# Hierarchical and High-Girth QC LDPC codes

Authors: Yige Wang, Stark C. Draper, Jonathan S. Yedidia
Publication: IEEE T. Info.Theory, July 2013
Speaker: Jeong-Min Ryu

**Short summary:**

They present **an approach to designing capacity approaching high-girth low-density parity-check (LDPC) codes** that are friendly to hardware implementation, and compatible with some desired input code structure defined using a protograph. The approach is based on a mapping of any class of codes defined using a protograph into a family of hierarchical quasi-cyclic (HQC) LDPC codes. Next, they present **a girth-maximizing algorithm** that optimizes the degrees of freedom within the family of codes to yield a high-girth HQC LDPC code, subject to bounds imposed by the fact that HQC codes are still quasi-cyclic. Finally, they discuss **how certain characteristics of a code protograph will lead to inevitable short cycles** and show that **these short cycles can be eliminated** using a "squashing" procedure that results in a high-girth QC LDPC code.

(The "girth" of a code is the length of the shortest cycle in the code graph)

## I. INTRODUCTION

### 1. The construction of LDPC codes

- Highly random graph construction
- Algebraic construction

**1) Highly random graph construction**

→ It can produce LDPC codes that closely approach the Shannon capacity

→ **Not easy to implement** in hardware as the irregular connections imply wiring complexity.

**2) Algebraic construction**

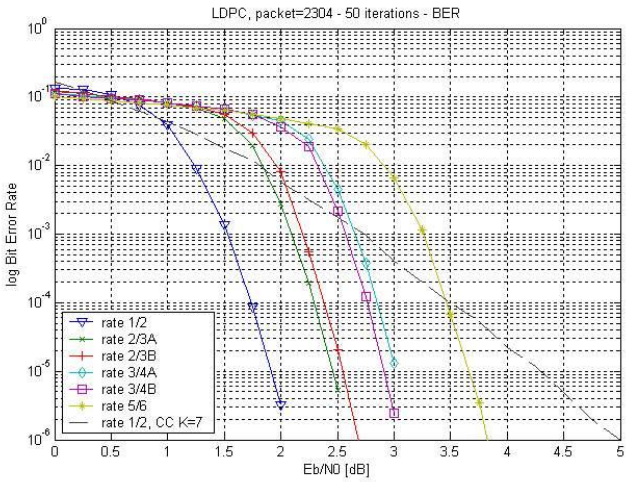
→ In actual implementations, more structured constructions have been strongly preferred

→ Quasi- cyclic LDPC (QC LDPC) codes are a particularly practical and widely used class of structured LDPC codes.

→ In view of the practicality, **they focus in this paper on the design of QC LDPC codes** that have good decoding performance

## 2. Optimizing the decoding performance

- Water-fall
- Error floor




**1) Water-fall**

→ **"**Water-fall" is a regime where the signal-to-noise (**SNR**) is relatively **low**.

→ The standard way to do that for irregular random constructions is to use "**density-evolution**" or "**EXIT chart**" techniques to obtain the degree distribution that **optimizes the code threshold in the asymptotic limit of long block lengths**

**2) Error floor**

→ An "error floor" in the performance curve means that **the decoding failure rate does not continue to decrease rapidly as the SNR increases**.

**In this paper, they focus on how to take a code structure, such as a particular spatial-coupling structure, that has been designed to perform near the Shannon limit in the waterfall regime, and constructing a QC LDPC code with that structure that also empirically has excellent error floor performance.**

## II. QC LDPC CODES

- **Review of Standard QC LDPC codes**

QC LDPC codes are defined in terms of **circulant permutation matrices**. Let $I_{i,p}$ denote the circulant permutation matrix, or "cyclic shift matrix," obtained by cyclically left-shifting a $p \times p$ identity matrix by $i$ positions, where $0 \le i \le p-1$; $I_{0,p}$ is thus the $p \times p$ identity matrix. We often suppress the dependence on p, writing $I_i$ instead of $I_{i,p}$. As an example, if $p = 4$, then

$$I_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

An important special case of QC LDPC codes is "weight-I ($J$, $L$) regular" QC LDPC code. The parity check matrix of such a code consists of $J$ rows and $L$ columns of $p \times p$ cyclic shift submatrices. The submatrix in the $j$th row and $l$th column is $I_{i_{j,l}} = (I_1)^{i_{j,l}}$ and the code has blocklength $N = pL$. They abstractly represent the $(j,l)$th submatrix as a power of dummy variable $x$ as $x^{i_{j,l}}$.

