can be practically implemented, encoding of these codes can be rather complex since most of these codes, especially by computer-generated random codes, do not exhibit a strong mathematical structure to allow simple encoding. Generally, it is widely believed that good error performance may be resulted in if a code of sufficient length employed is

more like the random code as Shannon used in the early time. However, the subsequent practical encoding problem makes the engineers to adopt a class of structured LDPC codes that allows low-complexity encoding, which are known as the quasi-cyclic LDPC codes. It is well known in coding theory [111] that QC codes can be encoded with simple shift registers with linear complexity based on their generators or generator matrices. Well-designed QC LDPC codes have been shown to perform as well as the random regular or irregular LDPC codes generated by computer [112], in terms of bit-error rate, block-error rate, and error floor, collectively. Hence, they are very strong competitors to the random LDPC codes in many practical applications due to their very simple encoding and low error floors. These codes also have advantages in integrated circuit (IC) decoder implementations due to their cyclic symmetry, which results in simple regular writing and modular structure.

Usually, LDPC codes are defined by their parity-check matrices. The parity-check matrix of a QC-LDPC code is given as an array of sparse circulants of the same size [112] [113]. Simply saying, the parity-check matrix is in circulant form. In this chapter we mainly deal with efficient encoding of binary QC-LDPC codes and investigate the performance of QC-LDPC over an AWGN channel. Two methods are given to find the generator matrix of a QC-LDPC code in a systematic-circulant (SC) form based on its parity-check matrix in circulant form. By applying the resulted generator matrix in SC form, encoding of a QC-LDPC code can be accomplished with an array of shift registers with complexity linearly proportional to the number of parity-check bits of the code for serial encoding, and to the length of the code for high-speed parallel encoding.

The aforementioned methods can be similarly extended to nonbinary QC-LDPC codes that are decoder by a Fast Fourier Transform based q-ary sum-product algorithm (QSPA), called FFT-QSPA [114]. For more details the reader can refer to [115].

10.2 Circulant Matrix and Related Properties

A circulant matrix, or simply saying circulant, is a very useful mathematical tool in designing QC-LDDPC codes. The definition of this matrix is

Definition 10.1: An $n\times n$ matrix $\mathbf{C}$ of the form in (10-1) is called a circulant matrix.

$$\mathbf{C}=\begin{bmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{bmatrix} \tag{10-1}$$

Remarks:

(1) A circular is a square matrix where each row is the cyclic shift (one place to the right) of the row above it. In particular, the first row is the cyclic shift of the last row. For such a circulant, each column is the downward cyclic shift of the column on its left, and similarly the first column is the cyclic shift of the last column.

(2) A circulant matrix is fully specified by one vector c, which can be any column (or row) in $\mathbf{C}$. But for the sake of convenience, we can designate it as the first column (or row) in $\mathbf{C}$, which is called the generator of the circulant.

(3) The row and column weights of a circulant are the same, say w. For simplicity, we say that that the circulant has weight w. If w=1, then the circulant is a permutation matrix, called a circulant permutation matrix.

(4) For a circulant, the set of columns (reading top-down) is the same as the set of rows (reading from right to left). The first column is the same as the last row in the corresponding order.

(5) For a $b\times b$ circulant $\mathbf{A}$ over GF(2), if its rank is b, then all its rows are linearly independent. If its rank r is less than b, then any consecutive r rows (columns) of $\mathbf{A}$ may be regarded as linearly independent, and the other $b-r$ rows (columns) are linearly dependent. For simplicity, based on the structure of a circulant we usually take the first (or the last) r rows (or columns) as the independent rows (or columns).

Moreover, we can easily obtain the following properties [114][115] of the circulant matrix, which are particularly useful in decoding the nonbinary quasi cyclic LDPC codes by using FFT-QSPA.

(1) The set of $n\times n$ circulant matrices forms an n-dimensional vector space.

(2) Circulant matrices forms a commutative algebra, i.e., for any two given circulant matrices A and B, the sum $A+B$ is circulant, the product AB is circulant, and $AB=BA$.

(3) The eigenvectors of a circulant matrix of given size are the columns of the direct Fourier transform matrix of the same size. Consequently, the eigenvalues of a circulant matrix can be readily calculated by a Fast Fourier transform (FFT).

(4) If an FFT of the first row of a circulant matrix is performed, then the determinant of the circulant matrix is the product of the spectral values.

10.3. Fundamentals of Quasi Cyclic LDPC Codes

The definition of a quasi cyclic LDPC codes family is given as follows:

Definition 10.2: A QC-LDPC code is given by the null space of an array of sparse circulants of the same size. For two positive integers c and t with $c \le t$, consider the following $c \times t$ array of $b \times b$ circulants over GF(2):

$$\mathbf{H}_{qc} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{c,1} & \mathbf{A}_{c,2} & \cdots & A_{c,t} \end{bmatrix} \tag{10-2}$$

which has the following structural properties:

(a) The weight of circulant $\mathbf{A}_{i,j}$ $(1 \le i \le c,\ 1 \le j \le t)$ is small compared with the size b.

(b) No two rows (or two columns) of $\mathbf{H}_{qc}$ have more than one "1-component" in common, which is called the row-column (RC) constraint.

The null space of $\mathbf{H}_{qc}$ defines a QC-LDPC code C_{qc} of length $n = tb$ based on the parity-check matrix $\mathbf{H}_{qc}$. □

Remarks:

(1) Property (a) implies that each circulant in $\mathbf{H}_{qc}$ is a sparse circulant, which leads to a sparse parity-check matrix of QC-LDPC code C_{qc}.

(2) The RC constraint ensures that there are no four "1-entries" at the four corners of a rectangular in $\mathbf{H}_{qc}$, thus the Tanner graph of the QC-LDPC codes defined by $\mathbf{H}_{qc}$ is free of cycles of length four, and has a girth of at least six.

(3) If all the circulants in $\mathbf{H}_{qc}$ have the same weight w, then $\mathbf{H}_{qc}$ has constant column weight cw and constant row weight tw. In this case, C_{qc} is a regular QC-LDPC code.

(4) If the weight distribution of the circulants in $\mathbf{H}_{qc}$ leads to multiple column weights or multiple row weights in $\mathbf{H}_{qc}$, then C_{qc} is an irregular QC-LDPC code.

Codeword of a QC-LDPC code

Based on the parity-check matrix given in (10-2), any codeword $\mathbf{v}$ in C_{qc} can be divided into t sections as $\mathbf{v}=(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t)$, where each section $\mathbf{v}_j$ $(1\le j\le t)$ is made up of b consecutive components of $\mathbf{v}$. Note that the b components of the jth section $\mathbf{v}_j$ are associated with the b components of the jth column of circulants of $\mathbf{H}_{qc}$.

Sectionized Cyclic Structure of a QC-LDPC code

Let $\mathbf{v}_j^{(l)}$ denote the vector by cyclically shifting each of the b components of the jth section $\mathbf{v}_j$ to the right l places. Obviously, $\mathbf{v}_j^{(0)}=\mathbf{v}_j^{(n)}=\mathbf{v}_j$ due to $n=tb$. Note that $\mathbf{v}_j^{(l)}$ is also called the lth cyclic shift of $\mathbf{v}_j$. It immediately follows from the circulants structure of $\mathbf{H}_{qc}$ that the vector $\mathbf{v}^{(l)}=(\mathbf{v}_1^{(l)}, \mathbf{v}_2^{(l)}, \ldots, \mathbf{v}_t^{(l)})$ is also a codeword in C_{qc}. Thus we call that a QC-LDPC code has a property of sectionized cyclic structure. In particular, if the parity-check matrix $\mathbf{H}_{qc}$ has a single circulant or a single column of circulants, then C_{qc} is a cyclic code. Hence, this provides an effective way to construct cyclic LDPC codes, which actually forms a subclass of QC-LDPC codes.

10.4. Generator Matrix in Systematic-Circulant Form in Case I

In this section we will consider the case that the rank r of the parity-check matrix $\mathbf{H}_{qc}$ given by (10-1) is equal to the number cb of rows of $\mathbf{H}_{qc}$. Also, we assume there

exists a $c\times c$ subarray in $\mathbf{H}_{qc}$ with rank r. Hence, the columns of circulants of $\mathbf{H}_{qc}$ can be arranged in such a way by column operations in circulant that the $c\times c$ subarray with rank r is given as follows

$$\mathbf{D}=\begin{bmatrix} \mathbf{A}_{1,t-c+1} & \mathbf{A}_{1,t-c+2} & \cdots & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,t-c+1} & \mathbf{A}_{2,t-c+2} & \cdots & \mathbf{A}_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{c,t-c+1} & \mathbf{A}_{c,t-c+2} & \cdots & \mathbf{A}_{c,t} \end{bmatrix} \tag{10-3}$$

which has the same rank as that of $\mathbf{H}_{qc}$. Without loss of generality, we also assume that the coded bits corresponding to the first $(t-c)b$ columns of $\mathbf{H}_{qc}$ are the information bits, while the remaining cb coded bits related to the last cb columns of $\mathbf{H}_{qc}$ (cb columns of $\mathbf{D}$) are the redundant (parity-check) bits. Hence, we can write the generator matrix of C_{qc} in systematic form as

$$\mathbf{G}_{qc}=\begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \vdots \\ \mathbf{G}_{t-c} \end{bmatrix}=\begin{bmatrix} \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{G}_{1,1} & \mathbf{G}_{1,2} & \cdots & \mathbf{G}_{1,c} \\ \mathbf{0} & \mathbf{I} & \cdots & \mathbf{0} & \mathbf{G}_{2,1} & \mathbf{G}_{2,2} & \cdots & \mathbf{G}_{2,c} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{G}_{t-c,1} & \mathbf{G}_{t-c,2} & \cdots & \mathbf{G}_{t-c,c} \end{bmatrix}=[\mathbf{I}_{(t-c)b}\ \mathbf{P}] \tag{10-4}$$

where $\mathbf{I}$ is a $b\times b$ identity matrix, $\mathbf{0}$ is a $b\times b$ zero matrix, and $\mathbf{G}_{i,j}$ ($1\le i\le t-c$ and $1\le j\le c$) is a $b\times b$ circulant. From coding theory principle, we have

$$\mathbf{H}_{qc}\mathbf{G}_{qc}^{T}=\mathbf{0} \tag{10-5}$$

where $\mathbf{0}$ is a $cb\times(t-c)b$ zero matrix.

The generator matrix given by (10-4) is in a systematic-circulant (SC) form since $\mathbf{G}_{qc}$ is a systematic generator and the matrix $\mathbf{P}$ is an array of circulants consisting of $\mathbf{G}_{i,j}$'s.

Note that the most advantage of employing generator matrix in SC form is that it allows us to encode a QC-LDPC code with simple shift registers.

Let $\mathbf{g}_{i,j}$ ($1 \le i \le t-c$ and $1 \le j \le c$) be the generator of the circulant $\mathbf{G}_{i,j}$. Clearly, we can easily form all the circulants $\mathbf{G}_{i,j}$'s of $\mathbf{G}_{qc}$ if the corresponding $\mathbf{g}_{i,j}$'s are known. Therefore, $\mathbf{G}_{qc}$ is completely finalized by a set of $c(t-c)$ $\mathbf{g}_{i,j}$'s which are called the generators of the code C_{qc}. Note that here the generator differs from the generator matrix, which is also called generator in some circumstances. The reader can easily recognize the difference from the context.

10.4.1 Encoding of a QC-LDPC code by determining the generators

Determining the generators

Let $\mathbf{u}$=(1, 0, …, 0) be the unit b-tuple. The first row of the submatrix of $\mathbf{G}_i$ ($1 \le i \le t-c$) in (10-4) is

$$\mathbf{g}_i = (\underbrace{\mathbf{0}, ..., \mathbf{0}}_{i-1}, \ \mathbf{u}, \ \underbrace{\mathbf{0}, ..., \mathbf{0}}_{t-c-i}, \ \mathbf{g}_{i,1}, \ \mathbf{g}_{i,2}, \ \ldots, \ \mathbf{g}_{i,c}) \tag{10-6}$$

where $\mathbf{0}$ is the all-zero b-tuple, and the b-dimensional row vector $\mathbf{g}_{i,j}$ ($1 \le i \le t-c$, $1 \le j \le c$) corresponds to the first row of the matrix $\mathbf{G}_{i,j}$. Since $\mathbf{g}_i$ is a codeword of a QC-LDPC code defined by $\mathbf{H}_{qc}$, thus it must satisfy the requirement as

$$\mathbf{H}_{qc}\mathbf{g}_i^T = \mathbf{0} \tag{10-7a}$$

Let $\mathbf{z}_i$=($\mathbf{g}_{i,1}$, $\mathbf{g}_{i,2}$, …, $\mathbf{g}_{i,c}$) and $\mathbf{M}_i$=($\mathbf{A}_{1,i}$, …, $\mathbf{A}_{c,i}$)^T. Then (10.7a) can be further expressed as

$$\mathbf{M}_i\mathbf{u}^T + \mathbf{D}\mathbf{z}_i^T = \mathbf{0} \tag{10-7b}$$

Since $\mathbf{D}$ is a nonsingular square matrix with full rank, it follows from (10-7b) that

$$\mathbf{z}_i^T = \mathbf{D}^{-1}\mathbf{M}_i\mathbf{u}^T \tag{10-7c}$$

Thus, from the obtained $\mathbf{z}_1$, $\mathbf{z}_2$, …, $\mathbf{z}_{t-c}$, we get all the generators $\mathbf{g}_{i,j}$'s of the circulants in $\mathbf{G}_{qc}$. Then $\mathbf{G}_{qc}$ can be constructed readily.

Codewords formed by generator matrix in systematic-circulant (*SC*) *form*

Let $\mathbf{a}=(a_1, a_2, \ldots, a_{(t-c)b})$ be the information sequence of $(t-c)b$ bits for the encoding. Divide the sequence $\mathbf{a}$ into $(t-c)$ sections of length b as $\mathbf{a}=(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-c})$, where the ith section $\mathbf{a}_i=(a_{(i-1)b+1}, a_{(i-1)b+2}, \ldots, a_{ib})$. Thus, the codeword with respect to the information sequence $\mathbf{a}$ is $\mathbf{v}=\mathbf{a}\mathbf{G}_{qc}$, which can be written in a systematic form as $\mathbf{v}=(\mathbf{a}, \mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_c)$ with $\mathbf{p}_j=(p_{j,1}, p_{j,2}, \ldots, p_{j,b})$ $(1\le j\le c)$ expressed as

$$\mathbf{p}_j = \mathbf{a}_1\mathbf{G}_{1,j} + \mathbf{a}_2\mathbf{G}_{2,j} + \ldots. + \mathbf{a}_{t-c}\mathbf{G}_{t-c,j} \tag{10-8a}$$

To gain an insight view of (10-8a), let $\mathbf{g}_{i,j}^{(l)}$ be the lth right cyclic shift of the generator $\mathbf{g}_{i,j}$. Obviously, we have $\mathbf{g}_{i,j}^{(0)}=\mathbf{g}_{i,j}^{(b)}=\mathbf{g}_{i,j}$. Thus, it yields

$$\mathbf{a}_i\mathbf{G}_{i,j} = a_{(i-1)b+1}\mathbf{g}_{i,j}^{(0)} + a_{(i-1)b+2}\mathbf{g}_{i,j}^{(1)} + \ldots. + a_{ib}\mathbf{g}_{i,j}^{(b-1)} \tag{10-8b}$$

Therefore, the jth parity-check section $\mathbf{p}_j$ can be evaluated in a step-by-step encoding approach as the information sequence $\mathbf{a}$ is shifted into the encoder sequentially. The detailed steps are presented as

Step 1: For $k=1$ at the 1st step, the initial vector $\mathbf{s}_{1,j}$ is calculated as

$$\mathbf{s}_{1,j} = \mathbf{a}_1\mathbf{G}_{1,j} \tag{10-9}$$

which is temporarily stored in a register.