More generally, a QC LDPC code is represented by a polynomial parity check matrix $H(x)$ whose entries are polynomials in $x$:

$$H(x)=\begin{bmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,L}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,L}(x) \\ \vdots & & \ddots & \vdots \\ h_{J,1}(x) & h_{J,2}(x) & \cdots & h_{J,L}(x) \end{bmatrix}$$

where $h_{j,l}(x)=\sum_{s=0}^{p-1} c_s[j,l]x^s$ for $1\le j\le J, 1\le l\le L$, $c_s[j,l]\in\{0,1\}$.

*Example 1*: Let *C* be a length-9 QC LDPC code described by

$$\mathbf{H}=\left[\begin{array}{ccc|ccc|ccc} 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1\\ \hline 0&0&0&1&0&0&0&1&1\\ 0&0&0&0&1&0&1&0&1\\ 0&0&0&0&0&1&1&1&0 \end{array}\right]$$

For this code, $J=2, L=3$, and $p=3$, and H can equivalently be written as

$$\mathbf{H}=\begin{bmatrix} \mathbf{I}_0 & \mathbf{I}_0 & \mathbf{I}_0 \\ \mathbf{0} & \mathbf{I}_0 & \mathbf{I}_1+\mathbf{I}_2 \end{bmatrix}.$$

The polynomial version of the parity check matrix is

$$\mathbf{H}(x)=\begin{bmatrix} x^0 & x^0 & x^0 \\ 0 & x^0 & x^1+x^2 \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & x^1+x^2 \end{bmatrix}.$$

For the maximum weight *M* among all polynomial entries $h_{j,l}(x)$ in $H(x)$, they call such a code a weight-*M* QC-LDPC code.

The code in Example 1 is a weight-II QC LDPC code.

## III. Graphical Representations of QC LDPC Codes

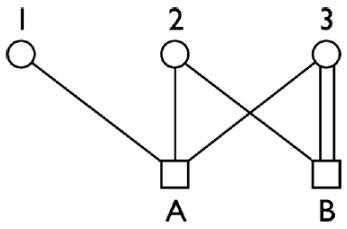



Fig. 1. A simple protograph with three types of variables and two types of checks.

A "**protograph**," as introduced by Thorpe in [30], is a template that can be used to derive a class of Tanner graphs. **Each node in a protograph represents a "type" of node** in a Tanner graph. The nodes will all be duplicated $p$ times in the Tanner graph derived from the protograph.

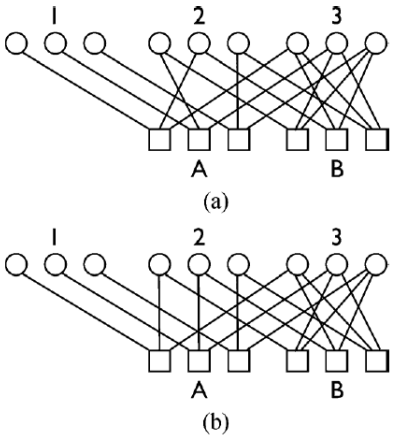



Fig. 2. Two Tanner graphs corresponding to the protograph shown in Fig. 1. The Tanner graph in (a) does not have a quasi-cyclic structure; the one in (b) does, and in fact has the parity check matrix of the QC LDPC code given in Example 1.

Fig. 2 shows two Tanner graphs derived from the protograph of Fig.1, with $p = 3$. Note that there are many possible Tanner graphs that one can construct, which correspond to a particular protograph, and they need not necessarily have a quasi-cyclic structure. The Tanner graph shown in Fig. 2(a) is not quasi- cyclic. But it is always easy to construct a quasi-cyclic version of any protograph.

Protographs can equivalently be described by an **"incidence" matrix**. An incidence matrix has a number of rows equal to the number of types of checks in the protograph and a number of

columns equal to the number of types of variables. Each entry in the incidence matrix tells you how many edges there are connecting a type of check node to a type of variable node in the protograph. For example, the incidence matrix $P$ for the protograph in Fig.1 would be

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix}.$$

- **Lifting procedure** (used to maximizes the girth of the code)

The lifting procedure is simply to replace each entry in the incidence matrix with a polynomial of weight equal to the entry.

For example, the protograph in Fig. 1, which has the incidence matrix $P$, can be lifted into a QC LDPC code with parity check matrix

$$H(x) = \begin{bmatrix} x^a & x^b & x^c \\ 0 & x^d & x^e + x^f \end{bmatrix},$$

where $a, b, c, d, e,$ and $f$ are integer exponents between 0 and $p-1$, with $e \neq f$. These integer exponents **parameterize an ensemble of QC LDPC codes** all of which are liftings of (and which cover) the original protograph. In our algorithms, **they will optimize over the choice of these exponents to find a lifting that maximizes the girth of the resulting code**.

## IV. Cycles in QC LDPC Codes

- How to identify cycles in QC LDPC codes from their parity check matrix
- For weight-I QC LDPC codes → For higher weight QC LDPC codes
- Review of an obstacle in constructing QC LDPC codes with good girth (The higher weight QC LDPC codes with certain characteristics are inevitable to have short cycles)
- HQC LDPC codes overcome the obstacle
- Applying a lifting transformation into HQC codes to obtain high-girth QC codes.

*A. Finding Cycles in Weight-I QC LDPC codes*

- **Cycle**

A cycle is a path through nodes in the Tanner graph of a code. It alternates between check and variable nodes, and starts and ends at the same node.

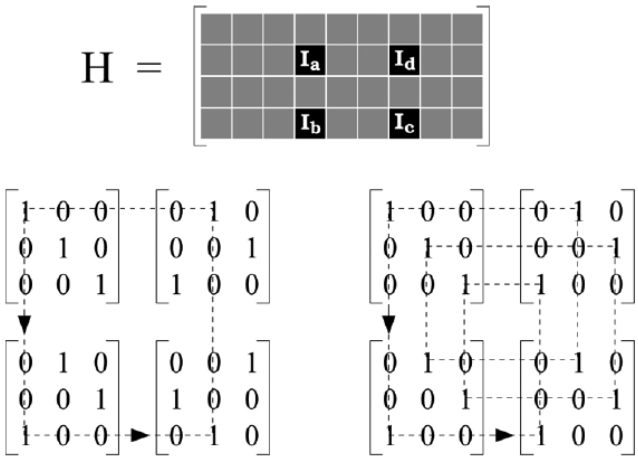



Fig. 3. A parity-check matrix and four $3 \times 3$ circulant permutation matrices ($\mathbf{I}_a$, $\mathbf{I}_b$, $\mathbf{I}_c$ and $\mathbf{I}_d$) selected from it. One set of parameters (lower left, $a = 0$, $b = 2$, $c = 1$, $d = 2$) results in a cycle of length four. An alternate set (lower right, $a = 0$, $b = c = d = 2$) results in a cycle of length twelve.

- **Condition of the cycles for weight-I QC LDPC codes**

They specify the conditions on the $\{a,b,c,d\}$ developed in [33] that result in a cycle. **Calculate an alternating sum of the shift indices associated with neighboring permutation matrices along a given path (every odd shift index is subtracted rather than added)**. For example, consider the left-hand path of Fig. 3. The sum is $-a+b-c+d$ . Only if the differences sum to zero (mod-$p$) at the end of the path will the path return to the same variable node in the starting permutation matrix, thereby forming a cycle. For the example of Fig. 3, the condition for a length-four cycle to exist is:

$$(-a+b-c+d) \mod p = 0,$$

which is satisfied for $a=0, b=2, c=1, d=2$, but is not satisfied by $a=0, b=c=d=2$.

*B. Finding Cycles in Higher Weight QC LDPC codes*

Let us take the matrix $H(x)$ of Exmple 1,

$$H(x)=\begin{bmatrix} x^0 & x^0 & x^0 \\ 0 & x^0 & x^1+x^2 \end{bmatrix}.$$

Now, consider the following ordered series:

$$O=\{(1,2),(2,2),(2,3),(2,3),(2,3),(1,3)\}$$

where each pair $(j,l)$ in $O$ satisfies $1\le j\le J=2$ and $1\le l\le L=3$. This ordered series specifies a sequence of rectilinear moves through $H(x)$.