Step 2: At the 2nd step, the second section $\mathbf{a}_2$ of information bits in $\mathbf{a}$ is shifted into the encoder, hence the partial sum $\mathbf{a}_2\mathbf{G}_{2,j}$ is evaluated by (10-8b) as

$$\mathbf{a}_2\mathbf{G}_{2,j} = a_{b+1}\mathbf{g}_{2,j}^{(0)} + a_{b+2}\mathbf{g}_{2,j}^{(1)} + \ldots\ldots + a_{2b-1}\mathbf{g}_{2,j}^{(b-2)} + a_{2b}\mathbf{g}_{2,j}^{(b-1)} \tag{10-10}$$

Step 3: Adding $\mathbf{a}_2\mathbf{G}_{2,j}$ to $\mathbf{s}_{1,j}$, we obtain the accumulated sum $\mathbf{s}_{2,j}$ as

$$\mathbf{s}_{2,j} = \mathbf{s}_{1,j} + \mathbf{a}_2\mathbf{G}_{2,j} \tag{10-11}$$

which is also temporarily stored in the register that is refreshed by $\mathbf{s}_{2,j}$.

The above steps are repeated for $t-c$ times and finally we arrive at the last step:

Step $t-c$: At the $(t-c)$th step, the accumulated sum $\mathbf{s}_{t-c,j}$ is

$$\mathbf{s}_{t-c,j} = \mathbf{s}_{t-(c-1),j} + \mathbf{a}_{t-c}\mathbf{G}_{t-c,j} \tag{10-12}$$

which gives the jth parity section $\mathbf{p}_j = \mathbf{s}_{t-c,j}$.

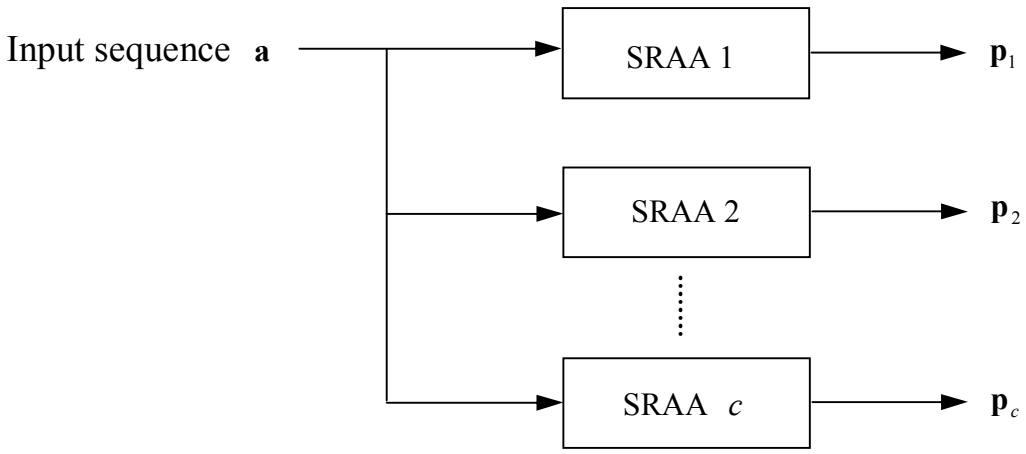

Fig. 10.1 A SRAA-based QC-LDPC encoder generating the parity sections $\mathbf{p}_i$ $(1 \le i \le c)$.

Based on the aforementioned encoding process, the jth parity section $\mathbf{p}_j$ can be obtained with a so-called *shift-register-adder-accumulator* (SRAA) process. The block

diagram for generating the parity sections of a QC-LDPC code is shown in Fig. 10.1 in terms of SRAA. The details of implementations of SRAA can be found in [107][108].

10.4.2 Encoding of a QC-LDPC code by two-stage encoder

In this section, we will present another effective method to encode the QC-LDPC code, which is called two-stage encoder.

Preliminaries

Assume that the first $b\times b$ circulant $\mathbf{A}_{1,t-c+1}$ of array $\mathbf{D}$ in (10-3) has rank b. This can be realize by arranging the columns and rows of circulants of $\mathbf{H}_{qc}$ so that $\mathbf{D}$ has rank cb. It follows from Schur's complement [116][117] that $\mathbf{D}^{-1}$ can be resulted in based on the circulants in $\mathbf{D}$. It is known that the inverses, products, and sums of circulants are also circulants [116]. Therefore, $\mathbf{D}^{-1}$ is also a $c\times c$ array of $b\times b$ circulants, which is expressed as

$$\mathbf{D}^{-1}=\begin{bmatrix}\mathbf{B}_{1,1} & \mathbf{B}_{1,2} & \cdots & \mathbf{B}_{1,c}\\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} & \cdots & \mathbf{B}_{2,c}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{B}_{c,1} & \mathbf{B}_{c,2} & \cdots & \mathbf{B}_{c,c}\end{bmatrix} \tag{10-13}$$

Clearly, a row of a generator matrix is a codeword of the code defined by the generator matrix. Thus, for the generator matrix given by (10-4), the rows of the $b\times bt$ matrix $(\underbrace{\mathbf{0},\ldots,\mathbf{0}}_{i-1},\ \mathbf{I},\ \underbrace{\mathbf{0},\ldots,\mathbf{0}}_{t-c-i},\ \mathbf{G}_{i,1},\ \mathbf{G}_{i,2},\ \ldots,\ \mathbf{G}_{i,c})$ are the b codewords of the binary QC-LDPC code, which must satisfy the relationships regarding the parity-check matrix $\mathbf{H}_{qc}$ in (10-2)

$$\begin{bmatrix} \mathbf{A}_{1,i} \\ \mathbf{A}_{2,i} \\ \vdots \\ \mathbf{A}_{c,i} \end{bmatrix} \mathbf{I}_{b\times b} + \mathbf{D} \begin{bmatrix} \mathbf{G}_{i,1}^T \\ \mathbf{G}_{i,2}^T \\ \vdots \\ \mathbf{G}_{i,c}^T \end{bmatrix} = \mathbf{0} \tag{10-14a}$$

Equivalently,

$$\begin{bmatrix} \mathbf{G}_{i,1}^T \\ \mathbf{G}_{i,2}^T \\ \vdots \\ \mathbf{G}_{i,c}^T \end{bmatrix} = \mathbf{D}^{-1} \begin{bmatrix} \mathbf{A}_{1,i} \\ \mathbf{A}_{2,i} \\ \vdots \\ \mathbf{A}_{c,i} \end{bmatrix} = \begin{bmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} & \dots & \mathbf{B}_{1,c} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} & \dots & \mathbf{B}_{2,c} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{B}_{c,1} & \mathbf{B}_{c,2} & \dots & \mathbf{B}_{c,c} \end{bmatrix} \begin{bmatrix} \mathbf{A}_{1,i} \\ \mathbf{A}_{2,i} \\ \vdots \\ \mathbf{A}_{c,i} \end{bmatrix} \tag{10-14b}$$

Let $\mathbf{B}_j = [\mathbf{B}_{j,1}, \mathbf{B}_{j,2}, \ldots, \mathbf{B}_{j,c}]$ for $1 \le j \le c$. The circulants $\mathbf{G}_{i,j}$'s $(1 \le i \le t-c)$ in $\mathbf{G}_{qc}$ are

$$\mathbf{G}_{i,j} = (\mathbf{B}_j \mathbf{M}_i)^T = \mathbf{M}_i^T \mathbf{B}_j^T \tag{10-15}$$

From (10-4) and (10-15), the generator matrix of C_{qc} in SC form is

$$\mathbf{G}_{qc} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{M}_1^T\mathbf{B}_1^T & \mathbf{M}_1^T\mathbf{B}_2^T & \dots & \mathbf{M}_1^T\mathbf{B}_c^T \\ \mathbf{0} & \mathbf{I} & \dots & \mathbf{0} & \mathbf{M}_2^T\mathbf{B}_1^T & \mathbf{M}_2^T\mathbf{B}_2^T & \dots & \mathbf{M}_2^T\mathbf{B}_c^T \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{I} & \mathbf{M}_{t-c}^T\mathbf{B}_1^T & \mathbf{M}_{t-c}^T\mathbf{B}_2^T & \dots & \mathbf{M}_{t-c}^T\mathbf{B}_c^T \end{bmatrix} \tag{10-16}$$

By (10-16) the j th $(1 \le j \le c)$ parity section $\mathbf{p}_j^T$ is

$$\begin{aligned} \mathbf{p}_j^T &= (\mathbf{a}_1\mathbf{M}_1^T\mathbf{B}_j^T)^T + (\mathbf{a}_2\mathbf{M}_2^T\mathbf{B}_j^T)^T + \ldots + (\mathbf{a}_{t-c}\mathbf{M}_{t-c}^T\mathbf{B}_j^T)^T \\ &= \mathbf{B}_j\mathbf{M}_1\mathbf{a}_1^T + \mathbf{B}_j\mathbf{M}_2\mathbf{a}_2^T + \ldots + \mathbf{B}_j\mathbf{M}_{t-c}\mathbf{a}_{t-c}^T \\ &= \mathbf{B}_j[\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{t-c}]\mathbf{a}^T \end{aligned} \tag{10-17}$$

Therefore, the computation of $\mathbf{p}_j^T$ can be separated into two steps. First, we calculate the vector with cb bits as follows:

$$\mathbf{y}^T = [\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{t-c}]\mathbf{a}^T \tag{10-18}$$

Second, compute the jth parity section $\mathbf{p}_j = \mathbf{B}_j \mathbf{y}^T$. Finally, the overall codeword is finalized. Now we introduce the details for each step as:

The first stage of the encoder

We divide the vector $\mathbf{y}$ into c sections, i.e., $\mathbf{y}=(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_c)$, and by (10-2) and (10-18) the kth $(1 \le k \le c)$ section $\mathbf{y}_k=(y_{k,1}, y_{k,2}, \ldots, y_{k,b})$ is given by

$$\mathbf{y}_k^T = \mathbf{A}_{k,1}\mathbf{a}_1^T + \mathbf{A}_{k,2}\mathbf{a}_2^T + \ldots + \mathbf{A}_{k,t-c}\mathbf{a}_{t-c}^T \tag{10-19}$$

Let $\mathbf{a}_i^{(l)}$ $(1 \le l \le b)$ denotes the lth left cyclic shift of $\mathbf{a}_i$, more specially, $\mathbf{a}_i^{(l)}$ is formed by cyclically shifting each component of $\mathbf{a}_i$ to the left l places. By (10-19), the lth bit of $\mathbf{y}_k$ can be expressed as

$$y_{k,l} = \mathbf{q}_{k,1}(\mathbf{a}_1^{(l-1)})^T + \mathbf{q}_{k,2}(\mathbf{a}_2^{(l-1)})^T + \ldots + \mathbf{q}_{k,t-c}(\mathbf{a}_{t-c}^{(l-1)})^T \tag{10-20}$$

where $\mathbf{q}_{k,i}$ $(1 \le i \le t-c)$ is the generator (first row) of the circulant $\mathbf{A}_{k,i}$ and $(\mathbf{a}_i^{(l-1)})^T$ is the transpose of $\mathbf{a}_i^{(l-1)}$. In particular, if all the generators $\mathbf{q}_{k,l}$'s have the same weight, saying w, then each term in (10-20) is the sum of w information bits. Note that $y_{k,l}$ is formulated in terms of the left cyclic shifts of the information sections $\mathbf{a}_i$, rather than the right cyclic shifts of the generators used in Section 10.4.1.

The practical implementation for $\mathbf{y}$ can be summarized as the following steps:

Step 1: All the $t-c$ sections of information bits are initially read into the $t-c$ feedback shift registers in one clock cycle.

Step 2: The bits $y_{1,1}, y_{2,1}, \ldots, y_{c,1}$ are calculated by (10-20) with l=1 related to the left cyclic shift of $\mathbf{a}_i$ $(1 \le i \le t-c)$ in zero place. These bits immediately appear at the outputs

of the c banks of XOR gates, which are then shifted into the first group of c buffer registers.

Step 3: For each of the $t-c$ information sections stored in the $t-c$ feedback shift registers, $\mathbf{a}_i$ is cyclically shifted to the left one place corresponding to l=2.

Step 4: By (10-20) the bits $y_{1,2}$, $y_{2,2}$, …, $y_{c,2}$ are obtained, which also appear at the outputs of the c banks of XOR gates and then shifted into the second group of c buffer registers.

The above encoding process in *Step* 3 and 4 is repeated for $b-1$ times, which leads to the determination of all $y_{k,l}$'s for $1\le k\le c$ and $1\le l\le b$. Finally, at the end of the bth clock cycle, all the c sections of $\mathbf{y}$ are stored in the last (bth) group of c buffer registers. Thus, the first stage of encoding is completed, which essentially requires a total of $(t-c)w-1$ XOR gates [107].

The second stage of the encoder

The second stage of encoding is to determine the c parity sections based on $\mathbf{p}_j^T = \mathbf{B}_j\mathbf{y}^T$. This can be also realized by another c banks of XOR gates. The parity-check bits are generated in the similar manner as that the bits of $\mathbf{y}$ vector in the first stage of encoding, where the parity-check bits of each parity section are generated serially one bit at a time simply by cyclically shifting the c buffer registers b times in left. In this way, the number of XOR gates required in each bank is approximately on the order of $cb/2$ [107] by assuming the average row weight of each circulant in $\mathbf{B}_j$ as $b/2$. This

completes the second of the second stage of encoding that finalizes the j th parity section $\mathbf{p}_j$ for $1 \le j \le c$.

10.5. Generator Matrix in Systematic-Circulant Form from in Case II

In this section we will further consider a more complicated case for which $r < cb$, or $r = cb$ and there does not exist a $c \times c$ subarray $\mathbf{D}$ in $\mathbf{H}_{qc}$ with rank r.

10.5.1 Finding the generator matrix

To solve the above problem, we first select the least number of columns of circulants in $\mathbf{H}_{qc}$, denoted by l with $c \le l \le t$, which results in that these l columns of circulants forms a $c \times l$ subarray $\mathbf{D}^*$ with the rank r. Then we permute the columns of circulants of $\mathbf{H}_{qc}$ to form a new $c \times l$ array $\mathbf{H}_{qc}^*$ of circulants so that the last l columns of circulants of $\mathbf{H}_{qc}^*$ forms the array $\mathbf{D}^*$ as

$$\mathbf{D}^* = \begin{bmatrix} \mathbf{A}_{1,t-l+1} & \mathbf{A}_{1,t-l+2} & .... & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,t-l+1} & A_{2,t-l+2} & ... & A_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{c,t-l+1} & A_{c,t-l+2} & ... & A_{c,t} \end{bmatrix} \tag{10-21}$$

Since the rank of the parity-check matrix $\mathbf{H}_{qc}$ is r, thus the generator matrix is a $(tb-r) \times tb$ matrix and we can design it as the following form

$$\mathbf{G}_{qc}^* = \begin{bmatrix} \mathbf{G} \\ \mathbf{Q} \end{bmatrix} \tag{10-22}$$

which consists of two submatrices $\mathbf{G}_{(t-l)b \times tb}$ and $\mathbf{Q}_{(lb-r) \times tb}$.

(a) Determining the submatrix $\mathbf{G}_{(t-l)b \times tb}$: The $\mathbf{G}$ submatrix is a $(t-l) \times t$ array of circulants in the form as

$$\mathbf{G}=\begin{bmatrix} \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{G}_{1,1} & \cdots & \mathbf{G}_{1,l} \\ \mathbf{0} & \mathbf{I} & \cdots & \mathbf{0} & \mathbf{G}_{2,1} & \cdots & \mathbf{G}_{2,l} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{G}_{t-l,1} & \cdots & \mathbf{G}_{t-l,l} \end{bmatrix} \tag{10-23}$$

where $\mathbf{I}$ is a $b\times b$ identity matrix, $\mathbf{0}$ is a $b\times b$ zero matrix, and $\mathbf{G}_{i,j}$ ($1\le i\le t-l$, $1\le j\le l$) is a $b\times b$ circulant. Evidently, $\mathbf{G}$ is in SC form that can be determined by solving (10-7b) by letting $bl-r$ linearly dependent bits in $\mathbf{z}_i=(\mathbf{g}_{i,1}, \mathbf{g}_{i,2}, \ldots, \mathbf{g}_{i,l})$ to zeros, where $g_{i,j}$ is the generator of circulants $\mathbf{G}_{i,j}$. Note that these zero elements are associated with the linearly dependent columns in $\mathbf{D}^*$. In other words, there only has r rather than lb parity-check bits.

(*b*) Determining the submatrix $\mathbf{Q}_{(lb-r)\times tb}$: The submatrix $\mathbf{Q}$ in $\mathbf{G}_{qc}^*$ is an $(lb-r)\times tb$ matrix. In order to guarantee that $\mathbf{G}_{qc}^*$ is a generator matrix of the null space of $\mathbf{H}_{qc}^*$, $\mathbf{Q}$ must satisfy the parity-check condition as

$$\mathbf{H}_{qc}^*\mathbf{Q}^T=\mathbf{0} \tag{10-24}$$

where $\mathbf{0}$ is a $cb\times(lb-r)$ zero matrix.

To find the matrix $\mathbf{Q}$, let d_1, d_2, …, d_l be the numbers of linearly dependent columns in the 1st, 2nd, …, lth columns of circulants in $\mathbf{D}^*$, respectively, such that

$$\sum_{i=1}^{l} d_i = lb-r \tag{10-25}$$

For the cyclic structure of circulants, the last $b-d_i$ columns of the ith column of circulants in $\mathbf{D}^*$ can be treated as linearly independent columns. In other words, the first

d_1, d_2, …, d_l columns of the 1st, 2nd, …, lth columns of circulants in $\mathbf{D}^*$ are linearly dependent. Let the matrix $\mathbf{Q}$ as follows:

$$\mathbf{Q}=\begin{bmatrix} \mathbf{0}_{1,1} & \mathbf{0}_{1,2} & \cdots & \mathbf{0}_{1,t-l} & \mathbf{Q}_{1,1} & \mathbf{Q}_{1,2} & \cdots & \mathbf{Q}_{1,l} \\ \mathbf{0}_{2,1} & \mathbf{0}_{2,2} & \cdots & \mathbf{0}_{2,t-l} & \mathbf{Q}_{2,1} & \mathbf{Q}_{2,2} & \cdots & \mathbf{Q}_{2,l} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{l,1} & \mathbf{0}_{l,2} & \cdots & \mathbf{0}_{l,t-l} & \mathbf{Q}_{l,1} & \mathbf{Q}_{l,2} & \cdots & \mathbf{Q}_{l,l} \end{bmatrix} \tag{10-26}$$

where each $\mathbf{0}_{i,k}$ $(1\le i\le l,\ 1\le k\le t-l)$ is a $d_i\times b$ zero matrix, and $\mathbf{Q}_{i,j}$ is a $d_i\times b$ matrix over GF(2) for $1\le j\le l$. Each nonzero matrix $\mathbf{Q}_{i,j}$ is a partial circulant resulted by cyclically shifting its first row (one place to the right) d_i-1 times to obtain the rest d_i-1 rows. Hence, $\mathbf{Q}$ has a circulant structure. Let the first row of the ith row of submatrices $[\mathbf{0}_{i,1}, \ldots, \mathbf{0}_{i,t-l}, \mathbf{Q}_{i,1}, \ldots, \mathbf{Q}_{i,l}]$ of $\mathbf{Q}$ be $\mathbf{q}_i$=(0, 0, …, 0, $q_{i,1}$, $q_{i,2}$, …, $q_{i,lb}$), where the first $(t-l)b$ bits are zeros, and the remaining $lb-r$ bits in $\mathbf{w}_i$=($q_{i,1}$, $q_{i,2}$, …, $q_{i,lb}$) corresponds to the linearly dependent columns of $\mathbf{D}^*$ in (10-21). Note that $\mathbf{q}_i$ is a codeword a QC-LDPC code defined by parity-check matrix $\mathbf{G}_{qc}^*$. Based on the structure of $\mathbf{w}_i$, the unknown components of $\mathbf{w}_i$ are r, which is the same as the rank $\mathbf{D}^*$. According to (10-24), we have the following check relation for $1\le i\le l$:

$$\mathbf{D}^*\mathbf{w}_i^T=\begin{bmatrix} \mathbf{A}_{1,t-l+1} & \mathbf{A}_{1,t-l+2} & .... & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,t-l+1} & A_{2,t-l+2} & ... & A_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{c,t-l+1} & A_{c,t-l+2} & ... & A_{c,t} \end{bmatrix}\begin{bmatrix} q_{i,1} \\ q_{i,2} \\ \vdots \\ q_{i,lb} \end{bmatrix}=\mathbf{0} \tag{10-27}$$

Hence, $\mathbf{w}_i$ is finalized by finding the solution of (10-27). The l sections of $\mathbf{w}_i$, denoted by $\mathbf{w}_{i,1}$, $\mathbf{w}_{i,2}$, …, $\mathbf{w}_{i,l}$, are obtained with each of them having b consecutive

components of $\mathbf{w}_i$. Finally, $\mathbf{Q}_{i,j}$ $(1 \le j \le l)$ is determined by using $\mathbf{w}_{i,j}$ as the first row and then cyclically shifting it $d_i - 1$ times to get the other $d_i - 1$ rows. Therefore, the submatrix $\mathbf{Q}$ of the generator matrix $\mathbf{G}_{qc}^*$ is found.

10.5.2 Two-stage encoder with parity-check matrix of rank $r \le cb$

Based on the generator matrix $\mathbf{G}_{qc}^*$ derived in last subsection, the whole encoding process can be carried out in two separate stages, which corresponds to two submatrices $\mathbf{G}$ and $\mathbf{Q}$, respectively. The first encoding stage is based on the submatrix $\mathbf{G}$ of $\mathbf{G}_{qc}^*$, which is related to the first $(t-l)b$ bits, denoted by $\mathbf{a}^{(1)}$, of the overall $tb - r$ information bits. The second encoding stage is based on the submatrix $\mathbf{Q}$ of $\mathbf{G}_{qc}^*$, which is related to the last $lb - r$ bits, denoted by $\mathbf{a}^{(2)}$, of all the information bits. Therefore, the encoder first encodes the information bits $[\mathbf{a}^{(1)}, \mathbf{0}_{1\times(lb-r)}]$ into a codeword generated by $\mathbf{G}$, then it encodes the information bits $[\mathbf{0}_{1\times(t-l)b}, \mathbf{a}^{(2)}]$ into another codeword generated by $\mathbf{Q}$. Finally, the codeword with respect to the whole information sequence $\mathbf{a} = [\mathbf{a}^{(1)}, \mathbf{a}^{(2)}]$ is linearly resulted in by adding the two codewords together.

(a) *The first stage of encoder*

The first encoding based on the submatrix $\mathbf{G}$ can be realized in exactly the same way as the two-stage encoding in section 10.4.2, where the rank r of the parity-check matrix $\mathbf{H}_{qc}$ is equal to the number of rows of $\mathbf{H}_{qc}$, cb, and there exists a $c \times c$ subarray $\mathbf{D}$ in $\mathbf{H}_{qc}$ with rank r.

(b) *The second stage of encoder*

To encode the second part $\mathbf{a}^{(2)}$ of the information sequence $\mathbf{a}$ into a codeword resulted by the submatrix $\mathbf{Q}$ of $\mathbf{Q}_{qc}$, we divide $\mathbf{a}^{(2)}$ into l sections, $\mathbf{a}_1^{(2)}$, $\mathbf{a}_2^{(2)}$, …, $\mathbf{a}_l^{(2)}$, with d_1, d_2, …, d_l bits, respectively. Then the codeword $\mathbf{v}^{(2)}$ with respect to $\mathbf{a}^{(2)}$ can be of the form as

$$\mathbf{v}^{(2)}=(\mathbf{0},\ \mathbf{0},\ \ \ \ ,\ \mathbf{0},\ \mathbf{v}_1^{(2)},\ \mathbf{v}_2^{(2)},\ \ldots,\ \mathbf{v}_l^{(2)}) \tag{10-28}$$

which has $t-l$ zero sections and l nonzero sections, $\mathbf{v}_1^{(2)}$, $\mathbf{v}_2^{(2)}$, …, $\mathbf{v}_l^{(2)}$, each section with b bits. The jth nonzero section $\mathbf{v}_j^{(2)}$ is evaluated as

$$\mathbf{v}_j^{(2)}=\mathbf{a}_1^{(2)}\mathbf{Q}_{1,j}+\mathbf{a}_2^{(2)}\mathbf{Q}_{2,j}+\ldots.+\mathbf{a}_l^{(2)}\mathbf{Q}_{l,j} \tag{10-29}$$

Note that each $\mathbf{Q}_{i,j}$ $(1\le i,j\le l)$ in $\mathbf{Q}$ is a partial circulant with d_i rows, the second encoding stage can effectively be realized by *shift-register-adder-accumulator* (SRAA) [107] scheme as discussed in Section 10.4.1.

10.6. Performance of QC-LDPC codes in AWGN channel

The performance of QC-LDPC codes is investigated in this section over an AWGN channel. Two QC-LDPC codes, which are (8176, 7154) and (8176, 7156) codes, respectively, are defined by their generator matrices in SC form from their parity-check matrices using the methods in the previous sections of this chapter. The component circulants are found based on the 3-D Euclidean geometry $EG(3,2^3)$ over $GF(2^3)$. For more details about the Euclidean geometry in mathematics, the reader can refer to [111]. The first QC-LDPC code is design by Li *et al*. [107]. The second QC-LDPC code was constructed by Chen, *et al*. [112] and has been recommended by the NASA for near-earth

high-speed satellite communications and other missions where a bit error rate (BER) below 10^{-10} is required.

The performance of (8176, 7154) irregular QC-LDPC code with BP-based iterative decoding algorithm and BPSK modulation scheme is shown in Fig. 10.2 over an AWGN channel. We can observe that at the BER of 10^{-6}, it is only 1dB away from the ultimate Shannon limit. At the BER of 10^{-9}, the gap is 1.2dB. Note that its BER curve does not exhibit error floor down to the BER of 10^{-9}. It was also reported in [107] that it has no error floor down to the BER of 10^{-10} for a field-programmable gate array (FPGA) decoder implementation.

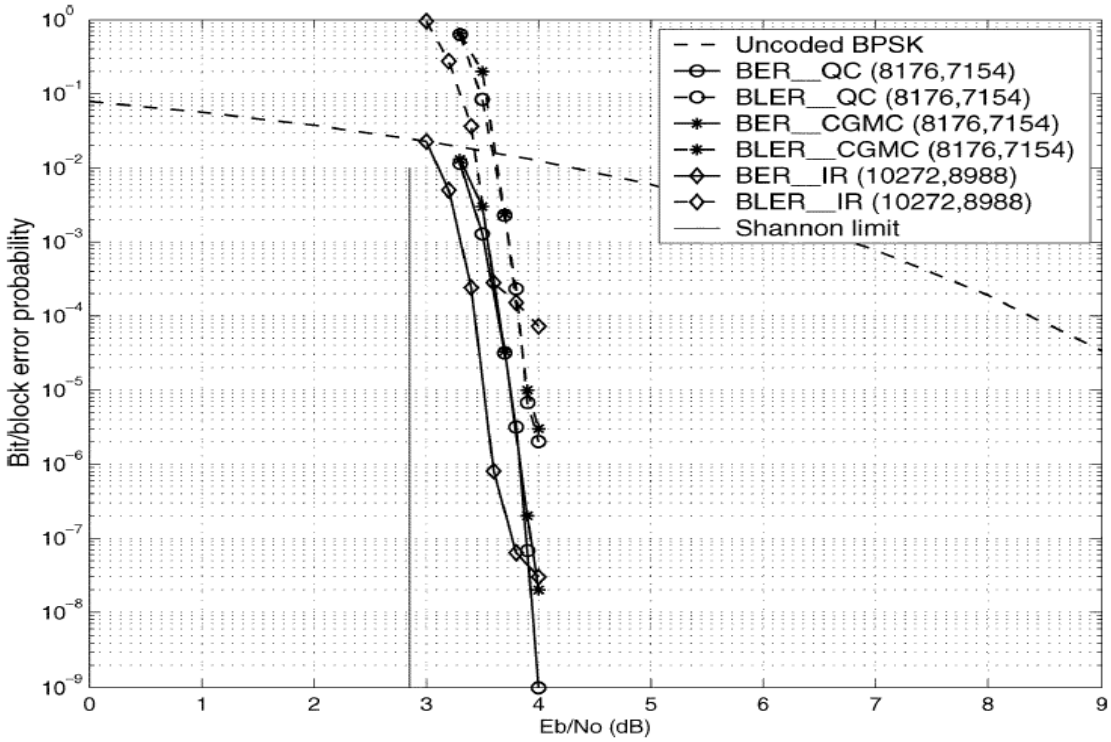

Fig. 10.2. Error performance of the (8176, 7154) irregular QC-LDPC code in an AWGN channel: IR, BER, and BLER represent irregular, bit and block error rates, respectively.

The performance of a computer-generated random MacKay (CGRM) code with the same parameters is also included in Fig. 10.2 for an explicit comparison. It shows that the

constructed QC-LDPC code and the CGRM code have almost the same performance above the BER of 10^{-7}. But the QC-LDPC code outperforms the CGRM code for the BER less than 10^{-7}. We also compare the performance of QC-LDPC code with the irregular LDPC code designed based on degree distributions of its bipartite graph by density evolution [8][9]. Fig. 10.2 demonstrates that the irregular LDPC code gains 0.2dB over the QC-LDPC code above the BER of 10^{-7}. But the QC-LDPC code outperforms the irregular LDPC code below the BER of 10^{-8} since the latter code begins to exhibit the error floor at this critical BER. The iterative decoding of this QC-LDPC code also converges very fast as shown in Fig. 10.3, where the BER difference between 10 and 200 decoding iterations is less than 0.2dB.