To specify a candidate cycle through the Tanner graph, we associate a coefficient index *s* with each pair $(j,l)$ in $O$, such that $c_s[j,l]\neq 0$. They denote this series of coefficient indices by $S$. **The candidate cycle will be a cycle if the alternating sum of coefficient indices in *S* modulo *p* equals zero**.

In their example, consider the two following choices for the respective (ordered) sets of coefficient indices:

$$S_a=\{0,0,1,2,1,0\}$$
$$S_b=\{0,0,2,1,2,0\}.$$

Each of these choices corresponds to a cycle of length-6 through the Tanner graph of the code. The alternating sums modulo-3 can be verified to be equal to zero. Respectively, these sums are

$$(-0+0-1+2-1+0)\bmod 3=0$$
$$(-0+0-2+1-2+0)\bmod 3=0.$$

### *C. Invertible Cycles in Higher Weight QC LDPC codes*

An important theorem proven by Smarandache and Vontobel [35] states that any weight-III QC LDPC code will inevitably contain cycles of length six. Suppose that, without loss of generality, the polynomial $h_{j,l}(x)$ is weight-III and has the form $x^a + x^b + x^c$. To see that a cycle must exist using thier notation, choose the length-six ordered series

$$O = \{(j,l),(j,l),(j,l),(j,l),(j,l),(j,l)\},$$

and choose $S = \{a,b,c,a,b,c\}$. We find that

$$(-a+b-c+a-b+c) \mod p = 0,$$

for any value of *p*.

One can also prove (see [35, Th. 17] or [27, Example 3.3]) that a parity check matrix of a weight-II QC LDPC code that contains two weight-2 polynomials in the same row or the same column will inevitably have eight-cycles. To see this, suppose the two weight-2 polynomials are in the same row $j$, but in two different columns $l_1 \neq l_2$. Let $h_{j,l_1} = x^a + x^b$ and $h_{j,l_2} = x^c + x^d$. Consider the length-eight ordered series

$$O = \{(j,l_1),(j,l_1),(j,l_2),(j,l_2),(j,l_1),(j,l_1),(j,l_2),(j,l_2)\}$$

and choose

$$S = \{a,b,c,d,b,a,d,c\}.$$

We again find that

$$(-a+b-c+d-b+a-d+c) \mod p = 0,$$

regardless of the value of *p*.

These inevitable six-cycles and eight-cycles appear to put serious limitations on what protographs can be converted into quasi-cyclic codes with high girth.

## V. HQC LDPC CODES

- To solve the problem of invertible short cycles, they introduce HQC LDPC codes.
- An HQC LDPC code is formed from "levels" that each has a quasi-cyclic structure. The structure can be specified in two forms:
  1) Polynomial parity check matrices
  2) Tree structure
- They connect the hierarchical structure to a particular sequence of liftings of a base graph.

### *A. Parity Check Matrices of HQC LDPC Codes*

*Example 2*: Consider the polynomial parity check matrix specified in (18) with $p=8$. Because the highest weight of any of the polynomial entries is 2, and because there are 12 columns in the matrix, this is a length-96 weight-II QC LDPC code

$$\mathbf{H}(x)=\left[\begin{array}{ccc|ccc|ccc|ccc} x^6 & 0 & x^1+x^7 & 0 & x & 1+x^2 & 0 & 0 & 0 & x^6 & x^3 & 1 \\ x^1+x^7 & x^6 & 0 & 1+x^2 & 0 & x & 0 & 0 & 0 & 1 & x^6 & x^3 \\ 0 & x^1+x^7 & x^6 & x & 1+x^2 & 0 & 0 & 0 & 0 & x^3 & 1 & x^6 \\ \hline 0 & x & 1+x^2 & x^6 & 0 & x^1+x^7 & x^6 & x^3 & 1 & 0 & 0 & 0 \\ 1+x^2 & 0 & x & x^1+x^7 & x^6 & 0 & 1 & x^6 & x^3 & 0 & 0 & 0 \\ x & 1+x^2 & 0 & 0 & x^1+x^7 & x^6 & x^3 & 1 & x^6 & 0 & 0 & 0 \end{array}\right] \tag{18}$$

$$\mathbf{H}(x,y)=\left[\begin{array}{c|c|c|c} x^6+(x+x^7)y & (1+x^2)y+xy^2 & 0 & x^6+y+x^3y^2 \\ \hline (1+x^2)y+xy^2 & x^6+(x+x^7)y & x^6+y+x^3y^2 & 0 \end{array}\right] \tag{19}$$

$$\mathbf{H}(x,y,z)=\left[x^6+(x+x^7)y+((1+x^2)y+xy^2)z \;\middle|\; (x^6+y+x^3y^2)z\right] \tag{20}$$

Each of the three contractions of the parity check matrix of this code into the polynomial parity check matrices represented by (18), (19), and (20), corresponds to a "level" in the hierarchy of this **three-level** HQC LDPC code.