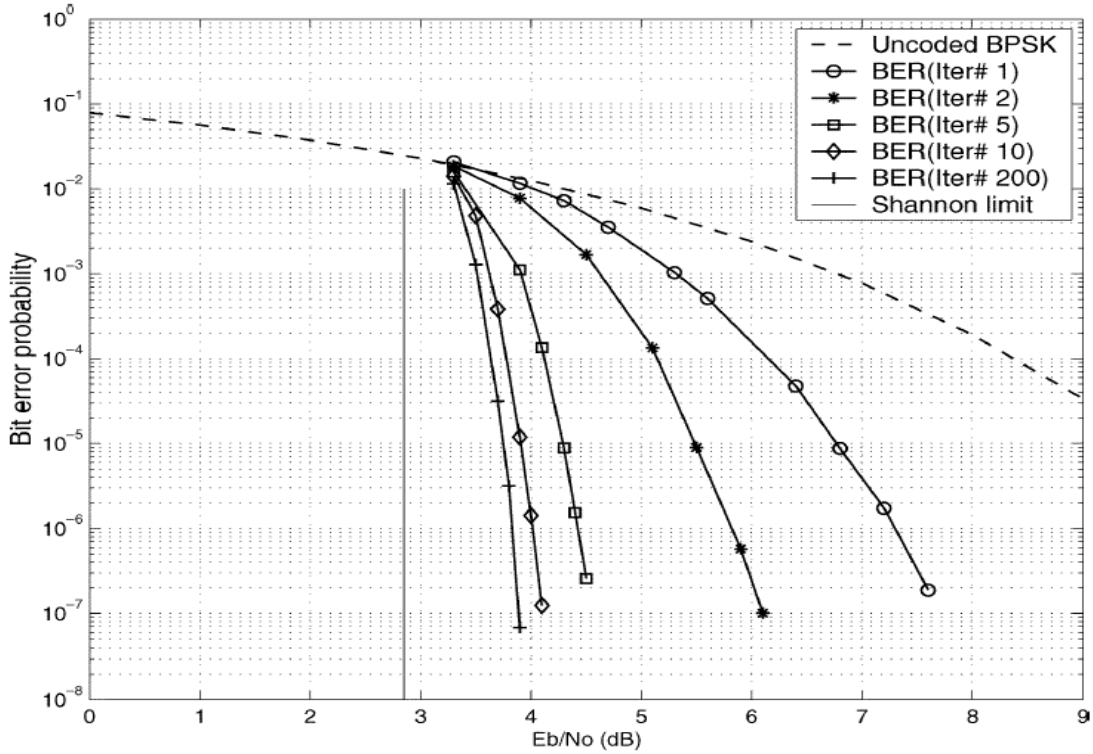

Fig. 10.3. Decoding convergence of the (8176, 7154) irregular QC-LDPC code in an AWGN channel, where the decoding iterations are 1, 2, 5, 10 and 200, respectively.

The performance of (8176, 7156) irregular QC-LDPC code with BP-based iterative decoding algorithm and BPSK modulation scheme is shown in Fig. 10.4 over an AWGN channel. At the BER of 10^{-6}, it performs 1dB from the Shannon limit. Fig. 10.5 also shows that it has no error floor at a BER of 10^{-10}. The decoding of this code also converges very fast. For example, at a BER of 10^{-6}, the difference between 10 and 50 decoding iterations is less than 0.18dB.

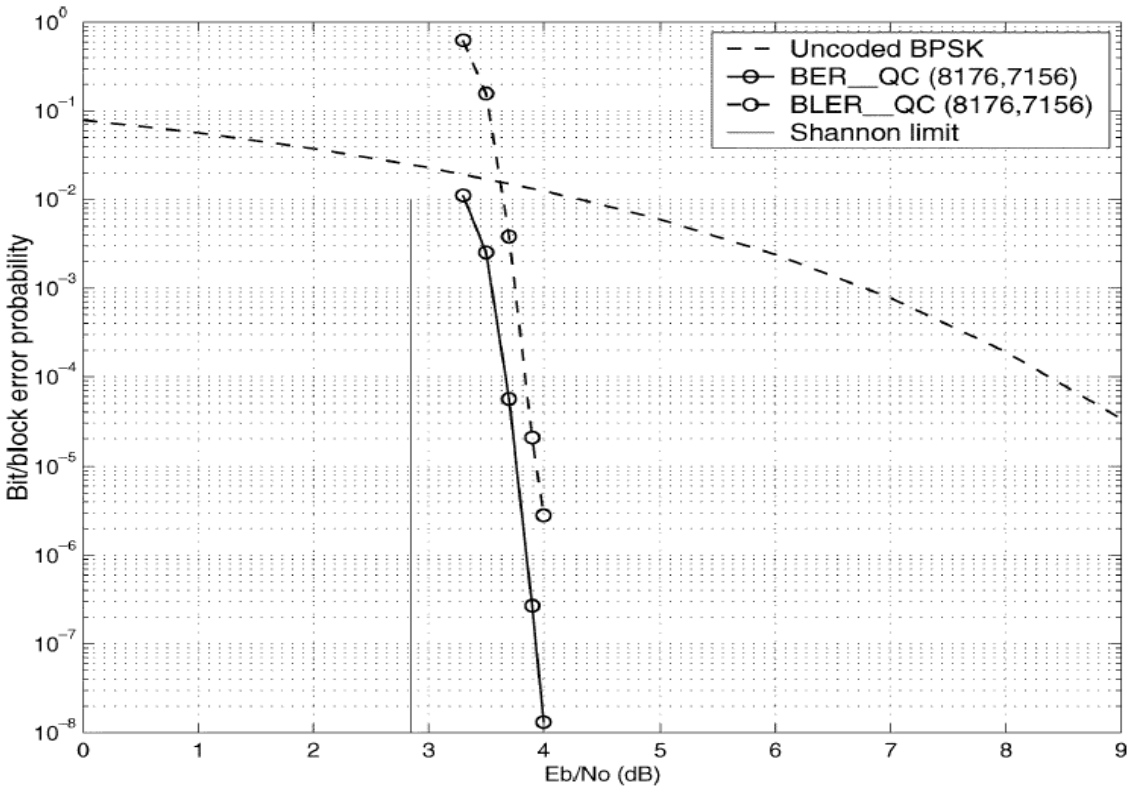

Fig. 10.4. Error performance of the (8176, 7156) irregular QC-LDPC code in an AWGN channel.

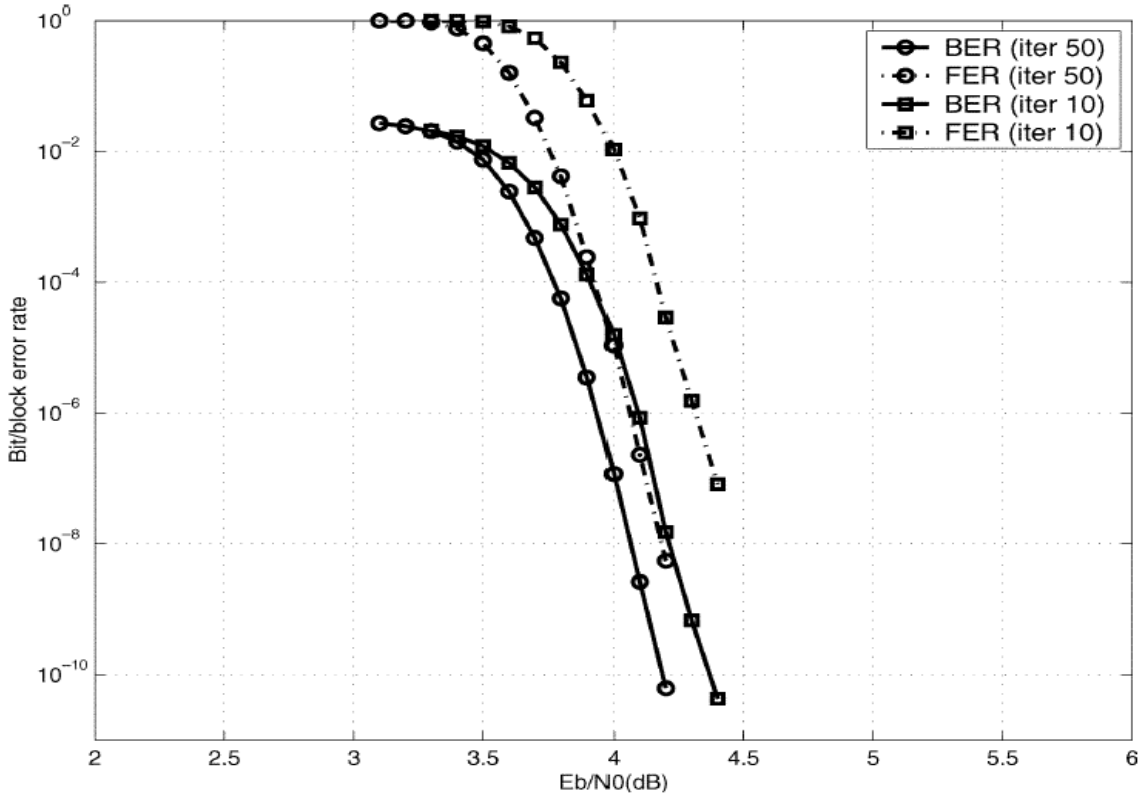

Fig. 10.5. Error performance of the (8176, 7156) irregular QC-LDPC code in an AWGN channel, where the decoding iterations are 10 and 50, respectively.

10.7. Construction of Quasi Cyclic Low-Density Parity-Check Codes Based on Balanced Incomplete Block Designs

10.7.1 Introduction to Balanced Incomplete Block Designs

In this section we will focus on the construction of structured LDPC codes based on a branch in combinatorial mathematics, which is known as balanced incomplete block designs (BIBDs) [118][119][120][122]. An important subject in combinatorial mathematics is the design of experiments, i.e., combinatoric design. The objective of this subject is to design experiments systematically with a view to their statistical analysis. One such design is called BIBD, which was ever employed for constructing block codes

in the early 1970s and later was used in the interleaver design for turbo product code [121].

A binary regular LDPC code defined by its parity-check matrix H based on a special class of BIBDs, which is constructed in this chapter, has the similar structural properties as that for QC-LDPC described in last section, which are categorized as: (1) each row has the weight ρ (d_c) and each column has weight γ (d_v), where ρ and γ are both very small compared to the code length; (2) no two rows (or two columns) have more than one 1-component in common. Hence, property (1) means that H is a sparse parity-check matrix. Property (2) guarantees that the Tanner graph of the code is free of cycles of length 4 and has girth at least 6.

10.7.2 Fundamentals of Balanced Incomplete Block Designs

The mathematical definition of balanced incomplete block design (BIBD) is given as follows:

Definition 10.3: Let $X=\{x_1, x_2, \ldots, x_v\}$ be a set of v objects. A BIBD of X is a collection of n γ-subsets of X, denoted by $B_1, B_2, \ldots, B_n$, called blocks, such that the following conditions are satisfied:

(1) Each object appears in exactly ρ of the n blocks.

(2) Every two objects appear together in exactly λ of the n blocks.

(3) The number of objects in each block γ is very small compared to the total number v of objects in X.

Remarks:

(a) The BIBD is fully characterized by five parameters, i.e., n, v, ρ, γ and λ, simply denoted by (n, v, ρ, γ, λ).

(b) The total number of the γ-blocks designed from the v objects in X is $\binom{v}{\gamma}$, which is greater than n. Thus, in this sense the word "incomplete block design" of BIBD is used to depict this scenario.

An alternative way instead of a list of the blocks to define the BIBD is by a $v \times n$ matrix $\mathbf{Q}=[q_{i,j}]$ over GF(2) that has the following properties:

(1) The rows of $\mathbf{Q}$ correspond to the v objects in X.

(2) The columns of $\mathbf{Q}$ correspond to the n γ-blocks of the design.

(3) The entry $q_{i,j}$ at the ith row and jth column is 1 if and only if the ith object x_i is contained in the jth block B_j of the design, otherwise it is 0.

Note that the matrix $\mathbf{Q}$ is called the incidence matrix of the design, whose row and column weights are ρ and γ, respectively. Any two rows of $\mathbf{Q}$ has exactly λ "1-components" in common.

Example 10.1: Let $X=\{x_1, x_2, \ldots, x_9\}$ be a set of nine objects. The following blocks forms a BIBD for the set X.

$$B_1: x_1, x_2, x_3; \quad B_2: x_4, x_5, x_6; \quad B_3: x_7, x_8, x_9;$$

$$B_4: x_1, x_4, x_7; \quad B_5: x_2, x_5, x_8; \quad B_6: x_3, x_6, x_9;$$

$$B_7: x_1, x_5, x_9; \quad B_8: x_2, x_6, x_7; \quad B_9: x_3, x_4, x_8;$$

$$B_{10}: x_1, x_6, x_8; \quad B_{11}: x_2, x_4, x_9; \quad B_{12}: x_3, x_5, x_7;$$

Every block consists of three objects (γ=3), each object appears in four blocks (ρ=4), and every two objects appear together in exactly one block, i.e., λ=1. The incidence matrix $\mathbf{Q}_{9\times12}$ of this BIBD is given as follows:

$$\mathbf{Q}_{9\times12}=\begin{bmatrix}1&0&0&1&0&0&1&0&0&1&0&0\\1&0&0&0&1&0&0&1&0&0&1&0\\1&0&0&0&0&1&0&0&1&0&0&1\\0&1&0&1&0&0&0&0&1&0&1&0\\0&1&0&0&1&0&1&0&0&0&0&1\\0&1&0&0&0&1&0&1&0&1&0&0\\0&0&1&1&0&0&0&1&0&0&0&1\\0&0&1&0&1&0&0&0&1&1&0&0\\0&0&1&0&0&1&1&0&0&0&1&0\end{bmatrix} \tag{10-30}$$

The above BIBD is simply denoted by (12, 9, 4, 3, 1). □

Example 10.2: Let $X=\{x_1, x_2, \ldots, x_{15}\}$ be a set of fifteen objects. The following blocks forms a BIBD for the set X.

B_1: x_1, x_2, x_3, x_4, x_5, x_6, x_7; B_2: x_1, x_2, x_3, x_8, x_9, x_{10}, x_{11};

B_3: x_1, x_2, x_3, x_{12}, x_{13}, x_{14}, x_{15}; B_4: x_1, x_4, x_5, x_8, x_9, x_{12}, x_{13};

B_5: x_1, x_4, x_5, x_{10}, x_{11}, x_{14}, x_{15}; B_6: x_1, x_6, x_7, x_8, x_9, x_{14}, x_{15};

B_7: x_1, x_6, x_7, x_{10}, x_{11}, x_{12}, x_{13}; B_8: x_2, x_4, x_6, x_8, x_{10}, x_{12}, x_{14};

B_9: x_2, x_4, x_7, x_8, x_{11}, x_{13}, x_{15}; B_{10}: x_2, x_5, x_6, x_9, x_{11}, x_{12}, x_{15};

B_{11}: x_2, x_5, x_7, x_9, x_{10}, x_{13}, x_{14}; B_{12}: x_3, x_4, x_6, x_9, x_{11}, x_{13}, x_{14};

B_{13}: x_3, x_4, x_7, x_9, x_{10}, x_{12}, x_{15}; B_{14}: x_3, x_5, x_6, x_8, x_{10}, x_{13}, x_{15};

B_{15}: x_3, x_5, x_7, x_8, x_{11}, x_{12}, x_{14};

Every block consists of seven objects (γ=7), each object appears in seven blocks (ρ=7), and every two objects appear together in exactly three of the total blocks, i.e., λ=3. The incidence matrix $\mathbf{Q}_{15\times15}$ of this BIBD is expressed as follows:

$$\mathbf{Q}_{15\times15}=\begin{bmatrix}
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&1&1&1&1\\
1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
1&0&0&1&1&0&0&0&0&1&1&0&0&1&1\\
1&0&0&0&0&1&1&1&0&1&0&1&0&1&0\\
1&0&0&0&0&1&1&0&1&0&1&0&1&0&1\\
0&1&0&1&0&1&0&1&1&0&0&0&0&1&1\\
0&1&0&1&0&1&0&0&0&1&1&1&1&0&0\\
0&1&0&0&1&0&1&1&0&0&1&0&1&1&0\\
0&1&0&0&1&0&1&0&1&1&0&1&0&0&1\\
0&0&1&1&0&0&1&1&0&1&0&0&1&0&1\\
0&0&1&1&0&0&1&0&1&0&1&1&0&1&0\\
0&0&1&0&1&1&0&1&0&0&1&1&0&0&1\\
0&0&1&0&1&1&0&0&1&1&0&0&1&1&0
\end{bmatrix} \tag{10-31}$$

The above BIBD is denoted by (15, 15, 7, 7, 3). □

We can easily draw the conclusions that are stated in the following theorem:

Theorem 10.1: A BIBD (n, v, ρ, γ, λ) must satisfy the requirements as

$$n\gamma=\rho v \tag{10-32a}$$

$$\rho(\gamma-1)=\lambda(v-1) \tag{10-32b}$$

The proof is straightforward. □

The reader can easily check the relationships in (10-32a) and (10-32b) by using the parameters of the two BIBDs as give in the last two examples. The next example is concerned with a special BIDB with a circulant incidence matrix.