We now present a formal definition of the family of *K*-level HQC LDPC codes which generalizes our example.

*Definition 1*: An HQC LDPC code with K levels is defined by a $J_{[k]} \times L_{[k]}$ multivariate polynomial parity check matrix $H(\cdot)$ in *K* variables. The entry in the *j*th row and *l*th column of $H(\cdot)$, $1 \le j \le J_{[k]}$, $1 \le l \le L_{[k]}$ is a *K*-variate polynomial $h_{j,l}(\cdot,\cdots,\cdot)$ over the *K* variables $x_{[1]},\ldots,x_{[k]}$. With these definitions, we defined the code by the $J_{[k]} \cdot L_{[k]}$ polynomials

$$h_{j,l}(x_{[1]},\ldots,x_{[K]}) = \sum_{s_K=0}^{p_{[K]}-1} \cdots \sum_{s_1=0}^{p_{[1]}-1} c_{s_1,\ldots,s_K}[j,l] \left( \prod_{k=1}^{K} x_{[k]}^{s_k} \right).$$

Example) We can rewrite the term $h_{1,1}(x,y,z)$ of (20) as

$$\mathbf{H}(x,y,z) = \left[ x^6 + (x+x^7)y + ((1+x^2)y + xy^2)z \;\middle|\; (x^6 + y + x^3y^2)z \right] \tag{20}$$

$$\begin{aligned} & h_{1,1}(x_{[1]},x_{[2]},x_{[3]}) \\ &= x_{[1]}^6 + \left(x_{[1]} + x_{[1]}^7\right) x_{[2]} + \left(\left(1 + x_{[1]}^2\right) x_{[2]} + x_{[1]} x_{[2]}^2\right) x_{[3]} \\ &= \sum_{s_3=0}^{1} \sum_{s_2=0}^{2} \sum_{s_1=0}^{7} c_{s_1,s_2,s_3}[1,1] x_{[1]}^{s_1} x_{[2]}^{s_2} x_{[3]}^{s_3}, \end{aligned}$$

where all coefficients $c_{s1,s2,s3}[1,1]$ are zero except for

$$c_{6,0,0}[1,1] = c_{1,1,0}[1,1] = c_{7,1,0}[1,1] = c_{0,1,1}[1,1] = c_{2,1,1}[1,1] = c_{1,2,1}[1,1] = 1.$$

### *B. Tree Structure of HQC LDPC Codes*

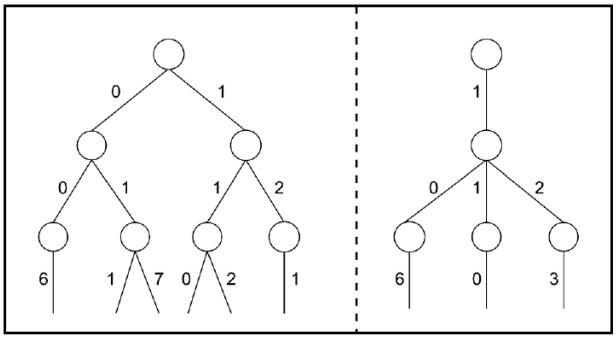



Fig. 4. Example of the tree structure of a family of three-level HQC LDPC codes. The left-hand tree is $\mathbf{T}_{1,1}$, and the right-hand tree is $\mathbf{T}_{1,2}$.

**Remained contests**

- **Finding cycles in HQC LDPC codes**
- **Inevitable cycles in HQC LDPC codes**

- **Proposing girth maximization using hill climbing**

- **Design of restricted two-level HQC LDPC codes (The additional "restriction" is that the weight of the first(lowest) level must be one)**
  **→The restricted two-level HQC LDPC codes can considered weight-I QC LDPC codes**
- **Squaring sets of trees to eliminate inevitable cycles**

- **Design of high-girth codes**

**Numerical Result**

In Figs. 9, 10, and 11, they plot the respective error rate performance of the three codes for the binary symmetric channel (BSC). For purposes of comparison, they plot analogous results for some randomly generated girth-6 QC LDPC codes. These codes have the same length, same rate, and same nonzero positions in the base matrix (i.e., same protograph structure) as the girth-10 and girth-8 codes to which they are compared.