Example 10.3: Let $X=\{x_1,\ x_2,\ \ldots,\ x_7\}$ be a set of seven objects. The following blocks form a BIBD for the set X.

$$B_1:\ x_1,\ x_2,\ x_4;\quad B_2:\ x_2,\ x_3,\ x_5;\quad B_3:\ x_3,\ x_4,\ x_6;$$

$$B_4:\ x_4,\ x_5,\ x_7;\quad B_5:\ x_5,\ x_6,\ x_1;\quad B_6:\ x_6,\ x_7,\ x_2;$$

$$B_7:\ x_7,\ x_1,\ x_3;$$

Every block consists of three objects ($\gamma=3$), each object appears in three blocks ($\rho=3$), and every two objects appear together in exactly one blocks, i.e., $\lambda=1$. Interestingly, the incidence matrix $\mathbf{Q}_{7\times7}$ of this BIBD is circulant and given as follows:

$$\mathbf{Q}_{7\times7}=\begin{bmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix} \tag{10-33}$$

The above BIBD is denoted by (7, 7, 3, 3, 1). Note that each row of $\mathbf{Q}_{7\times7}$ is a cyclic right -shift of the row just above it and the first row is the cyclic shift of the last row. Also, each column is downward cyclic shift of the column on its left and the first column is the downward cyclic shift of the last column. Evidently, $\mathbf{Q}_{7\times7}$ is a square circulant matrix (circulant) of rank 4. □

Remark:

(1) For a BIBD with $\lambda=1$, its incidence matrix $\mathbf{Q}$ has the structural properties of the parity-check matrix of a regular LDPC codes whose Tanner graph has girth at least 6.

Thus, the null space of $\mathbf{Q}$ gives a (γ, ρ)-regular LDPC code, called a BIBD-*LDPC* code. This kind of special BIBD is very important in the design of regular LDPC codes.

(2) Let $\mathbf{Q}^*$ be a submatrix of $\mathbf{Q}$ corresponding to a BIBD with λ=1. If $\mathbf{Q}^*$ has constant row and column weights, then the null space of $\mathbf{Q}^*$ also results in a regular LDPC code with girth at least 6 because $\mathbf{Q}^*$ is related to another BIBD with λ=1. thus, a proper section of a submatrix of $\mathbf{Q}$ also gives a regular LDPC code.

Example 10.4: Consider the BIBD of seven objects given in Example 10-3. The rank of the incidence matrix $\mathbf{Q}_{7\times7}$ of the BIBD is 4. Hence, the null space of $\mathbf{Q}_{7\times7}$ results in a regular (7, 3) LDPC code. We can easily check that a zero vector is resulted by adding columns 1, 2 3 and 6 together. Therefore, the minimum distance is exactly 4. The reader can further prove that this LDPC code is also a cyclic code by finding the generator matrix $\mathbf{G}_{3\times7}$ from $\mathbf{Q}_{7\times7}$. □

10.7.3 Three Classes Bose Designs

Combinatoric design is one of the old and rich subjects in combinatory mathematics. For years, many BIBDs have been constructed by various design methods [119][120]. In this section we only deal with several special classes of BIBDs with λ=1, which was constructed by R. C. Bose using the method of symmetrically repeated differences [118]. The design of BIBDs is based on the Abelian group of finite fields.

Preliminaries:

Let $G=\{x^{(i)}: 1\le i\le k\}$ be an additive Abelian group of order k. For each element $x^{(i)}$ in G, we repeat it q times and label them as $x_1^{(i)}$, $x_2^{(i)}$, …., $x_q^{(i)}$. This leads to a set X

of kq symbols (objects) related to the group G. The symbols in X is partitioned into q classes. The j th $(1 \le j \le q)$ class is

$$G_j = \{ x_j^{(1)},\ x_j^{(2)},\ \ldots.,\ x_j^{(k)} \} \tag{10-34}$$

Evidently, $G_j = G$ due to G_j as the j th repetition of G.

Let $B = \{ x_{j_1}^{(i_1)},\ x_{j_2}^{(i_2)},\ \ldots.,\ x_{j_\gamma}^{(i_\gamma)} \}$ $(1 \le j_1,\ j_2,\ \ldots,\ j_\gamma \le q$ and $1 \le i_1,\ i_2,\ \ldots,\ i_\gamma \le k)$ be a γ-subset of X, called a block. We can form $\gamma(\gamma - 1)$ differences in the following form in block B.

$$x_{j_a}^{(i_b)} - x_{j_c}^{(i_d)} = \left(x^{(i_b)} - x^{(i_d)} \right)_{j_a j_c} \tag{10-35}$$

Note that the difference is carried out under the group addition and called a difference of type $j_a j_c$. More specially, it is called pure if $j_a = j_c$, otherwise it is called mixed.

Example 10.5: Consider a Abelian group $G = \{0, 1, 2, 3, 4\}$ under modulo-5 addition. If a is an element in G, then a and $5 - a$ are additive inverses to each other. Let $q = 2$. Repeating each element in G twice, we form the set X of 10 objects as follows:

$$X = \{ 0_1,\ 0_2,\ 1_1,\ 1_2,\ 2_1,\ 2_2,\ 3_1,\ 3_2,\ 4_1,\ 4_2 \} \tag{10-36}$$

Consider the block $B = \{ 0_1,\ 2_2,\ 3_2 \}$ of three objects. The following differences are calculated as

$$0_1 - 2_2 = 0_1 + 3_2 = 3_{12},\ \ 2_2 - 0_1 = 2_{21},\ \ 0_1 - 3_2 = 0_1 + 2_2 = 2_{12}$$

$$3_2 - 0_1 = 3_{21},\ \ 2_2 - 3_2 = 2_2 + 2_2 = 4_{22},\ \ 3_2 - 2_2 = 1_{22} \tag{10-37}$$

Evidently, there are two pure differences, i.e., 4_{22} and 1_{22}, and four mixed differences, i.e., 3_{12}, 2_{21}, 2_{12}, and 3_{21}. □

Definition 10.4: If in s blocks every pure difference except 0 is repeated λ times and every mixed difference is also repeated λ times, then the differences are said *symmetrically repeated*.

Bose [118] presented several ways for the design of BIBDs based on the two theorems given below:

Theorem 10.2: Let $G=\{x^{(i)}: 1\le i\le k\}$ be an additive Abelian group of order k. A set X of kq symbols is formed by repeating each element in G q times. Partition the kq symbols into q classes as given by (10-34). Suppose s γ-subsets (blocks) B_1, B_2, …, B_s of X are chosen such that:

(1) among the γs symbols in the s blocks, exactly ρ symbols belong to each of the q classes;

(2) the differences formed from the symbols in the s blocks are symmetrically repeated, each occurring λ times.

Then by adding each element of G in turn to each of the blocks B_1, B_2, …, B_s, we obtain a BIBD with parameters $v=kq$, $n=ks$, γ, ρ and λ. The blocks B_1, B_2, …, B_s are called the *base blocks*. □

For the proof of the theorem, the reader can refer to the original Bose design [118].

Example 10.6: Let $G=\{0, 1, 2, 3, 4, 5, 6\}$ be the Abelian group under modulo-7 addition. Let $q=1$. Then $X=G$. Let $\gamma=3$ and $s=1$. Suppose we select the block $B=\{0, 1, 3\}$. It can be easily check that B satisfies the conditions as given in Theorem 10.2. Adding each element of G in turn to B, it results in the following seven blocks:

$$B_1=0+B=\{0, 1, 3\},\quad B_2=1+B=\{1, 2, 4\},\quad B_3=2+B=\{2, 3, 5\}$$

$$B_4=3+B=\{3, 4, 6\},\quad B_5=4+B=\{4, 5, 0\},\quad B_6=5+B=\{5, 6, 1\}$$

$$B_7=6+B=\{6, 0, 2\} \tag{10-38}$$

Evidently, they form a BIBD of seven objects with parameters $v=kq=7$, $n=ks=7$, $\gamma=3$, $\rho=3$ and $\lambda=1$, which is the same BIBD as given in Example 10.3. □

Theorem 10.3: Let X be the set of kq symbols associated to the additive Abelian group G as defined in Theorem 10.2. Partition X into q classes as given in (10-34). Adjoin to X a new symbol, denoted ∞. Suppose $(s+e)$ γ-subsets B_1, B_2, …, B_s, D_1, D_2, …, D_e of $X\cup\{\infty\}$ are chosen such that:

(1) each of the s blocks B_1, B_2, …, B_s contains only symbols from X, and each of the e blocks D_1, D_2, …, D_e contains the symbol ∞ together with symbols form X;

(2) among the γs symbols of X in B_1, B_2, …, B_s, exactly $ke-\gamma$ of them belong to each of the q classes of X, and among the $(\gamma-1)e$ symbols of X in D_1, D_2, …, D_e, exactly λ of them belong to each of the q classes of X;

(3) the differences formed from the symbols of X in the $s+e$ blocks are symmetrically repeated, each occurring λ times.

Then by adding each element of G in turn to each of the blocks B_1, B_2, …, B_s, D_1, D_2, …, D_e with $\infty+x=\infty$ we obtain a BIBD with parameters $v=kq+1$, $n=k(s+e)$, $\rho=ke$, ρ and λ. The blocks B_1, …, B_s, D_1, …, D_e are called the *base blocks*. □

The reader can refer to [118] for the proof of the theorem.

Bose [118][122] had developed several effective methods in design of BIBDs with various $\lambda's$. Here we only concentrate on BIBDs with $\lambda=1$ for construction of LDPC codes. In this section three classes of Bose designs with $\gamma=4$ or 5 and $\lambda=1$ by the Abelian groups of finite fields are introduced. BIBDs designed by the finite field $GF(p^m)$, where p is a prime, have cyclic (or circulant) structure due to the fact the p^m elements of $GF(p^m)$ forms an additive Abelian group under its addition operation and the p^m-1 nonzero elements form a multiplicative group (or cyclic group) under multiplication.

Case-I Bose Designs

In this part of this section we present two types of class-I BIBD designs, which are both based on Theorem 10.2 and the additive and cyclic groups of finite fields.

(1) *Type-1 Designs*: Let t be a positive integer such that $12t+1$ is a power of a prime. There exists a Galois field $GF(12t+1)$ with $12t+1$ elements. Suppose $GF(12t+1)$ has a primitive element x such that $x^{4t}-1=x^c$, where c is an odd integer less than $12t+1$. Then we have a BIBD with parameters $v=12t+1$, $n=t(12t+1)$, $\gamma=4$, $\rho=4t$ and $\lambda=1$, which is formed by the following t base blocks

$$B_i=\{0,\ x^{2i},\ x^{2i+4t},\ x^{2i+8t}\} \tag{10-39}$$

for $0\le i<t$. By adding each element of the finite field $GF(12t+1)$ in turn to the elements in B_i, it results in $12t+1$ blocks. Finally, we obtain the BIBD of $t(12t+1)$ blocks. The incidence matrix $\mathbf{Q}$ is a $(12t+1)\times[t(12t+1)]$ matrix. We can put it in cyclic form [122] in a row of circulants as follows:

$$\mathbf{Q}=[\mathbf{Q}_1, \mathbf{Q}_2, ..., \mathbf{Q}_t] \tag{10-40}$$

where the ith circulant $\mathbf{Q}_i$ is a $(12t+1)\times(12t+1)$ incidence matrix consisting of $12t+1$ blocks constructed by adding each element in $GF(12t+1)$ to the elements of the ith base block B_i. This leads to the fact that the row and column weights are $4t$ and 4, respectively. The rank of $\mathbf{Q}$ (or a circulant $\mathbf{Q}_i$) is $12t$ [122].

Example 10.7: Let t=1. Then $12t$+1=13, which is prime. Evidently, the element 6 of $GF(13)$={0, 1, 2, …, 12} is a primitive element. It can be checked easily that for x=6, $x^4-1=x^3 \pmod{13}$. Hence, c=3. Based on the principle of Type-1 designs, the only base block is $\{0, 6^0, 6^4, 6^8\}$={0, 1, 9, 3}. There exists a BIBD by adding each element in $GF(13)$ to the elements of the base block, which results in 13 blocks as follows:

$$\begin{aligned}&\{0, 1, 9, 3\}, \{1, 2, 10, 4\}, \{2, 3, 11, 5\}, \{3, 4, 12, 6\}, \{4, 5, 0, 7\}\\ &\{5, 6, 1, 8\}, \{6, 7, 2, 9\}, \{7, 8, 3, 10\}, \{8, 9, 4, 11\}, \{9, 10, 5, 12\}\\ &\{10, 11, 6, 0\}, \{11, 12, 7, 1\}, \{12, 0, 8, 2\}\end{aligned} \tag{10-41}$$

The incidence matrix $\mathbf{Q}_{13\times13}$ of this BIBD is

$$\mathbf{Q}_{13\times13}=\begin{bmatrix}1&0&0&0&1&0&0&0&0&0&1&0&1\\1&1&0&0&0&1&0&0&0&0&0&1&0\\0&1&1&0&0&0&1&0&0&0&0&0&1\\1&0&1&1&0&0&0&1&0&0&0&0&0\\0&1&0&1&1&0&0&0&1&0&0&0&0\\0&0&1&0&1&1&0&0&0&1&0&0&0\\0&0&0&1&0&1&1&0&0&0&1&0&0\\0&0&0&0&1&0&1&1&0&0&0&1&0\\0&0&0&0&0&1&0&1&1&0&0&0&1\\1&0&0&0&0&0&1&0&1&1&0&0&0\\0&1&0&0&0&0&0&1&0&1&1&0&0\\0&0&1&0&0&0&0&0&1&0&1&1&0\\0&0&0&1&0&0&0&0&0&1&0&1&1\end{bmatrix} \tag{10-42}$$

Thus, the parameters of Type-1 BIBD are $v=13$, $n=13$, $\gamma=4$, $\rho=4$ and $\lambda=1$, respectively. □

(2) *Type-2 Designs*: Let t be a positive integer such that $20t+1$ is a power of a prime. Suppose $GF(20t+1)$ has a primitive element x such that $x^{4t}+1=x^{c}$, where c is a positive odd integer less than $20t+1$. Then we obtains a BIBD for a set of $20t+1$ objects with parameters $v=20t+1$, $n=t(20t+1)$, $\gamma=5$, $\rho=5t$ and $\lambda=1$, which is constructed by the t base blocks as follows

$$B_i=\{x^{2i},\ x^{2i+4t},\ x^{2i+8t},\ x^{2i+12t},\ x^{2i+16t}\} \tag{10-43}$$

for $0\le i<t$. The incidence matrix $\mathbf{Q}$ of this design is a $(20t+1)\times[t(20t+1)]$ matrix. Similar as (10-40) for *Type-1 designs*, $\mathbf{Q}$ can be written in cyclic form in a row of circulants, where the ith circulant $\mathbf{Q}_i$ is a $(20t+1)\times(20t+1)$ incidence matrix having $20t+1$ blocks formed by adding each element in $GF(20t+1)$ to the elements of the ith base block B_i. Thus, the row and column weights of the resulted matrix $\mathbf{Q}$ are $5t$ and 5, respectively.

Case-II Bose Designs

This class of BIBD designs is designed based on Theorem 10.3. Let t be a positive integer such that $4t+1$ is a power of a prime. Suppose each element of the Galois field $GF(4t+1)$ is repeated three times ($q=3$). We obtain a set X of $3(4t+1)$ symbols. Adjoin to X the symbol ∞. Based on Theorem 10.3 with $s=3t$ and $e=1$ there exists a BIBD for the set $X\cup\{\infty\}$ of $12t+4$ objects, which has the parameters $v=12t+4$, $n=$

$(3t+1)(4t+1)$, γ=4, $\rho=4t+1$ and λ=1. Let x be a primitive element in GF($4t$+1) that satisfies the requirement

$$(x^c+1)/(x^c-1)=x^d \tag{10-44}$$

where c and d are two odd integers. Then the base blocks for the BIBD design are

$$\{x_1^{2i},\ x_1^{2i+2t},\ x_2^{2i+c},\ x_2^{2i+2t+c}\},\{x_2^{2i},\ x_2^{2i+2t},\ x_3^{2i+c},\ x_3^{2i+2t+c}\}$$

$$\{x_3^{2i},\ x_3^{2i+2t},\ x_1^{2i+c},\ x_1^{2i+2t+c}\},\{\infty,\ 0_1,\ 0_2,\ 0_3\} \tag{10-45}$$

for $0\le i<t$. Suppose the symbols in $X\cup\{\infty\}$ is ordered by

$$\{0_1,\ 1_1,\ \ldots,\ (k-1)_1,\ 0_2,\ 1_2,\ \ldots,\ (k-1)_2,\ \ldots,\ 0_q,\ 1_q,\ \ldots,\ (k-1)_q,\ \infty\} \tag{10-46}$$

where $k=4t+1$. Thus, based on the above arrangement the incidence matrix $\mathbf{Q}$ of a Class-II Bose-BIBD can be written in the following form:

$$\mathbf{Q}=\begin{bmatrix}\mathbf{M} & \mathbf{O} & \mathbf{C} & \mathbf{I}\\ \mathbf{C} & \mathbf{M} & \mathbf{O} & \mathbf{I}\\ \mathbf{O} & \mathbf{C} & \mathbf{M} & \mathbf{I}\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{z}\end{bmatrix} \tag{10-47}$$

where $\mathbf{M}=[\mathbf{M}_1,\ \mathbf{M}_2,\ \ldots,\ \mathbf{M}_t]$ and $\mathbf{C}=[\mathbf{C}_1,\ \mathbf{C}_2,\ \ldots,\ \mathbf{C}_t]$, $\mathbf{M}_i$ and $\mathbf{C}_i$ are two $(4t+1)\times(4t+1)$ circulants for the partial blocks formed by adding each element of GF($4t$+1) in turn to the first and last two elements of the ith base block B_i, respectively, $\mathbf{O}$ is a $(4t+1)\times t(4t+1)$ zero matrix, $\mathbf{I}$ is a $(4t+1)\times(4t+1)$ identity matrix, $\mathbf{z}$ and $\mathbf{0}$ are two row vectors with $(4t+1)$ "ones" and $t(4t+1)$ "zeros", respectively. The row and column weights of $\mathbf{M}_i$ and $\mathbf{C}_i$ are both 2. Hence, the row and column weights of $\mathbf{Q}$ are $4t+1$ and 4, respectively. The rank of $\mathbf{Q}$ is $12t+1$.

Case-III Bose Designs

Let t be a positive integer such that $4t+1$ is a power of a prime. Each element of the Galois field $GF(4t+1)$ is repeated five times (q=5) so that it leads to a set X of $5(4t+1)$ symbols. Let x be a primitive element in GF($4t$+1) that satisfies the condition $(x^c+1)/(x^c-1)=x^d$ where c and d are two positive odd integers. Based on Theorem 10.2, we obtain a BIBD for the set X with the parameters $v=20t+5$, $n=(5t+1)(4t+1)$, γ=5, $\rho=5t+1$ and λ=1. The base blocks for this design are

$$\{x_1^{2i},\ x_1^{2i+2t},\ x_3^{2i+c},\ x_3^{2i+2t+c},\ 0_2\},\{x_2^{2i},\ x_2^{2i+2t},\ x_4^{2i+c},\ x_4^{2i+2t+c},\ 0_3\}$$

$$\{x_3^{2i},\ x_3^{2i+2t},\ x_5^{2i+c},\ x_5^{2i+2t+c},\ 0_4\},\{x_4^{2i},\ x_4^{2i+2t},\ x_1^{2i+c},\ x_1^{2i+2t+c},\ 0_5\}$$

$$\{x_5^{2i},\ x_5^{2i+2t},\ x_2^{2i+c},\ x_2^{2i+2t+c},\ 0_1\},\{0_1,\ 0_2,\ 0_3,\ 0_4,\ 0_5\} \qquad (10\text{-}48)$$

for $0\le i<t$. Similarly, we arrange the symbols of X in the following order without the symbol ∞

$$\{0_1,\ 1_1,\ \ldots,\ (k-1)_1,\ 0_2,\ 1_2,\ \ldots,\ (k-1)_2,\ \ldots,\ 0_q,\ 1_q,\ \ldots,\ (k-1)_q\} \qquad (10\text{-}49)$$

where $k=4t+1$. The incidence matrix $\mathbf{Q}$ of a Class-III Bose-BIBD can be expressed in the form as

$$\mathbf{Q}=\begin{bmatrix}\mathbf{M} & \mathbf{O} & \mathbf{O} & \mathbf{C} & \mathbf{D} & \mathbf{I}\\ \mathbf{D} & \mathbf{M} & \mathbf{O} & \mathbf{O} & \mathbf{C} & \mathbf{I}\\ \mathbf{C} & \mathbf{D} & \mathbf{M} & \mathbf{O} & \mathbf{O} & \mathbf{I}\\ \mathbf{O} & \mathbf{C} & \mathbf{D} & \mathbf{M} & \mathbf{O} & \mathbf{I}\\ \mathbf{O} & \mathbf{O} & \mathbf{C} & \mathbf{D} & \mathbf{M} & \mathbf{I}\end{bmatrix} \qquad (10\text{-}50)$$

where $\mathbf{M}=[\mathbf{M}_1,\ \mathbf{M}_2,\ \ldots,\ \mathbf{M}_t]$ and $\mathbf{C}=[\mathbf{C}_1,\ \mathbf{C}_2,\ \ldots,\ \mathbf{C}_t]$, $\mathbf{M}_i$ and $\mathbf{C}_i$ are two $(4t+1)\times(4t+1)$ circulants for the partial blocks formed by adding each element of GF($4t$+1) in turn to the first and second two elements of the ith base block B_i, respectively, $\mathbf{O}$ is a

$(4t+1)\times t(4t+1)$ zero matrix, $\mathbf{I}$ is a $(4t+1)\times(4t+1)$ identity matrix corresponding to the base block $\{0_1, 0_2, 0_3, 0_4, 0_5\}$, the submatrix $\mathbf{D}$ as a row of t identity matrices $\mathbf{I}$'s is related to the symbol 0_i in each base block. The row and column weights of $\mathbf{M}_i$ and $\mathbf{C}_i$ are both 2. Hence, the row and column weights of $\mathbf{Q}$ are $5t+1$ and 5, respectively.

10.7.4 Construction and Performance of QC-BIBD-LDPC Codes Based on Bose Designs

In this section QC-LDPC codes are effectively designed based on three classes of BIBDs with $\lambda=1$ introduced in last section, and their performance is also studied by simulations. This kind of LDPC codes are called BIBD-LDPC codes whose Tanner graphs have girths at least 6.

Class-I BIBD-LDPC Codes

The incidence matrix $\mathbf{Q}$ of a class-I Bose-BIBD consists of a row of t circulants $\mathbf{Q}_1$, $\mathbf{Q}_2$, …, $\mathbf{Q}_t$. For $1\le m\le t$, we have the following matrix:

$$\mathbf{H}^{(1)}[m]=[\mathbf{Q}_1, \mathbf{Q}_2, ..., \mathbf{Q}_m] \tag{10-51}$$

Evidently, $\mathbf{H}^{(1)}[m]$ can be viewed as a parity-check matrix of a regular LDPC code since it satisfies all the required structural properties. For a Type-1 design, $\mathbf{H}^{(1)}[m]$ is a $(12t+1)\times m(12t+1)$ matrix with row and column weights $4m$ and 4, respectively. A BIBD-LDPC code of length $N=m(12t+1)$ is resulted as the null space of $\mathbf{H}^{(1)}[m]$, whose code rate is

$$r=1-\frac{12t}{N}\approx 1-\frac{1}{m}=\frac{m-1}{m} \tag{10-52}$$

The constructed LDPC code is a QC-LDPC code since $\mathbf{H}^{(1)}[m]$ consists of a row of circulants $\mathbf{Q}_i$ $(1 \le i \le m)$. For a Type-2 design, $\mathbf{H}^{(1)}[m]$ is a $(20t+1) \times m(20t+1)$ matrix with row and column weights $5m$ and 5, respectively. Hence, the null space of $\mathbf{H}^{(1)}[m]$ gives a QC-BIBD-LDPC code of length $N = m(20t+1)$. Consequently, for m=1, 2, …, t, we can construct a sequence of QC-BIBD-LDPC codes with various lengths and rates.

Example 10.8: Consider a Type-1 Class-I Bose-BIBD. The design has the following five parameters for t=15: $v = 12t+1$=181, $n = t(12t+1)$=2715, γ=4, $\rho = 4t$=60, and λ=1. The incidence matrix has 15 181×181 circulants, $\mathbf{Q}_1$, $\mathbf{Q}_2$, …, $\mathbf{Q}_{15}$.

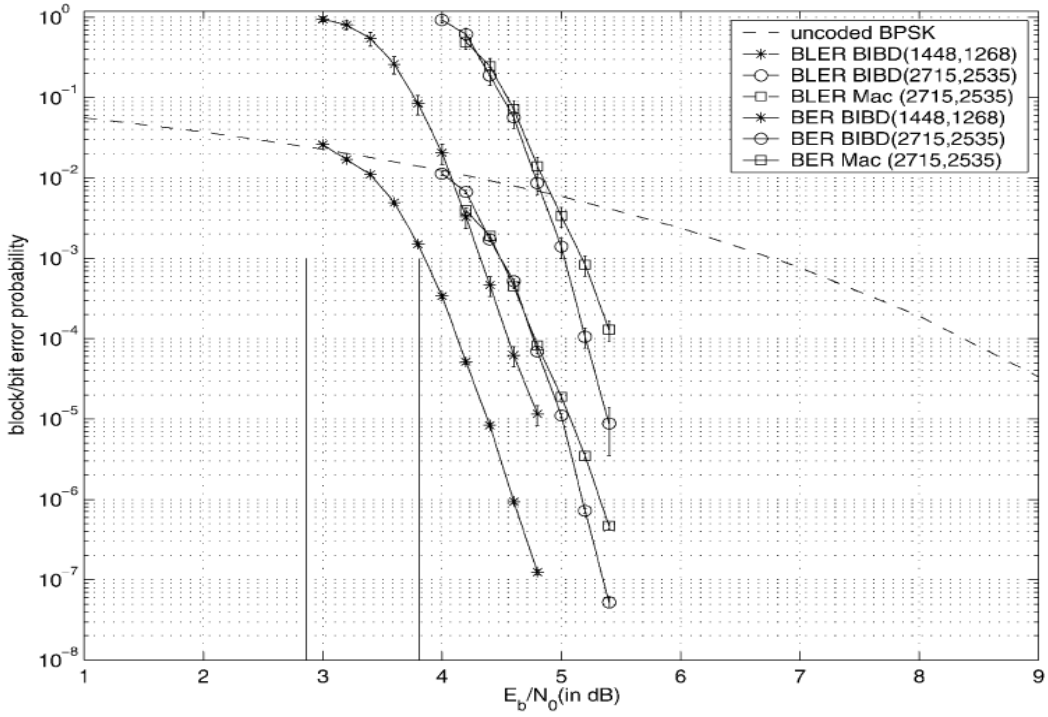

Fig. 10.6. Error performance of the regular (1448, 1268) and (2715, 2535) QC Class-I (Type-1) BIBD-LDPC codes, and the random (2715, 2535) regular LDPC code (MacKay code, denoted by "Mac") in an AWGN channel, where the block error rate is denoted by "BLER".

(a) m=8: It results in a 181×1448 parity-check matrix $\mathbf{H}^{(1)}[8]=[\mathbf{Q}_1, \mathbf{Q}_2, ..., \mathbf{Q}_8]$ whose row and column weights are 32 and 4, respectively. The null space of $\mathbf{H}^{(1)}[8]$ is a (1448, 1268)

regular QC-LDPC code with rate 7/8=0.875. In decoding codes given in this and other examples in this section using BP algorithm, the number of iterations is 100. The performance [122] of this code is shown in Fig. 10.6, which has 1.7dB gap from the Shannon limit at the BER of 10^{-6}.

(b) m=15: We obtain a (2715, 2535) regular QC-LDPC code with rate 14/15=0.933. The performance of this code is also depicted in Fig. 10.6, which exhibits only 1.35dB from the Shannon limit at the same BER as m=8.

An equivalent random (2715, 2535) regular LDPC code (or MacKay code [6][122]) is generated by computer for an explicit comparison, whose parity-check matrix has column weight 4 and average row weight 60. The performance is also plotted in Fig. 10.6, which shows that the (2715, 2535) regular QC-LDPC code outperforms the MacKay code for a BER less than 10^{-4}. □

Class-II BIBD-LDPC Codes

This class of code is effectively designed by the Class-II Bose-BIBDs. The parity-check matrix, denoted by $\mathbf{H}^{(2)}$, of a Class-II BIBD-LDPC code is simply the incidence matrix $\mathbf{Q}$ of a Class-II BIBD given by (10-47), i.e., $\mathbf{H}^{(2)}=\mathbf{Q}$. The null space of $\mathbf{H}^{(2)}$ gives a Class-II BIBD-LDPC code of length $N=(3t+1)(4t+1)$ whose rate is

$$r=1-\frac{12t+1}{N}=\frac{12t^2-5t}{12t^2+7t+1} \tag{10-53}$$

Clearly, the rate is very high for large t.

Example 10.9: For t=25, there is a Class-II Bose-BIBD with parameters: $v=12t+4$=304, $n=(3t+1)(4t+1)$=7676, $\rho=4t+1$=101, γ=4, and λ=1. The incidence matrix $\mathbf{Q}$ of

this design is a 304×7676 with row and column weights 101 and 4, respectively, whose rank is $12t+1=301$. Thus, the null space of $\mathbf{H}^{(2)}$ results in a (7676, 7375) Class-II BIBD-LDPC code with very high rate $r=7375/7676=0.9608$. The performance of the code is shown in Fig. 10.7 where only 0.95dB exists from the Shannon limit at a BER of 10^{-6}. Meanwhile, the error performance of an equivalent random (7676, 7375) regular LDPC code (MacKay code [6][122]) is also include for an explicit comparison, which shows that the BIBD -LDPC code outperforms the random LDPC code.