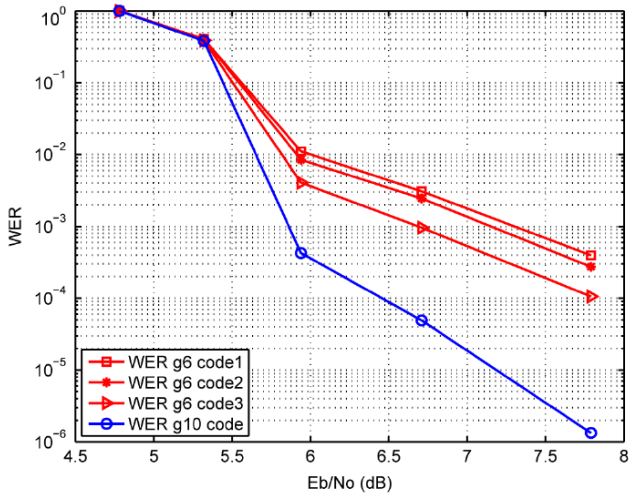



Fig. 9. Word-error rate plots of the Gallager-B algorithm for the rate-0.45, length-8000 girth-6 and girth-10 QC LDPC codes over the BSC.

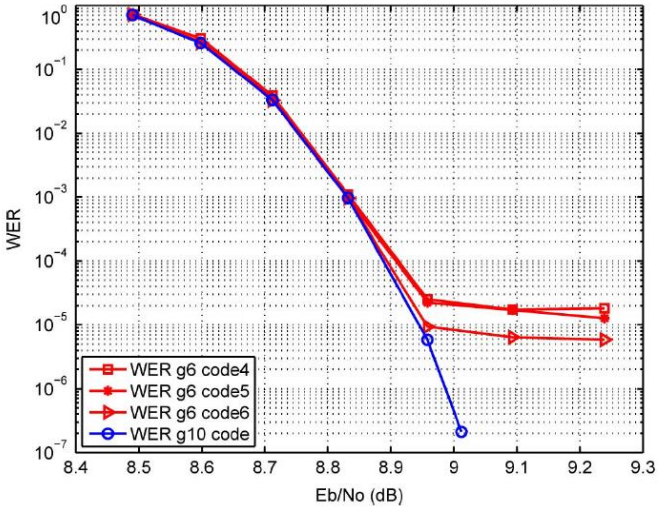



Fig. 10. Word-error rate plots of the Gallager-B algorithm for the rate-1/3, length-24000 girth-6 and girth-10 QC LDPC codes over the BSC.

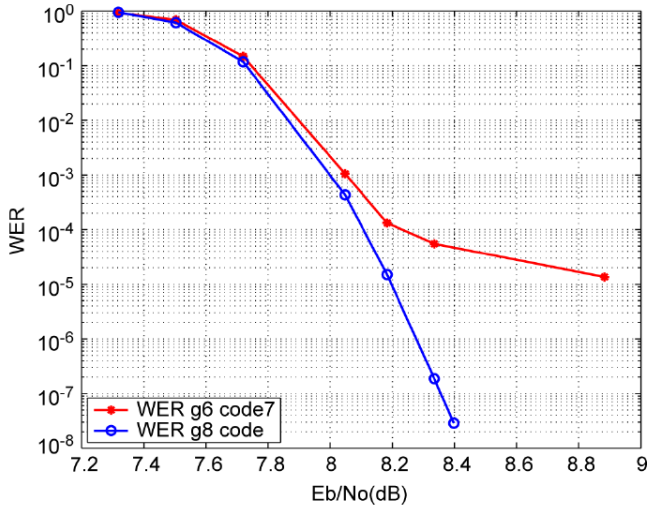



Fig. 11. Word-error rate plots of the Gallager-B algorithm for the rate-0.7, length-28000 girth-6 and girth-8 QC LDPC codes over the BSC.

- High girth or High rate → Low error floor