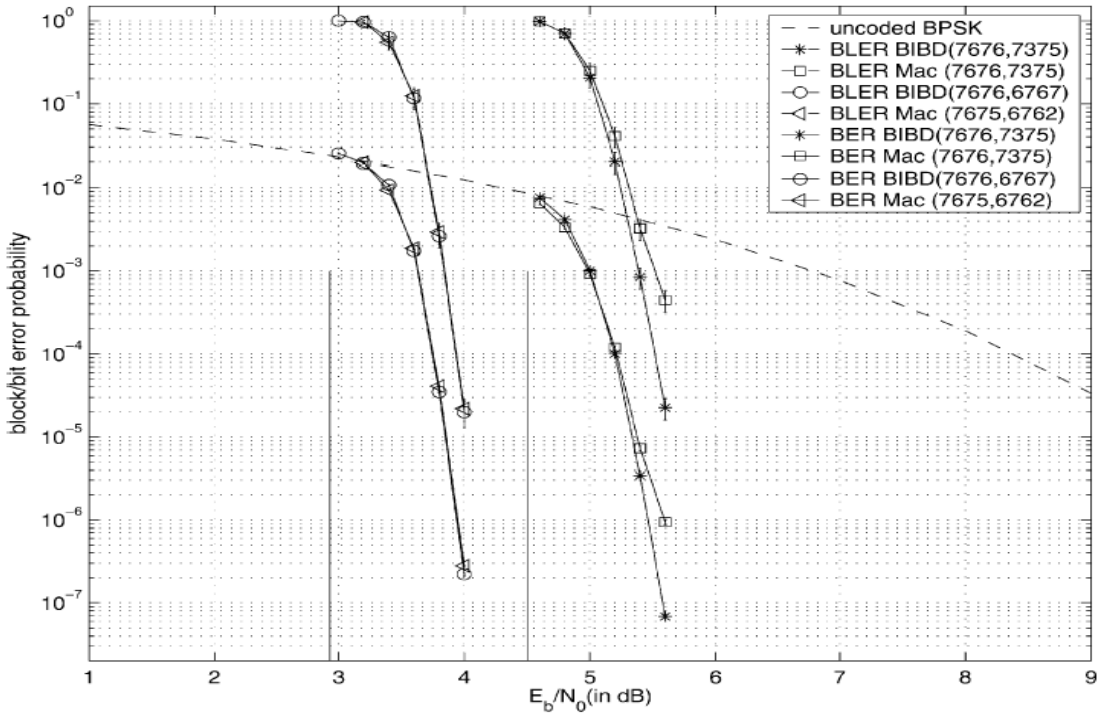

Fig. 10.7. Error performance of the regular (7676, 7375) and (7676, 6767) Class-II BIBD-LDPC codes, the random (7676, 7375) and (7676, 6762) regular LDPC code (MacKay code, denoted by "Mac") in an AWGN channel, where the block error rate is denoted by "BLER".

A lower rate code of the same length can be constructed by splitting each row of $\mathbf{H}^{(2)}$ into multiple rows. In this example, we split each row of $\mathbf{H}^{(2)}$ into three rows, i.e., two rows has weight 34 and the other one has weight 33. The systematic ways to lower the code rate by splitting each row of parity-check matrix using a circular manner is

explicitly introduced in [122][123]. Hence, a new 912×7676 parity-check matrix $\mathbf{H}_0^{(2)}$ is resulted, whose null space leads to a (7676, 6767) regular LDPC code with a lower rate r=6767/7676=0.88. The performance of this code is also shown in Fig. 10.7, which indicates that there has 1.05dB from the Shannon limit at the BER of 10^{-6}. Again, an equivalent random (7676, 6762) regular LDPC code (MacKay code) is generated for comparison. We observe that the (7676, 6767) Class-II BIBD-LDPC code performs equally well as the MacKay code. □

Class-III BIBD-LDPC Codes

This class of codes is designed based on the Class-III Bose-BIBDs introduced in Section 10.7.3. The parity-check matrix $\mathbf{H}^{(3)}$ of a Class-III BIBD-LDPC code is the incidence matrix $\mathbf{Q}$ of a Class-III design given by (10-50). Therefore, the resulted regular LDPC code has length $N=(5t+1)(4t+1)$ with rate r

$$r \approx 1-\frac{20t+5}{N}=\frac{20t^2-11t-4}{20t^2+9t+1} \tag{10-54}$$

Evidently, the rate r is very high for large t. Since $\mathbf{Q}$ can be expressed by an array of circulants, thus the constructed code is a QC-LDPC code.

Example 10.10: The design of Class-III BIBD-LDPC codes:

(a) t=7: There exists a Class-III Bose-BIBD with parameters: $v=20t$+5=145, $n=(5t+1)(4t+1)$=1044, $\rho=5t$+1=36, γ=5, and λ=1. Hence, the incidence matrix $\mathbf{Q}$ of this design is a 145×1044 matrix with row and column weights 36 and 5, respectively, whose rank is 145. Thus, the null space of $\mathbf{H}^{(3)}$ ($\mathbf{H}^{(3)}=\mathbf{Q}$) results in a (1044, 899) QC-BIBD-LDPC code with rate r=899/1044=0.86. The performance of the coded system is

shown in Fig. 10.8, where the coded has 2.1 dB from the Shannon limit at the BER of 10^{-6}.

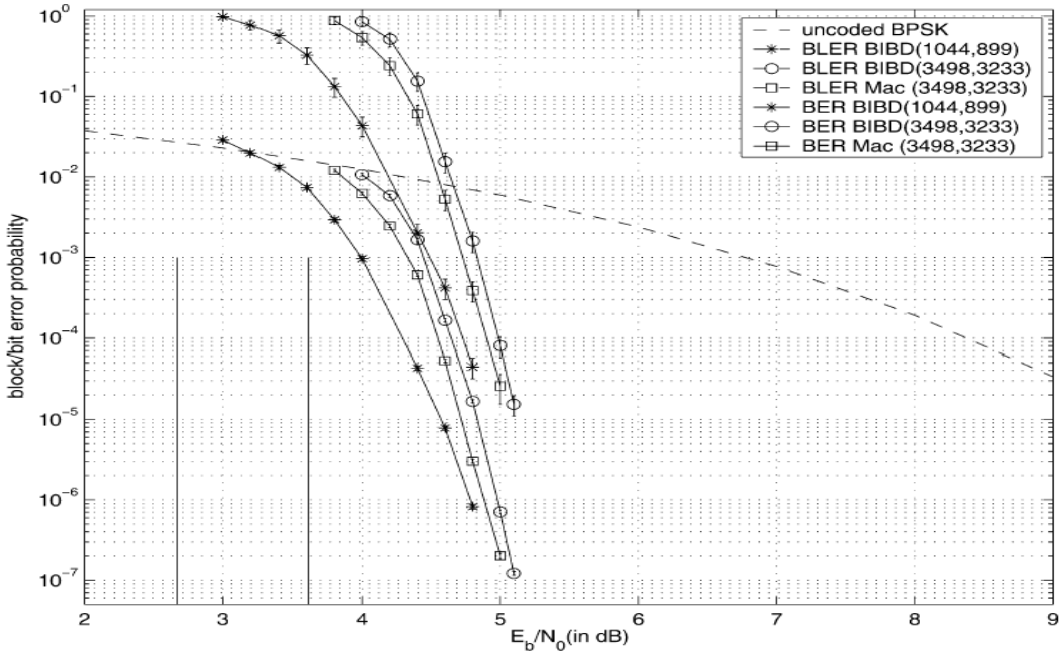

Fig. 10.8. Error performance of the regular (1044, 899) and (3498, 3233) Class-III QC-BIBD-LDPC codes, the random (3498, 3233) regular LDPC code (MacKay code, denoted by "Mac") in an AWGN channel, where the block error rate is denoted by "BLER".

(b) t=13: The Class-III Bose-BIBD with parameters: $v=20t+5=265$, $n=(5t+1)(4t+1)=3498$, $\rho=5t+1=66$, $\gamma=5$, and $\lambda=1$. The incidence matrix $\mathbf{Q}$ is a 265×3498 matrix with row and column weights 66 and 5, respectively. The null space of $\mathbf{H}^{(3)}$ ($\mathbf{H}^{(3)}=\mathbf{Q}$) results in a (3498, 3233) QC-BIBD-LDPC code with rate r=3233/3498=0.92. The performance of the code is also given in Fig. 10.8, which shows that there is only 1.35 dB from the Shannon limit at the BER of 10^{-6}. For comparison, we design a random (3498, 3233) regular LDPC code (MacKay code [6][122]), which gives slight better performance than the QC-BIBD-LDPC code for BERs above 10^{-7}. Two codes seem to have almost the same error performance below 10^{-7} BER. □

In this section, a systematic way for construction of QC-LDPC codes has been presented based on a special type of BIBDS, i.e., Bose BIBDs with λ=1. Simulation results demonstrate that these LDPC codes perform well with the iterative decoding using BP algorithm.

Besides BIBDs with λ=1, there also has other families of BIBDs with λ=2 [118][119][120]. The Tanner graph of these codes must have cycles of length 4 if these BIBDs are applied to the constructions. However, we may break all the length-4 circles or reduce their number by the decomposition of the incidence matrices and thus produce good LDPC codes. In addition to BIBDs, there are other types of combinatoric designs [118][119][120][123] that show to be potential in the design of ideal LDPC codes. Generally, combinatoric design is a very rich and powerful tool for the construction of good LDPC codes.

References

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

[2] R. M. Tanner, "A recursive approach to low complexity codes," IEEE Trans. Inform. Theory, vol. IT-27, pp. 533-547, Sept. 1981.

[3] V. Zablov and M. Pinsker, "Estimation of the error-correction complexity of Gallager low-density codes," *Probl*. *Pered*. Inform., vol. 11, pp. 23-26, Jan. 1975.

[4] G. A. Margulis, "Explicit construction of graphs without short cycles and low density codes," Combinatorica, vol. 2, No. 1, pp. 71-78, 1982.

[5] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," Electric Lett., vol. 32, pp. 1645-1646, Aug. 1996.

[6] D. J. C. MacKay, "Good Error-correction Codes Based on Very Sparse Matrices," IEEE Trans. Inform. Theory, vol. 45, No. 2, pp. 399-431, Mar. 1999.

[7] T. J. Richardson and Rudiger L. Urbanke, "Efficient Encoding of Low-Density Parity-Check Codes," IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 638-656, Feb. 2001.

[8] T. J. Richardson, M. Amin Shkrollahi, and Rudiger L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," IEEE Trans. Inform. Theory, vol. 47, No. 2, 619-637, Feb. 2001.

[9] T. J. Richardson and Rudiger L. Urbanke, "The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding, "IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 599-618, Feb. 2001.

[10] C. Berrou, A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo Codes," IEEE Trans. Commun., vol. 44, No. 10, pp. 1261-1271, Oct. 1996.

[11] R. G. Gallager, "Low-Density Parity-Check Codes," IRE Transactions on Information Theory, pp. 21-28, Jan. 1962.

[12] S. Young Chung, G. D. Forney, T. J. Richardson and R. Urbanke, "On the Design of Low-Density Parity-Check Codes within 0.0045dB of the Shannon Limit," IEEE Commun., Lett. Vol. 5, No. 2, pp. 58-60, Feb. 2001.

[13] D. J. C. Mackay, S. T. Wilson and M. C. Davey, "Comparison of Constructions of Irregular Gallager Codes," IEEE Trans. Commun., vol. 47, No. 10, pp. 1449-1454, Oct. 1999.

[14] R. M. Tanner, "Minimum-Distance Bounds by Graph Analysis," IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 808-821, Feb. 2001.

[15] G. D. Forney, JR., "Codes on Graphs: Normal Realizations," IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 520-548, Feb. 2001.

[16] S. Y. Chung, T. J. Richardson and R. L. Urbanke, "Analysis of Sum-product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation," IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 657-670, Feb. 2001.

[17] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi and D. A. Spielman, "Improved Low-Density Parity-Check Codes Using Irregular Graphs," IEEE Trans. Inform. Theory, vol. 47, No. 2, pp. 585-598, Feb. 2001.

[18] G. Miller, D. Burshtein, "Bounds on the Maximum-Likelihood Decoding Error Probability of Low-Density Parity-Check Codes," IEEE Trans. Inform. Theory, vol. 47, No. 7, pp. 2696-2710, Nov. 2001.

[19] B. M. Kurkoski, P. H. Siegel and J. K. Wolf, "Joint Message-Passing Decoding of LDPC Codes and Partial-Response Channel," IEEE Trans. Inform. Theory, vol. 48, No. 6, pp. 1410-1422, June 2002.

[20] D. Burshtein, M. Krivelevich, S. Litsyn and G. Miller, "Upper Bound on the Rate of LDPC Codes," IEEE Trans. Inform. Theory, vol. 48, No. 9, pp. 2437-2449, Sept. 2002.

[21] M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman and V. Stemann, "Practical loss-resilient codes," in Proc. 29th Anun., ACM Symp. Theory of Computing, pp. 150-159, 1997.

[22] R. J. McEliece, D. J. C. MacKay and J. F. Cheng, "Turbo Decoding as an Instance of Pearl's "Belief Propagation" Algorithm," IEEE Journal on Selected Areas in Communications. vol. 16, No. 2, pp. 140-152, Feb. 1998.

[23] F. R. Kschischang and B. J. Frey, "Iterative Decoding of Compound Codes by Probability Propagation in Graphical Models," IEEE Journal on Selected Areas in Communications, vol. 16, No. 2, pp. 219-230, Feb. 1998.

[24] B. J. Frey and F. R. Kschischang, "Early Detection and Trellis Splicing: Reduced-Complexity Iterative Decoding," IEEE Journal on Selected Areas in Communications, vol. 16, No. 2, pp. 153-159, Feb. 1998.

[25] F. R. Kschischang, B. J. Frey and H. A. Loeliger, "Factor Graphs and the Sum-Product Algorithm," IEEE Trans. on Inform. Theory, vol. 47, No. 2, pp. 498-519, Feb. 2001.

[26] Li Ping and K. Y. Wu, "Concatenated Tree Codes: A Low-Complexity, High-Performance Approach," IEEE Trans. on Inform. Theory, vol. 47, No. 2, pp. 791-799, Feb. 2001.

[27] Lin Ping and W. K. Leung, "Decoding Low Density Parity Check Codes with Finite Quantization Bits," IEEE Communications Letters, vol. 4, No. 2, pp. 62-64, Feb. 2000.

[28] D. Spielman, "Linear-Time Encodeable and Decodable Error-Correcting Codes," IEEE Trans. Inform. Theory, vol. 42, pp. 1723-1731, Nov. 1996.

[29] J. Whittaker, Graphical Models in Applied Multivariable Statistics. Chichester, UK.: Wiley, 1990.

[30] F. V. Jensen, An Introduction to Bayesian Networks. New York: Spring-Verlag, 1996.

[31] G. Chartrand and L. Lesniak, Graphs & Digraphs, Third Edition, Boca Raton, London, New York and Washington, D.C, Chapman & Hall/CRC, 1996.

[32] Vera Pless, Introduction to the Theory of Error-Correcting Codes, New York, Chichester, Weinheim, Brisbane, Singapore, Toronto, A Wiley-Interscience Pulication JOHN WILEY & SONS, INC.

[33] R. M. Pyndiah, "Near-Optimal Decoding of Product Codes: Block Turbo Codes," IEEE Trans. on Commun., vol. 46, No. 8, pp. 1003-1010, Aug. 1998.

[34] S. Hirasawa, M. Kasahara, Y. Sugiyaha and T. Noamekawa, "Modified Product Codes," IEEE Trans. on Inform. Theory, vol.. IT-30, No. 2, pp. 299-306, Mar. 1984.

[35] H. Nickl, J. Hagenauer, and Burkert, "Approaching Shannon's capacity limit by 0.27dB using simple Hamming codes," IEEE Commun., Lett., vol. 1, pp. 130-132, Sept. 1997.

[36] D. Chase, "A Class of Algorithms for Decoding Block Codes with Channel Measurement Information," IEEE Trans. Inform. Theory, vol. IT-18, pp. 170-182, Jan. 1972.

[37] S. Benedetto D. Divsalar G. Montorsi and F. Pollara, "A Soft-Input Soft-Output APP Module for Iterative Decoding of Concatenated Codes," IEEE Commun., Lett., vol. 1, No. 1, pp. 22-24, Jan. 1997.

[38] J. Pear, "Fusion propagation and structuring in belief networks," Artif. Intell., vol. 29, pp. 241-288, 1986.

[39] L. Ping, S. Chen, and K. L. Yeung, "Iterative Decoding of Multidimensional Concatenated Signal Parity Check Codes," in Proc. IEEE Int. Communications, Conf. (ICC'98), pp. 131-135, June 1998.

[40] D. Divsalar and F. Pollara, "Multiple Turbo Codes," in Proc. IEEE MILCOM'95, vol. 1, pp. 279-285, 1995.

[41] M. Sipser and D. A. Spielman, "Expander Codes," IEEE Trans. on Inform. Theory, vol. 42, No. 6, pp. 1710-1722, Nov. 1996.

[42] 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. on Commun., vol. 47, no. 5, pp. 673-680, May 1999.

[43] R. Lucas, M. Fossorier, Y. Kou and S. Lin, "Iterative Decoding of One-Step Majority Logic Decodable Codes Based on Belief Propagation," IEEE Trans. Commun., vol. 48, no. 6, pp. 931-937, Jun. 2000.

[44] S. Litsyn and V. Shevelev, "On Ensembles of Low-Density Parity-Check Codes: Asymptotic Distance Distributions," IEEE Trans. on Inform. Theory, vol. 48, No. 4, pp. 887-908, April 2002.

[45] J. Hagenauer, E. Offer and L. Papke, "Iterative Decoding of Binary Block and Convolutional Codes," IEEE Trans. on Inform. Theory, vol. 42, No. 2, pp. 429-445, Mar. 1996.

[46] J. Chen, A. Dholakia, E. Eleftheriou, M. P. C. Fossorier and Xiao-Yu Hu, "Reduced -Complexity Decoding of LDPC Codes," IEEE Trans. on Commun., vol. 53, No. 8, pp. 1288−1299, August, 2005.

[47] A. Bag and G. David Forney, Jr., "Random Codes: Minimum Distances and Error Exponents," IEEE Trans. on Inform. Theory, vol. 48, No. 9, pp. 2568-2573, Sept. 2002.

[48] M. R. YazdaNi, S. Hemati and A. H. Banihashemi, "Improving Belief Propagation on Graphs with Cycles," IEEE Commun. Lett., vol. 8, no. 1, pp. 57-59, Jan. 2004.

[49] E. Eleftheriou, T. Mittelholzer and A. Dholakia, "Reduced-Complexity Decoding Algorithm for Low-Density Parity-Check Codes," IEE Electron Lett., vol. 37, pp. 102-104, Jan. 2001.

[50] A. Anastasopoulos, "A Comparison between the Sum-Product and the Min-Sum Iterative Detection Algorithms Based on Density Evolution," in Proc. IEEE Globecom, San Antonio, TX, Nov. 2001, pp. 1021–1025.

[51] J. Erfanian, S. Pasupathy and G. Gulak, "Reduced-Complexity Symbol Detectors with Parallel Structures for ISI Channels," IEEE Trans. Commun., vol. 42, No. 2-4. pp. 1661-1671, Feb.-Apr. 1994.

[52] J. Chen, and M. P. C. Fossorier, "Density Evolution for Two Improved BP-Basd Decoding Algorithms of LDPC Codes," IEEE Commun., Lett. Vol. 6, No. 5, pp. 208-210, May 2002.

[53] 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, Mar. 2002.

[54] Y. C. He, H. P. Li, S. H. Sun and L. Li, "Threshold-Based Design of Quantized Decoder for LDPC codes," in Proc. IEEE *Int*. *Symp*. *Inf*. *Theory*, Yokohama, Japan, Jan.-Jul. 2003, p.149.

[55] H. Sankar and K. R. Narayanan, "Memory-Efficient Sum-Product Decoding of LDPC Codes," IEEE Trans. on Commun., vol. 52, No. 8, pp. 1225-1230, Aug. 2004.

[56] M. M. Mansour and N. R. Shanbhag, "Memory-Efficient Turbo Decoder Architectures for LDPC Codes," in Proc. IEEE Workshop Signal Processing Systems, pp. 159-164, Oct. 2002.

[57] M. Reza Soleymani, Y. Gao and U. Vilaipornsawai, Turbo Coding for Satellite and Wireless Communications, Kluwer Academic Publisher, 2002.

[58] K. Sripimanwat, Turbo Codes Applications: A Journey from a Paper to Realization, Springer 2005.

[59] M. Ardakani and Frank R. Kschischang, "Gear-Shift Decoding," IEEE Trans. on Commun., vol. 54, No. 7, pp. 1235-1242, July 2006.

[60] L. Bazzj, T. J. Richardson and R. L. Urbanke, "Exact Threshold and Optimal Codes for the Binary-Symmetry Channel and Gallager's Decoding Algorithm A," IEEE Trans. on Inform. Theory, vol. 59, No.9, pp. 2010-2022, Sept. 2004.

[61] Irwin Miller and Marylees Miller, John E. Freund's Mathematical Statistics with Applications, Seventh Edition, Prentice Hall, 2004.

[62] H. Pishro-Nik and F. Fekri, "On Decoding of Low-Density Parity-Check Codes over the Binary Erasure Channel," IEEE Transactions on Inform. Theory, vol. 50, No. 3, pp. 439-453, Mar. 2004.

[63] P. Henrici, Applied and Computational Complex Analysis. New York: Wiley, 1974, vol. 1.

[64] David. G. Luenberger, "Linear and Nonlinear Programming, Second Edition, Ontario, Sydney, Addison-Wesley Publisher Company, 1984.

[65] Saul I. Gass, Linear Programming: Methods and Applications, Third Edition, McGraw-Hill Book Company, New York, Toronto, 1969.

[66] A. Schrijver, Theory of Linear and Integer Programming. New York; Wiley, 1986.

[67] J. M. Wozencraft and I. M. Jacobs, "Principles of Communication Engineering. New York: Wiley, 1965.

[68] I. S. Gradshtein and I. M. Ryzhik, Table of Integrals, Series, and Products. New York: Academic, 1965.

[69] S-Y. Chung, "On the Construction of some capacity-approaching coding schemes," Ph.D. dissertation, MIT, MA, 2000.

[70] P. E. O'Neil, "Asymptotics and random Matrices with row-sum and column-sum restrictions," Bull. Amer. Math. Soc., vol. 75, pp.1276-1282, 1969.

[71] I. J. Good and J. F. Crook, "The enumeration of arrays and a generalization related to contingency tables," Discr. Math., vol. 19, no. 1, pp. 23-45, 1977.

[72] S. Litsyn and V. Shevelev, "On ensemble of low-density parity-check codes: Asymptotic distance distributions," IEEE Trans. on Inform. Theory, vol. 48, No. 4, pp. 887-908, April, 2002.

[73] S. Litsyn and V. Shevelev, "Distance distributions in ensembles of irregular low-density parity-check codes," IEEE Trans. on Inform. Theory, vol. 49, No. 12, pp. 3140-3159, Dec. 2003.

[74] T. M. Cover, A. A. El Gamal, "Capacity theorems for the relay channel," IEEE Trans. On Inform. Theory, vol. 25, No. 5, pp. 572-584, Sept. 1979.

[75] A. Sendonaris, E. Erkip, B. Aazhang, "User cooperation diversity-Part I: System description," IEEE Trans. on Commun., vol. 51, No. 11, pp. 1927-1938, Nov. 2003.

[76] A. Sendonaris, E. Erkip, B. Aazhang, "User cooperation diversity-Part II: Implementation aspects and performance analysis," IEEE Trans. on Commun., vol. 51, No. 11, pp. 1939-1948, Nov. 2003.

[77] P. Gupta and P. R. Kumar, "Towards an information theory of large networks: An achievable rate region," IEEE Trans. on Inform. Theory, vol. 49, No. 8, pp. 1877-1894, Aug. 2003.

[78] A. Host-Madsen and J. Zhang, "Capactity bound and power allocation for wireless relay channels," IEEE Trans. on Inform. Theory, vol. 51, No. 6, pp. pp. 1020-2040, June 2005.

[79] L. L. Xie and P. R. Kumar, "A network information theory for wireless communications: Scaling laws and optimal operation," IEEE Trans. on Inform. Theory, vol. 50, No. 5, pp. 748-767, May 2004.

[80] J. N. Laneman, David N. C. Tse and G. W. Wornell, 'Cooperative diversity in wireless networks: Efficient protocols and outage behaviour," IEEE Trans. on Inform. Theory, vol. 50, No. 12, pp. 3062-3080, Dec. 2004.

[81] G. Kramer, M. Gastpar and P. Gupta, "Cooperative strategies and capacity theorems for relay channel," IEEE Trans. on Inform. Theory, vol. 51, No. 9, pp. 3037-3063, Sept. 2005.

[82] L. L. Xie and P. R. Kumar, "An achievable rate for the multiple-level relay channel, IEEE Trans. on Inform. Theory, vol. 51, No. 4, pp. 1348-1358, April 2005.

[83] E. C. van der Meulen, "Three-terminal communication channels," *Adv. Appl. Probab.*, vol. 3, pp. 120-154, 1971.

[84] T. Cover and J. Thomas, Elements of Information Theory, New York: Wiley, 1991.

[85] A. Chakrabarti, A. de Baynast, A. Sabharwal, and B. Anzhang, "Low Density Parity Check Codes for the Rayleigh Channel," IEEE J-SAC, vol. 25, no. 2, pp. 280-291, Feb. 2007.

[86] D. Slepian and J. Wolf, "Noiseless coding of correlative information source," IEEE Trans. Inform. Theory, vol. 10, no. 4, pp. 471-480, July, 1973.

[87] S. M. Ali and Robert J. McEliece, "The generalized distributive law," IEEE Trans. on Inform. Theory, vol. 46, No. 2, pp. 325-343, March, 2000.

[88] A. R. Calderbank, G. David Forney, Jr., and Alexander Vardy, "Minimal tail-biting trellis: The Golay code and more," IEEE Trans. on Inform. Theory, vol. 45, No. 5, pp. 1435-1455, July, 1999.

[89] H. Imai et al., Essentials of Error-Control Coding Techniques, Academic Press, New York, 1990.

[90] G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. Inform. Theory, vol. 28, no. 1. pp. 55-67, Jan. 1982.

[91] G. Ungerboeck, J. Hagenauer, and T. Abdel-Nabi, "Coded 8PSK experimental modem for the INTELSAT SCPC system," Proceedings, ICDSC, 7th, pp. 299-304, 1986.

[92] M. Mouly and M. B. Pautet, The GSM System for Mobile Communications, ISBN 2-9507190-0-7, 1993.

[93] TIA/EIA/IS-95 interim standard, mobile station-base station compatibility standard for dual-mode wideband spread spectrum cellular systems, Telecommunications Industry Association, Washington, D.C., July 1993.

[94] C. E. Shannon, "A mathematical theory of communications," Bell Syst. Tech. J., vol. 27, pp. 379-423, July 1948.

[95] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, New York, 1988.

[96] Christian B. Schlegel and Lance C. Perez, Trellis and Turbo Coding, IEEE Press, 2004.

[97] A. Roumy, S. Guemghar, G. Caire abd S. Verdu, "Design of Methods for Irregular Repeat-Accumulate Codes," IEEE Trans. On Inform. Theory, vol. 50, no. 8, pp, 1711-1727, August 2004.

[98] D. Reynolds, Xiaodong Wang, "Turbo Multiuser Detection with Unknown Interferers," IEEE Trans. on Commun., vol. 50, no. 4, pp. 616-622, April 2002.

[99] R. Koetter, A. C. Singer and M. Tuchler, "Turbo Equalization: An Iterative Equalization and Decoding Technique for Coded Data Transmission," IEEE Signal Processing Magazine, vol. 21, no.1, pp. 67-80, Jan. 2004.

[100] S. Benedetto, D. Divsalar, G. Montorsi and F. Pollara, "Serial Concatenation of Interleaved Codes: Performance Analysis, Design, and Iterative Decoding," IEEE Trans. on Inform. Theory, vol. 44, No. 3, pp. 909-926, May 1998.

[101] B. Vucetic and J. Yuan, Turbo Codes: Principles and Applications, Kluwer Academic Publisher, 2000.

[102] M. Reza Soleymani, Yingzi Gao and U. Vilaipornsawai, Turbo Coding for Satellite and Wireless Communications, Kluwer Academic Publishers, 2002.

[103] Ezio Biglieri, Coding for Wireless Channels, Springer, 2005.

[104] Stephen G. Wilson, Digital Modulation and Coding, Prentice Hall, 2996.

[105] Ron M. Roth, Introduction to Coding Theory, Cambridge university press, 2006.

[106] Berlekamp, E. R. Algebraic coding theory, McGraw-Hill, New York, 1968.

[107] Zongwang Li, Lei Chen, Lingqi Zeng, Shu Lin, and Wai H. Fong, "Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check Codes," IEEE Trans. on Commun., Vol. 54, No.1, pp. 71-81, Jan. 2006.

[108] Lingqi Zeng, Lan Lan, Ying Y. Tai, Shumei Song, Shu Lin, and Khaled Abdel-Ghaffar, "Constructions of Nonbinary Quasi-Cyclic LDPC Codes: A Finite Approach," IEEE Trans. on Commun., Vol. 56, No. 4, pp. 545-554, April 2008.

[109] Gianluigi Liva, William E. Ryan, and Marco Chiani, "Quasi-Cyclic Generalized LDPC Codes with Low Error Floors," IEEE Trans. on Commun., Vol. 56, No. 1, pp. 49-57, Jan. 2008.

[110] Lan Lan, Ying Yu Tai, Shu Lin, Behshas Memari, and Bahram Honary, "New Constructions of Quasi-Cyclic LDPC Codes Based on Special Classes of BIBD's for the AWGN and Binary Erasure Channels," IEEE Trans. on Commun., Vol. 56, No. 1, pp. 39-48, Jan. 2008.

[111] S. Lin and D. J. Costello, Jr., Error Control Coding: Fundamentals and Applications, 2nd edition, Upper Saddle River, NJ: Prentice-Hall, 2004.

[112] 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. 1028-1042, July, 2004.

[113] R. M. Tanner, "Spectral graphs for quasi-cyclic LDPC codes," in Proc. IEEE Int. Symp. Inf. Theory, Washington, DC, pp. 226, June 2001.

[114] D. J. MacKay and M. C. Davey, "Evaluation of Gallager codes of short block length and high rate applications," in Proc. IMA International Conference on Mathematics and Its Applications: Codes, Systems and Graphical Models, pp. 113-130, Springer-Verlas, New York, 2000.

[115] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over GF(2^q)," in Proc. ITW 2003, pp. 70-73, Pairs, France, Mar. 2003.

[116] I. N. Iman and L. M. Lamout, "An algorithm using the Schur complement in inverting large matrices," in Proc. IEEE *Southeast Conf. Energy Inf. Technol. Southeast*," vol. 2, Apr. 9-12, 1989, pp. 421-426.

[117] R. M. Gray, Toeplitz and Circulants Matrices: A Review. Stanford, CA: Stanford Univ. 2001.

[118] R. C. Bose, "On the construction of balanced incomplete block designs," Ann. Eugenics 9, pp. 353-399, 1939.

[119] H. B. Mann, Analysis and Design of Experiments. New York: Dover, 1949.

[120] A. P. Street and D. J. Street, Combinatoric of Experimental Design. Oxford, UK: Oxford Science/Clarendon, 1987.

[121] J. E. M. Nilsson and P. Kotter, "Iterative decoding of product code construction," in *Proc. Int. Symp. Information Theory and Its applications*, Sydney, Australia, Nov. 1994, pp. 1059-1064.

[122] B. Ammar, B. Honary, Yu Kou, Jun Xu, Shu Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," IEEE Trans. Inform. Theory, vol. 50, no. 6, pp. 1257-1268, June 2004.

[123] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," IEEE Trans. Inform. Theory, vol. 47, pp. 2711-2736, Nov. 2001.